

vSphere 보안

업데이트 2

수정 날짜: 2022년 4월 27일

VMware vSphere 6.0

VMware ESXi 6.0

vCenter Server 6.0

다음 VMware 웹 사이트에서 최신 기술 문서를 확인할 수 있습니다.

<https://docs.vmware.com/kr/>

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

VMware 코리아
서울시 강남구
영동대로 517
아셈타워 13층
(우) 06164
전화: +82 2 3016 6500
팩스: +82 2 3016 6501
www.vmware.com/kr

Copyright © 2009-2022 VMware, Inc. All rights reserved. [저작권 및 상표 정보](#)

목차

vSphere 보안 정보 13

업데이트된 정보 15

1 vSphere 환경의 보안 17

ESXi 하이퍼바이저 보안 17

vCenter Server 시스템 및 관련 서비스 보안 19

가상 시스템 보안 20

가상 네트워킹 계층 보호 21

vSphere 환경의 암호 22

보안 모범 사례 및 리소스 23

2 vCenter Single Sign-On으로 vSphere 인증 25

vCenter Single Sign-On 이해 26

vCenter Single Sign-On으로 환경을 보호하는 방법 26

vCenter Single Sign-On 구성 요소 28

vCenter Single Sign-On이 설치에 미치는 영향 29

vCenter Single Sign-On이 업그레이드에 미치는 영향 30

vSphere와 함께 vCenter Single Sign-On 사용 32

vsphere.local 도메인의 그룹 34

vCenter Server 암호 요구 사항 및 잠금 동작 35

vCenter Single Sign-On ID 소스 구성 36

vCenter Single Sign-On을 사용하는 vCenter Server에 대한 ID 소스 37

vCenter Single Sign-On의 기본 도메인 설정 39

vCenter Single Sign-On ID 소스 추가 39

Active Directory ID 소스 설정 41

Active Directory LDAP 서버 및 OpenLDAP 서버 ID 소스 설정 42

vCenter Single Sign-On ID 소스 편집 43

vCenter Single Sign-On ID 소스 제거 44

Windows 세션 인증을 사용하는 vCenter Single Sign-On 사용 44

vCenter Server 이중 인증 45

vCenter Single Sign-On을 위한 스마트 카드 인증 구성 46

명령줄을 사용하여 스마트 카드 인증 구성 47

Platform Services Controller 웹 인터페이스를 사용하여 스마트 카드 인증 관리 50

스마트 카드 인증에 대한 해지 정책 설정 53

RSA SecurID 인증 설정 54

로그인 배너 관리	57
vCenter Single Sign-On을 다른 서비스 제공자의 ID 제공자로 사용	57
SAML 서비스 제공자 추가	58
STS(Security Token Service)	59
장치에 새 STS 서명 인증서 생성	60
vCenter Windows 설치에서 새 STS 서명 인증서 생성	61
보안 토큰 서비스 인증서 새로 고침	63
LDAPS SSL 인증서의 만료 날짜 확인	64
vCenter Single Sign-On 정책 관리	65
vCenter Single Sign-On 암호 정책 편집	65
vCenter Single Sign-On 잠금 정책 편집	66
vCenter Single Sign-On 토큰 정책 편집	67
vCenter Single Sign-On 사용자 및 그룹 관리	68
vCenter Single Sign-On 사용자 추가	69
vCenter Single Sign-On 사용자 사용 안 함/사용	70
vCenter Single Sign-On 사용자 삭제	70
vCenter Single Sign-On 사용자 편집	71
vCenter Single Sign-On 그룹 추가	71
vCenter Single Sign-On 그룹에 멤버 추가	72
vCenter Single Sign-On 그룹에서 멤버 제거	72
vCenter Single Sign-On 솔루션 사용자 삭제	73
vCenter Single Sign-On 암호 변경	74
vCenter Single Sign-On 보안 모범 사례	75
vCenter Single Sign-On 문제 해결	75
Lookup Service 오류의 원인 확인	75
Active Directory 도메인 인증을 사용하여 로그인할 수 없음	76
사용자 계정 잠김으로 인한 vCenter Server 로그인 실패	78
VMware 디렉토리 서비스 복제에 시간이 많이 걸릴 수 있음	78
3 vSphere 보안 인증서	80
다양한 솔루션 경로에 대한 인증서 요구 사항	81
인증서 관리 개요	84
인증서 교체 개요	86
vSphere 6.0에서 인증서를 사용하는 위치	89
VMCA 및 VMware 핵심 ID 서비스	91
VMware Endpoint 인증서 저장소 개요	91
인증서 해지 관리	93
대규모 배포에서 인증서 교체	93
Platform Services Controller 웹 인터페이스를 사용하여 인증서 관리	95
Platform Services Controller 웹 인터페이스에서 인증서 저장소 탐색	96

Platform Services Controller 웹 인터페이스에서 인증서를 새로운 VMCA 서명 인증서로 교체	97
Platform Services Controller 웹 인터페이스에서 WMCA를 중간 인증 기관으로 만들기	99
사용자 지정 인증서를 사용하도록 Platform Services Controller에서 시스템 설정	101
vSphere Certificate Manager를 사용하여 인증서 서명 요청 생성(사용자 지정 인증서)	101
신뢰할 수 있는 루트 인증서를 인증서 저장소에 추가	102
Platform Services Controller에서 사용자 지정 인증서 추가	103
vSphere Certificate Manager 유틸리티를 사용하여 인증서 관리	104
이전 인증서를 다시 게시하여 직전에 수행한 작업 되돌리기	105
모든 인증서 재설정	106
새 VMCA 루트 인증서 다시 생성 및 모든 인증서 교체	106
VMCA를 중간 CA(인증 기관)로 만들기(인증서 관리자)	107
vSphere Certificate Manager를 사용하여 CSR 생성 및 루트 인증서(중간 CA) 준비	107
사용자 지정 서명 인증서로 VMCA 루트 인증서 교체 및 모든 인증서 교체	108
VMCA 인증서로 시스템 SSL 인증서 교체(중간 CA)	110
VMCA 인증서로 솔루션 사용자 인증서 교체(중간 CA)	111
모든 인증서를 사용자 지정 인증서로 교체(인증서 관리자)	112
vSphere Certificate Manager를 사용하여 인증서 서명 요청 생성(사용자 지정 인증서)	112
시스템 SSL 인증서를 사용자 지정 인증서로 교체	113
솔루션 사용자 인증서를 사용자 지정 인증서로 교체	114
수동 인증서 교체	116
서비스의 시작 및 중지 이해	116
새 VMCA 서명된 인증서로 기존 VMCA 서명된 인증서 교체	116
새 VMCA 서명 루트 인증서 생성	117
VMCA 서명된 인증서로 시스템 SSL 인증서 교체	119
새 VMCA 서명된 인증서로 솔루션 사용자 인증서 교체	122
혼합 모드 환경에서 VMware 디렉토리 서비스 인증서 교체	127
중간 CA(인증 기관)로 VMCA 사용	128
루트 인증서 교체(중간 CA)	129
시스템 SSL 인증서 교체(중간 CA)	132
솔루션 사용자 인증서 교체(중간 CA)	135
VMware 디렉토리 서비스 인증서 교체	140
혼합 모드 환경에서 VMware 디렉토리 서비스 인증서 교체	141
vSphere와 함께 타사 인증서 사용	142
인증서 요청 및 사용자 지정 루트 인증서 가져오기	143
시스템 SSL 인증서를 사용자 지정 인증서로 교체	145
솔루션 사용자 인증서를 사용자 지정 인증서로 교체	147
VMware 디렉토리 서비스 인증서 교체	148
혼합 모드 환경에서 VMware 디렉토리 서비스 인증서 교체	149
CLI 명령으로 인증서 및 서비스 관리	150
인증서 관리 작업에 필요한 권한	151

certool 구성 변경	152
certool 초기화 명령 참조	153
certool 관리 명령 참조	156
vecs-cli 명령 참조	158
dir-cli 명령 참조	162
vSphere Web Client를 사용하여 vCenter 인증서 보기	167
vCenter 인증서 만료 경고의 임계값 설정	168

4 vSphere 사용 권한 및 사용자 관리 작업 169

vSphere의 권한 부여 이해	170
vCenter Server 권한 모델 이해	170
사용 권한의 계층적 상속	172
여러 가지 사용 권한 설정	174
예 1: 여러 사용 권한의 상속	175
예 2: 상위 사용 권한을 재정의하는 하위 사용 권한	175
예 3: 그룹 역할을 재정의하는 사용자 역할	176
vCenter 구성 요소에 대한 사용 권한 관리	176
인벤토리 개체에 사용 권한 추가	177
사용 권한 변경	178
사용 권한 제거	179
사용 권한 유효성 검사 설정 변경	179
글로벌 사용 권한	180
글로벌 사용 권한 추가	181
태그 개체에 대한 사용 권한	181
역할을 사용하여 권한 할당	183
vCenter Server 시스템 역할	184
사용자 지정 역할 생성	185
역할 복제	185
역할 편집	186
역할 및 권한에 대한 모범 사례	186
일반 작업에 필요한 권한	187

5 ESXi 호스트 보안 190

스크립트를 사용하여 호스트 구성 설정 관리	191
호스트 프로파일을 사용하여 ESXi 호스트 구성	192
일반 ESXi 보안 권장 사항	193
ESXi 암호 및 계정 잠금	194
ESXi 네트워킹 보안 권장 사항	196
MOB(Managed Object Browser) 사용 안 함	197
인증(SSH) 키 사용 안 함	197

ESXi 호스트에 대한 인증서 관리	198
호스트 업그레이드 및 인증서	200
ESXi 인증서 기본 설정	201
여러 ESXi 호스트에 대한 인증서 만료 정보 보기	202
단일 ESXi 호스트에 대한 인증서 세부 정보 보기	202
ESXi 인증서 갱신 또는 새로 고침	203
인증서 기본 설정 변경	204
인증서 모드 전환 이해	204
인증서 모드 변경	206
ESXi SSL 인증서 및 키 교체	207
ESXi 인증서 서명 요청에 대한 요구 사항	208
ESXi Shell에서 기본 인증서 및 키 교체	208
vifs 명령을 사용하여 기본 인증서 및 키 교체	209
HTTPS PUT를 사용하여 기본 인증서 교체	210
vCenter Server TRUSTED_ROOTS 스토어 업데이트(사용자 지정 인증서)	210
Auto Deploy와 함께 사용자 지정 인증서 사용	211
ESXi 인증서 및 키 파일 복원	213
보안 프로파일을 사용하여 호스트 사용자 지정	214
ESXi 방화벽 구성	214
ESXi 방화벽 설정 관리	215
ESXi 호스트에 대해 허용되는 IP 주소 추가	215
ESXi 호스트에 대해 들어오고 나가는 방화벽 포트	216
NFS 클라이언트 방화벽 동작	219
ESXi ESXCLI 방화벽 명령	220
보안 프로파일에서 ESXi 서비스 사용자 지정	220
보안 프로파일에서 서비스 사용 또는 사용 안 함	222
잠금 모드	223
잠금 모드 동작	224
vSphere Web Client를 사용하여 잠금 모드 사용	226
vSphere Web Client를 사용하여 잠금 모드 사용 안 함	226
Direct Console User Interface에서 정상 잠금 모드 사용 또는 사용 안 함	227
잠금 모드에서 액세스 권한을 가진 계정 지정	228
호스트 및 VIB의 수락 수준 확인	229
ESXi에 대한 사용 권한 할당	231
루트 사용자 권한	232
vpxuser 권한	232
dcui 사용자 권한	233
Active Directory를 통해 ESXi 사용자 관리	233
vSphere Authentication Proxy 설치 또는 업그레이드	233
Active Directory를 사용하도록 호스트 구성	234

