vSphere 인증

업데이트 3

VMware vSphere 8.0
VMware ESXi 8.0
vCenter Server 8.0

vmware
by Broadcom

VMware by Broadcom 웹 사이트

https://docs.vmware.com/kr에서 최신 기술 문서를 찾을 수 있습니다.

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

목차

"vSphere 인증" 정보

"vSphere 인증" 설명서는 인증서 관리 및 vCenter Single Sign-On 구성과 같은 일반적인 작업을 수행하는 데 유용한 정보를 제공합니다.

VMware는 포용성을 중요하게 생각합니다. 고객, 파트너 및 내부 커뮤니티 안에서 이러한 원칙을 강화하기 위해 포용성 있는 언어를 사용하여 컨텐츠를 만듭니다.

"vSphere 인증" 에서는 vCenter Server및 관련 서비스에 대한 인증서를 관리하고 vCenter Single Sign-On으로 인증을 설정하는 방법을 설명합니다.

표 1-1. "vSphere 인증" 하이라이트

항목	컨텐츠 하이라이트
인증 시작	■ 인증 서비스 관리 ■ vCenter Server 관리 인터페이스를 사용하여 vCenter Server 관리
vSphere 보안 인증서	■ 인증서 모델 및 인증서 교체 옵션 ■ UI에서 인증서 교체(간단한 경우) ■ Certificate Manager 유틸리티를 사용한 인증서 교체 ■ CLI를 사용한 인증서 교체(복잡한 환경) ■ 인증서 관리 CLI 참조
vCenter Single Sign-On으로 vSphere 인증	■ 인증 프로세스의 아키텍처 ■ 도메인 사용자 인증을 위한 ID 소스를 추가하는 방법 ■ 2단계 인증 ■ 사용자,그룹 및 정책 관리 ■ vCenter Server ID 제공자 페더레이션

Platform Services Controller 변경 사항

vSphere 7.0부터 vCenter Server를 새로 배포하거나 vCenter Server 7.0으로 업그레이드하려면 vCenter Server 실행을 위해 최적화된 미리 구성된 가상 시스템인 vCenter Server Appliance를 사용해야 합니다. 새 vCenter Server에는 인증, 인증서 관리, 태그 및 라이센싱을 포함하여 기능 및 워크플로를 보존하는 모든 Platform Services Controller 서비스가 포함되어 있습니다. 더 이상 외부 Platform Services Controller를 배포할 필요가 없으며 배포할 수도 없습니다. 모든 Platform Services Controller 서비스가 vCenter Server에 통합되고 배포 및 관리가 간소화됩니다.

이제 이러한 서비스는 vCenter Server의 일부이며 더 이상 Platform Services Controller의 일부로 설명되지 않습니다. vSphere 7.0에서 "vSphere 인증" 자료는 "Platform Services Controller 관리" 자료를 대체합니다. 새 자료에는 인증 및 인증서 관리에 대한 모든 정보가 포함되어 있습니다. 기존의 외부 Platform Services Controller를 사용하는 vSphere 6.5 및 6.7 배포에서 vCenter Server Appliance를 사용하는 vSphere 7.0으로 업그레이드하거나 마이그레이션하는 데 대한 자세한 내용은 "vSphere 업그레이드" 설명서를 참조하십시오.

관련 설명서

함께 제공되는 문서인 "vSphere 보안" 에는 사용 가능한 보안 기능과 공격으로부터 환경을 보호하기 위해 취할 수 있는 조치와 사용 권한을 설정하는 방법이 설명되어 있으며 권한에 대한 참조가 포함되어 있습니다.

VMware는 이러한 문서 외에도 각 vSphere 릴리스에 대해 "vSphere 보안 구성 가이드" (이전 명칭: "강화 지침")를 https://core.vmware.com/security에 게시합니다. "vSphere 보안 구성 가이드" 에는 고객이 설정해야 하거나 설정할 수 있는 보안 설정 및 고객이 감사를 수행하여 기본값으로 유지해야 하는 VMware 제공 보안 설정에 대한 지침이 나와 있습니다.

대상 사용자

이 정보는 vCenter Server 인증을 구성하고 인증서를 관리하려는 관리자를 위한 것입니다. 이 정보는 가상 시스템 기술과 데이터 센터 운영에 대해 잘 알고 있는 숙련된 Linux 시스템 관리자를 대상으로 작성되었습니다.

vSphere 인증서 관리 및 인증 시작

1

vSphere는 vCenter Server 및 ESXi 구성 요소 모두에 대한 인증서를 관리하고 vCenter Single Sign-On으로 인증을 관리하기 위한 공통 인프라 서비스를 제공합니다.

vSphere 인증서를 관리하는 방법

기본적으로 vSphere를 사용하면 VMCA(VMware Certificate Authority)를 통해 vCenter Server 구성 요소 및 ESXi 호스트를 프로비저닝할 수 있습니다. 또한 VECS(VMware Endpoint Certificate Store)에 저장된 사용자 지정 인증서를 사용할 수도 있습니다. 자세한 내용은 vSphere 인증서 관리에 사용할 수 있는 옵션의 내용을 참조하십시오.

vCenter Single Sign-On이란?

vCenter Single Sign-On을 사용하면 안전한 토큰 메커니즘을 통해 vSphere 구성 요소가 서로 통신할 수 있습니다. vCenter Single Sign-On에서는 이해가 필요한 몇 가지 중요한 용어와 정의가 사용됩니다.

표 1-1. vCenter Single Sign-On 용어집

용어	정의
주체	사용자와 같이 인증될 수 있는 엔티티입니다.
ID 제공자	ID 소스를 관리하고 주체를 인증하는 서비스입니다. 예: Microsoft AD FS(Active Directory Federation Services) 및 vCenter Single Sign-On.
ID 소스(디렉토리 서비스)	주체를 저장하고 관리합니다. 주체는 이름, 주소, 이메일, 그룹 멤버 자격과 같이 특정 사용자 또는 서비스에 대한 특성 모음으로 구성됩니다. 예: Microsoft Active Directory 및 VMware Directory Service(vmdir).
인증	누군가 또는 무언가가 실제로 자신을 누구로 또는 무엇으로 선언할지 결정하는 방법입니다. 예를 들어 사용자는 스마트 카드, 사용자 이름, 올바른 암호 등과 같은 자신의 자격 증명을 제공할 때 인증됩니다.
권한 부여	개체 주체가 액세스할 수 있는 대상을 확인하는 프로세스입니다.

표 1-1. vCenter Single Sign-On 용어집 (계속)

용어	정의
토큰	지정된 주체에 대한 ID 정보를 구성하는 서명된 데이터의 모음입니다. 토큰에는 이메일 주소, 전체 이름과 같이 주체에 대한 기본 정보를 비롯하여 토큰 유형에 따라 주체의 그룹 및 역할도 포함될 수 있습니다.
vmdir	VMware Directory Service. 사용자 ID, 그룹 및 구성 데이터가 들어 있는 vCenter Server의 내부(로컬) LDAP 저장소입니다.
OAuth 2.0	주체의 자격 증명을 노출하지 않고 주체와 웹 서비스 간에 정보를 교환할 수 있는 개방형 권한 부여 표준입니다.
OIDC(OpenID Connect)	사용자 식별 정보로 OAuth를 보강하는 OAuth 2.0 기반 인증 프로토콜입니다. 인증 서버가 OAuth 인증 중에 액세스 토큰과 함께 반환하는 ID 토큰으로 표시됩니다. vCenter Server는 AD FS(Active Directory Federation Services), Okta, Microsoft Entra ID 및 PingFederate와 상호 작용할 때 OIDC 기능을 사용합니다.
SCIM(System for Cross-domain Identity Management)	ID 도메인 또는 IT 시스템 간의 사용자 ID 정보 교환을 자동화하기 위한 표준입니다.
VMware Identity Services	버전 8.0 업데이트 1부터 VMware Identity Services는 외부 ID 제공자에 대한 ID 페더레이션에 사용할 수 있는 vCenter Server 내의 기본 제공 컨테이너입니다. vCenter Server 내에서 독립적인 ID 브로커 역할을 하며 자체 API 집합이 함께 제공됩니다. 현재 VMware Identity Services는 Okta, Microsoft Entra ID 및 PingFederate를 외부 ID 제공자로 지원합니다.
테넌트	VMware Identity Services 개념입니다. 테넌트는 하나의 동일한 가상 환경에서 데이터를 다른 테넌트의 데이터와 논리적으로 분리합니다.
JWT(JSON Web Token)	OAuth 2.0 규격에 의해 정의된 토큰 형식입니다. JWT 토큰은 주체에 대한 인증 및 권한 부여 정보를 전달합니다.
신뢰 당사자	신뢰 당사자는 ID 관리를 위해 권한 부여 서버인 VMware Identity Services 또는 AD FS에 "의존"합니다. 예를 들어 vCenter Server는 페더레이션을 통해 VMware Identity Services 또는 AD FS에 대한 신뢰 당사자 트러스트를 설정합니다.
SAML(Security Assertion Markup Language)	vCenter Server에서 사용되는 당사자 간에 인증 및 권한 부여 데이터를 교환하기 위한 XML 기반 개방형 표준입니다. 주체는 vCenter Single Sign-On에서 SAML 토큰을 가져온 다음, 세션 식별자를 위해 vSphere Automation API 끝점으로 보냅니다.

vCenter Single Sign-On 인증 유형이란?

vCenter Single Sign-On은 기본 제공 vCenter Server ID 제공자 또는 외부 ID 제공자가 관련되어 있는지 여부에 따라 서로 다른 인증 유형을 사용합니다.

표 1-2. vCenter Single Sign-On 인증 유형

인증 유형	ID 제공자 역할을 수행하는 것은 무엇입니까?	vCenter Server가 암호를 처리합니까?	설명
토큰 기반 인증	외부 ID 제공자. 예: AD FS.	아니요	vCenter Server는 특정 프로토콜을 통해 외부 ID 제공자에 연결하고 특정 사용자 ID를 나타내는 토큰을 가져옵니다.
단순 인증	vCenter Server	예	사용자 이름과 암호가 vCenter Server에 직접 전달되고 여기에서 해당 ID 소스를 통해 자격 증명을 검증합니다.

다음으로 아래 항목을 읽으십시오.

- vCenter Server 인증서 관리
- vCenter Server 인증 서비스 관리
- vCenter Server 관리

vCenter Server 인증서 관리

vCenter Server 인증서는 vSphere Client에서 관리하거나 API, 스크립트 또는 CLI를 사용하여 관리합니다.

다음 표에서는 vCenter Server 인증서를 관리하는 데 사용할 수 있는 인터페이스에 대해 설명합니다.

표 1-3. vSphere 인증서 관리를 위한 인터페이스

인터페이스	설명
vSphere Client	웹 인터페이스(HTML5 기반 클라이언트)입니다. vSphere Client를 사용하여 인증서 관리의 내용을 참조하십시오.
vSphere Automation API	"VMware vSphere Automation SDK 프로그래밍 가이드" 를 참조하십시오.
인증서 관리 유틸리티	CSR(인증서 서명 요청) 생성 및 인증서 교체를 지원하는 명령줄 도구입니다. vSphere Certificate Manager 유틸리티를 사용하여 인증서 관리의 내용을 참조하십시오.
인증서 및 디렉토리 서비스를 관리하기 위한 CLI	인증서, VECS(VMware Endpoint 인증서 저장소) 및 VMware Directory Service(vmdir) 관리를 위한 명령 집합입니다. 장 3 vSphere 인증서 및 서비스 CLI 명령 참조의 내용을 참조하십시오.

vSphere Client를 사용하여 vCenter Server 인증서 관리

vSphere Client에서 vCenter Server 인증서를 관리할 수 있습니다.

절차

1 로컬 vCenter Single Sign-On 도메인에서 관리자 권한을 가진 사용자로 vCenter Server에 로그인합니다.

기본 도메인은 vsphere.local입니다.

2 **관리**를 선택합니다.

3 **인증서**에서 **인증서 관리**를 클릭합니다.

다양한 인증서 유형에 대한 인증서 탭이 나타납니다.

4 인증서 세부 정보 보기, 인증서 갱신 또는 새로 고침, 신뢰할 수 있는 루트 인증서 추가와 같은 인증서 작업을 수행합니다.

자세한 내용은 vSphere Client를 사용하여 인증서 관리의 내용을 참조하십시오.

CLI를 사용하여 vCenter Server 인증서 관리

vCenter Server에는 CSR(인증서 서명 요청) 생성, 인증서 관리 및 서비스 관리를 위한 CLI가 포함되어 있습니다.

예를 들어 `certool` 명령을 사용하면 CSR을 생성하고 인증서를 교체할 수 있습니다.

CLI를 사용하여 vSphere Client에서는 지원하지 않는 관리 작업을 수행하거나 환경에 맞게 사용자 지정 스크립트를 생성할 수 있습니다.

표 1-4. vCenter Server 인증서 및 관련 서비스를 관리하기 위한 CLI

CLI	설명	링크
`certool`	인증서와 키를 생성하고 관리합니다. VMCA(VMware Certificate Authority)의 일부입니다.	certool 초기화 명령 참조
`vecs-cli`	VMware Certificate Store 인스턴스의 컨텐츠를 관리합니다. VMAFD(VMware 인증 프레임워크 대몬)의 일부입니다.	vecs-cli 명령 참조
`dir-cli`	VMware Directory Service에서 인증서를 만들고 업데이트합니다. VMAFD의 일부입니다.	dir-cli 명령 참조
`sso-config`	STS(Security Token Service) 인증서를 업데이트합니다.	명령줄을 사용하여 vCenter Server STS 인증서 교체
`service-control`	서비스를 시작, 중지 및 나열하는 명령입니다.	다른 CLI 명령을 실행하기 전에 이 명령을 실행하여 서비스를 중지합니다.

사전 요구 사항

vCenter Server에 대한 SSH 로그인을 사용하도록 설정합니다. SSH 로그인 활성화 및 비활성화를 위해 vCenter Server 관리 인터페이스(`https://vcenter_server_ip:5480`)에서 **액세스** 탭을 사용할 수 있습니다.

절차

1 vCenter Server 셸에 로그인합니다.

보통 루트 사용자 또는 관리자 사용자여야 합니다. 자세한 내용은 vSphere CLI 실행을 위한 필수 권한 항목을 참조하십시오.

2 다음의 기본 위치 중 하나에서 CLI에 액세스할 수 있습니다.

필요한 권한은 수행할 작업이 무엇인지에 따라 다릅니다. 경우에 따라 중요한 정보를 보호하기 위해 암호를 두 번 입력하라는 메시지가 표시됩니다.

```
/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` 명령에는 경로를 입력하지 않아도 됩니다.

자세한 내용은 vSphere 인증서 수동 교체의 내용을 참조하십시오.

vCenter Server 인증 서비스 관리

vSphere Client에서 또는 CLI를 사용하여 인증 서비스를 관리합니다. API를 사용하여 vCenter Server ID 제공자 페더레이션 구성 프로세스를 관리할 수도 있습니다.

다양한 인터페이스를 사용하여 vCenter Server 인증을 관리할 수 있습니다.

표 1-5. vCenter Server 인증 서비스 관리를 위한 인터페이스

인터페이스	설명
vSphere Client	웹 인터페이스(HTML5 기반 클라이언트)입니다.
API	vCenter Server ID 제공자 페더레이션 구성 프로세스를 관리합니다.
`sso-config`	vCenter Server 기본 제공 ID 제공자 구성을 위한 명령줄 유틸리티입니다.

vSphere Client를 사용하여 vCenter Server 인증 서비스 관리

vSphere Client에서 vCenter Server 인증 서비스를 관리할 수 있습니다.

절차

1 로컬 vCenter Single Sign-On 도메인에서 관리자 권한을 가진 사용자로 vCenter Server에 로그인합니다.

기본 도메인은 vsphere.local입니다.

2 **관리**를 선택합니다.

3 **Single Sign-On**에서 **구성**을 클릭하여 ID 제공자를 관리하고 암호 및 잠금 정책을 구성합니다.

자세한 내용은 장 4 vCenter Single Sign-On으로 vSphere 인증의 내용을 참조하십시오.

스크립트를 사용하여 vCenter Server 인증 서비스 관리

vCenter Server에는 인증 서비스 관리를 위한 유틸리티인 `sso-config`가 포함되어 있습니다.

vSphere Client에서 지원하지 않는 관리 작업을 위해 `sso-config` 유틸리티를 사용하거나 현재 환경에 맞게 사용자 지정 스크립트를 생성할 수 있습니다.

표 1-6. 인증 및 연결된 서비스를 관리하기 위한 CLI

CLI	설명	링크
`sso-config`	vCenter Server 기본 제공 ID 제공자 구성을 위한 명령줄 유틸리티입니다.	`sso-config.sh -help`를 실행하여 `sso-config` 도움말을 참조하거나 VMware 기술 자료 문서(https://kb.vmware.com/s/article/67304)에서 사용 예를 참조하십시오.
`service-control`	서비스를 시작, 중지 및 나열하는 명령입니다.	다른 CLI 명령을 실행하기 전에 이 명령을 실행하여 서비스를 중지합니다. `service-control` 명령에는 경로를 지정하지 않아도 됩니다.

사전 요구 사항

vCenter Server에 대한 SSH 로그인을 사용하도록 설정합니다. SSH 로그인 활성화 및 비활성화를 위해 vCenter Server 관리 인터페이스(`https://vcenter_server_ip:5480`)에서 **액세스 설정** 탭을 사용할 수 있습니다.

절차

1 vCenter Server 셸에 로그인합니다.

보통 루트 사용자 또는 관리자 사용자여야 합니다. 자세한 내용은 vSphere CLI 실행을 위한 필수 권한 항목을 참조하십시오.

2 다음 기본 위치에서 `sso-config` 유틸리티에 액세스합니다.

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

필요한 권한은 수행할 작업이 무엇인지에 따라 다릅니다. 경우에 따라 중요한 정보를 보호하기 위해 암호를 두 번 입력하라는 메시지가 표시됩니다.

vCenter Server 관리

vCenter Server 관리 인터페이스 또는 vCenter Server 셸에서 vCenter Server를 관리할 수 있습니다.

vCenter Server 관리에 대한 자세한 내용은 "vCenter Server 구성" 항목을 참조하십시오.

표 1-7. vCenter Server 관리를 위한 인터페이스

인터페이스	설명
vCenter Server 관리 인터페이스	이 인터페이스를 사용하여 시스템 설정을 재구성합니다. 관리 인터페이스를 사용하여 vCenter Server 관리의 내용을 참조하십시오.
vCenter Server 셸	VMCA, VECS 및 VMDIR에서 서비스 관리 작업을 수행하려면 이 명령줄 인터페이스를 사용합니다. vSphere Certificate Manager 유틸리티를 사용하여 인증서 관리 및 장 3 vSphere 인증서 및 서비스 CLI 명령 참조 항목을 참조하십시오.

관리 인터페이스를 사용하여 vCenter Server 관리

vCenter Server 관리 인터페이스를 사용하여 시스템 설정을 구성할 수 있습니다.

vCenter Server 관리 인터페이스 설정에는 시간 동기화, 네트워크 설정 및 SSH 로그인 설정이 포함됩니다. 루트 암호를 변경하고, 장치를 Active Directory 도메인에 가입시키고, Active Directory 도메인에서 탈퇴할 수도 있습니다.

참고 **네트워킹** 창에서 가상 NIC 0은 관리 트래픽용으로 예약됩니다. 이 트래픽은 NIC 0에서 다른 NIC로 다시 할당할 수 없습니다. VCHA를 사용하는 경우 이 트래픽은 NIC 1을 사용합니다. vCenter Server Appliance에 NIC를 추가할 수 있습니다. VMware 기술 자료 문서(https://kb.vmware.com/article/2147155)를 참조하십시오.

절차

1 브라우저에서 웹 인터페이스(`https://vcenter_server_ip:5480`)로 이동합니다.

2 신뢰할 수 없는 SSL 인증서에 대한 주의 메시지가 표시되면 회사의 보안 정책 및 현재 사용 중인 브라우저에 따라 문제를 해결합니다.

3 root로 로그인합니다.

기본 루트 암호는 vCenter Server를 배포할 때 설정한 루트 암호입니다.

결과

vCenter Server 관리 인터페이스의 [요약] 페이지가 표시됩니다.

vCenter Server 셸을 사용하여 vCenter Server 관리

vCenter Server 셸에서 서비스 관리 유틸리티와 CLI를 사용할 수 있습니다. TTY1을 사용하여 콘솔에 로그인하거나 SSH를 사용하여 셸에 연결할 수 있습니다.

절차

1 필요한 경우 SSH 로그인을 활성화합니다.

   a vCenter Server 관리 인터페이스(https://*vcenter_server_ip*:5480)에 로그인합니다.

   b 탐색기에서 **액세스**를 선택하고 **편집**을 클릭합니다.

   c **SSH 로그인 활성화**를 설정하고 **확인**을 클릭합니다.

   동일한 단계에 따라 vCenter Server에 대해 Bash 셸을 활성화할 수 있습니다.

2 셸에 액세스합니다.

   - vCenter Server 콘솔에 직접 액세스할 수 있는 경우에는 **로그인**을 선택한 후 Enter 키를 누릅니다.
   - 원격으로 연결하려면 SSH 또는 다른 원격 콘솔 연결을 사용하여 vCenter Server에 대한 세션을 시작합니다.

3 vCenter Server를 처음 배포할 때 설정한 암호를 사용하여 루트로 로그인합니다.

   루트 암호를 변경한 경우에는 새 암호를 사용합니다.

Active Directory 도메인에 vCenter Server 추가

vCenter Server에 Active Directory ID 소스를 추가하려면 vCenter Server를 Active Directory 도메인에 가입시켜야 합니다.

vCenter Server ID 제공자 페더레이션 또는 LDAPS를 통한 Active Directory를 사용할 수 없는 경우 vCenter Server는 IWA(통합 Windows 인증)을 지원합니다. IWA를 사용하려면 vCenter Server를 Active Directory 도메인에 가입시켜야 합니다.

절차

1 vSphere Client를 사용하여, 로컬 vCenter Single Sign-On 도메인(기본적으로 vsphere.local)에서 관리자 권한을 가진 사용자로 vCenter Server에 로그인합니다.

2 **관리**를 선택합니다.

3 **Single Sign On**을 확장하고 **구성**을 클릭합니다.

4 **ID 제공자** 탭에서 **Active Directory 도메인**을 클릭합니다.

5 **AD 가입**을 클릭하고 도메인, 조직 구성 단위(선택 사항) 및 사용자 이름과 암호를 입력한 후 **가입**을 클릭합니다.

6 vCenter Server을 다시 시작합니다.

다음에 수행할 작업

가입된 Active Directory 도메인의 사용자 및 그룹을 연결하려면 가입된 도메인을 vCenter Single Sign-On ID 소스로 추가합니다. vCenter Single Sign-On ID 소스 추가 또는 편집의 내용을 참조하십시오.

vSphere 보안 인증서

2

vSphere는 인증서를 사용하여 통신을 암호화하고 서비스를 인증하며 토큰에 서명하여 보안을 제공합니다.

vSphere에서 인증서를 사용하는 방법

vSphere는 다음과 같은 용도로 인증서를 사용합니다.

- vCenter Server 및 ESXi 호스트와 같은 두 노드 간의 통신을 암호화합니다.
- vSphere 서비스를 인증합니다.
- 토큰 서명과 같은 내부 작업을 수행합니다.

VMware Certificate Authority란?

vSphere의 내부 인증 기관인 VMCA(VMware Certificate Authority)는 vCenter Server 및 ESXi에 필요한 모든 인증서를 제공합니다. VMCA는 모든 vCenter Server 호스트에 설치되며 다른 수정을 할 필요 없이 솔루션을 즉시 보호합니다. 이 기본 구성을 유지할 경우 인증서 관리의 운영 오버헤드가 가장 낮습니다. vSphere는 이러한 인증서가 만료될 때마다 인증서를 갱신하는 메커니즘을 제공합니다.

또한 vSphere는 특정 인증서를 사용자 고유의 인증서로 교체하는 메커니즘을 제공합니다. 하지만 인증서 관리 오버헤드를 최소화하려면 노드 간에서 암호화를 제공하는 SSL 인증서만 교체하십시오.

vSphere 인증서 관리에 사용할 수 있는 옵션

인증서 관리에는 다음과 같은 옵션이 권장됩니다.

표 2-1. vSphere 인증서 관리에 권장되는 옵션

모드	설명	장점
VMCA 기본 인증서	VMCA는 vCenter Server 및 ESXi 호스트를 위한 모든 인증서를 제공합니다.	가장 간단하고 오버헤드 가장 적습니다. VMCA는 vCenter Server 및 ESXi 호스트에 대한 인증서 수명 주기를 관리합니다.
VMCA 기본 인증서와 외부 SSL 인증서(하이브리드 모드)	vCenter Server SSL 인증서를 교체하고, VMCA가 솔루션 사용자 및 ESXi 호스트의 인증서를 관리하게 할 수 있습니다. 필요한 경우 보안이 중요한 배포에서 ESXi 호스트 SSL 인증서를 교체할 수 있습니다.	간단하고 안전합니다. VMCA가 내부 인증서를 관리하지만 사용자는 회사에서 승인한 SSL 인증서를 사용하고 브라우저에서 이러한 인증서를 신뢰하게 하는 이점을 누릴 수 있습니다.

vSphere 인증서를 교체하는 데 사용할 수 있는 도구

다음 옵션을 사용하여 기존 인증서를 교체할 수 있습니다.

표 2-2. 여러 가지 vSphere 인증서 교체 방법

옵션	자세한 내용은
vSphere Client를 사용합니다.	vSphere Client를 사용하여 인증서 관리
vSphere Automation API를 사용하여 인증서의 수명 주기를 관리합니다.	"VMware vSphere Automation SDK 프로그래밍 가이드"
명령줄에서 vSphere Certificate Manager 유틸리티를 사용합니다.	vSphere Certificate Manager 유틸리티를 사용하여 인증서 관리
CLI 명령을 사용하여 수동으로 인증서를 교체합니다.	장 3 vSphere 인증서 및 서비스 CLI 명령 참조

다음으로 아래 항목을 읽으십시오.

- 다양한 솔루션 경로에 대한 vSphere 인증서 요구 사항
- vSphere 인증서 관리
- vSphere Client를 사용하여 인증서 관리
- vSphere Certificate Manager 유틸리티를 사용하여 인증서 관리
- vSphere 인증서 수동 교체

다양한 솔루션 경로에 대한 vSphere 인증서 요구 사항

인증서 요구 사항은 VMCA(VMware Certificate Authority)를 중간 CA(인증 기관)로 사용하는지, 아니면 사용자 지정 인증서를 사용하는지에 따라 달라집니다. 시스템 인증서에 대한 요구 사항도 다릅니다.

인증서 변경을 시작하기 전에 vSphere 환경의 모든 노드에서 시간이 동기화되는지 확인합니다.

참고 vSphere는 서버 인증을 위해 RSA 인증서만 배포하고 ECDSA 인증서 생성을 지원하지 않습니다. vSphere는 다른 서버에서 제공한 ECDSA 인증서를 확인합니다. 예를 들어 vSphere가 syslog 서버에 연결되고 syslog 서버에 ECDSA 인증서가 있는 경우 vSphere는 해당 인증서 확인을 지원합니다.

가져온 모든 vSphere 인증서에 대한 요구 사항

- 키 크기: 2048비트(최소)~8192비트(최대)(PEM 인코딩) vSphere Client 및 API는 인증서 서명 요청을 생성할 때 키 크기를 여전히 최대 16384비트까지 수락합니다.

  참고 vSphere 8.0에서는 vSphere Client 또는 vSphere Certificate Manager를 사용할 때 최소 키 길이가 3072비트인 CSR만 생성할 수 있습니다. vCenter Server는 키 길이가 2048비트인 사용자 지정 인증서를 여전히 허용합니다. vSphere 8.0 업데이트 1 이상에서는 vSphere Client를 사용하여 키 길이가 2048비트인 CSR을 생성할 수 있습니다.

  참고 vSphere의 FIPS 인증서는 2048비트 및 3072비트의 RSA 키 크기만 검증합니다.

- PEM 형식. VMware는 PKCS8 및 PKCS1(RSA 키)을 지원합니다. 키가 VECS에 추가되면 추가된 키가 PKCS8로 변환됩니다.
- x509 버전 3
- SubjectAltName에는 DNS Name=*machine_FQDN*이 포함되어야 합니다.
- CRT 형식
- 다음과 같은 키 사용이 포함되어 있습니다. 디지털 서명, 키 암호화
- vpxd-extension 솔루션 사용자 인증서를 제외하는 경우 확장 키 사용이 비어 있거나 서버 인증을 포함할 수 있습니다.

vSphere는 다음 인증서를 지원하지 않습니다.

- 와일드카드가 있는 인증서.
- md2WithRSAEncryption, md5WithRSAEncryption, RSASSA-PSS, dsaWithSHA1, ecdsa_with_SHA1 및 sha1WithRSAEncryption 알고리즘은 지원되지 않습니다.
- vCenter Server용 사용자 정의 시스템 SSL 인증서를 생성할 때 서버 인증 및 클라이언트 인증은 지원되지 않으며 Microsoft CA(인증 기관) 템플릿을 사용할 때 제거해야 합니다. 자세한 내용은 VMware 기술 자료 문서 https://kb.vmware.com/s/article/2112009를 참조하십시오.

vSphere 인증서의 RFC 2253 규정 준수

인증서는 RFC 2253 규정을 준수해야 합니다.

vSphere Certificate Manager를 사용하여 CSR을 생성하지 않는 경우 CSR에 다음 필드가 포함되어 있어야 합니다.

문자열	X.500 특성 유형
CN	commonName
L	localityName
ST	stateOrProvinceName
O	organizationName
OU	organizationalUnitName
C	countryName
STREET	streetAddress
DC	domainComponent
UID	userid

vSphere Certificate Manager를 사용하여 CSR을 생성하는 경우 다음 정보를 묻는 메시지가 나타나며 vSphere Certificate Manager가 CSR 파일에 해당 필드를 추가합니다.

- 연결하는 vCenter Single Sign-On 도메인의 관리자 또는 dministrator@vsphere.local 사용자의 암호
- vSphere Certificate Manager가 `certool.cfg` 파일에 저장하는 정보. 대부분의 필드에서 기본값을 수락하거나 사이트별 값을 제공할 수 있습니다. 시스템의 FQDN은 필수 항목입니다.
  - administrator@vsphere.local의 암호
  - 두 글자의 국가 코드
  - 회사 이름
  - 조직 이름
  - 조직 구성 단위
  - 상태
  - 구/군/시
  - IP 주소(선택 사항)
  - 이메일
  - 호스트 이름, 즉 인증서를 교체하려고 하는 시스템의 정규화된 도메인 이름. 호스트 이름이 FQDN과 일치하지 않으면 인증서 교체가 올바르게 완료되지 않으며 환경이 불안정한 상태가 될 수 있습니다.
  - vSphere Certificate Manager를 실행하는 vCenter Server 노드의 IP 주소.

참고 OU(organizationalUnitName) 필드는 더 이상 필수가 아닙니다.

VMCA를 중간 CA(인증 기관)으로 사용하는 경우 인증서 요구 사항

VMCA를 중간 CA로 사용하는 경우 인증서가 다음 요구 사항을 충족해야 합니다.

인증서 유형	인증서 요구 사항

루트 인증서	■ vSphere Certificate Manager를 사용하여 CSR을 생성할 수 있습니다. Certificate Manager를 사용하여 CSR 생성 및 루트 인증서(중간 CA) 준비의 내용을 참조하십시오.
	■ CSR을 수동으로 생성하려는 경우에는 서명을 위해 보내는 인증서가 다음 요구 사항을 충족해야 합니다.
	■ 키 크기: 2048비트(최소)~8192비트(최대)(PEM 인코딩)
	■ PEM 형식. VMware는 PKCS8 및 PKCS1(RSA 키)을 지원합니다. 키가 VECS에 추가되면 해당 키가 PKCS8로 변환됩니다.
	■ x509 버전 3
	■ 루트 인증서에 대해 CA 확장을 true로 설정해야 하며 인증서 서명이 요구 사항 목록에 있어야 합니다. 예:
	`basicConstraints = critical,CA:true`
	`keyUsage = critical,digitalSignature,keyCertSign`
	■ CRL 서명을 사용하도록 설정해야 합니다.
	■ 확장 키 사용은 비워 두거나 서버 인증을 포함할 수 있습니다.
	■ 인증서 체인의 길이에 대한 명시적 제한이 없습니다. VMCA는 OpenSSL 기본값인 10개의 인증서를 사용합니다.
	■ 와일드카드 또는 2개 이상의 DNS 이름이 있는 인증서는 지원되지 않습니다.
	■ VMCA의 부수적인 CA를 생성할 수 없습니다.
	Microsoft CA(인증 기관)를 사용하는 예는 VMware 기술 자료 문서(https://kb.vmware.com/s/article/2112009)인 'vSphere 6.x에서 SSL 인증서 생성에 사용할 Microsoft CA(인증 기관) 템플릿 생성'을 참조하십시오.

시스템 SSL 인증서	vSphere Certificate Manager를 사용하여 CSR을 생성하거나 수동으로 CSR을 생성할 수 있습니다. CSR을 수동으로 생성하는 경우 앞의 "가져온 모든 vSphere 인증서에 대한 요구 사항" 목록에 나온 요구 사항을 충족해야 합니다. 또한 호스트의 FQDN을 지정해야 합니다.
솔루션 사용자 인증서	vSphere Certificate Manager를 사용하여 CSR을 생성하거나 수동으로 CSR을 생성할 수 있습니다. **참고** 각 솔루션 사용자의 이름에 다른 값을 사용해야 합니다. 인증서를 수동으로 생성하는 경우 사용하는 도구에 따라 **주체** 아래에 **CN**으로 표시될 수 있습니다. vSphere Certificate Manager를 사용하는 경우 각 솔루션 사용자에 대한 인증서 정보를 입력하라는 메시지가 표시됩니다. vSphere Certificate Manager가 이 정보를 `certool.cfg`에 저장합니다.

인증서 유형	인증서 요구 사항
	vpxd-extension 솔루션 사용자의 경우 확장 키 사용을 비워두거나 "TLS WWW 클라이언트 인증"을 사용할 수 있습니다.

사용자 지정 인증서 사용 시 요구 사항

사용자 지정 인증서를 사용하려면 인증서가 다음 요구 사항을 충족해야 합니다.

인증서 유형	인증서 요구 사항
시스템 SSL 인증서	각 노드의 시스템 SSL 인증서는 타사 또는 엔터프라이즈 CA에서 받은 별도의 인증서를 가져야 합니다. ■ vSphere Client 또는 vSphere Certificate Manager를 사용하여 CSR을 생성하거나 CSR을 수동으로 생성할 수 있습니다. CSR은 앞의 "가져온 모든 vSphere 인증서에 대한 요구 사항" 목록에 나온 요구 사항을 충족해야 합니다. ■ 대부분의 필드에서 기본값을 수락하거나 사이트별 값을 제공할 수 있습니다. 시스템의 FQDN은 필수 항목입니다.
솔루션 사용자 인증서	각 노드의 각 솔루션 사용자는 타사 또는 엔터프라이즈 CA에서 받은 별도의 인증서를 가져야 합니다. ■ vSphere Certificate Manager를 사용하여 CSR을 생성하거나 직접 준비할 수 있습니다. CSR은 앞의 "가져온 모든 vSphere 인증서에 대한 요구 사항" 목록에 나온 요구 사항을 충족해야 합니다. ■ vSphere Certificate Manager를 사용하는 경우 각 솔루션 사용자에 대한 인증서 정보를 입력하라는 메시지가 유틸리티에 표시됩니다. vSphere Certificate Manager가 이 정보를 `certool.cfg`에 저장합니다. **참고** 각 솔루션 사용자의 이름에 다른 값을 사용해야 합니다. 수동으로 생성된 인증서는 사용하는 도구에 따라 **주체** 아래에 **CN**으로 표시될 수 있습니다. 이후에 솔루션 사용자 인증서를 사용자 지정 인증서로 교체하는 경우 타사 CA의 전체 서명 인증서 체인을 제공해야 합니다. vpxd-extension 솔루션 사용자의 경우 확장 키 사용을 비워두거나 "TLS WWW 클라이언트 인증"을 사용할 수 있습니다.

vSphere 인증서 관리

vSphere 인증서 인프라를 설정하거나 업데이트하는 데 필요한 작업은 사용자 환경의 요구 사항에 따라 다릅니다. 새로 설치를 수행할지 아니면 업그레이드를 수행할지 그리고 ESXi 또는 vCenter Server를 고려할지 여부를 고려해야 합니다.

VMware Certificate Authority 인증서를 사용하는 환경

VMCA(VMware Certificate Authority)는 모든 인증서 관리를 처리할 수 있습니다. VMCA는 VMCA를 루트 인증 기관으로 사용하는 인증서로 vCenter Server 구성 요소와 ESXi 호스트를 프로비저닝합니다. 이전 버전의 vSphere에서 vSphere 6.0 이상으로 업그레이드 중인 경우에는 자체 서명된 모든 인증서가 VMCA에 의해 서명된 인증서로 교체됩니다.

VMware 인증서를 현재 교체하지 않으면 사용자 환경에서는 자체 서명된 인증서 대신 VMCA 서명 인증서를 사용하기 시작합니다.

사용자 지정 인증서를 사용하는 환경

회사 정책에 따라 타사 또는 엔터프라이즈 CA(인증 기관)에서 서명하거나, 사용자 지정 인증서 정보가 필요한 인증서를 사용해야 하는 경우에는 몇 가지 방법으로 새로 설치할 수 있습니다.

- 타사 CA 또는 엔터프라이즈 CA에서 VMCA 루트 인증서에 서명하도록 합니다. 이 서명된 인증서로 VMCA 루트 인증서를 교체합니다. 이 시나리오에서는 VMCA 인증서가 중간 인증서입니다. VMCA는 전체 인증서 체인이 포함된 인증서로 vCenter Server 구성 요소와 ESXi 호스트를 프로비저닝합니다.
- 회사 정책에 따라 체인에 중간 인증서가 허용되지 않는 경우에는 인증서를 명시적으로 교체할 수 있습니다. vSphere Client 또는 vSphere Certificate Manager 유틸리티를 사용하거나 인증서 관리 CLI를 사용한 수동 인증서 교체를 수행할 수 있습니다.

사용자 지정 인증서를 사용하는 환경을 업그레이드할 때는 일부 인증서를 유지할 수 있습니다.

- ESXi 호스트는 업그레이드 중 자체 사용자 지정 인증서를 유지합니다. vCenter Server 업그레이드 프로세스에서 모든 관련 루트 인증서를 vCenter Server에서 VECS(VMware Certificate Endpoint Store)의 TRUSTED_ROOTS 저장소에 추가해야 합니다.

  vSphere 6.0 이상으로 업그레이드한 후 인증서 모드를 **사용자 지정**으로 설정할 수 있습니다. 인증서 모드가 VMCA(기본값)이고 사용자가 vSphere Client에서 인증서 새로 고침을 수행하면 VMCA 서명 인증서가 사용자 지정 인증서를 교체합니다.
- 단순 vCenter Server 설치를 내장형 배포로 업그레이드할 경우 vCenter Server에서는 사용자 지정 인증서를 보존합니다. 업그레이드 후 환경은 이전처럼 작동합니다. 기존 vCenter Server 및 vCenter Single Sign-On 인증서가 보존됩니다. 인증서는 시스템 SSL 인증서로 사용됩니다. 또한 VMCA는 VMCA 서명 인증서를 각 솔루션 사용자(vCenter 서비스 모음)에게 할당합니다. 솔루션 사용자는 이 인증서를 vCenter Single Sign-On에 인증하는 데만 사용합니다. VMware는 솔루션 사용자 인증서를 교체하는 것을 권장하지 않습니다.

vSphere 인증서 인터페이스

vCenter Server의 경우 다음의 도구 및 인터페이스를 사용하여 인증서를 보고 교체할 수 있습니다.

표 2-3. vCenter Server 인증서 관리를 위한 인터페이스

인터페이스	사용
vSphere Client	그래픽 사용자 인터페이스를 사용하여 일반적인 인증서 작업을 수행합니다.
vSphere Automation API	"VMware vSphere Automation SDK 프로그래밍 가이드" 를 참조하십시오.
vSphere Certificate Manager 유틸리티	vCenter Server 설치의 명령줄에서 일반적인 인증서 교체 작업을 수행합니다.
vSphere 인증서 관리 CLI	`dir-cli`, `certool` 및 `vecs-cli`를 사용하여 모든 인증서 관리 작업을 수행합니다.
`sso-config` 유틸리티	vCenter Server 설치의 명령줄에서 STS 인증서 관리를 수행합니다.
PowerCLI 12.4 이상(vSphere 7.0 이상 필요)	신뢰할 수 있는 인증서 저장소 관리를 수행하고 vCenter Server 시스템 SSL 인증서와 ESXi 시스템 SSL 인증서를 관리합니다.

ESXi의 경우 vSphere Client에서 인증서 관리를 수행합니다. VMCA가 인증서를 프로비저닝하고 ESXi 호스트에 로컬로 저장합니다. VMCA는 ESXi 호스트 인증서를 VMDIR 또는 VECS에 저장하지 않습니다. "vSphere 보안" 설명서를 참조하십시오.

지원되는 vCenter Server 인증서

vCenter Server 및 관련 시스템과 서비스의 경우 다음 인증서가 지원됩니다.

- VMCA(VMware Certificate Authority)에서 생성하고 서명한 인증서.
- 사용자 지정 인증서.
  - 자체 내부 PKI에서 생성된 엔터프라이즈 인증서.
  - Verisign, GoDaddy 등과 같은 외부 PKI가 생성한 타사 CA 서명 인증서.

루트 CA 없이 OpenSSL을 사용하여 생성된 자체 서명 인증서는 지원되지 않습니다.

vSphere 인증서 교체

구성하는 시스템에 대한 요구 사항과 회사 정책에 따라 다양한 유형의 인증서 교체를 수행할 수 있습니다. vSphere Certificate Manager 유틸리티를 사용하거나 설치에 포함된 CLI를 사용하여 수동으로 vSphere Client에서 인증서 교체를 수행할 수 있습니다.

VMCA(VMware Certificate Authority)는 각 vCenter Server 배포에 포함됩니다. VMCA는 각 노드, 각 vCenter Server 솔루션 사용자 및 각 ESXi 호스트를 인증 기관인 VMCA에서 서명한 인증서로 프로비저닝합니다.

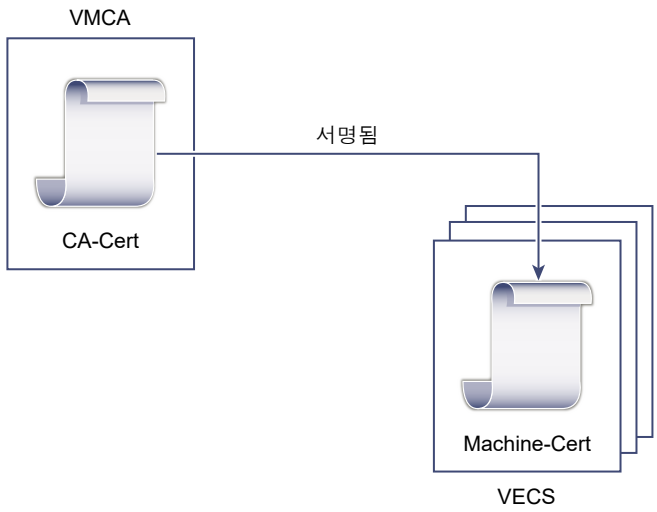
기본 인증서를 교체할 수 있습니다. vCenter Server 구성 요소의 경우 설치에 포함된 명령줄 도구 집합을 사용할 수 있습니다. 여러 옵션이 있습니다.

참고 vCenter Server가 NSX-T Manager에 연결되어 있고 vCenter Server 인증서를 교체하는 경우 vCenter Server 계산 관리자의 지문을 업데이트해야 합니다. "NSX-T Data Center 마이그레이션 조정기 가이드" 에서 "계산 관리자 추가" 항목을 참조하십시오.

인증서를 VMCA 서명 인증서로 교체

VMCA 인증서가 만료되거나 다른 이유로 인증서를 교체하려는 경우 인증서 관리 CLI를 사용하여 해당 프로세스를 수행할 수 있습니다. 기본적으로 VMCA 루트 인증서는 10년 후에 만료되고 VMCA에서 서명한 모든 인증서는 루트 인증서가 만료될 때, 즉 최대 10년 후에 만료됩니다.

그림 2-1. VMCA에서 서명한 인증서가 VECS에 저장됨



다음과 같은 vSphere Certificate Manager 옵션을 사용할 수 있습니다.

- VMCA 인증서로 시스템 SSL 인증서 교체
- VMCA 인증서로 솔루션 사용자 인증서 교체

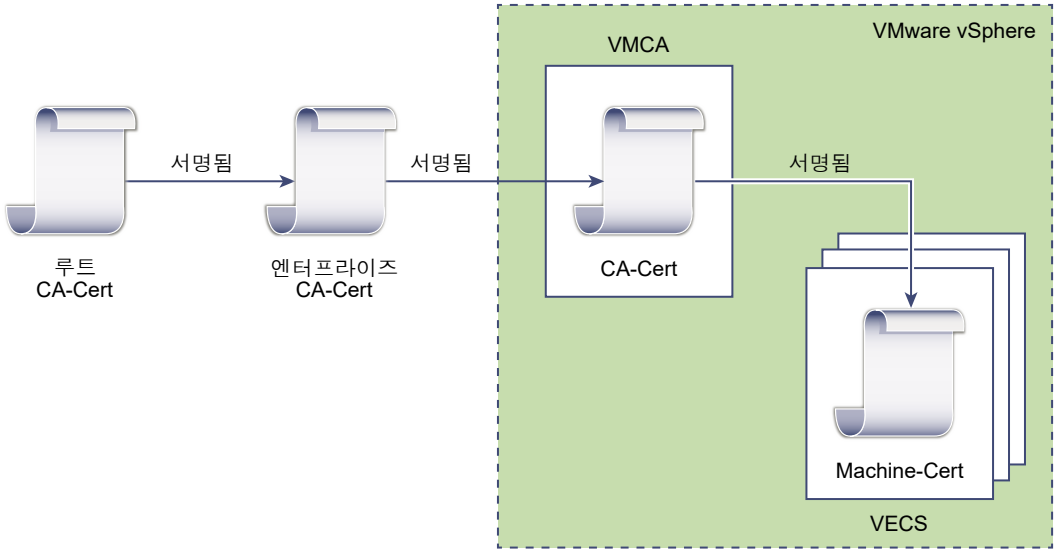
수동 인증서 교체는 CLI를 사용하여 기존 VMCA 서명 인증서를 VMCA 서명 인증서로 교체 항목을 참조하십시오.

VMCA를 중간 CA(인증 기관)로 만들기

VMCA 루트 인증서를 엔터프라이즈 CA(인증 기관) 또는 타사 CA에서 서명한 인증서로 교체할 수 있습니다. VMCA는 인증서를 프로비저닝하고 VMCA를 중간 CA로 만들 때마다 사용자 지정 루트 인증서에 서명합니다.

참고 vCenter Server를 사용하여 새로 설치를 수행하는 경우 ESXi 호스트를 추가하기 전에 VMCA 루트 인증서를 교체합니다. 이렇게 VMCA가 체인 전체에 서명하므로 새 인증서를 생성하지 않아도 됩니다.

그림 2-2. 타사 또는 엔터프라이즈 CA에서 서명한 인증서가 VMCA를 중간 CA로 사용



다음과 같은 vSphere Certificate Manager 옵션을 사용할 수 있습니다.

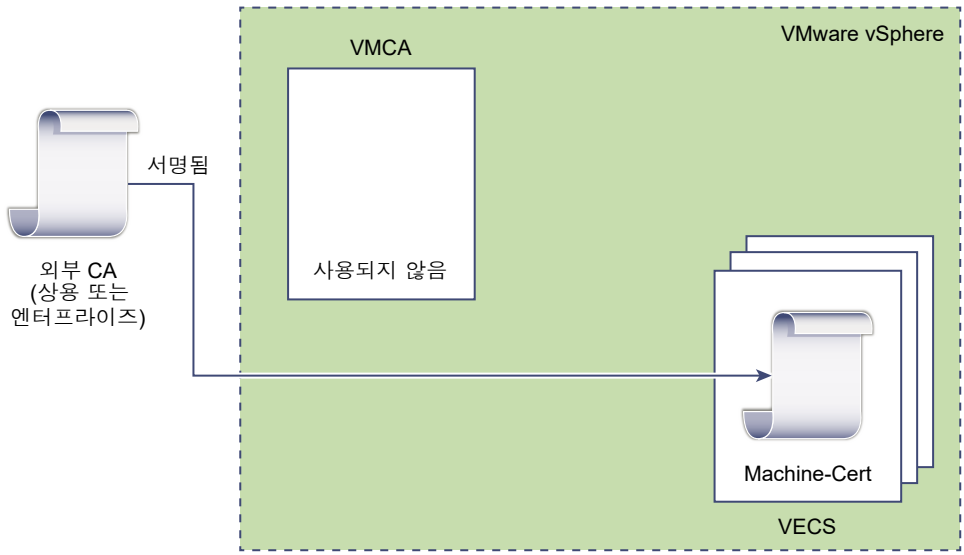
- 사용자 지정 서명 인증서로 VMCA 루트 인증서 교체 및 모든 인증서 교체
- VMCA 인증서로 시스템 SSL 인증서 교체(다중 노드 고급 연결 모드 배포)
- VMCA 인증서로 솔루션 사용자 인증서 교체(다중 노드 고급 연결 모드 배포)

수동 인증서 교체는 CLI를 사용하여 VMCA를 중간 CA(인증 기관)로 만들기 항목을 참조하십시오.

VMCA 서명 인증서를 사용자 지정 인증서로 교체

사용자 지정 인증서로 기존 VMCA 서명된 인증서를 교체할 수 있습니다. 해당 접근 방식을 사용하는 경우 모든 인증서 프로비저닝 및 모니터링에 대한 책임이 있습니다.

그림 2-3. 외부 인증서가 VECS에 직접 저장됨



다음과 같은 vSphere Certificate Manager 옵션을 사용할 수 있습니다.

- 시스템 SSL 인증서를 사용자 지정 인증서로 교체
- 솔루션 사용자 인증서를 사용자 지정 인증서로 교체

수동 인증서 교체는 CLI를 사용하여 인증서를 사용자 지정 인증서로 교체 항목을 참조하십시오.

vSphere Client를 사용하여 시스템 SSL 인증서에 대한 CSR을 생성하고(사용자 지정) CA에서 인증서를 반환한 후 인증서를 교체할 수 있습니다. vSphere Client를 사용하여 시스템 SSL 인증서에 대한 인증서 서명 요청 생성(사용자 지정 인증서)의 내용을 참조하십시오.

인증서 배포에 하이브리드 방식 사용

하이브리드 방식에서는 VMCA가 인증서 중 일부를 제공하도록 하면서 인프라의 다른 부분에 사용자 지정 인증서를 사용할 수 있습니다. 예를 들어 솔루션 사용자 인증서는 vCenter Single Sign-On에 인증하는 데에만 사용되므로 VMCA를 통해 이러한 인증서를 프로비저닝하는 것을 고려합니다. 모든 SSL 트래픽을 보호하려면 사용자 지정 인증서로 시스템 SSL 인증서를 교체합니다.

회사 정책에서는 대개 중간 CA를 허용하지 않습니다. 이런 경우에는 하이브리드 배포가 솔루션으로 적합합니다. 하이브리드 배포는 교체할 인증서 수를 최소화하고 모든 트래픽을 보호합니다. 하이브리드 배포를 사용할 경우 내부 트래픽, 즉 솔루션 사용자 트래픽만 기본 VMCA 서명 인증서를 사용합니다.

자세한 내용은 http://vmware.com/go/hybridvmca에서 블로그 게시글 "New Product Walkthrough - Hybrid vSphere SSL Certificate Replacement(신제품 둘러보기 - 하이브리드 vSphere SSL 인증서 교체)"를 참조하십시오.

ESXi 인증서 교체

ESXi 호스트의 경우 vSphere Client에서 인증서 프로비저닝 동작을 변경할 수 있습니다. 자세한 내용은 "vSphere 보안" 설명서를 참조하십시오.

표 2-4. ESXi 인증서 교체 옵션

옵션	설명
VMware Certificate Authority 모드(기본값)	vSphere Client에서 인증서를 갱신하는 경우 VMCA는 해당 호스트에 대한 인증서를 발급합니다. 인증서 체인을 포함하도록 VMCA 루트 인증서를 변경한 경우 호스트 인증서에는 전체 체인이 포함됩니다.
사용자 지정 인증 기관 모드	VMCA에서 서명하거나 발급하지 않은 인증서를 수동으로 업데이트하고 사용할 수 있습니다.
지문 모드	새로 고침 동안 5.5 인증서를 유지하는 데 사용할 수 있습니다. 디버깅 상황에서만 일시적으로 이 모드를 사용합니다.

vSphere에서 인증서를 사용하는 위치

VMCA(VMware인증 기관)는 인증서를 사용하여 환경을 프로비저닝합니다. 인증서에는 연결을 보호하기 위한 시스템 SSL 인증서, vCenter Single Sign-On에서 서비스를 인증하기 위한 솔루션 사용자 인증서 및 ESXi 호스트에 대한 인증서가 포함됩니다.

다음의 인증서가 사용됩니다.

표 2-5. vSphere의 인증서

인증서	프로비저닝됨	주석
ESXi 인증서	VMCA(기본값)	ESXi 호스트에 로컬로 저장됩니다.
시스템 SSL 인증서	VMCA(기본값)	VECS(VMware Endpoint 인증서 저장소)에 저장됩니다.
솔루션 사용자 인증서	VMCA(기본값)	VECS에 저장됩니다.
vCenter Single Sign-On SSL 서명 인증서	설치 도중 프로비저닝됩니다.	명령줄에서 이 인증서를 관리합니다. **참고** 파일 시스템에서 이 인증서를 변경하지 마십시오. 변경할 경우 예기치 않은 동작이 발생합니다.
VMDIR(VMware Directory Service) SSL 인증서	설치 도중 프로비저닝됩니다.	vSphere 6.5 이상에서 시스템 SSL 인증서가 vmdir 인증서로 사용됩니다.
SMS 자체 서명된 인증서	IOFilter 제공자 등록 도중 프로비저닝됩니다.	vSphere 7.0 이상에서 SMS 자체 서명된 인증서는 `/etc/vmware/ssl/iofiltervp_castore.pem`에 저장됩니다. vSphere 7.0 이전에 SMS 자체 서명된 인증서는 `/etc/vmware/ssl/castore.pem`에 저장됩니다. 또한 SMS 저장소는 retainVasaProviderCertificate=True인 경우 VVOL VASA 제공자의 자체 서명된 인증서(버전 4.0 이하)도 저장할 수 있습니다.

ESXi 인증서

ESXi 인증서는 각 호스트의 `/etc/vmware/ssl` 디렉토리에 로컬로 저장됩니다. ESXi 인증서는 기본적으로 VMCA에 의해 프로비저닝되지만 사용자 지정 인증서를 대신 사용할 수 있습니다. ESXi 인증서는 호스트가 처음 vCenter Server에 추가될 때와 호스트가 다시 연결될 때 프로비저닝됩니다. 자세한 내용은 "vSphere 보안" 설명서를 참조하십시오.

시스템 SSL 인증서

각 노드의 시스템 SSL 인증서는 서버 측에서 SSL 소켓을 생성하는 데 사용됩니다. SSL 클라이언트는 SSL 소켓에 연결됩니다. 인증서는 서버 확인 및 HTTPS나 LDAPS와 같은 보안 통신에 사용됩니다.

각 vCenter Server 노드에는 고유한 시스템 SSL 인증서가 있습니다. vCenter Server 노드에서 실행되는 모든 서비스는 시스템 SSL 인증서를 사용하여 SSL 끝점을 표시합니다.

시스템 SSL 인증서를 사용하는 서비스는 다음과 같습니다.

- 역방향 프록시 서비스. 개별 vCenter 서비스로의 SSL 연결은 항상 역방향 프록시로 이동합니다. 트래픽이 서비스 자체로 이동하지 않습니다.
- vCenter Server 서비스(vpxd).
- VMware Directory Service(vmdir).

VMware 제품은 표준 X.509 버전 3(X.509v3) 인증서를 사용하여 세션 정보를 암호화합니다. 세션 정보는 SSL을 통해 구성 요소 간에 전송됩니다.

솔루션 사용자 인증서

솔루션 사용자는 하나 이상의 vCenter Server 서비스를 캡슐화합니다. 각 솔루션 사용자는 vCenter Single Sign-On에 인증되어야 합니다. 솔루션 사용자는 인증서를 사용하여 SAML 토큰 교환을 통해 vCenter Single Sign-On에 인증됩니다.

솔루션 사용자는 처음 인증해야 할 때, 재부팅 후, 시간 제한 경과 후에 vCenter Single Sign-On에 인증서를 제출해야 합니다. 시간 제한(키 소유자 시간 제한)은 vSphere Client에서 설정할 수 있으며 기본값은 2592000초(30일)입니다.

예를 들어 vpxd 솔루션 사용자는 vCenter Single Sign-On에 연결할 때 vCenter Single Sign-On에 인증서를 제공합니다. 그러면 vpxd 솔루션 사용자는 vCenter Single Sign-On으로부터 SAML 토큰을 받고 이 토큰을 사용하여 다른 솔루션 사용자 및 서비스에 인증할 수 있습니다.

다음 솔루션 사용자 인증서 저장소는 VECS에 포함되어 있습니다.

- `machine`: License Server 및 로깅 서비스에서 사용됩니다.

  참고 이 시스템 솔루션 사용자 인증서는 시스템 SSL 인증서와 아무 관련이 없습니다. 이 시스템 솔루션 사용자 인증서는 SAML 토큰 교환에 사용되며 시스템 SSL 인증서는 시스템에 대한 보안 SSL 연결에 사용됩니다.

- `vpxd`: vCenter 서비스 대몬(vpxd) 저장소. vpxd는 이 저장소에 저장된 솔루션 사용자 인증서를 사용하여 vCenter Single Sign-On에 인증합니다.
- `vpxd-extension`: vCenter 확장 저장소입니다. Auto Deploy 서비스, Inventory Service를 비롯해 다른 솔루션 사용자의 일부가 아닌 기타 서비스가 포함됩니다.
- `vsphere-webclient`: vSphere Client 저장소입니다. 성능 차트 서비스와 같은 일부 추가 서비스도 포함됩니다.
- `wcp`: VMware Tanzu™ 저장소가 있는 VMware vSphere®. vSphere 클러스터 서비스에도 사용됩니다.

내부 인증서

vCenter Single Sign-On 인증서는 VECS에 저장되지 않으며 인증서 관리 도구로 관리되지 않습니다. 원칙적으로 변경이 불필요하지만 특별한 경우 이 인증서를 교체할 수 있습니다.

vCenter Single Sign-On 서명 인증서

vCenter Single Sign-On 서비스에는 vSphere를 통한 인증에 사용되는 SAML 토큰을 발급하는 ID 제공자 서비스가 포함됩니다. SAML 토큰은 사용자의 ID를 나타내며 그룹 멤버 자격 정보도 포함합니다. vCenter Single Sign-On이 SAML 토큰을 발급하는 경우 서명 인증서로 각 토큰에 서명하므로 vCenter Single Sign-On의 클라이언트가 SAML 토큰이 신뢰할 수 있는 소스로부터 전송되었는지 확인할 수 있습니다.

CLI에서 이 인증서를 교체할 수 있습니다. 명령줄을 사용하여 vCenter Server STS 인증서 교체의 내용을 참조하십시오.

VMware 디렉토리 서비스 SSL 인증서

vSphere 6.5 이상에서 시스템 SSL 인증서가 VMware 디렉토리 인증서로 사용됩니다. 이전 버전의 vSphere는 해당 설명서를 참조하십시오.

vSphere 가상 시스템 암호화 인증서

vSphere 가상 시스템 암호화 솔루션은 키 서버와 연결됩니다. 솔루션이 키 서버에 인증되는 방식에 따라 인증서가 생성되어 VECS에 저장될 수 있습니다. "vSphere 보안" 설명서를 참조하십시오.

VMware 인증 기관 및 VMware 핵심 ID 서비스

핵심 ID 서비스는 모든 vCenter Server 시스템에 속합니다. VMCA(VMware 인증 기관)는 모든 VMware 핵심 ID 서비스 그룹에 속합니다. 이러한 서비스와 상호 작용하려면 관리 CLI 및 vSphere Client를 사용합니다.

VMware 핵심 ID 서비스에는 몇 개의 구성 요소가 포함됩니다.

표 2-6. 핵심 ID 서비스

서비스	설명
VMware Directory Service(vmdir)	vCenter Single Sign-On을 사용한 인증의 SAML 인증서 관리를 처리하는 ID 소스입니다.
VMCA(VMware 인증 기관)	VMware 솔루션 사용자용 인증서, 서비스가 실행 중인 시스템용 시스템 인증서 및 ESXi 호스트 인증서를 발급합니다. VMCA는 그대로 사용하거나 중간 인증 기관으로 사용할 수 있습니다. VMCA는 동일한 도메인에서 vCenter Single Sign-On에 인증될 수 있는 클라이언트에만 인증서를 발급합니다.
VMAFD(VMware 인증 프레임워크 대몬)	VECS(VMware Endpoint 인증서 저장소) 및 몇 가지 다른 인증 서비스가 포함됩니다. VMware 관리자는 VECS와 상호 작용하며 다른 서비스는 내부적으로 사용됩니다.

VMware Endpoint 인증서 저장소

VECS(VMware Endpoint 인증서 저장소)는 인증서, 개인 키 및 키 저장소에 저장할 수 있는 다른 인증서 정보의 로컬(클라이언트 측) 저장소 역할을 합니다. VMCA를 인증 기관 및 인증서 서명자로 사용하지 않도록 결정할 수 있지만, vCenter 인증서, 키 등을 저장하기 위해서는 VECS를 사용해야 합니다. ESXi 인증서는 각 호스트에 로컬로 저장되며 VECS에 저장되지 않습니다.

VECS는 VMAFD(VMware Authentication Framework 대몬)의 일부로 실행됩니다. VECS는 모든 vCenter Server 노드에서 실행되며 인증서와 키가 포함된 키 저장소를 포함합니다.

VECS는 신뢰할 수 있는 루트 저장소에 대한 업데이트를 위해 vmdir(VMware 디렉토리 서비스)를 주기적으로 폴링합니다. 또한 `vecs-cli` 명령을 사용하여 VECS에서 인증서 및 키를 명시적으로 관리할 수도 있습니다. vecs-cli 명령 참조의 내용을 참조하십시오.

VECS에는 다음과 같은 저장소가 포함됩니다.

표 2-7. VECS의 저장소

저장소	설명
시스템 SSL 저장소(MACHINE_SSL_CERT)	■ 모든 vSphere 노드의 역방향 프록시 서비스에서 사용됩니다. ■ 각 vCenter Server 노드의 VMware Directory Service(vmdir)가 사용합니다. vSphere 6.0 이상에서 모든 서비스는 시스템 SSL 인증서를 사용하는 역방향 프록시를 통해 통신합니다. 역방향 호환성을 위해 5.x 서비스는 여전히 특정 포트를 사용합니다. 그 결과 vpxd와 같은 일부 서비스는 여전히 자체 포트를 열어둡니다.
솔루션 사용자 저장소 ■ `machine` ■ `vpxd` ■ `vpxd-extension` ■ `vsphere-webclient` ■ `wcp`	VECS에는 각 솔루션 사용자에 대한 하나의 저장소가 포함됩니다. 각 솔루션 사용자 인증서의 주체는 고유해야 합니다. 예를 들어 시스템 인증서는 vpxd 인증서와 동일한 주체를 가질 수 없습니다. 솔루션 사용자 인증서는 vCenter Single Sign-On 인증에 사용됩니다. vCenter Single Sign-On은 인증서가 유효한지 확인하지만 다른 인증서 특성은 확인하지 않습니다. 다음 솔루션 사용자 인증서 저장소는 VECS에 포함되어 있습니다. ■ `machine`: License Server 및 로깅 서비스에서 사용됩니다. **참고** 이 시스템 솔루션 사용자 인증서는 시스템 SSL 인증서와 아무 관련이 없습니다. 이 시스템 솔루션 사용자 인증서는 SAML 토큰 교환에 사용되며 시스템 SSL 인증서는 시스템에 대한 보안 SSL 연결에 사용됩니다. ■ `vpxd`: vCenter 서비스 대몬(vpxd) 저장소. vpxd는 이 저장소에 저장된 솔루션 사용자 인증서를 사용하여 vCenter Single Sign-On에 인증합니다. ■ `vpxd-extension`: vCenter 확장 저장소입니다. Auto Deploy 서비스, Inventory Service를 비롯해 다른 솔루션 사용자의 일부가 아닌 기타 서비스가 포함됩니다. ■ `vsphere-webclient`: vSphere Client 저장소입니다. 성능 차트 서비스와 같은 일부 추가 서비스도 포함됩니다. ■ `wcp`: VMware Tanzu™ 저장소가 있는 VMware vSphere®. vSphere 클러스터 서비스에도 사용됩니다. 각 vCenter Server 노드에는 `machine` 인증서가 포함되어 있습니다.
신뢰할 수 있는 루트 저장소(TRUSTED_ROOTS)	모든 신뢰할 수 있는 루트 인증서가 포함됩니다.
vSphere Certificate Manager 유틸리티 백업 저장소(BACKUP_STORE)	VMCA(VMware Certificate Manager)에서 인증서 복구를 지원하기 위해 사용합니다. 최근 상태만 백업으로 저장되며 한 단계까지만 되돌아갈 수 있습니다.
기타 저장소	솔루션을 통해 기타 저장소가 추가될 수 있습니다. 예를 들어 Virtual Volumes 솔루션은 SMS 저장소를 추가합니다. VMware 설명서 또는 VMware 기술 자료 문서에서 그렇게 하라고 지시하지 않는 이상 이러한 저장소의 인증서를 수정하지 마십시오. **참고** TRUSTED_ROOTS_CRLS 저장소를 삭제하면 인증서 인프라가 손상될 수 있습니다. TRUSTED_ROOTS_CRLS 저장소를 삭제하거나 수정하지 마십시오.

vCenter Single Sign-On 서비스는 토큰 서명 인증서와 해당 SSL 인증서를 디스크에 저장합니다. CLI에서 토큰 서명 인증서를 변경할 수 있습니다.

일부 인증서는 시작 도중 임시로 또는 영구적으로 파일 시스템에 저장됩니다. 파일 시스템의 인증서를 변경하지 마십시오.

참고 VMware 설명서 또는 기술 자료 문서에서 그렇게 하라고 지시하지 않는 한 인증서 파일을 변경하지 마십시오. 그렇지 않으면 예기치 않은 동작이 발생할 수 있습니다.

vSphere 인증서 해지 관리

인증서 중 하나의 손상이 의심되는 경우 VMCA 루트 인증서를 포함하여 기존의 모든 인증서를 교체하십시오.

vSphere는 인증서 교체를 지원하지만 ESXi 호스트 또는 vCenter Server 시스템에 대한 인증서 해지는 적용하지 않습니다.

해지된 인증서를 모든 노드에서 제거합니다. 해지된 인증서를 제거하지 않으면 공격자가 메시지 가로채기(man-in-the-middle) 공격을 통해 계정의 자격 증명을 가장하여 손상시키는 것이 가능해질 수 있습니다.

대규모 배포에서 vSphere 인증서 교체

많은 수의 vCenter Server 호스트가 포함된 배포에서 인증서를 교체할 때 vSphere 인증서 관리 유틸리티를 사용하거나 CLI를 사용하여 인증서를 수동으로 교체할 수 있습니다. 선택 프로세스를 안내하는 몇 가지 모범 사례가 있습니다.

여러 vCenter Server 시스템이 있는 환경에서 시스템 SSL 인증서 교체

환경에 여러 vCenter Server 시스템이 포함된 경우 시스템 SSL 인증서를 vSphere Client 또는 vSphere Certificate Manager 유틸리티를 사용하여 교체하거나 CLI 명령을 사용하여 수동으로 교체할 수 있습니다.

vSphere Certificate Manager를 사용하여 여러 vCenter Server 시스템에서 시스템 SSL 인증서 교체

각 시스템에서 vSphere Certificate Manager를 실행합니다. 수행하는 작업에 따라 인증서 정보를 묻는 메시지도 표시됩니다. 자세한 내용은 다음 항목을 참조하십시오.

- Certificate Manager를 사용하여 사용자 지정 서명 인증서로 VMCA 루트 인증서 교체 및 모든 인증서 교체
- Certificate Manager를 사용하여 시스템 SSL 인증서를 VMCA 인증서로 교체(중간 CA)
- Certificate Manager를 사용하여 솔루션 사용자 인증서를 VMCA 인증서로 교체(중간 CA)

CLI를 사용하여 여러 vCenter Server 시스템에서 수동으로 시스템 SSL 인증서 교체

수동으로 인증서를 교체할 때는 각 시스템에서 인증서 교체 CLI 명령을 실행합니다. 자세한 내용은 다음 항목을 참조하십시오.

- CLI를 사용하여 시스템 SSL 인증서를 VMCA 서명 인증서로 교체
- CLI를 사용하여 시스템 SSL 인증서 교체(중간 CA)
- CLI를 사용하여 시스템 SSL 인증서를 사용자 지정 인증서로 교체

여러 개의 vCenter Server 시스템이 있는 고급 연결 모드의 환경에서 솔루션 사용자 인증서 교체

고급 연결 모드에서 환경에 여러 개의 vCenter Server 시스템이 포함되어 있는 경우에는 다음 단계에 따라 솔루션 사용자 인증서를 교체합니다.

참고 대규모 배포의 솔루션 사용자 인증서를 나열할 경우 `/usr/lib/vmware-vmafd/bin/dir-cli list`의 출력에는 모든 노드의 모든 솔루션 사용자가 포함됩니다. 각 호스트의 로컬 시스템 ID를 찾으려면 `/usr/lib/vmware-vmafd/bin/vmafd-cli get-machine-id --server-name localhost`를 실행하십시오. 각 솔루션 사용자 이름에 시스템 ID가 포함되어 있습니다.

vSphere Certificate Manager를 사용하여 ELM의 vCenter Server 시스템에서 시스템 SSL 인증서 교체

각 시스템에서 vSphere Certificate Manager를 실행합니다. 수행하는 작업에 따라 인증서 정보를 묻는 메시지도 표시됩니다. vSphere Certificate Manager 유틸리티를 사용하여 인증서 관리의 내용을 참조하십시오.

CLI를 사용하여 ELM의 vCenter Server 시스템에서 수동으로 시스템 SSL 인증서 교체

ELM에서 vCenter Server의 시스템 SSL 인증서를 수동으로 교체하는 개략적인 단계는 다음과 같습니다.

1. 인증서를 생성 또는 요청합니다.

   다음 인증서가 필요합니다.

   - 각 vCenter Server의 시스템 솔루션 사용자용 인증서.
   - 각 노드에서 다음 솔루션 사용자 각각을 위한 인증서:
     - `vpxd` solution user
     - `vpxd-extension` solution user
     - `vsphere-webclient` solution user
     - `wcp` solution user
2. CLI 명령을 사용하여 각 노드에서 인증서를 교체합니다.

   정확한 프로세스는 수행 중인 인증서 교체의 유형에 따라 다릅니다. 자세한 내용은 다음 항목을 참조하십시오.

   - CLI를 사용하여 솔루션 사용자 인증서를 새 VMCA 서명된 인증서로 교체
   - CLI를 사용하여 솔루션 사용자 인증서 교체(중간 CA)
   - Certificate Manager를 사용하여 솔루션 사용자 인증서를 사용자 지정 인증서로 교체

외부 솔루션이 포함된 VMware 환경에서 인증서 교체

VMware vCenter Site Recovery Manager 또는 VMware vSphere Replication과 같은 일부 솔루션은 항상 vCenter Server 시스템이 아닌 다른 시스템에 설치됩니다. vCenter Server 시스템에서 기본 시스템 SSL 인증서를 교체하는 경우 해당 솔루션이 vCenter Server 시스템에 연결하려고 시도하면 연결 오류가 발생합니다.

`ls_update_certs` 스크립트를 실행하여 이 문제를 해결할 수 있습니다. VMware 기술 자료 문서(https://kb.vmware.com/s/article/2109074)를 참조하십시오.

vSphere Client를 사용하여 인증서 관리

vSphere Client를 사용하여 인증서를 보고 관리할 수 있습니다.

vSphere Client를 사용하여 이러한 관리 작업을 수행할 수 있습니다.

- 시스템 SSL, VMCA(VMware Certificate Authority) 루트, 신뢰할 수 있는 루트 및 STS(Security Token Service) 인증서를 봅니다.
- 신뢰할 수 있는 루트 인증서를 새로 추가하고 기존 시스템 SSL 및 STS 인증서를 갱신하거나 교체합니다.
- 시스템 SSL 인증서에 대해 사용자 지정 CSR(인증서 서명 요청)을 생성하고 인증 기관으로부터 인증서가 반환된 이후 인증서를 교체합니다.

인증서 교체 워크플로우 대부분은 vSphere Client에서 완벽하게 지원됩니다. 다른 인증서 교체 워크플로는 vSphere Certificate Manager 유틸리티에서 지원됩니다. vSphere Certificate Manager 유틸리티를 사용하여 인증서 관리의 내용을 참조하십시오.

기본 인증서를 교체하는 옵션에 대한 자세한 내용은 vSphere 인증서 교체의 내용을 참조하십시오.

참고 VMCA를 중간 CA로 사용하거나 사용자 지정 인증서를 사용하면 상당히 복잡한 문제가 발생할 수 있어 보안에 부정적인 영향을 미칠 수 있으며 운영 위험이 불필요하게 증가할 수 있습니다. vSphere 환경의 인증서 관리에 대한 자세한 내용은 http://vmware.com/go/hybridvmca에서 블로그 게시글 "New Product Walkthrough - Hybrid vSphere SSL Certificate Replacement(신제품 둘러보기 - 하이브리드 vSphere SSL 인증서 교체)" 를 참조하십시오.

vSphere Client를 사용하여 인증서 저장소 탐색

VECS(VMware Endpoint 인증서 저장소) 인스턴스는 각 vCenter Server 노드에 포함됩니다. 시스템 SSL, STS 및 신뢰할 수 있는 루트 인증서를 포함하여 vSphere Client에서 VMware Endpoint 인증서 저장소 내부의 여러 저장소를 탐색할 수 있습니다.

VECS 내의 여러 저장소에 대한 자세한 내용은 VMware Endpoint 인증서 저장소의 내용을 참조하십시오.

사전 요구 사항

대부분의 관리 작업의 경우 로컬 도메인 계정 administrator@vsphere.local의 관리자 암호 또는 설치 중에 도메인을 변경한 경우에는 다른 도메인의 관리자 암호가 필요합니다.

절차

1 vSphere Client를 사용하여 vCenter Server에 로그인합니다.

2 administrator@vsphere.local 또는 vCenter Single Sign-On 관리자 그룹에 속한 다른 멤버의 사용자 이름과 암호를 지정합니다.

   설치 시 다른 도메인을 지정한 경우에는 administrator@*mydomain*으로 로그인합니다.

3 인증서 관리 UI로 이동합니다.

   a **홈** 메뉴에서 **관리**를 선택합니다.

   b **인증서**에서 **인증서 관리**를 클릭합니다.

4 시스템에 메시지가 표시되면 vCenter Server의 자격 증명을 입력합니다.

5 VECS(VMware Endpoint 인증서 저장소) 내에 저장된 인증서를 탐색합니다.

   개별 저장소에 포함된 내용은 VMware Endpoint 인증서 저장소에 설명되어 있습니다.

6 인증서에 대한 세부 정보를 보려면 해당 인증서 탭을 선택하고 인증서를 선택한 후 인증서를 확장하여 세부 정보를 봅니다.

vSphere Client를 사용하여 vCenter 인증서 만료 경고의 임계값 설정

vCenter Server는 VECS(VMware Endpoint 인증서 저장소)의 모든 인증서를 관리하고 인증서 만료까지 남은 기간이 30일 이하인 경우 경보를 표시합니다. vSphere Client를 사용하여 `vpxd.cert.threshold` 고급 옵션에 따른 경고 표시 시기를 변경할 수 있습니다.

절차

1 vSphere Client에 로그인합니다.

2 vCenter Server 개체를 선택하고 **구성**을 클릭합니다.

3 **고급 설정**을 클릭합니다.

4 **설정 편집**을 클릭하고 **임계값**을 필터링합니다.

5 `vpxd.cert.threshold`의 설정을 원하는 값으로 변경하고 **저장**을 클릭합니다.

vSphere Client를 사용하여 VMCA 인증서를 새로운 VMCA 서명 인증서로 갱신

모든 VMCA 서명된 인증서를 새로운 VMCA 서명된 인증서로 교체할 수 있습니다. 이 프로세스를 인증서 갱신이라고 합니다. vSphere Client에서 선택한 인증서를 갱신하거나 환경 내의 모든 인증서를 갱신할 수 있습니다.

사전 요구 사항

인증서를 관리하려면 로컬 도메인(기본적으로 administrator@vsphere.local) 관리자의 암호를 입력해야 합니다. vCenter Server 시스템에 대한 인증서를 갱신하는 경우에는 vCenter Server 시스템에 대해 관리자 사용 권한을 가진 사용자의 vCenter Single Sign-On 자격 증명도 함께 제공해야 합니다.

절차

1 vSphere Client를 사용하여 vCenter Server에 로그인합니다.

2 administrator@vsphere.local 또는 vCenter Single Sign-On 관리자 그룹에 속한 다른 멤버의 사용자 이름과 암호를 지정합니다.

   설치 시 다른 도메인을 지정한 경우에는 administrator@*mydomain*으로 로그인합니다.

3 인증서 관리 UI로 이동합니다.

a **홈** 메뉴에서 **관리**를 선택합니다.

b **인증서**에서 **인증서 관리**를 클릭합니다.

4 시스템에 메시지가 표시되면 vCenter Server의 자격 증명을 입력합니다.

5 로컬 시스템의 VMCA 서명 시스템 SSL 인증서를 갱신합니다.

a **시스템 SSL** 탭에서 원하는 인증서를 선택하고 **갱신**을 클릭합니다.

b 인증서 기간을 일 단위로 지정합니다.

c 확인란을 클릭하여 vCenter Server 및 해당 데이터베이스를 백업했음을 확인합니다.

d **갱신**을 클릭합니다.

시스템에서 인증서가 갱신되고 성공 메시지가 표시됩니다.

e 인증서가 변경되었다는 메시지가 나타나면 **새로 고침**을 클릭하여 브라우저를 새로 고칩니다.

vSphere Client를 사용하여 인증서를 사용자 지정 인증서로 교체

vSphere Client를 사용하여 기본 인증서를 사용자 지정 인증서로 교체할 수 있습니다.

vSphere Client를 사용하여 각 시스템에 대한 CSR을 생성하고 내부 또는 타사 CA(인증 기관)에서 인증서를 받을 때 인증서를 교체할 수 있습니다. CSR을 내부 또는 타사 CA에 제출하면 CA는 서명된 인증서와 루트 인증서를 반환합니다. 루트 인증서와 서명된 인증서 둘 모두 vSphere Client에서 업로드할 수 있습니다.

vSphere Client를 사용하여 시스템 SSL 인증서에 대한 인증서 서명 요청 생성(사용자 지정 인증서)

시스템 SSL 인증서는 모든 vCenter Server 노드에서 역방향 프록시 서비스가 사용합니다. 각 시스템마다 다른 서비스와의 보안 통신을 위한 시스템 SSL 인증서가 있어야 합니다. vSphere Client를 사용하여 시스템 SSL 인증서에 대해 CSR(인증서 서명 요청)을 생성하고, 준비가 완료된 후 인증서를 바꿀 수 있습니다.

사전 요구 사항

인증서는 다음 요구 사항을 충족해야 합니다.

- 키 크기: 2048비트(최소)~8192비트(최대)(PEM 인코딩) vSphere Client 및 API는 인증서 서명 요청을 생성할 때 키 크기를 여전히 최대 16384비트까지 수락합니다.
- CRT 형식
- x509 버전 3
- SubjectAltName에는 DNS Name=<machine_FQDN>이 포함되어야 합니다.
- 다음과 같은 키 사용이 포함되어 있습니다. 디지털 서명, 키 암호화

참고 vSphere의 FIPS 인증서는 2048비트 및 3072비트의 RSA 키 크기만 검증합니다.

절차

1 vSphere Client를 사용하여 vCenter Server에 로그인합니다.

2 administrator@vsphere.local 또는 vCenter Single Sign-On 관리자 그룹에 속한 다른 멤버의 사용자 이름과 암호를 지정합니다.

설치 시 다른 도메인을 지정한 경우에는 administrator@*mydomain*으로 로그인합니다.

3 인증서 관리 UI로 이동합니다.

a **홈** 메뉴에서 **관리**를 선택합니다.

b **인증서**에서 **인증서 관리**를 클릭합니다.

4 vCenter Server의 자격 증명을 입력합니다.

5 CSR을 생성합니다.

a **시스템 SSL** 탭에서 원하는 인증서를 선택하고 **CSR(인증서 서명 요청) 생성**을 클릭합니다.

b 인증서 정보를 입력하고 **다음**을 클릭합니다.

2048(비트)은 키 크기의 기본값입니다. 필요에 따라 이 값을 변경합니다.

참고 vCenter Server를 사용하여 큰 키 크기의 CSR을 생성하는 경우 CPU를 많이 소모하는 작업의 특성상 생성을 완료하는 데에는 몇 분이 걸립니다.

c CSR을 복사하거나 다운로드합니다.

d **마침**을 클릭합니다.

e 인증 기관에 CSR을 제공합니다.

다음에 수행할 작업

인증 기관에서 인증서를 반환하면 인증서 저장소에서 기존 인증서를 바꿉니다. vSphere Client를 사용하여 사용자 지정 인증서 추가의 내용을 참조하십시오.

vSphere Client를 사용하여 신뢰할 수 있는 루트 인증서를 인증서 저장소에 추가

환경에서 타사 인증서를 사용하려면 신뢰할 수 있는 루트 인증서를 인증서 저장소에 추가해야 합니다. vSphere Client를 사용하여 이 작업을 수행할 수 있습니다.

사전 요구 사항

타사 또는 사내 CA(인증 기관)에서 사용자 지정 루트 인증서를 가져옵니다.

vSphere는 가져오기에 유효한 CA 인증서만 허용합니다. 유효하려면 CA 인증서의 CA 비트와 keyCertSign 비트가 기본 제약 조건과 키 용도 X.509 v3 인증서 확장에 각각 설정되어 있어야 합니다. 이는 인증서가 CA이고 해당 용도는 인증서 서명임을 의미합니다. 자세한 내용은 https://www.rfc-editor.org/rfc/rfc5280을 참조하십시오.

체인의 모든 인증서에 대해 keyCertSign 비트가 설정되어 있는지 확인합니다.

절차

1 vSphere Client를 사용하여 vCenter Server에 로그인합니다.

2 administrator@vsphere.local 또는 vCenter Single Sign-On 관리자 그룹에 속한 다른 멤버의 사용자 이름과 암호를 지정합니다.

설치 시 다른 도메인을 지정한 경우에는 administrator@*mydomain*으로 로그인합니다.

3 인증서 관리 UI로 이동합니다.

a **홈** 메뉴에서 **관리**를 선택합니다.

b **인증서**에서 **인증서 관리**를 클릭합니다.

4 시스템에 메시지가 표시되면 vCenter Server의 자격 증명을 입력합니다.

5 **신뢰할 수 있는 루트** 탭에서 **신뢰할 수 있는 루트 인증서 추가**를 클릭합니다.

6 **찾아보기**를 클릭하고 인증서 체인의 위치를 선택합니다.

CER, PEM 또는 CRT 유형의 파일을 사용할 수 있습니다.

7 **추가**를 클릭합니다.

인증서가 저장소에 추가됩니다.

참고 vSphere 8.0 업데이트 2 이상에서는 **vCenter 호스트로 루트 인증서 푸시 시작** 확인란이 제거됩니다. 인증서가 추가되면 vCenter Server가 루트 인증서를 인벤토리의 연결된 모든 호스트에 푸시합니다. vCenter Server와 다른 루트 인증서가 있는 호스트가 연결되면 vCenter Server는 해당 루트 인증서를 푸시하여 이러한 차이를 수정합니다. 이 경우 vCenter Server 루트 인증서가 호스트에 있는 인증서를 덮어쓰므로 관리자는 인벤토리 전체에 필요한 사용자 지정 루트 인증서가 vCenter Server에 추가되었는지 확인할 수 있습니다.

vSphere Client를 사용하여 사용자 지정 인증서 추가

vSphere Client를 사용하여 사용자 지정 시스템 SSL 인증서를 인증서 저장소에 추가할 수 있습니다.

대개는 각 구성 요소의 시스템 SSL 인증서를 교체하는 것으로도 충분합니다.

사전 요구 사항

교체할 각 인증서에 대해 CSR(인증서 서명 요청)을 생성합니다. vSphere Client를 사용하여 시스템 SSL 인증서에 대한 인증서 서명 요청 생성(사용자 지정 인증서)의 내용을 참조하십시오. 인증서와 개인 키를 vCenter Server에서 액세스할 수 있는 위치에 배치합니다.

절차

1 vSphere Client를 사용하여 vCenter Server에 로그인합니다.

2 administrator@vsphere.local 또는 vCenter Single Sign-On 관리자 그룹에 속한 다른 멤버의 사용자 이름과 암호를 지정합니다.

설치 시 다른 도메인을 지정한 경우에는 administrator@*mydomain*으로 로그인합니다.

3 인증서 관리 UI로 이동합니다.

   a **홈** 메뉴에서 **관리**를 선택합니다.

   b **인증서**에서 **인증서 관리**를 클릭합니다.

4 시스템에 메시지가 표시되면 vCenter Server의 자격 증명을 입력합니다.

5 **시스템 SSL** 탭에서 인증서를 선택하고 **인증서 가져오기 및 바꾸기**를 클릭합니다.

6 적절한 인증서 교체 옵션을 클릭한 후 **다음**을 클릭합니다.

옵션	설명
VMCA 인증서로 교체	현재 인증서를 교체할 VMCA에서 생성된 CSR을 생성합니다.
vCenter Server에서 생성된 CSR이 포함된 외부 CA 인증서로 교체(개인 키 포함)	vCenter Server에서 생성한 CSR을 사용하여 서명된 인증서로 현재 인증서를 교체합니다.
외부 CA 인증서로 교체(개인 키 필요)	외부 CA에서 서명한 인증서로 현재 인증서를 교체합니다.

7 CSR 정보를 입력하거나 적절한 인증서를 업로드합니다.

8 확인란을 클릭하여 vCenter Server 및 해당 데이터베이스를 백업했음을 확인합니다.

9 정보를 검토하고 **마침**을 클릭합니다.

   시스템이 인증서를 교체하고 성공 메시지를 표시합니다.

10 인증서가 변경되었다는 메시지가 나타나면 **새로 고침**을 클릭하여 브라우저를 새로 고칩니다.

VMCA 리프 인증서 생성

VMware 인프라에서 사용할 수 있도록 VMCA(VMware Certificate Authority)에서 서명한 리프 인증서를 생성할 수 있습니다.

VMCA(VMware Certificate Authority)가 모든 인증서 관리를 처리하는 것 외에도 리프 인증서를 생성할 수 있습니다. 리프 인증서는 VMCA에서 서명되며 다른 VMware 리소스를 식별하는 데 사용됩니다. VMCA에서 생성된 리프 인증서는 VECS에 저장되지 않습니다. 또한 vCenter Server는 이러한 리프 인증서의 만료를 추적하지 않습니다.

사전 요구 사항

리프 인증서를 설치하려는 VMware 인프라의 호스트에서 CSR(인증서 서명 요청)을 생성합니다.

절차

1 vSphere Client를 사용하여 vCenter Server에 로그인합니다.

2 administrator@vsphere.local 또는 vCenter Single Sign-On 관리자 그룹에 속한 다른 멤버의 사용자 이름과 암호를 지정합니다.

   설치 시 다른 도메인을 지정한 경우에는 administrator@*mydomain*으로 로그인합니다.

3 인증서 관리 UI로 이동합니다.

   a **홈** 메뉴에서 **관리**를 선택합니다.

   b **인증서**에서 **인증서 관리**를 클릭합니다.

4 시스템에 메시지가 표시되면 vCenter Server의 자격 증명을 입력합니다.

5 **신뢰할 수 있는 루트** 탭에서 VMCA 루트 인증서를 선택하고 **새 리프 인증서 발급**을 클릭합니다.

6 이전에 생성한 CSR을 찾아 기간을 지정한 후 **다음**을 클릭합니다.

7 **인증서 다운로드**를 클릭하여 리프 및 루트 인증서를 저장합니다.

결과

생성된 리프 및 루트 인증서가 만들어지고 지정된 위치에 다운로드됩니다.

다음에 수행할 작업

리프 및 루트 인증서를 VMware 인프라의 대상 호스트로 가져옵니다.

vSphere Certificate Manager 유틸리티를 사용하여 인증서 관리

vSphere Certificate Manager 유틸리티를 사용하면 대부분의 인증서 관리 작업을 명령줄에서 대화식으로 수행할 수 있습니다. vSphere Certificate Manager는 필요에 따라 수행할 작업, 인증서 위치 및 기타 정보를 요청한 다음 서비스를 중지했다가 시작하고 인증서를 교체합니다.

기본 인증서를 교체하는 옵션에 대한 자세한 내용은 vSphere 인증서 교체의 내용을 참조하십시오.

참고 VMCA를 중간 CA로 사용하거나 사용자 지정 인증서를 사용하면 상당히 복잡한 문제가 발생할 수 있어 보안에 부정적인 영향을 미칠 수 있으며 운영 위험이 불필요하게 증가할 수 있습니다. vSphere 환경의 인증서 관리에 대한 자세한 내용은 http://vmware.com/go/hybridvmca에서 블로그 게시글 "New Product Walkthrough - Hybrid vSphere SSL Certificate Replacement(신제품 둘러보기 - 하이브리드 vSphere SSL 인증서 교체)" 를 참조하십시오.

vSphere Certificate Manager를 사용하는 경우 VECS(VMware Endpoint 인증서 저장소)의 인증서 교체와 서비스 시작 및 중지를 사용자가 처리하지 않습니다.

vSphere Certificate Manager 옵션을 순서대로 실행하여 워크플로를 완료합니다. CSR 생성과 같은 여러 옵션이 각기 다른 워크플로에 사용됩니다. vSphere Certificate Manager를 실행하기 전에 교체 프로세스를 알아두고 사용할 인증서를 준비해야 합니다.

경고 vSphere Certificate Manager는 한 수준의 되돌리기를 지원합니다. vSphere Certificate Manager를 두 번 실행했는데 실수로 환경을 손상시킨 것을 발견한 경우, 도구는 두 차례의 실행 중 첫 번째 실행은 되돌릴 수 없습니다.

vSphere Certificate Manager 유틸리티 위치

vSphere Certificate Manager 유틸리티는 다음 위치에 있습니다.

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

참고 vSphere Certificate Manager를 실행할 때 몇 가지 옵션에서 다음과 같은 메시지를 표시합니다.

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

이 메시지가 표시되면 인증서 구성이 실행 중인 시스템의 FQDN(정규화된 도메인 이름)을 입력합니다.

vSphere Certificate Manager 유틸리티의 워크플로

다음 표에서는 vSphere Certificate Manager 유틸리티를 사용하여 수행할 수 있는 인증서 교체 워크플로의 개요를 제공합니다.

표 2-8. vSphere Certificate Manager 유틸리티의 워크플로

워크플로	설명	참조
VMCA 루트 인증서를 사용자 지정 서명 인증서로 교체 및 모든 인증서 교체	VMCA 루트 인증서를 생성하고 모든 인증서를 교체하려면 옵션 4, [새 VMCA 루트 인증서 다시 생성 및 모든 인증서 교체]를 사용합니다.	Certificate Manager를 사용하여 새 VMCA 루트 인증서 다시 생성 및 모든 인증서 교체
VMCA를 중간 CA(인증 기관)로 만들기	VMCA를 중간 CA로 만들려면 vSphere Certificate Manager 유틸리티를 여러 번 실행하고 여러 옵션을 사용해야 합니다. 이 워크플로는 시스템 SSL 인증서와 솔루션 사용자 인증서를 모두 교체하기 위한 전체 단계 집합을 제공합니다.	Certificate Manager를 사용하여 VMCA를 중간 CA(인증 기관)로 만들기
모든 인증서를 사용자 지정 인증서로 교체	모든 인증서를 사용자 지정 인증서로 교체하려면 vSphere Certificate Manager 유틸리티를 여러 번 실행하고 여러 옵션을 사용해야 합니다. 이 워크플로는 시스템 SSL 인증서와 솔루션 사용자 인증서를 모두 교체하기 위한 전체 단계 집합을 제공합니다.	Certificate Manager를 사용하여 모든 인증서를 사용자 지정 인증서로 교체
직전에 수행한 작업 되돌리기	직전에 수행한 인증서 작업을 되돌리고 이전 상태로 되돌아가려면 옵션 7, [이전 인증서를 다시 게시하여 직전에 수행한 작업 되돌리기]를 사용합니다.	Certificate Manager로 이전 인증서를 다시 게시하여 직전에 수행한 작업 되돌리기
모든 인증서 재설정	모든 기존 vCenter 인증서를 VMCA에서 서명한 인증서로 교체하려면 옵션 8, [모든 인증서 재설정]을 사용합니다.	Certificate Manager를 사용하여 모든 인증서 재설정

Certificate Manager를 사용하여 새 VMCA 루트 인증서 다시 생성 및 모든 인증서 교체

vSphere Certificate Manager 유틸리티를 사용하여 VMCA 루트 인증서를 다시 생성하고, 로컬 시스템 SSL 인증서 및 로컬 솔루션 사용자 인증서를 VMCA 서명 인증서로 교체할 수 있습니다. 여러 vCenter Server 인스턴스가 고급 연결 모드 구성에서 연결된 경우 각 vCenter Server에서 인증서를 교체해야 합니다.

기존 시스템 SSL 인증서를 새 VMCA 서명 인증서로 교체하는 경우 vSphere Certificate Manager가 정보를 요청하며 vCenter Server의 암호와 IP 주소를 제외한 모든 값을 `certool.cfg` 파일에 입력합니다.

- administrator@vsphere.local의 암호
- 두 글자의 국가 코드
- 회사 이름
- 조직 이름
- 조직 구성 단위
- 상태
- 구/군/시
- IP 주소(선택 사항)
- 이메일
- 호스트 이름, 즉 인증서를 교체하려고 하는 시스템의 정규화된 도메인 이름. 호스트 이름이 FQDN과 일치하지 않으면 인증서 교체가 올바르게 완료되지 않으며 환경이 불안정한 상태가 될 수 있습니다.
- vCenter Server의 IP 주소
- VMCA 이름, 즉 인증서 구성이 실행 중인 시스템의 FQDN(정규화된 도메인 이름)

참고 OU(organizationalUnitName) 필드는 더 이상 필수가 아닙니다.

사전 요구 사항

이 옵션으로 vSphere Certificate Manager를 실행할 때 다음 정보를 알고 있어야 합니다.

- administrator@vsphere.local의 암호
- 새 VMCA 서명 인증서를 생성하려는 시스템의 FDQN. 다른 모든 속성은 사전 정의된 값이 기본값으로 사용되지만 변경 가능합니다.

절차

1 vCenter Server 셸에 로그인하고 vSphere Certificate Manager를 시작합니다.

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

2 옵션 4, [새 VMCA 루트 인증서 다시 생성 및 모든 인증서 교체]를 선택합니다.

3 관리자 사용자 이름 및 암호를 입력합니다.

4 프롬프트에 응답합니다.

vSphere Certificate Manager가 사용자 입력을 기반으로 새로운 VMCA 루트 인증서를 생성하고 vSphere Certificate Manager를 실행 중인 시스템에 있는 모든 인증서를 교체합니다. vSphere Certificate Manager가 서비스를 다시 시작하면 교체 프로세스가 완료됩니다.

5 시스템 SSL 인증서를 교체하려면 옵션 3, [VMCA 인증서로 시스템 SSL 인증서 교체]와 함께 vSphere Certificate Manager를 실행합니다.

6 솔루션 사용자 인증서를 교체하려면 옵션 6, [솔루션 사용자 인증서를 VMCA 인증서로 교체]와 함께 Certificate Manager를 실행합니다.

Certificate Manager를 사용하여 VMCA를 중간 CA(인증 기관)로 만들기

vSphere Certificate Manager 유틸리티를 사용하여 VMCA를 중간 CA로 만들 수 있습니다. 해당 프로세스를 완료한 후 VMCA가 전체 체인으로 모든 새 인증서에 서명합니다. 원하는 경우 vSphere Certificate Manager를 사용하여 모든 기존 인증서를 새 VMCA 서명 인증서로 교체할 수 있습니다.

VMCA를 중간 CA로 만들려면 vSphere Certificate Manager를 여러 번 실행해야 합니다. 시스템 SSL 인증서와 솔루션 사용자 인증서를 모두 교체하는 개략적인 단계는 다음과 같습니다.

1 vSphere Certificate Manager 유틸리티를 시작합니다.

2 옵션 2, [사용자 지정 서명 인증서로 VMCA 루트 인증서 교체 및 모든 인증서 교체]를 실행하여 CSR을 생성합니다. 다음에 인증서에 대한 일부 정보를 제공해야 할 수 있습니다. 옵션을 다시 묻는 메시지가 표시되면 옵션 1, [VMCA 루트 서명 인증서에 대한 인증서 서명 요청 및 키 생성]을 선택합니다.

3 외부 또는 엔터프라이즈 CA에 CSR을 제출합니다. CA에서 서명된 인증서 및 루트 인증서가 수신됩니다.

4 VMCA 루트 인증서를 CA 루트 인증서와 결합하고 파일을 저장합니다.

5 옵션 2, [사용자 지정 서명 인증서로 VMCA 루트 인증서 교체 및 모든 인증서 교체]를 실행하여 인증서를 교체한 후 다음 메시지를 따릅니다. 이 프로세스는 로컬 시스템의 모든 인증서를 교체합니다.

6 (선택 사항) 고급 연결 모드 구성에서 여러 vCenter Server 인스턴스가 연결된 경우 다음 단계를 수행하여 각 노드에서 인증서를 교체합니다.

   a 우선 시스템 SSL 인증서를 새 VMCA 인증서로 교체합니다(옵션 3, [VMCA 인증서로 시스템 SSL 인증서 교체]).

   b 그런 다음 솔루션 사용자 인증서를 새 VMCA 인증서로 교체합니다(옵션 6, [솔루션 사용자 인증서를 VMCA 인증서로 교체]).

Certificate Manager를 사용하여 CSR 생성 및 루트 인증서(중간 CA) 준비

vSphere Certificate Manager 유틸리티를 사용하여 CSR(인증서 서명 요청)을 생성할 수 있습니다. 서명을 위해 이러한 CSR을 엔터프라이즈 CA 또는 외부 CA(인증 기관)에 제출합니다. 지원되는 다른 인증서 교체 프로세스를 통해 서명된 인증서를 사용할 수 있습니다.

- vSphere Certificate Manager를 사용하여 CSR을 생성할 수 있습니다.

  참고 vSphere 8.0 이상에서 vSphere Certificate Manager를 사용하여 CSR을 생성하는 경우 최소 키 크기가 2048비트에서 3072비트로 변경됩니다. vSphere 8.0 업데이트 1 이상에서는 vSphere Client를 사용하여 키 크기가 2048비트인 CSR을 생성합니다.

  참고 vSphere의 FIPS 인증서는 2048비트 및 3072비트의 RSA 키 크기만 검증합니다.

- CSR을 수동으로 생성하려는 경우에는 서명을 위해 보내는 인증서가 다음 요구 사항을 충족해야 합니다.
  - 키 크기: 2048비트(최소)~8192비트(최대)(PEM 인코딩)
  - PEM 형식. VMware는 PKCS8 및 PKCS1(RSA 키)을 지원합니다. 키가 VECS에 추가되면 해당 키가 PKCS8로 변환됩니다.
  - x509 버전 3
  - 루트 인증서에 대해 CA 확장을 true로 설정해야 하며 인증서 서명이 요구 사항 목록에 있어야 합니다. 예:

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

  - CRL 서명을 사용하도록 설정해야 합니다.
  - 확장 키 사용은 비워 두거나 서버 인증을 포함할 수 있습니다.
  - 인증서 체인의 길이에 대한 명시적 제한이 없습니다. VMCA는 OpenSSL 기본값인 10개의 인증서를 사용합니다.
  - 와일드카드 또는 2개 이상의 DNS 이름이 있는 인증서는 지원되지 않습니다.
  - VMCA의 부수적인 CA를 생성할 수 없습니다.

    Microsoft CA(인증 기관)를 사용하는 예는 VMware 기술 자료 문서(https://kb.vmware.com/s/article/2112009)인 'vSphere 6.x에서 SSL 인증서 생성에 사용할 Microsoft CA(인증 기관) 템플릿 생성'을 참조하십시오.

사전 요구 사항

vSphere Certificate Manager는 사용자에게 정보를 묻습니다. 묻는 정보는 해당 환경 및 사용자가 교체하려는 인증서의 유형에 따라 다릅니다.

CSR을 생성하는 경우 administrator@vsphere.local 사용자의 암호나 연결되어 있는 vCenter Single Sign-On 도메인 관리자의 암호를 묻습니다.

절차

1 vCenter Server 셸에 로그인하고 vSphere Certificate Manager를 시작합니다.

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

2 옵션 2를 선택하고 VMCA 루트 인증서를 사용자 지정 서명 인증서로 교체하고 모든 인증서를 교체합니다.

처음에는 이 옵션을 인증서를 교체하지 않고 CSR을 생성하는 데 사용합니다.

3 관리자 사용자 이름 및 암호를 입력합니다.

4 옵션 1, [VMCA 루트 서명 인증서에 대한 인증서 서명 요청 및 키 생성]을 선택하여 CSR을 생성하고 메시지에 응답합니다.

해당 프로세스의 일부로, 디렉토리를 제공해야 합니다. vSphere Certificate Manager는 서명할 인증서(`*.csr` 파일)와 해당 키 파일(`*.key` 파일)을 디렉토리에 배치합니다.

5 CSR(인증서 서명 요청)의 이름을 `root_signing_cert.csr`로 지정합니다.

6 서명을 위해 CSR을 엔터프라이즈 또는 외부 CA로 보내고 서명된 인증서의 이름을 `root_signing_cert.cer`로 지정합니다.

7 텍스트 편집기에서 인증서를 다음과 같이 결합합니다.

```
-----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 파일을 `root_signing_chain.cer`로 저장합니다.

다음에 수행할 작업

기존 루트 인증서를 체인 루트 인증서로 교체합니다. Certificate Manager를 사용하여 사용자 지정 서명 인증서로 VMCA 루트 인증서 교체 및 모든 인증서 교체의 내용을 참조하십시오.

Certificate Manager를 사용하여 사용자 지정 서명 인증서로 VMCA 루트 인증서 교체 및 모든 인증서 교체

vSphere Certificate Manager 유틸리티를 사용하여 CSR을 생성하고 서명을 위해 엔터프라이즈 또는 타사 CA에 CSR을 보낼 수 있습니다. 그런 다음 VMCA 루트 인증서를 사용자 지정 서명 인증서로 교체하고 모든 기존 인증서를 사용자 지정 CA에서 서명된 인증서로 교체할 수 있습니다.

vCenter Server에서 vSphere Certificate Manager를 실행하여 VMCA 루트 인증서를 사용자 지정 서명 인증서로 교체합니다.

사전 요구 사항

- 인증서 체인을 생성합니다.
  - vSphere Certificate Manager를 사용하여 CSR을 생성하거나 수동으로 CSR을 생성할 수 있습니다.
  - 타사 또는 엔터프라이즈 CA로부터 서명된 인증서를 받은 후에는 이 인증서를 초기 VMCA 루트 인증서와 결합하여 전체 체인을 생성합니다.

    인증서 요구 사항과 인증서 결합 프로세스는 Certificate Manager를 사용하여 CSR 생성 및 루트 인증서(중간 CA) 준비 항목을 참조하십시오.
- 필요한 정보를 수집합니다.
  - administrator@vsphere.local의 암호
  - 루트에 대한 유효한 사용자 지정 인증서(`.crt` 파일)
  - 루트에 유효한 사용자 지정 키(`.key` 파일)

절차

1 vCenter Server 셸에 로그인하고 vSphere Certificate Manager를 시작합니다.

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

2 옵션 2를 선택하고 VMCA 루트 인증서를 사용자 지정 서명 인증서로 교체하고 모든 인증서를 교체합니다.

3 관리자 사용자 이름 및 암호를 입력합니다.

4 옵션 2, [사용자 지정 인증서 및 키를 가져와서 기존 VMCA 루트 서명 인증서 교체]를 선택하고 메시지에 응답합니다.

   a 메시지가 표시되면 루트 인증서의 전체 경로를 지정합니다.

   b 인증서를 처음 교체하는 경우에는 시스템 SSL 인증서에 사용할 정보를 요청하는 메시지가 표시됩니다.

   이 정보는 시스템의 필수 FQDN을 포함하며, `certool.cfg` 파일에 저장됩니다.

Certificate Manager를 사용하여 시스템 SSL 인증서를 VMCA 인증서로 교체(중간 CA)

VMCA를 중간 CA로 사용하는 경우 vSphere Certificate Manager 유틸리티를 사용하여 시스템 SSL 인증서를 명시적으로 교체할 수 있습니다. 먼저 vCenter Server의 VMCA 루트 인증서를 교체한 다음, 시스템 SSL 인증서를 교체할 수 있습니다. 이것은 VMCA의 새로운 루트에 의해 서명됩니다. 또한 이 옵션을 사용하여 손상되거나 만료되려고 하는 시스템 SSL 인증서를 교체할 수 있습니다.

기존 시스템 SSL 인증서를 새 VMCA 서명 인증서로 교체하는 경우 vSphere Certificate Manager가 정보를 요청하며 vCenter Server의 암호와 IP 주소를 제외한 모든 값을 `certool.cfg` 파일에 입력합니다.

- administrator@vsphere.local의 암호
- 두 글자의 국가 코드
- 회사 이름

- 조직 이름
- 조직 구성 단위
- 상태
- 구/군/시
- IP 주소(선택 사항)
- 이메일
- 호스트 이름, 즉 인증서를 교체하려고 하는 시스템의 정규화된 도메인 이름. 호스트 이름이 FQDN과 일치하지 않으면 인증서 교체가 올바르게 완료되지 않으며 환경이 불안정한 상태가 될 수 있습니다.
- vCenter Server의 IP 주소
- VMCA 이름, 즉 인증서 구성이 실행 중인 시스템의 FQDN(정규화된 도메인 이름)

참고 OU(organizationalUnitName) 필드는 더 이상 필수가 아닙니다.

사전 요구 사항

- 이 옵션으로 vSphere Certificate Manager를 실행하려면 다음 정보를 알고 있어야 합니다.
  - administrator@vsphere.local의 암호
  - 새 VMCA 서명 인증서를 생성하려는 시스템의 FDQN. 다른 모든 속성은 사전 정의된 값이 기본값으로 사용되지만 변경 가능합니다.
  - vCenter Server 시스템의 호스트 이름 또는 IP 주소.

절차

1 vCenter Server 셸에 로그인하고 vSphere Certificate Manager를 시작합니다.

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

2 옵션 3, [시스템 SSL 인증서를 VMCA 인증서로 교체]를 선택합니다.

3 관리자 사용자 이름 및 암호를 입력합니다.

4 프롬프트에 응답합니다.

vSphere Certificate Manager가 `certool.cfg` 파일에 정보를 저장합니다.

결과

vSphere Certificate Manager가 시스템 SSL 인증서를 교체합니다.

Certificate Manager를 사용하여 솔루션 사용자 인증서를 VMCA 인증서로 교체(중간 CA)

VMCA를 중간 CA로 사용하는 경우 vSphere Certificate Manager 유틸리티를 사용하여 솔루션 사용자 인증서를 명시적으로 교체할 수 있습니다. 먼저 vCenter Server의 VMCA 루트 인증서를 교체한 다음, 솔루션 사용자

인증서를 교체할 수 있습니다. 이것은 VMCA의 새로운 루트에 의해 서명됩니다. 또한 이 옵션을 사용하여 손상되거나 만료 예정인 솔루션 인증서를 교체할 수 있습니다.

사전 요구 사항

- 고급 연결 모드 구성에서 여러 vCenter Server 인스턴스로 구성된 배포에서 VMCA 루트 인증서를 교체한 경우, 모든 vCenter Server 노드를 명시적으로 다시 시작합니다.
- 이 옵션으로 vSphere Certificate Manager를 실행하려면 다음 정보를 알고 있어야 합니다.
  - administrator@vsphere.local의 암호
  - vCenter Server 시스템의 호스트 이름 또는 IP 주소

절차

1 vCenter Server 셸에 로그인하고 vSphere Certificate Manager를 시작합니다.

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

2 옵션 6, [솔루션 사용자 인증서를 VMCA 인증서로 교체]를 선택합니다.

3 관리자 사용자 이름 및 암호를 입력합니다.

4 프롬프트에 응답합니다.

자세한 내용은 https://kb.vmware.com/s/article/2112281에서 VMware 기술 자료 문서를 참조하십시오.

결과

vSphere Certificate Manager가 모든 솔루션 사용자 인증서를 교체합니다.

Certificate Manager를 사용하여 모든 인증서를 사용자 지정 인증서로 교체

vSphere Certificate Manager 유틸리티를 사용하여 모든 인증서를 사용자 지정 인증서로 교체할 수 있습니다. 프로세스를 시작하기 전에 CSR을 CA(인증 기관)로 보내야 합니다. Certificate Manager를 사용하여 CSR을 생성할 수 있습니다.

옵션 하나는 시스템 SSL 인증서만 교체하고 VMCA에서 프로비저닝하는 솔루션 사용자 인증서를 사용하는 것입니다. 솔루션 사용자 인증서는 vSphere 구성 요소 간 통신에만 사용됩니다.

사용자 지정 인증서를 사용할 때 VMCA 서명 인증서를 사용자 지정 인증서로 교체합니다. vSphere Client, vSphere Certificate Manager 유틸리티 또는 수동 인증서 교체를 위한 CLI를 사용할 수 있습니다. 인증서는 VECS에 저장됩니다.

모든 인증서를 사용자 지정 인증서로 교체하려면 vSphere Certificate Manager 유틸리티를 여러 번 실행해야 합니다. 시스템 SSL 인증서와 솔루션 사용자 인증서를 모두 교체하는 개략적인 단계는 다음과 같습니다.

1 vSphere Certificate Manager 유틸리티를 시작합니다.

2 각 시스템에서 시스템 SSL 인증서 및 솔루션 사용자 인증서에 대한 인증서 서명 요청을 따로 생성합니다.

   a 시스템 SSL 인증서에 대한 CSR을 생성하려면 옵션 1, [시스템 SSL 인증서를 사용자 지정 인증서로 교체]를 선택합니다. 옵션을 다시 묻는 메시지가 표시되면 옵션 1, [시스템 SSL 인증서에 대한 인증서 서명 요청 및 키 생성]을 선택합니다.

   b 회사 정책이 하이브리드 배포를 허용하지 않는 경우 옵션 5, [솔루션 사용자 인증서를 사용자 지정 인증서로 교체]를 선택합니다.

3 외부 또는 엔터프라이즈 CA에 CSR을 제출합니다. CA에서 서명된 인증서 및 루트 인증서가 수신됩니다.

4 CA에서 서명된 인증서 및 루트 인증서를 수신한 후 옵션 1, [시스템 SSL 인증서를 사용자 지정 인증서로 교체]를 사용하여 각 시스템에서 시스템 SSL 인증서를 교체합니다.

5 솔루션 사용자 인증서도 교체하려면 옵션 5, [솔루션 사용자 인증서를 사용자 지정 인증서로 교체]를 선택합니다.

6 마지막으로, 여러 vCenter Server 인스턴스가 고급 연결 모드 구성에서 연결된 경우에는 각 노드에서 프로세스를 반복합니다.

Certificate Manager를 사용하여 인증서 서명 요청 생성(사용자 지정 인증서)

vSphere Certificate Manager 유틸리티를 사용하여, 엔터프라이즈 CA에서 사용하거나 외부 인증 기관에 전송할 수 있는 CSR(인증서 서명 요청)을 생성할 수 있습니다. 지원되는 다른 인증서 교체 프로세스를 통해 인증서를 사용할 수 있습니다.

사전 요구 사항

vSphere Certificate Manager는 사용자에게 정보를 묻습니다. 묻는 정보는 해당 환경 및 사용자가 교체하려는 인증서의 유형에 따라 다릅니다.

- CSR을 생성하는 경우 administrator@vsphere.local 사용자의 암호나 연결되어 있는 vCenter Single Sign-On 도메인 관리자의 암호를 묻습니다.
- vCenter Server의 호스트 이름 또는 IP주소를 묻는 메시지가 표시됩니다.
- 시스템 SSL 인증서에 대한 CSR을 생성하는 경우 `certool.cfg` 파일에 저장되는 인증서 속성을 묻습니다. 대부분의 필드에서 기본값을 수락하거나 사이트별 값을 제공할 수 있습니다. 시스템의 FQDN은 필수 항목입니다.

  참고 vSphere 8.0 이상에서 vSphere Certificate Manager를 사용하여 CSR을 생성하는 경우 최소 키 크기가 2048비트에서 3072비트로 변경됩니다. vSphere 8.0 업데이트 1 이상에서는 vSphere Client를 사용하여 키 크기가 2048비트인 CSR을 생성합니다.

  참고 vSphere의 FIPS 인증서는 2048비트 및 3072비트의 RSA 키 크기만 검증합니다.

절차

1 환경의 각 vCenter Server(vCenter Server셸)에 로그인하고 vSphere Certificate Manager를 시작합니다.

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

2 옵션 1, [시스템 SSL 인증서를 사용자 지정 인증서로 교체]를 선택합니다.

3 관리자 사용자 이름 및 암호를 입력합니다.

4 옵션 1, [시스템 SSL 인증서에 대한 인증서 서명 요청 및 키 생성]을 선택하여 CSR을 생성하고 메시지에 응답한 후 vSphere Certificate Manager를 종료합니다.

해당 프로세스의 일부로, 디렉토리를 제공해야 합니다. vSphere Certificate Manager가 디렉토리에 인증서 및 키 파일을 배치합니다.

5 모든 솔루션 사용자 인증서도 교체하려면 vSphere Certificate Manager를 다시 시작하고 옵션 5, [솔루션 사용자 인증서를 사용자 지정 인증서로 교체]를 선택합니다.

6 메시지가 표시되면 암호 및 vCenter Server IP 주소 또는 호스트 이름을 제공합니다.

7 옵션 1, [솔루션 사용자 인증서에 대한 인증서 서명 요청 및 키 생성]을 선택하여 CSR을 생성하고 메시지에 응답한 후 vSphere Certificate Manager를 종료합니다.

해당 프로세스의 일부로, 디렉토리를 제공해야 합니다. Certificate Manager가 디렉토리에 인증서 및 키 파일을 배치합니다.

다음에 수행할 작업

인증서 교체를 수행하려면 Certificate Manager를 사용하여 시스템 SSL 인증서를 사용자 지정 인증서로 교체의 내용을 참조하십시오.

Certificate Manager를 사용하여 시스템 SSL 인증서를 사용자 지정 인증서로 교체

vSphere Certificate Manager 유틸리티를 사용하여 각 노드의 시스템 SSL 인증서를 사용자 지정 인증서로 교체할 수 있습니다. 시스템 SSL 인증서는 모든 vCenter Server 노드에서 역방향 프록시 서비스가 사용합니다. 각 시스템마다 다른 서비스와의 보안 통신을 위한 시스템 SSL 인증서가 있어야 합니다.

사전 요구 사항

시작하기 전에 사용자 환경의 각 시스템에 대한 CSR이 필요합니다. vSphere Certificate Manager를 사용하거나 명시적으로 CSR을 생성할 수 있습니다.

1 vSphere Certificate Manager를 사용하여 CSR을 생성하려면 Certificate Manager를 사용하여 인증서 서명 요청 생성(사용자 지정 인증서)을 참조하십시오.

2 명시적으로 CSR을 생성하려면 타사 또는 엔터프라이즈 CA에 각 시스템용 인증서를 요청합니다. 인증서는 다음 요구 사항을 충족해야 합니다.

- 키 크기: 2048비트(최소)~8192비트(최대)(PEM 인코딩)
- CRT 형식

- x509 버전 3
- SubjectAltName에는 DNS Name=<machine_FQDN>이 포함되어야 합니다.
- 다음과 같은 키 사용이 포함되어 있습니다. 디지털 서명, 키 암호화

VMware 기술 자료 문서(https://kb.vmware.com/s/article/2112014)인 'Microsoft CA(인증 기관)에서 vSphere 인증서 받기'를 참조하십시오.

절차

1 vCenter Server에 로그인하고 vSphere Certificate Manager를 시작합니다.

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

2 옵션 1, [시스템 SSL 인증서를 사용자 지정 인증서로 교체]를 선택합니다.

3 관리자 사용자 이름 및 암호를 입력합니다.

4 옵션 2, [사용자 지정 인증서 및 키를 가져와서 기존 시스템 SSL 인증서 교체]를 선택하여 인증서 교체를 시작하고 메시지에 응답합니다.

vSphere Certificate Manager는 사용자에게 다음 정보를 묻습니다.

- administrator@vsphere.local의 암호
- 유효한 시스템 SSL 사용자 지정 인증서(`.crt` 파일)
- 유효한 시스템 SSL 사용자 지정 키(`.key` 파일)
- 사용자 지정 시스템 SSL 인증서에 대한 유효한 서명 인증서(`.crt` 파일)
- vCenter Server의 IP 주소

Certificate Manager를 사용하여 솔루션 사용자 인증서를 사용자 지정 인증서로 교체

대부분의 회사에서는 외부에서 액세스할 수 있는 서비스의 인증서만 교체하면 됩니다. 하지만 vSphere Certificate Manager 유틸리티는 솔루션 사용자 인증서를 교체하는 기능도 지원합니다. 솔루션 사용자는 서비스의 모음입니다. 예를 들어 vSphere Client와 연결된 모든 서비스입니다.

솔루션 사용자 인증서를 제공하라는 메시지가 표시되면 타사 CA의 전체 서명 인증서 체인을 제공합니다.

형식은 다음과 유사합니다.

```
-----BEGIN CERTIFICATE-----
Signing certificate
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
CA intermediate certificates
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
Root certificate of enterprise or external CA
-----END CERTIFICATE-----
```

사전 요구 사항

시작하기 전에 사용자 환경의 각 시스템에 대한 CSR이 필요합니다. vSphere Certificate Manager를 사용하거나 명시적으로 CSR을 생성할 수 있습니다.

1 vSphere Certificate Manager를 사용하여 CSR을 생성하려면 Certificate Manager를 사용하여 인증서 서명 요청 생성(사용자 지정 인증서)을 참조하십시오.

2 타사 또는 엔터프라이즈 CA에서 각 노드의 솔루션 사용자별로 인증서를 요청합니다. vSphere Certificate Manager를 사용하여 CSR을 생성하거나 직접 준비할 수 있습니다. CSR은 다음 요구 사항을 충족해야 합니다.

   - 키 크기: 2048비트(최소)~8192비트(최대)(PEM 인코딩)
   - CRT 형식
   - x509 버전 3
   - SubjectAltName에는 DNS Name=<machine_FQDN>이 포함되어야 합니다.
   - 각 솔루션 사용자 인증서마다 `Subject`가 서로 달라야 합니다. 예를 들어 솔루션 사용자 이름(예: vpxd) 또는 다른 고유한 ID를 포함하는 것을 고려하십시오.
   - 다음과 같은 키 사용이 포함되어 있습니다. 디지털 서명, 키 암호화

VMware 기술 자료 문서(http://kb.vmware.com/kb/2112014)인 'Microsoft CA(인증 기관)에서 vSphere 인증서 받기'를 참조하십시오.

절차

1 vCenter Server에 로그인하고 vSphere Certificate Manager를 시작합니다.

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

2 옵션 5, [솔루션 사용자 인증서를 사용자 지정 인증서로 교체]를 선택합니다.

3 SSO 사용자 이름 및 암호를 입력합니다.

4 옵션 2, [사용자 지정 인증서 및 키를 가져와서 기존 솔루션 사용자 인증서 교체]를 선택하고 메시지에 응답합니다.

   vSphere Certificate Manager는 사용자에게 다음 정보를 묻습니다.

   - administrator@vsphere.local의 암호
   - 시스템 솔루션 사용자의 인증서 및 키
   - 시스템 솔루션 사용자를 위한 인증서 및 키(`vpxd.crt` 및 `vpxd.key`)
   - 모든 솔루션 사용자를 위한 전체 인증서 및 키 집합(`vpxd.crt` 및 `vpxd.key`)

Certificate Manager로 이전 인증서를 다시 게시하여 직전에 수행한 작업 되돌리기

vSphere Certificate Manager 유틸리티를 사용하여 인증서 관리 작업을 수행할 때는 인증서가 교체되기 전에 현재 인증서 상태가 VECS의 BACKUP_STORE에 저장됩니다. 직전에 수행한 작업을 되돌려서 이전 상태로 돌아갈 수 있습니다.

참고 되돌리기 작업은 현재 BACKUP_STORE에 있는 항목을 복원합니다. 두 개의 서로 다른 옵션으로 vSphere Certificate Manager를 실행한 다음 되돌리기를 수행하면, 마지막 작업만 되돌려집니다..

절차

1 vCenter Server 셸에 로그인하고 vSphere Certificate Manager를 시작합니다.

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

2 옵션 7, [이전 인증서를 다시 게시하여 직전에 수행한 작업 되돌리기]를 선택합니다.

3 관리자 사용자 이름 및 암호를 입력합니다.

4 계속하려면 `Y`를 입력합니다.

Certificate Manager를 사용하여 모든 인증서 재설정

vSphere Certificate Manager 유틸리티를 사용하여 기존의 모든 vCenter 인증서를 VMCA에서 서명한 인증서로 교체합니다.

이 옵션을 사용하면 현재 VECS(VMware Endpoint Certificate Store)에 있는 모든 사용자 지정 인증서를 덮어씁니다.

vSphere Certificate Manager는 모든 인증서를 교체할 수 있습니다. 교체되는 인증서는 선택하는 옵션에 따라 달라집니다.

절차

1 vCenter Server 셸에 로그인하고 vSphere Certificate Manager를 시작합니다.

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

2 옵션 8, [모든 인증서 재설정]을 선택합니다.

3 관리자 사용자 이름 및 암호를 입력합니다.

4 메시지가 표시되면 인증서 정보를 입력합니다.

다음에 수행할 작업

인증서가 교체되고 서비스가 다시 시작되면 인증서 정보를 확인합니다.

vSphere 인증서 수동 교체

일부 특수 인증서 교체 사례의 경우 vSphere Certificate Manager 유틸리티를 사용할 수 없습니다. 대신 설치에 포함된 CLI를 인증서 교체에 사용할 수 있습니다.

vCenter Server 서비스 중지 및 시작에 대한 지침

수동 인증서 교체의 특정 부분에서는 모든 vCenter Server 서비스를 중지한 다음 인증서 인프라를 관리하는 서비스만 시작해야 합니다. 필요할 때만 서비스를 중지하면 다운타임을 최소화할 수 있습니다.

인증서 교체 프로세스의 일부로 서비스를 중지하고 시작해야 합니다. 서비스 시작 및 중지를 위해 `service-control` 명령을 사용할 수 있습니다. 모든 서비스 또는 개별 서비스를 시작하고 중지할 수 있습니다. 자세한 내용은 명령줄 도움말을 참조하십시오.

다음 지침을 따르십시오.