디렉토리 서비스 도메인에 호스트 추가	235
디렉토리 서비스 설정 보기	236
vSphere Authentication Proxy 사용	236
vSphere Authentication Proxy 설치 또는 업그레이드	237
인증에 vSphere Authentication Proxy를 사용하도록 호스트 구성	238
vSphere Authentication Proxy 설정	239
vSphere Authentication Proxy 인증서 내보내기	240
프록시 서버 인증서를 ESXi로 가져오기	240
vSphere Authentication Proxy를 사용하여 도메인에 호스트 추가	241
ESXi 호스트의 인증 프록시 인증서 교체	242
ESXi 보안 모범 사례	242
PCI와 PCIe 디바이스 및 ESXi	243
ESXi에 대한 스마트 카드 인증 구성	244
스마트 카드 인증 사용	244
스마트 카드 인증 사용 안 함	245
연결 문제의 경우 사용자 자격 증명 인증	245
잠금 모드에서 스마트 카드 인증 사용	245
ESXi SSH 키	246
SSH 보안	246
vifs 명령을 사용하여 SSH Key 업로드	247
HTTPS PUT를 사용하여 SSH 키 업로드	247
ESXi Shell 사용	248
vSphere Web Client를 사용하여 ESXi Shell에 액세스할 수 있도록 설정	249
vSphere Web Client에서 ESXi Shell 가용성에 대한 시간 초과 설정 생성	250
vSphere Web Client에서 유틸리티 ESXi Shell 세션에 대한 시간 초과 설정 생성	250
DCUI(Direct Console User Interface)를 사용하여 ESXi Shell에 액세스할 수 있도록 설정	251
Direct Console User Interface에서 ESXi Shell 가용성에 대한 시간 초과 설정 생성	252
유틸리티 ESXi Shell 세션에 대한 시간 제한 설정 생성	252
문제 해결을 위해 ESXi Shell에 로그인	253
ESXi 웹 프록시 설정 수정	253
vSphere Auto Deploy 보안 고려 사항	254
ESXi 로그 파일 관리	254
ESXi 호스트의 Syslog 구성	255
ESXi 로그 파일 위치	256
Fault Tolerance 로깅 트래픽 보안	257
6 vCenter Server 시스템 보안	258
vCenter Server 보안 모범 사례	258
vCenter Server 액세스 제어에 대한 모범 사례	258
vCenter Server 암호 정책 설정	260

vCenter Server Windows 호스트 보호	260
실패한 설치에서 만료되거나 해지된 인증서 및 로그 제거	261
vCenter Server 네트워크 연결 제한	261
Linux 클라이언트 사용 제한 고려	262
설치된 플러그인 검사	262
vCenter Server Appliance 보안 모범 사례	263
기존 ESXi 호스트 지문 확인	263
NFC(Network File Copy)를 통한 SSL 인증서 유효성 검사 사용 확인	264
vCenter Server TCP 및 UDP 포트	264
CIM 기반 하드웨어 모니터링 도구 액세스 제어	266

7 가상 시스템 보안 268

가상 시스템에서 VMX 파일로의 정보 메시지 제한	268
가상 디스크 축소 방지	269
가상 시스템 보안 모범 사례	269
일반 가상 시스템 보호	270
템플릿을 사용하여 가상 시스템 배포	271
가상 시스템 콘솔 사용 최소화	271
가상 시스템의 리소스 대체 방지	271
가상 시스템 내의 불필요한 기능 사용 안 함	272
불필요한 하드웨어 디바이스 제거	272
사용되지 않는 표시 기능 사용 안 함	273
표시되지 않는 기능 사용 안 함	274
HGFS 파일 전송 사용 안 함	275
게스트 운영 체제와 원격 콘솔 간에 복사하여 붙여넣기 작업 사용 안 함	275
클립보드에 복사된 중요한 데이터의 노출 제한	276
사용자가 가상 시스템 내에서 명령을 실행하지 못하도록 제한	276
가상 시스템 사용자 또는 프로세스가 디바이스와 연결이 끊어지지 않도록 방지	277
게스트 운영 체제 가변 메모리 제한 수정	278
게스트 운영 체제 프로세스가 호스트에 구성 메시지를 보내지 않도록 방지	278
독립형 비영구 디스크 사용 방지	279

8 vSphere 네트워킹 보호 280

vSphere 네트워크 보안 소개	280
방화벽으로 네트워크 보호	282
vCenter Server 구성을 위한 방화벽	282
방화벽을 통해 vCenter Server에 연결	283
vCenter Server가 없는 구성을 위한 방화벽	283
방화벽을 통해 ESXi 호스트 연결	284
방화벽을 통해 가상 시스템 콘솔에 연결	284

물리적 스위치 보호	285
보안 정책으로 표준 스위치 포트 보호	286
vSphere 표준 스위치 보안	286
MAC 주소 변경 사항	287
위조 전송	287
비규칙(Promiscuous) 모드 작업	288
vSphere Distributed Switch 및 분산 포트 그룹 보안	288
VLAN으로 가상 시스템 보호	289
VLAN에 대한 보안 고려 사항	290
VLAN 보호	291
단일 ESXi 호스트에 네트워크 DMZ 생성	291
단일 ESXi 호스트 내에 여러 네트워크 생성	293
인터넷 프로토콜 보안	295
사용 가능한 보안 연결 나열	295
IPsec 보안 연결 추가	295
IPsec 보안 연결 제거	296
사용 가능한 IPsec 보안 정책 나열	297
IPsec 보안 정책 생성	297
IPsec 보안 정책 제거	298
적절한 SNMP 구성 확인	299
필요한 경우에만 vSphere Network Appliance API의 가상 스위치 사용	299
vSphere 네트워킹 보안 모범 사례	300
일반 네트워킹 보안 권장 사항	300
네트워킹 구성 요소 레이블 지정	301
vSphere VLAN 환경 문서화 및 확인	302
건전한 네트워크 분리 방식 채택	303
9 여러 vSphere 구성 요소와 관련된 모범 사례	305
vSphere 네트워크에서 클럭 동기화	305
네트워크 시간 서버와 ESXi 클럭 동기화	305
vCenter Server Appliance에서 시간 동기화 설정 구성	306
VMware Tools 시간 동기화 사용	306
vCenter Server Appliance 구성에서 NTP 서버 추가 또는 바꾸기	307
NTP 서버와 vCenter Server Appliance의 시간 동기화	308
스토리지 보안 모범 사례	308
iSCSI 스토리지 보안	308
iSCSI 장치 보안	309
iSCSI SAN 보호	309
SAN 리소스 마스킹 및 영역 설정	310
NFS 4.1에 Kerberos 자격 증명 사용	310

게스트로 호스트 성능 데이터 보내기가 사용하지 않도록 설정되었는지 확인 311

ESXi Shell 및 vSphere Web Client에 대한 시간 제한 설정 312

10 TLS 재구성 유틸리티를 사용하여 TLS 프로토콜 구성 관리 313

TLS 버전을 사용하지 않도록 설정 가능한 포트 313

vSphere에서 TLS 버전을 사용하지 않도록 설정 315

TLS 구성 유틸리티 설치 316

선택적 수동 백업 수행 317

vCenter Server 시스템에서 TLS 버전을 사용하지 않도록 설정 319

ESXi 호스트에서 TLS 버전을 사용하지 않도록 설정 320

Platform Services Controller 시스템에서 TLS 버전을 사용하지 않도록 설정 321

TLS 구성 변경 내용 되돌리기 322

vSphere Update Manager에서 TLS 버전을 사용하지 않도록 설정 324

Update Manager 포트 9087에 대해 이전 TLS 버전을 사용하지 않도록 설정 324

Update Manager 포트 8084에 대해 이전 TLS 버전을 사용하지 않도록 설정 325

Update Manager 포트 9087에 대해 사용하지 않도록 설정된 TLS 버전을 다시 사용하도록 설정 326

Update Manager 포트 8084에 대해 사용하지 않도록 설정된 TLS 버전을 다시 사용하도록 설정 327

11 정의된 권한 328

경보 권한 329

Auto Deploy 및 이미지 프로파일 권한 330

인증서 권한 331

컨텐츠 라이브러리 권한 332

데이터 센터 권한 334

데이터스토어 권한 334

데이터스토어 클러스터 권한 335

Distributed Switch 권한 336

ESX Agent Manager 권한 336

확장 권한 337

폴더 권한 337

글로벌 권한 338

호스트 CIM 권한 339

호스트 구성 권한 339

호스트 인벤토리 340

호스트 로컬 작업 권한 341

호스트 vSphere 복제 권한 341

호스트 프로파일 권한 342

Inventory Service 제공자 권한 342

Inventory Service 태그 지정 권한	342
네트워크 권한	343
성능 권한	344
사용 권한에 대한 권한	344
프로파일 기반 스토리지 권한	345
리소스 권한	345
스케줄링된 작업 권한	346
세션 권한	346
스토리지 보기 권한	347
작업 권한	347
전송 서비스 권한	348
VRM 정책 권한	348
가상 시스템 구성 권한	348
가상 시스템 게스트 작업 권한	349
가상 시스템 상호 작용 권한	350
가상 시스템 인벤토리 권한	357
가상 시스템 프로비저닝 권한	358
가상 시스템 서비스 구성 권한	359
가상 시스템 스냅샷 관리 권한	360
가상 시스템 vSphere 복제 권한	360
dvPort 그룹 권한	360
vApp 권한	361
vServices 권한	362

vSphere 보안 정보

"vSphere 보안"에서는 VMware® vCenter® Server 및 VMware ESXi에 대한 vSphere® 환경 보호에 대한 정보를 제공합니다.

vSphere 환경을 보호할 수 있도록 이 설명서에서는 사용 가능한 보안 기능과 공격으로부터 환경을 보호하기 위해 취할 수 있는 조치에 대해 설명합니다.

vSphere 환경을 보호할 수 있도록 이 설명서에서는 사용 가능한 보안 기능과 공격으로부터 환경을 보호하기 위해 취할 수 있는 조치에 대해 설명합니다.

표 1-1. "vSphere 보안" 하이라이트

항목	컨텐츠 하이라이트
vCenter Single Sign-On을 사용한 인증	<ul style="list-style-type: none"> ■ vCenter Single Sign-On 기능 및 서비스. ■ ID 소스 추가 및 관리. ■ vCenter Single Sign-On 정책. ■ 사용자 및 그룹.
사용 권한 및 사용자 관리	<ul style="list-style-type: none"> ■ 사용 권한 모델(역할, 그룹, 개체) ■ 사용자 지정 역할 생성 ■ 사용 권한 설정 ■ 글로벌 사용 권한 관리
인증서 관리	<ul style="list-style-type: none"> ■ ESXi 인증서 관리 ■ vCenter Server 및 관련 서비스에 대한 인증서 관리. <ul style="list-style-type: none"> ■ UI를 사용한 인증서 관리. ■ Certificate Manager 유틸리티를 사용한 인증서 관리. ■ 수동 인증서 관리에 CLI 사용(예제 포함).
호스트 보안 기능	<ul style="list-style-type: none"> ■ 잠금 모드 및 기타 보안 프로파일 기능 ■ 호스트 스마트 카드 인증 ■ vSphere Authentication Proxy
보안 모범 사례 및 강화	<p>VMware 보안 전문가의 모범 사례 및 조언</p> <ul style="list-style-type: none"> ■ vCenter Server 보안. ■ 호스트 보안. ■ 가상 시스템 보안. ■ 네트워킹 보안.
vSphere 권한	이 릴리스에서 지원되는 모든 vSphere 권한의 전체 목록

관련 설명서

VMware는 이 문서 외에도 <http://www.vmware.com/security/hardening-guides.html>에서 액세스할 수 있는 각 vSphere 릴리스에 대한 "강화 가이드"를 게시합니다. "강화 가이드"는 다양한 잠재적 보안 문제에 대한 항목이 포함된 스프레드시트입니다. 여기에는 3개의 각기 다른 위험 프로파일에 대한 항목이 포함됩니다. 이 "vSphere 보안" 문서에는 위험 프로파일 1(극비 정부 기관과 같은 보안 수준이 가장 높은 환경)에 대한 정보가 포함되어 있지 않습니다.

대상 사용자

이 정보는 가상 시스템 기술과 데이터 센터 작업에 익숙한 숙련된 Windows 또는 Linux 시스템 관리자를 위해 작성되었습니다.

업데이트된 정보

이 "vSphere 보안" 설명서는 제품의 각 릴리스에 따라 또는 필요할 때 업데이트됩니다.

이 표에는 "vSphere 보안" 설명서의 업데이트 기록이 나와 있습니다.