- 새 공개/개인 키 쌍이나 새 인증서를 생성하기 위해 서비스를 중지하지 마십시오.
- 자신이 유일한 관리자일 경우에는 새 루트 인증서를 추가할 때 서비스를 중지할 필요가 없습니다. 이전 루트 인증서를 계속 사용할 수 있으며 모든 서비스가 계속해서 해당 인증서로 인증할 수 있습니다.
- VECS(VMware Endpoint 인증서 저장소)에서 시스템 SSL 인증서를 삭제하기 바로 전에 서비스를 중지합니다.

CLI를 사용하여 기존 VMCA 서명 인증서를 VMCA 서명 인증서로 교체

VMCA(VMware Certificate Authority) 루트 인증서가 곧 만료되거나 다른 이유로 이를 교체하려는 경우, CLI를 사용하여 새 루트 인증서를 생성하고 VMware 디렉토리 서비스에 추가할 수 있습니다. 그런 다음 새 루트 인증서를 사용하여 새 시스템 SSL 인증서 및 솔루션 사용자 인증서를 생성할 수 있습니다.

대개의 경우 vSphere Certificate Manager 유틸리티를 사용하여 인증서를 교체합니다.

세밀한 제어가 필요한 경우 이 시나리오는 CLI 명령을 사용하여 전체 인증서 집합을 교체하는 방법에 대한 자세한 단계별 안내를 제공합니다. 해당 작업의 절차를 사용하여 개별 인증서만 교체할 수도 있습니다.

사전 요구 사항

administrator@vsphere.local 또는 CAAdmins 그룹의 다른 사용자만 인증서 관리 작업을 수행할 수 있습니다. vCenter Single Sign-On 그룹에 멤버 추가의 내용을 참조하십시오.

CLI를 사용하여 새 VMCA 서명 루트 인증서 생성

`certool` CLI를 사용하여 새 VMCA 서명 인증서를 생성하고 이 인증서를 vmdir에 게시할 수 있습니다.

절차

1 vCenter Server에서 새 자체 서명 인증서 및 개인 키를 생성합니다.

```
certool --genselfcacert --outprivkey <key_file_path> --outcert <cert_file_path> --config
<config_file>
```

2 기존 루트 인증서를 새 인증서로 교체합니다.

```
certool --rootca --cert <cert_file_path> --privkey <key_file_path>
```

명령은 인증서를 생성하여 vmdir에 추가하고 VECS에 추가합니다.

3 모든 서비스를 중지하고 인증서 생성, 전파 및 저장을 처리하는 서비스를 시작합니다.

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

4 (선택 사항) 새 루트 인증서를 vmdir에 게시합니다.

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

명령은 vmdir의 모든 인스턴스를 즉시 업데이트합니다. 명령을 실행하지 않으면 새 인증서를 모든 노드에 전파하는 데 상당한 시간이 소요될 수 있습니다.

5 모든 서비스를 다시 시작합니다.

```
service-control --start --all
```

예제: 새 VMCA 서명 루트 인증서 생성

다음 예에서는 현재 루트 CA 정보를 확인하고 루트 인증서를 다시 생성하는 전체 단계를 보여 줍니다.

1 (선택 사항) vCenter Server에서 VMCA 루트 인증서를 나열하여 인증서 저장소에 있는지 확인합니다.

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

출력은 다음과 비슷합니다.

```
output:
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            cf:2d:ff:49:88:50:e5:af
    ...
```

2 (선택 사항) VECS TRUSTED_ROOTS 저장소를 나열하고 여기의 인증서 일련 번호를 1단계의 출력과 비교합니다.

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

루트 인증서가 하나만 있는 가장 간단한 경우 출력은 다음과 비슷합니다.

```
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 새 VMCA 루트 인증서를 생성합니다. 명령은 인증서를 VECS 및 vmdir(VMware Directory Service)의 TRUSTED_ROOTS 저장소에 추가합니다.

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

CLI를 사용하여 시스템 SSL 인증서를 VMCA 서명 인증서로 교체

새 VMCA 서명 루트 인증서를 생성한 후에는 `vecs-cli` 명령을 사용하여 환경의 모든 시스템 SSL 인증서를 교체할 수 있습니다.

각 시스템마다 다른 서비스와의 보안 통신을 위한 시스템 SSL 인증서가 있어야 합니다. 여러 vCenter Server 인스턴스가 고급 연결 모드 구성에서 연결된 경우 각 노드에서 시스템 SSL 인증서 생성 명령을 실행해야 합니다.

사전 요구 사항

모든 서비스를 중지하고 인증서 전파 및 저장을 처리하는 서비스를 시작할 준비를 마칩니다.

절차

1 새 인증서가 필요한 각 시스템에 대해 `certool.cfg` 사본 하나를 만듭니다.

`certool.cfg` 파일은 `/usr/lib/vmware-vmca/share/config/` 디렉토리에 있습니다.

2 해당 시스템의 FQDN을 포함하도록 각 시스템의 사용자 지정 구성 파일을 편집합니다.

시스템의 IP 주소에 대해 `NSLookup`을 실행하여 이름의 DNS 목록을 확인하고 이 이름을 파일의 Hostname 필드에 사용합니다.

3 공개/개인 키 파일 쌍과 각 파일에 대한 인증서를 생성하고 직전에 사용자 지정한 구성 파일을 사용하여 전달합니다.

예:

```
certool --genkey --privkey=machine1.priv --pubkey=machine1.pub
certool --gencert --privkey=machine1.priv --cert machine1.crt --Name=Machine1_Cert --
config machine1.cfg
```

4 모든 서비스를 중지하고 인증서 생성, 전파 및 저장을 처리하는 서비스를 시작합니다.

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

5 VECS에 새 인증서를 추가합니다.

모든 시스템은 SSL을 통해 통신하려면 로컬 인증서 저장소에 새 인증서가 필요합니다. 먼저 기존 항목을 삭제한 다음 새 항목을 추가합니다.

```
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 모든 서비스를 다시 시작합니다.

```
service-control --start --all
```

예제: 시스템 인증서를 VMCA 서명 인증서로 교체

1 SSL 인증서에 대한 구성 파일을 만들고 이를 현재 디렉토리에 `ssl-config.cfg`로 저장합니다.

```
Country = US
Name = vmca-<FQDN-example>
Organization = <my_company>
OrgUnit = <my_company Engineering>
State = <my_state>
Locality = <mytown>
Hostname = <FQDN>
```

2 시스템 SSL 인증서에 대한 키 쌍을 생성합니다. 고급 연결 모드 구성에서 연결된 여러 vCenter Server 인스턴스를 배포할 때 각 vCenter Server 노드에서 이 명령을 실행합니다.

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

`ssl-key.priv` 및 `ssl-key.pub` 파일이 현재 디렉토리에 생성됩니다.

3 새 시스템 SSL 인증서를 생성합니다. 이 인증서는 VMCA에 의해 서명됩니다. VMCA 루트 인증서를 사용자 지정 인증서로 교체한 경우 VMCA가 전체 체인을 사용하여 모든 인증서에 서명합니다.

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

`new-vmca-ssl.crt` 파일이 현재 디렉토리에 생성됩니다.

4 (선택 사항) VECS의 내용을 나열합니다.

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

- vCenter Server의 샘플 출력:

```
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 VECS의 시스템 SSL 인증서를 새로운 시스템 SSL 인증서로 교체합니다. `--store` 및 `--alias` 값은 기본 이름과 정확하게 일치해야 합니다.

- 각 vCenter Server에서 다음 명령을 실행하여 MACHINE_SSL_CERT 저장소의 시스템 SSL 인증서를 업데이트합니다. FQDN이 서로 다르므로 각 시스템용 인증서를 개별적으로 업데이트해야 합니다.

```
/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
```

다음에 수행할 작업

ESXi 호스트의 인증서를 교체할 수도 있습니다. "vSphere 보안" 자료를 참조하십시오.

CLI를 사용하여 솔루션 사용자 인증서를 새 VMCA 서명된 인증서로 교체

시스템 SSL 인증서를 교체한 후에는 `dir-cli` 명령을 사용하여 모든 솔루션 사용자 인증서를 교체할 수 있습니다. 솔루션 사용자는 만료되지 않은 유효한 상태여야 하지만 인증서 인프라는 인증서의 다른 정보를 사용하지 않습니다.

대부분의 VMware 고객은 솔루션 사용자 인증서를 교체하지 않고 시스템 SSL 인증서만 사용자 지정 인증서로 교체합니다. 이러한 하이브리드 방식은 사용자의 보안 팀 요구 사항을 충족합니다.

- 인증서는 프록시 뒤에 있는 인증서이거나, 사용자 지정 인증서입니다.
- 중간 CA는 사용되지 않습니다.

각 vCenter Server 시스템에서 시스템 솔루션 사용자 인증서와 솔루션 사용자 인증서를 교체합니다.

참고 대규모 배포의 솔루션 사용자 인증서를 나열할 경우 `/usr/lib/vmware-vmafd/bin/dir-cli list`의 출력에는 모든 노드의 모든 솔루션 사용자가 포함됩니다. 각 호스트의 로컬 시스템 ID를 찾으려면 `/usr/lib/vmware-vmafd/bin/vmafd-cli get-machine-id --server-name localhost`를 실행하십시오. 각 솔루션 사용자 이름에 시스템 ID가 포함되어 있습니다.

사전 요구 사항

모든 서비스를 중지하고 인증서 전파 및 저장을 처리하는 서비스를 시작할 준비를 마칩니다.

절차

1 `certool.cfg` 사본을 하나 만든 다음 이름, IP 주소, DNS 이름, 이메일 필드를 제거하고 파일의 이름을 변경합니다(예: `sol_usr.cfg`).

생성 과정의 일부로 명령줄에서 인증서의 이름을 지정할 수 있습니다. 기타 정보는 솔루션 사용자에게 필요하지 않습니다. 기본 정보를 그대로 두면 생성된 인증서가 혼란을 줄 수 있습니다.

2 공개/개인 키 파일 쌍과 각 솔루션 사용자에 대한 인증서를 생성하고 직전에 사용자 지정한 구성 파일을 사용하여 전달합니다.

예:

```
/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 각 솔루션 사용자의 이름을 찾습니다.

```
/usr/lib/vmware-vmafd/bin/dir-cli service list
```

인증서를 교체할 때 반환된 고유 ID를 사용할 수 있습니다. 입력 및 출력이 다음과 같을 수 있습니다.

```
/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
```

고급 연결 모드 구성에서 연결된 여러 vCenter Server 인스턴스를 배포하는 경우 `/usr/lib/vmware-vmafd/bin/dir-cli service list`의 출력에 모든 노드의 모든 솔루션 사용자가 포함됩니다. 각 호스트의 로컬 시스템 ID를 찾으려면 `/usr/lib/vmware-vmafd/bin/vmafd-cli get-machine-id --server-name localhost`를 실행하십시오. 각 솔루션 사용자 이름에 시스템 ID가 포함되어 있습니다.

4 모든 서비스를 중지하고 인증서 생성, 전파 및 저장을 처리하는 서비스를 시작합니다.

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

5 각 솔루션 사용자에 대해 vmdir 및 VECS에서 차례로 기존 인증서를 교체합니다.

다음 예는 vpxd 서비스에 대한 인증서를 교체하는 방법을 보여 줍니다.

```
/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
```

참고 vmdir에서 인증서를 교체하지 않으면 솔루션 사용자가 vCenter Single Sign-On에 인증할 수 없습니다.

6 모든 서비스를 다시 시작합니다.

```
service-control --start --all
```

예제: VMCA 서명 솔루션 사용자 인증서 사용

1 고급 연결 모드 구성에서 각 vCenter Server 노드의 솔루션 사용자 각각에 대해 공개/개인 키 쌍을 생성합니다. 여기에는 시스템 솔루션에 대한 쌍과 각 추가 솔루션 사용자(vpxd, vpxd-extension, vsphere-webclient, wcp)에 대한 쌍이 포함됩니다.

a 시스템 솔루션 사용자에 대한 키 쌍을 생성합니다.

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

b 각 노드에서 vpxd 솔루션 사용자에 대한 키 쌍을 생성합니다.

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

c 각 노드에서 vpxd-extension 솔루션 사용자에 대한 키 쌍을 생성합니다.

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

d 각 노드에서 vsphere-webclient 솔루션 사용자에 대한 키 쌍을 생성합니다.

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

e 각 노드에서 wcp 솔루션 사용자에 대한 키 쌍을 생성합니다.

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

2 각 vCenter Server 노드의 시스템 솔루션 사용자 및 각 추가 솔루션 사용자(vpxd, vpxd-extension, vsphere-webclient, wcp)에 대해 새 VMCA 루트 인증서로 서명된 솔루션 사용자 인증서를 생성합니다.

참고 `--Name` 매개 변수는 고유해야 합니다. 솔루션 사용자 저장소의 이름을 포함하면 각 인증서가 어느 솔루션 사용자에게 매핑되는지 쉽게 확인할 수 있습니다. 이 예제에서는 각각에 `vpxd` 또는 `vpxd-extension` 같은 이름이 포함됩니다.

a `/usr/lib/vmware-vmca/share/config/certool.cfg` 파일의 복사본 하나를 만든 다음, 필요에 따라 이름, IP 주소, DNS 이름 및 이메일 필드를 수정하거나 제거하고 파일 이름을 바꿉니다(예: `sol_usr.cfg`).

b 각 노드에서 시스템 솔루션 사용자용 인증서를 생성합니다.

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

c 각 노드에서 vpxd 솔루션 사용자용 인증서를 생성합니다.

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

d 각 노드에서 vpxd-extensions 솔루션 사용자용 인증서를 생성합니다.

```
/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 다음 명령을 실행하여 각 노드에서 vsphere-webclient 솔루션 사용자용 인증서를 생성합니다.

```
/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 다음 명령을 실행하여 각 노드에서 wcp 솔루션 사용자의 인증서를 생성합니다.

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

3 VECS의 솔루션 사용자 인증서를 새 솔루션 사용자 인증서로 교체합니다.

참고 `--store` 및 `--alias` 매개 변수는 서비스의 기본 이름과 정확하게 일치해야 합니다.

a 각 노드에서 시스템 솔루션 사용자 인증서를 교체합니다.

```
/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 각 노드에서 vpxd 솔루션 사용자 인증서를 교체합니다.

```
/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 각 노드에서 vpxd-extension 솔루션 사용자 인증서를 교체합니다.

```
/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 각 노드에서 vsphere-webclient 솔루션 사용자 인증서를 교체합니다.

```
/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 각 노드에서 wcp 솔루션 사용자 인증서를 교체합니다.

```
/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 VMware 디렉토리 서비스(vmdir)를 새 솔루션 사용자 인증서로 업데이트합니다. vCenter Single Sign-On 관리자 암호를 묻는 메시지가 나타납니다.

a `/usr/lib/vmware-vmafd/bin/dir-cli service list`를 실행하여 각 솔루션 사용자에 대한 고유한 서비스 ID 접미사를 가져옵니다. 이 명령은 vCenter Server 시스템에서 실행합니다.

```
/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
```

참고 대규모 배포의 솔루션 사용자 인증서를 나열할 경우 `/usr/lib/vmware-vmafd/bin/dir-cli list`의 출력에는 모든 노드의 모든 솔루션 사용자가 포함됩니다. 각 호스트의 로컬 시스템 ID를 찾으려면 `/usr/lib/vmware-vmafd/bin/vmafd-cli get-machine-id --server-name localhost`를 실행하십시오. 각 솔루션 사용자 이름에 시스템 ID가 포함되어 있습니다.

b 각 vCenter Server 노드에서 vmdir의 시스템 인증서를 교체합니다. 예를 들어 machine-6fd7f140-60a9-11e4-9e28-005056895a69가 vCenter Server의 시스템 솔루션 사용자인 경우 이 명령을 실행하십시오.

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

c 각 노드에서 vmdir의 vpxd 솔루션 사용자 인증서를 교체합니다. 예를 들어 vpxd-6fd7f140-60a9-11e4-9e28-005056895a69가 vpxd 솔루션 사용자 ID인 경우 이 명령을 실행하십시오.

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

d 각 노드에서 vmdir의 vpxd-extension 솔루션 사용자 인증서를 교체합니다. 예를 들어 vpxd-extension-6fd7f140-60a9-11e4-9e28-005056895a69가 vpxd-extension 솔루션 사용자 ID인 경우 이 명령을 실행하십시오.

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

e 각 노드에서 vsphere-webclient 솔루션 사용자 인증서를 교체합니다. 예를 들어 vsphere-webclient-6fd7f140-60a9-11e4-9e28-005056895a69가 vsphere-webclient 솔루션 사용자 ID인 경우 이 명령을 실행하십시오.

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

f 각 노드에서 wcp 솔루션 사용자 인증서를 교체합니다. 예를 들어 wcp-1cbe0a40-e4ce-4378-b5e7-9460e2b8200e이 wcp 솔루션 사용자 ID이면 다음 명령을 실행합니다.

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

다음에 수행할 작업

각 vCenter Server 노드에서 모든 서비스를 다시 시작합니다.

CLI를 사용하여 VMCA를 중간 CA(인증 기관)로 만들기

CLI를 사용하여 VMCA 루트 인증서를 인증서 체인에 VMCA가 포함된 타사 CA 서명 인증서로 교체할 수 있습니다. 그러면 VMCA가 생성하는 모든 인증서에 전체 체인이 포함됩니다. 기존 인증서를 새로 생성된 인증서로 교체할 수 있습니다.

VMCA를 중간 CA로 사용하거나 사용자 지정 인증서를 사용하면 상당히 복잡한 문제가 발생할 수 있어 보안에 부정적인 영향을 미칠 수 있으며 운영 위험이 불필요하게 증가할 수 있습니다. vSphere 환경 내의 인증서 관리에 대한 자세한 내용은 http://vmware.com/go/hybridvmca에서 블로그 게시글 "New Product Walkthrough - Hybrid vSphere SSL Certificate Replacement(신제품 둘러보기 - 하이브리드 vSphere SSL 인증서 교체)"를 참조하십시오.

CLI를 사용하여 루트 인증서 교체(중간 CA)

VMCA 인증서를 사용자 지정 인증서로 교체하는 첫 번째 단계는 CSR을 생성하고, 서명할 CSR을 보내고, CLI를 사용하여 서명된 인증서를 VMCA에 루트 인증서로 추가하는 것입니다.

Certificate Manager 유틸리티 또는 기타 도구를 사용하여 CSR을 생성할 수 있습니다. CSR은 다음 요구 사항을 충족해야 합니다.

- 키 크기: 2048비트(최소)~8192비트(최대)(PEM 인코딩)
- PEM 형식. VMware는 PKCS8 및 PKCS1(RSA 키)을 지원합니다. 키가 VECS에 추가되면 해당 키가 PKCS8로 변환됩니다.
- x509 버전 3
- 루트 인증서에 대해 CA 확장을 true로 설정해야 하며 인증서 서명이 요구 사항 목록에 있어야 합니다. 예:

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

- CRL 서명을 사용하도록 설정해야 합니다.
- 확장 키 사용은 비워 두거나 서버 인증을 포함할 수 있습니다.
- 인증서 체인의 길이에 대한 명시적 제한이 없습니다. VMCA는 OpenSSL 기본값인 10개의 인증서를 사용합니다.
- 와일드카드 또는 2개 이상의 DNS 이름이 있는 인증서는 지원되지 않습니다.
- VMCA의 부수적인 CA를 생성할 수 없습니다.

  Microsoft CA(인증 기관)를 사용하는 예는 VMware 기술 자료 문서(https://kb.vmware.com/s/article/2112009)인 'vSphere 6.x에서 SSL 인증서 생성에 사용할 Microsoft CA(인증 기관) 템플릿 생성'을 참조하십시오.

참고 vSphere의 FIPS 인증서는 2048비트 및 3072비트의 RSA 키 크기만 검증합니다.

VMCA는 사용자가 루트 인증서를 교체할 때 다음의 인증서 특성을 확인합니다.

- 키 크기: 2048비트(최소)~8192비트(최대)
- 키 용도: 인증서 서명
- 기본 제약 조건: 주체 유형 CA

절차

1 CSR을 생성하여 CA에 보냅니다.

CA의 지시사항을 따릅니다.

2 서명된 VMCA 인증서와 타사 CA 또는 엔터프라이즈 CA의 전체 CA 체인이 함께 포함된 인증서 파일을 준비하고, `rootca1.crt`와 같은 이름으로 파일을 저장합니다.

이렇게 하려면 PEM 형식의 모든 CA 인증서를 하나의 파일로 복사합니다. VMCA 루트 인증서부터 시작하여 루트 CA PEM 인증서에서 마쳐야 합니다. 예:

```
-----BEGIN CERTIFICATE-----
<Certificate of VMCA>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Certificate of intermediary CA>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Certificate of Root CA>
-----END CERTIFICATE-----
```

3 모든 서비스를 중지하고 인증서 생성, 전파 및 저장을 처리하는 서비스를 시작합니다.

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

4 기존 VMCA 루트 CA를 교체합니다.

```
certool --rootca --cert=rootca1.crt --privkey=root1.key
```

이 명령은 실행 시 다음을 수행합니다.

- 파일 시스템의 인증서 위치에 새 사용자 지정 루트 인증서를 추가합니다.
- VCES의 TRUSTED_ROOTS 저장소에 사용자 지정 루트 인증서를 추가합니다(지연 후).
- vmdir에 사용자 지정 루트 인증서를 추가합니다(지연 후).

5 (선택 사항) 변경 내용을 vmdir(VMware 디렉토리 서비스)의 모든 인스턴스로 전파하려면 새 루트 인증서를 vmdir로 게시합니다. 이 때 각 파일의 전체 파일 경로를 제공합니다.

예를 들어 인증서의 체인에 인증서가 하나만 있는 경우:

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

인증서의 체인에 인증서가 두 개 이상 있는 경우:

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

30초마다 vmdir 노드 간 복제가 수행됩니다. VECS는 5분마다 vmdir을 폴링하여 새 루트 인증서 파일을 검색하므로 루트 인증서를 VECS에 명시적으로 추가할 필요가 없습니다.

6 (선택 사항) 필요한 경우 VECS를 강제로 새로 고칠 수 있습니다.

```
vecs-cli force-refresh
```

7 모든 서비스를 다시 시작합니다.

```
service-control --start --all
```

예제: 루트 인증서 교체

`certool` 명령을 `--rootca` 옵션과 함께 사용하여 VMCA 루트 인증서를 사용자 지정 CA 루트 인증서로 교체합니다.

```
/usr/lib/vmware-vmca/bin/certool --rootca --cert=<path>/root.pem --privkey=<path>/root.key
```

이 명령은 실행 시 다음을 수행합니다.

- 파일 시스템의 인증서 위치에 새 사용자 지정 루트 인증서를 추가합니다.
- VCES의 TRUSTED_ROOTS 저장소에 사용자 지정 루트 인증서를 추가합니다.
- 사용자 지정 루트 인증서를 vmdir에 추가합니다.

다음에 수행할 작업

회사 정책에 따라 필요한 경우 원래 VMCA 루트 인증서를 인증서 저장소에서 제거할 수 있습니다. 그렇게 하는 경우 vCenter Single Sign-On 서명 인증서를 교체해야 합니다. 명령줄을 사용하여 vCenter Server STS 인증서 교체의 내용을 참조하십시오.

CLI를 사용하여 시스템 SSL 인증서 교체(중간 CA)

CA에서 서명된 인증서를 받은 후에는 CLI를 사용하여 이 인증서를 VMCA 루트 인증서로 만들고 모든 시스템 SSL 인증서를 교체할 수 있습니다.

이러한 단계는 VMCA를 인증 기관으로 사용하는 인증서로 교체하는 단계와 기본적으로 동일합니다. 하지만 이 경우에는 VMCA가 전체 체인으로 모든 인증서에 서명합니다.

각 시스템마다 다른 서비스와의 보안 통신을 위한 시스템 SSL 인증서가 있어야 합니다. 여러 vCenter Server 인스턴스가 고급 연결 모드 구성에서 연결된 경우 각 노드에서 시스템 SSL 인증서 생성 명령을 실행해야 합니다.

사전 요구 사항

각 시스템 SSL 인증서에 대해 `SubjectAltName`에 `DNS Name=<Machine FQDN>`이 포함되어야 합니다.

절차

1 새 인증서가 필요한 각 시스템에 대해 `certool.cfg` 사본 하나를 만듭니다.

`certool.cfg` 파일은 `/usr/lib/vmware-vmca/share/config/` 디렉토리에 있습니다.

2 해당 시스템의 FQDN을 포함하도록 각 시스템의 사용자 지정 구성 파일을 편집합니다.

시스템의 IP 주소에 대해 `NSLookup`을 실행하여 이름의 DNS 목록을 확인하고 이 이름을 파일의 Hostname 필드에 사용합니다.

3 공개/개인 키 파일 쌍과 각 시스템에 대한 인증서를 생성하고 직전에 사용자 지정한 구성 파일에 전달합니다.

예:

```
certool --genkey --privkey=machine1.priv --pubkey=machine1.pub
certool --gencert --privkey=machine1.priv --cert machine42.crt --Name=Machine42_Cert --
config machine1.cfg
```

4 모든 서비스를 중지하고 인증서 생성, 전파 및 저장을 처리하는 서비스를 시작합니다.

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

5 VECS에 새 인증서를 추가합니다.

모든 시스템은 SSL을 통해 통신하려면 로컬 인증서 저장소에 새 인증서가 필요합니다. 먼저 기존 항목을 삭제한 다음 새 항목을 추가합니다.

```
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 모든 서비스를 다시 시작합니다.

```
service-control --start --all
```

예제: 시스템 SSL 인증서 교체(VMCA가 중간 CA)

1 SSL 인증서에 대한 구성 파일을 만들고 이를 현재 디렉토리에 `ssl-config.cfg`로 저장합니다.

```
Country = US
Name = vmca-<FQDN-example>
Organization = VMware
OrgUnit = VMware Engineering
State = California
Locality = Palo Alto
Hostname = <FQDN>
```

2 시스템 SSL 인증서에 대한 키 쌍을 생성합니다. 고급 연결 모드 구성에서 연결된 여러 vCenter Server 인스턴스를 배포할 때 각 vCenter Server 노드에서 이 명령을 실행합니다.

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

`ssl-key.priv` 및 `ssl-key.pub` 파일이 현재 디렉토리에 생성됩니다.

3 새 시스템 SSL 인증서를 생성합니다. 이 인증서는 VMCA에 의해 서명됩니다. VMCA 루트 인증서를 사용자 지정 인증서로 교체한 경우 VMCA가 전체 체인을 사용하여 모든 인증서에 서명합니다.

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

`new-vmca-ssl.crt` 파일이 현재 디렉토리에 생성됩니다.

4 (선택 사항) VECS의 내용을 나열합니다.

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

- vCenter Server의 샘플 출력:

```
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 VECS의 시스템 SSL 인증서를 새로운 시스템 SSL 인증서로 교체합니다. `--store` 및 `--alias` 값은 기본 이름과 정확하게 일치해야 합니다.

- 각 vCenter Server에서 다음 명령을 실행하여 MACHINE_SSL_CERT 저장소의 시스템 SSL 인증서를 업데이트합니다. FQDN이 서로 다르므로 각 시스템용 인증서를 개별적으로 업데이트해야 합니다.

```
/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
```

CLI를 사용하여 솔루션 사용자 인증서 교체(중간 CA)

시스템 SSL 인증서를 교체한 후에는 CLI를 사용하여 솔루션 사용자 인증서를 교체할 수 있습니다.

대부분의 VMware 고객은 솔루션 사용자 인증서를 교체하지 않고 시스템 SSL 인증서만 사용자 지정 인증서로 교체합니다. 이러한 하이브리드 방식은 사용자의 보안 팀 요구 사항을 충족합니다.

- 인증서는 프록시 뒤에 있는 인증서이거나, 사용자 지정 인증서입니다.
- 중간 CA는 사용되지 않습니다.

각 vCenter Server 시스템에서 시스템 솔루션 사용자 인증서와 솔루션 사용자 인증서를 교체합니다.

참고 대규모 배포의 솔루션 사용자 인증서를 나열할 경우 `/usr/lib/vmware-vmafd/bin/dir-cli list`의 출력에는 모든 노드의 모든 솔루션 사용자가 포함됩니다. 각 호스트의 로컬 시스템 ID를 찾으려면 `/usr/lib/vmware-vmafd/bin/vmafd-cli get-machine-id --server-name localhost`를 실행하십시오. 각 솔루션 사용자 이름에 시스템 ID가 포함되어 있습니다.

사전 요구 사항

각 솔루션 사용자 인증서마다 `Subject`가 서로 달라야 합니다. 예를 들어 솔루션 사용자 이름(예: vpxd) 또는 다른 고유한 ID를 포함하는 것을 고려하십시오.

절차

1 `certool.cfg` 사본을 하나 만든 다음 이름, IP 주소, DNS 이름, 이메일 필드를 제거하고 파일의 이름을 변경합니다(예: `sol_usr.cfg`).

생성 과정의 일부로 명령줄에서 인증서의 이름을 지정할 수 있습니다. 기타 정보는 솔루션 사용자에게 필요하지 않습니다. 기본 정보를 그대로 두면 생성된 인증서가 혼란을 줄 수 있습니다.

2 공개/개인 키 파일 쌍과 각 솔루션 사용자에 대한 인증서를 생성하고 직전에 사용자 지정한 구성 파일을 사용하여 전달합니다.

예:

```
certool --genkey --privkey=vpxd.priv --pubkey=vpxd.pub
certool --gencert --privkey=vpxd.priv --cert vpxd.crt --Name=VPXD_1 --config sol_usr.cfg
```

3 각 솔루션 사용자의 이름을 찾습니다.

```
/usr/lib/vmware-vmafd/bin/dir-cli service list
```

인증서를 교체할 때 반환된 고유 ID를 사용할 수 있습니다. 입력 및 출력이 다음과 같을 수 있습니다.

```
/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
```

고급 연결 모드 구성에서 연결된 여러 vCenter Server 인스턴스를 배포하는 경우 `/usr/lib/vmware-vmafd/bin/dir-cli service list`의 출력에 모든 노드의 모든 솔루션 사용자가 포함됩니다. 각 호스트의 로컬 시스템 ID를 찾으려면 `/usr/lib/vmware-vmafd/bin/vmafd-cli get-machine-id --server-name localhost`를 실행하십시오. 각 솔루션 사용자 이름에 시스템 ID가 포함되어 있습니다.

4 모든 서비스를 중지하고 인증서 생성, 전파 및 저장을 처리하는 서비스를 시작합니다.

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

5 vmdir과 VECS에서 차례로 기존 인증서를 교체합니다.

솔루션 사용자의 경우 이 순서대로 인증서를 추가해야 합니다. 예:

```
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
```

참고 vmdir에서 인증서를 교체하지 않으면 솔루션 사용자가 vCenter Single Sign-On에 로그인할 수 없습니다.

6 모든 서비스를 다시 시작합니다.

```
service-control --start --all
```

예제: 솔루션 사용자 인증서 교체(중간 CA)

1 고급 연결 모드 구성에서 각 vCenter Server 노드의 솔루션 사용자 각각에 대해 공개/개인 키 쌍을 생성합니다. 여기에는 시스템 솔루션에 대한 쌍과 각 추가 솔루션 사용자(vpxd, vpxd-extension, vsphere-webclient, wcp)에 대한 쌍이 포함됩니다.

a 시스템 솔루션 사용자에 대한 키 쌍을 생성합니다.

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

b 각 노드에서 vpxd 솔루션 사용자에 대한 키 쌍을 생성합니다.

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

c 각 노드에서 vpxd-extension 솔루션 사용자에 대한 키 쌍을 생성합니다.

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

d 각 노드에서 vsphere-webclient 솔루션 사용자에 대한 키 쌍을 생성합니다.

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

e 각 노드에서 wcp 솔루션 사용자에 대한 키 쌍을 생성합니다.

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

2 각 vCenter Server 노드의 시스템 솔루션 사용자 및 각 추가 솔루션 사용자(vpxd, vpxd-extension, vsphere-webclient, wcp)에 대해 새 VMCA 루트 인증서로 서명된 솔루션 사용자 인증서를 생성합니다.

참고 `--Name` 매개 변수는 고유해야 합니다. 솔루션 사용자 저장소의 이름을 포함하면 각 인증서가 어느 솔루션 사용자에게 매핑되는지 쉽게 확인할 수 있습니다. 이 예제에서는 각각에 `vpxd` 또는 `vpxd-extension` 같은 이름이 포함됩니다.

a `/usr/lib/vmware-vmca/share/config/certool.cfg` 파일의 복사본 하나를 만든 다음, 필요에 따라 이름, IP 주소, DNS 이름 및 이메일 필드를 수정하거나 제거하고 파일 이름을 바꿉니다(예: `sol_usr.cfg`).

b 각 노드에서 시스템 솔루션 사용자용 인증서를 생성합니다.

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

c 각 노드에서 vpxd 솔루션 사용자용 인증서를 생성합니다.

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

d 각 노드에서 vpxd-extensions 솔루션 사용자용 인증서를 생성합니다.

```
/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 다음 명령을 실행하여 각 노드에서 vsphere-webclient 솔루션 사용자용 인증서를 생성합니다.

```
/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 다음 명령을 실행하여 각 노드에서 wcp 솔루션 사용자의 인증서를 생성합니다.

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

3 VECS의 솔루션 사용자 인증서를 새 솔루션 사용자 인증서로 교체합니다.

참고 `--store` 및 `--alias` 매개 변수는 서비스의 기본 이름과 정확하게 일치해야 합니다.

a 각 노드에서 시스템 솔루션 사용자 인증서를 교체합니다.

```
/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 각 노드에서 vpxd 솔루션 사용자 인증서를 교체합니다.

```
/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 각 노드에서 vpxd-extension 솔루션 사용자 인증서를 교체합니다.

```
/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 각 노드에서 vsphere-webclient 솔루션 사용자 인증서를 교체합니다.

```
/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 각 노드에서 wcp 솔루션 사용자 인증서를 교체합니다.

```
/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 VMware 디렉토리 서비스(vmdir)를 새 솔루션 사용자 인증서로 업데이트합니다. vCenter Single Sign-On 관리자 암호를 묻는 메시지가 나타납니다.

a `/usr/lib/vmware-vmafd/bin/dir-cli service list`를 실행하여 각 솔루션 사용자에 대한 고유한 서비스 ID 접미사를 가져옵니다. 이 명령은 vCenter Server 시스템에서 실행합니다.

```
/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
```

참고 대규모 배포의 솔루션 사용자 인증서를 나열할 경우 `/usr/lib/vmware-vmafd/bin/dir-cli list`의 출력에는 모든 노드의 모든 솔루션 사용자가 포함됩니다. 각 호스트의 로컬 시스템 ID를 찾으려면 `/usr/lib/vmware-vmafd/bin/vmafd-cli get-machine-id --server-name localhost`를 실행하십시오. 각 솔루션 사용자 이름에 시스템 ID가 포함되어 있습니다.

b 각 vCenter Server 노드에서 vmdir의 시스템 인증서를 교체합니다. 예를 들어 machine-6fd7f140-60a9-11e4-9e28-005056895a69가 vCenter Server의 시스템 솔루션 사용자인 경우 이 명령을 실행하십시오.

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

c 각 노드에서 vmdir의 vpxd 솔루션 사용자 인증서를 교체합니다. 예를 들어 vpxd-6fd7f140-60a9-11e4-9e28-005056895a69가 vpxd 솔루션 사용자 ID인 경우 이 명령을 실행하십시오.

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

d 각 노드에서 vmdir의 vpxd-extension 솔루션 사용자 인증서를 교체합니다. 예를 들어 vpxd-extension-6fd7f140-60a9-11e4-9e28-005056895a69가 vpxd-extension 솔루션 사용자 ID인 경우 이 명령을 실행하십시오.

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

e 각 노드에서 vsphere-webclient 솔루션 사용자 인증서를 교체합니다. 예를 들어 vsphere-webclient-6fd7f140-60a9-11e4-9e28-005056895a69가 vsphere-webclient 솔루션 사용자 ID인 경우 이 명령을 실행하십시오.

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

f 각 노드에서 wcp 솔루션 사용자 인증서를 교체합니다. 예를 들어 wcp-1cbe0a40-e4ce-4378-b5e7-9460e2b8200e이 wcp 솔루션 사용자 ID이면 다음 명령을 실행합니다.

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

CLI를 사용하여 인증서를 사용자 지정 인증서로 교체

회사 정책에서 요구하는 경우 CLI를 사용하여 vSphere에 사용되는 일부 또는 모든 인증서를 타사 또는 엔터프라이즈 CA에서 서명한 인증서로 교체할 수 있습니다. 이렇게 하면 VMCA가 인증서 체인에 포함되지 않습니다. 모든 vCenter 인증서를 VECS에 직접 저장해야 합니다.

모든 인증서를 교체하거나 하이브리드 솔루션을 사용할 수 있습니다. 예를 들어 네트워크 트래픽에 사용되는 모든 인증서는 교체하고 VMCA 서명 솔루션 사용자 인증서는 남겨두는 것을 고려하십시오. 솔루션 사용자 인증서는 vCenter Single Sign-On에 대한 인증에만 사용됩니다. vCenter Server는 내부 통신에만 솔루션 사용자 인증서를 사용합니다. 솔루션 사용자 인증서는 외부 통신에 사용되지 않습니다.

참고 VMCA를 사용하지 않으려면 모든 인증서의 교체, 인증서를 사용한 새 구성 요소 프로비저닝 및 인증서 만료 추적을 사용자가 직접 처리해야 합니다.

사용자 지정 인증서를 사용하기로 결정한 경우에도 인증서 교체를 위해 VMware Certificate Manager 유틸리티를 계속 사용할 수 있습니다. Certificate Manager를 사용하여 모든 인증서를 사용자 지정 인증서로 교체의 내용을 참조하십시오.

인증서를 교체한 후 vSphere Auto Deploy 관련 문제가 발생하면 VMware 기술 자료 문서(https://kb.vmware.com/s/article/2000988)를 참조하십시오.

CLI를 사용하여 인증서 요청 및 사용자 지정 루트 인증서 가져오기

엔터프라이즈 또는 타사 CA의 사용자 지정 인증서를 사용할 수 있습니다. 첫 번째 단계는 CA(인증 기관)의 인증서를 요청하고 CLI를 사용하여 루트 인증서를 VECS(VMware Endpoint Certificate Store)로 가져오는 것입니다.

사전 요구 사항

인증서는 다음 요구 사항을 충족해야 합니다.

- 키 크기: 2048비트(최소)~8192비트(최대)(PEM 인코딩)
- PEM 형식. VMware는 PKCS8 및 PKCS1(RSA 키)을 지원합니다. 키가 VECS에 추가되면 추가된 키가 PKCS8로 변환됩니다.
- x509 버전 3
- 루트 인증서의 경우 CA 확장을 true로 설정해야 하며 인증서 서명이 요구 사항 목록에 있어야 합니다.
- SubjectAltName에는 DNS Name=<machine_FQDN>이 포함되어야 합니다.
- CRT 형식
- 다음과 같은 키 사용이 포함되어 있습니다. 디지털 서명, 키 암호화
- 현재 시간 하루 전 시작 시간
- ESXi 호스트가 vCenter Server 인벤토리에 가지고 있는 호스트 이름(또는 IP 주소)으로 설정된 CN (및 SubjectAltName).

참고 vSphere의 FIPS 인증서는 2048비트 및 3072비트의 RSA 키 크기만 검증합니다.

절차

1 다음 인증서에 대한 CSR(인증서 서명 요청)을 엔터프라이즈 또는 타사 인증서 제공자에게 보냅니다.

   - 각 시스템에 대한 시스템 SSL 인증서. 시스템 SSL 인증서의 경우 SubjectAltName 필드에는 정규화된 도메인 이름(DNS NAME=*machine_FQDN*)이 포함되어야 합니다.
   - 필요한 경우 각 노드에 대한 5개의 솔루션 사용자 인증서. 솔루션 사용자 인증서에는 IP 주소, 호스트 이름 또는 이메일 주소가 포함되지 않아도 됩니다. 각 인증서의 인증서 주체가 서로 달라야 합니다.

   일반적으로 신뢰할 수 있는 체인에 대한 PEM 파일과 각 vCenter Server 노드에 대한 서명된 SSL 인증서가 결과로 반환됩니다.

2 TRUSTED_ROOTS 및 시스템 SSL 저장소를 나열합니다.

```
vecs-cli store list
```

a 현재 루트 인증서 및 모든 시스템 SSL 인증서가 VMCA에 의해 서명되었는지 확인합니다.

b 일련 번호, 발급자 및 주체 CN 필드를 기록해 둡니다.

c (선택 사항) 웹 브라우저를 사용하여 인증서를 교체할 노드에 대한 HTTPS 연결을 열고 인증서 정보를 살펴보고 시스템 SSL 인증서와 일치하는지 확인합니다.

3 모든 서비스를 중지하고 인증서 생성, 전파 및 저장을 처리하는 서비스를 시작합니다.

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

4 사용자 지정 루트 인증서를 게시합니다.

```
dir-cli trustedcert publish --cert <my_custom_root>
```

명령줄에서 사용자 이름과 암호를 지정하지 않으면 이를 묻는 메시지가 나타납니다.

5 모든 서비스를 다시 시작합니다.

```
service-control --start --all
```

다음에 수행할 작업

회사 정책에 따라 필요한 경우 원래 VMCA 루트 인증서를 인증서 저장소에서 제거할 수 있습니다. 그렇게 하는 경우 vCenter Single Sign-On 인증서를 새로 고쳐야 합니다. 명령줄을 사용하여 vCenter Server STS 인증서 교체의 내용을 참조하십시오.

CLI를 사용하여 시스템 SSL 인증서를 사용자 지정 인증서로 교체

사용자 지정 인증서를 받은 후에는 CLI를 사용하여 각 시스템 인증서를 교체할 수 있습니다.

인증서 교체를 시작하기 전에 다음 정보를 준비해야 합니다.

- administrator@vsphere.local의 암호
- 유효한 시스템 SSL 사용자 지정 인증서(`.crt` 파일)
- 유효한 시스템 SSL 사용자 지정 키(`.key` 파일)
- 루트에 대한 유효한 사용자 지정 인증서(`.crt` 파일)

사전 요구 사항

타사 또는 엔터프라이즈 CA로부터 각 시스템에 대한 인증서를 받은 상태여야 합니다.

- 키 크기: 2048비트(최소)~8192비트(최대)(PEM 인코딩)

- CRT 형식
- x509 버전 3
- SubjectAltName에는 DNS Name=<machine_FQDN>이 포함되어야 합니다.
- 다음과 같은 키 사용이 포함되어 있습니다. 디지털 서명, 키 암호화

각 vCenter Server 호스트에서 단계를 수행합니다.

절차

1 현재 시스템 SSL 인증서를 백업합니다.

```
/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 각 호스트에 로그인하여 CA(인증 기관)에서 받은 새 시스템 인증서를 VECS에 추가합니다.

모든 호스트는 SSL을 통해 통신하려면 로컬 인증서 저장소에 새 인증서가 필요합니다.

a 기존 인증서를 삭제합니다.

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

b 새 인증서를 추가합니다.

```
/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 교체할 이전 인증서의 해시를 추출합니다.

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

다음과 유사한 출력이 나타납니다.

```
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 등록 끝점을 수동으로 업데이트합니다.

```
/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`를 실행하는 데 문제가 발생하는 경우 https://kb.vmware.com/s/article/95982 에서 VMware 기술 자료 문서를 참조하십시오.

5 모든 서비스를 다시 시작합니다.

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

vSphere 인증서 및 서비스 CLI 명령 참조

3

일련의 CLI를 사용하여 VMCA(VMware Certificate Authority), VECS(VMware Endpoint Certificate Store), VMware Directory Service(vmdir) 및 STS(Security Token Service) 인증서를 관리할 수 있습니다. vSphere Certificate Manager 유틸리티는 다양한 관련 작업도 지원하지만 수동 인증서 관리 및 기타 서비스 관리를 위해서는 CLI가 필요합니다.

일반적으로 SSH를 사용하여 장치 셸에 연결하여 인증서와 연결된 서비스를 관리하기 위해 CLI 도구에 액세스합니다. 자세한 내용은 https://kb.vmware.com/s/article/2100508에서 VMware 기술 자료 문서를 참조하십시오.

vSphere 인증서 수동 교체에는 CLI 명령을 사용하여 인증서를 교체하는 예제가 제공됩니다.

표 3-1. 인증서 및 연결된 서비스 관리를 위한 vSphere CLI 도구

CLI	설명	참조
`certool`	인증서와 키를 생성하고 관리합니다. VMware 인증서 관리 서비스인 VMCAD의 일부입니다.	certool 초기화 명령 참조
`vecs-cli`	VMware Certificate Store 인스턴스의 컨텐츠를 관리합니다. VMAFD(VMware 인증 프레임워크 대몬)의 일부입니다.	vecs-cli 명령 참조
`dir-cli`	VMware Directory Service에서 인증서를 만들고 업데이트합니다. VMAFD의 일부입니다.	dir-cli 명령 참조
`sso-config.sh`	STS 인증서를 관리합니다.	명령줄 도움말. 옵션 없이 `sso-config.sh`를 입력하면 명령줄 도움말이 표시됩니다.
`service-control`	예를 들면 인증서 교체 워크플로의 일부로 서비스를 시작 또는 중지합니다.	다른 CLI 명령을 실행하기 전에 이 명령을 실행하여 서비스를 중지합니다.

vSphere CLI 위치

기본적으로 다음 위치에서 CLI를 찾을 수 있습니다.

```
/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
```

참고 `service-control` 명령에는 경로를 지정하지 않아도 됩니다.

vSphere CLI 실행을 위한 필수 권한

필수 권한은 사용하는 CLI 및 실행하려는 명령에 따라 다릅니다. 예를 들어 대부분의 인증서 관리 작업을 수행하려면 로컬 vCenter Single Sign-On 도메인(기본적으로 vsphere.local)의 관리자여야 합니다. 일부 명령은 모든 사용자가 사용할 수 있습니다.

dir-cli

`dir-cli` 명령을 실행하려면 로컬 도메인(기본적으로 vsphere.local)에서 관리자 그룹의 멤버여야 합니다. 사용자 이름과 암호를 지정하지 않으면 로컬 vCenter Single Sign-On 도메인의 관리자(기본적으로 administrator@vsphere.local) 암호를 입력하라는 메시지가 표시됩니다.

vecs-cli

처음에는 블랭킷 액세스 권한을 가진 사용자와 저장소 소유자만 저장소에 액세스할 수 있습니다. 관리자 그룹의 사용자는 블랭킷 액세스 권한이 있습니다.

MACHINE_SSL_CERT 및 TRUSTED_ROOTS 저장소는 특별 저장소입니다. 설치 유형에 따라 루트 사용자 또는 관리자 사용자만 전체 액세스 권한을 갖습니다.

certool

대부분의 `certool` 명령을 실행하려면 사용자가 관리자 그룹에 속해 있어야 합니다. 다음 명령은 모든 사용자가 실행할 수 있습니다.

- `genselfcacert`
- `initscr`
- `getdc`
- `waitVMDIR`
- `waitVMCA`
- `genkey`
- `viewcert`

certool 구성 옵션 변경

`certool --gencert` 또는 특정한 다른 인증서 초기화 또는 관리 명령을 실행하면 명령이 구성 파일에서 모든 값을 읽습니다. 기존 파일을 편집하거나, `--config=<file name>` 옵션을 사용하여 기본 구성 파일을 재정의하거나, 명령줄에서 값을 재정의할 수 있습니다.

구성 파일(certool.cfg)은 기본적으로 /usr/lib/vmware-vmca/share/config/ 디렉토리에 있습니다.

파일에는 다음의 기본값을 가진 몇 개의 필드가 있습니다.

```
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
```

참고 OU(organizationalUnitName) 필드는 더 이상 필수가 아닙니다.

다음과 같이 수정된 파일을 명령줄에 지정하거나 명령줄에서 개별 값을 재정의하여 값을 변경할 수 있습니다.

- 구성 파일의 복사본을 생성하고 파일을 편집합니다. --config 명령줄 옵션을 사용하여 파일을 지정합니다. 경로 이름 문제가 발생하지 않도록 전체 경로를 지정합니다.
- ```
  /usr/lib/vmware-vmca/bin/certool --gencert --config /tmp/myconfig.cfg
  ```
- 명령줄에서 개별 값을 재정의합니다. 예를 들어 Locality를 재정의하려면 이 명령을 실행합니다.

  ```
  /usr/lib/vmware-vmca/bin/certool --gencert --privkey=private.key --Locality="Mountain View"
  ```

인증서 주체 이름의 CN 필드를 교체하려면 --Name을 지정합니다.

- 솔루션 사용자 인증서의 경우 이름은 규칙에 따라 <sol_user name>@<domain>이지만 환경에 다른 규칙이 사용되는 경우에는 이름을 변경할 수 있습니다.
- 시스템 SSL 인증서의 경우 시스템의 FQDN이 사용됩니다.

  VMCA에서는 DNSName(Hostname 필드)을 하나만 허용하며 다른 별칭 옵션은 허용하지 않습니다. 사용자가 IP 주소를 지정하는 경우 이 주소도 SubAltName에 저장됩니다.

--Hostname 매개 변수를 사용하여 인증서 SubAltName의 DNSName을 지정합니다.

다음으로 아래 항목을 읽으십시오.

- certool 초기화 명령 참조
- certool 관리 명령 참조
- vecs-cli 명령 참조
- dir-cli 명령 참조
  ```

certool 초기화 명령 참조

`certool` 초기화 명령을 사용하면 인증서 서명 요청을 생성하고 VMCA(VMware Certificate Authority)에서 서명한 인증서 및 키를 보고 생성하며 루트 인증서를 가져오고 기타 인증서 관리 작업을 수행할 수 있습니다.

대부분의 경우 `certool` 명령에 구성 파일을 전달합니다. certool 구성 옵션 변경의 내용을 참조하십시오. 몇 가지 사용 예는 CLI를 사용하여 기존 VMCA 서명 인증서를 VMCA 서명 인증서로 교체 항목을 참조하십시오. 명령줄 도움말은 옵션에 대한 세부 정보를 제공합니다.

certool --initcsr

CSR(인증서 서명 요청)을 생성합니다. 이 명령은 PKCS10 파일 및 개인 키를 생성합니다.

옵션	설명
`--gencsr`	CSR 생성에 필요합니다.
`--privkey <key_file>`	개인 키 파일의 이름입니다.
`--pubkey <key_file>`	공용 키 파일의 이름입니다.
`--csrfile <csr_file>`	CA 제공자에게 보낼 CSR 파일의 파일 이름입니다.
`--config <config_file>`	구성 파일의 이름입니다. 샘플 구성 파일은 `/usr/lib/vmware-vmca/share/config/certool.cfg`에 있습니다. 가장 좋은 방법은 기본 구성 파일의 복사본을 만들고 필요한 필드를 바꾸는 것입니다.

예:

```
certool --gencsr --privkey=<filename> --pubkey=<filename> --csrfile=<filename>
```

certool --selfca

자체 서명된 인증서를 생성하고 자체 서명된 루트 CA로 VMCA 서버를 프로비저닝합니다. 이 옵션 사용은 VMCA 서버를 프로비저닝하는 가장 간단한 방법 중 하나입니다. VMCA가 중간 CA가 되도록 대신 타사 루트 인증서를 사용하여 VMCA 서버를 프로비저닝할 수 있습니다. CLI를 사용하여 VMCA를 중간 CA(인증 기관)로 만들기의 내용을 참조하십시오.

이 명령은 표준 시간대 충돌을 방지하기 위해 3일 앞당겨 발급되는 인증서를 생성합니다.

옵션	설명
`--selfca`	자체 서명된 인증서 생성에 필요합니다.
`--predate <number_of_minutes>`	루트 인증서의 [유효한 시작 날짜] 필드를 현재 시간 기준으로 지정된 시간(분) 전으로 설정할 수 있습니다. 이 옵션은 잠재적인 표준 시간대 문제를 해결하는 데 유용할 수 있습니다. 최대값은 3일입니다.

옵션	설명
`--config <config_file>`	구성 파일의 이름입니다. 샘플 구성 파일은 `/usr/lib/vmware-vmca/share/config/certool.cfg`에 있습니다. 가장 좋은 방법은 기본 구성 파일의 복사본을 만들고 필요한 필드를 바꾸는 것입니다.
`--server <server>`	VMCA 서버의 선택적 이름입니다. 기본적으로 이 명령은 localhost를 사용합니다.

예:

```
machine-70-59:/usr/lib/vmware-vmca/bin # ./certool --predate=2280  --selfca --server=
192.0.2.24 --srp-upn=administrator@vsphere.local
```

certool --rootca

루트 인증서를 가져옵니다. 지정된 인증서 및 개인 키를 VMCA에 추가합니다. VMCA는 항상 가장 최신 루트 인증서를 서명에 사용합니다. 그러나 다른 루트 인증서도 사용자가 수동으로 삭제하기 전에는 신뢰할 수 있는 상태로 남아 있습니다. 즉, 인프라를 한 번에 하나씩 업데이트하고 최종적으로 더 이상 사용하지 않는 인증서를 삭제할 수 있습니다.

옵션	설명
`--rootca`	루트 CA 가져오기에 필요합니다.
`--cert <certfile>`	인증서 파일의 이름입니다.
`--privkey <key_file>`	개인 키 파일의 이름입니다. 이 파일은 PEM 인코딩 형식이어야 합니다.
`--server <server>`	VMCA 서버의 선택적 이름입니다. 기본적으로 이 명령은 localhost를 사용합니다.

예:

```
certool --rootca --cert=root.cert --privkey=privatekey.pem
```

certool --getdc

vmdir에서 사용하는 기본 도메인 이름을 반환합니다.

옵션	설명
`--server <server>`	VMCA 서버의 선택적 이름입니다. 기본적으로 이 명령은 localhost를 사용합니다.
`--port <port_num>`	선택적 포트 번호입니다. 기본값은 포트 389로 설정됩니다.

예:

```
certool --getdc
```

certool --waitVMDIR

VMware Directory Service가 실행될 때까지 대기하거나 `--wait`에서 지정된 시간 제한이 경과할 때까지 대기합니다. 이 옵션을 다른 옵션과 함께 사용하여 기본 도메인 이름 반환과 같은 특정 작업을 스케줄링합니다.

옵션	설명
`--wait`	대기할 선택적 시간(분)입니다. 기본값은 3입니다.
`--server <server>`	VMCA 서버의 선택적 이름입니다. 기본적으로 이 명령은 localhost를 사용합니다.
`--port <port_num>`	선택적 포트 번호입니다. 기본값은 포트 389로 설정됩니다.

예:

```
certool --waitVMDIR --wait 5
```

certool --waitVMCA

VMCA 서비스가 실행될 때까지 대기하거나 지정된 시간 제한이 경과할 때까지 대기합니다. 이 옵션을 다른 옵션과 함께 사용하여 인증서 생성과 같은 특정 작업을 스케줄링합니다.

옵션	설명
`--wait`	대기할 선택적 시간(분)입니다. 기본값은 3입니다.
`--server <server>`	VMCA 서버의 선택적 이름입니다. 기본적으로 이 명령은 localhost를 사용합니다.
`--port <port_num>`	선택적 포트 번호입니다. 기본값은 포트 389로 설정됩니다.

예:

```
certool --waitVMCA --selfca
```

certool --publish-roots

루트 인증서를 강제로 업데이트합니다. 이 명령에는 관리 권한이 필요합니다.

옵션	설명
`--server <server>`	VMCA 서버의 선택적 이름입니다. 기본적으로 이 명령은 localhost를 사용합니다.

예:

```
certool --publish-roots
```

certool 관리 명령 참조

certool 관리 명령을 사용하면 인증서를 보고 생성하고 해지하고 인증서에 대한 정보를 볼 수 있습니다.

certool --genkey

개인 및 공용 키 쌍을 생성합니다. 이러한 파일은 VMCA에서 서명한 인증서를 생성하는 데 사용될 수 있습니다.

옵션	설명
--genkey	개인 및 공용 키 생성에 필요합니다.
--privkey <keyfile>	개인 키 파일의 이름입니다.
--pubkey <keyfile>	공용 키 파일의 이름입니다.
--server <server>	VMCA 서버의 선택적 이름입니다. 기본적으로 이 명령은 localhost를 사용합니다.

예:

```
certool --genkey --privkey=<filename> --pubkey=<filename>
```

certool --gencert

VMCA 서버에서 인증서를 생성합니다. 이 명령은 certool.cfg 또는 지정된 구성 파일의 정보를 사용합니다. 인증서를 사용하여 시스템 인증서 또는 솔루션 사용자 인증서를 프로비저닝할 수 있습니다.

옵션	설명
--gencert	인증서 생성에 필요합니다.
--cert <certfile>	인증서 파일의 이름입니다. 이 파일은 PEM 인코딩 형식이어야 합니다.
--privkey <keyfile>	개인 키 파일의 이름입니다. 이 파일은 PEM 인코딩 형식이어야 합니다.
--config <config_file>	구성 파일의 이름입니다. 샘플 구성 파일은 /usr/lib/vmware-vmca/share/config/certool.cfg에 있습니다. 가장 좋은 방법은 기본 구성 파일의 복사본을 만들고 필요한 필드를 바꾸는 것입니다.
--server <server>	VMCA 서버의 선택적 이름입니다. 기본적으로 이 명령은 localhost를 사용합니다.

예:

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

certool --getrootca

사람이 읽을 수 있는 형식으로 현재 루트 CA 인증서를 인쇄합니다. 이 출력은 인증서로 사용할 수 없으며 사람이 읽을 수 있는 형식으로 변경됩니다.

옵션	설명
`--getrootca`	루트 인증서 인쇄에 필요합니다.
`--server <server>`	VMCA 서버의 선택적 이름입니다. 기본적으로 이 명령은 localhost를 사용합니다.

예:

```
certool --getrootca --server=remoteserver
```

certool --viewcert

사람이 읽을 수 있는 형식으로 인증서의 모든 필드를 인쇄합니다.

옵션	설명
`--viewcert`	인증서 보기에 필요합니다.
`--cert <certfile>`	구성 파일의 이름입니다. 샘플 구성 파일은 `/usr/lib/vmware-vmca/share/config/certool.cfg`에 있습니다. 가장 좋은 방법은 기본 구성 파일의 복사본을 만들고 필요한 필드를 바꾸는 것입니다.

예:

```
 certool --viewcert --cert=<filename>
```

certool --enumcert

VMCA 서버가 알고 있는 모든 인증서를 나열합니다. 필수 `filter` 옵션을 사용하면 모든 인증서를 나열하거나 해지되거나, 활성 또는 만료된 인증서만 나열할 수 있습니다.

옵션	설명
`--enumcert`	모든 인증서 나열에 필요합니다.
`--filter [all | active]`	필수 필터입니다. 모두 또는 활성을 지정합니다. 해지됨 및 만료됨 옵션은 현재 지원되지 않습니다.

예:

```
certool --enumcert --filter=active
```

certool --status

인증서가 해지되었는지 여부를 확인하기 위해 지정된 인증서를 VMCA 서버로 전송합니다. 인증서가 해지된 경우 인증서: 해지됨을 인쇄하고, 그렇지 않으면 인증서: 활성을 인쇄합니다.

옵션	설명
`--status`	인증서의 상태를 확인하는 데 필요합니다.
`--cert <certfile>`	구성 파일의 이름입니다. 샘플 구성 파일은 `/usr/lib/vmware-vmca/share/config/certool.cfg`에 있습니다. 가장 좋은 방법은 기본 구성 파일의 복사본을 만들고 필요한 필드를 바꾸는 것입니다.
`--server <server>`	VMCA 서버의 선택적 이름입니다. 기본적으로 이 명령은 localhost를 사용합니다.

예:

```
certool --status --cert=<filename>
```

certool --genselfcacert

구성 파일의 값을 기준으로 자체 서명된 인증서를 생성합니다. 이 명령은 표준 시간대 충돌을 방지하기 위해 3일 앞당겨 발급되는 인증서를 생성합니다.

옵션	설명
`--genselfcacert`	자체 서명된 인증서 생성에 필요합니다.
`--outcert <cert_file>`	인증서 파일의 이름입니다. 이 파일은 PEM 인코딩 형식이어야 합니다.
`--outprivkey <key_file>`	개인 키 파일의 이름입니다. 이 파일은 PEM 인코딩 형식이어야 합니다.
`--config <config_file>`	구성 파일의 이름입니다. 샘플 구성 파일은 `/usr/lib/vmware-vmca/share/config/certool.cfg`에 있습니다. 가장 좋은 방법은 기본 구성 파일의 복사본을 만들고 필요한 필드를 바꾸는 것입니다.

예:

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

vecs-cli 명령 참조

`vecs-cli` 명령 집합을 사용하면 VECS(VMware 인증서 저장소)의 인스턴스를 관리할 수 있습니다. 이러한 명령을 `dir-cli` 및 `certool`과 함께 사용하여 인증서 인프라 및 인증 서비스를 관리할 수 있습니다.

vecs-cli store create

인증서 저장소를 생성합니다.

옵션	설명
`--name <name>`	인증서 저장소의 이름입니다.
`--server <server-name>`	원격 VECS 인스턴스에 연결하는 경우 서버 이름을 지정하는 데 사용됩니다.
`--upn <user-name>`	`--server <server-name>` 에서 지정한 서버 인스턴스에 로그인하는 데 사용되는 사용자 계정 이름입니다. 저장소를 생성하는 경우 현재 사용자의 컨텍스트에서 생성됩니다. 따라서 저장소의 소유자가 현재 사용자 컨텍스트이며 항상 루트 사용자는 아닙니다.

예:

```
vecs-cli store create --name <store>
```

vecs-cli store delete

인증서 저장소를 삭제합니다. MACHINE_SSL_CERT, TRUSTED_ROOTS 및 TRUSTED_ROOT_CRLS 시스템 저장소는 삭제할 수 없습니다. 필수 권한을 가진 사용자는 솔루션 사용자 저장소를 삭제할 수 있습니다.

옵션	설명
`--name <name>`	삭제할 인증서 저장소의 이름입니다.
`--server <server-name>`	원격 VECS 인스턴스에 연결하는 경우 서버 이름을 지정하는 데 사용됩니다.
`--upn <user-name>`	`--server <server-name>` 에서 지정한 서버 인스턴스에 로그인하는 데 사용되는 사용자 계정 이름입니다. 저장소를 생성하는 경우 현재 사용자의 컨텍스트에서 생성됩니다. 따라서 저장소의 소유자가 현재 사용자 컨텍스트이며 항상 루트 사용자는 아닙니다.

예:

```
vecs-cli store delete --name <store>
```

vecs-cli store list

인증서 저장소를 나열합니다.

옵션	설명
`--server <server-name>`	원격 VECS 인스턴스에 연결하는 경우 서버 이름을 지정하는 데 사용됩니다.
`--upn <user-name>`	`--server <server-name>` 에서 지정한 서버 인스턴스에 로그인하는 데 사용되는 사용자 계정 이름입니다. 저장소를 생성하는 경우 현재 사용자의 컨텍스트에서 생성됩니다. 따라서 저장소의 소유자가 현재 사용자 컨텍스트이며 항상 루트 사용자는 아닙니다.

VECS에는 다음과 같은 저장소가 포함됩니다.

표 3-2. VECS의 저장소

저장소	설명
시스템 SSL 저장소(MACHINE_SSL_CERT)	■ 모든 vSphere 노드의 역방향 프록시 서비스에서 사용됩니다. ■ 각 vCenter Server 노드의 VMware Directory Service(vmdir)가 사용합니다. vSphere 6.0 이상에서 모든 서비스는 시스템 SSL 인증서를 사용하는 역방향 프록시를 통해 통신합니다. 역방향 호환성을 위해 5.x 서비스는 여전히 특정 포트를 사용합니다. 그 결과 vpxd와 같은 일부 서비스는 여전히 자체 포트를 열어둡니다.
솔루션 사용자 저장소 ■ `machine` ■ `vpxd` ■ `vpxd-extension` ■ `vsphere-webclient` ■ `wcp`	VECS에는 각 솔루션 사용자에 대한 하나의 저장소가 포함됩니다. 각 솔루션 사용자 인증서의 주체는 고유해야 합니다. 예를 들어 시스템 인증서는 vpxd 인증서와 동일한 주체를 가질 수 없습니다. 솔루션 사용자 인증서는 vCenter Single Sign-On 인증에 사용됩니다. vCenter Single Sign-On은 인증서가 유효한지 확인하지만 다른 인증서 특성은 확인하지 않습니다. 다음 솔루션 사용자 인증서 저장소는 VECS에 포함되어 있습니다. ■ `machine`: License Server 및 로깅 서비스에서 사용됩니다. **참고** 이 시스템 솔루션 사용자 인증서는 시스템 SSL 인증서와 아무 관련이 없습니다. 이 시스템 솔루션 사용자 인증서는 SAML 토큰 교환에 사용되며 시스템 SSL 인증서는 시스템에 대한 보안 SSL 연결에 사용됩니다. ■ `vpxd`: vCenter 서비스 대몬(vpxd) 저장소. vpxd는 이 저장소에 저장된 솔루션 사용자 인증서를 사용하여 vCenter Single Sign-On에 인증합니다. ■ `vpxd-extension`: vCenter 확장 저장소입니다. Auto Deploy 서비스, Inventory Service를 비롯해 다른 솔루션 사용자의 일부가 아닌 기타 서비스가 포함됩니다. ■ `vsphere-webclient`: vSphere Client 저장소입니다. 성능 차트 서비스와 같은 일부 추가 서비스도 포함됩니다. ■ `wcp`: VMware Tanzu™ 저장소가 있는 VMware vSphere®. vSphere 클러스터 서비스에도 사용됩니다. 각 vCenter Server 노드에는 `machine` 인증서가 포함되어 있습니다.
신뢰할 수 있는 루트 저장소(TRUSTED_ROOTS)	모든 신뢰할 수 있는 루트 인증서가 포함됩니다.

표 3-2. VECS의 저장소 (계속)

저장소	설명
vSphere Certificate Manager 유틸리티 백업 저장소 (BACKUP_STORE)	VMCA(VMware Certificate Manager)에서 인증서 복구를 지원하기 위해 사용합니다. 최근 상태만 백업으로 저장되며 한 단계까지만 되돌아갈 수 있습니다.
기타 저장소	솔루션을 통해 기타 저장소가 추가될 수 있습니다. 예를 들어 Virtual Volumes 솔루션은 SMS 저장소를 추가합니다. VMware 설명서 또는 VMware 기술 자료 문서에서 그렇게 하라고 지시하지 않는 이상 이러한 저장소의 인증서를 수정하지 마십시오. **참고** TRUSTED_ROOTS_CRLS 저장소를 삭제하면 인증서 인프라가 손상될 수 있습니다. TRUSTED_ROOTS_CRLS 저장소를 삭제하거나 수정하지 마십시오.

예:

```
vecs-cli store list
```

vecs-cli store permissions

저장소에 사용 권한을 부여하거나 취소합니다. `--grant` 또는 `--revoke` 옵션을 사용합니다.

저장소 소유자는 사용 권한의 부여 및 해지를 포함하여 모든 작업을 수행할 수 있습니다. 기본적으로 로컬 vCenter Single Sign-On 도메인의 관리자인 administrator@vsphere.local은 사용 권한의 부여 및 해지를 포함하여 모든 저장소에 대해 모든 권한을 갖습니다.

`vecs-cli get-permissions --name <store-name>`을 사용하여 저장소에 대한 현재 설정을 검색할 수 있습니다.

옵션	설명
`--name <name>`	인증서 저장소의 이름입니다.
`--user <username>`	사용 권한이 부여된 사용자의 고유한 이름입니다.
`--grant [read|write]`	부여할 사용 권한(읽기 또는 쓰기)입니다.
`--revoke [read|write]`	읽기 또는 쓰기 사용 권한을 취소합니다. 현재는 지원되지 않습니다.

vecs-cli store get-permissions

저장소에 대한 현재 사용 권한 설정을 검색합니다.

옵션	설명
`--name <name>`	인증서 저장소의 이름입니다.
`--server <server-name>`	원격 VECS 인스턴스에 연결하는 경우 서버 이름을 지정하는 데 사용됩니다.
`--upn <user-name>`	`--server <server-name>` 에서 지정한 서버 인스턴스에 로그인하는 데 사용되는 사용자 계정 이름입니다. 저장소를 생성하는 경우 현재 사용자의 컨텍스트에서 생성됩니다. 따라서 저장소의 소유자가 현재 사용자 컨텍스트이며 항상 루트 사용자는 아닙니다.

vecs-cli entry create

VECS에 항목을 생성합니다. 저장소에 개인 키 또는 인증서를 추가하려면 이 명령을 사용합니다.

참고 이 명령을 사용하여 루트 인증서를 TRUSTED_ROOTS 저장소에 추가하지 마십시오. 대신 `dir-cli` 명령을 사용하여 루트 인증서를 게시하십시오.

옵션	설명
`--store <NameOfStore>`	인증서 저장소의 이름입니다.
`--alias <Alias>`	인증서에 대한 선택적 별칭입니다. 이 옵션은 신뢰할 수 있는 루트 저장소에 대해 무시됩니다.
`--cert <certificate_file_path>`	인증서 파일의 전체 경로입니다.
`--key <key-file-path>`	인증서에 해당하는 키의 전체 경로입니다. 선택 사항입니다.
`--password <password>`	개인 키를 암호화하는 선택적 암호입니다.
`--server <server-name>`	원격 VECS 인스턴스에 연결하는 경우 서버 이름을 지정하는 데 사용됩니다.
`--upn <user-name>`	`--server <server-name>` 에서 지정한 서버 인스턴스에 로그인하는 데 사용되는 사용자 계정 이름입니다. 저장소를 생성하는 경우 현재 사용자의 컨텍스트에서 생성됩니다. 따라서 저장소의 소유자가 현재 사용자 컨텍스트이며 항상 루트 사용자는 아닙니다.

vecs-cli entry list

지정된 저장소의 모든 항목을 나열합니다.

옵션	설명
`--store <NameOfStore>`	인증서 저장소의 이름입니다.

vecs-cli entry getcert

VECS에서 인증서를 검색합니다. 출력 파일에 인증서를 보내거나 사람이 읽을 수 있는 텍스트로 표시할 수 있습니다.

옵션	설명
`--store <NameOfStore>`	인증서 저장소의 이름입니다.
`--alias <Alias>`	인증서의 별칭입니다.
`--output <output_file_path>`	인증서를 쓰는 파일입니다.
`--text`	사람이 읽을 수 있는 인증서 버전을 표시합니다.
`--server <server-name>`	원격 VECS 인스턴스에 연결하는 경우 서버 이름을 지정하는 데 사용됩니다.
`--upn <user-name>`	`--server <server-name>` 에서 지정한 서버 인스턴스에 로그인하는 데 사용되는 사용자 계정 이름입니다. 저장소를 생성하는 경우 현재 사용자의 컨텍스트에서 생성됩니다. 따라서 저장소의 소유자가 현재 사용자 컨텍스트이며 항상 루트 사용자는 아닙니다.

vecs-cli entry getkey

VECS에 저장된 키를 검색합니다. 이 키는 출력 파일에 보내거나 사람이 읽을 수 있는 텍스트로 표시할 수 있습니다.

옵션	설명
`--store <NameOfStore>`	인증서 저장소의 이름입니다.
`--alias <Alias>`	키의 별칭입니다.
`--output <output_file_path>`	키를 쓰는 출력 파일입니다.
`--text`	사람이 읽을 수 있는 키 버전을 표시합니다.
`--server <server-name>`	원격 VECS 인스턴스에 연결하는 경우 서버 이름을 지정하는 데 사용됩니다.
`--upn <user-name>`	`--server <server-name>` 에서 지정한 서버 인스턴스에 로그인하는 데 사용되는 사용자 계정 이름입니다. 저장소를 생성하는 경우 현재 사용자의 컨텍스트에서 생성됩니다. 따라서 저장소의 소유자가 현재 사용자 컨텍스트이며 항상 루트 사용자는 아닙니다.

vecs-cli entry delete

인증서 저장소에서 항목을 삭제합니다. VECS에서 항목을 삭제하는 경우 VECS에서 영구적으로 제거합니다. 유일한 예외는 현재 루트 인증서입니다. VECS는 vmdir을 폴링하여 루트 인증서를 검색합니다.

옵션	설명
`--store <NameOfStore>`	인증서 저장소의 이름입니다.
`--alias <Alias>`	삭제하려는 항목의 별칭입니다.
`--server <server-name>`	원격 VECS 인스턴스에 연결하는 경우 서버 이름을 지정하는 데 사용됩니다.
`--upn <user-name>`	`--server <server-name>` 에서 지정한 서버 인스턴스에 로그인하는 데 사용되는 사용자 계정 이름입니다. 저장소를 생성하는 경우 현재 사용자의 컨텍스트에서 생성됩니다. 따라서 저장소의 소유자가 현재 사용자 컨텍스트이며 항상 루트 사용자는 아닙니다.
`-y`	확인 프롬프트를 표시하지 않습니다. 고급 사용자 전용 옵션입니다.

vecs-cli force-refresh

VECS를 강제로 새로 고칩니다. 기본적으로 VECS는 5분 간격으로 vmdir을 폴링하여 새 루트 인증서 파일을 검색합니다. vmdir에서 VECS를 즉시 업데이트하려면 이 명령을 사용합니다.

옵션	설명
`--server <server-name>`	원격 VECS 인스턴스에 연결하는 경우 서버 이름을 지정하는 데 사용됩니다.
`--upn <user-name>`	`--server <server-name>` 에서 지정한 서버 인스턴스에 로그인하는 데 사용되는 사용자 계정 이름입니다. 저장소를 생성하는 경우 현재 사용자의 컨텍스트에서 생성됩니다. 따라서 저장소의 소유자가 현재 사용자 컨텍스트이며 항상 루트 사용자는 아닙니다.

dir-cli 명령 참조

`dir-cli` 유틸리티는 VMware Directory Service(vmdir)에서의 솔루션 사용자 생성과 업데이트, 계정 관리 및 인증서와 암호 관리를 지원합니다. `dir-cli`를 사용하여 vCenter Server 인스턴스의 도메인 기능 수준을 관리하고 쿼리할 수 있습니다.

dir-cli nodes list

vCenter Server 시스템에 연결된 모든 고급 연결 모드를 나열합니다.

옵션	설명
`--login <admin_user_id>`	기본적으로 로컬 vCenter Single Sign-On 도메인인 administrator@vsphere.local의 관리자입니다.
`--password <admin_password>`	관리자의 암호입니다. 암호를 지정하지 않으면 메시지가 표시됩니다.
`--server <psc_ip_or_fqdn>`	다른 vCenter Server에 연결하여 해당 복제 파트너를 보려면 이 옵션을 사용합니다.

dir-cli computer password-reset

도메인 내에서 시스템 계정의 암호를 재설정할 수 있습니다.

옵션	설명
`--login <admin_user_id>`	기본적으로 로컬 vCenter Single Sign-On 도메인인 administrator@vsphere.local의 관리자입니다.
`--password <admin_password>`	관리자의 암호입니다. 암호를 지정하지 않으면 메시지가 표시됩니다.
`--live-dc-hostname <server name>`	vCenter Server 인스턴스의 현재 이름입니다.

dir-cli service create

솔루션 사용자를 생성합니다. 기본적으로 타사 솔루션에 사용됩니다.

옵션	설명
`--name <name>`	생성할 솔루션 사용자의 이름입니다.
`--cert <cert file>`	인증서 파일의 경로입니다. VMCA에서 서명한 인증서나 타사 인증서일 수 있습니다.
`--ssogroups <comma-separated-groupnames>`	솔루션 사용자를 지정된 그룹의 멤버로 만듭니다.
`--wstrustrole <ActAsUser>`	솔루션 사용자를 기본 제공 관리자 또는 사용자 그룹의 멤버로 만듭니다. 즉, 솔루션 사용자에게 관리 권한이 있는지 여부를 결정합니다.
`--ssoadminrole <Administrator/User>`	솔루션 사용자를 ActAsUser 그룹의 멤버로 만듭니다. ActAsUser 역할은 사용자가 다른 사용자를 대신하여 작업할 수 있도록 합니다.
`--login <admin_user_id>`	기본적으로 로컬 vCenter Single Sign-On 도메인인 administrator@vsphere.local의 관리자입니다.
`--password <admin_password>`	관리자의 암호입니다. 암호를 지정하지 않으면 메시지가 표시됩니다.

dir-cli service list

`dir-cli`가 알고 있는 솔루션 사용자를 나열합니다.

옵션	설명
`--login <admin_user_id>`	기본적으로 로컬 vCenter Single Sign-On 도메인인 administrator@vsphere.local의 관리자입니다.
`--password <admin_password>`	관리자의 암호입니다. 암호를 지정하지 않으면 메시지가 표시됩니다.

dir-cli service delete

vmdir에서 솔루션 사용자를 삭제합니다. 솔루션 사용자를 삭제하면 이 vmdir 인스턴스를 사용하는 모든 관리 노드에서 관련 서비스 모두를 사용할 수 없게 됩니다.

옵션	설명
`--name`	삭제할 솔루션 사용자의 이름입니다.
`--login <admin_user_id>`	기본적으로 로컬 vCenter Single Sign-On 도메인인 administrator@vsphere.local의 관리자입니다.
`--password <admin_password>`	관리자의 암호입니다. 암호를 지정하지 않으면 메시지가 표시됩니다.

dir-cli service update

지정된 솔루션 사용자에 대한 인증서, 즉 서비스 모음을 업데이트합니다. 이 명령을 실행한 후 `vecs-cli entry create` 명령을 실행하여 VECS에서 솔루션 사용자 인증서 항목을 업데이트합니다. vecs-cli 명령 참조의 내용을 참조하십시오.

옵션	설명
`--name <name>`	업데이트할 솔루션 사용자의 이름입니다.
`--cert <cert_file>`	서비스에 할당할 인증서의 이름입니다.
`--login <admin_user_id>`	기본적으로 로컬 vCenter Single Sign-On 도메인인 administrator@vsphere.local의 관리자입니다.
`--password <admin_password>`	관리자의 암호입니다. 암호를 지정하지 않으면 메시지가 표시됩니다.

dir-cli user create

vmdir 내부에 일반 사용자를 생성합니다. 이 명령은 사용자 이름 및 암호를 사용하여 vCenter Single Sign-On에 인증하는 인간 사용자에 대해 사용할 수 있습니다. 프로토타이핑 동안에만 이 명령을 사용합니다.

옵션	설명
`--account <name>`	생성할 vCenter Single Sign-On 사용자의 이름입니다.
`--user-password <password>`	사용자의 초기 암호입니다.
`--first-name <name>`	사용자의 이름입니다.
`--last-name <name>`	사용자의 성입니다.
`--login <admin_user_id>`	기본적으로 로컬 vCenter Single Sign-On 도메인인 administrator@vsphere.local의 관리자입니다.
`--password <admin_password>`	관리자의 암호입니다. 암호를 지정하지 않으면 메시지가 표시됩니다.

dir-cli user modify

vmdir 내에서 지정된 사용자를 수정합니다.

옵션	설명
`--account <name>`	수정할 vCenter Single Sign-On 사용자의 이름입니다.
`--password-never-expires`	vCenter Server에 인증해야 하는 자동화 작업을 위해 사용자 계정을 수정하고 암호 만료 때문에 작업이 중지되지 않게 하려면 이 옵션을 true로 설정합니다. 이 옵션은 주의해서 사용해야 합니다.
`--password-expires`	`--password-never-expires` 옵션을 되돌리려면 이 옵션을 true로 설정합니다.
`--login <admin_user_id>`	기본적으로 로컬 vCenter Single Sign-On 도메인인 administrator@vsphere.local의 관리자입니다.
`--password <admin_password>`	관리자의 암호입니다. 암호를 지정하지 않으면 메시지가 표시됩니다.

dir-cli user delete

vmdir 내부의 지정된 사용자를 삭제합니다.

옵션	설명
`--account <name>`	삭제할 vCenter Single Sign-On 사용자의 이름입니다.
`--login <admin_user_id>`	기본적으로 로컬 vCenter Single Sign-On 도메인인 administrator@vsphere.local의 관리자입니다.
`--password <admin_password>`	관리자의 암호입니다. 암호를 지정하지 않으면 메시지가 표시됩니다.

dir-cli user find-by-name

vmdir에서 이름으로 사용자를 찾습니다. 이 명령이 반환하는 정보는 `--level` 옵션에 지정하는 내용에 따라 다릅니다.

옵션	설명
`--account <name>`	찾을 vCenter Single Sign-On 사용자의 이름입니다.
`--level <info level 0|1|2>`	다음 정보를 반환합니다. ■ 수준 0 - 계정 및 UPN ■ 수준 1 - 수준 0 정보 + 이름 및 성 ■ 수준 2 - 수준 0 + 계정 비활성화됨 플래그, 계정 잠금 플래그, 암호 만료 없음 플래그, 암호 만료됨 플래그 및 암호 만료 플래그. 기본 수준은 0입니다.
`--login <admin_user_id>`	기본적으로 로컬 vCenter Single Sign-On 도메인인 administrator@vsphere.local의 관리자입니다.
`--password <admin_password>`	관리자의 암호입니다. 암호를 지정하지 않으면 메시지가 표시됩니다.

dir-cli group modify

사용자 또는 그룹을 기존 그룹에 추가합니다.

옵션	설명
`--name <name>`	vmdir의 그룹 이름입니다.
`--add <user_or_group_name>`	추가할 사용자 또는 그룹의 이름입니다.
`--login <admin_user_id>`	기본적으로 로컬 vCenter Single Sign-On 도메인인 administrator@vsphere.local의 관리자입니다.
`--password <admin_password>`	관리자의 암호입니다. 암호를 지정하지 않으면 메시지가 표시됩니다.

dir-cli group list

지정된 vmdir 그룹을 나열합니다.

옵션	설명
`--name <name>`	vmdir의 그룹의 선택적 이름입니다. 이 옵션을 사용하면 특정 그룹이 있는지 여부를 확인할 수 있습니다.
`--login <admin_user_id>`	기본적으로 로컬 vCenter Single Sign-On 도메인인 administrator@vsphere.local의 관리자입니다.
`--password <admin_password>`	관리자의 암호입니다. 암호를 지정하지 않으면 메시지가 표시됩니다.

dir-cli ssogroup create

로컬 도메인(기본적으로 vsphere.local) 내에 그룹을 생성합니다.

이 명령은 vCenter Single Sign-On 도메인의 사용자 사용 권한을 관리하기 위해 그룹을 생성하려는 경우에 사용합니다. 예를 들어 그룹을 생성한 후에 vCenter Single Sign-On 도메인의 관리자 그룹에 추가하면 해당 그룹에 추가하는 모든 사용자가 도메인에 대해 관리자 사용 권한을 갖습니다.

vCenter 인벤토리 개체에 대한 사용 권한을 vCenter Single Sign-On 도메인 내의 그룹에 부여할 수도 있습니다. "vSphere 보안" 설명서를 참조하십시오.

옵션	설명
`--name <name>`	vmdir의 그룹 이름입니다. 최대 길이는 487자입니다.
`--description <description>`	그룹에 대한 설명입니다(선택 사항).
`--login <admin_user_id>`	기본적으로 로컬 vCenter Single Sign-On 도메인인 administrator@vsphere.local의 관리자입니다.
`--password <admin_password>`	관리자의 암호입니다. 암호를 지정하지 않으면 메시지가 표시됩니다.

dir-cli trustedcert publish

신뢰할 수 있는 루트 인증서를 vmdir에 게시합니다. 이 명령을 실행하면 VECS가 1분 후에 인증서 변경을 적용합니다. 또는 `vecs-cli force-refresh` 명령을 실행하여 인증서를 즉시 동기화할 수 있습니다.

참고 vSphere 8.0 업데이트 3부터 vSphere Client 또는 API를 사용하여 신뢰할 수 있는 루트 인증서를 게시하고 서비스를 다시 시작하지 않아도 됩니다.

옵션	설명
`--cert <file>`	인증서 파일의 경로입니다.
`--crl <file>`	VMCA에서는 이 옵션이 지원되지 않습니다.
`--login <admin_user_id>`	기본적으로 로컬 vCenter Single Sign-On 도메인인 administrator@vsphere.local의 관리자입니다.
`--password <admin_password>`	관리자의 암호입니다. 암호를 지정하지 않으면 메시지가 표시됩니다.
`--chain`	이 옵션은 체인 인증서를 게시하는 경우에 지정합니다. 옵션 값이 필요하지 않습니다.

dir-cli trustedcert unpublish

현재 vmdir에 있는 신뢰할 수 있는 루트 인증서의 게시를 취소합니다. 예를 들어 현재 환경에 있는 다른 모든 인증서에 대한 루트 인증서인 vmdir에 다른 루트 인증서를 추가한 경우 이 명령을 사용합니다. 더 이상 사용되지 않는 인증서의 게시를 취소하는 것은 환경 강화의 일환입니다.

참고 vSphere 8.0 업데이트 3부터 vSphere Client 또는 API를 사용하여 신뢰할 수 있는 루트 인증서를 게시 취소하고 서비스를 다시 시작하지 않아도 됩니다.

옵션	설명
`--cert-file <file>`	게시를 취소할 인증서 파일의 경로입니다.
`--login <admin_user_id>`	기본적으로 로컬 vCenter Single Sign-On 도메인인 administrator@vsphere.local의 관리자입니다.
`--password <admin_password>`	관리자의 암호입니다. 암호를 지정하지 않으면 메시지가 표시됩니다.

dir-cli trustedcert list

모든 신뢰할 수 있는 루트 인증서와 해당 ID를 나열합니다. `dir-cli trustedcert get`을 사용하여 인증서를 검색하려면 인증서 ID가 필요합니다.

옵션	설명
`--login <admin_user_id>`	기본적으로 로컬 vCenter Single Sign-On 도메인인 administrator@vsphere.local의 관리자입니다.
`--password <admin_password>`	관리자의 암호입니다. 암호를 지정하지 않으면 메시지가 표시됩니다.

dir-cli trustedcert get

vmdir에서 신뢰할 수 있는 루트 인증서를 검색하고 지정된 파일에 씁니다.

옵션	설명
`--id <cert_ID>`	검색할 인증서의 ID입니다. `dir-cli trustedcert list` 명령은 ID를 표시합니다.
`--outcert <path>`	인증서 파일을 쓸 경로입니다.
`--outcrl <path>`	CRL 파일을 쓸 경로입니다. 현재 사용되지 않습니다.
`--login <admin_user_id>`	기본적으로 로컬 vCenter Single Sign-On 도메인인 administrator@vsphere.local의 관리자입니다.
`--password <admin_password>`	관리자의 암호입니다. 암호를 지정하지 않으면 메시지가 표시됩니다.

dir-cli password create

암호 요구 사항을 충족하는 임의 암호를 생성합니다. 이 명령은 타사 솔루션 사용자가 사용할 수 있습니다.

옵션	설명
`--login <admin_user_id>`	기본적으로 로컬 vCenter Single Sign-On 도메인인 administrator@vsphere.local의 관리자입니다.
`--password <admin_password>`	관리자의 암호입니다. 암호를 지정하지 않으면 메시지가 표시됩니다.

dir-cli password reset

관리자가 사용자의 암호를 재설정하도록 허용합니다. 암호를 재설정하려는 비관리자인 경우 대신 `dir-cli password change`를 사용합니다.

옵션	설명
`--account`	새 암호를 할당할 계정의 이름입니다.
`--new`	지정된 사용자의 새 암호입니다.

옵션	설명
`--login <admin_user_id>`	기본적으로 로컬 vCenter Single Sign-On 도메인인 administrator@vsphere.local의 관리자입니다.
`--password <admin_password>`	관리자의 암호입니다. 암호를 지정하지 않으면 메시지가 표시됩니다.

dir-cli password change

사용자가 암호를 변경하도록 허용합니다. 이 변경을 수행하려면 계정을 소유하는 사용자여야 합니다. 관리자는 `dir-cli password reset`을 사용하여 암호를 재설정할 수 있습니다.

옵션	설명
`--account`	계정 이름입니다.
`--current`	계정을 소유하는 사용자의 현재 암호입니다.
`--new`	계정을 소유하는 사용자의 새 암호입니다.

vCenter Single Sign-On으로 vSphere 인증

4

vCenter Single Sign-On은 인증 브로커이자 보안 토큰 교환 인프라입니다. vCenter Single Sign-On은 사용자가 인증할 때 토큰을 발급합니다. 사용자는 토큰을 사용하여 vCenter Server 서비스에 인증할 수 있습니다. 그런 다음 사용자는 사용자가 권한을 가진 작업을 수행할 수 있습니다.

트래픽이 모든 통신에 대해 암호화되고 인증된 사용자만 권한을 가진 작업을 수행할 수 있기 때문에 환경이 보호됩니다.

사용자와 서비스 계정은 토큰 또는 사용자 이름과 암호를 사용하여 인증합니다. 솔루션 사용자는 인증서를 사용하여 인증합니다. 솔루션 사용자 인증서 교체에 대한 자세한 내용은 장 2 vSphere 보안 인증서의 내용을 참조하십시오.

다음 단계에서는 특정 작업을 수행하도록 인증할 수 있는 사용자에게 권한을 부여합니다. 일반적으로 역할을 가진 그룹에 사용자를 할당하는 방법으로 vCenter Server 권한을 할당합니다. vSphere에는 글로벌 사용 권한 같은 다른 사용 권한 모델이 포함되어 있습니다. "vSphere 보안" 설명서를 참조하십시오.

다음으로 아래 항목을 읽으십시오.

- vCenter Single Sign-On으로 환경을 보호하는 방법
- vCenter Server ID 제공자 페더레이션
- vCenter Server ID 제공자 페더레이션 및 고급 연결 모드
- vCenter Server ID 제공자 페더레이션 구성
- vCenter Single Sign-On
- vCenter Single Sign-On ID 소스 구성
- vCenter Server Security Token Service 관리
- vCenter Single Sign-On 정책 관리
- vCenter Single Sign-On 사용자 및 그룹 관리
- 기타 vSphere 인증 옵션
- vSphere Client 로그인 페이지에 대한 로그인 메시지 관리
- vCenter Single Sign-On 보안 모범 사례

vCenter Single Sign-On으로 환경을 보호하는 방법

vCenter Single Sign-On을 사용하면 안전한 토큰 메커니즘을 통해 vSphere 구성 요소가 서로 통신할 수 있습니다.

vCenter Single Sign-On은 다음과 같은 서비스를 사용합니다.

- 외부 ID 제공자 페더레이션 또는 vCenter Server 기본 제공 ID 제공자를 통해 사용자를 인증합니다. 기본 제공 ID 제공자는 로컬 계정, Active Directory 또는 OpenLDAP, IWA(Windows 통합 인증) 및 기타 인증 메커니즘(스마트 카드 및 RSA SecurID)을 지원합니다.
- 인증서를 통해 솔루션 사용자를 인증합니다.
- STS(Security Token Service).
- 보안 트래픽용 SSL입니다.

vCenter Server 기본 제공 ID 제공자

vCenter Server에는 기본 제공 ID 제공자가 포함되어 있습니다. 기본적으로 vCenter Server는 vsphere.local 도메인을 ID 소스로 사용합니다(설치 중에 도메인 변경 가능함). LDAP/S, OpenLDAP/S 또는 IWA(Windows 통합 인증)를 사용하여 AD(Active Directory)를 ID 소스로 사용하도록 vCenter Server 기본 제공 ID 제공자를 구성할 수 있습니다. 그러한 구성을 사용하면 고객이 해당 AD 계정을 통해 vCenter Server에 로그인할 수 있습니다.

vCenter Server및 외부 ID 제공자

vSphere 7.0 이상에서는 페더레이션 인증을 사용하여 외부 ID 제공자에 대해 vCenter Server를 구성할 수 있습니다. 그러한 구성에서 vCenter Server를 ID 제공자로 바꿉니다.

vSphere는 다음 ID 제공자를 지원합니다.

- vSphere 7.0 이상: AD FS(Active Directory Federation Services)
- vSphere 8.0 업데이트 1 이상: Okta
- vSphere 8.0 업데이트 2 이상: Microsoft Entra ID(이전 이름: Azure AD)
- vSphere 8.0 업데이트 3부터: PingFederate

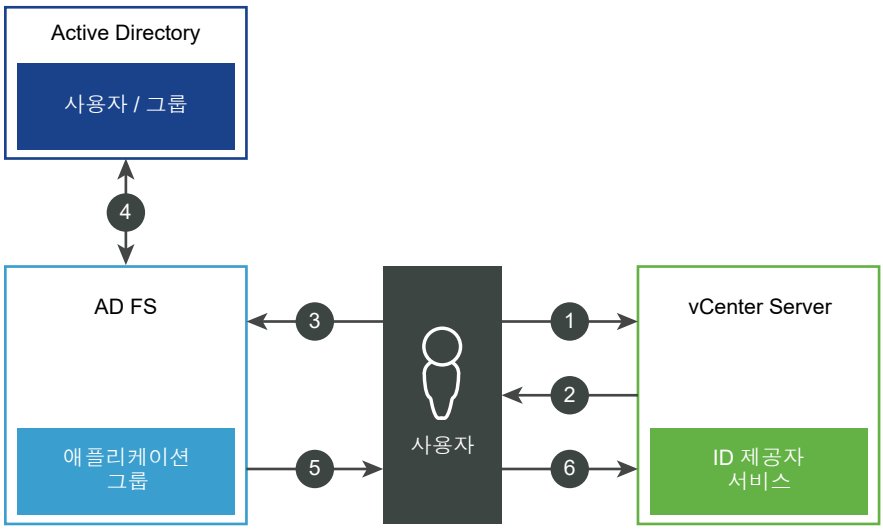
외부 ID 제공자를 사용하도록 vSphere를 구성하면 외부 ID 제공자가 vCenter Server 대신 ID 소스와 상호 작용합니다.

vCenter Server ID 제공자 페더레이션된 인증을 사용한 사용자 로그인

외부 ID 제공자를 사용하여 vCenter Server에 인증하는 경우 vCenter Server는 로그인 요청을 외부 ID 제공자로 리디렉션합니다. 외부 ID 제공자는 해당 디렉토리 서비스로 사용자를 인증한 다음 사용자 로그인에 사용할 vCenter Server용 토큰을 발급합니다.

예를 들어 다음 그림은 AD FS를 사용하는 vCenter Server ID 제공자 페더레이션에 대한 사용자 로그인 흐름을 자세히 보여줍니다.

그림 4-1. AD FS ID 제공자 페더레이션을 사용한 vCenter Server 사용자 로그인



vCenter Server, AD FS 및 Active Directory는 다음과 같이 상호 작용합니다.

1 사용자가 사용자 이름을 입력하여 vCenter Server 랜딩 페이지에서 시작합니다.

2 사용자 이름이 페더레이션된 도메인의 이름이면 vCenter Server는 인증 요청을 AD FS로 리디렉션합니다.

3 필요한 경우 AD FS는 사용자에게 Active Directory 자격 증명으로 로그인하라는 메시지를 표시합니다.

4 AD FS가 사용자를 Active Directory에 인증합니다.

5 AD FS가 Active Directory의 그룹 정보와 함께 보안 토큰을 발급합니다.

6 vCenter Server에서 토큰을 사용하여 사용자에 로그인합니다.

이제 사용자가 인증되었으며 사용자의 역할에 권한이 있는 모든 개체를 살펴보고 수정할 수 있습니다.

참고 처음에는 각 사용자에게 권한 없음 역할이 할당됩니다. 사용자가 로그인하려면 vCenter Server 관리자가 해당 사용자에게 최소한 읽기 전용 역할을 할당해야 합니다. "vSphere 보안" 설명서를 참조하십시오.

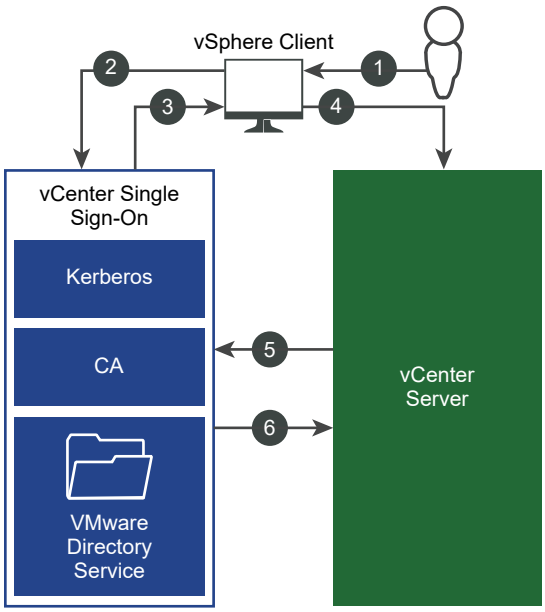
외부 ID 제공자에 연결할 수 없는 경우에는 로그인 프로세스가 vCenter Server 랜딩 페이지로 돌아가고 적절한 정보 메시지가 표시됩니다. 사용자는 vsphere.local ID 소스에서 로컬 계정을 사용하여 계속 로그인할 수 있습니다.

vCenter Server와 Okta, Microsoft Entra ID 또는 PingFederate 간의 상호 작용은 vCenter Server가 VMware Identity Services를 사용한다는 점을 제외하면 AD FS와의 상호 작용과 유사합니다. VMware Identity Services 인증 프로세스의 내용을 참조하십시오.

vCenter Server 기본 제공 ID 제공자를 사용한 사용자 로그인

다음 그림은 vCenter Server가 ID 제공자로 작동하는 경우의 사용자 로그인 흐름을 보여 줍니다.

그림 4-2. vCenter Server 기본 제공 ID 제공자를 사용한 사용자 로그인



1 사용자가 vCenter Server 시스템이나 다른 vCenter 서비스에 액세스하기 위해 사용자 이름과 암호로 vSphere Client에 로그인합니다.

2 vSphere Client는 로그인 정보를 vCenter Single Sign-On 서비스로 전달하고, 이 서비스는 vSphere Client의 SAML 토큰을 확인합니다. vSphere Client의 토큰이 유효한 경우 vCenter Single Sign-On은 사용자가 구성된 ID 소스(예: Active Directory)에 속해 있는지 확인합니다.

   - 사용자 이름만 사용하는 경우 vCenter Single Sign-On은 기본 도메인에서 확인합니다.
   - 도메인 이름이 사용자 이름과 함께 포함되어 있는 경우(*DOMAIN*\user1 또는 user1@*DOMAIN*), vCenter Single Sign-On은 해당 도메인을 확인합니다.

3 사용자가 ID 소스에 인증할 수 있는 경우 vCenter Single Sign-On은 사용자를 나타내는 토큰을 vSphere Client에 반환합니다.

4 vSphere Client는 토큰을 vCenter Server 시스템으로 전달합니다.

5 vCenter Server는 vCenter Single Sign-On Server에 토큰이 유효하며 만료되지 않았는지 확인합니다.

6 vCenter Single Sign-On 서버는 사용자 액세스를 허용하기 위한 vCenter Server 인증 프레임워크를 사용하여 토큰을 vCenter Server 시스템에 반환합니다.

이제 사용자가 인증되었으며 사용자의 역할에 권한이 있는 모든 개체를 살펴보고 수정할 수 있습니다.

참고 처음에는 각 사용자에게 권한 없음 역할이 할당됩니다. 사용자가 로그인하려면 vCenter Server 관리자가 해당 사용자에게 최소한 읽기 전용 역할을 할당해야 합니다. "vSphere 보안" 설명서를 참조하십시오.

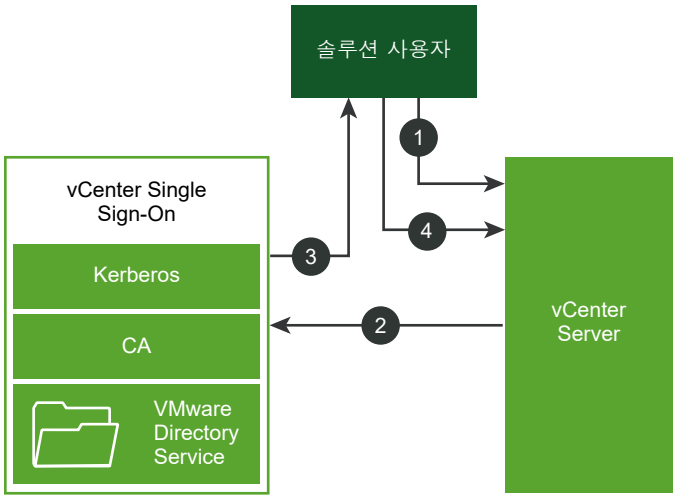
솔루션 사용자를 위한 로그인

솔루션 사용자는 vCenter Server 인프라에서 사용되는 서비스 집합(예: vCenter Server 확장)입니다. VMware 확장 및 잠재적 타사 확장도 vCenter Single Sign-On에 인증될 수 있습니다.

참고 vCenter Server는 내부 통신용으로만 솔루션 사용자 인증서를 사용합니다. 솔루션 사용자 인증서는 외부 통신에 사용되지 않습니다.

다음 그림은 솔루션 사용자에 대한 로그인 흐름을 보여 줍니다.

그림 4-3. 솔루션 사용자를 위한 로그인



1 솔루션 사용자가 vCenter Server 서비스에 연결하려고 합니다.

2 솔루션 사용자가 vCenter Single Sign-On으로 리디렉션됩니다. 솔루션 사용자가 vCenter Single Sign-On을 처음 사용하는 경우 유효한 인증서를 제공해야 합니다.

3 인증서가 유효한 경우 vCenter Single Sign-On이 SAML 토큰(보유자 토큰)을 솔루션 사용자에게 할당합니다. 토큰은 vCenter Single Sign-On에 의해 서명됩니다.

4 그런 다음 솔루션 사용자가 vCenter Single Sign-On으로 리디렉션되고 해당 사용 권한을 기반으로 작업을 수행할 수 있습니다.

   다음에 솔루션 사용자가 인증해야 할 때 SAML 토큰을 사용하여 vCenter Server에 로그인할 수 있습니다.

기본적으로 이 핸드셰이크는 자동입니다. 왜냐하면 VMCA가 시작 중 인증서를 사용하여 솔루션 사용자를 프로비저닝하기 때문입니다. 회사 정책에 따라 타사 CA 서명된 인증서가 필요한 경우 솔루션 사용자 인증서를 타사 CA 서명된 인증서로 교체할 수 있습니다. 이러한 인증서가 유효한 경우 vCenter Single Sign-On이 SAML 토큰을 솔루션 사용자에게 할당합니다. Certificate Manager를 사용하여 솔루션 사용자 인증서를 사용자 지정 인증서로 교체의 내용을 참조하십시오.

vSphere에서 지원되는 암호화

최고 수준의 암호화인 AES 암호화가 지원됩니다. 지원되는 암호화는 vCenter Single Sign-On이 Active Directory를 ID 소스로 사용하는 경우 보안에 영향을 줍니다.

또한 ESXi 호스트 또는 vCenter Server가 Active Directory에 가입될 때마다 보안에 영향을 줍니다.

vCenter Server ID 제공자 페더레이션

vSphere 7.0 이상에서는 vCenter Server가 vCenter Server에 로그인하기 위한 페더레이션된 인증을 지원합니다.

vCenter Server에 대한 페더레이션된 인증을 사용하도록 설정하려면 외부 ID 제공자에 대한 연결을 구성합니다. 구성하는 ID 제공자 인스턴스가 vCenter Server를 ID 제공자로 바꿉니다. 현재 vCenter Server는 외부 ID 제공자로 AD FS(Active Directory 페더레이션 서비스), Okta, Microsoft Entra ID(이전 명칭: Azure AD) 및 PingFederate를 지원합니다. vCenter Server는 vSphere 7.0 이상에서 AD FS를, vSphere 8.0 업데이트 1 이상에서 Okta를, vSphere 8.0 업데이트 2 이상에서 Microsoft Entra ID를, vSphere 8.0 업데이트 3부터 PingFederate를 지원합니다.

참고 vSphere에서 토큰 기반 인증으로 전환하고 있으므로 페더레이션된 인증을 사용하는 것이 좋습니다. vCenter Server는 관리 액세스 및 오류 복구를 위해 계속 로컬 계정을 보유합니다.

vCenter Server ID 제공자 페더레이션의 작동 방식

vCenter Server ID 제공자 페더레이션을 사용하면 페더레이션된 인증에 대해 외부 ID 제공자를 구성할 수 있습니다. 이 구성에서 외부 ID 제공자는 vCenter Server를 대신하여 ID 소스와 상호 작용합니다.

vCenter Server ID 제공자 페더레이션 기본 사항

vSphere 7.0 이상에서 vCenter Server는 페더레이션된 인증을 지원합니다. 이 시나리오에서 사용자가 vCenter Server에 로그인하면 vCenter Server가 사용자 로그인을 외부 ID 제공자로 리디렉션합니다. 사용자 자격 증명은 더 이상 vCenter Server에 직접 제공되지 않습니다. 대신 사용자가 외부 ID 제공자에 자격 증명을 제공합니다. vCenter Server는 외부 ID 제공자를 신뢰하여 인증을 수행합니다. 페더레이션 모델에서 사용자는 ID 제공자 외에 어떤 서비스 또는 애플리케이션에도 자격 증명을 직접 제공하지 않습니다. 따라서 애플리케이션 및 서비스(예: vCenter Server)를 ID 제공자와 "페더레이션"합니다.

vCenter Server 외부 ID 제공자 지원

vCenter Server는 다음과 같은 외부 ID 제공자를 지원합니다.

- AD FS(vSphere 7.0 이상)
- Okta(vSphere 8.0 업데이트 1 이상)
- Microsoft Entra ID(이전 이름: Azure AD)(vSphere 8.0 업데이트 2 이상)
- PingFederate(vSphere 8.0 업데이트 3부터)

vCenter Server ID 제공자 페더레이션 이점

vCenter Server ID 제공자 페더레이션은 다음과 같은 이점을 제공합니다.

- 기존의 페더레이션된 인프라 및 애플리케이션에서 Single Sign-On을 사용할 수 있습니다.
- vCenter Server에서 사용자의 자격 증명을 처리하지 않으므로 데이터 센터 보안을 향상시킬 수 있습니다.
- 외부 ID 제공자가 지원하는 인증 메커니즘(예: 다단계 인증)을 사용할 수 있습니다.

vCenter Server ID 제공자 페더레이션 아키텍처

vCenter Server와 외부 ID 제공자 간 당사자 신뢰를 설정하려면 서로 간에 식별 정보 및 공유 암호를 설정해야 합니다. vCenter Server는 OIDC(OpenID Connect) 프로토콜을 사용하여 vCenter Server로 사용자를 인증하는 ID 토큰을 수신합니다.

vCenter Server를 사용하여 외부 ID 제공자를 구성하는 개략적인 단계는 다음과 같습니다.

1 OIDC 구성을 생성하여 vCenter Server와 외부 ID 제공자 간에 신뢰 당사자 트러스트를 설정합니다. AD FS의 경우 애플리케이션 그룹 또는 애플리케이션을 생성합니다. Okta, Microsoft Entra ID 및 PingFederate의 경우 OpenID Connect를 로그온 방법으로 사용하여 네이티브 애플리케이션을 생성합니다. OIDC 구성은 서버 애플리케이션과 웹 API로 구성됩니다. 이 두 구성 요소는 외부 ID 제공자를 신뢰하고 통신하기 위해 vCenter Server에서 사용하는 정보를 지정합니다.

2 vCenter Server에서 해당 ID 제공자를 생성합니다.

3 외부 ID 제공자 도메인 사용자의 로그인을 인증하도록 vCenter Server에서 그룹 멤버 자격을 구성합니다.

ID 제공자 관리자는 vCenter Server ID 제공자 구성을 생성하기 위해 다음 정보를 제공해야 합니다.

- 클라이언트 식별자: 애플리케이션 그룹(또는 애플리케이션)을 생성할 때 AD FS에서 생성되고 애플리케이션 그룹(또는 애플리케이션)을 식별하거나 OpenID Connect 애플리케이션을 생성할 때 Okta, Microsoft Entra ID 또는 PingFederate에서 생성되는 UUID 문자열입니다.
- 공유 암호: 애플리케이션 그룹(또는 애플리케이션)을 생성할 때 AD FS에서 생성되거나 OpenID Connect 애플리케이션을 생성할 때 Okta, Microsoft Entra ID 또는 PingFederate에서 생성되고 외부 ID 제공자로 vCenter Server를 인증하는 데 사용되는 암호입니다.
- OpenID 주소: 외부 ID 제공자 서버의 OpenID 제공자 검색 끝점 URL이며, 잘 알려진 주소를 지정합니다(일반적으로 발급자 끝점에 "`/.well-known/openid-configuration`" 경로 연결). 다음은 AD FS 구성에 대한 OpenID 주소 예시입니다.

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

  마찬가지로 Okta 구성에 대한 OpenID 주소 예시는 다음과 같습니다.

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

  다음은 Microsoft Entra ID 구성에 대한 OpenID 주소 예시입니다.

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

다음은 PingFederate 구성에 대한 OpenID 주소 예시입니다.

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

VMware Identity Services 및 페더레이션된 인증

vSphere 8.0 업데이트 1 이상에서 VMware Identity Services는 페더레이션된 ID 제공자로서 외부 ID 제공자와의 통합을 제공합니다. VMware Identity Services는 vSphere에 기본 제공되는 VMware Workspace ONE의 "축소된" 버전으로 생각할 수 있습니다.

vSphere 8.0 업데이트 1 이상을 설치하거나 이 버전으로 업그레이드하는 경우 vCenter Server에서 VMware Identity Services가 기본적으로 활성화됩니다. Okta, Microsoft Entra ID 또는 PingFederate를 외부 ID 제공자로 구성하면 vCenter Server는 VMware Identity Services를 사용하여 Okta, Microsoft Entra ID 또는 PingFederate 서버와 통신합니다.

vCenter Server는 고급 연결 모드 구성에서 Okta, Microsoft Entra ID 및 PingFederate를 외부 ID 제공자로 지원합니다. 고급 연결 모드 구성에서는 여러 vCenter Server 시스템이 VMware Identity Services를 실행하더라도 단일 vCenter Server 및 해당 VMware Identity Services만 외부 ID 제공자 서버와 통신합니다. 예를 들어, 3개의 vCenter Server 시스템(A, B, C)의 고급 연결 모드 구성이 있고 vCenter Server A에서 Okta 외부 ID 제공자를 구성하는 경우 모든 Okta 로그인을 처리하는 유일한 시스템은 vCenter Server A입니다. vCenter Server B 및 vCenter Server C는 Okta 서버와 직접 통신하지 않습니다. 외부 IDP 서버와 상호 작용하도록 ELM 구성의 다른 vCenter Server에서 VMware Identity Services를 구성하려면 고급 연결 모드 구성의 외부 ID 제공자에 대한 활성화 프로세스 항목을 참조하십시오.

참고 Okta를 외부 ID 제공자로 구성할 때 고급 연결 모드 구성의 모든 vCenter Server 시스템은 vSphere 8.0 업데이트 1 이상을 실행해야 합니다. Microsoft Entra ID의 경우 요구 사항은 vSphere 8.0 업데이트 2 이상입니다. PingFederate의 경우 요구 사항은 vSphere 8.0 업데이트 3 이상입니다.

경고 Okta, Microsoft Entra ID 또는 PingFederate에서 고급 연결 모드 구성을 사용하는 경우 VMware Identity Services를 실행하고 ID 제공자와 통신하는 vCenter Server를 ELM 구성에서 제거할 수 없습니다.

VMware Identity Services 인증 프로세스

VMware Identity Services를 사용하여 외부 ID 제공자와 통신하도록 vCenter Server를 구성하면 다음 인증 프로세스가 발생합니다.

1. 사용자가 vSphere Client를 사용하여 vCenter Server에 로그인합니다.
2. vCenter Single Sign-On는 사용자 인증을 위임하고 사용자 요청을 VMware Identity Services로 리디렉션합니다.
3. VMware Identity Services 프로세스는 사용자 세션을 설정하기 위해 외부 ID 제공자의 토큰을 요청합니다.
4. 외부 ID 제공자는 사용자를 인증하고(MFA(다단계 인증) 또는 SSO 자격 증명을 사용할 수 있음) 토큰을 VMware Identity Services에 반환합니다.

   토큰에는 사용자 클레임이 포함됩니다.

5 VMware Identity Services 프로세스는 ID 제공자 토큰의 유효성을 검사하고 해당 VMware Identity Services 토큰을 생성하며 VMware Identity Services 토큰을 vCenter Single Sign-On으로 보냅니다.

6 vCenter Single Sign-On은 토큰의 유효성을 검사하고 로그인 요청을 승인합니다.

참고 AD FS는 페더레이션된 인증에 VMware Identity Services를 사용하지 않습니다.

vCenter Server가 SCIM에서 푸시한 사용자 및 그룹과 상호 작용하는 방법

외부 ID 제공자를 구성하면 vCenter Server는 사용자 및 그룹 관리를 위해 SCIM(System for Cross-domain Identity Management)을 사용합니다. SCIM은 사용자 ID 정보 교환을 자동화하기 위한 개방형 표준입니다. 외부 IDP 서버에서 생성한 SCIM 애플리케이션은 vCenter Server로 푸시하려는 외부 ID 제공자의 사용자 및 그룹을 관리합니다. vCenter Server는 사용자 및 그룹을 검색하여 vCenter Server 개체에 대한 사용 권한을 할당할 때도 SCIM을 사용합니다.

참고 AD FS 구성은 LDAP를 사용하여 Active Directory를 검색합니다. SCIM을 사용하지 않습니다.

vCenter Server ID 제공자 페더레이션 구성 요소

다음 구성 요소는 vCenter Server ID 제공자 페더레이션 구성에 포함됩니다.

- vCenter Server
  - AD FS: vCenter Server 7.0 이상
  - Okta: vCenter Server 8.0 업데이트 1 이상
  - Microsoft Entra ID: vCenter Server 8.0 업데이트 2 이상
  - PingFederate: vCenter Server 8.0 업데이트 3
- vCenter Server에서 구성된 ID 제공자 서비스
- 외부 ID 제공자(AD FS, Okta, Microsoft Entra ID 또는 PingFederate)
- OIDC(OpenID Connect) 구성:
  - AD FS: 애플리케이션 그룹(애플리케이션이라고도 함)
  - Okta, Microsoft Entra ID 또는 PingFederate: OpenID Connect 애플리케이션
- 사용자 및 그룹 관리를 위한 SCIM(System for Cross-domain Identity Management) 애플리케이션(Okta, Microsoft Entra ID 또는 PingFederate에만 해당)
- vCenter Server 그룹 및 사용자에 매핑되는 외부 ID 제공자 그룹 및 사용자
- vCenter Server에서 사용하도록 설정된 VMware Identity Services(Okta, Microsoft Entra ID 또는 PingFederate에만 해당)
- 필요한 경우 PingFederate 서버의 PingFederate, SSL 인증서 또는 인증서 체인(잘 알려진 공용 인증 기관에서 이 인증서를 발급하지 않은 경우). PingFederate SSL 인증서를 vCenter Server로 가져옵니다.

vCenter Server ID 제공자 페더레이션 주의 사항 및 상호 운용성

vCenter Server ID 제공자 페더레이션은 다른 많은 VMware 기능과 상호 운용할 수 있습니다.

vCenter Server ID 제공자 페더레이션 전략을 계획할 때는 상호 운용성 제한 사항을 고려해야 합니다.

인증 메커니즘

vCenter Server ID 제공자 페더레이션 구성에서 외부 ID 제공자는 인증 메커니즘(암호, MFA, 생체 인식 등)을 처리합니다.

AD FS 및 단일 Active Directory 도메인 지원

AD FS에 대한 vCenter Server ID 제공자 페더레이션을 구성할 때 [기본 ID 제공자 구성] 마법사에 vCenter Server에 액세스하려는 사용자 및 그룹이 포함된 단일 AD 도메인에 대한 LDAP 정보를 입력하라는 메시지가 표시됩니다. vCenter Server는 마법사에 지정한 사용자 기반 DN에서 권한 부여 및 사용 권한에 사용할 AD 도메인을 파생합니다. 이 AD 도메인의 사용자 및 그룹에 대해서만 vSphere 개체에 대한 사용 권한을 추가할 수 있습니다. AD 하위 도메인 또는 AD 포리스트의 다른 도메인에 있는 사용자 또는 그룹은 vCenter Server ID 제공자 페더레이션에서 지원되지 않습니다.

Okta, Microsoft Entra ID 및 PingFederate의 여러 도메인 지원

Okta, Microsoft Entra ID 또는 PingFederate에 대한 vCenter Server ID 제공자 페더레이션을 구성할 때 [기본 ID 제공자 구성] 마법사를 사용하여 vCenter Server에 액세스하려는 사용자 및 그룹이 포함된 여러 도메인에 대한 LDAP 정보를 입력할 수 있습니다.

암호, 잠금 및 토큰 정책

vCenter Server가 ID 제공자 역할을 하는 경우 기본 도메인(vsphere.local 또는 vSphere 설치 시 입력한 도메인 이름)에 대한 vCenter Server 암호, 잠금 및 토큰 정책을 제어합니다. vCenter Server에서 페더레이션 인증을 사용하면, 외부 ID 제공자가 Active Directory와 같은 ID 소스에 저장된 계정에 대한 암호, 잠금 및 토큰 정책을 제어합니다.

감사 및 규정 준수

vCenter Server ID 제공자 페더레이션을 사용하는 경우 vCenter Server는 성공적인 사용자 로그인을 위해 로그 항목을 계속 생성합니다. 하지만, 실패한 암호 입력 시도 및 사용자 계정 잠금과 같은 작업의 추적 및 로깅은 외부 ID 제공자가 담당합니다. vCenter Server는 이러한 이벤트가 vCenter Server에 더 이상 보이지 않기 때문에 기록하지 않습니다. 예를 들어 AD FS가 ID 제공자인 경우 AD FS가 페더레이션 로그인에 대한 오류를 추적하고 기록합니다. vCenter Server가 로컬 로그인에 대한 ID 제공자이면, vCenter Server가 로컬 로그인에 대한 오류를 추적하고 기록합니다. 페더레이션된 구성에서 vCenter Server는 로그인 후에 사용자 작업을 계속 기록합니다.

외부 ID 제공자와 기존 VMware 제품 통합

vCenter Server와 통합된 VMware 제품(예: VMware Aria Operations, vSAN, NSX 등)은 이전처럼 계속 작동합니다.

로그인 후 통합 제품

로그인 후 통합하는 제품(즉, 별도의 로그인이 필요하지 않음)은 이전처럼 계속 작동합니다.

API, SDK 및 CLI 액세스를 위한 간단한 인증

단순 인증(즉, 사용자 이름 및 암호)을 사용하는 API, SDK 또는 CLI 명령에 의존하는 기존 스크립트, 제품 및 기타 기능은 계속 이전처럼 작동합니다. 내부적으로 인증은 사용자 이름과 암호를 전달하여 발생합니다. 사용자 이름과 암호를 전달하면 ID 페더레이션을 사용하는 이점이 일부 손상됩니다. 암호가 vCenter Server(및 스크립트)에 노출되기 때문입니다. 가능한 경우 토큰 기반 인증으로 마이그레이션을 고려해 보십시오.

vCenter Server 관리 인터페이스 액세스

사용자가 vCenter Server 관리자 그룹의 멤버인 경우 vCenter Server 관리 인터페이스(이전 이름: vCenter Server Appliance 관리 인터페이스 또는 VAMI)에 대한 액세스가 지원됩니다.

AD FS 로그인 페이지에서 사용자 이름 텍스트 입력

AD FS 로그인 페이지는 사용자 이름 텍스트 상자를 미리 채우는 텍스트 전달을 지원하지 않습니다. 따라서 AD FS를 통한 페더레이션 로그인 중에 vCenter Server 랜딩 페이지에 사용자 이름을 입력하고 AD FS 로그인 페이지로 리디렉션한 후 AD FS 로그인 페이지에 사용자 이름을 다시 입력해야 합니다. vCenter Server 랜딩 페이지에 입력하는 사용자 이름은 로그인을 적절한 ID 공급자로 리디렉션하는 데 필요하며, AD FS 로그인 페이지의 사용자 이름은 AD FS로 인증하는 데 필요합니다. 사용자 이름을 AD FS 로그인 페이지에 전달할 수 없는 것은 AD FS의 제한 사항입니다. 이러한 동작은 vCenter Server에서 직접 구성하거나 변경할 수 없습니다.

IPv6 주소 지원

AD FS, Microsoft Entra ID 및 PingFederate는 IPv6주소를 지원합니다. Okta는 IPv6 주소를 지원하지 않습니다.

VMware Identity Services 단일 인스턴스 구성

기본적으로 vSphere 8.0 업데이트 1 이상을 설치하거나 vSphere 8.0 업데이트 1 이상으로 업그레이드하면 vCenter Server에서 VMware Identity Services가 사용되도록 설정됩니다. 고급 연결 모드 구성에서 Okta, Microsoft Entra ID 또는 PingFederate를 구성하는 경우 단일 vCenter Server 시스템에서 VMware Identity Services를 사용합니다. 예를 들어 3개의 vCenter Server 시스템으로 구성된 고급 연결 모드 구성에서 Okta를 사용하는 경우, VMware Identity Services 인스턴스 중 하나의 vCenter Server만 Okta 서버와 통신하는 데 사용됩니다.

경고 VMware Identity Services를 사용하는 ELM 구성에서 외부 ID 제공자와 통신하는 vCenter Server 시스템을 사용할 수 없게 되면 ELM 구성의 다른 vCenter Server에서 VMware Identity Services를 구성하여 외부 IDP 서버와 상호 작용할 수 있습니다. 고급 연결 모드 구성의 외부 ID 제공자에 대한 활성화 프로세스의 내용을 참조하십시오.

기본 네트워크 식별자 재구성

vCenter Server의 PNID(기본 네트워크 식별자)를 재구성하려면 다음과 같이 외부 ID 제공자 구성을 업데이트해야 합니다.

- AD FS: 새 리디렉션 URI를 AD FS 서버에 추가합니다.
- Okta: Okta를 재구성합니다. Okta에 대한 vCenter Server ID 제공자 페더레이션 구성 항목을 참조하고 단계에 따라 vCenter Server에 ID 제공자를 생성합니다.
- Microsoft Entra ID: Entra ID를 재구성합니다. Microsoft Entra ID에 대한 vCenter Server ID 제공자 페더레이션 구성 항목을 참조하고 단계에 따라 vCenter Server에 ID 제공자를 생성합니다.
- PingFederate: PingFederate를 재구성합니다. PingFederate에 대한 vCenter Server ID 제공자 페더레이션 구성 항목을 참조하고 단계에 따라 vCenter Server에 ID 제공자를 생성합니다.

vCenter Server ID 제공자 페더레이션 수명 주기

vCenter Server ID 제공자 페더레이션의 수명 주기를 관리할 때 몇 가지 특정한 고려 사항이 있습니다.

다음과 같은 방법으로 vCenter Server ID 제공자 페더레이션 수명 주기를 관리할 수 있습니다.

Active Directory 사용에서 외부 ID 제공자로 마이그레이션

Active Directory를 vCenter Server의 ID 소스로 사용하는 경우 외부 ID 제공자 사용으로 마이그레이션하는 작업은 간단합니다. Active Directory 그룹 및 역할이 ID 제공자 그룹 및 역할과 일치하는 경우 추가 작업을 수행할 필요가 없습니다. 그룹 및 역할이 일치하지 않는 경우에는 몇 가지 추가 작업을 수행해야 합니다. vCenter Server가 도메인 멤버인 경우에는 도메인에서 제거하는 것이 좋습니다. ID 페더레이션에 필요하거나 사용되지 않기 때문입니다.

도메인 간 연결 대상 변경 및 마이그레이션

vCenter Server ID 제공자 페더레이션은 도메인 간 연결 대상 변경을 지원합니다. 즉, vCenter Server를 하나의 vSphere SSO 도메인에서 다른 도메인으로 옮길 수 있습니다. 연결 대상이 변경된 vCenter Server는 vCenter Server 시스템 또는 이것이 가리키는 시스템에서 복제된 ID 제공자 구성을 수신합니다.

일반적으로 다음 중 하나에 해당하지 않는 한, 도메인 간 연결 대상 변경에 대해 추가 ID 제공자 재구성을 수행할 필요가 없습니다.

1 연결 대상이 변경된 vCenter Server의 ID 제공자 구성이 이것이 가리키는 vCenter Server의 ID 제공자 구성과 다릅니다.

2 연결 대상이 변경된 vCenter Server가 ID 제공자 구성을 처음 수신합니다.

이러한 경우 몇 가지 추가 작업이 필요합니다. 예를 들어 AD FS의 경우 vCenter Server 시스템의 리디렉션 URI를 AD FS 서버의 해당 애플리케이션 그룹에 추가해야 합니다. 예를 들어 AD FS 애플리케이션 그룹 A가 있는 vCenter Server 1(또는 AD FS 구성 없음)이 AD FS 애플리케이션 그룹 B가 있는 vCenter Server 2로 연결 대상이 변경된 경우, vCenter Server 1의 리디렉션 URI를 애플리케이션 그룹 B에 추가해야 합니다.

사용자 및 그룹 동기화 및 vCenter Server 백업 및 복원

사용자 및 그룹을 vCenter Server와 동기화하는 시기와 vCenter Server를 백업하는 시기에 따라 vCenter Server를 복원해야 하는 경우 SCIM에서 푸시한 사용자 및 그룹을 다시 동기화해야 할 수도 있습니다.

삭제된 사용자 또는 그룹을 복원하려면 외부 ID 제공자에서 vCenter Server로 사용자나 그룹을 단지 푸시만 하면 안 됩니다. 누락된 사용자 또는 그룹으로 외부 ID 제공자의 SCIM 2.0 애플리케이션을 업데이트해야 합니다. 삭제된 SCIM 사용자 및 그룹 복원의 내용을 참조하십시오.

vCenter Server ID 제공자 페더레이션 및 고급 연결 모드

고급 연결 모드를 사용하여 vCenter Server 환경에서 ID 제공자 페더레이션을 사용하도록 설정하면 인증 및 워크플로가 이전과 같이 계속 작동합니다.

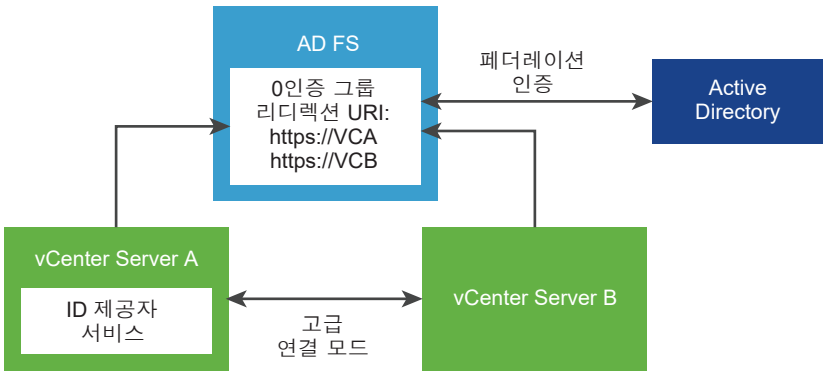
고급 연결 모드 구성을 사용하는 경우 페더레이션된 인증을 사용하여 vCenter Server에 로그인할 때에는 다음에 유의하십시오.

- 사용자는 vCenter Server 사용 권한 및 역할 모델을 기반으로 동일한 인벤토리를 계속 보고 동일한 작업을 수행할 수 있습니다.
- 고급 연결 모드에서 vCenter Server 호스트는 서로의 ID 제공자에 액세스할 필요가 없습니다. 예를 들어 A와 B라는 두 개의 vCenter Server 시스템이 있고 고급 연결 모드를 사용 중이라고 가정합니다. vCenter Server A가 사용자에게 권한을 부여하면 이 사용자는 vCenter Server B에 대한 권한도 부여받습니다.

고급 링크 모드 및 AD FS

다음 그림에서는 고급 연결 모드로 AD FS를 사용할 때의 인증 워크플로를 보여 제공합니다.

그림 4-4. 고급 연결 모드 및 AD FS ID 제공자 페더레이션



1 두 개의 vCenter Server 노드가 고급 연결 모드 구성에 배포되었습니다.

2 vSphere Client에서 [ID 제공자 변경] 마법사를 사용하여 AD FS 설정이 vCenter Server A에 구성되었습니다. AD FS 사용자 또는 그룹에 대한 그룹 멤버 자격 및 사용 권한도 설정되었습니다.

3 vCenter Server A가 AD FS 구성을 vCenter Server B에 복제합니다.

4 두 vCenter Server 노드의 모든 리디렉션 URI가 AD FS의 OAuth 애플리케이션 그룹에 추가됩니다. 하나의 OAuth 애플리케이션 그룹만 생성됩니다.

5 사용자가 vCenter Server A에 로그인하여 권한을 부여받으면 vCenter Server B에서도 권한이 부여됩니다. 사용자가 vCenter Server B에 먼저 로그인한 경우에도 마찬가지입니다.

AD FS를 사용하는 고급 연결 모드 구성 시나리오

vCenter Server 고급 연결 모드는 AD FS에 대해 다음과 같은 구성 시나리오를 지원합니다. 이 섹션에서 "AD FS 설정"과 "AD FS 구성"이라는 용어는 vSphere Client에서 [ID 제공자 변경] 마법사를 사용하여 구성하는 설정 및 AD FS 사용자 또는 그룹에 대해 설정한 그룹 멤버 자격 또는 사용자 권한을 의미합니다.

기존 고급 연결 모드 구성에서 AD FS 사용

개략적인 단계:

1 고급 연결 모드 구성에서 N개의 vCenter Server 노드를 배포합니다.

2 연결된 vCenter Server 노드 중 하나에 AD FS를 구성합니다.

3 AD FS 구성이 모든 다른 (N-1)개 vCenter Server 노드로 복제됩니다.

4 모든 N개 vCenter Server 노드에 대한 리디렉션 URI를 AD FS에 구성된 OAuth 애플리케이션 그룹에 모두 추가합니다.

새 vCenter Server를 기존 고급 연결 모드 AD FS 구성에 연결

개략적인 단계:

1 (사전 요구 사항) vCenter Server N개 노드 고급 연결 모드 구성에서 AD FS를 설정합니다.

2 독립적인 새 vCenter Server 노드를 배포합니다.

3 *N*개 노드 중 하나를 복제 파트너로 사용하여 새 vCenter Server의 연결 대상을 N개 노드 AD FS 고급 연결 모드 도메인으로 변경합니다.

4 기존 고급 연결 모드 구성의 모든 AD FS 설정이 새로운 vCenter Server로 복제됩니다.

   N개 노드 AD FS 고급 연결 모드 도메인에 있는 AD FS 설정이 새로 연결된 vCenter Server의 모든 기존 AD FS 설정을 덮어씁니다.

5 새 vCenter Server에 대한 리디렉션 URI를 AD FS에 구성된 기존 OAuth 애플리케이션 그룹에 모두 추가합니다.

고급 연결 모드 AD FS 구성에서 vCenter Server 연결 해제

개략적인 단계:

1 (사전 요구 사항) N개 노드 vCenter Server 고급 연결 모드 구성에서 AD FS를 설정합니다.

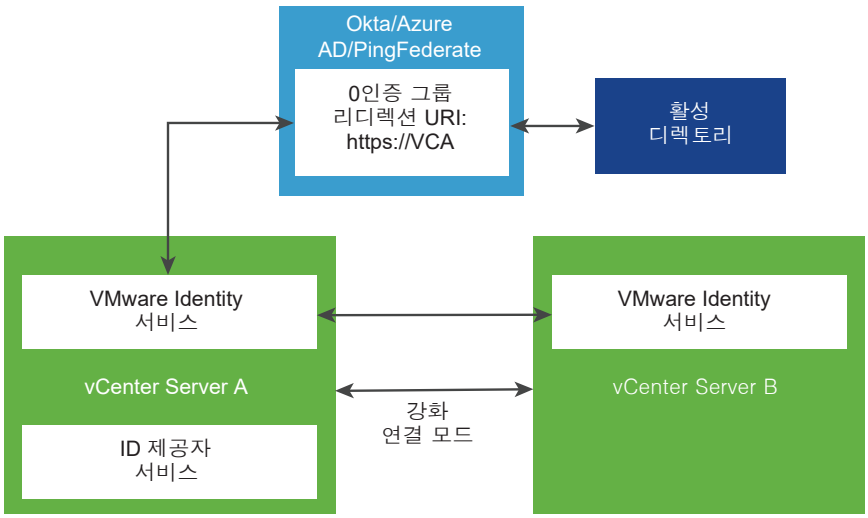
2 N개 노드 구성에서 vCenter Server 호스트 중 하나의 등록을 취소하고 그 연결 대상을 새 도메인으로 변경하여 N개 노드 구성에서 연결을 해제합니다.

3 도메인 연결 대상 변경 프로세스는 SSO 설정을 유지하지 않으므로 연결 해제된 vCenter Server 노드의 모든 AD FS 설정은 되돌려지고 손실됩니다. 연결 해제된 이 vCenter Server 노드에서 AD FS를 계속 사용하려면 AD FS를 처음부터 재구성하거나 vCenter Server를 AD FS가 이미 설정된 고급 연결 모드 구성에 다시 연결해야 합니다.

고급 연결 모드 및 Okta, Microsoft Entra ID 또는 PingFederate ID 제공자 페더레이션

다음 그림에서는 고급 연결 모드로 Okta, Microsoft Entra ID 또는 PingFederate를 사용할 때의 인증 워크플로를 보여줍니다.

그림 4-5. 고급 연결 모드 및 Okta, Microsoft Entra ID 또는 PingFederate ID 제공자 페더레이션



참고 Okta, Microsoft Entra ID 또는 PingFederate를 외부 ID 제공자로 구성하는 경우 고급 연결 모드 구성의 모든 vCenter Server 시스템은 Okta의 경우 vSphere 8.0 업데이트 1, Microsoft Entra ID의 경우 vSphere 8.0 업데이트 2 이상 및 PingFederate의 경우 vSphere 8.0 업데이트 3을 실행해야 합니다.

1 두 개의 vCenter Server 노드가 고급 연결 모드 구성에 배포되었습니다.

2 vSphere Client에서 [ID 제공자 변경] 마법사를 사용하여 Okta, Microsoft Entra ID 또는 PingFederate 설정이 vCenter Server A에 구성되었습니다. 또한 Okta, Microsoft Entra ID 또는 PingFederate 사용자 또는 그룹에 대한 그룹 멤버 자격 및 사용 권한도 설정되었습니다.

   참고 vCenter Server A와 B 모두에 VMware Identity Services가 사용되도록 설정되어 있지만 vCenter Server A에 대한 VMware Identity Services만 ID 제공자 서버와 통신합니다.

3 vCenter Server A에서 실행되는 VMware Identity Services를 사용하면 vCenter Server B가 해당 끝점에 액세스할 수 있습니다.

4 vCenter Server A에 대한 리디렉션 URI가 Okta, Microsoft Entra ID 또는 PingFederate의 OAuth 애플리케이션에 추가됩니다. 하나의 OAuth 애플리케이션만 생성됩니다.

5 사용자가 vCenter Server A에 로그인하여 권한을 부여받으면 vCenter Server B에서도 권한이 부여됩니다. 사용자가 vCenter Server B에 먼저 로그인한 경우에도 마찬가지입니다.

Okta, Microsoft Entra ID 또는 PingFederate를 사용하는 고급 연결 모드 구성 시나리오

vCenter Server 고급 연결 모드는 Okta, Microsoft Entra ID 또는 PingFederate에 대해 다음과 같은 구성 시나리오를 지원합니다. 이 섹션에서 'Okta 설정' 및 'Okta 구성', 'Microsoft Entra ID 설정' 및 'Microsoft Entra ID 구성' 또는 'PingFederate 설정' 및 'PingFederate 구성'이라는 용어는 vSphere Client에서 [ID 제공자 변경] 마법사를 사용하여 구성하는 설정 및 Okta, Microsoft Entra ID 또는 PingFederate 사용자 또는 그룹에 대해 설정한 그룹 멤버 자격 또는 사용 권한을 의미합니다.

기존 고급 연결 모드 구성에서 Okta, Microsoft Entra ID 또는 PingFederate 사용

개략적인 단계:

1 고급 연결 모드 구성에서 N개의 vCenter Server 노드를 배포합니다.

2 연결된 vCenter Server 노드 중 하나에서 Okta, Microsoft Entra ID 또는 PingFederate를 구성합니다.

3 VMware Identity Services 끝점 정보가 모두 다른 (N-1)개 vCenter Server 노드로 복제됩니다.

Okta, Microsoft Entra ID 또는 PingFederate 구성(공유 클라이언트 ID 등) 정보 및 사용자/그룹 정보는 복제되지 않습니다.

새 vCenter Server를 기존 고급 연결 모드 Okta, Microsoft Entra ID 또는 PingFederate 구성에 연결

개략적인 단계:

1 (사전 요구 사항) vCenter Server N개 노드 고급 연결 모드 구성에서 Okta, Microsoft Entra ID 또는 PingFederate를 설정합니다.

2 독립적인 새 vCenter Server 노드를 배포합니다.

3 *N*개 노드 중 하나를 복제 파트너로 사용하여 새 vCenter Server의 연결 대상을 N개 노드 Okta, Microsoft Entra ID 또는 PingFederate 고급 연결 모드 도메인으로 변경합니다.

4 VMware Identity Services 끝점 정보가 모두 다른 (N-1)개 vCenter Server 노드로 복제됩니다.

Okta, Microsoft Entra ID 또는 PingFederate 구성(공유 클라이언트 ID 등) 정보 및 사용자/그룹 정보는 복제되지 않습니다.

참고 기존 VMware Identity Services 구성에서 vCenter Server 노드를 추가할 수 있습니다. 이 시나리오에서는 기존 VMware Identity Services 구성이 가입 중인 VMware ID 서비스 고급 연결 모드 구성으로 대체됩니다.

VMware Identity Services로 구성되지 않은 ELM 구성에는 기존 VMware Identity Services 구성에서 vCenter Server 노드를 추가할 수 없습니다. 이 시나리오에서는 ELM 구성에 추가하기 전에 먼저 기존 VMware Identity Services 구성을 vCenter Server에서 제거합니다.

기존 고급 연결 모드 Okta, Microsoft Entra ID 또는 PingFederate 구성에서 vCenter Server 연결 해제

개략적인 단계:

1 (사전 요구 사항) N개 노드 vCenter Server 고급 연결 모드 구성에서 Okta, Microsoft Entra ID 또는 PingFederate를 설정합니다.

2 N개 노드 구성에서 vCenter Server 호스트 중 하나의 등록을 취소하고 그 연결 대상을 새 도메인으로 변경하여 N개 노드 구성에서 연결을 해제합니다.

3 도메인 연결 대상 변경 프로세스는 SSO 설정을 유지하지 않으므로 연결 해제된 vCenter Server 노드의 모든 Okta, Microsoft Entra ID 또는 PingFederate 설정은 되돌려지고 손실됩니다. 연결 해제된 이 vCenter Server 노드에서 Okta, Microsoft Entra ID 또는 PingFederate를 계속 사용하려면 Okta, Microsoft Entra ID 또는 PingFederate를 처음부터 재구성하거나 vCenter Server를 Okta, Microsoft Entra ID 또는 PingFederate가 이미 설정된 고급 연결 모드 구성에 다시 연결해야 합니다.

참고 활성 VMware Identity Services 구성에서 vCenter Server를 연결 해제할 수 없습니다.

고급 연결 모드 구성의 외부 ID 제공자에 대한 활성화 프로세스

Okta, Microsoft Entra ID 또는 PingFederate를 사용하는 고급 연결 모드 구성의 가용성 고려 사항에 대해 자세히 알아봅니다.

사전 요구 사항

- 고급 연결 모드 구성에서 둘 이상의 vCenter Server 시스템. 예를 들어 시스템에는 VC_1, VC_2, VC_3 ~ VC_N이라는 레이블이 지정되며, 여기서 N은 고급 연결 모드 구성의 vCenter Server 시스템 수입니다.
- Okta 및 Microsoft Entra ID의 경우 모든 vCenter Server 시스템은 vSphere 8.0 업데이트 2 이상을 실행해야 합니다. PingFederate의 경우 모든 vCenter Server 시스템은 최소한 vSphere 8.0 업데이트 3을 실행해야 합니다.
- Okta, Microsoft Entra ID 또는 PingFederate는 vCenter Server 시스템 중 하나에서 외부 ID 제공자로 구성됩니다. 예를 들어 시스템에는 VC_1이라는 레이블이 지정됩니다.
- 외부 ID 제공자는 모든 필수 OAuth2 및 SCIM 애플리케이션으로 구성됩니다.

절차

1 지정된 vCenter Server VC_i(여기서 i는 2와 N 사이)를 활성화하려면 다음을 수행합니다.

a 활성화 스크립트를 실행하기 위해 VC_i에 대한 로컬 셸 액세스 권한을 확보합니다.

참고 아래 단계를 수행하기 위해 명령줄 또는 콘솔 프롬프트에서 관리 권한이 있는 vCenter Server 사용자 계정을 부여할 수 있습니다.

b 활성화 스크립트에서 `'status'`를 실행하여 vCenter Server의 현재 활성화 상태를 가져옵니다.

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

c `'status'` 명령이 vCenter Server가 활성화되지 않았음을 나타내는 활성화 스크립트에서 `'activate'`를 실행합니다.

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

d `'status'` 명령이 vCenter Server가 이미 활성화되어 있음을 나타내면 `'deactivate'` 옵션을 실행한 다음, `'activate'` 옵션을 실행합니다.

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

- 예를 들어 `'activate'` 옵션을 실행합니다.
- 또는 `'activate'` 명령에서 `'--force-replace'` 옵션을 지정할 수 있습니다.

2 브라우저에서 vCenter Server VC_i를 열고 vCenter Server에 관리자로 로그인합니다.

a **홈 > 관리 > Single Sign-On > 구성**으로 이동합니다.

b **사용자 프로비저닝**에서 **테넌트 URL**에 VC_i의 FQDN이 포함되어 있는지 확인합니다.

c **테넌트 URL** 문자열을 복사하고 이 정보를 외부 ID 제공자와 함께 사용할 수 있도록 저장합니다.

d **비밀 토큰** 아래에서 **생성**을 클릭하고 생성된 토큰 문자열을 복사한 후 외부 ID 제공자와 함께 사용할 수 있도록 이 정보를 저장합니다.

e **OpenID Connect** 아래에서 **리디렉션 URI**에 VC_i의 FQDN이 포함되어 있는지 확인합니다.

f **리디렉션 URI** 문자열을 복사하고 이 정보를 외부 ID 제공자와 함께 사용하기 위해 저장합니다.

3 브라우저를 열고 외부 ID 제공자의 관리 페이지로 이동합니다.

참고 자세한 내용은 외부 ID 제공자 관련 세부 정보를 참조하여 다음 단계를 수행하십시오.

a 외부 ID 제공자가 원래 VC_1 구성되었을 때 설정된 OAuth2 등록을 찾습니다.

b OAuth2 등록을 편집하고 이전에 VC_i 대해 가져온 리디렉션 URI를 추가합니다.

c 외부 ID 제공자가 대상이 여러 개인 SCIM 푸시 구성을 지원하는 경우에는:
   - 외부 ID 제공자가 원래 VC_1 구성되었을 때 설정된 SCIM 푸시 구성을 찾습니다.
   - SCIM 푸시 구성을 편집하고 이전에 VC_i에 대해 가져온 **테넌트 URL** 및 **비밀 토큰**을 추가합니다.

d 외부 ID 제공자가 대상이 하나뿐인 SCIM 푸시 구성을 지원하는 경우:
   - 이전에 VC_i에 대해 가져온 **테넌트 URL** 및 **비밀 토큰**을 사용하여 새 SCIM 푸시 구성을 생성합니다.
   - SCIM 푸시 구성이 외부 ID 제공자가 원래 VC_1 구성되었을 때 설정된 SCIM 푸시 구성과 동일한 사용자/그룹 데이터를 푸시하는지 확인합니다.

e VC_I 최신 사용자 또는 그룹 데이터로 채워지도록 SCIM 푸시 작업을 시작합니다.

vCenter Server ID 제공자 페더레이션 구성

vCenter Server를 처음 배포한 후 페더레이션 인증을 위한 외부 ID 제공자를 구성할 수 있습니다.

vSphere 7.0 이상은 AD FS(Active Directory Federation Services)를 지원합니다. vSphere 8.0 업데이트 1 이상은 Okta를 지원합니다. vSphere 8.0 업데이트 2 이상은 Microsoft Entra ID(이전 이름: Azure AD)를 지원합니다. vSphere 8.0 업데이트 3부터 vSphere는 PingFederate를 지원합니다.

vSphere Client 또는 API에서 vCenter Server ID 제공자 페더레이션을 구성합니다. 또한 외부 ID 제공자에 대한 구성도 수행해야 합니다. vCenter Server ID 제공자 페더레이션을 구성하려면 vCenter Single Sign-On 관리자 권한이 있어야 합니다. vCenter Single Sign-On 관리자 권한은 vCenter Server 또는 ESXi의 관리자 역할과 다릅니다. 새 설치의 경우에는 vCenter Single Sign-On 관리자(기본적으로 administrator@vsphere.local)만 vCenter Single Sign-On에 인증할 수 있습니다.

vCenter Server ID 제공자 페더레이션 구성 프로세스 흐름

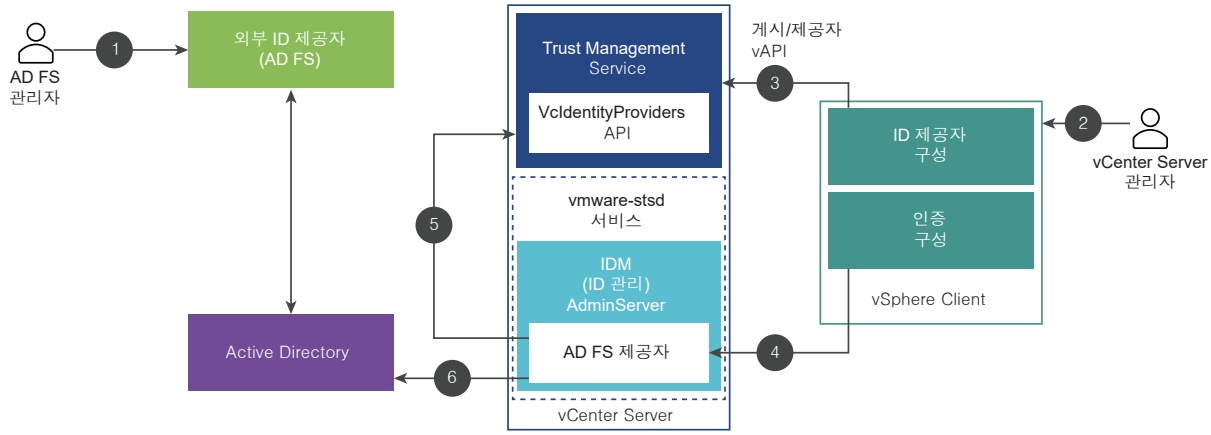
vCenter Server ID 제공자 페더레이션을 효과적으로 구성하려면 발생하는 통신 흐름을 이해해야 합니다.

AD FS, Microsoft Entra ID(이전 명칭: Azure AD), Okta 또는 PingFederate에 대한 vCenter Server ID 제공자 페더레이션을 구성할 수 있습니다.

AD FS에 대한 vCenter Server ID 제공자 페더레이션 구성 프로세스 흐름

다음 그림은 AD FS에 대한 vCenter Server ID 제공자 페더레이션을 구성할 때 발생하는 프로세스 흐름을 보여 줍니다.

그림 4-6. AD FS에 대한 vCenter Server ID 제공자 페더레이션 구성 프로세스 흐름



vCenter Server, AD FS 및 Active Directory는 다음과 같이 상호 작용합니다.

1 AD FS 관리자가 vCenter Server에 대한 AD FS OIDC 애플리케이션을 구성합니다.

2 vCenter Server 관리자가 vSphere Client를 사용하여 vCenter Server에 로그인합니다.

3 vCenter Server 관리자가 AD FS ID 제공자를 vCenter Server에 추가하고 Active Directory 도메인에 대한 정보를 입력합니다.

   vCenter Server에서 AD FS 서버의 Active Directory 도메인에 LDAP를 연결하려면 이 정보가 필요합니다. vCenter Server는 이 연결을 사용하여 사용자와 그룹을 검색하여 다음 단계에서 vCenter Server 로컬 그룹에 추가합니다. 자세한 내용은 아래에 나오는 "Active Directory 도메인 검색" 섹션을 참조하십시오.

4 vCenter Server 관리자가 AD FS 사용자를 위해 vCenter Server에서 권한 부여 권한을 구성합니다.

5 AD FS 제공자가 VcIdentityProviders API를 쿼리하여 Active Directory 소스에 대한 LDAP 연결 정보를 얻습니다.

6 AD FS 제공자가 Active Directory에서 쿼리된 사용자 또는 그룹을 검색하고 권한 부여 구성을 마칩니다.

Active Directory 도메인 검색

vSphere Client에서 [기본 ID 제공자 구성] 마법사를 사용하여 AD FS를 vCenter Server에서 외부 ID 제공자로 구성합니다. 구성 프로세스의 일부로, 사용자 및 그룹 고유 이름 정보를 포함하여 Active Directory 도메인에 대한 정보를 입력해야 합니다. 인증을 위해 AD FS를 구성하려면 이 Active Directory 연결 정보가 필요합니다. 이 연결은 Active Directory 사용자 이름 및 그룹을 검색하여 vCenter Server의 역할 및 권한에 매핑하는 데 필요하고 AD FS는 사용자 인증에 사용됩니다. 이 [기본 ID 제공자 구성] 마법사 단계는 LDAP를 통한 Active Directory ID 소스를 생성하지 않습니다. 대신, vCenter Server는 이 정보를 사용하여 Active Directory 도메인에 대한 유효한 검색 가능한 연결을 설정하여 여기에서 사용자 및 그룹을 찾습니다.

다음 고유 이름 항목을 사용하는 예를 고려해 보십시오.

- 사용자의 기본 고유 이름: cn=Users,dc=corp,dc=local
- 그룹의 기본 고유 이름: dc=corp,dc=local
- 사용자 이름: cn=Administrator,cn=Users,dc=corp,dc=local

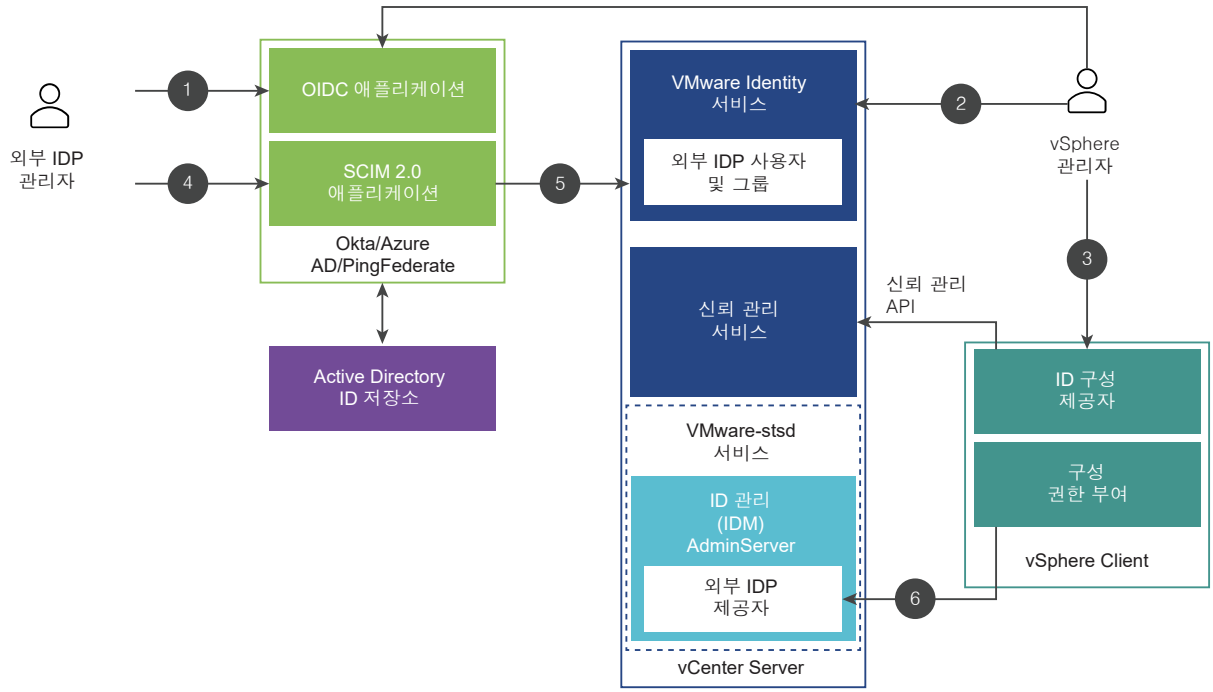
AdfsUser@corp.local 사용자가 ADGroup@corp.local 그룹의 멤버인 경우 마법사에 이 정보를 입력하면 vCenter Server 관리자가 ADGroup@corp.local 그룹을 검색하고 찾아서 vCenter Server Administrators@vsphere.local 그룹에 추가할 수 있습니다. 그러면 AdfsUser@corp.local 사용자는 로그인했을 때 vCenter Server에서 관리 권한이 부여됩니다.

vCenter Server는 사용자가 Active Directory 사용자 및 그룹에 대해 글로벌 사용 권한을 구성할 때에도 이 검색 프로세스를 사용합니다. 글로벌 사용 권한을 구성하거나 사용자 또는 그룹을 추가하는 이 두 가지 경우 모두, **도메인** 드롭다운 메뉴에서 AD FS ID 제공자에 대해 입력한 도메인을 선택하여 Active Directory 도메인에서 사용자 및 그룹을 검색하고 선택할 수 있습니다.

VMware Identity Services를 사용한 vCenter Server ID 제공자 페더레이션 구성 프로세스 흐름

Okta, Microsoft Entra ID 및 PingFederate를 구성하려면 VMware Identity Services를 사용하면 됩니다. 다음 그림은 VMware Identity Services를 사용하여 vCenter Server ID 제공자 페더레이션을 구성할 때 발생하는 프로세스 흐름을 보여줍니다.

그림 4-7. VMware Identity Services를 사용한 vCenter Server ID 제공자 페더레이션 구성 프로세스 흐름



vCenter Server, VMware Identity Services 및 Active Directory는 다음과 같이 상호 작용합니다.

1 외부 IDP 관리자가 vCenter Server에 대한 OIDC 애플리케이션을 구성합니다.

2 vCenter Server 관리자는 vSphere Client를 사용하여 vCenter Server에 로그인한 후 vCenter Server에 ID 제공자를 추가하고 도메인 정보도 입력합니다.

3 vCenter Server 관리자는 리디렉션 URI(vSphere Client의 ID 제공자 구성 페이지에서 가져옴)를 ID 제공자 관리자에게 제공하여 2단계에서 생성된 OIDC 애플리케이션에 추가합니다.

4 외부 IDP 관리자는 SCIM 2.0 애플리케이션을 구성합니다.

5 외부 IDP 관리자는 SCIM 2.0 애플리케이션에 사용자 및 그룹을 할당하고 사용자 및 그룹을 vCenter Server에 푸시합니다.

6 vCenter Server 관리자가 외부 IDP 사용자를 위해 vCenter Server에서 권한 부여 권한을 구성합니다.

외부 IDP 사용자 및 그룹

외부 ID 제공자는 사용자 및 그룹에 대해 SCIM(System for Cross-domain Identity Management)을 사용하기 때문에 해당 사용자 및 그룹이 vCenter Server에 상주합니다. 예를 들어 사용 권한을 할당하기 위해 외부 ID 제공자에서 사용자 및 그룹을 검색하는 경우 검색은 vCenter Server에서 로컬로 수행됩니다.

vCenter Server는 외부 IDP 사용자 및 그룹에 대한 글로벌 사용 권한을 구성할 때도 이 검색 프로세스를 사용합니다. 글로벌 사용 권한을 구성하거나 사용자 또는 그룹을 추가하는 이 두 가지 경우 모두, **도메인** 드롭다운 메뉴에서 ID 제공자에 대해 입력한 도메인을 선택하여 도메인에서 사용자 및 그룹을 검색하고 선택할 수 있습니다.

JRE 신뢰 저장소 대신 신뢰할 수 있는 루트 인증서 저장소를 사용합니다.

vSphere 7.0 업데이트 1부터 자체 내부 CA(인증 기관)에서 발급한 루트 CA 인증서를 vSphere 7.0의 JRE 신뢰 저장소로 가져온 경우 해당 인증서를 신뢰할 수 있는 루트 인증서 저장소에 등록할 수 있습니다.

자체 내부 CA(인증 기관)에서 발급한 루트 CA 인증서로 vSphere 7.0에서 vCenter Server ID 제공자 페더레이션을 구성하려면 해당 인증서를 JRE 신뢰 저장소로 가져와야 했습니다. vSphere 7.0 업데이트 1부터는 인증서를 신뢰할 수 있는 루트 인증서 저장소에 등록할 수 있습니다. 이러한 변경은 자체 내부 CA(인증 기관)에서 발급한 루트 CA 인증서를 신뢰할 수 있는 루트 인증서 저장소(VMware Endpoint 인증서 저장소 또는 VECS라고도 함)에 추가해야 함을 의미합니다. JRE 신뢰 저장소의 인증서는 계속 작동하지만 vCenter Server가 신뢰할 수 있는 루트 인증서 저장소 사용에 대해 표준화하고 있습니다.

절차

1 vSphere Client를 사용하여 vCenter Server에 로그인합니다.

참고 자세한 내용은 vSphere Client를 사용하여 신뢰할 수 있는 루트 인증서를 인증서 저장소에 추가에서 참조하십시오.

2 **관리 > 인증서 > 인증서 관리**로 이동합니다.

3 **신뢰할 수 있는 루트 인증서** 옆의 **추가**를 클릭합니다.

4 AD FS 루트 인증서를 찾아서 **추가**를 클릭합니다.

인증서가 **신뢰할 수 있는 루트 인증서** 아래 패널에 추가됩니다.

AD FS에 대한 vCenter Server ID 제공자 페더레이션 구성

vSphere 7.0 이상을 설치하거나 업그레이드한 후 AD FS에 대한 vCenter Server ID 제공자 페더레이션을 외부 ID 제공자로 구성할 수 있습니다.

참고 이 지침은 vSphere 8.0 업데이트 1 이상에 대한 것입니다. vSphere 8.0의 경우 https://docs.vmware.com/kr/VMware-vSphere/8.0/vsphere-documentation-80.zip의 "vSphere 인증" 설명서에서 AD FS에 대한 vCenter Server ID 제공자 페더레이션 구성에 대한 항목을 참조하십시오.

vCenter Server는 구성된 외부 ID 제공자(하나의 소스)와 vsphere.local ID 소스를 하나만 지원합니다. 외부 ID 제공자를 여러 개 사용할 수 없습니다. vCenter Server ID 제공자 페더레이션은 OIDC(OpenID Connect)를 사용하여 사용자가 vCenter Server에 로그인되도록 합니다.

이 작업에서는 사용 권한을 제어하는 방법으로 AD FS 그룹을 vSphere 관리자 그룹에 추가하는 방법을 설명합니다. vCenter Server에서 글로벌 또는 개체 사용 권한을 통해 AD FS 인증을 사용하여 권한을 구성할 수도 있습니다. 사용 권한 추가에 대한 자세한 내용은 "vSphere 보안" 설명서를 참조하십시오.

경고 이전에 vCenter Server에 추가한 Active Directory ID 소스를 AD FS ID 소스로 사용하는 경우에는 vCenter Server에서 기존 ID 소스를 삭제하지 마십시오. 그렇게 하면 이전에 할당된 역할 및 그룹 멤버 자격으로 회귀가 발생합니다. 글로벌 사용 권한이 있는 AD FS 사용자와 관리자 그룹에 추가된 사용자가 모두 로그인할 수 없습니다.

해결 방법: 이전에 할당된 역할 및 그룹 멤버 자격이 필요하지 않은 경우 이전 Active Directory ID 소스를 제거하려면, AD FS 제공자를 생성하고 vCenter Server에서 그룹 멤버 자격을 구성하기 전에 ID 소스를 제거합니다.

사전 요구 사항

참고 AD FS ID 제공자를 구성하는 이 프로세스에서는 vCenter Server 및 AD FS 서버 모두에 대한 관리 액세스 권한이 있어야 합니다. 구성 프로세스 중에 먼저 vCenter Server에 정보를 입력한 다음 AD FS 서버에 입력한 후 vCenter Server에 입력합니다.

Active Directory Federation Service 요구 사항:

- Windows Server 2016 이상용 AD FS가 이미 배포되어 있어야 합니다.
- AD FS가 Active Directory에 연결되어 있어야 합니다.
- 구성 프로세스의 일환으로 AD FS에서 vCenter Server용 애플리케이션 그룹을 생성해야 합니다. VMware 기술 자료 문서(https://kb.vmware.com/s/article/78029)를 참조하십시오.
- 신뢰할 수 있는 루트 인증서 저장소에 추가하는 AD FS 서버 인증서(또는 AD FS 서버 인증서에 서명한 CA 또는 중간 인증서).
- vCenter Server 관리자 권한을 부여하려는 사용자가 포함된 vCenter Server 관리자 그룹을 AD FS에 생성했습니다.

AD FS 구성에 대한 자세한 내용은 Microsoft 설명서를 참조하십시오.

vCenter Server 및 기타 요구 사항:

- vSphere 7.0 이상
- vCenter Server는 AD FS 검색 끝점, 권한 부여, 토큰, 로그아웃, JWKS 및 검색 끝점 메타데이터에 보급된 기타 끝점에 연결할 수 있어야 합니다.
- 페더레이션 인증에 필요한 vCenter Server ID 제공자를 생성, 업데이트 또는 삭제하려면 **VcIdentityProviders.Manage** 권한이 필요합니다. 사용자가 ID 제공자 구성 정보만 보도록 제한하려면 **VcIdentityProviders.Read** 권한을 할당합니다.

절차

1 vSphere Client를 사용하여 vCenter Server에 로그인합니다.

2 AD FS 서버 인증서(또는 AD FS 서버 인증서에 서명한 CA 또는 중간 인증서)를 신뢰할 수 있는 루트 인증서 저장소에 추가합니다.

참고 자세한 내용은 vSphere Client를 사용하여 신뢰할 수 있는 루트 인증서를 인증서 저장소에 추가에서 참조하십시오.

a **관리 > 인증서 > 인증서 관리**로 이동합니다.

b **신뢰할 수 있는 루트 저장소** 옆에 있는 **추가**를 클릭합니다.

c AD FS 인증서를 찾아서 **추가**를 클릭합니다.

인증서가 **신뢰할 수 있는 루트 인증서** 아래 패널에 추가됩니다.

3 vCenter Server에서 ID 제공자를 생성하기 시작합니다.

a vSphere Client를 사용하여 vCenter Server에 관리자로 로그인합니다.

b **홈 > 관리 > Single Sign On > 구성**으로 이동합니다.

c **제공자 변경**을 클릭하고 **ADFS**를 선택합니다.

기본 ID 제공자 구성 마법사가 열립니다.

d **사전 요구 사항** 패널에서 AD FS 및 vCenter Server 요구 사항을 검토합니다.

e **사전 검사 실행**을 클릭합니다.

사전 검사에서 오류가 발견되면 **세부 정보 보기**를 클릭하고 표시된 대로 오류를 해결하는 단계를 수행합니다.

f 사전 검사가 통과되면 확인란을 클릭하고 **다음**을 클릭합니다.

g **사용자 및 그룹** 패널에서 LDAP를 통한 Active Directory 연결의 사용자 및 그룹 정보를 입력하여 사용자 및 그룹을 검색합니다.

vCenter Server는 사용자의 기본 고유 이름에서 권한 부여 및 사용 권한에 사용할 AD 도메인을 파생합니다. 이 AD 도메인의 사용자 및 그룹에 대해서만 vSphere 개체에 대한 사용 권한을 추가할 수 있습니다. AD 하위 도메인 또는 AD 포리스트의 다른 도메인에 있는 사용자 또는 그룹은 vCenter Server ID 제공자 페더레이션에서 지원되지 않습니다.

옵션	설명
사용자의 기본 고유 이름	사용자의 기본 고유 이름입니다.
그룹의 기본 고유 이름	그룹의 기본 고유 이름입니다.
사용자 이름	도메인에서 사용자 및 그룹의 기본 DN에 대해 최소한 읽기 전용 액세스 권한이 있는 사용자의 ID입니다.
암호	도메인에서 사용자 및 그룹의 기본 DN에 대해 최소한 읽기 전용 액세스 권한이 있는 사용자의 ID입니다.
기본 서버 URL	도메인의 기본 도메인 컨트롤러 LDAP 서버입니다. **`ldap://hostname:port`** 또는 **`ldaps://hostname:port`** 형식을 사용합니다. 일반적으로 포트는 LDAP 연결의 경우 389이고 LDAPS 연결의 경우 636입니다. Active Directory 다중 도메인 컨트롤러 배포의 경우 일반적으로 포트는 LDAP의 경우 3268이고 LDAPS의 경우 3269입니다. 기본 또는 보조 LDAP URL에 **`ldaps://`**를 사용하는 경우 Active Directory 서버의 LDAPS 끝점에 대한 신뢰를 설정하는 인증서가 필요합니다.
보조 서버 URL	페일오버에서 사용되는 보조 도메인 컨트롤러 LDAP 서버의 주소입니다.
SSL 인증서	Active Directory LDAP 서버 또는 OpenLDAP 서버 ID 소스와 함께 LDAPS를 사용하려는 경우 **찾아보기**를 클릭하여 인증서를 선택합니다.

h **다음**을 클릭합니다.

i **OpenID Connect** 패널에서 리디렉션 URI 및 로그아웃 리디렉션 URI를 복사합니다.

지금은 다른 필드를 비워둡니다. 다음 단계에서 OpenID Connect 구성을 생성한 후 **OpenID Connect** 패널로 돌아갑니다.

4 AD FS에서 OpenID Connect 구성을 생성하고 vCenter Server에 맞게 구성합니다.

vCenter Server와 ID 제공자 간 당사자 신뢰를 설정하려면 서로 간에 식별 정보 및 공유 암호를 설정해야 합니다. AD FS에서는 서버 애플리케이션과 웹 API로 구성된, 애플리케이션 그룹이라고 하는 OpenID Connect 구성을 생성하여 이 작업을 수행합니다. 이 두 구성 요소는 AD FS 서버를 신뢰하고 이 서버와 통신하기 위해 vCenter Server에서 사용하는 정보를 지정합니다. AD FS에서 OpenID Connect를 사용하도록 설정하려면 https://kb.vmware.com/s/article/78029에서 VMware 기술 자료 문서를 참조하십시오.

AD FS 애플리케이션 그룹을 생성할 때는 다음 내용에 유의하십시오.

- 이전 단계에서 가져온 두 개의 vCenter Server 리디렉션 URI가 필요합니다.

- 다음 단계에서 vCenter Server ID 제공자 생성을 완료할 때 사용할 수 있도록 AD FS 애플리케이션 그룹에서 다음 정보를 파일로 복사하거나 적어둡니다.
  - 클라이언트 식별자
  - 공유 암호
  - AD FS 서버의 OpenID 주소

참고 필요한 경우 다음 PowerShell 명령을 AD FS 관리자로 실행하여 AD FS 서버의 OpenID 주소를 가져옵니다.

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

반환된 URL을 복사합니다(닫는 괄호 또는 초기 `"@{FullUrl="` 부분이 아닌 URL 자체만 선택).

5 vCenter Server **OpenID Connect** 패널에서:

a AD FS 애플리케이션 그룹을 만들 때 이전 단계에서 확보한 다음 정보를 입력합니다.
  - 클라이언트 식별자
  - 공유 암호
  - OpenID 주소

  ID 제공자 이름은 자동으로 Microsoft ADFS로 채워집니다.

b **다음**을 클릭합니다.

6 정보를 검토하고 **마침**을 클릭합니다.

vCenter Server는 AD FS ID 제공자를 생성하고 구성 정보를 표시합니다.

7 AD FS 인증을 위해 vCenter Server에서 그룹 멤버 자격을 구성합니다.

a **홈** 메뉴에서 **관리**를 선택합니다.

b **Single Sign-On**에서 **사용자 및 그룹**을 클릭합니다.

c **그룹** 탭을 클릭합니다.

d **관리자** 그룹을 클릭하고 **멤버 추가**를 클릭합니다.

e 드롭다운 메뉴에서 도메인을 선택합니다.

f 드롭다운 메뉴 아래의 텍스트 상자에 추가하려는 AD FS 그룹의 처음 몇 자를 입력한 다음, 드롭다운 선택 항목이 나타날 때까지 기다립니다.

  vCenter Server가 Active Directory에 연결을 설정하고 검색하는 동안 선택 항목이 나타나려면 몇 초 정도 걸릴 수 있습니다.

g AD FS 그룹을 선택하여 관리자 그룹에 추가합니다.

h **저장**을 클릭합니다.

8 Active Directory 사용자로 vCenter Server에 로그인되는지 확인합니다.

Okta에 대한 vCenter Server ID 제공자 페더레이션 구성

vSphere 8.0 업데이트 1 이상을 설치하거나 이 버전으로 업그레이드한 후 Okta에 대한 vCenter Server ID 제공자 페더레이션을 외부 ID 제공자로 구성할 수 있습니다.

vCenter Server는 구성된 외부 ID 제공자(하나의 소스)와 vsphere.local ID 소스(로컬 소스)를 하나만 지원합니다. 외부 ID 제공자를 여러 개 사용할 수 없습니다. vCenter Server ID 제공자 페더레이션은 OIDC(OpenID Connect)를 사용하여 사용자가 vCenter Server에 로그인되도록 합니다.

vCenter Server에서 전역 또는 개체 사용 권한을 통해 Okta 그룹 및 사용자를 사용하여 권한을 구성할 수 있습니다. 사용 권한 추가에 대한 자세한 내용은 "vSphere 보안" 설명서를 참조하십시오.

사전 요구 사항

Okta 요구 사항:

- Okta를 사용 중이고 전용 도메인 공간(예: https://*your-company*.okta.com)이 있습니다.
- OIDC 로그인을 수행하고 사용자 및 그룹 권한을 관리하려면 다음 Okta 애플리케이션을 생성해야 합니다.
  - OpenID Connect를 로그온 방법으로 사용하는 Okta 네이티브 애플리케이션. 네이티브 애플리케이션에는 인증 코드, 새로 고침 토큰 및 리소스 소유자 암호의 권한 부여 유형이 포함되어야 합니다.
  - Okta 서버와 vCenter Server 간에 사용자 및 그룹 동기화를 수행하기 위한 OAuth 2.0 보유자 토큰이 있는 SCIM(System for Cross-domain Identity Management) 2.0 애플리케이션.

  VMware 기술 자료 문서(https://kb.vmware.com/s/article/90835)를 참조하십시오.
- vCenter Server와 공유하려는 Okta 사용자 및 그룹을 식별했습니다. 이 공유는 SCIM 작업입니다(OIDC 작업이 아님).

Okta 연결 요구 사항:

- vCenter Server는 Okta 검색 끝점, 권한 부여, 토큰, 로그아웃, JWKS 및 검색 끝점 메타데이터에 보급된 기타 끝점에 연결할 수 있어야 합니다.
- Okta는 SCIM 프로비저닝을 위해 사용자 및 그룹 데이터를 보내기 위해 vCenter Server와 연결할 수 있어야 합니다.

vCenter Server 요구 사항:

- vSphere 8.0 업데이트 1 이상
- Okta ID 소스를 생성하려는 vCenter Server에서 VMware Identity Services가 활성화되었는지 확인합니다.

  참고 vSphere 8.0 업데이트 1 이상으로 업그레이드하거나 설치하는 경우 VMware ID 서버가 기본적으로 활성화됩니다. vCenter Server 관리 인터페이스를 사용하여 VMware Identity Services의 상태를 확인할 수 있습니다. VMware Identity Services 중지 및 시작의 내용을 참조하십시오.

vSphere 권한 요구 사항:

- 페더레이션 인증에 필요한 vCenter Server ID 제공자를 생성, 업데이트 또는 삭제하려면 **VcIdentityProviders.Manage** 권한이 있어야 합니다. 사용자가 ID 제공자 구성 정보만 보도록 제한하려면 **VcIdentityProviders.Read** 권한을 할당합니다.

고급 연결 모드 요구 사항:

- 고급 연결 모드 구성에서 Okta에 대한 vCenter Server ID 제공자 페더레이션을 구성할 수 있습니다. 고급 연결 모드 구성에서 Okta를 구성하는 경우 단일 vCenter Server시스템에서 VMware Identity Services를 사용하도록 Okta ID 제공자를 구성합니다. 예를 들어 고급 연결 모드 구성이 두 개의 vCenter Server 시스템으로 구성된 경우 하나의 vCenter Server와 해당 VMware Identity Services 인스턴스만 Okta 서버와 통신하는 데 사용됩니다. 이 vCenter Server 시스템을 사용할 수 없게 되면 ELM 구성의 다른 vCenter Server에서 VMware Identity Services를 구성하여 Okta서버와 상호 작용할 수 있습니다. 자세한 내용은 고급 연결 모드 구성의 외부 ID 제공자에 대한 활성화 프로세스의 내용을 참조하십시오.
- Okta를 외부 ID 제공자로 구성할 때 고급 연결 모드 구성의 모든 vCenter Server 시스템은 vSphere 8.0 업데이트 1 이상을 실행해야 합니다.

네트워킹 요구 사항:

- 네트워크를 공개적으로 사용할 수 없는 경우 vCenter Server 시스템과 Okta 서버 사이에 네트워크 터널을 생성한 다음 공개적으로 액세스할 수 있는 적절한 URL을 기본 URI로 사용해야 합니다.

절차

1 Okta에서 OpenID Connect 애플리케이션을 생성하고 OpenID Connect 애플리케이션에 그룹 및 사용자를 할당합니다.

   OpenID Connect 애플리케이션을 생성하고 그룹 및 사용자를 할당하려면 https://kb.vmware.com/s/article/90835에서 VMware 기술 자료 문서를 참조하십시오. "OpenID Connect 애플리케이션 생성" 섹션의 단계를 따르십시오. Okta OpenID Connect 애플리케이션을 생성한 후 다음 단계에서 vCenter Server ID 제공자를 구성할 때 사용할 수 있도록 Okta OpenID Connect 애플리케이션에서 파일로 다음 정보를 복사합니다.

   - 클라이언트 식별자
   - 클라이언트 암호(vSphere Client에서 공유 암호로 표시됨)
   - Active Directory 도메인 정보 또는 Active Directory를 실행하지 않는 경우 Okta 도메인 정보

2 vCenter Server에서 ID 제공자를 생성하려면 다음을 수행합니다.

   a vSphere Client를 사용하여 vCenter Server에 관리자로 로그인합니다.

   b **홈 > 관리 > Single Sign On > 구성**으로 이동합니다.

   c **제공자 변경**을 클릭하고 **Okta**를 선택합니다.

      기본 ID 제공자 구성 마법사가 열립니다.

   d **사전 요구 사항** 패널에서 Okta 및 vCenter Server 요구 사항을 검토합니다.

e **사전 검사 실행**을 클릭합니다.

사전 검사에서 오류가 발견되면 **세부 정보 보기**를 클릭하고 표시된 대로 오류를 해결하는 단계를 수행합니다.

f 사전 검사가 통과되면 확인란을 클릭하고 **다음**을 클릭합니다.

g **디렉토리 정보** 패널에서 다음 정보를 입력합니다.

- 디렉토리 이름: Okta에서 푸시된 사용자 및 그룹을 저장하는 vCenter Server에 생성할 로컬 디렉토리의 이름입니다. 예: **`vcenter-okta-directory`**.
- 도메인 이름: vCenter Server와 동기화하려는 Okta 사용자 및 그룹이 포함된 Okta 도메인 이름을 입력합니다.

  Okta 도메인 이름을 입력한 후 더하기 아이콘(+)을 클릭하여 추가합니다. 여러 도메인 이름을 입력하는 경우 기본 도메인을 지정합니다.

h **다음**을 클릭합니다.

i **OpenID Connect** 패널에서 다음 정보를 입력합니다.

- 리디렉션 URI: 자동으로 채워집니다. OpenID Connect 애플리케이션을 생성하는 데 사용할 리디렉션 URI를 Okta 관리자에게 제공합니다.
- ID 제공자 이름: Okta로 자동 입력됩니다.
- 클라이언트 식별자: 1단계에서 Okta에서 OpenID Connect 애플리케이션을 생성할 때 확보합니다. (Okta는 클라이언트 식별자를 클라이언트 ID라고 합니다.)
- 공유 암호: 1단계에서 Okta에서 OpenID Connect 애플리케이션을 생성할 때 확보합니다. (Okta는 공유 암호를 클라이언트 암호라고 합니다.)
- OpenID 주소: https://*Okta domain space*/oauth2/default/.well-known/openid-configuration 형식을 사용합니다.

  예를 들어 Okta 도메인 공간이 example.okta.com인 경우 OpenID 주소는 `https://example.okta.com/oauth2/default/.well-known/openid-configuration`입니다.

  자세한 내용은 https://developer.okta.com/docs/reference/api/oidc/#well-known-openid-configuration의 내용을 참조하십시오.

j **다음**을 클릭합니다.

k 정보를 검토하고 **마침**을 클릭합니다.

vCenter Server는 Okta ID 제공자를 생성하고 구성 정보를 표시합니다.

l 필요한 경우 아래로 스크롤하여 리디렉션 URI에 대한 **복사** 아이콘을 클릭하고 파일에 저장합니다.

Okta OpenID Connect 애플리케이션에서 리디렉션 URI를 사용합니다.

m 테넌트 URL에 대한 **복사** 아이콘을 클릭하고 파일에 저장합니다.

참고 네트워크를 공개적으로 사용할 수 없는 경우 vCenter Server 시스템과 Okta 서버 사이에 네트워크 터널을 생성해야 합니다. 네트워크 터널을 생성한 후 공개적으로 액세스할 수 있는 적절한 URL을 기본 URI로 사용합니다.

n **사용자 프로비저닝**에서 **생성**을 클릭하여 비밀 토큰을 생성하고 드롭다운에서 토큰 수명 기간을 선택한 다음, **클립보드에 복사**를 클릭합니다. 토큰을 안전한 위치에 저장합니다.

Okta SCIM 2.0 애플리케이션에서 테넌트 URL 및 토큰을 사용합니다. Okta SCIM 2.0 애플리케이션은 토큰을 사용하여 Okta 사용자 및 그룹을 VMware Identity Services에 동기화합니다. 이 정보는 Okta 사용자 및 그룹을 Okta에서 vCenter Server로 푸시하는 데 필요합니다.

3 VMware 기술 자료 문서(https://kb.vmware.com/s/article/90835)로 돌아가서 Okta 리디렉션 URI를 업데이트합니다.

"Okta 리디렉션 URI 업데이트" 섹션의 단계를 따릅니다.

4 SCIM 2.0 애플리케이션을 생성하려면 VMware 기술 자료 문서(https://kb.vmware.com/s/article/90835)를 계속 참조하십시오.

"SCIM 2.0 애플리케이션 생성 및 사용자 및 그룹을 vCenter Server에 푸시" 섹션의 단계를 따릅니다.

기술 자료 문서에 설명된 대로 SCIM 2.0 애플리케이션 생성이 완료되면 다음 단계를 계속 진행합니다.

5 Okta 인증을 위해 vCenter Server를 구성합니다.

Okta 사용자를 vCenter Server 그룹에 할당하거나 Okta 사용자에게 인벤토리 수준 및 글로벌 사용 권한을 할당할 수 있습니다. 로그인에 필요한 최소 사용 권한은 읽기 전용 입니다.

Okta 사용자를 그룹에 할당하려면 vCenter Single Sign-On 그룹에 멤버 추가 항목을 참조하십시오. Okta 사용자에게 인벤토리 수준 및 글로벌 사용 권한을 할당하려면 "vSphere 보안" 설명서에서 vCenter Server 구성 요소에 대한 사용 권한 관리에 대한 항목을 참조하십시오.

6 Okta 사용자로 vCenter Server에 로그인되는지 확인합니다.

Microsoft Entra ID에 대한 vCenter Server ID 제공자 페더레이션 구성

vSphere 8.0 업데이트 2 이상을 설치하거나 이 버전으로 업그레이드한 후 Microsoft Entra ID(이전 이름: Azure AD)에 대한 vCenter Server ID 제공자 페더레이션을 외부 ID 제공자로 구성할 수 있습니다.

vCenter Server는 구성된 외부 ID 제공자(하나의 소스)와 vsphere.local ID 소스(로컬 소스)를 하나만 지원합니다. 외부 ID 제공자를 여러 개 사용할 수 없습니다. vCenter Server ID 제공자 페더레이션은 OIDC(OpenID Connect)를 사용하여 사용자가 vCenter Server에 로그인되도록 합니다.

vCenter Server에서 전역 또는 개체 사용 권한을 통해 Microsoft Entra ID 그룹 및 사용자를 사용하여 권한을 구성할 수 있습니다. 사용 권한 추가에 대한 자세한 내용은 "vSphere 보안" 설명서를 참조하십시오.

구성 워크스루에 대한 자세한 내용은 다음 비디오를 참조하십시오.

vCenter 인증: AzureAD/Entra ID 통합 | vSphere 8 업데이트 2

사전 요구 사항

Microsoft Entra ID 요구 사항:

- Microsoft의 고객이며 Microsoft Entra ID 계정이 있습니다.

Microsoft Entra ID 연결 요구 사항:

- OpenID Connect를 로그인 방법으로 사용하여 엔터프라이즈(비갤러리) 애플리케이션을 생성했습니다.
- 권한 부여 코드, 새로 고침 토큰 및 리소스 소유자 암호를 생성된 애플리케이션에 권한 부여 유형으로 추가합니다.
- 사용자 및 그룹 동기화의 경우 OAuth 2.0 Bearer 토큰을 사용하여 Microsoft Entra ID에서 SCIM 2.0 프로비저닝을 위한 VMware Identity Services Gallery 애플리케이션을 구성해야 합니다.

vCenter Server 요구 사항:

- vSphere 8.0 업데이트 2 이상, VMware Identity Services가 활성화된 경우(기본적으로 활성화됨).
- Microsoft Entra ID 소스를 생성하려는 vCenter Server에서 VMware Identity Services가 활성화되었는지 확인합니다.
- ID 제공자의 사용자 및 그룹이 vCenter Server에 프로비저닝됩니다.

vSphere 권한 요구 사항:

- 페더레이션 인증에 필요한 vCenter Server ID 제공자를 생성, 업데이트 또는 삭제하려면 **VcIdentityProviders.Manage** 권한이 있어야 합니다. 사용자가 ID 제공자 구성 정보를 볼 수만 있도록 제한하려면 **VcIdentityProviders.Read** 권한을 할당합니다.

고급 연결 모드 요구 사항:

- 고급 연결 모드 구성에서 Microsoft Entra ID에 대한 vCenter Server ID 제공자 페더레이션을 구성할 수 있습니다. 고급 연결 모드 구성에서 Microsoft Entra ID를 구성하는 경우 단일 vCenter Server 시스템에서 VMware Identity Services를 사용하도록 Microsoft Entra ID 제공자를 구성합니다. 예를 들어 고급 연결 모드 구성이 두 개의 vCenter Server 시스템으로 구성된 경우 하나의 vCenter Server와 해당 VMware Identity Services 인스턴스만 Microsoft Entra ID 서버와 통신하는 데 사용됩니다. 이 vCenter Server 시스템을 사용할 수 없게 되면 ELM 구성의 다른 vCenter Server에서 VMware Identity Services를 구성하여 Microsoft Entra ID 서버와 상호 작용할 수 있습니다. 자세한 내용은 고급 연결 모드 구성의 외부 ID 제공자에 대한 활성화 프로세스의 내용을 참조하십시오.
- Microsoft Entra ID를 외부 ID 제공자로 구성할 때 고급 연결 모드 구성의 모든 vCenter Server 시스템은 vSphere 8.0 업데이트 2 이상을 실행해야 합니다.

네트워킹 요구 사항:

- 네트워크를 공개적으로 사용할 수 없는 경우 vCenter Server 시스템과 Microsoft Entra ID 서버 사이에 네트워크 터널을 생성한 다음, 공개적으로 액세스할 수 있는 적절한 URL을 기본 URI로 사용해야 합니다.

절차

1 Microsoft Entra ID에서 OpenID Connect 애플리케이션을 생성하고 OpenID Connect 애플리케이션에 그룹 및 사용자를 할당합니다.

OpenID Connect 애플리케이션을 생성하고 그룹 및 사용자를 할당하려면 https://kb.vmware.com/s/article/94182에서 VMware 기술 자료 문서를 참조하십시오. "OpenID Connect 애플리케이션 생성" 섹션의 단계를 따르십시오. OpenID Connect 애플리케이션을 생성한 후 다음 단계에서 vCenter Server ID 제공자를 구성할 때 사용할 수 있도록 Microsoft Entra ID OpenID Connect 애플리케이션의 다음 정보를 파일에 복사합니다.

- 클라이언트 식별자
- 클라이언트 암호(vSphere Client에서 공유 암호로 표시됨).
- Active Directory 도메인 정보 또는 Microsoft Entra ID 도메인 정보(Active Directory를 실행하지 않는 경우).

2 vCenter Server에서 ID 제공자를 생성하려면 다음을 수행합니다.

a vSphere Client를 사용하여 vCenter Server에 관리자로 로그인합니다.

b **홈 > 관리 > Single Sign On > 구성**으로 이동합니다.

c **제공자 변경**을 클릭하고 **Microsoft Entra ID**를 선택합니다.

기본 ID 제공자 구성 마법사가 열립니다.

d **사전 요구 사항** 패널에서 Microsoft Entra ID 및 vCenter Server 요구 사항을 검토합니다.

e **사전 검사 실행**을 클릭합니다.

사전 검사에서 오류가 발견되면 **세부 정보 보기**를 클릭하고 표시된 대로 오류를 해결하는 단계를 수행합니다.

f 사전 검사가 통과되면 확인란을 클릭하고 **다음**을 클릭합니다.

g **디렉토리 정보** 패널에서 다음 정보를 입력합니다.

- 디렉토리 이름: Microsoft Entra ID에서 푸시된 사용자 및 그룹을 저장하는 vCenter Server에 생성할 로컬 디렉토리의 이름입니다. 예: **`vcenter-entraid-directory`**.
- 도메인 이름: vCenter Server와 동기화하려는 Microsoft Entra ID 사용자 및 그룹이 포함된 Microsoft Entra ID 도메인 이름을 입력합니다.

  Microsoft Entra ID 도메인 이름을 입력한 후 더하기 아이콘(+)을 클릭하여 추가합니다. 여러 도메인 이름을 입력하는 경우 기본 도메인을 지정합니다.

h **다음**을 클릭합니다.

i **OpenID Connect** 패널에서 다음 정보를 입력합니다.

- 리디렉션 URI: 자동으로 채워집니다. OpenID Connect 애플리케이션을 생성하는 데 사용할 리디렉션 UI를 Microsoft Entra ID 관리자에게 제공합니다.
- ID 제공자 이름: Microsoft Entra ID로 자동 입력됩니다.
- 클라이언트 식별자: 1단계에서 Microsoft Entra ID에서 OpenID Connect 애플리케이션을 생성할 때 확보합니다. (Microsoft Entra ID는 클라이언트 식별자를 클라이언트 ID라고 합니다.)
- 공유 암호: 1단계에서 Microsoft Entra ID에서 OpenID Connect 애플리케이션을 생성할 때 확보합니다. (Microsoft Entra ID는 공유 암호를 클라이언트 암호라고 합니다.)
- OpenID 주소: https://*Microsoft Entra ID domain space*/oauth2/default/.well-known/openid-configuration 형식을 사용합니다.

  예를 들어 Microsoft Entra ID 도메인 공간이 example.EntraID.com인 경우 OpenID 주소는 `https://example.EntraID.com/oauth2/default/.well-known/openid-configuration` 입니다.

j **다음**을 클릭합니다.

k 정보를 검토하고 **마침**을 클릭합니다.

vCenter Server는 Microsoft Entra ID라는 ID 제공자를 생성하고 구성 정보를 표시합니다.

l 필요한 경우 아래로 스크롤하여 리디렉션 URI에 대한 **복사** 아이콘을 클릭하고 파일에 저장합니다.

Microsoft Entra ID OpenID Connect 애플리케이션에서 리디렉션 URI를 사용합니다.

m 테넌트 URL에 대한 **복사** 아이콘을 클릭하고 파일에 저장합니다.

참고 네트워크를 공개적으로 사용할 수 없는 경우 vCenter Server 시스템과 Microsoft Entra ID 서버 사이에 네트워크 터널을 생성해야 합니다. 네트워크 터널을 생성한 후 공개적으로 액세스할 수 있는 적절한 URL을 기본 URI로 사용합니다.

n **사용자 프로비저닝**에서 **생성**을 클릭하여 비밀 토큰을 생성하고 드롭다운에서 토큰 수명 기간을 선택한 다음, **클립보드에 복사**를 클릭합니다. 토큰을 안전한 위치에 저장합니다.

Microsoft Entra ID SCIM 2.0 애플리케이션에서 테넌트 URL 및 토큰을 사용합니다. Microsoft Entra ID SCIM 2.0 애플리케이션은 토큰을 사용하여 Microsoft Entra ID 사용자 및 그룹을 VMware Identity Services로 동기화합니다. 이 정보는 Microsoft Entra ID 사용자 및 그룹을 Microsoft Entra ID에서 vCenter Server로 푸시하는 데 필요합니다.

3 VMware 기술 자료 문서(https://kb.vmware.com/s/article/94182)로 Microsoft Entra ID 리디렉션 URI를 업데이트합니다.

"Azure AD 리디렉션 URI 업데이트" 섹션의 단계를 따릅니다.

4 SCIM 2.0 애플리케이션을 생성하려면 VMware 기술 자료 문서(https://kb.vmware.com/s/article/94182)를 계속 참조하십시오.

"SCIM 2.0 애플리케이션 생성 및 사용자 및 그룹을 vCenter Server에 푸시" 섹션의 단계를 따릅니다.

기술 자료 문서에 설명된 대로 SCIM 2.0 애플리케이션 생성이 완료되면 다음 단계를 계속 진행합니다.

5 Microsoft Entra ID 인증을 위해 vCenter Server에서 그룹 멤버 자격을 구성합니다.

Microsoft Entra ID 사용자가 vCenter Server에 로그인하려면 먼저 그룹 멤버 자격을 구성해야 합니다.

a vSphere Client에서 로컬 관리자로 로그인한 상태에서 **관리 > Single Sign On > 사용자 및 그룹**으로 이동합니다.

b **그룹** 탭을 클릭합니다.

c **관리자** 그룹을 클릭하고 **멤버 추가**를 클릭합니다.

d 드롭다운 메뉴에서 추가하려는 Microsoft Entra ID 그룹의 도메인 이름을 선택합니다.

e 드롭다운 메뉴 아래의 텍스트 상자에 추가하려는 Microsoft Entra ID 그룹의 처음 몇 자를 입력한 다음, 드롭다운 선택 항목이 나타날 때까지 기다립니다.

f Microsoft Entra ID 그룹을 선택하고 관리자 그룹에 추가합니다.

g **저장**을 클릭합니다.

6 Microsoft Entra ID 사용자로 vCenter Server에 로그인되는지 확인합니다.

7 Microsoft Entra ID 사용자에게 인벤토리 수준 및 글로벌 사용 권한을 할당하려면 "vSphere 보안" 설명서에서 vCenter Server 구성 요소에 대한 사용 권한 관리에 대한 항목을 참조하십시오.

PingFederate에 대한 vCenter Server ID 제공자 구성

vSphere 8.0 업데이트 1을 설치하거나 이 버전으로 업그레이드한 후 PingFederate에 대한 vCenter Server ID 제공자 페더레이션을 외부 ID 제공자로 구성할 수 있습니다.

PingFederate에 대한 vCenter Server ID 제공자를 구성하는 개략적인 단계

PingFederate에 대해 vCenter Server를 구성하려면 다음과 같은 개략적인 단계를 수행해야 합니다.

1 PingFederate에서 vCenter Server/VMware Identity Services 특정 구성(PingFederate 워크플로의 범위 및 공통 구성 포함)을 생성합니다.

2 PingFederate에서 암호 부여 흐름 구성 및 인증 코드 흐름 구성을 비롯한 글로벌 항목을 생성합니다.

3 PingFederate에서 SCIM Provisioner를 설치합니다.

4 vCenter Server에서 PingFederate ID 제공자를 생성합니다.

5 PingFederate에서 SCIM 애플리케이션(SP 연결)을 생성합니다.

6 vCenter Server에서 PingFederate 사용자에게 권한을 부여합니다.

참고 이 설명서의 지침은 PingFederate 서버에 대한 일반적인 설정을 생성합니다. 사용 환경은 다를 수 있으며, 따라서 다른 선택을 할 수도 있습니다.

PingFederate에 대한 vCenter Server ID 제공자를 구성하기 위한 사전 요구 사항

PingFederate 요구 사항:

- 온-프레미스에 PingFederate 서버를 설치했습니다.
- PingFederate ID 제공자를 구성하는 vCenter Server에서 신뢰할 수 있는 루트 인증서를 확보하여 PingFederate 서버로 가져와야 합니다.
- 필요한 경우, PingFederate SSL 인증서가 자체 서명된 경우(즉, 잘 알려진 공용 CA(인증 기관)에서 발급되지 않은 경우) PingFederate SSL 인증서 또는 인증서 체인을 vCenter Server로 가져와야 할 수도 있습니다. 잘 알려진 CA(인증 기관)에서 PingFederate SSL 인증서 또는 체인의 인증서 중 하나가 발급된 경우에는 vCenter Server에서 해당 인증서가 자동으로 신뢰되므로 가져올 필요가 없습니다. PingFederate 서버 SSL 인증서에 대해 하나 이상의 중간 서명 기관을 사용하는 경우에는 전체 인증서 체인을 포함합니다.

  PingFederate SSL 인증서를 내보내려면 PingFederate 관리 콘솔에서 **보안 > SSL 서버 인증서** 이동한 후 기본 인증서를 선택하고 **작업 선택** 드롭다운에서 **내보내기**를 선택합니다.

  ID 제공자 구성 워크플로의 일부로 **OpenID Connect** 패널에서 vSphere Client를 사용하여 PingFederate SSL 인증서를 가져옵니다.
- OIDC 로그인을 수행하고 사용자 및 그룹 권한을 관리하려면 다음 PingFederate 애플리케이션을 생성해야 합니다.
  - OpenID Connect를 로그온 방법으로 사용하는 PingFederate 네이티브 애플리케이션. 네이티브 애플리케이션에는 인증 코드, 새로 고침 토큰 및 리소스 소유자 암호의 권한 부여 유형이 포함되어야 합니다.
  - PingFederate 서버와 vCenter Server 간에 사용자 및 그룹 동기화를 수행하기 위한 OAuth 2.0 Bearer 토큰이 있는 SCIM(System for Cross-domain Identity Management) 2.0 애플리케이션(PingFederate에서는 SP 연결이라고 함).
- vCenter Server와 공유하려는 PingFederate 사용자 및 그룹을 식별했습니다. 이 공유는 SCIM 작업입니다(OIDC 작업이 아님).

PingFederate 연결 요구 사항:

- vCenter Server는 PingFederate 검색 끝점, 권한 부여, 토큰, 로그아웃, JWKS 및 검색 끝점 메타데이터에 보급된 기타 끝점에 연결할 수 있어야 합니다.
- PingFederate는 SCIM 프로비저닝을 위해 사용자 및 그룹 데이터를 보내기 위해 vCenter Server와 연결할 수 있어야 합니다.

vCenter Server 요구 사항:

- vSphere 8.0 업데이트 3
- PingFederate ID 소스를 생성하려는 vCenter Server에서 VMware Identity Services가 활성화되었는지 확인합니다.

참고 vSphere 8.0 업데이트 1 이상으로 업그레이드하거나 설치하는 경우 VMware ID 서버가 기본적으로 활성화됩니다. vCenter Server 관리 인터페이스를 사용하여 VMware Identity Services의 상태를 확인할 수 있습니다. VMware Identity Services 중지 및 시작의 내용을 참조하십시오.

vSphere 권한 요구 사항:

- 페더레이션 인증에 필요한 vCenter Server ID 제공자를 생성, 업데이트 또는 삭제하려면 **VcIdentityProviders.Manage** 권한이 있어야 합니다. 사용자가 ID 제공자 구성 정보만 보도록 제한하려면 **VcIdentityProviders.Read** 권한을 할당합니다.

고급 연결 모드 요구 사항:

- 고급 연결 모드 구성에서 PingFederate에 대한 vCenter Server ID 제공자 페더레이션을 구성할 수 있습니다. 고급 연결 모드 구성에서 PingFederate를 구성하는 경우 단일 vCenter Server시스템에서 VMware Identity Services를 사용하도록 PingFederate ID 제공자를 구성합니다. 예를 들어 고급 연결 모드 구성이 두 개의 vCenter Server 시스템으로 구성된 경우 하나의 vCenter Server와 해당 VMware Identity Services 인스턴스만 PingFederate 서버와 통신하는 데 사용됩니다. 이 vCenter Server 시스템을 사용할 수 없게 되면 ELM 구성의 다른 vCenter Server에서 VMware Identity Services를 구성하여 PingFederate 서버와 상호 작용할 수 있습니다. 자세한 내용은 고급 연결 모드 구성의 외부 ID 제공자에 대한 활성화 프로세스의 내용을 참조하십시오.
- PingFederate를 외부 ID 제공자로 구성할 때 고급 연결 모드 구성의 모든 vCenter Server 시스템은 vSphere 8.0 업데이트 3 이상을 실행해야 합니다.

다음으로 읽을 항목

절차

1 범위 생성

PingFederate는 범위 사용을 지원하여 액세스 권한을 제한하고 정의합니다.

2 PingFederate 워크플로에 대한 공통 구성 생성

PingFederate에 대한 일반 구성 생성에는 액세스 토큰 관리자, objectID 특성, OpenID Connect 정책 및 OAuth 클라이언트 애플리케이션 생성이 포함됩니다.

3 암호 부여 흐름 구성 생성

PingFederate가 vCenter Server를 인증하려면 암호 부여 흐름을 설정합니다.

4 인증 코드 흐름 구성 생성

PingFederate에서 인증 코드 흐름을 생성하려면 IdP 어댑터를 생성하고 구성해야 합니다.

5 SCIM 프로비저너 설치

토큰을 사용하여 PingFederate 사용자 및 그룹을 VMware Identity Services로 동기화하는 SCIM(System for Cross-domain Identity Management) 애플리케이션을 생성합니다.

6 PingFederate에 대한 vCenter Server ID 제공자 페더레이션 구성

vSphere 8.0 업데이트 1을 설치하거나 이 버전으로 업그레이드한 후 PingFederate에 대한 vCenter Server ID 제공자 페더레이션을 외부 ID 제공자로 구성할 수 있습니다.

7 SCIM 애플리케이션(SP 연결) 생성

vCenter Server에 푸시할 PingFederate 사용자 및 그룹을 지정할 수 있도록 SCIM(Cross-domain Identity Management) 2.0 애플리케이션용 시스템 생성이 필요합니다.

8 PingFederate 권한 부여에 대한 vCenter Server 구성

PingFederate 사용자를 vCenter Server 그룹에 할당하거나 PingFederate 사용자에게 인벤토리 수준 및 글로벌 사용 권한을 할당할 수 있습니다.

범위 생성

PingFederate는 범위 사용을 지원하여 액세스 권한을 제한하고 정의합니다.

사전 요구 사항

PingFederate에 대한 vCenter Server ID 제공자를 구성하기 위한 사전 요구 사항 항목을 검토하십시오.

PingFederate 관리자 콘솔에 관리자 계정으로 로그인합니다.

절차

1 **시스템 > OAuth 설정 > 범위 관리**로 이동합니다.

2 **일반 범위** 탭에서 다음 **범위 값**을 설명과 함께 추가합니다. 각 값과 설명을 입력한 후 **추가**를 클릭합니다.

- **openid**
- **profile**
- **이메일**

3 **개별 범위** 탭을 건너뜁니다.

4 **기본 범위** 탭에서 **기본 범위**에 대한 설명을 입력합니다.

설명은 필수입니다. **기본 범위 설명**이 비어 있으면 PingFederate는 다음 오류를 기록합니다.

요청한 범위가 유효하지 않거나 알 수 없거나 형식이 잘못되었거나 클라이언트가 요청할 수 있는 범위를 초과합니다.

5 **저장**을 클릭합니다.

다음에 수행할 작업

PingFederate 워크플로에 대한 공통 구성 생성 단계로 계속 진행합니다.

PingFederate 워크플로에 대한 공통 구성 생성

PingFederate에 대한 일반 구성 생성에는 액세스 토큰 관리자, objectID 특성, OpenID Connect 정책 및 OAuth 클라이언트 애플리케이션 생성이 포함됩니다.

사전 요구 사항

다음 작업을 완료합니다.

- 범위 생성

PingFederate 관리자 콘솔에 관리자 계정으로 로그인합니다.

절차

1 액세스 토큰 관리자를 생성합니다.

a **애플리케이션 > OAuth > 액세스 토큰 관리**로 이동합니다.

b **새 인스턴스 생성**을 클릭합니다.

c **유형** 탭에서 다음을 수행합니다.

- **인스턴스 이름**: 인스턴스 이름을 입력합니다. 예: vIDB 액세스 토큰 관리자.
- **인스턴스 ID**: 인스턴스 ID를 입력합니다. 예: vIDB.
- **유형**: **JSON Web Token**을 선택합니다.
- **상위 인스턴스**: 기본값인 **None**을 그대로 둡니다.

d **인스턴스 구성** 탭에서 다음을 수행합니다.

- **중앙 집중식 서명 키 사용**: 확인란을 선택합니다.

  이 확인란을 선택하지 않은 상태로 두면 PingFederate에서는 "활성 서명 인증서 키 ID"가 구성될 것으로 예상됩니다.

- **JWS 알고리즘**: 알고리즘을 선택합니다. 예: **RSA using SHA-256**.
- 화면 하단에서 **고급 필드 표시**를 클릭합니다.
  - **JWT ID 클레임 길이**: 0보다 큰 숫자를 추가합니다. 예: 24. 값을 입력하지 않으면 액세스 토큰에서 JTI 클레임이 생략됩니다.

e **다음**을 클릭합니다.

f **액세스 토큰 특성 계약** 탭에서 다음을 수행합니다.

- **계약 연장** 텍스트 상자에 Ping 액세스 토큰에서 생성할 다음 클레임을 추가합니다. 각 클레임을 입력한 후 **추가**를 클릭합니다.
  - **aud**
  - **iss**
  - **exp**
  - **iat**
  - **userName**
- **주체 특성 이름**: 감사 목적으로 사용할 클레임을 하나 선택합니다. 예: **iss**.

g **다음**을 두 번 클릭하여 **리소스 URI** 및 **액세스 제어** 탭을 건너뜁니다.

h **저장**을 클릭합니다.

2 objectGUID 특성을 추가합니다.

a **시스템 > 데이터스토어 > *내 데이터스토어* > LDAP 구성**으로 이동합니다.

b **LDAP 구성** 탭에서 아래쪽의 **고급**을 클릭합니다.

c **LDAP 바이너리 특성** 탭의 **바이너리 특성** 이름 필드에서 **objectGUID**를 사용하고 **추가**를 클릭합니다.

d **저장**을 클릭합니다.

3 OpenID Connect 정책을 생성합니다.

a **애플리케이션 > OAuth > OpenID Connect 정책 관리**로 이동합니다.

b **정책 추가**를 클릭합니다.

c **정책 관리** 탭에서 다음을 수행합니다.

- **정책 ID**: 정책 ID를 입력합니다. 예: OIDC.
- **이름**: 정책 이름을 입력합니다. 예: OIDC 정책
- **액세스 토큰 관리자**: 이전에 생성한 액세스 토큰 관리자를 선택합니다. 예: vIDB 액세스 토큰 관리자.

d **다음**을 클릭합니다.

e **특성 계약** 탭에서 다음을 수행합니다.

- **삭제**를 클릭하여 **sub**을 제외한 모든 특성을 제거합니다. 그렇지 않으면 나중에 **계약 이행** 탭의 값에 특성을 매핑해야 합니다.

f **다음**을 클릭한 후 **다음**을 다시 클릭하여**특성 범위** 탭을 건너뜁니다.

g **특성 소스 및 사용자 조회** 탭에서 **특성 소스 추가**를 클릭합니다.

다음 각 탭에 정보를 입력한 후 **다음**을 클릭하여 진행합니다.

- **데이터스토어**:
  - **특성 소스 ID**: 특성 소스 ID를 입력합니다. 예: vIDBLDAP.
  - **특성 소스 설명**: 설명을 입력합니다. 예: vIDBLDAP.
  - **활성 데이터스토어**: 드롭다운에서 Active Directory 또는 OpenLDAP 도메인 이름을 선택합니다.
- **LDAP 디렉토리 검색**:
  - **기본 DN**: 사용자 및 그룹을 찾을 기본 DN을 입력합니다.
  - **검색 범위**: 기본값인 **하위 트리**를 그대로 둡니다.
  - **검색에서 반환할 특성**: **<모든 특성 표시>**를 선택하고 **objectGUID**를 선택합니다.

    특성 추가를 클릭합니다.
- **LDAP 바이너리 특성 인코딩 유형**:
  - **ObjectGUID**: **특성 인코딩 유형**으로 **16진수**를 선택합니다.
- **LDAP 필터**:
  - **필터**: 필터를 입력합니다. 예: **`userPrincipalName=${userName}`**.

h **요약** 페이지에서 **완료**를 클릭합니다.

i **다음**을 클릭하여 계속 진행하고 **계약 이행** 탭에서 ID 토큰에 대한 **특성 계약**을 매핑합니다.

특성 계약	소스	값
sub	이전에 생성된 특성 소스 ID를 선택합니다. 이 설명서에서 사용된 예는 vIDBLDAP입니다.	objectGUID

j **다음**을 클릭한 후 **다음**을 다시 클릭하여 **보험 조건** 탭을 건너뜁니다.

k **저장**을 클릭합니다.

4 OAuth 클라이언트 애플리케이션을 생성합니다.

a **애플리케이션 > OAuth > 클라이언트**로 이동합니다.

b **클라이언트 추가**를 클릭합니다.

c **클라이언트에서** | **클라이언트** 페이지에서:

- **클라이언트 ID**: 클라이언트 ID를 입력합니다. 예: vIDB.

  참고 클라이언트 ID를 복사하고 저장하여 나중에 PingFederate에 대한 vCenter Server ID 제공자를 생성할 때 사용할 수 있도록 합니다.

- **이름**: 이름을 입력합니다. 예: vIDB.
- **클라이언트 인증**: **클라이언트 암호**를 선택합니다.
  - **클라이언트 암호**: 자신의 클라이언트 암호를 입력하거나 암호를 생성할 수 있습니다. 이 페이지에서 나가면 암호를 다시 볼 수 없습니다. 암호를 변경할 수 있는 옵션만 있습니다.

    참고 암호를 복사하고 저장하여 나중에 vCenter Server ID 제공자를 생성할 때 사용할 수 있도록 합니다.
- **리디렉션 URI**: 리디렉션 URI를 `https://vCenter_Server_FQDN:port/federation/t/CUSTOMER/auth/response/oauth2` 형태로 입력합니다.
  - **추가**를 클릭합니다.
- **허용되는 부여 유형**: **권한 부여 코드**, **새로 고침 토큰**, **클라이언트 자격 증명** 및 **리소스 소유자 암호 자격 증명**을 확인합니다.
- **기본 액세스 토큰 관리자**: 이전에 생성한 액세스 토큰 관리자를 선택합니다. 예를 들어 이 설명서에서 사용된 것은 vIDB 액세스 토큰 관리자입니다.
- OpenID Connect: **정책**의 경우 이전에 생성한 정책을 선택합니다. 예를 들어 이 설명서에서 사용된 것은 OIDC입니다.

d **저장**을 클릭합니다.

다음에 수행할 작업

암호 부여 흐름 구성 생성 단계로 계속 진행합니다.

암호 부여 흐름 구성 생성

PingFederate가 vCenter Server를 인증하려면 암호 부여 흐름을 설정합니다.

사전 요구 사항

다음 작업을 완료합니다.

- 범위 생성
- PingFederate 워크플로에 대한 공통 구성 생성

PingFederate 관리자 콘솔에 관리자 계정으로 로그인합니다.

절차

1 암호 자격 증명 유효성 검사기를 생성합니다.

a **시스템 > 데이터 및 자격 증명 저장소 > 암호 자격 증명 유효성 검사기**로 이동합니다.

b **새 인스턴스 생성**을 클릭합니다.

c **암호 자격 증명 유효성 검사기 | 새 인스턴스 생성** 페이지에서 각 탭에 대해 다음과 같이 정보를 입력한 후 **다음**을 클릭하여 진행합니다.

- **유형** 탭에서 다음을 수행합니다.
  - **인스턴스 이름**: 인스턴스 이름을 입력합니다. 예: vIDB Validator.
  - **인스턴스 ID**: 인스턴스 ID를 입력합니다. 예: vIDB.
  - **유형**: **LDAP 사용자 이름 암호 자격 증명 유효성 검사기**를 선택합니다.
- **인스턴스 구성** 탭에서 다음을 수행합니다.
  - **LDAP 데이터스토어**: 사용 중인 데이터스토어를 선택합니다.
  - **검색 기준**: 사용자 및 그룹을 찾을 기본 DN을 입력합니다.
  - **검색 필터**: 필터를 입력합니다. 예: **`userPrincipalName=${username}`**.
  - **검색 범위**: **하위 트리**를 선택합니다.
- **연장된 계약** 탭에서 다음을 수행합니다.
  - 기본적으로 다음이 추가됩니다.
    - DN
    - **이메일**
    - givenName
    - username

d **다음**을 클릭한 후 **저장**을 클릭합니다.

2 권한 부여 서버 설정에서 유효성 검사기를 매핑합니다.

a **시스템 > OAuth 설정 > 권한 부여 서버 설정**으로 이동합니다.

b **암호 자격 증명 유효성 검사기**에서 이전에 생성한 것을 선택합니다. 예를 들어 이 설명서에서는 vIDB Validator를 사용합니다.

c **저장**을 클릭합니다.

3 리소스 소유자 자격 증명 부여 매핑을 생성합니다.

a **인증 > OAuth > 리소스 소유자 자격 증명 매핑**으로 이동합니다.

b **리소스 소유자 자격 증명 부여 매핑** 창에서 다음을 수행합니다.

- **소스 암호 유효성 검사기 인스턴스**: 이전에 생성한 항목을 선택하고 **매핑 추가**를 클릭합니다.

c **리소스 소유자 자격 증명 부여 매핑 | 리소스 소유자 자격 증명 매핑** 페이지에서 **다음**을 클릭하여 **특성 소스 및 사용자 조회** 탭을 건너뜁니다.

d **계약 이행** 탭에서 다음을 수행합니다.

- **USER_KEY**의 경우 **암호 자격 증명 유효성 검사기**를 선택하고 **값**에 **username**을 선택합니다.

e **다음**을 클릭하여 **보험 조건** 탭을 건너뛴 후 **저장**을 클릭합니다.

4 액세스 토큰 매핑 생성 - 암호 자격 증명 유효성 검사기를 액세스 토큰 관리자에 매핑합니다.

이 매핑은 암호 부여 워크플로에 필요합니다. 매핑이 없으면 PingFederate는 다음 오류를 기록합니다.

선택한 클라이언트 및 인증 컨텍스트에 사용할 수 있는 액세스 토큰 관리자가 없습니다.

a **애플리케이션 > 액세스 토큰 매핑**으로 이동합니다.

- **컨텍스트**: 이전에 생성한 항목을 선택합니다. 예를 들어 이 설명서에서는 vIDB Validator를 사용합니다.
- **액세스 토큰 관리자**: 이전에 생성한 항목을 선택합니다. 예를 들어 이 설명서에서는 vIDB 액세스 토큰 관리자를 사용합니다.

b **매핑 추가**를 클릭합니다.

c **다음**을 클릭하여 **특성 소스 및 사용자 조회** 탭을 건너뜁니다.

d **계약 이행** 탭에서 다음 표를 사용합니다.

계약	소스	값
aud	**컨텍스트**	이전에 생성된 클라이언트 ID입니다. 예를 들어 이 설명서에 사용된 ID는 vIDB입니다.
exp	**매핑 없음**	-
iat	**표현식**	다음을 입력합니다. `@org.jose4j.jwt.NumericDate@now().getValue()`
iss	**표현식** (표시되지 않으면 https://docs.pingidentity.com/r/en-us/pingfederate-120/pf_enable_disable_express에서 PingFederate 설명서를 참조하십시오.)	다음을 입력합니다. `#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	**매핑 없음**	- 이 계약은 나중에 LDAP 필터에서 권한 부여 코드에 대한 OIDC 정책 워크플로에 사용됩니다. PingFederate 워크플로에는 필요하지 않습니다.

e **다음**을 클릭하여 **보험 조건** 탭을 건너뛴 후 **저장**을 클릭합니다.

다음에 수행할 작업

인증 코드 흐름 구성 생성 단계로 계속 진행합니다.

인증 코드 흐름 구성 생성

PingFederate에서 인증 코드 흐름을 생성하려면 IdP 어댑터를 생성하고 구성해야 합니다.

사전 요구 사항

다음 작업을 완료합니다.

- 범위 생성
- PingFederate 워크플로에 대한 공통 구성 생성
- 암호 부여 흐름 구성 생성

PingFederate 관리자 콘솔에 관리자 계정으로 로그인합니다.

절차

1 IdP 어댑터를 생성합니다.

a **인증 > 통합 > IdP 어댑터**로 이동합니다.

b **새 인스턴스 생성**을 생성합니다.

c **유형** 탭에서 다음을 수행합니다.

- **인스턴스 이름**: 이름(예: HTML 양식 Auth 어댑터)을 입력합니다.
- **인스턴스 ID**: ID(예: HTMLFormAuthAdapter)를 입력합니다.
- **유형**: HTML 양식 IdP 어댑터를 선택합니다.
- **상위 인스턴스**: **없음**을 선택합니다.

d **다음**을 클릭합니다.

e **IdP 어댑터** 탭에서 다음을 수행합니다.

암호 자격 증명 유효성 검사기 인스턴스에서 **'자격 증명 유효성 검사기'에 새 행을 추가합니다.**를 클릭한 후 유효성 검사기(이 설명서에서는 vIDB Validator가 사용됨)를 선택하고 **업데이트**를 클릭합니다.

f **IdP 어댑터** 탭에서 다음을 수행합니다.

- **영역**: **USER_KEY**를 선택합니다.

g **다음**을 클릭합니다.

h **다음**을 클릭하여**연장된 계약** 탭을 건너뜁니다.

i **어댑터 특성** 탭에서 다음을 수행합니다.

- **고유한 사용자 키 특성**: **username**을 선택하고 **Pseudonym**을 확인합니다.

j **다음**을 클릭하여 **어댑터 계약 매핑** 탭을 건너뛰고 **저장**을 클릭합니다.

2 IdP 어댑터 부여 매핑을 생성합니다.

a **인증 > OAuth > IdP 어댑터 부여 매핑**으로 이동합니다.

b **소스 어댑터 인스턴스**: 방금 생성한 어댑터 인스턴스를 선택하고 **매핑 추가**를 클릭합니다.

c **특성 소스 및 사용자 조회** 페이지에서 **특성 소스 추가**를 클릭합니다.

d 각 탭에 대해 다음과 같이 정보를 입력한 후 **다음**을 클릭하여 진행합니다.

- **데이터스토어** 탭에서 다음을 수행합니다.
  - **특성 소스 ID**: 영숫자 값이 있는 ID를 입력합니다.
  - **특성 소스 설명**. 설명을 입력합니다.
  - **활성 데이터스토어**: 사용 중인 활성 디렉토리를 선택합니다.
- **LDAP 디렉토리 검색** 탭에서 다음을 수행합니다.
  - **기본 DN**: 사용자 및 그룹을 찾을 기본 DN을 입력합니다.
  - **검색 범위**: 기본값인 **하위 트리**를 사용합니다.
  - **검색에서 반환할 특성**: **<모든 특성 표시>**를 선택한 다음, 로드되면 특성 목록에서 **userPrincipalName**을 선택합니다.

e **특성 추가**를 클릭한 후 **다음**을 클릭합니다.

f **LDAP 필터** 탭에서 다음을 수행합니다.

- **필터**: 필터를 입력합니다. 예: **`userPrincipalName=${username}`**.

g **다음**을 클릭한 후 **저장**을 클릭합니다.

h **IdP 어댑터 부여 매핑** | **IdP 어댑터 매핑** 페이지에서 IdP 부여 매핑 생성을 마칩니다.

계약 이행 조회 탭에서 다음 표를 사용합니다.

계약	소스	값
USER_KEY	이전에 생성한 소스를 선택합니다.	**주체 DN**
USER_NAME	이전에 생성한 소스를 선택합니다.	**userPrincipalName**

i **다음**을 클릭한 후 **저장**을 클릭합니다.

생성된 IdP 어댑터 부여 매핑은 **영구 부여 계약에 대한 '*어댑터 이름*'**으로 표시됩니다.

3 IdP 어댑터를 액세스 토큰 관리자에 매핑합니다.

a **애플리케이션 > OAuth > 액세스 토큰 매핑**으로 이동합니다.

- **컨텍스트**: **IdP 어댑터: *어댑터 이름***을 선택합니다.
- **액세스 토큰 관리자**: 이전에 생성된 액세스 토큰 관리자 인스턴스를 선택합니다. 예를 들어 이 설명서에서는 vIDB 액세스 토큰 관리자 입니다.

b **매핑 추가**를 클릭합니다.

이 매핑을 수행하지 않으면 PingFederate가 다음 로그 파일 메시지를 생성합니다.

선택할 수 있는 매핑된 인증 소스가 없습니다. 먼저 IdP 어댑터 또는 IdP 연결을 매핑하십시오.

c **특성 소스 및 사용자 조회** 탭을 건너뛰고 **계약 이행** 탭에서 다음 표를 사용합니다.

계약	소스	값
aud	매핑 없음	-
exp	매핑 없음	-
iat	매핑 없음	-
iss	매핑 없음	-
userName	어댑터	username

d **다음**을 클릭하여 **보험 조건** 탭을 건너뛴 후 **저장**을 클릭합니다.

다음에 수행할 작업

SCIM 프로비저너 설치 단계로 계속 진행합니다.

SCIM 프로비저너 설치

토큰을 사용하여 PingFederate 사용자 및 그룹을 VMware Identity Services로 동기화하는 SCIM(System for Cross-domain Identity Management) 애플리케이션을 생성합니다.

PingFederate 서버에서 SCIM 프로비저너를 설치하여 SCIM을 사용하여 사용자 및 그룹의 프로비저닝을 사용하도록 설정해야 합니다.

참고 기존 PingFederate 환경을 사용하는 경우 SCIM 프로비저너를 이미 설치했을 수 있습니다.

사전 요구 사항

다음 작업을 완료합니다.

- 범위 생성
- PingFederate 워크플로에 대한 공통 구성 생성
- 암호 부여 흐름 구성 생성
- 인증 코드 흐름 구성 생성

절차

1 https://support.pingidentity.com/s/marketplace-integration/a7i1W0000004IDNQA2/scim-provisioner에서 SCIM 프로비저너를 다운로드합니다.

PingIdentity 포털에 로그인해야 합니다.

2 `pf-scim-quickconnection-1.4.jar` 파일을 PingFederate 서버의 `/opt/out folder`에 마운트된 폴더에 복사합니다.

예를 들어 파일을 `/opt/out/instance/server/default/deploy` 폴더에 배치합니다.

3 `/opt/out/instance/bin/run.properties` 파일을 보고 이 설정이 있는지 확인합니다.
`pf.provisioner.mode=STANDALONE`

PingFederate 설명서에 따르면 다음과 같습니다.

독립형 - 이 서버는 UI 콘솔과 프로토콜 엔진(기본값)을 모두 실행하는 독립형 인스턴스입니다.

4 PingFederate 서버 인스턴스가 컨테이너 이미지로 실행 중이고 `run.properties` 파일을 업데이트한 경우 서버를 다시 시작해야 할 수 있습니다. 예:

a SSH를 사용하여 PingFederate 서버에 연결합니다.

b `/root/ping` 디렉토리로 변경합니다.

c 다음 명령을 실행합니다.