개정	설명
2022년 4월 27일	■ 스토리지 보기 권한 에 대한 부분적 업데이트.
2021년 11월 5일	■ ESXi 보안 모범 사례 에 대한 부분적 업데이트. ■ vCenter Server에 로그인하는 단계를 설명하기 위해 ESXi 호스트에서 TLS 버전을 사용하지 않도록 설정 항목이 수정되었습니다.
2020년 8월 14일	VMware는 포용성을 중요하게 생각합니다. 고객, 파트너 및 내부 커뮤니티 내에서 이 원칙을 권장하기 위해 콘텐츠에서 일부 용어를 대체하고 있습니다. 비포괄 언어 인스턴스를 제거하기 위해 이 가이드를 업데이트했습니다. ■ 가상 시스템 보안 에 대한 부분적 업데이트.
2017년 10월 4일	■ 인증서 모드 전환 이해 에서 호스트를 유지 보수 모드로 전환하고 연결을 끊는 것은 모든 전환을 수행하기 위해 허용됩니다. 호스트 제거는 필요하지 않습니다.
KO-001949-07	■ 인증서 요구 사항을 자세히 설명하는 새 항목 다양한 솔루션 경로에 대한 인증서 요구 사항 이 추가되고, 관련 설명이 부족한 이전 항목이 제거되었습니다. ■ 새로운 장인 장 10 TLS 재구성 유틸리티를 사용하여 TLS 프로토콜 구성 관리 가 추가되었습니다.
KO-001949-06	■ 웹포로 구분된 인증서 목록 에는 공백이 허용되지 않음을 명시하도록 명령줄을 사용하여 스마트 카드 인증 구성 항목이 업데이트되었습니다. ■ 명령줄을 사용하여 스마트 카드 인증 구성 에 스크립트 위치를 포함시켰습니다. ■ 솔루션 사용자 인증서를 사용자 지정 인증서로 교체 에서 전체 인증서 체인이 필요하다는 것을 명확히 했습니다. ■ 여러 가지 사용 권한 설정 소개에서 문제 하나를 수정했습니다.
KO-001949-05	■ 검증 및 검증 기간에 대한 정보가 사용 권한 유효성 검사 설정 변경 항목에 추가되었습니다.
KO-001949-04	■ NFC(Network File Copy) 를 통한 SSL 인증서 유효성 검사 사용 확인 항목에서 매개 변수 이름 오류가 수정되었습니다. ■ Windows에서 service-control 명령의 위치에 대한 정보가 CLI 명령으로 인증서 및 서비스 관리 항목에 추가되었습니다.
KO-001949-03	■ 태그 사용 권한에 대한 정보가 태그 개체에 대한 사용 권한 항목에 추가되었습니다. ■ vSphere Certificate Manager 를 사용하여 CSR 생성 및 루트 인증서(중간 CA) 준비 에서 인증서 순서가 명확히 설명되었습니다.
KO-001949-02	■ vSphere Client를 사용한 로그인에 대한 참고 사항이 장 2 vCenter Single Sign-On으로 vSphere 인증 항목에 추가되었습니다. ■ Active Directory ID 소스 설정 항목에 설명이 추가되었습니다. 시스템을 Active Directory 이름에 연결해야 하고 DNS를 통해 도메인 이름을 확인할 수 있어야 합니다.

개정	설명
KO-001949-01	<ul style="list-style-type: none"> ■ vSphere Certificate Manager를 사용하여 CSR 생성 및 루트 인증서(중간 CA) 준비 항목에서 인증서 순서가 수정되었습니다. ■ ESXi 암호 및 계정 잠금 항목이 업데이트되었습니다. 암호 문구는 기본적으로 사용되지 않도록 설정됩니다. ■ 명령줄을 사용하여 스마트 카드 인증 구성 항목에서 장치 셀에 액세스하기 위한 단계가 수정되었습니다. ■ vCenter Single Sign-On 암호 변경 항목이 수정되었습니다. 암호가 만료되면 관리자에게 문의해야 합니다. ■ 스크립트를 사용하여 호스트 구성 설정 관리 항목에서 PowerCLI 스크립트가 업데이트되었습니다. ■ vCenter Single Sign-On이 설치에 미치는 영향에서 vCenter Server 인스턴스 번호에 대한 정보를 업데이트했습니다. ■ 명령줄을 사용하여 스마트 카드 인증 구성, Platform Services Controller 웹 인터페이스를 사용하여 스마트 카드 인증 관리 및 RSA SecurID 인증 설정 항목이 일부 업데이트되었습니다. ■ vCenter Server TCP 및 UDP 포트 항목이 수정되었습니다. 예를 들어 포트 903 및 포트 5900-5964는 vCenter Server 시스템이 아니라 호스트에서 사용되며, 포트 9090 같은 일부 다른 포트는 내부용으로만 사용됩니다. ■ DSA 키에 대한 정보가 vifs 명령을 사용하여 SSH Key 업로드 항목에서 제거되었습니다. ■ 새 STS 서명 인증서를 생성하는 절차를 포함하도록 STS(Security Token Service) 항목이 업데이트되었습니다.
KO-001949-00	최초 릴리스

vSphere 환경의 보안

1

vSphere 환경의 구성 요소는 인증서, 권한 부여, 각 ESXi의 방화벽, 제한된 액세스 등과 같은 다양한 기능으로 즉시 보호됩니다. 여러 가지 방법으로 기본 설정을 수정할 수 있습니다. 예를 들어 vCenter 개체에 대해 사용 권한을 설정하거나, 방화벽 포트를 열거나, 기본 인증서를 변경할 수 있습니다. 그러면 vCenter Server 시스템, ESXi 호스트 및 가상 시스템 보안의 유연성이 최대화됩니다.

주의가 필요한 vSphere의 여러 영역을 개괄적으로 파악하면 보안 전략을 계획하는 데 도움이 됩니다. 또한 VMware 웹 사이트에서 추가적인 vSphere 보안 리소스도 활용할 수 있습니다.

본 장은 다음 항목을 포함합니다.

- ESXi 하이퍼바이저 보안
- vCenter Server 시스템 및 관련 서비스 보안
- 가상 시스템 보안
- 가상 네트워킹 계층 보호
- vSphere 환경의 암호
- 보안 모범 사례 및 리소스

ESXi 하이퍼바이저 보안

ESXi 하이퍼바이저 보안이 기본적으로 제공됩니다. 잠금 모드 및 다른 기본 제공 기능을 사용하여 추가로 ESXi 호스트를 보호할 수 있습니다. 참조 호스트를 설정하고 해당 호스트의 호스트 프로파일에 따라 모든 호스트를 변경하는 경우 또는 스크립트로 작성된 관리를 수행하는 경우 변경 내용이 모든 호스트에 적용되도록 하면 환경이 추가로 보호됩니다.

이 가이드에 나와 있는 세부 정보대로 다음 기능을 사용하여 vCenter Server에서 관리되는 ESXi 호스트의 보호를 강화합니다. "VMware vSphere Hypervisor의 보안" 백서도 참조하십시오.

ESXi 액세스 제한

기본적으로 ESXi Shell 및 SSH 서비스는 실행되지 않고 루트 사용자만 DCUI(Direct Console User Interface)에 로그인할 수 있습니다. ESXi 또는 SSH 액세스를 사용하도록 설정하는 경우 시간 제한을 설정하여 인증되지 않은 액세스에 대한 위험을 제한할 수 있습니다.

ESXi 호스트에 액세스할 수 있는 사용자는 호스트를 관리하는 사용 권한이 있어야 합니다. 호스트를 관리하는 vCenter Server에서 호스트 개체에 대한 사용 권한을 설정합니다.

명명된 사용자 및 최소 권한 사용

기본적으로 루트 사용자에게 의해 여러 작업이 수행될 수 있습니다. 루트 사용자 계정을 사용하여 관리자가 ESXi 호스트에 로그인하는 것을 허용하는 대신, 다른 호스트 구성 권한을 vCenter Server 사용 권한 관리 인터페이스에서 다른 명명된 사용자에게 적용할 수 있습니다. vSphere Web Client에서 사용자 지정 역할을 생성하고, 권한을 역할에 할당하고, 명명된 사용자 및 ESXi 호스트 개체에 역할을 연결할 수 있습니다.

단일 호스트 시나리오에서는 사용자를 직접 관리합니다. "vSphere Client를 통한 vSphere 관리" 설명서를 참조하십시오.

열린 ESXi 방화벽 포트의 수 최소화

기본적으로 ESXi 호스트의 방화벽 포트는 해당 서비스를 시작할 때만 열립니다. vSphere Web Client 나 ESXCLI 또는 PowerCLI 명령을 사용하여 방화벽 포트 상태를 확인하고 관리할 수 있습니다.

[ESXi 방화벽 구성](#)를 참조하십시오.

ESXi 호스트 관리 자동화

동일한 데이터 센터의 다른 호스트가 동기화된 상태에 있는 것이 중요한 경우가 많기 때문에 스크립트로 작성된 설치 또는 vSphere Auto Deploy를 사용하여 호스트를 프로비저닝합니다. 스크립트를 사용하여 호스트를 관리할 수 있습니다. 스크립트로 작성된 관리 대신 호스트 프로파일을 사용할 수도 있습니다. 참조 호스트를 설정하고 호스트 프로파일을 내보내고 호스트 프로파일을 호스트에 적용합니다. 호스트 프로파일을 직접 또는 Auto Deploy로 프로비저닝 작업의 일부로 적용할 수 있습니다.

vSphere Auto Deploy에 대한 자세한 내용은 [스크립트를 사용하여 호스트 구성 설정 관리 및 "vSphere 설치 및 설정"](#) 항목을 참조하십시오.

잠금 모드 이용

잠금 모드에서 ESXi 호스트는 기본적으로 vCenter Server를 통해서만 액세스할 수 있습니다.

vSphere 6.0부터 엄격 잠금 모드 또는 정상 잠금 모드를 선택하고 예외 사용자를 정의하여 백업 에이전트와 같은 서비스 계정에 직접 액세스하도록 할 수 있습니다.

[잠금 모드](#)를 참조하십시오.

VIB 패키지 무결성 검사

각 VIB 패키지에는 관련된 허용 수준이 있습니다. 허용 수준이 호스트의 허용 수준과 동일하거나 더 나은 경우에만 VIB를 ESXi 호스트에 추가할 수 있습니다. 명시적으로 호스트의 허용 수준을 변경하지 않는 한 CommunitySupported 또는 PartnerSupported VIB를 호스트에 추가할 수 없습니다.

[호스트 및 VIB의 수락 수준 확인](#)를 참조하십시오.

ESXi 인증서 관리

vSphere 6.0 이상에서 VMCA(VMware 인증 기관)는 기본적으로 각 ESXi 호스트에 루트 인증 기관이 VMCA인 서명된 인증서를 프로비저닝합니다. 회사 정책에서 요구하는 경우 기존 인증서를 타사 CA에서 서명된 인증서로 바꿀 수 있습니다.

[ESXi 호스트에 대한 인증서 관리](#) 항목을 참조하십시오.

스마트 카드 인증

vSphere 6.0부터 ESXi는 사용자 이름 및 암호 인증 대신 옵션으로 스마트 카드 인증을 지원합니다.

[ESXi에 대한 스마트 카드 인증 구성](#)를 참조하십시오.

ESXi 계정 잠금

vSphere 6.0부터 SSH 및 vSphere Web Services SDK를 통한 액세스에 대해 계정 잠금이 지원됩니다. DCUI(Direct Console Interface) 및 ESXi Shell은 계정 잠금을 지원하지 않습니다. 기본적으로, 계정이 잠기기 전에 최대 10번의 시도 실패가 허용되고 2분 후에는 계정에 대한 잠금이 해제됩니다.

[ESXi 암호 및 계정 잠금](#)를 참조하십시오.

관리 작업은 다를 수 있지만 독립형 호스트에 대한 보안 고려 사항은 유사합니다. "vSphere Client를 통한 vSphere 관리" 설명서를 참조하십시오.

vCenter Server 시스템 및 관련 서비스 보안

vCenter Server 시스템 및 관련 서비스는 vCenter Single Sign-On을 통한 인증 및 vCenter Server 사용 권한 모델을 통한 권한 부여에 의해 보호됩니다. 기본 동작을 수정하거나 추가 단계를 수행하여 환경에 대한 액세스를 보호할 수 있습니다.

vSphere 환경을 보호할 때 vCenter Server 인스턴스와 관련된 모든 서비스가 보호되어야 한다는 것을 고려하십시오. 일부 환경에서는 여러 개의 vCenter Server 인스턴스와 하나 이상의 Platform Services Controller 인스턴스를 보호해야 할 수 있습니다.

모든 vCenter 호스트 시스템 강화

vCenter 환경을 보호하는 첫 번째 단계는 vCenter Server 또는 관련 서비스가 실행되는 각 시스템을 강화하는 것입니다. 물리적 시스템 또는 가상 시스템에 적용되는 고려 사항은 유사합니다. 운영 체제에 항상 최신 보안 패치를 설치하고 업계 표준 모범 사례를 따라 호스트 시스템을 보호합니다.

vCenter 인증서 모델 학습

기본적으로 VMware Certificate Authority는 VMCA로 서명된 인증서를 사용하여 각 ESXi 호스트, 환경의 각 시스템 및 각 솔루션 사용자를 프로비저닝합니다. 해당 환경이 바로 작동하지만 회사 정책에서 요구하는 경우 기본 동작을 변경할 수 있습니다. [장 3 vSphere 보안 인증서](#)를 참조하십시오.