```
docker-compose down
docker-compose up
```

결과

SCIM 애플리케이션(SP 연결) 생성에서 사용자 프로비저닝을 구성할 때 SCIM 커넥터가 옵션으로 표시됩니다.

다음에 수행할 작업

PingFederate에 대한 vCenter Server ID 제공자 페더레이션 구성 단계로 계속 진행합니다.

PingFederate에 대한 vCenter Server ID 제공자 페더레이션 구성

vSphere 8.0 업데이트 1을 설치하거나 이 버전으로 업그레이드한 후 PingFederate에 대한 vCenter Server ID 제공자 페더레이션을 외부 ID 제공자로 구성할 수 있습니다.

vCenter Server는 구성된 외부 ID 제공자(하나의 소스)와 vsphere.local ID 소스(로컬 소스)를 하나만 지원합니다. 외부 ID 제공자를 여러 개 사용할 수 없습니다. vCenter Server ID 제공자 페더레이션은 OIDC(OpenID Connect)를 사용하여 사용자가 vCenter Server에 로그인되도록 합니다.

vCenter Server에서 전역 또는 개체 사용 권한을 통해 PingFederate 그룹 및 사용자를 사용하여 권한을 구성할 수 있습니다. 사용 권한 추가에 대한 자세한 내용은 "vSphere 보안" 설명서를 참조하십시오.

사전 요구 사항

다음 작업을 완료합니다.

- 범위 생성
- PingFederate 워크플로에 대한 공통 구성 생성
- 암호 부여 흐름 구성 생성
- 인증 코드 흐름 구성 생성
- SCIM 프로비저너 설치

PingFederate OpenID Connect 애플리케이션에서 다음 정보가 있는지 확인합니다.

- 클라이언트 식별자
- 클라이언트 암호(vSphere Client에서 공유 암호로 표시됨)
- Active Directory 도메인 정보 또는 Active Directory를 실행하지 않는 경우 PingFederate 도메인 정보

절차

1 vCenter Server에서 ID 제공자를 생성하려면 다음을 수행합니다.

   a vSphere Client를 사용하여 vCenter Server에 관리자로 로그인합니다.

   b **홈 > 관리 > Single Sign-On > 구성**으로 이동합니다.

   c **제공자 변경**을 클릭하고 **PingFederate**를 선택합니다.

   기본 ID 제공자 구성 마법사가 열립니다.

   d **사전 요구 사항** 패널에서 PingFederate 및 vCenter Server 및 기타 요구 사항을 검토합니다.

   e **사전 검사 실행**을 클릭합니다.

   사전 검사에서 오류가 발견되면 **세부 정보 보기**를 클릭하고 표시된 대로 오류를 해결하는 단계를 수행합니다.

   f 사전 검사가 통과되면 확인란을 클릭하고 **다음**을 클릭합니다.

   g **디렉토리 정보** 패널에서 다음 정보를 입력합니다.

      - 디렉토리 이름: PingFederate에서 푸시된 사용자 및 그룹을 저장하는 vCenter Server에 생성할 로컬 디렉토리의 이름입니다. 예: **`vcenter-PingFederate-directory`**.
      - 도메인 이름: vCenter Server와 동기화하려는 PingFederate 사용자 및 그룹이 포함된 PingFederate 도메인 이름을 입력합니다.

        PingFederate 도메인 이름을 입력한 후 더하기 아이콘(+)을 클릭하여 추가합니다. 여러 도메인 이름을 입력하는 경우 기본 도메인을 지정합니다.

   h **다음**을 클릭합니다.

i **OpenID Connect** 패널에서 다음 정보를 입력합니다.

- 리디렉션 URI: 자동으로 채워집니다. 이 리디렉션 UI는 PingFederate에서 OpenID Connect 애플리케이션을 생성하는 데 사용하는 것과 일치해야 합니다.
- ID 제공자 이름: PingFederate로 자동 입력됩니다.
- 클라이언트 식별자: OpenID Connect 애플리케이션을 생성할 때 확보됩니다. (PingFederate에서는 클라이언트 식별자를 클라이언트 ID라고 합니다.)
- 공유 암호: PingFederate에서 OpenID Connect 애플리케이션을 생성할 때 확보됩니다. (PingFederate에서는 공유 암호를 클라이언트 암호라고 합니다.)
- OpenID 주소: https://*PingFederate_domain_space*/idp/.well-known/openid-configuration 형식을 사용합니다.

  예를 들어, PingFederate 도메인 공간이 example.PingFederate.com인 경우 OpenID 주소는 `https://example.PingFederate.com/idp/.well-known/openid-config`입니다.
- SSL 인증서: 필요한 경우 PingFederate SSL 인증서 또는 인증서 체인(이 인증서가 잘 알려진 공용 CA(인증 기관)에서 발급되지 않은 경우)을 찾아 vCenter Server에 업로드합니다. PingFederate SSL 인증서를 내보내려면 관리 콘솔에서 **보안 > SSL 서버 인증서**로 이동하여 기본 인증서를 선택한 다음, **작업 선택** 드롭다운에서 **내보내기**를 선택합니다. 자세한 내용은 https://docs.pingidentity.com/r/en-us/pingfederate-111/nfv1585678806463에서 인증서 내보내기 항목을 참조하세요. vCenter Server 구성에 필요하지 않으므로 개인 키 없이 PingFederate SSL 인증서를 내보낼 수 있습니다.

j **다음**을 클릭합니다.

k 정보를 검토하고 **마침**을 클릭합니다.

vCenter Server는 PingFederate ID 제공자를 생성하고 구성 정보를 표시합니다.

2 **사용자 프로비저닝**에서 **생성**을 클릭하여 비밀 토큰을 생성하고 드롭다운에서 토큰 수명 기간을 선택한 다음, **클립보드에 복사**를 클릭합니다. 토큰을 안전한 위치에 저장합니다.

PingFederate SP 연결(SCIM 애플리케이션)을 생성할 때 토큰을 사용하여 PingFederate 사용자 및 그룹을 VMware Identity Services로 동기화합니다.

다음에 수행할 작업

SCIM 애플리케이션(SP 연결) 생성으로 계속 진행합니다.

SCIM 애플리케이션(SP 연결) 생성

vCenter Server에 푸시할 PingFederate 사용자 및 그룹을 지정할 수 있도록 SCIM(Cross-domain Identity Management) 2.0 애플리케이션용 시스템 생성이 필요합니다.

사전 요구 사항

다음 작업을 완료합니다.

- 범위 생성
- PingFederate 워크플로에 대한 공통 구성 생성
- 암호 부여 흐름 구성 생성
- 인증 코드 흐름 구성 생성
- SCIM 프로비저너 설치
- PingFederate에 대한 vCenter Server ID 제공자 페더레이션 구성

절차

1 vCenter Server 신뢰할 수 있는 루트 인증서를 PingFederate 서버에 추가합니다.

시작하기 전에 vCenter Server에서 신뢰할 수 있는 루트 인증서를 내보냅니다. `/var/lib/vmware/vmca/root.cer`에 있는 vCenter Server의 파일 시스템에서 인증서를 가져올 수 있습니다. 또는 https://kb.vmware.com/s/article/2108294의 기술 자료 문서를 참조하십시오.

a PingFederate 관리자 콘솔에 관리자 계정으로 로그인합니다.

b **보안 > 인증서 및 키 관리**로 이동합니다.

c **신뢰할 수 있는 CA**를 선택한 다음, **가져오기**를 클릭하여 vCenter Server의 SSL 인증서를 추가합니다.

d PingFederate 서버 인스턴스가 컨테이너 이미지로 실행 중인 경우 인증서를 신뢰 저장소에 추가하려면 서버를 다시 시작해야 할 수도 있습니다. 예:

1 SSH를 사용하여 PingFederate 서버에 연결합니다.

2 `/root/ping` 디렉토리로 변경합니다.

3 다음 명령을 실행합니다.

```
docker-compose down
docker-compose up
```

2 SP 연결을 생성합니다.

a PingFederate 관리자 콘솔에 관리자 계정으로 로그인합니다.

b **애플리케이션 > 통합 > SP 연결**로 이동합니다.

c **연결 생성**을 클릭합니다.

d **이 연결에 템플릿 사용**을 선택하고 드롭다운에서 **SCIM 커넥터**를 선택합니다.

SCIM 커넥터 옵션이 드롭다운에 나타나지 않으면 SCIM 커넥터 `.jar` 파일을 올바른 폴더(PingFederate 서버의 `/opt/out` 폴더)에 배치했는지 확인합니다.

e **다음**을 클릭합니다.

f **아웃바운드 프로비저닝**만 선택하고 **다음**을 클릭합니다.

g **일반 정보** 탭에서 다음을 수행합니다.

- **파트너의 엔티티 ID(연결 ID)**: **SCIM 커넥터**를 원하는 이름으로 업데이트합니다.
- **연결 이름**: 이름을 입력합니다.
- **기본 URL**: PingFederate 외부 ID 제공자를 구성하는 vCenter Server의 HTTPS 주소를 입력합니다(예: **`https://vcenter1.example.com`**).

h **다음**을 클릭합니다.

i **프로비저닝 구성**을 클릭합니다.

대상 탭에서 다음을 수행합니다.

- **SCIM URL**: 사용자 그룹 끝점을 입력합니다.

  vCenter Server **구성** 페이지의 **사용자 프로비저닝**에서 가져온 테넌트 URL입니다. 예: **`https://vcenter1.example.com/usergroup/t/CUSTOMER/scim/v2`**
- **인증 방법**: 드롭다운에서 **OAuth 2 Bearer 토큰**을 선택합니다.
- **액세스 토큰**: vCenter Server에서 생성되었으며 이전에 저장했어야 하는 비밀 토큰을 붙여넣습니다. PingFederate에 대한 vCenter Server ID 제공자 페더레이션 구성의 2단계를 참조하십시오.
- **고유한 사용자 식별자**: 드롭다운에서 **userName**을 선택합니다.
- **필터 표현식**: 다음 표현식을 텍스트 상자에 복사합니다. **`externalId eq "%s"`**

j 나머지 기본 구성 설정 값을 수락하고 **다음**을 클릭합니다.

- **프로비저닝 옵션**: **사용자 생성**, **사용자 업데이트** 및 **사용자 사용 안 함/삭제**를 선택합니다.
- **사용자 작업 제거**: **사용 안 함**이 선택되었습니다.

  참고 **사용 안 함**을 선택한 경우 사용자가 Active Directory에서 삭제되면 VMware Identity Services에 자동으로 "사용 안 함"으로 표시되지 않습니다. 이는 예상되는 동작입니다.

  - Active Directory에서는 다음 프로비저닝 주기에서 사용자를 삭제하는 대신 사용자 속성이 "active"="false"가 됩니다.
  - 다음 프로비저닝 주기에 Active Directory에서 다른 사용자가 생성되거나 업데이트될 때까지 사용자는 VMware Identity Services에서 "사용 안 함"으로 표시되지 않습니다. 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-specified의 해결 방법을 따르십시오.
- **그룹 이름 소스**: **일반 이름**이 선택됩니다.

k **채널 관리** 탭에서 **생성**을 클릭합니다.

- **채널 정보** 탭에서 다음을 수행합니다.
  - **채널 이름**: 이름을 입력합니다.
  - **최대 스레드** 및 **시간 초과(초)** 기본값을 수락합니다.

l **다음**을 클릭합니다.

- **소스** 탭에서 다음을 수행합니다.
  - **활성 데이터스토어**: Active Directory 도메인을 선택합니다.

m **다음**을 클릭합니다.

- **소스 위치** 탭에서 다음을 수행합니다.
  - **기본 DN**: 사용자 및 그룹을 찾을 기본 DN을 입력합니다.
  - **사용자**: 환경에 맞게 사용자 지정합니다. 예:
    - **그룹 DN:** 사용하지 마십시오.
    - **필터**: `(|(objectClass=person)(objectClass=organizationalPerson)(objectClass=user))`를 입력합니다.
  - 그룹: 환경에 맞게 사용자 지정합니다. 예:
    - **그룹 DN**: 사용하지 마십시오.
    - **필터**: `(objectClass=group)`을 입력합니다.

n **다음**을 클릭합니다.

o **특성 매핑** 탭에서 기본값을 수락합니다.

p **다음**을 클릭합니다.

활성화 및 요약 탭에서 다음을 수행합니다.

- **채널 상태**: **활성**을 선택합니다.

q **완료**를 클릭합니다.

SP 연결이 생성되고 SP 연결 화면이 표시됩니다.

r **완료**를 클릭합니다.

s **아웃바운드 프로비저닝** 탭에서 **다음**을 클릭합니다.

t 요약을 검토한 다음, **저장**을 클릭합니다.

u 연결을 활성화하려면 **사용** 슬라이더를 전환합니다.

결과

이제 PingFederate는 구성된 데이터스토어의 사용자 및 그룹을 vCenter Server로 푸시합니다. 푸시가 발생할 때까지 잠시 기다려 주십시오. vSphere Client에서 푸시된 사용자 및 그룹을 볼 수 있습니다. **관리 > Single Sign-On > 사용자 및 그룹**으로 이동한 후 PingFederate 도메인을 선택합니다.

다음에 수행할 작업

PingFederate 권한 부여에 대한 vCenter Server 구성 단계로 계속 진행합니다.

PingFederate 권한 부여에 대한 vCenter Server 구성

PingFederate 사용자를 vCenter Server 그룹에 할당하거나 PingFederate 사용자에게 인벤토리 수준 및 글로벌 사용 권한을 할당할 수 있습니다.

PingFederate 사용자가 로그인하는 데 필요한 최소 사용 권한은 읽기 전용 입니다.

사전 요구 사항

다음 작업을 완료합니다.

- 범위 생성
- PingFederate 워크플로에 대한 공통 구성 생성
- 암호 부여 흐름 구성 생성
- 인증 코드 흐름 구성 생성
- SCIM 프로비저너 설치
- PingFederate에 대한 vCenter Server ID 제공자 페더레이션 구성
- SCIM 애플리케이션(SP 연결) 생성

절차

1. PingFederate 사용자를 그룹에 할당하려면 vCenter Single Sign-On 그룹에 멤버 추가 항목을 참조하십시오.
2. PingFederate 사용자에게 인벤토리 수준 및 글로벌 사용 권한을 할당하려면 "vSphere 보안" 설명서에서 vCenter Server 구성 요소에 대한 사용 권한 관리에 대한 항목을 참조하십시오.
3. PingFederate 사용자 사용 권한을 할당한 후 사용자가 로그인할 수 있는지 확인합니다.

VMware Single Sign-On 구성

vSphere 8.0 업데이트 3을 설치하거나 이 버전으로 업그레이드한 후 VMware Single Sign-On을 위해 vCenter Server 호스트를 구성할 수 있습니다. VMware Single Sign-On을 구성할 때 외부 ID 제공자를 사용하여 vCenter Server 호스트에 로그인합니다.

VMware Single Sign-On을 사용하면 고급 연결 모드가 아닌 구성에서 vCenter Server 호스트에 연결할 수 있습니다. 즉, 외부 ID 제공자를 구성하기만 하면 이 구성을 다른 vCenter Server 호스트에 대한 Single Sign-On에 활용할 수 있습니다.외부 ID 제공자가 구성된 vCenter Server 호스트는 다른 vCenter Server 호스트의 ID 제공자 역할을 합니다.

VMware Single Sign-On을 수행하도록 여러 vCenter Server 호스트를 구성할 수 있습니다. 이렇게 하려면 외부 ID 제공자로 구성된 vCenter Server 호스트를 가리키도록 각 vCenter Server 호스트를 구성해야 합니다.

VMware Single Sign-On 구성을 수행한 후에도 로컬 계정으로 vCenter Server 호스트에 로그인할 수 있습니다.

참고 VMware Single Sign-On은 고급 연결 모드에서 발생하는 것처럼 vCenter Server 호스트 간에 인벤토리를 공유하지 않습니다.

사전 요구 사항

VMware Single Sign-On 요구 사항:

- VMware Single Sign-On을 구성하는 vCenter Server는 vSphere 8.0 업데이트 3을 실행합니다.
- 연결하려는 vCenter Server 호스트는 vSphere 8.0 업데이트 1 이상을 실행합니다.
- 다음 외부 ID 제공자 중 하나를 구성했습니다.
  - Microsoft Entra ID
  - Okta
  - PingFederate
- 외부 ID 제공자가 구성된 vCenter Server 호스트의 신뢰할 수 있는 루트 인증서를 VMware Single Sign-On을 구성한 vCenter Server 호스트에 추가해야 합니다.

절차

1. 외부 ID 제공자가 구성된 vCenter Server 호스트에서 신뢰할 수 있는 루트 인증서를 다운로드합니다. 예를 들어 https://kb.vmware.com/s/article/2108294에서 VMware 기술 자료 문서를 참조하십시오.
2. 신뢰할 수 있는 루트 인증서를 VMware SSO를 구성 중인 vCenter Server 호스트에 업로드합니다.

   vSphere Client를 사용하여 신뢰할 수 있는 루트 인증서를 인증서 저장소에 추가의 내용을 참조하십시오.
3. vSphere Client를 사용하여 VMware SSO를 구성 중인 vCenter Server 호스트에 관리자로 로그인합니다.
4. **홈 > 관리 > Single Sign On > 구성**으로 이동합니다.
5. **제공자 변경**을 클릭하고 **VMware SSO**를 선택합니다.

   기본 ID 제공자 구성 마법사가 열립니다.
6. **사전 요구 사항** 패널에서 vCenter Server 요구 사항을 검토합니다.

7 **사전 검사 실행**을 클릭합니다.

사전 검사에서 오류가 발견되면 **세부 정보 보기**를 클릭하고 표시된 대로 오류를 해결하는 단계를 수행합니다.

8 사전 검사가 통과되면 확인란을 클릭하고 **다음**을 클릭합니다.

9 **OpenID Connect** 패널에서 다음 정보를 입력합니다.

- ID 제공자 이름: VMware SSO로 자동 입력됩니다.
- vCenter Server FQDN: 외부 ID 제공자가 구성된 vCenter Server 호스트의 FQDN을 입력합니다.
- 포트 번호: 기본값인 443을 그대로 사용하거나 사용하려는 포트로 변경합니다.
- 사용자 이름 및 암호: 외부 ID 제공자가 구성된 이 vCenter Server 호스트의 관리자 계정에 대한 사용자 이름과 암호를 입력합니다.

10 **다음**을 클릭합니다.

11 정보를 검토하고 **마침**을 클릭합니다.

vCenter Server는 VMware SSO 제공자를 생성하고 구성 정보를 표시합니다. 이 vCenter Server 호스트에는 이제 구성이 생성된 호스트와 동일한 외부 ID 제공자 구성이 포함됩니다. 예를 들어 두 호스트 간의 OpenID 구성을 비교해 보면 동일합니다.

12 권한 부여에 외부 ID 제공자를 사용하도록 이 vCenter Server를 구성합니다.

외부 ID 제공자 사용자를 vCenter Server 그룹에 할당하거나 사용자에게 인벤토리 수준 및 글로벌 사용 권한을 할당할 수 있습니다. 로그인에 필요한 최소 사용 권한은 읽기 전용 입니다.

외부 ID 제공자 사용자를 그룹에 할당하려면 vCenter Single Sign-On 그룹에 멤버 추가 항목을 참조하십시오. 사용자에게 인벤토리 수준 및 글로벌 사용 권한을 할당하려면 "vSphere 보안" 설명서에서 vCenter Server 구성 요소에 대한 사용 권한 관리에 대한 항목을 참조하십시오.

13 외부 ID 제공자 사용자로 이 vCenter Server 호스트에 로그인되는지 확인합니다.

vSphere Client를 시작하면 VMware vSphere 시작 화면이 **SSO로 로그인** 버튼과 함께 표시됩니다. 이 버튼을 클릭하면 외부 ID 제공자의 로그인 화면으로 리디렉션됩니다.

VMware Identity Services 관리

VMware Identity Services를 중지 및 시작하고, SCIM 토큰을 재생성하고, 삭제된 SCIM 사용자 및 그룹을 복원할 수 있습니다.

작업에 따라 vSphere Client 또는 외부 ID 제공자의 관리 콘솔을 사용합니다.

VMware Identity Services 중지 및 시작

Okta, Microsoft Entra ID(이전 명칭: Azure AD) 또는 PingFederate를 외부 ID 제공자로 구성하고 실행하려면 vCenter Server에서 VMware Identity Services를 시작해야 합니다. 기본적으로 를 설치하거나 vSphere 8.0 업데이트 1 이상으로 업그레이드하면 VMware Identity Services가 시작됩니다. vCenter Server 관리 인터페이스를 사용하여 VMware Identity Services를 관리합니다.

버전 8.0 업데이트 1부터 vSphere에는 Okta에 대한 인증을 지원하기 위한 VMware Identity Services가 포함됩니다. 버전 8.0 업데이트 2부터 VMware Identity Services는 Microsoft Entra ID에 대한 인증을 지원합니다. 버전 8.0 업데이트 3부터 VMware Identity Services는 PingFederate에 대한 인증을 지원합니다.

사전 요구 사항

vSphere 8.0 업데이트 1 이상을 설치하거나 이 버전으로 업그레이드하면 VMware Identity Services가 자동으로 시작됩니다. Okta, Microsoft Entra ID 또는 PingFederate를 외부 ID 제공자로 구성할 때 VMware Identity Services가 이미 실행 중이므로 이를 시작할 필요가 없습니다. VMware Identity Services를 시작하거나 중지하려면 사용자가 루트여야 합니다.

외부 ID 제공자는 단일 vCenter Server만 구성합니다. 이 vCenter Server는 VMware Identity Services의 인스턴스를 통해 ID 제공자와 통신합니다. 고급 연결 모드 구성의 다른 vCenter Server 시스템에도 VMware Identity Services가 실행되고 있지만 ID 제공자와 직접 통신하지는 않습니다.

절차

1. 웹 브라우저에서 vCenter Server 관리 인터페이스(https://*vcenter-IP-address-or-FQDN*:5480)로 이동합니다.
2. 루트로 로그인합니다.

   기본 루트 암호는 vCenter Server를 배포하는 중에 설정하는 암호입니다.
3. **서비스**를 선택합니다.
4. VMware Identity Services의 상태를 봅니다.
5. 서비스를 중지하거나 시작하려면 **VMware Identity Services**를 선택한 다음 **중지** 또는 **시작**을 클릭합니다.

   VMware Identity Services를 시작한 후 vCenter Server 재부팅이 필요하지 않습니다.

vCenter Server에서 SCIM 토큰 다시 생성

vCenter Server에서 외부 ID 제공자에 대한 SCIM(도메인 간 ID 관리를 위한 시스템) 토큰을 다시 생성할 수 있습니다.

다른 토큰을 생성하면 즉시 활성화되고 이전 토큰이 해지됩니다.

사전 요구 사항

vCenter Server에서 외부 ID 제공자를 생성했어야 합니다.

절차

1. vSphere Client를 사용하여 vCenter Server에 관리자로 로그인합니다.
2. 구성 UI로 이동합니다.
   a. **홈** 메뉴에서 **관리**를 선택합니다.
   b. **Single Sign-On**에서 **구성**을 클릭합니다.

3 **구성** 페이지의 **사용자 프로비저닝/비밀 토큰** 아래에서 **재생성**을 클릭하여 비밀 토큰을 다시 생성하고 드롭다운에서 토큰 수명을 선택한 다음 **클립보드에 복사**를 클릭합니다. 토큰을 안전한 위치에 저장합니다.

4 복사된 토큰을 사용하여 외부 ID 제공자 구성을 업데이트할 수 있습니다.

삭제된 SCIM 사용자 및 그룹 복원

vCenter Server의 SCIM 푸시 사용자 및 그룹이 외부 ID 제공자와 동기화되지 않으면 문제를 해결하기 위한 단계를 수행할 수 있습니다.

vCenter Server에서 삭제한 SCIM 푸시 사용자 또는 그룹을 복원하려는 경우 단순히 ID 제공자에서 사용자 또는 그룹을 푸시할 수는 없습니다. vCenter Server가 사용자 및 그룹 관리를 위해 SCIM(System for Cross-domain Identity Management)을 사용하는 방식 때문에 SCIM 2.0 애플리케이션 자체를 누락된 사용자 또는 그룹으로 업데이트해야 합니다.

절차

1 외부 IDP 관리 콘솔에 로그인합니다.

2 SCIM 2.0 애플리케이션으로 이동합니다.

3 삭제되었거나 누락된 사용자 또는 그룹을 할당합니다.

4 푸시된 그룹 또는 사용자를 연결 해제하려면 푸시된 그룹 또는 사용자를 삭제하기 위한 적절한 작업을 선택합니다.

5 그룹을 푸시하기 위한 적절한 작업을 선택합니다.

6 vCenter Server에서 외부 IDP가 그룹 또는 사용자를 동기화했는지 확인합니다.

vCenter Single Sign-On

외부 ID 제공자를 사용하지 않는 경우, 기본 제공 ID 제공자인 vCenter Single Sign-On의 기본 아키텍처와 이것이 설치 및 업그레이드에 미치는 영향을 이해해야 합니다.

vCenter Single Sign-On 구성 요소

vCenter Single Sign-On에는 STS(Security Token Service), 관리 서버, vCenter Lookup Service 및 VMware Directory Service(vmdir)가 포함됩니다. VMware 디렉토리 서비스도 인증서 관리에 사용됩니다.

설치하는 동안 다음 구성 요소가 vCenter Server 배포의 일부로 배포됩니다.

STS(Security Token Service)

STS 서비스는 SAML(Security Assertion Markup Language) 토큰을 발급합니다. 이러한 보안 토큰은 vCenter Server에서 지원하는 ID 소스 유형 중 하나로 사용자의 ID를 나타냅니다. SAML 토큰을 사용하면 vCenter Single Sign-On에 성공적으로 인증하는 대화형 사용자, 스크립트로 작성된 사용자 및 서비스 사용자(솔루션 사용자 포함)가 각 서비스에 대해 다시 인증하지 않고도 vCenter Single Sign-On이 지원하는 모든 vCenter 서비스를 사용할 수 있습니다.

vCenter Single Sign-On 서비스는 서명 인증서를 사용하여 모든 토큰을 서명하고, 토큰 서명 인증서를 디스크에 저장합니다. 서비스 자체의 인증서도 디스크에 저장됩니다.

관리 서버

관리 서버에서는 vCenter Single Sign-On에 대한 관리자 권한이 있는 사용자가 vCenter Single Sign-On 서버를 구성하고 vSphere Client에서 사용자 및 그룹을 관리할 수 있습니다. 처음에는 administrator@*your_domain_name* 사용자만 이 권한을 가지고 있습니다. vCenter Server를 설치할 때 vSphere 도메인을 변경할 수 있습니다. 도메인 이름을 Microsoft Active Directory 또는 OpenLDAP 도메인 이름으로 명명하지 마십시오.

VMware Directory Service(vmdir)

VMware Directory Service(vmdir)는 설치 중에 지정하는 도메인에 연결되며 각 vCenter Server 배포에 포함됩니다. 이 서비스는 포트 389에서 LDAP 디렉토리를 사용할 수 있도록 하는 다중 테넌트, 피어 복제 디렉토리 서비스입니다. 또한 SHA-512 해싱 알고리즘으로 보호되는 vCenter Single Sign-On 사용자 계정과 암호를 저장하고 관리합니다.

환경에 연결 모드로 구성된 여러 개의 vCenter Server 인스턴스가 포함되어 있으면 vmdir 인스턴스 하나의 vmdir 컨텐츠 업데이트가 다른 모든 vmdir 인스턴스에 전파됩니다.

VMware Directory Service는 vCenter Single Sign-On 정보 뿐만 아니라 인증서 정보도 저장합니다.

ID 관리 서비스

ID 소스 및 STS 인증 요청을 처리합니다.

vSphere와 함께 vCenter Single Sign-On 사용

사용자가 vSphere 구성 요소에 로그인하거나 vCenter Server 솔루션 사용자가 다른 vCenter Server 서비스에 액세스하면 vCenter Single Sign-On이 인증을 수행합니다. 사용자는 vCenter Single Sign-On에 인증되어야 하며 vSphere 개체와 상호 작용하는 데 필요한 권한을 갖고 있어야 합니다.

vCenter Single Sign-On은 솔루션 사용자와 기타 사용자를 모두 인증합니다.

- 솔루션 사용자는 vSphere 환경에서 서비스 집합을 나타냅니다. 설치할 때 VMCA는 기본적으로 각 솔루션 사용자에게 인증서를 할당합니다. 솔루션 사용자는 해당 인증서를 vCenter Single Sign-On에 인증하는 데 사용합니다. vCenter Single Sign-On은 솔루션 사용자에게 SAML 토큰을 제공하고 솔루션 사용자는 환경의 다른 서비스와 상호 작용할 수 있습니다.
- 다른 사용자가 환경에 로그인하면(예를 들어 vSphere Client에서), vCenter Single Sign-On에서 사용자 이름과 암호를 묻습니다. vCenter Single Sign-On이 해당 ID 소스에서 해당 자격 증명을 가진 사용자를 찾으면 사용자에게 SAML 토큰을 할당합니다. 이제 사용자는 다시 인증 과정을 거치지 않은 채 환경의 다른 서비스에 액세스할 수 있습니다.

  사용자가 어떤 개체를 볼 수 있고 어떤 작업을 수행할 수 있는지는 일반적으로 vCenter Server 사용 권한 설정에 따라 결정됩니다. vCenter Server 관리자는 vCenter Single Sign-On을 통해서가 아니라 vSphere Client의 **사용 권한** 인터페이스에서 이러한 사용 권한을 할당합니다. "vSphere 보안" 설명서를 참조하십시오.

vCenter Single Sign-On 및 vCenter Server 사용자

사용자는 로그인 페이지에 자격 증명을 입력하여 vCenter Single Sign-On에 대한 인증을 받습니다. vCenter Server에 연결한 후, 인증된 사용자는 역할에 따라 권한이 부여된 모든 vCenter Server 인스턴스 또는 vSphere 개체를 볼 수 있습니다. 추가 인증이 필요하지 않습니다.

설치 후 vCenter Single Sign-On 도메인의 관리자(기본적으로 administrator@vsphere.local)는 vCenter Single Sign-On과 vCenter Server 모두에 관리자로 액세스할 수 있습니다. 그런 다음 ID 소스를 추가하고, 기본 ID 소스를 설정하고, vCenter Single Sign-On 도메인의 사용자 및 그룹을 관리할 수 있습니다.

vCenter Single Sign-On에 인증이 가능한 모든 사용자는 암호를 재설정할 수 있습니다. vCenter Single Sign-On 암호 변경 의 내용을 참조하십시오. 더 이상 암호가 없는 사용자의 암호는 vCenter Single Sign-On 관리자만 재설정할 수 있습니다.

vCenter Single Sign-On 관리자

vCenter Single Sign-On 관리 인터페이스는 vSphere Client에서 액세스할 수 있습니다.

vCenter Single Sign-On을 구성하고 vCenter Single Sign-On 사용자 및 그룹을 관리하려면 administrator@vsphere.local 사용자나 vCenter Single Sign-On 관리자 그룹의 사용자가 vSphere Client에 로그인해야 합니다. 이러한 사용자는 인증 후 vSphere Client에서 vCenter Single Sign-On 관리 인터페이스에 액세스하여 ID 소스 및 기본 도메인을 관리하고, 암호 정책을 지정하고, 그 밖의 관리 작업을 수행할 수 있습니다.

참고 설치 시 다른 도메인을 지정한 경우에는 vCenter Single Sign-On 관리자의 기본 이름인 administrator@vsphere.local 또는 administrator@*mydomain*은 변경할 수 없습니다. 보안을 강화하려면 vCenter Single Sign-On 도메인에 이름이 지정된 사용자를 추가로 생성하고 이러한 사용자에게 관리 권한을 할당하는 것이 좋습니다. 이렇게 하면 관리자 계정을 더 사용하지 않아도 됩니다.

vCenter Server의 기타 사용자 계정

다음 사용자 계정은 vsphere.local 도메인(또는 설치 시 생성한 기본 도메인)의 vCenter Server 내에서 자동으로 생성됩니다. 이러한 사용자 계정은 셸 계정입니다. vCenter Single Sign-On 암호 정책은 이러한 계정에 적용되지 않습니다.

표 4-1. 기타 vCenter Server 사용자 계정

계정	설명
K/M	Kerberos 키 관리용입니다.
krbtgt/VSPHERE.LOCAL	통합 Windows 인증 호환성용입니다.
waiter-*random_string*	Auto Deploy용입니다.

ESXi 사용자

독립 실행형 ESXi 호스트는 vCenter Single Sign-On와 통합되지 않습니다. ESXi 호스트를 Active Directory에 추가하는 데 대한 자세한 내용은 "vSphere 보안" 을 참조하십시오.

VMware Host Client, ESXCLI 또는 PowerCLI를 사용하여 관리 ESXi 호스트에 대한 로컬 ESXi 사용자를 생성하는 경우 vCenter Server가 해당 사용자를 인식하지 못합니다. 따라서 로컬 사용자를 생성하면 사용자 이름이 동일한 경우에는 특히 혼동을 야기할 수 있습니다. vCenter Single Sign-On에 인증할 수 있는 사용자가 ESXi 호스트 개체에 대해 해당하는 사용 권한을 가지고 있으면 이 사용자는 ESXi 호스트를 보고 관리할 수 있습니다.

참고 가능하면 vCenter Server를 통해 ESXi 호스트에 대한 사용 권한을 관리하십시오.

vCenter Server 구성 요소에 로그인하는 방법

vSphere Client에 연결하여 로그인할 수 있습니다.

사용자가 vSphere Client에서 vCenter Server 시스템에 로그인할 때 로그인 동작은 해당 사용자가 기본 ID 소스로 설정된 도메인에 있는지 여부에 따라 달라집니다.

- 기본 도메인에 있는 사용자는 자신의 사용자 이름과 암호로 로그인할 수 있습니다.
- vCenter Single Sign-On에 ID 소스로 추가되었지만 기본 도메인은 아닌 도메인에 있는 사용자는 vCenter Server에 로그인할 수는 있지만 다음 방법 중 하나로 도메인을 지정해야 합니다.
  - 도메인 이름 접두사 포함(예: MYDOMAIN\user1)
  - 도메인 포함(예: user1@mydomain.com)
- vCenter Single Sign-On ID 소스가 아닌 도메인에 있는 사용자는 vCenter Server에 로그인할 수 없습니다. vCenter Single Sign-On에 추가하는 도메인이 도메인 계층의 일부이면 Active Directory에서는 해당 계층에 있는 다른 도메인의 사용자가 인증되었는지 여부를 확인합니다.

환경에 Active Directory 계층 구조가 포함되어 있는 경우 VMware 기술 자료 문서 https://kb.vmware.com/s/article/2064250에서 지원되는 설정과 지원되지 않는 설정에 대한 자세한 내용을 참조하십시오.

vCenter Single Sign-On 도메인의 그룹

vCenter Single Sign-On 도메인(기본적으로 vsphere.local)은 몇 가지 미리 정의된 그룹을 포함합니다. 이러한 그룹 중 하나에 사용자를 추가하여 해당 작업을 수행할 수 있도록 합니다.

vCenter Single Sign-On 사용자 및 그룹 관리의 내용을 참조하십시오.

vCenter Server 계층의 모든 개체의 경우 사용자 및 역할을 개체와 쌍으로 연결함으로써 사용 권한을 할당할 수 있습니다. 예를 들어 리소스 풀을 선택하고 사용자 그룹에 해당하는 역할을 부여하여 리소스 풀 개체에 대한 읽기 권한을 부여할 수 있습니다.

vCenter Server에서 직접 관리되지 않는 일부 서비스의 경우 vCenter Single Sign-On 그룹 중 하나에 대한 멤버 자격에 의해 권한이 결정됩니다. 예를 들어 관리자 그룹의 멤버인 사용자는 vCenter Single Sign-On을 관리할 수 있습니다. CAAdmins 그룹의 멤버인 사용자는 VMware Certificate Authority를 관리할 수 있으며 LicenseService.Administrators 그룹에 있는 사용자는 라이센스를 관리할 수 있습니다.

다음 그룹은 vsphere.local에서 사전 정의됩니다. 이들 중 많은 그룹이 vsphere.local 내부에서 사용되거나 사용자에게 상위 수준의 관리 권한을 제공합니다. 위험에 대해 신중하게 고려한 후에만 이러한 그룹에 사용자를 추가하십시오.

경고 vsphere.local 도메인에서 미리 정의된 그룹 중 어느 것도 삭제하지 마십시오. 그렇게 할 경우 인증 또는 인증서 프로비저닝 관련 오류가 발생할 수 있습니다.

표 4-2. vsphere.local 도메인의 그룹

권한	설명
사용자	vCenter Single Sign-On 도메인(기본적으로 vsphere.local)의 사용자.
SolutionUsers	vCenter Services를 위한 솔루션 사용자 그룹입니다. 각 솔루션 사용자는 인증서를 사용하여 개별적으로 vCenter Single Sign-On에 인증합니다. 기본적으로 VMCA는 인증서로 솔루션 사용자를 프로비저닝합니다. 이 그룹에 멤버를 명시적으로 추가하지 마십시오.
CAAdmins	CAAdmins 그룹의 멤버는 VMCA의 관리자 권한이 있습니다. 반드시 필요한 경우가 아니라면 이 그룹에 멤버를 추가하지 마십시오.
DCAdmins	DCAdmins 그룹의 멤버는 VMware 디렉토리 서비스에서 도메인 컨트롤러 관리자 작업을 수행할 수 있습니다. **참고** 도메인 컨트롤러를 직접 관리하지 마십시오. 대신 `vmdir` CLI 또는 vSphere Client를 사용하여 해당 작업을 수행합니다.
SystemConfiguration.BashShellAdministrators	이 그룹의 사용자는 모든 장치 관리 API에 대한 전체 액세스 권한을 갖습니다. 기본적으로 SSH를 사용하여 vCenter Server에 연결하는 사용자는 제한된 셸의 명령에만 액세스할 수 있지만 이 그룹의 사용자는 SSH를 통한 Bash 셸 액세스 권한을 가지며 루트 사용자와 유사한 전체 권한을 얻습니다.
ActAsUsers	Act-As 사용자 멤버는 vCenter Single Sign-On에서 Act-As 토큰을 가져올 수 있습니다.
ExternalIDPUsers	이 내부 그룹은 vSphere에서 사용되지 않습니다. VMware vCloud Air를 사용하려면 이 그룹이 있어야 합니다.
SystemConfiguration.Administrators	SystemConfiguration.Administrators 그룹의 멤버는 포트 5480에서 실행되는 vCenter Server 관리 인터페이스에서 시스템 구성을 보고 관리할 수 있습니다. 이러한 사용자는 서비스를 보고, 서비스를 시작 및 다시 시작하고, 서비스 문제를 해결할 수 있습니다. 이러한 사용자는 중요한 시스템 구성을 수정하는 API를 제외하고 장치 관리 API에도 액세스할 수 있습니다.
DCClients	이 그룹은 VMware 디렉토리 서비스에서 데이터에 대한 관리 노드 액세스를 허용하기 위해 내부적으로 사용됩니다. **참고** 이 그룹을 수정하지 마십시오. 변경하면 인증서 인프라가 손상될 수 있습니다.

표 4-2. vsphere.local 도메인의 그룹 (계속)

권한	설명
ComponentManager.Administrators	ComponentManager.Administrators 그룹의 멤버는 서비스를 등록하거나 등록 취소하는 구성 요소 관리자 API를 호출할 수 있습니다. 즉 서비스를 수정할 수 있습니다. 서비스에 대한 읽기 액세스 권한에는 이 그룹의 멤버 자격이 필요하지 않습니다.
LicenseService.Administrators	LicenseService.Administrators의 멤버는 모든 라이센싱 관련 데이터에 대한 전체 쓰기 액세스 권한이 있으며 라이센싱 서비스에 등록된 모든 제품 자산의 일련 번호 키를 추가, 제거, 할당 및 할당 취소할 수 있습니다.
관리자	VMware 디렉토리 서비스(vmdir)의 관리자입니다. 이 그룹의 멤버는 vCenter Single Sign-On 관리 작업을 수행할 수 있습니다. 반드시 필요하고 그 결과를 이해하는 경우가 아니라면 이 그룹에 멤버를 추가하지 마십시오.
신뢰할 수 있는 관리자	이 그룹의 멤버는 VMware® vSphere 신뢰 기관™ 구성 및 관리 작업을 수행할 수 있습니다. 기본적으로 이 그룹에는 멤버가 포함되어 있지 않습니다. vSphere 신뢰 기관 작업을 수행할 수 있도록 이 그룹에 멤버를 추가해야 합니다.
AutoUpdate	이 그룹은 vCenter Cloud Gateway에 대해 내부적으로 사용됩니다.
SyncUsers	이 그룹은 vCenter Cloud Gateway에 대해 내부적으로 사용됩니다.
vSphereClientSolutionUsers	이 그룹은 vSphere Client에 대해 내부적으로 사용됩니다.
ServiceProviderUsers	이 그룹의 멤버는 vSphere with Tanzu 및 VMware Cloud on AWS 인프라를 관리할 수 있습니다.
NsxAdministrators	이 그룹은 VMware NSX에 사용됩니다.
WorkloadStorage	워크로드 스토리지 그룹입니다.
RegistryAdministrators	이 그룹의 멤버는 레지스트리를 관리할 수 있습니다.
NsxAuditors	이 그룹은 VMware NSX에 사용됩니다.
NsxViAdministrators	이 그룹은 VMware NSX에 사용됩니다.
SystemConfiguration.SupportUsers	SystemConfiguration.SupportUsers 그룹의 멤버는 지원 번들 API에 액세스할 수 있습니다.
SystemConfiguration.ReadOnly	이 그룹의 멤버는 장치 관리에서 vCenter Server Appliance 읽기 전용 작업에 액세스할 수 있습니다.
VCLSAdmin	이 그룹의 멤버에게는 vCLS(vSphere 클러스터 서비스)에 대한 관리 권한이 있습니다.
AnalyticsService.Administrators	이 그룹은 VMware Analytics Service API에 사용됩니다.
vStatsGroup	이 그룹은 vStats 수집에 사용됩니다.

vCenter Single Sign-On ID 소스 구성

사용자가 사용자 이름만으로 로그인하면 vCenter Single Sign-On은 해당 사용자를 인증할 수 있는지를 기본 ID 소스에서 확인합니다. 사용자가 로그인할 때 로그인 화면에 도메인 이름을 포함하면 vCenter Single Sign-On은 해당 도메인이 ID 소스로 추가되었는지를 지정된 도메인에서 확인합니다. ID 소스를 추가하고, ID 소스를 제거하고, 기본값을 변경할 수 있습니다.

vCenter Single Sign-On은 vSphere Client에서 구성합니다. vCenter Single Sign-On을 구성하려면 vCenter Single Sign-On 관리자 권한이 있어야 합니다. vCenter Single Sign-On 관리자 권한은 vCenter Server 또는 ESXi의 관리자 역할과 다릅니다. 새 설치의 경우에는 vCenter Single Sign-On 관리자(기본적으로 administrator@vsphere.local)만 vCenter Single Sign-On에 인증할 수 있습니다.

vCenter Single Sign-On을 사용하는 vCenter Server에 대한 ID 소스

ID 소스를 사용하여 하나 이상의 도메인을 vCenter Single Sign-On에 연결할 수 있습니다. 도메인은 vCenter Single Sign-On 서버가 사용자 인증에 사용할 수 있는 사용자 및 그룹의 저장소입니다.

참고 vSphere 7.0 업데이트 2 이상은 vCenter Server에서 FIPS를 사용하도록 설정할 수 있습니다. "vSphere 보안" 설명서를 참조하십시오. FIPS를 사용하도록 설정한 경우 LDAP를 통한 AD는 지원되지 않습니다. FIPS 모드에 있을 때에는 외부 ID 제공자 페더레이션을 사용합니다. vCenter Server ID 제공자 페더레이션 구성의 내용을 참조하십시오.

관리자는 ID 소스를 추가하고, 기본 ID 소스를 설정하고, vsphere.local ID 소스에서 사용자 및 그룹을 생성할 수 있습니다.

사용자 및 그룹 데이터는 Active Directory, OpenLDAP 또는 vCenter Single Sign-On이 설치된 시스템의 운영 체제 로컬 위치에 저장됩니다. 설치 후 vCenter Single Sign-On의 모든 인스턴스에는 ID 소스 *your_domain_name*이 있습니다(예: vsphere.local). 이 ID 소스는 vCenter Single Sign-On 내부에 있습니다.

참고 기본 도메인은 항상 하나만 존재합니다. 기본 도메인이 아닌 도메인의 사용자는 로그인할 때 도메인 이름을 추가해야 성공적으로 인증할 수 있습니다. 도메인 이름의 형식은 다음과 같습니다.

```
DOMAIN\user
```

다음과 같은 ID 소스를 사용할 수 있습니다.

- LDAP를 통한 Active Directory. vCenter Single Sign-On은 LDAP ID 소스를 통한 여러 Active Directory를 지원합니다.
- Active Directory(통합 Windows 인증) 버전 2003 이상. vCenter Single Sign-On을 사용하면 단일 Active Directory 도메인을 ID 소스로 지정할 수 있습니다. 도메인은 하위 도메인을 포함할 수도 있고 그 자체가 포리스트 루트 도메인일 수도 있습니다. https://kb.vmware.com/s/article/2064250의 VMware 기술 자료 문서에서는 vCenter Single Sign-On에서 지원되는 Microsoft Active Directory 트러스트에 대해 설명합니다.

- OpenLDAP 버전 2.4 이상. vCenter Single Sign-On은 여러 OpenLDAP ID 소스를 지원합니다.

참고 Microsoft Windows 업데이트는 강력한 인증 및 암호화를 요구하도록 Active Directory의 기본 동작을 변경했습니다. 이러한 변경은 vCenter Server가 Active Directory에 인증하는 방식에 영향을 미칩니다. Active Directory를 vCenter Server의 ID 소스로 사용하는 경우 LDAPS를 사용하도록 설정해야 합니다. 자세한 내용은 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV190023 및 https://blogs.vmware.com/vsphere/2020/01/microsoft-ldap-vsphere-channel-binding-signing-adv190023.html을 참조하십시오.

vCenter Single Sign-On의 기본 도메인 설정

각 vCenter Single Sign-On ID 소스는 도메인과 연결되어 있습니다. vCenter Single Sign-On은 도메인 이름 없이 로그인하는 사용자를 인증하는 데 기본 도메인을 사용합니다. 기본 도메인이 아닌 도메인에 속한 사용자는 로그인할 때 도메인 이름을 포함해야 합니다.

사용자가 vSphere Client에서 vCenter Server 시스템에 로그인할 때 로그인 동작은 해당 사용자가 기본 ID 소스로 설정된 도메인에 있는지 여부에 따라 달라집니다.

- 기본 도메인에 있는 사용자는 자신의 사용자 이름과 암호로 로그인할 수 있습니다.
- vCenter Single Sign-On에 ID 소스로 추가되었지만 기본 도메인은 아닌 도메인에 있는 사용자는 vCenter Server에 로그인할 수는 있지만 다음 방법 중 하나로 도메인을 지정해야 합니다.
  - 도메인 이름 접두사 포함(예: MYDOMAIN\user1)
  - 도메인 포함(예: user1@mydomain.com)
- vCenter Single Sign-On ID 소스가 아닌 도메인에 있는 사용자는 vCenter Server에 로그인할 수 없습니다. vCenter Single Sign-On에 추가하는 도메인이 도메인 계층의 일부이면 Active Directory에서는 해당 계층에 있는 다른 도메인의 사용자가 인증되었는지 여부를 확인합니다.

절차

1. vSphere Client를 사용하여 vCenter Server에 로그인합니다.
2. administrator@vsphere.local 또는 vCenter Single Sign-On 관리자 그룹에 속한 다른 멤버의 사용자 이름과 암호를 지정합니다.

   설치 시 다른 도메인을 지정한 경우에는 administrator@*mydomain*으로 로그인합니다.
3. 구성 UI로 이동합니다.
   a **홈** 메뉴에서 **관리**를 선택합니다.
   b **Single Sign-On**에서 **구성**을 클릭합니다.
4. **ID 제공자** 탭에서 **ID 소스**를 클릭한 후 ID 소스를 선택하고 **기본값으로 설정**을 클릭합니다.
5. **확인**을 클릭합니다.

   도메인 화면에서 기본 도메인은 유형 열에 (기본값)이 표시됩니다.

vCenter Single Sign-On ID 소스 추가 또는 편집

사용자는 vCenter Single Sign-On ID 소스로 추가된 도메인에 있는 경우에만 vCenter Server에 로그인할 수 있습니다. vCenter Single Sign-On 관리자 사용자는 ID 소스를 추가하거나 추가한 ID 소스에 대한 설정을 변경할 수 있습니다.

ID 소스는 LDAP를 통한 Active Directory, 네이티브 Active Directory(통합 Windows 인증) 도메인 또는 OpenLDAP 디렉토리 서비스일 수 있습니다. vCenter Single Sign-On을 사용하는 vCenter Server에 대한 ID 소스의 내용을 참조하십시오.

설치 직후 vCenter Single Sign-On 내부 사용자가 있는 vsphere.local 도메인(또는 설치 중에 지정한 도메인)을 사용할 수 있습니다.

참고 Active Directory SSL 인증서를 업데이트했거나 교체한 경우 vCenter Server에서 ID 소스를 제거하고 다시 추가해야 합니다.

사전 요구 사항

Active Directory(통합 Windows 인증) ID 소스를 추가하는 경우 vCenter Server가 Active Directory 도메인에 있어야 합니다. Active Directory 도메인에 vCenter Server 추가의 내용을 참조하십시오.

절차

1. vSphere Client를 사용하여 vCenter Server에 로그인합니다.
2. administrator@vsphere.local 또는 vCenter Single Sign-On 관리자 그룹에 속한 다른 멤버의 사용자 이름과 암호를 지정합니다.

   설치 시 다른 도메인을 지정한 경우에는 administrator@*mydomain*으로 로그인합니다.
3. 구성 UI로 이동합니다.
   a. **홈** 메뉴에서 **관리**를 선택합니다.
   b. **Single Sign-On**에서 **구성**을 클릭합니다.
4. **ID 제공자** 탭에서 **ID 소스**를 클릭하고 **추가**를 클릭합니다.

5 ID 소스를 선택하고 ID 소스 설정을 입력합니다.

옵션	설명
Active Directory(통합 Windows 인증)	이 옵션은 네이티브 Active Directory를 구현하는 데 사용합니다. 이 옵션을 사용하려면 vCenter Single Sign-On 서비스가 실행 중인 시스템이 Active Directory 도메인에 있어야 합니다. Active Directory ID 소스 설정의 내용을 참조하십시오.
LDAP를 통한 Active Directory	이 옵션을 사용하려면 도메인 컨트롤러 및 기타 정보를 지정해야 합니다. LDAP를 통한 Active Directory 및 OpenLDAP 서버 ID 소스 설정의 내용을 참조하십시오.
OpenLDAP	이 옵션은 OpenLDAP ID 소스에 사용합니다. LDAP를 통한 Active Directory 및 OpenLDAP 서버 ID 소스 설정의 내용을 참조하십시오.

참고 사용자 계정을 잠그거나 비활성화하면 Active Directory 도메인에서 인증 및 그룹과 사용자 검색에 실패합니다. 사용자 계정은 사용자 및 그룹 OU에 대한 읽기 전용 액세스 권한이 있어야 하며 사용자 및 그룹 특성을 읽을 수 있어야 합니다. Active Directory는 기본적으로 이 액세스를 제공합니다. 향상된 보안을 위해 특수 서비스 사용자를 사용합니다.

6 **추가**를 클릭합니다.

다음에 수행할 작업

처음에는 각 사용자에게 권한 없음 역할이 할당됩니다. 사용자가 로그인하려면 vCenter Server 관리자가 해당 사용자에게 최소한 읽기 전용 역할을 할당해야 합니다. "vSphere 보안" 설명서에서 역할을 사용하여 권한을 할당하는 방법에 대한 항목을 참조하십시오.

LDAP를 통한 Active Directory 및 OpenLDAP 서버 ID 소스 설정

LDAP를 통한 Active Directory ID 소스는 Active Directory(통합 Windows 인증) 옵션보다 선호됩니다. OpenLDAP 서버 ID 소스는 OpenLDAP를 사용하는 환경에서 사용할 수 있습니다.

OpenLDAP ID 소스를 구성하는 경우 추가 요구 사항은 VMware 기술 자료 문서(https://kb.vmware.com/s/article/2064977)를 참조하십시오.

중요 AD-over-LDAP ID 소스의 그룹은 각 도메인에 대해 추가 ID 소스를 생성하더라도 다른 도메인의 사용자를 사용할 수 없습니다.

LDAP ID 소스의 그룹은 지정된 사용자 기반 DN에 존재하는 사용자만 인식합니다. 이로 인해 하위 도메인이 있는 대규모 Active Directory 환경에서 예기치 않은 문제가 발생할 수 있습니다. 예를 들어 다음과 같은 시나리오를 고려해야 합니다.

1 하위 도메인 2개(Child 및 Child)가 있는 Active Directory 포리스트.

2 AD-over-LDAP ID 소스 2개(하위 도메인 ChildA용 1개 및 하위 도메인 ChildB용 1개)로 구성된 vCenter Server.

3 ChildA에는 UserA1 및 UserA2라는 2명의 사용자가 포함되어 있습니다.

4 ChildB에는 UserB1 및 UserB2라는 2명의 사용자가 포함되어 있습니다.

vCenter Server 관리자가 ChildA에 UserA1, UserA2, UserB1 및 UserB2를 포함하는 TestGroup이라는 그룹을 생성합니다. vCenter Server 관리자가 TestGroup에 로그인(또는 임의) 권한을 부여합니다. 안타깝게도 UserB1과 UserB2는 그룹과 다른 도메인에 상주하기 때문에 로그인할 수 없습니다.

이 문제를 해결하려면 다음을 수행합니다.

1 ChildB에 SecondTestGroup이라는 다른 그룹을 생성합니다.

2 TestGroup에서 UserB1 및 UserB2를 제거합니다.

3 UserB1 및 UserB2를 SecondTestGroup에 추가합니다.

4 vCenter Server에서 SecondTestGroup에 TestGroup에 부여된 것과 동일한 권한을 할당합니다.

참고 Microsoft Windows에서는 강력한 인증 및 암호화를 요구하도록 Active Directory의 기본 동작을 변경했습니다. 이러한 변경은 vCenter Server가 Active Directory에 인증하는 방식에 영향을 미칩니다. Active Directory를 vCenter Server의 ID 소스로 사용하는 경우 LDAPS를 사용하도록 설정해야 합니다. Microsoft 보안 업데이트에 대한 자세한 내용은 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV190023 및 https://blogs.vmware.com/vsphere/2020/01/microsoft-ldap-vsphere-channel-binding-signing-adv190023.html의 내용을 참조하십시오.

표 4-3. LDAP를 통한 Active Directory 및 OpenLDAP 서버 설정

옵션	설명
이름	ID 소스의 이름입니다.
사용자의 기본 DN	사용자의 기본 고유 이름입니다. 사용자 검색을 시작할 DN을 입력합니다. 예: cn=Users,dc=myCorp,dc=com.
그룹의 기본 DN	그룹의 기본 고유 이름입니다. 그룹 검색을 시작할 DN을 입력합니다. 예: cn=Groups,dc=myCorp,dc=com.
도메인 이름	도메인의 FQDN입니다.

표 4-3. LDAP를 통한 Active Directory 및 OpenLDAP 서버 설정 (계속)

옵션	설명
도메인 별칭	Active Directory ID 소스의 경우 도메인의 NetBIOS 이름입니다. SSPI 인증을 사용하는 경우 Active Directory 도메인의 NetBIOS 이름을 ID 소스의 별칭으로 추가합니다. OpenLDAP ID 소스의 경우 별칭을 지정하지 않으면 대문자로 표시된 도메인 이름이 추가됩니다.
사용자 이름	도메인에서 사용자 및 그룹의 기본 DN에 대해 최소한 읽기 전용 액세스 권한이 있는 사용자의 ID입니다. ID는 다음 형식 중 하나일 수 있습니다. ■ UPN(user@domain.com) ■ NetBIOS(DOMAIN\user) ■ DN(cn=user,cn=Users,dc=domain,dc=com) 사용자 이름은 정규화되어야 합니다. "user" 항목은 작동하지 않습니다.
암호	**사용자 이름**에서 지정된 사용자의 암호입니다.
연결 대상	연결할 도메인 컨트롤러입니다. 도메인의 모든 도메인 컨트롤러 또는 특정 컨트롤러가 될 수 있습니다.
기본 서버 URL	도메인의 기본 도메인 컨트롤러 LDAP 서버입니다. 호스트 이름 또는 IP 주소를 사용할 수 있습니다. **`ldap://hostname_or_IPaddress:port`** 또는 **`ldaps://hostname_or_IPaddress:port`** 형식을 사용합니다. 일반적으로 포트는 LDAP 연결의 경우 389이고 LDAPS 연결의 경우 636입니다. Active Directory 다중 도메인 컨트롤러 배포의 경우 일반적으로 포트는 LDAP의 경우 3268이고 LDAPS의 경우 3269입니다. 기본 또는 보조 LDAP URL에 **`ldaps://`**를 사용하는 경우 Active Directory 서버의 LDAPS 끝점에 대한 신뢰를 설정하는 인증서가 필요합니다.

표 4-3. LDAP를 통한 Active Directory 및 OpenLDAP 서버 설정 (계속)

옵션	설명
보조 서버 URL	기본 도메인 컨트롤러를 사용할 수 없을 때 사용되는 보조 도메인 컨트롤러 LDAP 서버의 주소입니다. 호스트 이름 또는 IP 주소를 사용할 수 있습니다. 모든 LDAP 작업에 대해 vCenter Server는 보조 도메인 컨트롤러로 폴백하기 전에 항상 기본 도메인 컨트롤러를 시도합니다. 따라서 기본 도메인 컨트롤러를 사용할 수 없을 때는 Active Directory 로그인에 다소 시간이 걸리고 실패할 수도 있습니다. **참고** 기본 도메인 컨트롤러에 장애가 발생해도 보조 도메인 컨트롤러가 자동으로 그 역할을 인계받지 못할 수 있습니다.
인증서(LDAPS용)	Active Directory LDAP 서버 또는 OpenLDAP 서버 ID 소스와 함께 LDAPS를 사용하려면 **찾아보기**를 클릭하여 LDAPS URL에 지정된 도메인 컨트롤러에서 내보낸 인증서를 선택합니다. (여기에 사용된 인증서는 루트 CA 인증서가 아닙니다.) Active Directory에서 인증서를 내보내려면 Microsoft 설명서를 참조하십시오. 여러 인증서를 찾아서 선택할 수 있습니다. **팁** 여러 인증서를 찾아서 선택할 때는 해당 인증서가 동일한 디렉토리에 있어야 합니다. vCenter Server는 등록되고 신뢰할 수 있는 CA(인증 기관)에서 직접 서명한 인증서만 신뢰합니다. vCenter Server는 등록된 CA 인증서까지의 경로를 추적하지 않으며 인증서가 등록되고 신뢰할 수 있는 CA(인증 기관)에서 서명했는지 여부만 확인합니다. 인증서가 공개적으로 신뢰할 수 있는 인증 기관에서 서명했거나 자체 서명된 것이라면 추가 작업이 필요하지 않습니다. 그러나 자체 내부 인증서를 만드는 경우(즉, 사설 CA(인증 기관)를 사용하는 경우) 해당 인증서를 포함해야 할 수도 있습니다. 예를 들어, 조직에서 Microsoft Enterprise Root CA(인증 기관)를 사용하여 LDAPS 인증서를 생성하는 경우 Enterprise Root 인증서도 선택하여 vCenter Server에 추가해야 합니다. 또한 LDAPS 인증서와 Enterprise Root 인증서 사이에 중간 인증 기관을 사용하는 경우 해당 중간 인증서도 선택하여 vCenter Server에 추가해야 합니다.

Active Directory ID 소스 설정

Active Directory(통합 Windows 인증) ID 소스 유형을 선택하면 로컬 시스템 계정을 SPN(서비스 사용자 이름)으로 사용하거나 SPN을 명시적으로 지정할 수 있습니다. vCenter Single Sign-On 서버가 Active Directory 도메인에 가입된 경우에만 이 옵션을 사용할 수 있습니다.

Active Directory(통합 Windows 인증) ID 소스 사용을 위한 필수 구성 요소

해당 ID 소스를 사용할 수 있는 경우에만 Active Directory(통합 Windows 인증) ID 소스를 사용하도록 vCenter Single Sign-On을 설정할 수 있습니다. "vCenter Server 구성" 설명서에 나와 있는 지침을 따르십시오.

참고 Active Directory(통합 Windows 인증)는 항상 Active Directory 도메인 포리스트의 루트를 사용합니다. Active Directory 포리스트 내에 하위 도메인을 가진 통합 Windows 인증 ID 소스를 구성하려면 VMware 기술 자료 문서(https://kb.vmware.com/s/article/2070433)를 참조하십시오.

구성 속도를 높이려면 **시스템 계정 사용**을 선택합니다. If you expect to rename the local machine on which vCenter Single Sign-On runs, specifying an SPN explicitly is preferable.

강화가 필요한 위치를 식별하기 위해 Active Directory에서 진단 이벤트 로깅을 사용하도록 설정한 경우, 해당 디렉토리 서버에서 이벤트 ID가 2889인 로그 이벤트를 볼 수 있습니다. 통합 Windows 인증을 사용하는 경우 ID 2889는 이벤트 보안 위험이 아닌 이상 징후로 생성됩니다. 이벤트 ID 2889에 대한 자세한 내용은 https://kb.vmware.com/s/article/78644에서 VMware 기술 자료 문서를 참조하십시오.

표 4-4. ID 소스 추가 설정

텍스트 상자	설명
도메인 이름	도메인 이름의 FQDN입니다(예: mydomain.com). IP 주소를 제공하지 마십시오. 이 도메인 이름은 vCenter Server 시스템을 통해 DNS에서 확인할 수 있어야 합니다.
시스템 계정 사용	로컬 시스템 계정을 SPN으로 사용하려면 이 옵션을 선택합니다. 이 옵션을 선택하는 경우 도메인 이름만 지정하십시오. 이 시스템의 이름을 변경해야 할 경우에는 이 옵션을 선택하지 마십시오.
SPN(서비스 사용자 이름) 사용	로컬 시스템의 이름을 변경해야 할 경우 이 옵션을 선택합니다. SPN, ID 소스를 사용하여 인증할 수 있는 사용자 및 사용자 암호를 지정해야 합니다.
SPN(서비스 사용자 이름)	Kerberos가 Active Directory 서비스를 식별하는 데 도움이 되는 SPN입니다. 이름에 도메인을 포함합니다(예: `STS/example.com`). SPN은 전체 도메인에서 고유해야 합니다. `setspn -S` 명령을 실행하면 중복이 생성되지 않았는지 확인할 수 있습니다. `setspn`에 대한 자세한 내용은 Microsoft 설명서를 참조하십시오.
UPN(사용자 계정 이름) **암호**	이 ID 소스를 사용하여 인증할 수 있는 사용자의 이름 및 암호입니다. 이메일 주소 형식(예: `jchin@mydomain.com`)을 사용합니다. Active Directory 서비스 인터페이스 편집기(ADSI 편집)를 사용하여 사용자 계정 이름을 확인할 수 있습니다.

CLI를 사용하여 ID 소스 추가 또는 제거

`sso-config` 유틸리티를 사용하여 ID 소스를 추가하거나 제거할 수 있습니다.

ID 소스는 네이티브 Active Directory(통합 Windows 인증) 도메인, LDAP를 통한 AD, LDAPS를 사용하는 LDAP를 통한 AD(SSL을 통한 LDAP) 또는OpenLDAP일 수 있습니다. vCenter Single Sign-On을 사용하는 vCenter Server에 대한 ID 소스의 내용을 참조하십시오. 또한 `sso-config` 유틸리티를 사용하여 스마트 카드 및 RSA SecurID 인증을 설정할 수 있습니다.

사전 요구 사항

Active Directory ID 소스를 추가하는 경우 vCenter Server가 Active Directory 도메인에 있어야 합니다. Active Directory 도메인에 vCenter Server 추가의 내용을 참조하십시오.

SSH 로그인을 사용하도록 설정합니다. vCenter Server 셸을 사용하여 vCenter Server 관리의 내용을 참조하십시오.

절차

1. SSH 또는 다른 원격 콘솔 연결을 사용하여 vCenter Server 시스템에서 세션을 시작합니다.
2. root로 로그인합니다.
3. `sso-config` 유틸리티가 있는 디렉토리로 변경합니다.

   ```
   cd /opt/vmware/bin
   ```

4. `sso-config.sh -help`를 실행하여 `sso-config` 도움말을 참조하거나 VMware 기술 자료 문서(https://kb.vmware.com/s/article/67304)에서 사용 예를 참조하십시오.

vCenter Server Security Token Service 관리

vCenter Server STS(Security Token Service)는 보안 토큰을 발급, 검증 및 갱신하는 웹 서비스입니다.

토큰 발급자인 STS(Security Token Service)는 개인 키를 사용하여 토큰에 서명하고 서비스에 대한 공용 인증서를 게시하여 토큰 서명을 확인합니다. vCenter Server는 STS 서명 인증서를 관리하고 VMware Directory Service(vmdir)에 저장합니다. 토큰의 수명은 상당히 길 수 있고, 이전에는 여러 키 중 하나를 사용하여 서명이 가능했습니다.

사용자는 자신의 기본 자격 증명을 STS 인터페이스에 제공하여 토큰을 획득합니다. 기본 자격 증명은 사용자 유형에 따라 다릅니다.

표 4-5. STS 사용자 및 자격 증명

사용자 유형	기본 자격 증명
솔루션 사용자	유효한 인증서
기타 사용자	vCenter Single Sign-On ID 소스에서 사용할 수 있는 사용자 이름 및 암호

STS는 기본 자격 증명에 기반하여 사용자를 인증하고 사용자 특성이 포함된 SAML 토큰을 구성합니다.

기본적으로 VMCA(VMware Certificate Authority)는 STS 서명 인증서를 생성합니다. 새 VMCA 인증서를 사용하여 STS 서명 인증서를 새로 고칠 수 있습니다. 기본 STS 서명 인증서를 가져와서 사용자 지정 또는 타사 생성 STS 서명 인증서로 바꿀 수도 있습니다. 회사의 보안 정책에 따라 모든 인증서를 교체해야 하는 경우가 아니면 STS 서명 인증서를 교체하지 마십시오.

vSphere Client를 사용하여 다음을 수행할 수 있습니다.

- STS 인증서 새로 고침
- 사용자 지정 및 타사 생성 STS 인증서 가져오기 및 바꾸기
- 만료 날짜와 같은 STS 인증서 세부 정보 보기

명령줄을 사용하여 사용자 지정 및 타사 생성 STS 인증서를 바꿀 수도 있습니다.

STS 인증서 기간 및 만료

vSphere 7.0 업데이트 1 이상을 새로 설치하면 기간이 10년인 STS 서명 인증서가 생성됩니다. STS 서명 인증서가 곧 만료되는 경우 90일 전부터 일주일에 한 번씩 경보가 표시되고 7일 이전부터는 매일 경보가 표시됩니다.

참고 특정 상황에서 STS 서명 인증서를 교체하면 인증서 기간이 변경될 수 있습니다. 인증서 교체를 수행할 때는 발급 날짜와 만료 날짜에 주의를 기울여야 합니다.

STS 인증서 자동 갱신

vSphere 8.0 이상에서 vCenter Single Sign-On은 VMCA 생성 STS 서명 인증서를 자동으로 갱신합니다. 자동 갱신은 STS 서명 인증서가 만료되기 전과 90일 만료 경보가 트리거되기 전에 이루어집니다. 자동 갱신이 실패하면 vCenter Single Sign-On이 로그 파일에 오류 메시지를 생성합니다. 필요한 경우 STS 서명 인증서를 수동으로 새로 고칠 수 있습니다.

참고 vCenter Single Sign-On은 사용자 지정 생성 또는 타사 STS 서명 인증서의 자동 갱신을 수행하지 않습니다.

STS 인증서 새로 고침 및 가져오기 및 교체

vSphere 8.0 이상에서는 STS 서명 인증서를 새로 고치거나 가져와서 교체할 때 vCenter Server를 다시 시작할 필요가 없으므로 다운타임이 발생하지 않습니다. 또한 연결된 구성에서 단일 vCenter Server의 STS 서명 인증서를 새로 고치거나 가져와서 교체하면 연결된 모든 vCenter Server 시스템의 STS 인증서가 업데이트됩니다.

참고 경우에 따라 STS 서명 인증서를 새로 고치거나 가져와서 교체하려면 vCenter Server 시스템을 수동으로 다시 시작해야 할 수 있습니다.

vSphere Client를 사용하여 vCenter Server STS 인증서 새로 고침

vSphere Client를 사용하여 vCenter Server STS 서명 인증서를 새로 고칠 수 있습니다. VMCA(VMware Certificate Authority)는 새 인증서를 발급하고 현재 인증서를 대체합니다.

STS 서명 인증서를 새로 고치면 VMCA(VMware Certificate Authority)에서 새 인증서가 발급되고 VMware Directory Service(vmdir)의 현재 인증서가 대체됩니다. STS는 새 인증서를 사용하여 새 토큰을 발급하기 시작합니다. 고급 연결 모드 구성에서 vmdir은 발급 vCenter Server 시스템의 새 인증서를 연결된 모든 vCenter Server 시스템에 업로드합니다. STS 서명 인증서를 새로 고치면 vCenter Server 시스템 그리고 고급 연결 모드 구성의 일부인 다른 vCenter Server 시스템을 다시 시작할 필요가 없습니다.

사용자 지정 생성 또는 타사 STS 서명 인증서를 사용하는 경우 새로 고침을 수행하면 해당 인증서를 VMCA 발급 인증서로 덮어씁니다. 사용자 지정 생성 또는 타사 STS 서명 인증서를 업데이트하려면 가져오기 및 바꾸기 옵션을 사용합니다. vSphere Client를 사용하여 vCenter Server STS 인증서 가져오기 및 바꾸기의 내용을 참조하십시오.

VMCA 발급 STS 서명 인증서는 10년간 유효하며 외부용 인증서가 아닙니다. 회사의 보안 정책에 따라 필요한 경우가 아니면 이 인증서를 교체하지 마십시오.

사전 요구 사항

인증서 관리를 이해 로컬 도메인(기본적으로 administrator@vsphere.local) 관리자의 암호를 입력해야 합니다. 인증서를 갱신하는 경우에는 vCenter Server 시스템에 대한 관리자 권한이 있는 사용자의 vCenter Single Sign-On 자격 증명도 제공해야 합니다.

절차

1 vSphere Client를 사용하여 vCenter Server에 로그인합니다.

2 administrator@vsphere.local 또는 vCenter Single Sign-On 관리자 그룹에 속한 다른 멤버의 사용자 이름과 암호를 지정합니다.

   설치 시 다른 도메인을 지정한 경우에는 administrator@*mydomain*으로 로그인합니다.

3 인증서 관리 UI로 이동합니다.

   a **홈** 메뉴에서 **관리**를 선택합니다.

   b **인증서**에서 **인증서 관리**를 클릭합니다.

4 시스템에 메시지가 표시되면 vCenter Server의 자격 증명을 입력합니다.

5 **STS 서명** 탭에서 원하는 인증서를 선택하고 **vCenter 인증서로 새로 고침**을 클릭합니다.

   사용자 지정 생성 또는 타사 STS 서명 인증서를 사용하는 경우 새로 고침 작업을 수행하면 해당 인증서를 VMCA 생성 인증서로 덮어씁니다.

   참고 규정 준수를 위해 타사 인증서를 사용하는 경우 새로 고침으로 인해 vCenter Server 시스템이 규정을 준수하지 못할 수 있습니다. 또한 사용자 지정 생성 또는 타사 STS 서명 인증서를 사용하는 경우 Security Token Service는 해당 사용자 지정 또는 타사 인증서를 토큰 서명에 더 이상 사용하지 않습니다.

6 **새로 고침**을 클릭합니다.

   VMCA는 이 vCenter Server 시스템 및 연결된 vCenter Server 시스템에서 STS 서명 인증서를 새로 고칩니다.

7 (선택 사항) **강제 새로 고침** 버튼이 나타나면 vCenter Single Sign-On이 문제를 감지한 것입니다. **강제 새로 고침**을 클릭하기 전에 다음과 같은 잠재적 결과를 고려하십시오.

- 영향을 받은 모든 vCenter Server 시스템에서 vSphere 7.0 업데이트 3 이상을 실행하지 않는 경우 인증서 새로 고침이 지원되지 않습니다.
- **강제 새로 고침**을 선택하면 모든 vCenter Server 시스템을 다시 시작해야 하며, 그렇게 할 때까지 해당 시스템이 작동하지 않을 수 있습니다.

a 영향이 확실하지 않은 경우 **취소**를 클릭하고 환경을 조사합니다.

b 영향이 확실하지 않은 경우 **강제 새로 고침**을 클릭하여 새로 고침을 진행한 다음 vCenter Server 시스템을 수동으로 다시 시작합니다.

vSphere Client를 사용하여 vCenter Server STS 인증서 가져오기 및 바꾸기

vSphere Client를 사용하여 vCenter Server STS 인증서를 가져오고 사용자 지정 생성 인증서 또는 타사 인증서로 교체할 수 있습니다.

기본 STS 서명 인증서를 가져오고 교체하려면 먼저 새 인증서를 생성해야 합니다. STS 서명 인증서를 가져오고 교체하면 VMware Directory Service(vmdir)는 발급 vCenter Server 시스템에서 연결된 모든 vCenter Server 시스템으로 새 인증서를 업로드합니다.

STS 인증서는 외부용 인증서가 아닙니다. 회사의 보안 정책에 따라 필요한 경우가 아니면 이 인증서를 교체하지 마십시오.

사전 요구 사항

인증서 관리를 이해 로컬 도메인(기본적으로 administrator@vsphere.local) 관리자의 암호를 입력해야 합니다. 또한 vCenter Server 시스템에 대한 관리자 권한이 있는 사용자의 vCenter Single Sign-On 자격 증명을 제공해야 합니다.

절차

1 vSphere Client를 사용하여 vCenter Server에 로그인합니다.

2 administrator@vsphere.local 또는 vCenter Single Sign-On 관리자 그룹에 속한 다른 멤버의 사용자 이름과 암호를 지정합니다.

설치 시 다른 도메인을 지정한 경우에는 administrator@*mydomain*으로 로그인합니다.

3 인증서 관리 UI로 이동합니다.

a **홈** 메뉴에서 **관리**를 선택합니다.

b **인증서**에서 **인증서 관리**를 클릭합니다.

4 시스템에 메시지가 표시되면 vCenter Server의 자격 증명을 입력합니다.

5 **STS 서명** 탭에서 원하는 인증서를 선택하고 **인증서 가져오기 및 바꾸기**를 클릭합니다.

6 PEM 파일을 선택합니다.

PEM 파일에는 서명 인증서 체인과 개인 키가 포함됩니다.

7 **바꾸기**를 클릭합니다.

STS 서명 인증서는 이 vCenter Server 시스템 및 연결된 vCenter Server 시스템에서 교체됩니다. 달리 명시되지 않는 한 vCenter Server 시스템을 다시 시작할 필요가 없습니다.

명령줄을 사용하여 vCenter Server STS 인증서 교체

CLI를 사용하여 vCenter Server STS 인증서를 사용자 지정 생성 인증서 또는 타사 인증서로 교체할 수 있습니다.

회사의 필수 인증서를 사용하거나 곧 만료되는 인증서를 새로 고치려면 기존 STS 서명 인증서를 교체하면 됩니다. 기본 STS 서명 인증서를 교체하려면 먼저 새 인증서를 생성해야 합니다.

STS 인증서는 외부용 인증서가 아닙니다. 회사의 보안 정책에 따라 필요한 경우가 아니면 이 인증서를 교체하지 마십시오.

경고 여기에 설명된 절차를 사용해야 합니다. 파일 시스템에서 직접 인증서를 교체하지 마십시오.

사전 요구 사항

vCenter Server에 대한 SSH 로그인을 사용하도록 설정합니다. vCenter Server 셸을 사용하여 vCenter Server 관리의 내용을 참조하십시오.

절차

1 vCenter Server 셸에 루트로 로그인합니다.

2 인증서를 생성합니다.

a 새 인증서를 저장할 최상위 디렉토리를 생성하고 디렉토리의 위치를 확인합니다.

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

b `certool.cfg` 파일을 새 디렉토리에 복사합니다.

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

c Vim과 같은 명령줄 편집기를 사용하여 `certool.cfg` 파일 사본을 열고, 로컬 vCenter Server IP 주소와 호스트 이름을 사용하도록 편집합니다. 국가는 필수 항목이며, 아래 예제에 나와 있는 대로 2자여야 합니다.

```
#
# 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 키를 생성합니다.

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

e 인증서를 생성합니다.

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

f 인증서 체인과 개인 키를 사용하여 PEM 파일을 생성합니다.

```
cat newsts.cer /var/lib/vmware/vmca/root.cer sts.key > newsts.pem
```

3 다음과 같이 STS 서명 인증서를 업데이트합니다.

```
/opt/vmware/bin/sso-config.sh -set_signing_cert -t vsphere.local /root/newsts/newsts.pem
```

VMCA는 이 vCenter Server 시스템 및 연결된 vCenter Server 시스템에서 STS 서명 인증서를 새로 고칩니다.

vSphere Client를 사용하여 활성 vCenter Server STS 서명 인증서 체인 보기

vSphere Client를 사용하여 활성 vCenter Server STS 서명 인증서 체인 및 유효 기간 종료 날짜와 같은 인증서 정보를 볼 수 있습니다.

절차

1 vSphere Client를 사용하여 vCenter Server에 로그인합니다.

2 최소한 읽기 권한이 있는 사용자의 사용자 이름과 암호를 입력합니다.

3 인증서 관리 UI로 이동합니다.

a **홈** 메뉴에서 **관리**를 선택합니다.

b **인증서**에서 **인증서 관리**를 클릭합니다.

4 시스템에 메시지가 표시되면 vCenter Server의 자격 증명을 입력합니다.

5 **STS서명** 탭에서 인증서를 선택한 다음, 인증서를 확장합니다.

다음을 비롯한 인증서 및 문제 정보가 표시됩니다.

- 유효 기간 종료 날짜
- 유효한 인증서를 나타내는 녹색 확인 표시 및 만료된 인증서에 대한 주의를 나타내는 주황색 확인 표시

명령줄을 사용하여 LDAPS SSL 인증서의 만료 날짜 확인

LDAP를 통한 Active Directory를 사용하는 경우 LDAP 트래픽에 대한 SSL 인증서를 업로드할 수 있습니다. SSL 인증서는 미리 지정한 기간이 지나면 만료됩니다. `sso-config.sh` 명령을 사용하여 인증서가 만료되기 전에 인증서를 교체 또는 갱신할 수 있도록 인증서의 만료 날짜를 볼 수 있습니다.

vCenter Server는 활성 LDAP SSL 인증서의 만료 날짜에 가까워질 때 경고 메시지를 표시합니다.

LDAP를 통한 Active Directory 또는 OpenLDAP ID 소스를 사용하고 서버에 `ldaps://` URL을 지정한 경우에만 인증서 만료 정보가 표시됩니다.

사전 요구 사항

vCenter Server에 대한 SSH 로그인을 사용하도록 설정합니다. vCenter Server 셸을 사용하여 vCenter Server 관리의 내용을 참조하십시오.

절차

1 vCenter Server에 루트로 로그인합니다.

2 다음 명령을 실행합니다.

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

SLF4J 메시지를 무시합니다.

3 만료 날짜를 확인하려면 SSL 인증서의 세부 정보를 살펴보고 `NotAfter` 필드를 확인합니다.

vCenter Single Sign-On 정책 관리

vCenter Single Sign-On 정책은 일반적으로 로컬 계정 및 토큰에 대한 보안 규칙을 적용합니다. 기본 vCenter Single Sign-On 암호 정책, 잠금 정책 및 토큰 정책을 보고 편집할 수 있습니다.

vCenter Single Sign-On 암호 정책 편집

vCenter Single Sign-On 암호 정책은 암호 형식 및 암호 만료를 결정합니다. 암호 정책은 vCenter Single Sign-On 도메인(vsphere.local)의 사용자에게만 적용됩니다.

기본적으로, vCenter Single Sign-On 기본 제공 사용자 계정 암호는 90일 후에 만료됩니다. vSphere Client는 암호가 만료되려고 할 때 미리 알려 줍니다.

vCenter Single Sign-On 암호 변경 의 내용을 참조하십시오.

참고 관리자 계정(administrator@vsphere local)은 잠기지 않거나 암호가 만료되지 않습니다. 적절한 보안 사례는 이 계정에서 로그인을 감사하고 정기적으로 암호를 교체하는 것입니다.

절차

1 vSphere Client를 사용하여 vCenter Server에 로그인합니다.

2 administrator@vsphere.local 또는 vCenter Single Sign-On 관리자 그룹에 속한 다른 멤버의 사용자 이름과 암호를 지정합니다.

설치 시 다른 도메인을 지정한 경우에는 administrator@*mydomain*으로 로그인합니다.

3 구성 UI로 이동합니다.

a **홈** 메뉴에서 **관리**를 선택합니다.

b **Single Sign-On**에서 **구성**을 클릭합니다.

4 **로컬 계정** 탭을 클릭합니다.

5 **암호 정책** 행의 **편집**을 클릭합니다.

6 암호 정책을 편집합니다.

옵션	설명
설명	암호 정책 설명입니다.
최대 수명	사용자가 변경해야 될 때까지 암호가 유효한 최대 일수입니다. 입력할 수 있는 최대 일 수는 999999999일입니다. 0 값은 암호가 만료되지 않음을 의미합니다.
재사용 제한	재사용될 수 없는 이전 암호의 수입니다. 예를 들어 6을 입력하는 경우 사용자가 마지막 6개 암호를 재사용할 수 없습니다.
최대 길이	암호에 허용되는 최대 문자 수입니다.

옵션	설명
최소 길이	암호에 요구되는 최소 문자 수입니다. 최소 길이는 영문자, 숫자 및 특수 문자 결합의 최소 요구 사항을 충족해야 합니다.
문자 요구 사항	암호에 요구되는 다양한 문자 유형의 최소 수입니다. 다음과 같은 문자 유형의 수를 지정할 수 있습니다. ■ 특수 문자: & # % ■ 영문자: A b c D ■ 대문자: A B C ■ 소문자: a b c ■ 숫자: 1 2 3 ■ 인접한 동일 문자: 숫자가 0보다 커야 합니다. 예를 들면 1을 입력하면 p@$$word와 같은 암호가 허용되지 않습니다. 최소 영문자 수는 최소 대문자 수 및 최소 소문자 수의 합보다 크거나 같아야 합니다. 암호에서는 ASCII가 아닌 문자를 지원합니다. vCenter Single Sign-On 이전 버전에서는 지원되는 문자에 대한 제한이 있습니다.

참고 암호 정책은 최소 길이가 20자를 초과하는 경우에만 최대 길이 값을 선택합니다. 최소 길이 값이 20자를 초과하고 최대 길이가 임의의 값으로 설정된 경우 암호 정책의 동작이 정의되지 않거나 서비스가 실패할 수 있습니다. 잠재적인 문제를 방지하려면 최소 길이를 기본값인 8자로 설정하거나 20자 이하로 설정합니다.

7 **저장**을 클릭합니다.

vCenter Single Sign-On 잠금 정책 편집

vCenter Single Sign-On 잠금 정책은 사용자가 잘못된 자격 증명을 사용하여 로그인하려고 할 때 사용자의 vCenter Single Sign-On 계정이 잠기는 경우를 지정합니다. 관리자는 잠금 정책을 편집할 수 있습니다.

사용자가 잘못된 암호로 vsphere.local에 로그인하려고 여러 번 시도하면 해당 사용자가 잠깁니다. 잠금 정책을 통해 관리자는 실패한 최대 로그인 시도 횟수를 지정하고 실패 사이의 시간 간격을 설정할 수 있습니다. 또한 계정이 자동으로 잠금 해제될 때까지의 경과 시간을 지정할 수도 있습니다.

참고 잠금 정책은 administrator@vsphere.local과 같은 시스템 계정이 아닌 사용자 계정에만 적용됩니다.

절차

1 vSphere Client를 사용하여 vCenter Server에 로그인합니다.

2 administrator@vsphere.local 또는 vCenter Single Sign-On 관리자 그룹에 속한 다른 멤버의 사용자 이름과 암호를 지정합니다.

설치 시 다른 도메인을 지정한 경우에는 administrator@*mydomain*으로 로그인합니다.

3 구성 UI로 이동합니다.

a **홈** 메뉴에서 **관리**를 선택합니다.

b **Single Sign-On**에서 **구성**을 클릭합니다.

4 **로컬 계정** 탭을 클릭합니다.

5 **잠금 정책** 행의 **편집**을 클릭합니다.

잠금 정책 행을 보려면 아래로 스크롤해야 할 수 있습니다.

6 매개 변수를 편집합니다.

옵션	설명
설명	잠금 정책에 대한 선택적 설명.
실패한 최대 로그인 시도 횟수	계정이 잠길 때까지 허용되는 최대 로그인 시도 실패 횟수입니다.
실패 사이의 시간 간격	잠금을 트리거하기 위해 실패한 로그인 시도가 발생해야 하는 기간입니다.
잠금 해제 시간	계정이 잠김 상태로 유지되는 기간입니다. 0을 입력하면 관리자가 해당 계정을 명시적으로 잠금 해제해야 합니다.

7 **저장**을 클릭합니다.

vCenter Single Sign-On 토큰 정책 편집

vCenter Single Sign-On 토큰 정책은 클럭 허용 오차 및 갱신 수와 같은 토큰 속성을 지정합니다. 토큰 규격이 회사의 보안 표준에 맞도록 토큰 정책을 편집할 수 있습니다.

절차

1 vSphere Client를 사용하여 vCenter Server에 로그인합니다.

2 administrator@vsphere.local 또는 vCenter Single Sign-On 관리자 그룹에 속한 다른 멤버의 사용자 이름과 암호를 지정합니다.

설치 시 다른 도메인을 지정한 경우에는 administrator@*mydomain*으로 로그인합니다.

3 구성 UI로 이동합니다.

a **홈** 메뉴에서 **관리**를 선택합니다.

b **Single Sign-On**에서 **구성**을 클릭합니다.

4 **로컬 계정** 탭을 클릭합니다.

5 **토큰 신뢰도** 행의 **편집**을 클릭합니다.

토큰 신뢰도 행을 보려면 아래로 스크롤해야 할 수 있습니다.

6 토큰 정책 구성 매개 변수를 편집합니다.

옵션	설명
클럭 허용 오차	vCenter Single Sign-On에서 허용하는 클라이언트 클럭과 도메인 컨트롤러 클럭 간 시간 차이(밀리초)입니다. 시간 차이가 지정된 값보다 크면 vCenter Single Sign-On은 토큰을 잘못된 것으로 선언합니다.
토큰 갱신 최대 횟수	토큰을 갱신할 수 있는 최대 횟수입니다. 갱신 최대 횟수를 초과한 경우 새 보안 토큰이 필요합니다.

옵션	설명
토큰 위임 최대 횟수	키 소유자 토큰은 vSphere 환경의 서비스에 위임할 수 있습니다. 위임된 토큰을 사용하는 서비스는 토큰을 제공한 주체 대신 서비스를 수행합니다. 토큰 요청은 DelegateTo ID를 지정합니다. DelegateTo 값은 솔루션 토큰 또는 솔루션 토큰에 대한 참조일 수 있습니다. 이 값은 단일 키 소유자 토큰을 위임할 수 있는 횟수를 지정합니다.
보유자 토큰 최대 수명	보유자 토큰은 토큰 소유 여부에 따라서만 인증을 제공합니다. 보유자 토큰은 단기 단일 작업에 사용됩니다. 보유자 토큰은 요청을 보내는 사용자 또는 엔티티의 ID를 확인하지 않습니다. 이 값은 토큰을 재발급하기 전까지의 보유자 토큰 수명 값을 지정합니다.
키 소유자 토큰 최대 수명	키 소유자 토큰은 토큰에 포함된 보안 아티팩트를 기반으로 인증을 제공합니다. 키 소유자 토큰은 위임에 사용될 수 있습니다. 클라이언트는 키 소유자 토큰을 가져와 다른 엔티티에 위임할 수 있습니다. 토큰에는 원래 소유자와 대리자를 식별하기 위한 클레임이 포함되어 있습니다. vSphere 환경에서는 vCenter Server 시스템이 사용자 대신 위임된 토큰을 가져오고 해당 토큰을 사용하여 작업을 수행합니다. 이 값은 토큰이 잘못된 것으로 표시되기 전까지의 키 소유자 토큰 수명을 결정합니다.

7 **저장**을 클릭합니다.

Active Directory(통합 Windows 인증) 사용자의 암호 만료 알림 편집

Active Directory 암호 만료 알림은 vCenter Server SSO 암호 만료와는 별개입니다. Active Directory 사용자의 기본 암호 만료 알림은 30일이지만 실제 암호 만료는 Active Directory 시스템에 따라 다릅니다. vSphere Client는 만료 알림을 제어합니다. 회사의 보안 표준에 맞게 기본 만료 알림을 변경할 수 있습니다.

사전 요구 사항

- vCenter Server에 대한 SSH 로그인을 사용하도록 설정합니다. vCenter Server 셸을 사용하여 vCenter Server 관리의 내용을 참조하십시오.

절차

1 관리자 권한이 있는 사용자로 vCenter Server 셸에 로그인합니다.