추가로 보호하려면 만료되거나 해지된 인증서 및 실패한 설치를 명시적으로 제거하십시오.

vCenter Single Sign-On 구성

vCenter Server 및 관련 서비스는 vCenter Single Sign-On 인증 프레임워크에 의해 보호됩니다. 처음 소프트웨어를 설치할 때 administrator@vsphere.local 사용자의 암호를 지정하고 해당 도메인만

ID 소스로 사용할 수 있습니다. Active Directory 또는 LDAP를 사용하는 다른 ID 소스를 추가하고 기본 ID 소스를 설정할 수 있습니다. 그러면 ID 소스에 인증할 수 있는 사용자는 권한이 부여된 경우 개체를 보고 작업을 수행할 수 있습니다. [장 2 vCenter Single Sign-On으로 vSphere 인증](#)을 참조하십시오.

사용자 또는 그룹에 역할 할당

로그인을 향상시키기 위해 개체에 제공하는 각 사용 권한을 명명된 사용자 또는 그룹 및 사전 정의된 역할 또는 사용자 지정 역할과 연결합니다. vSphere 6.0 사용 권한 모델은 사용자 또는 그룹을 인증하는 다양한 방법을 통해 뛰어난 유연성을 제공합니다. [vSphere의 권한 부여 이해](#) 및 [일반 작업에 필요한 권한 항목](#)을 참조하십시오.

관리자 권한 및 관리자 역할의 사용을 제한하십시오. 가능한 경우 익명의 관리자 사용자를 사용하지 마십시오.

NTP 설정

환경의 각 노드에 대해 NTP를 설정합니다. 인증서 인프라는 정확한 타임 스탬프가 필요하며 노드가 동기화되지 않은 경우 제대로 작동하지 않습니다.

[vSphere 네트워크에서 클럭 동기화](#)를 참조하십시오.

가상 시스템 보안

VM을 보호하려면 게스트 운영 체제가 패치되도록 유지하고 환경을 물리적 시스템을 보호하는 것처럼 보호합니다. 불필요한 기능을 사용하지 않도록 설정하는 것을 고려하고 VM 콘솔 사용을 최소화하고 기타 모범 사례를 따릅니다.

게스트 운영 체제 보호

게스트 운영 체제를 보호하려면 게스트 운영 체제에서 최신 패치를 사용하고 적합한 경우 스파이웨어 방지 및 맬웨어 방지 애플리케이션을 사용합니다. 게스트 운영 체제 벤더의 설명서 그리고 책이나 인터넷에서 제공되는 해당 운영 체제 관련 기타 정보를 참조하십시오.

불필요한 기능 사용 안 함

잠재적 공격 지점을 최소화하기 위해 불필요한 기능이 사용하지 않도록 설정되었는지 확인합니다. 드물게 사용되는 기능의 대부분은 기본적으로 사용하지 않도록 설정되어 있습니다. 불필요한 하드웨어를 제거하고 HGFS(Host-Guest Filesystem) 또는 VM과 원격 콘솔 간에 복사하여 붙여넣기와 같은 특정 기능을 사용하지 않도록 설정합니다.

[가상 시스템 내의 불필요한 기능 사용 안 함](#)의 내용을 참조하십시오.

템플릿 및 스크립트로 작성된 관리 기능 사용

VM 템플릿을 사용하면 요구 사항을 충족하도록 운영 체제를 설정하고 동일한 설정으로 다른 VM을 생성할 수 있습니다.

초기 배포 후 VM 설정을 변경하려면 PowerCLI와 같은 스크립트 사용을 고려합니다. 이 설명서에서는 GUI를 사용하여 작업을 수행하는 방법을 설명합니다. 환경의 일관성을 유지하기 위해 GUI 대신 스크

립트를 사용하는 것이 좋습니다. 대규모 환경에서는 스크립팅을 최적화하기 위해 VM을 폴더로 그룹화할 수 있습니다.

템플릿에 대한 자세한 내용은 [템플릿을 사용하여 가상 시스템 배포](#) 및 "vSphere 가상 시스템 관리" 항목을 참조하십시오. PowerCLI에 대한 자세한 내용은 VMware PowerCLI 설명서를 참조하십시오.

가상 시스템 콘솔 사용 최소화

가상 시스템 콘솔은 물리적 서버의 모니터가 제공하는 VM에 동일한 기능을 제공합니다. 가상 시스템 콘솔에 대한 액세스 권한이 있는 사용자는 VM 전원 관리 및 이동식 디바이스 연결 제어에 대한 액세스 권한이 있습니다. 따라서 가상 시스템 콘솔 액세스로 인해 VM이 악의적인 공격을 받을 수 있습니다.

가상 네트워킹 계층 보호

가상 네트워킹 계층에는 가상 네트워크 어댑터, 가상 스위치, 분산 가상 스위치, 포트 및 포트 그룹이 포함됩니다. ESXi는 가상 시스템과 가상 시스템 사용자 간의 통신을 지원하기 위해 가상 네트워킹 계층에 의존합니다. ESXi 역시 iSCSI SAN, NAS 스토리지 등과 통신하기 위해 가상 네트워킹 계층을 사용합니다.

vSphere에는 보안 네트워킹 인프라에 필요한 전체 기능 어레이가 포함됩니다. 가상 스위치, 분산 가상 스위치, 가상 네트워크 어댑터 등과 같은 각 인프라 요소를 별도로 보호할 수 있습니다. 또한 [장 8 vSphere 네트워킹 보호](#)에서 보다 자세하게 논의된 다음 지점을 고려하십시오.

네트워크 트래픽 분리

네트워크 트래픽 분리는 ESXi 환경 보호에 필수적입니다. 필요한 액세스 및 분리 수준은 네트워크마다 다릅니다. 관리 네트워크에서는 클라이언트 트래픽, CLI(명령줄 인터페이스) 또는 API 트래픽, 타사 소프트웨어 트래픽을 일반적인 트래픽에서 분리합니다. 이 네트워크에는 시스템 관리자, 네트워크 관리자 및 보안 관리자만 액세스할 수 있어야 합니다.

[ESXi 네트워킹 보안 권장 사항](#)을 참조하십시오.

방화벽을 사용하여 가상 네트워크 요소 보호

방화벽 포트를 열고 닫는 것은 물론 가상 네트워크에서 각 요소를 별도로 보호할 수 있습니다. 방화벽 규칙은 서비스를 해당 방화벽과 연결하며 서비스의 상태에 따라 ESXi 방화벽을 열고 닫을 수 있습니다.

[ESXi 방화벽 구성](#)을 참조하십시오.

네트워크 보안 정책 고려

네트워킹 보안 정책은 MAC 주소 가장 행위 및 원치 않는 포트 검색으로부터 트래픽을 보호합니다. 표준 스위치 또는 Distributed Switch의 보안 정책은 네트워크 프로토콜 스택의 계층 2(데이터 링크 계층)에서 구현됩니다. 보안 정책의 세 가지 요소는 비규칙(promiscuous) 모드, MAC 주소 변경 및 위조 전송입니다.

지침은 "vSphere 네트워킹" 설명서를 참조하십시오.

가상 시스템 네트워킹 보호

가상 시스템 네트워크를 보호하기 위해 사용하는 방법은 설치되어 있는 게스트 운영 체제의 종류, 가상 시스템이 신뢰할 수 있는 환경에서 작동하는지 여부 등을 비롯한 다양한 요소에 따라 달라집니다. 가상 스위치 및 분산 가상 스위치는 방화벽 설치와 같은 다른 공통적인 보안 모범 사례와 함께 사용할 경우 상당한 수준의 보호를 제공합니다.

장 8 vSphere 네트워킹 보호를 참조하십시오.

환경 보호에 VLAN 고려

ESXi는 IEEE 802.1q VLAN을 지원하며 이를 통해 가상 시스템 네트워크나 스토리지 구성을 추가적으로 보호할 수 있습니다. VLAN을 사용하면 물리적 네트워크를 세그먼트로 나눠 동일한 물리적 네트워크에 있는 두 시스템이 동일한 VLAN에 속하지 않는 한 서로 패킷을 주고받지 못하게 만들 수 있습니다.

VLAN으로 가상 시스템 보호를 참조하십시오.

가상화된 스토리지에 대한 연결 보호

가상 시스템은 운영 체제 파일, 프로그램 파일 및 기타 데이터를 가상 디스크에 저장합니다. 각 가상 디스크는 가상 시스템에 SCSI 컨트롤러에 연결된 SCSI 드라이브로 표시됩니다. 가상 시스템은 스토리지 세부 정보와 분리되었으며 가상 디스크가 상주하는 LUN에 대한 정보에 액세스할 수 없습니다.

VMFS(가상 시스템 파일 시스템)는 가상 볼륨을 ESXi 호스트에 제공하는 분산 파일 시스템 및 볼륨 관리자입니다. 사용자는 스토리지에 대한 연결을 보호할 책임이 있습니다. 예를 들어 iSCSI 스토리지를 사용 중인 경우 CHAP를 사용하도록 환경을 설정하고 회사 정책에 따라 필요한 경우에는 vSphere Web Client 또는 CLI를 사용하여 상호 CHAP를 사용하도록 환경을 설정할 수 있습니다.

스토리지 보안 모범 사례를 참조하십시오.

IPSec의 사용 평가

ESXi는 IPv6을 통한 IPSec을 지원합니다. IPv4를 통한 IPSec은 사용할 수 없습니다.

인터넷 프로토콜 보안을 참조하십시오.

또한 VMware NSX for vSphere가 환경의 네트워킹 계층 보호에 적합한 솔루션인지 평가합니다.

vSphere 환경의 암호

vSphere 환경의 암호 제한, 잠금 및 만료는 사용자의 대상 시스템이 무엇인지, 사용자가 누구인지, 정책이 어떻게 설정되었는지에 따라 달라집니다.

ESXi 암호

ESXi 암호 제한은 Linux PAM 모듈 pam_passwdqc에 의해 결정됩니다. ESXi 암호 및 계정 잠금을 참조하십시오.

vCenter Server 및 기타 vCenter 서비스에 대한 암호

vCenter Single Sign-On은 vCenter Server 및 기타 vCenter 서비스에 로그인하는 모든 사용자의 인증을 관리합니다. 암호 제한, 잠금 및 만료는 사용자의 도메인과 사용자가 누구인지에 따라 달라집니다.

administrator@vsphere.local

administrator@vsphere.local 사용자의 암호 또는 설치 중 다른 도메인을 선택한 경우 administrator@mydomain 사용자의 암호는 만료되지 않으며 잠금 정책의 적용을 받지 않습니다. 다른 모든 사용자의 암호는 vCenter Single Sign-On 암호 정책에 설정된 제한을 따라야 합니다. [vCenter Single Sign-On 암호 정책 편집](#)를 참조하십시오.

이 사용자의 암호를 잊은 경우 VMware 기술 자료 시스템에서 암호 재설정에 대한 정보를 찾아보십시오.

다른 vsphere.local 사용자

다른 vsphere.local 사용자 또는 설치 중 지정한 로컬 도메인의 사용자에 대한 암호는 vCenter Single Sign-On 암호 정책 및 잠금 정책에 의해 설정된 제한을 따라야 합니다. [vCenter Single Sign-On 암호 정책 편집](#) 및 [vCenter Single Sign-On 잠금 정책 편집](#) 항목을 참조하십시오. 이러한 암호는 기본적으로 90일 후에 만료되지만 관리자가 암호 정책의 일부로 만료 날짜를 변경할 수 있습니다.

사용자가 자신의 vsphere.local 암호를 잊은 경우 관리자가 dir-cli 명령을 사용하여 암호를 재설정할 수 있습니다.

기타 사용자

다른 모든 사용자의 암호 제한, 잠금 및 만료는 사용자가 인증할 수 있는 도메인(ID 소스)에 의해 결정됩니다.

vCenter Single Sign-On은 하나의 기본 ID 소스를 지원하며 사용자는 자신의 사용자 이름만으로 vSphere Client에 로그인할 수 있습니다. 암호 매개 변수는 도메인에 의해 결정됩니다. 사용자가 기본 값이 아닌 도메인의 사용자로 로그인하려는 경우에는 도메인 이름을 포함할 수 있습니다. 즉, *user@domain* 또는 *domain\user*를 지정합니다. 도메인 암호 매개 변수는 이 경우에도 적용됩니다.

vCenter Server Appliance Direct Console User Interface 사용자의 암호

vCenter Server Appliance는 Linux에서 vCenter Server 및 관련 서비스를 실행하도록 최적화된 사전 구성 Linux 기반 가상 시스템입니다.

vCenter Server Appliance를 배포할 때 장치 Linux 운영 체제의 루트 사용자에 대한 암호와 administrator@vsphere.local 사용자에 대한 암호를 지정합니다. Direct Console User Interface에서 루트 사용자 암호를 변경하고 기타 vCenter Server Appliance 로컬 사용자 관리 작업을 수행할 수 있습니다. "vCenter Server Appliance 구성"를 참조하십시오.

보안 모범 사례 및 리소스

모범 사례를 따르는 경우 ESXi 및 vCenter Server가 가상화를 포함하지 않는 환경과 동일하게 또는 그 이상으로 안전할 수 있습니다.

이 설명서에는 vSphere 인프라의 다양한 구성 요소에 대한 모범 사례가 포함되어 있습니다.

표 1-1. 보안 모범 사례

vSphere 구성 요소	리소스
ESXi 호스트	ESXi 보안 모범 사례
vCenter Server 시스템	vCenter Server 보안 모범 사례
가상 시스템	가상 시스템 보안 모범 사례
vSphere 네트워킹	vSphere 네트워킹 보안 모범 사례

이 설명서는 보안 환경을 보장하는 데 필요한 소스 중 하나일 뿐입니다.

보안 경고 및 다운로드를 포함한 VMware 보안 리소스를 웹에서 사용할 수 있습니다.

표 1-2. 웹의 VMware 보안 리소스

주제	리소스
VMware 보안 정책, 최신 보안 경고, 보안 다운로드 및 보안 관련 집중 토론	http://www.vmware.com/go/security
기업 보안 대응 정책	http://www.vmware.com/support/policies/security_response.html VMware는 고객이 안전한 환경을 유지할 수 있도록 최선을 다하고 있습니다. 보안 문제를 적시에 해결합니다. VMware 보안 대응 정책에는 제품에서 발생할 수 있는 취약점을 해결하기 위해 최선을 다한다는 약속이 명시되어 있습니다.
타사 소프트웨어 지원 정책	http://www.vmware.com/support/policies/ VMware는 다양한 스토리지 시스템을 지원하며 백업 에이전트와 시스템 관리 에이전트 같은 소프트웨어 에이전트를 지원합니다. http://www.vmware.com/vmtn/resources/ 에서 ESXi 호환성 가이드를 검색하여 ESXi를 지원하는 에이전트, 도구 및 기타 소프트웨어 목록을 찾을 수 있습니다. 업체에서는 VMware가 테스트할 수 있는 것보다 훨씬 많은 제품과 구성을 제공합니다. VMware의 호환성 가이드에 없는 제품이나 구성인 경우 기술 지원에서 문제 해결에 도움을 줄 수 있지만 제품이나 구성을 사용할 수 있다는 보장을 할 수는 없습니다. 지원되지 않는 제품이나 구성에 대해서는 항상 보안 위험을 주의하여 평가하십시오.
규정 준수 및 보안 표준, 파트너 솔루션 및 가상화와 규정 준수에 대한 심층적인 관련 자료	http://www.vmware.com/go/compliance
다양한 버전의 vSphere 구성 요소에 대한 CCEVS, FIPS 등의 보안 인증 및 검증 관련 정보	https://www.vmware.com/support/support-resources/certifications.html
다양한 버전의 vSphere 및 기타 VMware 제품에 대한 강화 가이드	https://www.vmware.com/support/support-resources/hardening-guides.html
"VMware vSphere Hypervisor의 보안" 백서	http://www.vmware.com/files/pdf/techpaper/vmw-wp-secrty-vsphr-hyprvsr-uslet-101.pdf

vCenter Single Sign-On으로 vSphere 인증

2

vCenter Single Sign-On은 인증 브로커이자 보안 토큰 교환 인프라입니다. 사용자 또는 솔루션 사용자가 vCenter Single Sign-On에 인증할 수 있는 경우 해당 사용자는 SAML 토큰을 받습니다. 앞으로 해당 사용자는 SAML 토큰을 사용하여 vCenter 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.

vSphere 6.0부터 vCenter Single Sign-On은 Platform Services Controller의 일부입니다. Platform Services Controller에는 vCenter Server 및 vCenter Server 구성 요소를 지원하는 공유 서비스가 포함되어 있습니다. 이러한 서비스에는 vCenter Single Sign-On, VMware Certificate Authority, 라이선스 서비스 및 Lookup Service가 포함됩니다. Platform Services Controller에 대한 자세한 내용은 "vSphere 설치 및 설정" 항목을 참조하십시오.

처음 핸드셰이크의 경우 사용자는 사용자 이름 및 암호로 인증하고 솔루션 사용자는 인증서로 인증합니다. 솔루션 사용자 인증서 바꾸기에 대한 자세한 내용은 [장 3 vSphere 보안 인증서](#)를 참조하십시오.

사용자가 vCenter Single Sign-On으로 인증한 후에는 해당 사용자에게 특정 작업을 수행하도록 권한을 부여할 수 있습니다. 대부분의 경우 vCenter Server 권한을 할당하지만 vSphere에는 다른 사용 권한 모델이 들어 있습니다. [vSphere의 권한 부여 이해](#)의 내용을 참조하십시오.

참고 Active Directory 사용자가 SSPI와 함께 vSphere Client를 사용하여 vCenter Server 인스턴스에 로그인할 수 있게 하려면 vCenter Server 인스턴스를 Active Directory 도메인에 가입시켜야 합니다. 외부 Platform Services Controller가 있는 vCenter Server Appliance를 Active Directory 도메인에 가입시키는 방법에 대한 자세한 내용은 VMware 기술 자료 문서(<http://kb.vmware.com/kb/2118543>)를 참조하십시오.

본 장은 다음 항목을 포함합니다.

- vCenter Single Sign-On 이해
- vCenter Single Sign-On ID 소스 구성
- vCenter Server 이중 인증
- vCenter Single Sign-On을 다른 서비스 제공자의 ID 제공자로 사용
- STS(Security Token Service)

- vCenter Single Sign-On 정책 관리
- vCenter Single Sign-On 사용자 및 그룹 관리
- vCenter Single Sign-On 보안 모범 사례
- vCenter Single Sign-On 문제 해결

vCenter Single Sign-On 이해

vCenter Single Sign-On을 효율적으로 관리하려면 기본 아키텍처와 이 아키텍처가 설치 및 업그레이드에 미치는 영향을 이해해야 합니다.



vCenter Single Sign-On 6.0 도메인 및 사이트

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

vCenter Single Sign-On으로 환경을 보호하는 방법

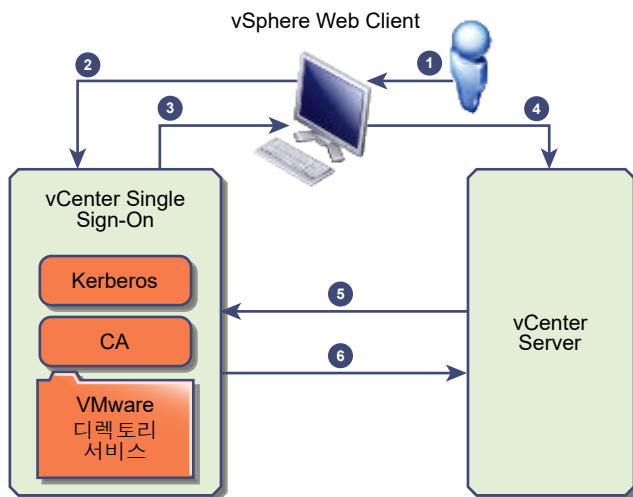
vCenter Single Sign-On을 사용하면 사용자가 각 vSphere 구성 요소를 별도로 인증하는 대신 안전한 토큰 메커니즘을 통해 vSphere 구성 요소가 서로 통신할 수 있습니다.

vCenter Single Sign-On은 STS(Security Token Service), 보안 트래픽용 SSL, Active Directory 또는 OpenLDAP를 통한 인간 사용자 인증 및 인증서를 통한 솔루션 사용자 인증을 조합하여 사용합니다.

인간 사용자를 위한 vCenter Single Sign-On 핸드셰이크

다음 그림에서는 인간 사용자를 위한 핸드셰이크를 보여 줍니다.

그림 2-1. 인간 사용자를 위한 vCenter Single Sign-On 핸드셰이크



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

또한 사용자는 **Windows 세션 인증 사용** 확인란을 선택하여 암호 없이 로그인할 수도 있습니다.

- 2 vSphere Web Client는 로그인 정보를 vCenter Single Sign-On 서비스로 전달하며, 이 서비스는 vSphere Web Client의 SAML 토큰을 확인합니다. vSphere Web 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 Web Client에 반환합니다.
- 4 vSphere Web 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 활용하여 토큰을 vCenter Server 시스템에 반환합니다.

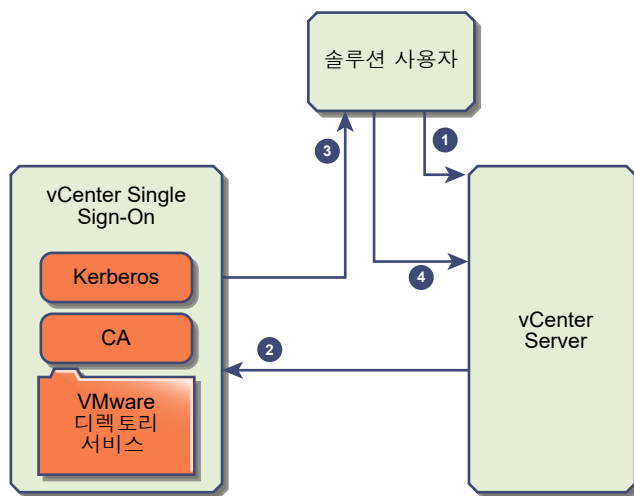
사용자는 이제 인증할 수 있으며 해당 사용자 역할에 권한이 있는 모든 개체를 보고 수정할 수 있습니다.

참고 처음에는 각 사용자에게 권한 없음 역할이 할당됩니다. 사용자가 로그인하려면 vCenter Server 관리자가 해당 사용자에게 최소한 읽기 전용 역할을 할당해야 합니다. [인벤토리 개체에 사용 권한 추가](#) 항목을 참조하십시오.

솔루션 사용자를 위한 vCenter Single Sign-On 핸드셰이크

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

그림 2-2. 솔루션 사용자를 위한 vCenter Single Sign-On 핸드셰이크



솔루션 사용자의 경우 상호 작용이 다음과 같이 진행됩니다.

- 1 솔루션 사용자가 vCenter 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.
- 5 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. [vSphere와 함께 타사 인증서 사용](#)을 참조하십시오.

vCenter Single Sign-On 구성 요소

vCenter Single Sign-On에는 STS(Security Token Service), 관리 서버 및 vCenter Lookup Service와 VMware 디렉토리 서비스(vmdir)가 포함되어 있습니다. VMware 디렉토리 서비스도 인증서 관리에 사용됩니다.

설치 중 구성 요소가 내장된 배포의 일부로 배포되거나 Platform Services Controller의 일부로 배포됩니다.

STS(Security Token Service)

STS 서비스는 SAML(Security Assertion Markup Language) 토큰을 발급합니다. 이러한 보안 토큰은 vCenter Single Sign-On에서 지원하는 ID 소스 유형 중 하나로 사용자의 ID를 나타냅니다. SAML 토큰을 사용하면 vCenter Single Sign-On에 성공적으로 인증하는 인간 사용자 및 솔루션 사용자 모두가 각 서비스에 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 Web Client에서 사용자 및 그룹을 관리할 수 있습니다. 처음에는 `administrator@your_domain_name` 사용자만 이 권한을 가지고 있습니다. vSphere 5.5에서 이 사용자는 `administrator@vsphere.local`이었습니다. vSphere 6.0에서는 새 Platform Services Controller와 함께 vCenter Server를 설치하거나 vCenter Server Appliance를 배포할 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 내장된 배포와 각 Platform Services Controller에 포함됩니다. 이 서비스는 포트 389에서 LDAP 디렉토리를 사용할 수 있도록 하는 다중 테넌트, 피어 복제 디렉토리 서비스입니다. 이 서비스는 vSphere 5.5 및 이전 시스템과의 역호환성을 위해 포트 11711을 여전히 사용합니다.