수퍼 관리자 역할이 있는 기본 사용자는 루트입니다.

2 vSphere Client `webclient.properties` 파일이 있는 디렉토리로 변경합니다.

```
cd /etc/vmware/vsphere-ui
```

3 텍스트 편집기에서 `webclient.properties` 파일을 엽니다.

4 다음 변수를 편집합니다.

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

5 vSphere Client를 다시 시작합니다.

```
service-control --stop vsphere-ui
service-control --start vsphere-ui
```

vCenter Single Sign-On 사용자 및 그룹 관리

vCenter Single Sign-On 관리자는 vSphere Client에서 vsphere.local 도메인의 사용자 및 그룹을 관리할 수 있습니다.

vSphere Client는 vSphere 도메인(기본적으로 vsphere.local)의 사용자 및 그룹 보기를 제공합니다. 이 보기에서 사용자를 추가, 편집 및 비활성화할 수 있습니다. 그룹을 추가하고 그룹 멤버 자격을 관리할 수도 있습니다.

vCenter Single Sign-On 사용자 추가

vSphere Client의 **사용자** 탭에 나열된 사용자는 vsphere.local 도메인에 속한 vCenter Single Sign-On 내부 사용자입니다. vCenter Single Sign-On 관리 인터페이스 중 하나에서 해당 도메인에 사용자를 추가합니다.

해당 도메인에서 다른 도메인을 선택하고 해당 도메인의 사용자에 대한 정보를 볼 수는 있지만 vCenter Single Sign-On 관리 인터페이스에서 사용자를 다른 도메인에 추가할 수는 없습니다.

절차

1 vSphere Client를 사용하여 vCenter Server에 로그인합니다.

2 administrator@vsphere.local 또는 vCenter Single Sign-On 관리자 그룹에 속한 다른 멤버의 사용자 이름과 암호를 지정합니다.

설치 시 다른 도메인을 지정한 경우에는 administrator@*mydomain*으로 로그인합니다.

3 vCenter Single Sign-On 사용자 구성 UI로 이동합니다.

a **홈** 메뉴에서 **관리**를 선택합니다.

b **Single Sign-On**에서 **사용자 및 그룹**을 클릭합니다.

4 현재 선택된 도메인이 vsphere.local이 아닌 경우 드롭다운 메뉴에서 vsphere.local을 선택합니다.

다른 도메인에는 사용자를 추가할 수 없습니다.

5 **사용자** 탭에서 **추가**를 클릭합니다.

6 새 사용자의 사용자 이름과 암호를 입력합니다.

사용자 이름에 허용되는 최대 문자 수는 300자입니다.

사용자를 생성한 후에는 사용자 이름을 변경할 수 없습니다. 암호는 시스템의 암호 정책 요구 사항을 충족해야 합니다.

7 (선택 사항) 새 사용자의 성과 이름을 입력합니다.

8 (선택 사항) 사용자의 이메일 주소 및 설명을 입력합니다.

9 **추가**를 클릭합니다.

결과

사용자를 추가하면 처음에는 해당 사용자에게 관리 작업을 수행할 수 있는 권한이 없습니다.

다음에 수행할 작업

사용자를 vsphere.local 도메인의 그룹(예: VMCA를 관리할 수 있는 사용자 그룹(CAAdmins) 또는 vCenter Single Sign-On을 관리할 수 있는 사용자 그룹(Administrators))에 추가합니다. vCenter Single Sign-On 그룹에 멤버 추가의 내용을 참조하십시오.

vCenter Single Sign-On 사용자 비활성화 및 활성화

vCenter Single Sign-On 사용자 계정이 비활성화된 경우 관리자가 해당 계정을 활성화할 때까지 사용자가 vCenter Single Sign-On 서버에 로그인할 수 없습니다. vCenter Single Sign-On 관리 인터페이스 중 하나에서 계정을 비활성화 및 활성화할 수 있습니다.

비활성화된 사용자 계정은 vCenter Single Sign-On 시스템에서 사용할 수 있는 상태로 유지되지만 사용자는 로그인하거나 서버에서 작업을 수행할 수 없습니다. 관리자 권한이 있는 사용자는 vCenter Server **사용자 및 그룹** 페이지에서 계정을 비활성화 및 활성화할 수 있습니다.

사전 요구 사항

vCenter Single Sign-On 사용자를 비활성화 및 활성화하려면 vCenter Single Sign-On 관리자 그룹의 멤버여야 합니다.

절차

1. vSphere Client를 사용하여 vCenter Server에 로그인합니다.
2. administrator@vsphere.local 또는 vCenter Single Sign-On 관리자 그룹에 속한 다른 멤버의 사용자 이름과 암호를 지정합니다.

   설치 시 다른 도메인을 지정한 경우에는 administrator@*mydomain*으로 로그인합니다.
3. vCenter Single Sign-On 사용자 구성 UI로 이동합니다.
   a. **홈** 메뉴에서 **관리**를 선택합니다.
   b. **Single Sign-On**에서 **사용자 및 그룹**을 클릭합니다.
4. 사용자 이름을 선택하고 **더 보기**를 클릭한 다음 **사용 안 함**을 클릭합니다.
5. **확인**을 클릭합니다.
6. 사용자를 다시 활성화하려면 **더 보기**를 클릭하고 **사용**을 클릭한 다음 **확인**을 클릭합니다.

vCenter Single Sign-On 사용자 삭제

vsphere.local 도메인에 있는 사용자를 vCenter Single Sign-On 관리 인터페이스에서 삭제할 수 있습니다. 로컬 운영 체제 사용자나 다른 도메인의 사용자는 vCenter Single Sign-On 관리 인터페이스에서 삭제할 수 없습니다.

경고 vsphere.local 도메인의 관리자를 삭제하면 더 이상 vCenter Single Sign-On에 로그인할 수 없습니다. 이 경우 vCenter Server 및 해당 구성 요소를 다시 설치해야 합니다.

절차

1 vSphere Client를 사용하여 vCenter Server에 로그인합니다.

2 administrator@vsphere.local 또는 vCenter Single Sign-On 관리자 그룹에 속한 다른 멤버의 사용자 이름과 암호를 지정합니다.

설치 시 다른 도메인을 지정한 경우에는 administrator@*mydomain*으로 로그인합니다.

3 vCenter Single Sign-On 사용자 구성 UI로 이동합니다.

a **홈** 메뉴에서 **관리**를 선택합니다.

b **Single Sign-On**에서 **사용자 및 그룹**을 클릭합니다.

4 **사용자**를 선택하고 드롭다운 메뉴에서 vsphere.local 도메인을 선택합니다.

5 사용자 목록에서 삭제할 사용자를 선택합니다.

6 **삭제**를 클릭합니다.

주의해서 진행하십시오. 이 작업은 실행 취소할 수 없습니다.

7 **제거**를 클릭합니다.

vCenter Single Sign-On 사용자 편집

vCenter Single Sign-On 관리 인터페이스에서 vCenter Single Sign-On 사용자의 암호 또는 기타 세부 정보를 변경할 수 있습니다. vsphere.local 도메인의 사용자 이름은 바꿀 수 없습니다. 따라서 administrator@vsphere.local은 이름을 바꿀 수 없습니다.

administrator@vsphere.local과 동일한 권한을 가진 추가 사용자를 생성할 수 있습니다.

vCenter Single Sign-On 사용자는 vCenter Single Sign-On vsphere.local 도메인에 저장됩니다.

vCenter Single Sign-On에서 vSphere Client 암호 정책을 검토할 수 있습니다. administrator@vsphere.local로 로그인하고 **관리** 메뉴에서 **구성 > 로컬 계정 > 암호 정책**을 선택합니다.

vCenter Single Sign-On 암호 정책 편집 항목을 참조하십시오.

절차

1 vSphere Client를 사용하여 vCenter Server에 로그인합니다.

2 administrator@vsphere.local 또는 vCenter Single Sign-On 관리자 그룹에 속한 다른 멤버의 사용자 이름과 암호를 지정합니다.

설치 시 다른 도메인을 지정한 경우에는 administrator@*mydomain*으로 로그인합니다.

3 vCenter Single Sign-On 사용자 구성 UI로 이동합니다.

a **홈** 메뉴에서 **관리**를 선택합니다.

b **Single Sign-On**에서 **사용자 및 그룹**을 클릭합니다.

4 **사용자**를 클릭합니다.

5 사용자를 선택하고 **편집**을 클릭합니다.

6 사용자 특성을 편집합니다.

사용자의 사용자 이름은 변경할 수 없습니다.

암호는 시스템의 암호 정책 요구 사항을 충족해야 합니다.

7 **저장**을 클릭합니다.

vCenter Single Sign-On 그룹 추가

vCenter Single Sign-On **그룹** 탭에는 기본적으로 로컬 도메인인 vsphere.local의 그룹이 표시됩니다. 그룹 멤버(주체)를 위한 컨테이너가 필요한 경우 그룹을 추가합니다.

vCenter Single Sign-On **그룹** 탭에서 다른 도메인(예: Active Directory 도메인)에 그룹을 추가할 수 없습니다.

vCenter Single Sign-On에 ID 소스를 추가하지 않는 경우 그룹 생성 및 사용자 추가가 로컬 도메인을 구성하는 데 도움이 될 수 있습니다.

절차

1 vSphere Client를 사용하여 vCenter Server에 로그인합니다.

2 administrator@vsphere.local 또는 vCenter Single Sign-On 관리자 그룹에 속한 다른 멤버의 사용자 이름과 암호를 지정합니다.

설치 시 다른 도메인을 지정한 경우에는 administrator@*mydomain*으로 로그인합니다.

3 vCenter Single Sign-On 사용자 구성 UI로 이동합니다.

a **홈** 메뉴에서 **관리**를 선택합니다.

b **Single Sign-On**에서 **사용자 및 그룹**을 클릭합니다.

4 **그룹**을 선택하고 **그룹 생성**을 클릭합니다.

5 그룹의 이름과 설명을 입력합니다.

그룹 이름에 허용되는 최대 문자 수는 300자입니다. 그룹을 생성한 후에는 그룹 이름을 변경할 수 없습니다.

6 **멤버 추가** 드롭다운 메뉴에서 그룹에 추가할 멤버가 포함된 ID 소스를 선택합니다.

외부 ID 제공자(예: AD FS)를 구성한 경우, 해당 ID 제공자의 도메인을 **멤버 추가** 드롭다운 메뉴에서 선택할 수 있습니다.

7 검색어를 입력합니다.

8 멤버를 선택합니다.

둘 이상의 멤버를 추가할 수 있습니다.

9 **완료**를 클릭합니다.

다음에 수행할 작업

vCenter Single Sign-On 그룹에 멤버 추가의 내용을 참조하십시오.

vCenter Single Sign-On 그룹에 멤버 추가

vCenter Single Sign-On 그룹 멤버는 하나 이상의 ID 소스에 속하는 사용자 또는 다른 그룹일 수 있습니다. vSphere Client에서 새 멤버를 추가할 수 있습니다.

배경 정보는 VMware 기술 자료 문서(https://kb.vmware.com/s/article/2095342)를 참조하십시오.

웹 인터페이스의 **그룹** 탭에 나열된 그룹은 vsphere.local 도메인에 속합니다. vCenter Single Sign-On 도메인의 그룹의 내용을 참조하십시오.

절차

1 vSphere Client를 사용하여 vCenter Server에 로그인합니다.

2 administrator@vsphere.local 또는 vCenter Single Sign-On 관리자 그룹에 속한 다른 멤버의 사용자 이름과 암호를 지정합니다.

   설치 시 다른 도메인을 지정한 경우에는 administrator@*mydomain*으로 로그인합니다.

3 vCenter Single Sign-On 사용자 구성 UI로 이동합니다.

   a **홈** 메뉴에서 **관리**를 선택합니다.

   b **Single Sign-On**에서 **사용자 및 그룹**을 클릭합니다.

4 **그룹**을 클릭하고 관리자 등의 그룹을 클릭합니다.

5 **편집**을 클릭합니다.

6 **도메인** 드롭다운 메뉴에서 그룹에 추가할 멤버가 포함된 ID 소스를 선택합니다.

   외부 ID 제공자(예: AD FS)를 구성한 경우, 해당 ID 제공자의 도메인을 **도메인** 드롭다운 메뉴에서 선택할 수 있습니다.

7 검색어를 입력합니다.

8 멤버를 선택합니다.

   둘 이상의 멤버를 추가할 수 있습니다.

9 vSphere+ 환경의 경우 **도메인** 드롭다운 메뉴에서 **VMware ID**를 선택한 경우 **사용자 이름** 필드에 CSP 계정의 이름을 입력합니다.

   참고 **사용자 이름** 필드에 CSP 계정의 이메일 주소를 입력합니다. VMwareID 도메인에서 CSP 계정을 검색할 수 없습니다.

10 **저장**을 클릭합니다.

vCenter Single Sign-On 그룹에서 멤버 제거

vSphere Client를 사용하여 vCenter Single Sign-On 그룹의 멤버를 제거할 수 있습니다. 그룹에서 멤버(사용자 또는 그룹)를 제거하는 경우 해당 멤버가 시스템에서 삭제되지는 않습니다.

절차

1 vSphere Client를 사용하여 vCenter Server에 로그인합니다.

2 administrator@vsphere.local 또는 vCenter Single Sign-On 관리자 그룹에 속한 다른 멤버의 사용자 이름과 암호를 지정합니다.

설치 시 다른 도메인을 지정한 경우에는 administrator@*mydomain*으로 로그인합니다.

3 vCenter Single Sign-On 사용자 구성 UI로 이동합니다.

a **홈** 메뉴에서 **관리**를 선택합니다.

b **Single Sign-On**에서 **사용자 및 그룹**을 클릭합니다.

4 **그룹**을 클릭하고 그룹을 선택합니다.

5 **편집**을 클릭합니다.

6 현재 멤버 목록에서 제거하려는 사용자 또는 그룹을 클릭합니다.

7 **완료**를 클릭합니다.

결과

사용자 또는 그룹이 그룹에서 제거되지만 시스템에서는 계속 사용할 수 있습니다.

vCenter Single Sign-On 암호 변경

로컬 도메인 vsphere.local에 속해 있는 사용자는 기본적으로 vSphere Client에서 본인의 vCenter Single Sign-On 암호를 변경할 수 있습니다. 다른 도메인의 사용자는 해당 도메인의 규칙에 따라 자신의 암호를 변경할 수 있습니다.

vCenter Single Sign-On 잠금 정책은 암호가 만료되는 시점을 결정합니다. 기본적으로 vCenter Single Sign-On 암호는 90일 후 만료되지만 관리자 암호(예: administrator@vsphere.loal의 암호)는 만료되지 않습니다. vCenter Single Sign-On 관리 인터페이스에는 암호가 만료되려고 할 때 주의가 표시됩니다.

참고 암호는 만료되지 않은 경우에만 변경할 수 있습니다.

암호가 만료된 경우에는 로컬 도메인의 관리자(기본적으로 administrator@vsphere.local)가 `dir-cli password reset` 명령을 사용하여 암호를 재설정할 수 있습니다. vCenter Single Sign-On 도메인의 관리자 그룹 멤버만 암호를 재설정할 수 있습니다.

절차

1 vSphere Client를 사용하여 vCenter Server에 로그인합니다.

2 administrator@vsphere.local 또는 vCenter Single Sign-On 관리자 그룹에 속한 다른 멤버의 사용자 이름과 암호를 지정합니다.

   설치 시 다른 도메인을 지정한 경우에는 administrator@*mydomain*으로 로그인합니다.

3 위쪽 탐색 창에서 사용자 이름을 클릭하여 풀다운 메뉴를 표시하고 **암호 변경**을 선택합니다.

4 현재 암호를 입력합니다.

5 새 암호를 입력하고 확인을 위해 한 번 더 입력합니다.

   암호는 암호 정책을 준수해야 합니다.

6 **확인**을 클릭합니다.

   또는 **Single Sign On > 사용자 및 그룹**을 선택하고 사용자를 선택한 다음 **편집**을 클릭할 수 있습니다.

기타 vSphere 인증 옵션

vSphere 7.0 이상에서는 외부 ID 제공자 페더레이션이 vCenter Server의 기본 인증 방법입니다. 스마트 카드(UPN 기반의 CAC 즉 Common Access Card) 또는 RSA SecurID 토큰을 사용한 인증도 계속 지원됩니다.

이중 인증 방법

정부 기관이나 대기업에는 2단계 인증이 필요한 경우가 많습니다. vSphere는 다음과 같은 2단계 인증 방법을 지원합니다.

외부 ID 제공자 페더레이션

외부 ID 제공자 페더레이션을 사용하면 다단계 인증을 비롯한 외부 ID 제공자가 지원하는 인증 메커니즘을 사용할 수 있습니다.

스마트 카드 인증

스마트 카드 인증의 경우 자신이 로그인하는 컴퓨터에 물리적 카드 판독기를 연결한 사용자만 액세스할 수 있습니다. CAC(Common Access Card) 인증이 한 가지 예입니다.

관리자는 스마트 카드 인증서가 CA에서 발급하는 유일한 클라이언트 인증서가 되도록 PKI를 배포할 수 있습니다. 이러한 배포의 경우 스마트 카드 인증서만 사용자에게 제공됩니다. 사용자가 인증서를 선택하면 PIN을 묻는 메시지가 표시됩니다. 물리적 카드 및 인증서와 일치하는 PIN을 모두 가진 사용자만 로그인할 수 있습니다.

RSA SecurID 인증

RSA SecurID 인증의 경우 올바르게 구성된 RSA Authentication Manager가 환경에 포함되어 있어야 합니다. vCenter Server가 RSA 서버를 가리키도록 구성되어 있고 RSA SecurID 인증이 활성화되어 있으면 사용자는 자신의 사용자 이름 및 토큰을 사용하여 로그인할 수 있습니다.

자세한 내용은 vSphere 블로그 게시물 RSA SecurID 설정을 참조하십시오.

참고 vCenter Single Sign-On은 네이티브 SecurID만 지원합니다. RADIUS 인증은 지원하지 않습니다.

vCenter Server 기본값이 아닌 인증 방법 지정

vSphere Client에서 또는 `sso-config` 스크립트를 사용하여 기본값이 아닌 인증 방법을 설정할 수 있습니다.

- 스마트 카드 인증의 경우 vSphere Client에서 또는 `sso-config`를 사용하여 vCenter Single Sign-On 설정을 수행할 수 있습니다. 설정은 스마트 카드 인증을 활성화하고 인증서 해지 정책을 구성하는 것을 포함합니다.
- RSA SecurID의 경우 `sso-config` 스크립트를 사용하여 도메인에 대해 RSA Authentication Manager를 구성하고 RSA 토큰 인증을 사용하도록 설정합니다. RSA SecurID 인증은 vSphere Client에서 구성할 수 없습니다. 하지만 RSA SecurID를 사용하도록 설정하면 해당 인증 방법이 vSphere Client에 나타납니다.

vCenter Server 인증 방법 결합

`sso-config`를 사용하여 각 인증 방법을 개별적으로 활성화하거나 비활성화할 수 있습니다. 처음에 이중 인증 방법을 테스트하는 동안은 사용자 이름과 암호 인증을 사용하도록 설정된 상태를 유지하고 테스트 후에는 인증 방법을 하나만 사용하도록 설정하십시오.

스마트 카드 인증 로그인

스마트 카드는 집적 회로 칩이 내장된 소형 플라스틱 카드입니다. 여러 정부 기관 및 대기업에서는 시스템 보안을 강화하고 보안 규정을 준수하기 위해 CAC(Common Access Card) 같은 스마트 카드를 사용합니다. 스마트 카드는 각 시스템에 스마트 카드 판독기가 포함되어 있는 환경에서 사용됩니다. 스마트 카드를 관리하는 스마트 카드 하드웨어 드라이버는 일반적으로 미리 설치되어 있습니다.

참고 vSphere 7.0 업데이트 2 이상은 vCenter Server에서 FIPS를 사용하도록 설정할 수 있습니다. "vSphere 보안" 설명서를 참조하십시오. FIPS를 사용하도록 설정한 경우 RSA SecureID 및 CAC 인증은 지원되지 않습니다. MFA 인증에는 외부 ID 제공자 페더레이션을 사용합니다. vCenter Server ID 제공자 페더레이션 구성의 내용을 참조하십시오.

vCenter Server 시스템에 로그인하는 사용자에게 다음과 같이 스마트 카드와 PIN 조합을 사용하여 인증하라는 메시지가 표시됩니다.

1 사용자가 스마트 카드를 스마트 카드 판독기에 넣으면 브라우저가 카드의 인증서를 읽습니다.

2 사용자에게 인증서를 선택하라는 메시지가 표시된 후 해당 인증서의 PIN을 묻는 메시지가 브라우저에 표시됩니다.

3 vCenter Single Sign-On은 스마트 카드의 인증서가 알려진 인증서인지 확인합니다. 해지 확인이 설정되어 있으면 vCenter Single Sign-On은 인증서가 해지되었는지 여부도 확인합니다.

4 인증서가 vCenter Single Sign-On에 알려진 인증서이고 해지된 인증서가 아니면, 사용자가 인증되며 자신에게 권한이 있는 작업을 수행할 수 있습니다.

참고 일반적으로 테스트 중에는 사용자 이름 및 암호 인증을 사용하도록 설정해 두는 것이 좋습니다. 테스트가 완료된 후에는 사용자 이름 및 암호 인증을 비활성화하고 스마트 카드 인증을 활성화합니다. 이후에는 vSphere Client에서 스마트 카드 로그인만 허용합니다. 시스템에서 루트 또는 관리자 권한을 가진 사용자만 vCenter Server에 직접 로그인하여 사용자 이름 및 암호 인증을 재활성화할 수 있습니다.

스마트 카드 인증 구성 및 사용

사용자가 vSphere Client에서 vCenter Server에 연결할 때 스마트 카드 인증이 필요하도록 환경을 설정할 수 있습니다.

스마트 카드 인증을 구성하려면 다음과 같은 개략적인 단계를 수행해야 합니다.

1 클라이언트 인증서를 요청하도록 vCenter Server 시스템 구성.

2 스마트 카드 구성 활성화.

vSphere Client 또는 `sso-config` 유틸리티를 사용하여 구성을 활성화할 수 있습니다.

3 인증서 해지 검사 사용자 지정.

vSphere Client 또는 `sso-config` 유틸리티를 사용하여 검사를 사용자 지정할 수 있습니다.

클라이언트 인증서를 요청하도록 vCenter Server 구성

스마트 카드 인증을 활성화하기 전에 클라이언트 인증서를 요청하도록 vCenter Server를 구성해야 합니다.

이 구성은 vCenter Server에서 자동으로 설정되고 열리는 포트 3128을 사용합니다.

사전 요구 사항

신뢰할 수 있는 클라이언트 CA 저장소를 생성하는 데 사용할 CA(인증 기관) 인증서를 vCenter Server 시스템에 복사합니다. 이 저장소에는 클라이언트 인증서에 대해 CA에서 발급한 신뢰할 수 있는 인증서가 포함되어 있어야 합니다. 여기서 클라이언트는 스마트 카드 프로세스가 최종 사용자에게 정보 요청 메시지를 표시하는 브라우저입니다.

참고 vCenter Server 7.0 이상은 HTTP/2 프로토콜을 지원합니다. vSphere Client를 포함하여, 모든 최신 브라우저 및 애플리케이션은 HTTP/2를 사용하여 vCenter Server에 연결합니다. 하지만 스마트 카드 인증을 위해서는 HTTP/1.1 프로토콜을 사용해야 합니다. 스마트 카드 인증을 활성화하면 HTTP/2에 대해 애플리케이션 계층 프로토콜 협상(ALPN, https://tools.ietf.org/html/rfc7301)이 비활성화되어 브라우저가 HTTP/2를 효과적으로 사용할 수 없게 됩니다. ALPN에 의존하지 않고 HTTP/2만 사용하는 애플리케이션은 계속 작동합니다.

스마트 카드 인증을 완료하려면 적절한 vCenter Server의 포트 3128/TCP에 대한 액세스가 클라이언트에 허용되어야 합니다. 액세스 권한이 부여되었는지 경계 방화벽을 확인합니다.

스마트 카드 로그인 중에 연결이 포트 3128로 리디렉션됩니다. 포트 3128은 미리 구성된 상호 인증 연결만 지원하며 직접 브라우저 끝점으로 사용되지 않습니다. HSTS 헤더를 반환하지 않습니다. 취약성 스캐너가 이 동작을 보고하는 경우 무시해도 됩니다.

절차

1 vCenter Server 셸에 루트 사용자로 로그인합니다.

2 정확한 경로와 PEM 이름(`/usr/lib/vmware-sso/vmware-sts/conf/clienttrustCA.pem`)을 사용하여 vCenter Server에 신뢰할 수 있는 클라이언트 CA 저장소를 생성합니다.

경고 정확한 경로와 PEM 이름(`/usr/lib/vmware-sso/vmware-sts/conf/clienttrustCA.pem`)을 사용해야 합니다.

a `/usr/lib/vmware-sso/` 디렉토리로 변경합니다.

```
cd /usr/lib/vmware-sso/
```

b 신뢰할 수 있는 클라이언트 CA 저장소를 생성하려면 신뢰할 수 있는 서명 인증서를 입력으로 사용하여 `openssl` 명령을 실행합니다. 예를 들어 다음 명령은 `xyzCompanySmartCardSigningCA.cer` 신뢰할 수 있는 서명 인증서에서 `clienttrustCA.pem` 파일을 생성합니다.

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

`openssl` 명령을 " > >" 연산자와 함께 실행하여 인증서를 추가하면 신뢰할 수 있는 클라이언트 CA 저장소에 인증서를 더 추가할 수 있습니다. 예를 들어 다음 명령은 기존 `clienttrustCA.pem` 파일에 `xyzCompanySmartCardSigningCA2.cer`를 추가합니다.

```
openssl x509 -inform PEM -in xyzCompanySmartCardSigningCA2.cer >> /usr/lib/vmware-sso/
vmware-sts/conf/clienttrustCA.pem
```

3 `clienttrustCA.pem` 파일의 컨텐츠에 스마트 카드 인증서에 서명한 신뢰할 수 있는 CA가 포함되어 있는지 확인하려면 `keytool` 명령을 실행합니다.

예:

```
keytool -printcert -file /usr/lib/vmware-sso/vmware-sts/conf/clienttrustCA.pem | grep -i
"owner\|sha1\|issuer:\|valid"
```

4 CA 이름이 스마트 카드 사용자 인증서 체인과 일치하는지 확인합니다.

예를 들어 다음 명령을 실행할 수 있습니다.

```
sso-config.sh -get_authn_policy -t vsphere.local | grep trusted
```

루트 및 중간 인증서에는 일치하는 지문, 이름, 유효한 날짜 등이 있어야 합니다.

참고 vSphere Client(**관리 > Single Sign-On > 구성 > ID 제공자 > 스마트 카드 인증 > 스마트 카드 인증 설정 > 신뢰할 수 있는 CA 인증서 > 추가**)를 사용할 수도 있습니다.

5 STS 서비스를 다시 시작합니다.

```
service-control --restart sts
```

vSphere Client를 사용하여 스마트 카드 인증 관리

vSphere Client에서 스마트 카드 인증을 활성화 및 비활성화하고, 로그인 배너를 사용자 지정하고, 해지 정책을 설정할 수 있습니다.

스마트 카드 인증을 활성화하고 다른 인증 방법을 비활성화한 경우 사용자는 스마트 카드 인증을 사용하여 로그인해야 합니다.

사용자 이름 및 암호 인증이 비활성화된 경우 스마트 카드 인증에 문제가 발생하면 사용자가 로그인할 수 없습니다. 이 경우 루트 또는 관리자 사용자가 vCenter Server 명령줄에서 사용자 이름 및 암호 인증을 설정할 수 있습니다. 다음 명령은 사용자 이름 및 암호 인증을 활성화합니다.

```
sso-config.sh -set_authn_policy -pwdAuthn true -t tenant_name
```

사전 요구 사항

- 환경에 엔터프라이즈 PKI(공개 키 인프라)가 설정되어 있고 인증서가 다음과 같은 요구 사항을 충족하는지 확인합니다.
  - UPN(사용자 계정 이름)이 SAN(주체 대체 이름) 확장의 Active Directory 계정에 해당해야 합니다.
  - 인증서가 [애플리케이션 정책] 또는 [확장 키 사용] 필드에 클라이언트 인증을 지정해야 하며 그렇지 않으면 브라우저에 인증서가 표시되지 않습니다.
- vCenter Single Sign-On에 Active Directory ID 소스를 추가합니다.
- Active Directory ID 소스에 속한 사용자 한 명 이상에게 vCenter Server 관리자 역할을 할당합니다. 그런 다음 이러한 사용자는 인증될 수 있으며 vCenter Server 관리자 권한이 있기 때문에 관리 작업을 수행할 수 있습니다.
- 역방향 프록시를 설정하고 물리적 시스템 또는 가상 시스템을 다시 시작했는지 확인합니다.

절차

1 인증서를 가져온 후 `sso-config` 유틸리티에서 볼 수 있는 폴더에 복사합니다.

a vCenter Server 콘솔에 직접 로그인하거나 SSH를 사용하여 로그인합니다.

b 다음과 같이 셸을 활성화합니다.

```
Command> shell
chsh -s "/bin/bash" root
chsh -s "bin/appliancesh" root
```

c WinSCP 또는 유사한 유틸리티를 사용하여 인증서를 vCenter Server의 `/usr/lib/vmware-sso/vmware-sts/conf` 디렉토리에 복사합니다.

d 필요한 경우 다음과 같이 셸을 비활성화합니다.

```
chsh -s "/bin/appliancesh" root
```

2 vSphere Client를 사용하여 vCenter Server에 로그인합니다.

3 administrator@vsphere.local 또는 vCenter Single Sign-On 관리자 그룹에 속한 다른 멤버의 사용자 이름과 암호를 지정합니다.

설치 시 다른 도메인을 지정한 경우에는 administrator@*mydomain*으로 로그인합니다.

4 구성 UI로 이동합니다.

a **홈** 메뉴에서 **관리**를 선택합니다.

b **Single Sign-On**에서 **구성**을 클릭합니다.

5 **ID 제공자** 탭에서 **스마트 카드 인증**을 클릭한 후 **편집**을 클릭합니다.

6 인증 방법을 선택하거나 선택 취소하고 **저장**을 클릭합니다.

RSA SecurID 인증은 이 웹 인터페이스에서 활성화 또는 비활성화할 수 없습니다. 그러나 명령줄에서 RSA SecurID를 활성화한 경우 해당 상태가 웹 인터페이스에 표시됩니다.

신뢰할 수 있는 CA 인증서 탭이 표시됩니다.

7 **신뢰할 수 있는 CA 인증서** 탭에서 다음을 수행합니다.

a **추가**를 클릭하고 **찾아보기**를 클릭합니다.

b 신뢰할 수 있는 CA 인증서를 선택하고 **추가**를 클릭합니다.

8 신뢰할 수 있는 CA 인증서를 더 추가하려면 7단계를 반복합니다.

다음에 수행할 작업

환경에 향상된 OCSP 구성이 필요할 수 있습니다.

- OCSP 응답이 스마트 카드의 서명 CA와 다른 CA에 의해 발급된 경우 OCSP 서명 CA 인증서를 제공합니다.
- 다중 사이트 배포 환경에서 각 vCenter Server 사이트에 대한 하나 이상의 로컬 OCSP 응답자를 구성할 수 있습니다. CLI를 사용하여 이러한 대체 OCSP 응답자를 구성할 수 있습니다. CLI를 사용하여 스마트 카드 인증 관리의 내용을 참조하십시오.

CLI를 사용하여 스마트 카드 인증 관리

`sso-config` 유틸리티를 사용하면 명령줄에서 스마트 카드 인증을 관리할 수 있습니다. 이 유틸리티는 모든 스마트 카드 구성 작업을 지원합니다.

다음 위치에서 `sso-config` 스크립트를 찾을 수 있습니다.

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

지원되는 인증 유형의 구성 및 해지 설정은 VMware Directory Service에 저장되며 vCenter Single Sign-On 도메인 내의 모든 vCenter Server 인스턴스에 복제됩니다.

사용자 이름 및 암호 인증이 비활성화된 경우 스마트 카드 인증에 문제가 발생하면 사용자가 로그인할 수 없습니다. 이 경우 루트 또는 관리자 사용자가 vCenter Server 명령줄에서 사용자 이름 및 암호 인증을 설정할 수 있습니다. 다음 명령은 사용자 이름 및 암호 인증을 활성화합니다.

```
sso-config.sh -set_authn_policy -pwdAuthn true -t tenant_name
```

기본 테넌트를 사용하는 경우 vsphere.local을 테넌트 이름으로 사용합니다.

해지 확인에 OCSP를 사용하는 경우 스마트 카드 인증서 AIA 확장에 지정된 기본 OCSP에 의존할 수 있습니다. 기본값을 재정의하고 하나 이상의 대체 OCSP 응답자를 구성할 수도 있습니다. 예를 들어 vCenter Single Sign-On 사이트에 대해 로컬인 OCSP 응답자를 설정하여 해지 확인 요청을 처리할 수 있습니다.

참고 인증서에 OCSP가 정의되어 있지 않은 경우 대신 CRL(인증서 해지 목록)을 사용합니다.

사전 요구 사항

- 환경에 엔터프라이즈 PKI(공개 키 인프라)가 설정되어 있고 인증서가 다음과 같은 요구 사항을 충족하는지 확인합니다.
  - UPN(사용자 계정 이름)이 SAN(주체 대체 이름) 확장의 Active Directory 계정에 해당해야 합니다.
  - 인증서가 [애플리케이션 정책] 또는 [확장 키 사용] 필드에 클라이언트 인증을 지정해야 하며 그렇지 않으면 브라우저에 인증서가 표시되지 않습니다.
- vCenter Single Sign-On에 Active Directory ID 소스를 추가합니다.
- Active Directory ID 소스에 속한 사용자 한 명 이상에게 vCenter Server 관리자 역할을 할당합니다. 그런 다음 이러한 사용자는 인증될 수 있으며 vCenter Server 관리자 권한이 있기 때문에 관리 작업을 수행할 수 있습니다.
- 역방향 프록시를 설정하고 물리적 시스템 또는 가상 시스템을 다시 시작했는지 확인합니다.

절차

1 인증서를 가져온 후 `sso-config` 유틸리티에서 볼 수 있는 폴더에 복사합니다.

   a 장치 콘솔에 직접 로그인하거나 SSH를 사용하여 로그인합니다.

   b 다음과 같이 장치 셸을 활성화합니다.

```
shell
chsh -s "/bin/bash" root
```

   c WinSCP 또는 유사한 유틸리티를 사용하여 인증서를 vCenter Server의 `/usr/lib/vmware-sso/vmware-sts/conf`에 복사합니다.

   d 필요한 경우 다음과 같이 셸을 비활성화합니다.

```
chsh -s "/bin/appliancesh" root
```

2 스마트 카드 인증을 활성화하려면 다음 명령을 실행합니다.

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

예:

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

인증서가 여러 개인 경우 인증서를 쉼표로 구분하되 쉼표 사이에 공백을 사용하지 않습니다.

3 다른 모든 인증 방법을 비활성화하려면 다음 명령을 실행합니다.

```
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 (선택 사항) 인증서 정책 허용 목록을 설정하려면 다음 명령을 실행합니다.

```
sso-config.sh -set_authn_policy -certPolicies policies
```

정책을 여러 개 지정하려면 다음과 같이 각 정책을 쉼표로 구분합니다.

```
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
```

이 허용 목록은 인증서의 인증서 정책 확장에서 허용되는 정책의 개체 ID를 지정합니다. X509 인증서는 인증서 정책 확장을 가질 수 있습니다.

5 (선택 사항) OCSP를 사용하여 해지 확인을 설정 및 구성합니다.

a OCSP를 사용하여 해지 확인을 설정합니다.

```
sso-config.sh  -set_authn_policy -t tenantName  -useOcsp true
```

b OCSP 응답자 링크가 인증서의 AIA 확장을 통해 제공되지 않는 경우 재정의하는 OCSP 응답자 URL 및 OCSP 기관 인증서를 제공합니다.

대체 OCSP는 각 vCenter Single Sign-On 사이트에 대해 구성됩니다. 페일오버를 허용할 vCenter Single Sign-On 사이트에 대한 2개 이상의 대체 OCSP 응답자를 지정할 수 있습니다.

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

참고 구성은 기본적으로 현재 vCenter Single Sign-On 사이트에 적용됩니다. 기타 vCenter Single Sign-On 사이트에 대한 대체 OCSP를 구성하는 경우에만 `siteID` 매개 변수를 지정합니다.

다음 예를 고려하십시오.

```
 .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 현재 대체 OCSP 응답자 설정을 표시하려면 이 명령을 실행합니다.

```
sso-config.sh -t tenantName -get_alt_ocsp]
```

d 현재 대체 OCSP 응답자 설정을 제거하려면 이 명령을 실행합니다.

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

6 (선택 사항) 구성 정보를 나열하려면 다음 명령을 실행합니다.

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

스마트 카드 인증에 대한 해지 정책 설정

인증서 해지 확인을 사용자 지정할 수 있으며 vCenter Single Sign-On이 해지된 인증서에 대한 정보를 검색하는 위치를 지정할 수 있습니다.

vSphere Client를 사용하거나 `sso-config` 스크립트를 사용하여 동작을 사용자 지정할 수 있습니다. 선택하는 설정은 CA에서 지원하는 기능에 따라 부분적으로 달라집니다.

- 해지 확인을 비활성화하면 vCenter Single Sign-On이 모든 CRL 또는 OCSP 설정을 무시합니다. vCenter Single Sign-On은 어떠한 인증서에도 확인을 수행하지 않습니다.
- 해지 확인을 활성화하면 PKI 설정에 따라 설정이 달라집니다.

  OCSP 전용

  발급하는 CA에서 OCSP 응답자를 지원하는 경우 **OCSP**를 활성화하고 **CRL을 OCSP에 대한 페일오버로 사용**을 비활성화합니다.

  CRL 전용

  발급하는 CA에서 OSCP를 지원하지 않는 경우, **CRL 확인**을 활성화하고 **OSCP 확인**을 비활성화합니다.

  OSCP 및 CRL 모두

  발급하는 CA에서 OCSP 응답자와 CRL 둘 모두 지원하는 경우, vCenter Single Sign-On은 OCSP 응답자부터 확인합니다. 응답자가 사용 가능한 상태가 아니거나 알 수 없는 상태를 반환하면 vCenter Single Sign-On은 CRL을 확인합니다. 이 경우에는 **OCSP 확인** 및 **CRL 확인** 둘 모두 활성화하고 **CRL을 OCSP에 대한 페일오버로 사용**을 활성화합니다.
- 해지 확인을 활성화하면 고급 사용자가 다음과 같은 추가 설정을 지정할 수 있습니다.

  OSCP URL

  기본적으로 vCenter Single Sign-On은 검증 중인 인증서에 정의된 OCSP 응답자의 위치를 확인합니다. 인증서에 기관 정보 액세스 확장이 없거나 확장을 재정의하려는 경우 위치를 명시적으로 지정할 수 있습니다.

  인증서의 CRL 사용

  기본적으로 vCenter Single Sign-On은 검증 중인 인증서에 정의된 CRL의 위치를 확인합니다. CRL 배포 지점 확장이 인증서에 없거나, 기본값을 재정의하려면 이 옵션을 비활성화합니다.

  CRL 위치

  인증서의 CRL 사용 옵션을 비활성화하고, CRL의 위치(파일 또는 HTTP URL)를 지정하려면 이 속성을 사용합니다.

인증서 정책을 추가하여 vCenter Single Sign-On이 허용하는 인증서를 추가적으로 제한할 수 있습니다.

사전 요구 사항

- 환경에 엔터프라이즈 PKI(공개 키 인프라)가 설정되어 있고 인증서가 다음과 같은 요구 사항을 충족하는지 확인합니다.
  - UPN(사용자 계정 이름)이 SAN(주체 대체 이름) 확장의 Active Directory 계정에 해당해야 합니다.
  - 인증서가 [애플리케이션 정책] 또는 [확장 키 사용] 필드에 클라이언트 인증을 지정해야 하며 그렇지 않으면 브라우저에 인증서가 표시되지 않습니다.
- 최종 사용자의 워크스테이션에서 vCenter Server 인증서를 신뢰하는지 확인합니다. 신뢰하지 않으면 브라우저가 인증을 시도하지 않습니다.
- vCenter Single Sign-On에 Active Directory ID 소스를 추가합니다.
- Active Directory ID 소스에 속한 사용자 한 명 이상에게 vCenter Server 관리자 역할을 할당합니다. 그런 다음 이러한 사용자는 인증될 수 있으며 vCenter Server 관리자 권한이 있기 때문에 관리 작업을 수행할 수 있습니다.

절차

1. vSphere Client를 사용하여 vCenter Server에 로그인합니다.
2. administrator@vsphere.local 또는 vCenter Single Sign-On 관리자 그룹에 속한 다른 멤버의 사용자 이름과 암호를 지정합니다.

   설치 시 다른 도메인을 지정한 경우에는 administrator@*mydomain*으로 로그인합니다.
3. 구성 UI로 이동합니다.
   a. **홈** 메뉴에서 **관리**를 선택합니다.
   b. **Single Sign-On**에서 **구성**을 클릭합니다.
4. **ID 제공자** 탭에서 **스마트 카드 인증**을 클릭합니다.
5. **인증서 해지**를 클릭한 후 **편집**을 클릭하여 해지 검사를 활성화하거나 비활성화합니다.
6. 현재 환경에 인증서 정책이 적용되어 있으면 **인증서 정책** 창에서 정책을 추가할 수 있습니다.

RSA SecurID 인증 설정

사용자가 RSA SecurID 토큰을 사용하여 로그인하도록 환경을 설정할 수 있습니다. SecurID 설정은 명령줄에서만 지원됩니다.

세부 정보는 RSA SecurID 설정에 관한 vSphere 블로그 게시물 두 개를 참조하십시오.

참고 RSA Authentication Manager에서 사용자 ID는 1~255개 ASCII 문자를 사용하는 고유 식별자여야 합니다. 문자 앰퍼샌드(&), 백분율(%), 보다 큼(>), 보다 작음(<) 및 작은 따옴표(`)는 허용되지 않습니다.

사전 요구 사항

- 환경에 RSA Authentication Manager가 올바르게 구성되어 있고 사용자에게 RSA 토큰이 있는지 확인합니다. RSA Authentication Manager 버전 8.0 이상이 필요합니다.

- RSA Manager가 사용하는 ID 소스가 vCenter Single Sign-On에 추가되었는지 확인합니다. vCenter Single Sign-On ID 소스 추가 또는 편집의 내용을 참조하십시오.
- RSA Authentication Manager 시스템에서 vCenter Server 호스트 이름을 확인할 수 있고 vCenter Server 시스템에서 RSA Authentication Manager 호스트 이름을 확인할 수 있는지 확인합니다.
- **액세스 > 인증 에이전트 > 구성 파일 생성**을 선택하여 RSA Manager에서 `sdconf.rec` 파일을 내보냅니다. `sdconf.rec` 파일을 찾으려면 결과 파일인 `AM_Config.zip`의 압축을 해제합니다.
- `sdconf.rec` 파일을 vCenter Server 노드에 복사합니다.

절차

1 `sso-config` 스크립트가 있는 디렉토리로 변경합니다.

```
/opt/vmware/bin
```

2 RSA SecurID 인증을 활성화하려면 다음 명령을 실행합니다.

```
sso-config.sh -t tenantName -set_authn_policy -securIDAuthn true
```

*tenantName*은 vCenter Single Sign-On 도메인의 이름이며, 기본값은 vsphere.local입니다.

3 (선택 사항) 다른 인증 방법을 비활성화하려면 다음 명령을 실행합니다.

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

4 현재 사이트에 있는 테넌트가 RSA 사이트를 사용하도록 환경을 구성하려면 다음 명령을 실행합니다.

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

예:

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

다음 옵션을 지정할 수 있습니다.

옵션	설명
siteID	선택적 Platform Services Controller 사이트 ID. Platform Services Controller는 사이트당 RSA Authentication Manager 인스턴스 또는 클러스터를 하나 지원합니다. 이 옵션을 명시적으로 지정하지 않으면 RSA 구성은 현재 Platform Services Controller 사이트에 적용됩니다. 이 옵션은 다른 사이트를 추가할 때만 사용합니다.
agentName	RSA Authentication Manager에 정의됩니다.
sdConfFile	RSA Manager에서 다운로드한 `sdconf.rec` 파일의 사본이며, RSA Manager에 대한 구성 정보(예: IP 주소)를 포함합니다.

5 (선택 사항) 테넌트 구성을 기본값이 아닌 값으로 변경하려면 다음 명령을 실행합니다.

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

일반적으로 기본값은 적절합니다. 예:

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

6 (선택 사항) ID 소스가 UPN(사용자 계정 이름)을 사용자 ID로 사용하지 않으면 ID 소스 userID 특성을 설정합니다. (LDAP ID 소스를 통한 Active Directory에서만 지원됩니다.)

userID 특성은 RSA userID로 사용할 LDAP 특성을 결정합니다.

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

예:

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

7 현재 설정을 표시하려면 다음 명령을 실행합니다.

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

결과

사용자 이름 및 암호 인증이 비활성화되고 RSA 인증이 활성화된 경우 사용자는 자신의 사용자 이름과 RSA 토큰으로 로그인해야 합니다. 사용자 이름과 암호 로그인은 더 이상 가능하지 않습니다.

참고 사용자 이름 형식 ***userID@domainName*** 또는 ***userID@domain_upn_suffix***를 사용합니다.

vSphere Client 로그인 페이지에 대한 로그인 메시지 관리

vSphere Client 로그인 페이지에 표시되는 메시지를 생성할 수 있습니다.

메시지, 고지 사항 또는 약관을 설정할 수 있습니다. 또한 로그인하기 전에 메시지 확인을 요구하도록 메시지를 구성할 수 있습니다.

vSphere Client 로그인 페이지에 대한 로그인 메시지 관리

vSphere Client 로그인 페이지에 로그인 메시지를 추가할 수 있습니다. 사용자 지정 로그인 메시지를 구성하고 사용자 동의를 위한 확인란을 제공할 수도 있습니다.

절차

1 vSphere Client를 사용하여 vCenter Server에 로그인합니다.

2 administrator@vsphere.local 또는 vCenter Single Sign-On 관리자 그룹에 속한 다른 멤버의 사용자 이름과 암호를 지정합니다.

   설치 시 다른 도메인을 지정한 경우에는 administrator@*mydomain*으로 로그인합니다.

3 구성 UI로 이동합니다.

   a **홈** 메뉴에서 **관리**를 선택합니다.

   b **Single Sign-On**에서 **구성**을 클릭합니다.

4 **로그인 메시지** 탭을 클릭합니다.

5 **편집**을 클릭하고 로그인 메시지를 구성합니다.

옵션	설명
로그인 메시지 표시	로그인 메시지를 사용하도록 설정하려면 **로그인 메시지 표시**를 켭니다. 이 스위치를 전환하지 않으면 로그인 메시지를 변경할 수 없습니다.
로그인 메시지	메시지 제목입니다. 기본적으로 **동의 확인란**이 켜져 있는 경우 로그인 메시지 텍스트는 `I agree to Terms and Conditions`입니다. 사용자 고유의 텍스트로 `Terms and Conditions`를 바꿔야 합니다. **동의 확인란**이 꺼져 있으면 `Login message`가 나타나고 그 위에 메시지를 입력할 수 있습니다.
동의 확인란	사용자가 로그인하기 전에 확인란을 클릭하도록 요구하려면 **동의 확인란**을 켭니다. 확인란 없이 메시지를 표시할 수도 있습니다.
로그인 메시지의 세부 정보	로그인 메시지를 클릭할 때 사용자에게 표시되는 메시지(예: 약관 텍스트)입니다. 이 텍스트 상자에 일부 세부 정보를 입력해야 합니다.

6 **저장**을 클릭합니다.

vCenter Single Sign-On 보안 모범 사례

vCenter Single Sign-On 보안 모범 사례를 따라 vSphere 환경을 보호합니다.

vSphere 인증 인프라는 vSphere 환경의 보안을 향상합니다. 인프라가 손상되지 않도록 하려면 이러한 vCenter Single Sign-On 모범 사례를 따릅니다.

암호 만료 확인

기본 vCenter Single Sign-On 암호 정책의 암호 지속 시간은 90일입니다. 90일 후 암호가 만료되고 더 이상 로그인할 수 없습니다. 만료를 확인하고 적시에 암호를 새로 고칩니다.

네트워크 시간 프로토콜 구성

NTP(네트워크 시간 프로토콜)를 사용하여 모든 시스템이 동일한 상대적 시간 소스(관련 지역화 오프셋 포함)를 사용하며 상대적 시간 소스를 합의된 시간 표준(예: 협정 세계시—UTC)에 연관시킬 수 있는지 확인합니다. 동기화된 시스템은 vCenter Single Sign-On 인증서 유효성 및 기타 vSphere 인증서의 유효성에 필수적입니다.

또한 NTP는 로그 파일의 침입자 추적을 용이하게 합니다. 잘못된 시간 설정은 공격을 감지하기 위해 로그 파일을 검사하고 연관시키기 어렵게 할 뿐 아니라 감사를 부정확하게 할 수 있습니다.

NTP를 사용한 시간 동기화 구성에 대한 지침은 "vSphere 보안" 설명서를 참조하십시오.

vCenter Server 인증 문제 해결

5

다음 항목에서는 vCenter Server 인증 문제의 해결을 위한 시작 지점을 제공합니다. 이 설명서 센터와 VMware 기술 자료 시스템에서 추가 포인터를 검색하십시오.

다음으로 아래 항목을 읽으십시오.

- Lookup Service 오류의 원인 확인
- Active Directory 도메인 인증을 사용하여 로그인할 수 없음
- 사용자 계정 잠김으로 인한 vCenter Server 로그인 실패
- VMware 디렉토리 서비스 복제에 시간이 많이 걸릴 수 있음
- vCenter Server 지원 번들 내보내기
- vCenter Server 인증 서비스 로그 참조

Lookup Service 오류의 원인 확인

vCenter Single Sign-On 설치 시 vCenter Server 또는 vSphere Client를 나타내는 오류가 표시됩니다.

문제

vCenter Server 및 Web Client 설치 관리자에 `Could not contact Lookup Service. Please check VM_ssoreg.log...` 오류가 표시됩니다.

원인

이 문제의 원인은 호스트 시스템의 클럭이 동기화되지 않았거나, 방화벽이 차단하고 있거나, 서비스를 시작해야 하는 등 여러 가지입니다.

해결책

1. vCenter Single Sign-On, vCenter Server 및 Web Client를 실행하는 호스트 시스템의 클럭이 동기화되었는지 확인합니다.
2. 오류 메시지에 나와 있는 특정 로그 파일을 확인합니다.

   오류 메시지에서 시스템 임시 폴더는 `%TEMP%`를 의미합니다.

3 해당 로그 파일 내에서 다음과 같은 오류 메시지를 검색합니다.

로그 파일에는 모든 설치 시도에 대한 출력 메시지가 포함되어 있습니다. `Initializing registration provider...`이 표시된 마지막 메시지를 찾습니다.

메시지	원인 및 해결 방법
`java.net.ConnectException: Connection timed out: connect`	IP 주소가 잘못되었거나, 방화벽이 vCenter Single Sign-On으로의 액세스를 차단하고 있거나, vCenter Single Sign-On이 오버로드된 경우입니다. 방화벽에 의해 vCenter Single Sign-On 포트(기본값: 7444)가 차단되고 있지 않은지 확인합니다. 또한 vCenter Single Sign-On이 설치되어 있는 시스템에 사용 가능한 CPU, I/O 및 RAM 용량이 충분한지 확인합니다.
`java.net.ConnectException: Connection refused: connect`	IP 주소 또는 FQDN이 잘못되었고 vCenter Single Sign-On 서비스가 아직 시작되지 않았거나, 시작된 지 1분이 지나지 않은 경우입니다. vCenter Single Sign-On vmware-sso 데몬의 상태를 확인하여 vCenter Single Sign-On이 작동 중인지 확인합니다. 서비스를 다시 시작합니다. 다시 시작으로 문제를 해결할 수 없으면 "vSphere 문제 해결 가이드" 의 복구 섹션을 참조하십시오.
`Unexpected status code: 404. SSO Server failed during initialization`	vCenter Single Sign-On을 다시 시작합니다. 다시 시작으로 문제를 해결할 수 없으면 "vSphere 문제 해결 가이드" 의 복구 섹션을 참조하십시오.
UI에 나와 있는 오류가 `Could not connect to vCenter Single Sign-On` 로 시작하는 경우입니다.	또한 `SslHandshakeFailed`라는 반환 코드도 표시됩니다. vCenter Single Sign-On 호스트로 확인되는, 지정된 IP 주소나 FQDN이 vCenter Single Sign-ON을 설치할 때 사용한 주소와 다르다는 것을 나타냅니다. `VM_ssoreg.log`에서 다음 메시지가 포함된 줄을 찾습니다. `host name in certificate did not match: <install-configured FQDN or IP> != <A> or <B> or <C>` 여기서 A는 vCenter Single Sign-On을 설치할 때 입력한 FQDN이며, B와 C는 시스템에서 대신 사용할 수 있게 생성된 FQDN입니다. 로그 파일에서 `!=` 기호의 오른쪽에 나와 있는 FQDN을 사용하도록 구성을 수정합니다. 대부분의 경우 vCenter Single Sign-On 설치 시 지정한 FQDN을 사용합니다. 사용할 수 있는 대체 FQDN이 네트워크 구성에 없는 경우에는 vCenter Single Sign-On SSL 구성을 복구해야 합니다.

Active Directory 도메인 인증을 사용하여 로그인할 수 없음

vSphere Client에서 vCenter Server 구성 요소에 로그인합니다. Active Directory 사용자 이름 및 암호를 사용합니다. 인증이 실패합니다.

문제

Active Directory ID 소스를 vCenter Single Sign-On에 추가해도 사용자가 vCenter Server에 로그인할 수 없습니다.

원인

사용자가 사용자 이름 및 암호를 사용하여 기본 도메인에 로그인합니다. 다른 모든 도메인에 로그인할 때는 도메인 이름을 포함해야 합니다(user@domain 또는 DOMAIN\user).

해결책

모든 vCenter Single Sign-On 배포에 대해 기본 ID 소스를 변경할 수 있습니다. 변경 후 사용자는 사용자 이름 및 암호만 사용하여 기본 ID 소스에 로그인할 수 있습니다.

Active Directory 포리스트 내에 하위 도메인을 가진 통합 Windows 인증 ID 소스를 구성하려면 VMware 기술 자료 문서(https://kb.vmware.com/s/article/2070433)를 참조하십시오. 기본적으로 통합 Windows 인증은 Active Directory 포리스트의 루트 도메인을 사용합니다.

기본 ID 소스를 변경한 후에도 문제가 해결되지 않으면 다음과 같은 추가 문제 해결 단계를 수행합니다.

1 vCenter Server와 Active Directory 도메인 컨트롤러 간에 클럭을 동기화합니다.

2 각 도메인 컨트롤러의 PTR(포인터 레코드)이 Active Directory 도메인 DNS 서비스에 있으며

   도메인 컨트롤러의 PTR 레코드 정보가 컨트롤러의 DNS 이름과 일치하는지 확인합니다. vCenter Server를 사용하는 경우 다음 명령을 실행하여 작업을 수행합니다.

   a 도메인 컨트롤러를 나열하려면 다음 명령을 실행합니다.

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

   다음 예와 같이 관련 주소가 응답 섹션(ANSWER SECTION)에 표시됩니다.

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

   b 각 도메인 컨트롤러에 대해 다음 명령을 실행하여 정방향 및 역방향 분석을 확인합니다.

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

   다음 예와 같이 관련 주소가 응답 섹션(ANSWER SECTION)에 표시됩니다.

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

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

   다음 예와 같이 관련 주소가 응답 섹션(ANSWER SECTION)에 표시됩니다.

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

3 이렇게 해도 문제가 해결되지 않으면 vCenter Server를 Active Directory 도메인에서 제거한 후 도메인에 다시 가입합니다. "vCenter Server 구성" 설명서를 참조하십시오.

4 vCenter Server에 연결된 모든 브라우저 세션을 닫고 모든 서비스를 다시 시작합니다.

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

사용자 계정 잠김으로 인한 vCenter Server 로그인 실패

vSphere Client 로그인 페이지에서 vCenter Server에 로그인할 때 계정이 잠겨 있다는 오류가 발생합니다.

문제

몇 차례의 로그인 시도가 실패하면 vCenter Single Sign-On을 사용하여 vSphere Client에 로그인할 수 없습니다. 이 경우 계정이 잠겼다는 메시지가 표시됩니다.

원인

실패한 최대 로그인 시도 횟수를 초과한 것입니다.

해결책

- 시스템 도메인(기본적으로 vsphere.local)의 사용자로 로그인을 시도한 경우 vCenter Single Sign-On 관리자에게 계정 잠금 해제를 요청하십시오. 잠금이 만료되도록 잠금 정책에 설정된 경우에는 계정 잠금이 해제될 때까지 기다릴 수 있습니다. vCenter Single Sign-On 관리자는 CLI 명령을 사용하여 사용자의 계정을 잠금 해제할 수 있습니다.
- Active Directory 또는 LDAP 도메인의 사용자로 로그인하는 경우 Active Directory 또는 LDAP 관리자에게 계정 잠금 해제를 요청하십시오.

VMware 디렉토리 서비스 복제에 시간이 많이 걸릴 수 있음

환경에 고급 연결 모드를 통해 연결된 여러 개의 vCenter Server 인스턴스가 있으면 vCenter Server 인스턴스 중 하나를 사용할 수 없더라도 환경은 계속 작동합니다. vCenter Server를 다시 사용할 수 있게 되면 사용자 데이터 및 기타 정보는 고급 연결 모드를 통해 연결된 파트너를 통해 보통 30초 이내에 복제됩니다. 하지만 특정 상황에서는 복제에 시간이 많이 걸릴 수 있습니다.

문제

환경 내 여러 위치에 여러 개의 vCenter Server 인스턴스가 있을 때 vCenter Server 하나를 사용할 수 없는 상황에서 많은 변경 작업을 수행하면, VMware 디렉토리 서비스 인스턴스 전체에 복제가 곧바로 표시되지 않습니다. 예를 들어 다른 인스턴스에서 사용 가능 상태의 vCenter Server 인스턴스에 새 사용자를 추가한 경우 복제 완료 전까지는 새 사용자가 표시되지 않습니다. 고급 연결 모드 토폴로지에 따라 복제에 많은 시간이 걸릴 수도 있습니다.

원인

정상 작동 중에는 한 vCenter Server 인스턴스(노드)의 vmdir(VMware Directory Service) 인스턴스를 변경하면 이 변경 내용은 약 30초 내에 직접 복제 파트너에 표시됩니다. 복제 토폴로지에 따라 한 노드의 변경 내용을 중간 노드를 통해 전파해야 각 노드의 각 vmdir 인스턴스에 도착할 수도 있습니다. 복제되는 정보에는 사용자 정보, 인증서 정보, VMware vMotion으로 생성, 복제 또는 마이그레이션되는 가상 시스템의 라이센스 정보 등이 포함됩니다.

네트워크가 중단되거나 노드를 사용할 수 없는 등과 같은 이유로 복제 링크가 끊기면 페더레이션의 변경 내용이 융합되지 않습니다. 사용할 수 없는 노드가 복원되면 각 노드는 모든 변경 내용을 가져오려고 시도합니다. 결과적으로 모든 vmdir 인스턴스가 일관된 상태로 융합되지만 하나의 노드를 사용할 수 없는 기간 동안 많은 변경이 발생한 경우에는 일관된 상태가 될 때까지 시간이 걸릴 수 있습니다.

해결책

복제 수행 중에도 환경은 정상적으로 작동합니다. 1시간 넘게 지속되는 경우가 아니면 문제 해결을 시도하지 마십시오.

vCenter Server 지원 번들 내보내기

vSphere Client에서 또는 API를 사용하여 vCenter Server 서비스에 대한 로그 파일이 포함된 지원 번들을 내보낼 수 있습니다. 내보내기를 완료한 후에는 로그를 로컬에서 확인하거나 VMware 지원팀에 번들을 보낼 수 있습니다.

API에 대한 자세한 내용은 "vCenter Server 관리 프로그래밍 가이드" 를 참조하십시오.

사전 요구 사항

vCenter Server가 배포되고 실행 중인지 확인합니다.

절차

1. 웨부 브라우저에서 vCenter Server 구성 관리 인터페이스(https://*vcenter_server_ip*:5480)에 연결합니다.
2. vCenter Server에 루트 사용자로 로그인합니다.
3. **작업** 메뉴에서 **지원 번들 생성**을 선택합니다.
4. 브라우저 설정으로 인해 즉시 다운로드할 수 없는 경우를 제외하고는 지원 번들이 로컬 시스템에 저장됩니다.

vCenter Server 인증 서비스 로그 참조

vCenter Server 인증 서비스는 syslog를 사용하여 로깅합니다. 로그 파일을 검토하여 실패 원인을 파악할 수 있습니다.

표 5-1. vCenter Server 인증 서비스 로그

서비스	설명
VMware Directory Service	기본적으로 vmdir 로깅은 `/var/log/messages` 또는 `/var/log/vmware/vmdird/`로 이동합니다. 배포 중에 나타나는 문제의 경우 `/var/log/vmware/vmdir/vmafdvmdirclient.log`에도 유용한 문제 해결 데이터가 포함될 수 있습니다.
VMware Single Sign-On	vCenter Single Sign-On 로깅은 `/var/log/vmware/sso/`로 이동합니다.

표 5-1. vCenter Server 인증 서비스 로그 (계속)

서비스	설명
VMCA(VMWare Certificate Authority)	VMCA 서비스 로그는 `/var/log/vmware/vmcad/vmcad-syslog.log`에 있습니다.
VECS(VMware Endpoint 인증서 저장소)	VECS 서비스 로그는 `/var/log/vmware/vmafdd/vmafdd-syslog.log`에 있습니다.
VMware Lookup Service	조회 서비스 로그는 `/var/log/vmware/sso/lookupServer.log`에 있습니다.