환경에 여러 개의 Platform Services Controller 인스턴스가 포함되어 있으면 한 vmdir 인스턴스의 vmdir 콘텐츠 업데이트가 다른 모든 vmdir 인스턴스에 전파됩니다.

vSphere 6.0부터 VMware Directory Service는 vCenter Single Sign-On 정보뿐만 아니라 인증서 정보도 저장합니다.

ID 관리 서비스

ID 소스 및 STS 인증 요청을 처리합니다.

vCenter Single Sign-On이 설치에 미치는 영향

vSphere 버전 5.1부터는 vCenter Single Sign-On 서비스가 vCenter Server 관리 인프라의 일부로 포함됩니다. 이러한 변경은 vCenter Server 설치에 영향을 줍니다.

vCenter Single Sign-On을 사용한 인증은 vSphere의 보안을 강화합니다. 왜냐하면 vSphere 소프트웨어 구성 요소가 보안 토큰 교환 메커니즘을 사용하여 서로 간에 통신하고 다른 모든 사용자도 vCenter Single Sign-On을 사용하여 인증하기 때문입니다.

vSphere 6.0부터는 vCenter Single Sign-On이 내장된 배포에 포함되거나 Platform Services Controller의 일부로 포함됩니다. Platform Services Controller에는 vCenter Single Sign-On, VMware Certificate Authority, VMware Lookup Service 및 라이선싱 서비스를 포함한 vSphere 구성 요소 간의 통신에 필요한 모든 서비스가 포함됩니다.

설치 순서가 중요합니다.

첫 번째 설치

설치가 분산된 경우 Platform Services Controller를 설치한 후 vCenter Server를 설치하거나 vCenter Server Appliance를 배포해야 합니다. 내장된 배포의 경우 자동으로 올바른 순서의 설치가 수행됩니다.

이후 설치

하나의 Platform Services Controller가 대략 최대 4개의 vCenter Server 인스턴스로 구성된 전체 vSphere 환경을 지원할 수 있습니다. 새 vCenter Server 인스턴스를 동일한 Platform Services Controller에 연결할 수 있습니다. vCenter Server 인스턴스가 약 4개를 초과하는 경우 성능 향상을 위해 추가 Platform Services Controller를 설치할 수 있습니다. 각 Platform Services Controller의 vCenter Single Sign-On 서비스는 인증 데이터를 다른 모든 인스턴스와 동기화합니다. 정확한 수는 사용 중인 vCenter Server 인스턴스의 양과 기타 요소에 따라 다릅니다.

vCenter Single Sign-On이 업그레이드에 미치는 영향

단순 설치 환경을 vCenter Server 6 내장된 배포로 업그레이드하는 경우 원활한 업그레이드가 진행됩니다. 사용자 지정 설치를 업그레이드하는 경우 업그레이드 후 vCenter Single Sign-On 서비스는 Platform Services Controller의 일부입니다. 업그레이드 후 vCenter Server에 로그인할 수 있는 사용자는 업그레이드 이전 버전과 배포 구성에 따라 다릅니다.

업그레이드 도중 vsphere.local 대신 사용될 다른 vCenter Single Sign-On 도메인 이름을 정의할 수 있습니다.

업그레이드 경로

업그레이드의 결과는 선택한 설치 옵션 및 업그레이드할 대상 배포 모델에 따라 달라집니다.

표 2-1. 업그레이드 경로

소스	결과
vSphere 5.5 이전 단순 설치	내장된 Platform Services Controller가 있는 vCenter Server
vSphere 5.5 이전 사용자 지정 설치	<p>vCenter Single Sign-On이 vCenter Server와 다른 노드에 있는 경우에는 외부 Platform Services Controller가 있는 환경이 만들어집니다.</p> <p>vCenter Single Sign-On이 vCenter Server와 같은 노드에 있지만 기타 서비스는 다른 노드에 있는 경우, 내장된 Platform Services Controller가 있는 환경이 만들어집니다.</p> <p>사용자 지정 설치에 여러 개의 복제 vCenter Single Sign-On 서버가 포함된 경우 여러 개의 Platform Services Controller 인스턴스가 있는 환경이 만들어집니다.</p>

단순 설치 업그레이드 후 로그인 가능한 사용자

단순 설치 옵션을 사용하여 프로비저닝한 환경을 업그레이드하는 경우에는 항상 내장된 Platform Services Controller가 있는 설치 환경이 만들어집니다. 로그인할 수 있도록 인증되는 사용자는 소스 환경에 vCenter Single Sign-On이 포함되는지에 따라 다릅니다.

표 2-2. 단순 설치 환경 업그레이드 후 로그인 권한

소스 버전	로그인 액세스 권한을 부여할 대상	참고
vSphere 5.0	로컬 운영 체제 사용자 administrator@vsphere.local	사용자 저장소가 변경되므로 설치 도중 vSphere 인벤토리 계층 루트 폴더의 관리자를 묻는 메시지가 나타날 수 있습니다. 이전 설치 환경에서 Active Directory 사용자를 지원한 경우 Active Directory 도메인을 ID 소스로 추가할 수 있습니다.
vSphere 5.1	로컬 운영 체제 사용자 administrator@vsphere.local Admin@SystemDomain	vSphere 5.5부터는 vCenter Single Sign-On이 하나의 기본 ID 소스만 지원합니다. 기본 ID 소스를 설정할 수 있습니다. 기본값이 아닌 도메인에 있는 사용자는 로그인할 때 도메인을 지정할 수 있습니다(DOMAIN\user 또는 user@DOMAIN).
vSphere 5.5	administrator@vsphere.local 또는 업그레이드 도중 지정된 도메인의 관리자 모든 ID 소스의 모든 사용자가 이전처럼 로그인할 수 있습니다.	

vCenter Single Sign-On이 포함되지 않은 vSphere 5.0에서 vCenter Single Sign-On이 포함된 버전으로 업그레이드하는 경우 로컬 운영 체제 사용자는 Active Directory와 같은 디렉토리 서비스의 사용자보다 중요성이 훨씬 낮아집니다. 따라서 로컬 운영 체제 사용자를 인증된 사용자로 계속 유지하는 것이 항상 가능하지도 않을 뿐 아니라 경우에 따라서는 바람직하지도 않습니다.

사용자 지정 설치 업그레이드 후 로그인 가능한 사용자

사용자 지정 설치 옵션을 사용하여 프로비저닝한 환경을 업그레이드하는 경우의 결과는 초기 선택에 따라 달라집니다.

- vCenter Single Sign-On이 vCenter Server 시스템과 같은 노드에 있는 경우에는 내장된 Platform Services Controller가 있는 설치 환경이 만들어집니다.
- vCenter Single Sign-On이 vCenter Server 시스템과 다른 노드에 있는 경우에는 외부 Platform Services Controller가 있는 설치 환경이 만들어집니다.
- vSphere 5.0에서 업그레이드하는 경우 업그레이드 도중 외부 또는 내장된 Platform Services Controller를 선택할 수 있습니다.

업그레이드 후의 로그인 권한은 몇 가지 요소에 따라 달라집니다.

표 2-3. 사용자 지정 설치 환경 업그레이드 후 로그인 권한

소스 버전	로그인 액세스 권한을 부여할 대상	참고
vSphere 5.0	<p>vCenter Single Sign-On은 Platform Services Controller가 설치된 시스템의 로컬 운영 체제 사용자를 인식하지만 vCenter Server가 설치된 시스템의 경우는 인식하지 않습니다.</p> <p>참고 특히 페더레이션된 환경에서는 로컬 운영 체제 사용자를 관리에 사용하는 것을 권장하지 않습니다.</p> <p>administrator@vsphere.local은 vCenter Single Sign-On 및 각 vCenter Server 인스턴스에 관리자 로 로그인할 수 있습니다.</p>	<p>5.0 설치가 Active Directory 사용자를 지원하는 경우 업그레이드 후에는 해당 사용자가 더 이상 액세스 권한을 갖지 않습니다. Active Directory 도메인을 ID 소스로 추가할 수 있습니다.</p>
vSphere 5.1 또는 vSphere 5.5	<p>vCenter Single Sign-On은 Platform Services Controller가 설치된 시스템의 로컬 운영 체제 사용자를 인식하지만 vCenter Server가 설치된 시스템의 경우는 인식하지 않습니다.</p> <p>참고 특히 페더레이션된 환경에서는 로컬 운영 체제 사용자를 관리에 사용하는 것을 권장하지 않습니다.</p> <p>administrator@vsphere.local은 vCenter Single Sign-On 및 각 vCenter Server 인스턴스에 관리자 로 로그인할 수 있습니다.</p> <p>vSphere 5.1에서 업그레이드하는 경우 Admin@SystemDomain은 administrator@vsphere.local과 동일한 권한을 가집니다.</p>	<p>vSphere 5.5부터는 vCenter Single Sign-On이 하나의 기본 ID 소스만 지원합니다.</p> <p>기본 ID 소스를 설정할 수 있습니다.</p> <p>기본값이 아닌 도메인에 있는 사용자는 로그인할 때 도메인을 지정할 수 있습니다(DOMAIN/user 또는 user@DOMAIN).</p>

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 이 인증서를 사용하여 vCenter Single Sign-On에 인증합니다. vCenter Single Sign-On은 솔루션 사용자에게 SAML 토큰을 제공하며, 그러면 솔루션 사용자는 환경의 다른 서비스와 상호 작용할 수 있습니다.
- 다른 사용자가 환경에 로그인하면(예를 들어 vSphere Web 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 Web Client의 **관리 > 사용 권한** 인터페이스에서 이러한 사용 권한을 할당합니다. [장 4 vSphere 사용 권한 및 사용자 관리 작업](#)의 내용을 참조하십시오.

vCenter Single Sign-On 및 vCenter Server 사용자

vSphere Web Client를 사용하는 경우 사용자는 vSphere Web Client 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. [장 4 vSphere 사용 권한 및 사용자 관리 작업](#)의 내용을 참조하십시오.

설치가 완료되면 administrator@vsphere.local 사용자는 vCenter Single Sign-On과 vCenter Server 모두에 관리자 권한으로 액세스할 수 있습니다. 그런 다음 ID 소스를 추가하고, 기본 ID 소스를 설정하고, vCenter Single Sign-On 도메인(vsphere.local)의 사용자 및 그룹을 관리할 수 있습니다.

vCenter Single Sign-On에 인증할 수 있는 모든 사용자는 암호를 알고 있기만 하면 암호가 만료되더라도 자신의 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 Web 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 Web Client에 로그인해야 합니다. 이러한 사용자는 인증 후 vSphere Web Client에서 vCenter Single Sign-On 관리 인터페이스에 액세스하여 ID 소스 및 기본 도메인을 관리하고, 암호 정책을 지정하고, 그 밖의 관리 작업을 수행할 수 있습니다. [vCenter Single Sign-On ID 소스 구성](#)의 내용을 참조하십시오.

참고 administrator@vsphere.local 사용자의 이름을 바꿀 수는 없습니다. 보안을 강화하려면 vsphere.local 도메인에 이름 지정된 사용자를 추가로 생성하고 이러한 사용자에게 관리 권한을 할당하는 것이 좋습니다. 그러면 administrator@vsphere.local의 사용을 중지할 수 있습니다.

다양한 vSphere 버전에서의 인증

사용자가 5.0.x 이전 버전의 vCenter Server 시스템에 연결하는 경우 vCenter Server는 Active Directory 도메인이나 로컬 운영 체제 사용자 목록을 기준으로 사용자를 검증하여 인증합니다. vCenter Server 5.1 이상에서는 vCenter Single Sign-On을 통해 사용자가 인증됩니다.

참고 vSphere Web Client를 사용하여 vCenter Server 5.0 이전 버전을 관리할 수는 없으므로 vCenter Server를 버전 5.1 이상으로 업그레이드하십시오.

ESXi 사용자

ESXi는 vCenter Single Sign-On과 통합되어 있지 않으므로 ESXi 호스트를 Active Directory 도메인에 명시적으로 추가해야 합니다. [Active Directory를 사용하도록 호스트 구성](#)의 내용을 참조하십시오.

여전히 vSphere Client, vCLI 또는 PowerCLI를 사용하여 로컬 ESXi 사용자를 생성할 수 있습니다. vCenter Server는 ESXi의 로컬 사용자를 인식하지 못하고 ESXi는 vCenter Server 사용자를 인식하지 못합니다.

참고 가능하면 vCenter Server를 통해 ESXi 호스트에 대한 사용 권한을 관리하십시오.

vCenter Server 구성 요소에 로그인하는 방법

사용자가 vSphere Web Client에서 vCenter Server 시스템에 로그인할 때 로그인 동작은 해당 사용자가 기본 도메인(기본 ID 소스로 설정된 도메인)에 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.

참고 환경에 Active Directory 계층이 포함된 경우 VMware 기술 자료 문서 2064250에서 지원되는 설정과 지원되지 않는 설정에 대한 자세한 내용을 참조하십시오.

vsphere.local 도메인의 그룹

vsphere.local 도메인에는 사전 정의된 여러 그룹이 포함되어 있습니다. 해당 작업을 수행할 수 있는 그룹 중 하나에 사용자를 할당합니다.

vCenter Server 계층의 모든 개체의 경우 사용자 및 역할을 개체와 쌍으로 연결함으로써 사용 권한을 할당합니다. 예를 들어 리소스 풀을 선택하고 사용자 그룹에 해당하는 역할을 제공하여 리소스 풀에 대한 읽기 권한을 제공할 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 라이선스를 관리할 수 있습니다.

다음 그룹은 vsphere.local에서 사전 정의됩니다.

참고 이들 중 많은 그룹이 vsphere.local 내부에서 사용되거나 사용자에게 상위 수준의 관리 권한을 제공합니다. 위험에 대해 신중하게 고려한 후에만 이러한 그룹에 사용자를 추가하십시오.

참고 vsphere.local 도메인에서 미리 정의된 그룹 중 어느 것도 삭제하지 마십시오. 그렇게 할 경우 인증 또는 인증서 프로비저닝 관련 오류가 발생할 수 있습니다.

표 2-4. vsphere.local 도메인의 그룹

권한	설명
사용자	vsphere.local 도메인의 사용자입니다.
SolutionUsers	vCenter Services를 구성하는 솔루션 사용자입니다. 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. 이 그룹에 멤버를 추가하는 것은 일반적으로 권장되지 않습니다.
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 Web Client를 사용하여 해당 작업을 수행합니다.
SystemConfiguration.BashShellAdministrators	이 그룹은 vCenter Server Appliance 배포에서만 사용할 수 있습니다. 이 그룹의 사용자는 BASH 셸에 대한 액세스를 사용하거나 사용하지 않도록 설정할 수 있습니다. 기본적으로 SSH를 사용하여 vCenter Server Appliance에 연결하는 사용자는 제한된 셸의 명령에만 액세스할 수 있습니다. 이 그룹의 사용자는 BASH 셸에 액세스할 수 있습니다.
ActAsUsers	Act-As 사용자 멤버는 vCenter Single Sign-On에서 actas 토큰을 가져올 수 있습니다.
ExternalIPDUsers	이 그룹은 vSphere에서 사용되지 않습니다. 이 그룹은 VMware vCloud Air와 함께 사용해야 합니다.
SystemConfiguration.Administrators	SystemConfiguration.Administrators 그룹의 멤버는 vSphere Web Client에서 시스템 구성을 보고 관리할 수 있습니다. 이 사용자는 서비스 보기, 시작 및 다시 시작, 서비스 문제 해결, 사용 가능한 노드 보기 및 해당 노드 관리를 수행할 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.
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 라이선싱 관련 데이터에 대한 전체 쓰기 액세스 권한이 있으며 라이선싱 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. 이 그룹에 멤버를 추가하는 것은 일반적으로 권장되지 않습니다.

vCenter Server 암호 요구 사항 및 잠금 동작

환경을 관리하려면 vCenter Single Sign-On 암호 정책, vCenter Server 암호 및 잠금 동작을 알아야 합니다.

vCenter Single Sign-On 관리자 암호

administrator@vsphere.local의 암호가 다음과 같은 요구 사항을 충족해야 합니다.

- 8자 이상
- 소문자 1자 이상
- 숫자 1자 이상
- 특수 문자 1자 이상

administrator@vsphere.local의 암호의 길이가 20자를 초과할 수 없습니다. 표시되는 ASCII 문자만 허용됩니다. 즉, 예를 들어 공백 문자를 사용할 수 없습니다.

vCenter Server 암호

vCenter Server에서 암호 요구 사항은 vCenter Single Sign-On 또는 구성된 ID 소스(예: Active Directory, OpenLDAP 또는 vCenter Single Sign-On Server의 로컬 운영 체제)에 의해 지정됩니다(권장되지 않음).

잠금 동작

사용자는 미리 설정된 수의 연속 시도 실패 후에 잠깁니다. 기본적으로 사용자는 3분 동안 5번의 연속 시도 실패 후에 잠기며 5분 후에 자동으로 잠금이 해제됩니다. 잠금 정책을 사용하여 이러한 기본값을 변경할 수 있습니다. [vCenter Single Sign-On 잠금 정책 편집](#)를 참조하십시오.

vSphere 6.0부터 시스템 도메인 관리자(기본적으로 administrator@vsphere.local)는 잠금 정책의 영향을 받지 않습니다.

사용자는 `dir-cli password change` 명령을 사용하여 자신의 암호를 변경할 수 있습니다. 사용자가 암호를 잊은 경우 관리자가 `dir-cli password reset` 명령을 사용하여 암호를 재설정할 수 있습니다.

ESXi 로컬 사용자의 암호에 대한 자세한 내용은 [ESXi 암호 및 계정 잠금](#) 항목을 참조하십시오.

vCenter Single Sign-On ID 소스 구성

사용자가 로그인하면 vCenter Single Sign-On은 사용자를 인증할 수 있는지를 기본 ID 소스에서 확인합니다. ID 소스를 추가하고, ID 소스를 제거하고, 기본값을 변경할 수 있습니다.

vCenter Single Sign-On은 vSphere Web 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. 기본적으로 새 설치에서 administrator@vsphere.local 사용자에게만 vCenter Single Sign-On Server에 대한 관리자 권한이 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 Server가 사용자 인증에 사용할 수 있는 사용자 및 그룹의 저장소입니다.

■ 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.

■ vCenter Single Sign-On ID 소스 추가

사용자는 vCenter Single Sign-On ID 소스로 추가된 도메인에 속해 있는 경우에만 vCenter Server에 로그인할 수 있습니다. vCenter Single Sign-On 관리자는 vSphere Web Client에서 ID 소스를 추가할 수 있습니다.

■ vCenter Single Sign-On ID 소스 편집

vSphere 사용자는 ID 소스에 정의되어 있습니다. vCenter Single Sign-On과 연결된 ID 소스의 세부 정보를 편집할 수 있습니다.

■ vCenter Single Sign-On ID 소스 제거

vSphere 사용자는 ID 소스에 정의되어 있습니다. 등록된 ID 소스 목록에서 ID 소스를 제거할 수 있습니다.

■ Windows 세션 인증을 사용하는 vCenter Single Sign-On 사용

vCenter Single Sign-On을 Windows 세션 인증(SSPI)과 함께 사용할 수 있습니다. 로그인 페이지에 확인란이 표시되도록 하려면 클라이언트 통합 플러그인을 설치해야 합니다.

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 Server가 사용자 인증에 사용할 수 있는 사용자 및 그룹의 저장소입니다.

ID 소스는 사용자 및 그룹 데이터의 모음입니다. 사용자 및 그룹 데이터는 Active Directory, OpenLDAP 또는 vCenter Single Sign-On이 설치된 시스템의 운영 체제 로컬 위치에 저장됩니다.

설치 후에는 모든 vCenter Single Sign-On 인스턴스에 ID 소스 *your_domain_name*(예: vsphere.local)이 있습니다. 이 ID 소스는 vCenter Single Sign-On 내부에서만 사용됩니다. vCenter Single Sign-On 관리자는 ID 소스를 추가하고, 기본 ID 소스를 설정하고, vsphere.local ID 소스에서 사용자 및 그룹을 생성할 수 있습니다.

ID 소스 유형

버전 5.1 이전의 vCenter Server에서는 사용자 저장소로 Active Directory 및 로컬 운영 체제 사용자가 지원되었습니다. 따라서 로컬 운영 체제 사용자가 항상 vCenter Server 시스템에 인증할 수 있었습니다. vCenter Server 버전 5.1 및 버전 5.5에서는 인증에 vCenter Single Sign-On을 사용합니다. vCenter Single Sign-On 5.1에 지원되는 ID 소스 목록은 vSphere 5.1 설명서를 참조하십시오. vCenter Single Sign-On 5.5에서는 다음과 같은 유형의 사용자 저장소를 ID 소스로 지원하지만 하나의 기본 ID 소스만 지원합니다.

- Active Directory 버전 2003 이상. vSphere Web Client에서는 **Active Directory(통합 Windows 인증)**로 표시됩니다. vCenter Single Sign-On에서는 단일 Active Directory 도메인을 ID 소스로 지정할 수 있습니다. 도메인은 하위 도메인을 포함할 수도 있고 그 자체가 포리스트 루트 도메인일 수도 있습니다. VMware KB 문서 [2064250](#)에서는 vCenter Single Sign-On에서 지원되는 Microsoft Active Directory 트러스트에 대해 설명합니다.
- LDAP를 통한 Active Directory. vCenter Single Sign-On에서는 LDAP를 통한 Active Directory ID 소스가 여러 개 지원됩니다. 이 ID 소스 유형은 vSphere 5.1에 포함된 vCenter Single Sign-On 서비스와의 호환성을 위해 포함되며 vSphere Web Client에 **Active Directory LDAP 서버**로 표시됩니다.
- OpenLDAP 버전 2.4 이상. vCenter Single Sign-On에서는 여러 OpenLDAP ID 소스가 지원됩니다. vSphere Web Client에서는 **OpenLDAP**로 표시됩니다.
- 로컬 운영 체제 사용자. 로컬 운영 체제 사용자는 vCenter Single Sign-On Server가 실행 중인 운영 체제의 로컬에 위치합니다. 로컬 운영 체제 ID 소스는 기본 vCenter Single Sign-On Server 배포에만 존재하며 vCenter Single Sign-On 인스턴스가 여러 개인 배포에서는 사용할 수 없습니다. 로컬 운영 체제 ID 소스는 하나만 허용됩니다. vSphere Web Client에서는 **localos**로 표시됩니다.

참고 Platform Services Controller가 vCenter Server 시스템과 다른 시스템에 있는 경우 로컬 운영 체제 사용자를 사용하지 마십시오. 로컬 운영 체제 사용자 사용이 내장된 배포 환경에 적합할 수 있지만 권장되지는 않습니다.

- vCenter Single Sign-On 시스템 사용자. vCenter Single Sign-On을 설치할 때 vsphere.local이라는 시스템 ID 소스가 정확히 한 개 생성됩니다. vSphere Web Client에서는 **vsphere.local**로 표시됩니다.

참고 기본 도메인은 항상 하나만 존재합니다. 기본 도메인이 아닌 도메인의 사용자는 로그인할 때 도메인 이름(*DOMAIN\user*)을 추가해야 성공적으로 인증할 수 있습니다.

vCenter Single Sign-On ID 소스는 vCenter Single Sign-On 관리자가 관리합니다.

ID 소스를 vCenter Single Sign-On Server 인스턴스에 추가할 수 있습니다. 원격 ID 소스는 Active Directory 및 OpenLDAP 서버 구현으로 제한됩니다.

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 Web Client에서 vCenter Server 시스템에 로그인할 때 로그인 동작은 해당 사용자가 기본 도메인(기본 ID 소스로 설정된 도메인)에 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 Directory에 서는 해당 계층에 있는 다른 도메인의 사용자가 인증되었는지 여부를 확인합니다.

절차

- 1 administrator@vsphere.local 또는 vCenter Single Sign-On 관리자 권한을 가진 다른 사용자로 vSphere Web Client에 로그인합니다.

vCenter Single Sign-On 관리자 권한을 가진 사용자는 vsphere.local 도메인에서 Administrators 그룹에 있습니다.
- 2 **관리 > Single Sign-On > 구성**으로 이동합니다.
- 3 **ID 소스** 탭에서 ID 소스를 선택하고 **기본 도메인으로 설정** 아이콘을 클릭합니다.

도메인 화면에서 기본 도메인은 도메인 열에 (기본값)이 표시됩니다.

vCenter Single Sign-On ID 소스 추가

사용자는 vCenter Single Sign-On ID 소스로 추가된 도메인에 속해 있는 경우에만 vCenter Server에 로그인할 수 있습니다. vCenter Single Sign-On 관리자는 vSphere Web Client에서 ID 소스를 추가할 수 있습니다.

ID 소스는 네이티브 Active Directory(통합 Windows 인증) 도메인이거나 OpenLDAP 디렉토리 서비스일 수 있습니다. 이전 버전과의 호환성을 위해 Active Directory LDAP 서버를 사용할 수도 있습니다.

[vCenter Single Sign-On을 사용하는 vCenter Server에 대한 ID 소스 항목을 참조하십시오.](#)

설치가 완료되면 다음과 같은 기본 ID 소스와 사용자를 사용할 수 있습니다.

locals

모든 로컬 운영 체제 사용자. 업그레이드 중인 경우 이미 인증이 가능한 사용자는 계속 인증을 수행할 수 있습니다. localos ID 소스 사용은 Platform Services Controller를 사용하는 환경에서는 의미가 없습니다.

vsphere.local

vCenter Single Sign-On 내부 사용자를 포함합니다.

사전 요구 사항

ID 소스로 추가하려는 도메인은 vCenter Single Sign-On이 실행 중인 시스템에서 사용할 수 있어야 합니다. vCenter Server Appliance를 사용하는 경우에는 "vCenter Server Appliance 구성" 설명서를 참조하십시오.

절차

- 1 administrator@vsphere.local 또는 vCenter Single Sign-On 관리자 권한을 가진 다른 사용자로 vSphere Web Client에 로그인합니다.

vCenter Single Sign-On 관리자 권한을 가진 사용자는 vsphere.local 도메인에서 Administrators 그룹에 있습니다.
- 2 **관리 > Single Sign-On > 구성**으로 이동합니다.
- 3 **ID 소스** 탭에서 **ID 소스 추가** 아이콘을 클릭합니다.
- 4 ID 소스 유형을 선택하고 ID 소스 설정을 입력합니다.

옵션	설명
Active Directory(통합 Windows 인증)	이 옵션은 네이티브 Active Directory를 구현하는 데 사용합니다. 이 옵션을 사용하면 vCenter Single Sign-On 서비스가 실행 중인 시스템이 Active Directory 도메인에 있어야 합니다. Active Directory ID 소스 설정 항목을 참조하십시오.
Active Directory를 LDAP 서버로	이 옵션을 사용하면 이전 버전과 호환됩니다. 이 경우 도메인 컨트롤러 및 기타 정보를 지정해야 합니다. Active Directory LDAP 서버 및 OpenLDAP 서버 ID 소스 설정 항목을 참조하십시오.
OpenLDAP	이 옵션은 OpenLDAP ID 소스에 사용합니다. Active Directory LDAP 서버 및 OpenLDAP 서버 ID 소스 설정 항목을 참조하십시오.
LocalOS	이 옵션은 로컬 운영 체제를 ID 소스로 추가하는 데 사용합니다. 로컬 운영 체제의 이름에 대한 메시지만 표시됩니다. 이 옵션을 선택하면 지정한 시스템의 모든 사용자가 다른 도메인의 일부가 아니더라도 vCenter Single Sign-On에 표시됩니다.

참고 사용자 계정을 잠그거나 사용하지 않도록 설정하면 Active Directory 도메인에서 인증 및 그룹/사용자 검색에 실패합니다. 사용자 계정은 사용자 및 그룹 OU에 대한 읽기 전용 액세스 권한이 있어야 하며 사용자 및 그룹 특성을 읽을 수 있어야 합니다. 이것이 인증 권한에 대한 기본 Active Directory 도메인 구성입니다. 특별한 서비스 사용자를 사용하는 것이 좋습니다.

- 5 Active Directory LDAP 서버 또는 OpenLDAP ID 소스를 구성한 경우 **연결 테스트**를 클릭하여 ID 소스에 연결할 수 있는지 확인합니다.
- 6 **확인**을 클릭합니다.

다음에 수행할 작업

ID 소스가 추가되면 **권한 없음** 역할이 있는 사용자를 제외한 모든 사용자를 인증할 수 있습니다. vCenter Server **Modify.permissions** 권한이 있는 사용자는 사용자 또는 사용자 그룹에 vCenter Server에 로그인하여 개체를 보고 관리할 수 있는 권한을 할당할 수 있습니다. "vSphere 보안" 설명서를 참조하십시오.

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 ID 소스 사용을 위한 필수 구성 요소

해당 ID 소스를 사용할 수 있는 경우에만 Active Directory ID 소스를 사용하도록 vCenter Single Sign-On을 설정할 수 있습니다.

- Windows 설치의 경우 Windows 시스템을 Active Directory 도메인에 가입합니다.
- vCenter Server Appliance의 경우 "vCenter Server Appliance 구성" 설명서의 지침을 따릅니다.

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 [2070433](#)을 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.

참고 vSphere 5.5에서 vCenter Single Sign-On은 SPN을 지정하는 경우에도 시스템 계정을 사용합니다. VMware 기술 자료 문서 [2087978](#)를 참조하십시오.

표 2-5. 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. vCenter Server Appliance를 사용 중인 경우 네트워크 설정 구성에 대한 정보를 사용하여 DNS 서버 설정을 업데이트합니다.
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.

표 2-5. ID 소스 추가 설정 (계속)

텍스트 상자	설명
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 -s를 실행하면 중복 SPN이 생성되지 않았는지 확인할 수 있습니다. setspn에 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.

Active Directory LDAP 서버 및 OpenLDAP 서버 ID 소스 설정

이전 버전과의 호환성을 위해 Active Directory를 LDAP 서버 ID 소스로 사용할 수 있습니다. 입력이 거의 필요 없는 설치에는 Active Directory(통합 Windows 인증) 옵션을 사용하십시오. OpenLDAP 서버 ID 소스는 OpenLDAP를 사용하는 환경에서 사용할 수 있습니다.

OpenLDAP ID 소스를 구성하는 경우 추가 요구 사항은 VMware 기술 자료 문서 [2064977](#)을 참조하십시오.

표 2-6. LDAP 서버로 사용되는 Active Directory 및 OpenLDAP 설정

필드	설명
이름	ID 소스의 이름입니다.
사용자의 기본 DN	사용자의 기본 고유 이름입니다.
도메인 이름	도메인의 FDQN(예: example.com)입니다. 이 필드에 IP 주소를 입력하지 마십시오.
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.
그룹의 기본 DN	그룹의 기본 고유 이름입니다.

표 2-6. LDAP 서버로 사용되는 Active Directory 및 OpenLDAP 설정 (계속)

필드	설명
기본 서버 URL	<p>도메인의 기본 도메인 컨트롤러 LDAP 서버입니다.</p> <p>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 ldap: 연결의 경우 3268이고 ldaps: 연결의 경우 3269입니다.</p> <p>기본 또는 보조 LDAP URL에 ldaps://를 사용하는 경우 Active Directory 서버의 LDAPS 끝점에 대한 신뢰를 설정하는 인증서가 필요합니다.</p>
보조 서버 URL	<p>페일오버에서 사용되는 보조 도메인 컨트롤러 LDAP 서버의 주소입니다.</p>
인증서 선택	<p>Active Directory LDAP 서버 또는 OpenLDAP 서버 ID 소스와 함께 LDAPS를 사용하려는 경우 [URL] 필드에 ldaps://를 입력하면 [인증서 선택] 버튼을 사용할 수 있게 됩니다. 보조 URL은 필요하지 않습니다.</p>
사용자 이름	<p>도메인에서 사용자 및 그룹의 기본 DN에 대해 최소한 읽기 전용 액세스 권한이 있는 사용자의 ID입니다.</p>
암호	<p>사용자 이름에서 지정된 사용자의 암호입니다.</p>

vCenter Single Sign-On ID 소스 편집

vSphere 사용자는 ID 소스에 정의되어 있습니다. vCenter Single Sign-On과 연결된 ID 소스의 세부 정보를 편집할 수 있습니다.

절차

- 1 administrator@vsphere.local 또는 vCenter Single Sign-On 관리자 권한을 가진 다른 사용자로 vSphere Web Client에 로그인합니다.

vCenter Single Sign-On 관리자 권한을 가진 사용자는 vsphere.local 도메인에서 Administrators 그룹에 있습니다.
- 2 **관리 > Single Sign-On > 구성**을 찾습니다.
- 3 **ID 소스** 탭을 클릭합니다.
- 4 표의 ID 소스를 마우스 오른쪽 버튼으로 클릭하고 **ID 소스 편집**을 선택합니다.

5 ID 소스 설정을 편집합니다. 사용할 수 있는 옵션은 선택한 ID 소스 유형에 따라 다릅니다.

옵션	설명
Active Directory(통합 Windows 인증)	이 옵션은 네이티브 Active Directory를 구현하는 데 사용됩니다. 이 옵션을 사용하면 vCenter Single Sign-On 서비스가 실행 중인 시스템이 Active Directory 도메인에 있어야 합니다. Active Directory ID 소스 설정 항목을 참조하십시오.
Active Directory를 LDAP 서버로	이 옵션을 사용하면 이전 버전과 호환됩니다. 이 경우 도메인 컨트롤러 및 기타 정보를 지정해야 합니다. Active Directory LDAP 서버 및 OpenLDAP 서버 ID 소스 설정 항목을 참조하십시오.
OpenLDAP	이 옵션은 OpenLDAP ID 소스에 사용됩니다. Active Directory LDAP 서버 및 OpenLDAP 서버 ID 소스 설정 항목을 참조하십시오.
LocalOS	이 옵션은 로컬 운영 체제를 ID 소스로 추가하는 데 사용됩니다. 로컬 운영 체제의 이름에 대한 메시지만 표시됩니다. 이 옵션을 선택하면 지정한 시스템의 모든 사용자가 다른 도메인의 일부가 아니더라도 vCenter Single Sign-On에 표시됩니다.

6 **연결 테스트**를 클릭하여 ID 소스에 연결할 수 있는지 확인합니다.

7 **확인**을 클릭합니다.

vCenter Single Sign-On ID 소스 제거

vSphere 사용자는 ID 소스에 정의되어 있습니다. 등록된 ID 소스 목록에서 ID 소스를 제거할 수 있습니다.

절차

- 1 administrator@vsphere.local 또는 vCenter Single Sign-On 관리자 권한을 가진 다른 사용자로 vSphere Web Client에 로그인합니다.
vCenter Single Sign-On 관리자 권한을 가진 사용자는 vsphere.local 도메인에서 Administrators 그룹에 있습니다.
- 2 **관리 > Single Sign-On > 구성**을 찾습니다.
- 3 ID 소스 탭에서 ID 소스를 선택하고 **ID 소스 삭제** 아이콘을 클릭합니다.
- 4 삭제할 것인지 묻는 메시지가 표시되면 **예**를 클릭합니다.

Windows 세션 인증을 사용하는 vCenter Single Sign-On 사용

vCenter Single Sign-On을 Windows 세션 인증(SSPI)과 함께 사용할 수 있습니다. 로그인 페이지에 확인란이 표시되도록 하려면 클라이언트 통합 플러그인을 설치해야 합니다.

SSPI를 사용하면 현재 시스템에 로그인되어 있는 사용자의 로그인 속도가 향상됩니다.

사전 요구 사항

Windows 도메인을 올바르게 설정해야 합니다. VMware 기술 자료 문서 [2064250](#)를 참조하십시오.

절차

- 1 vSphere Web Client 로그인 페이지로 이동합니다.
- 2 **Windows 세션 인증 사용** 확인란을 사용할 수 없는 경우 로그인 페이지 아래쪽에서 **클라이언트 통합 플러그인 다운로드**를 클릭합니다.
- 3 브라우저에서 인증서 오류가 발생하거나 팝업 차단이 실행되어 설치가 차단되면 브라우저의 도움말 지침에 따라 문제를 해결합니다.
- 4 다른 브라우저를 닫으라는 메시지가 표시되면 브라우저를 닫습니다.
설치가 완료되면 모든 브라우저에 플러그인을 사용할 수 있습니다. 브라우저에서 요구하는 경우 개별 세션 또는 모든 세션에 대해 플러그인을 허용해야 할 수 있습니다.
- 5 브라우저를 종료했다가 다시 시작합니다.
다시 시작한 후에는 **Windows 세션 인증 사용** 확인란을 선택할 수 있습니다.

vCenter Server 이중 인증

vCenter Single Sign-On을 사용하면 vCenter Single Sign-On에 알려진 ID 소스에 포함된 사용자의 이름 및 암호를 사용하거나, Active Directory ID 소스에 대한 Windows 세션 인증을 사용하여 인증할 수 있습니다. vSphere 6.0 업데이트 2부터는 스마트 카드(UPN 기반의 CAC 즉 Common Access Card) 또는 RSA SecurID 토큰을 사용한 인증도 지원됩니다.

이중 인증 방법

이중 인증 방법은 주로 정부 기관 또는 대기업에서 사용됩니다.

CAC(Common Access Card) 인증

CAC 인증의 경우 사용자가 로그인하는 컴퓨터의 USB 드라이브에 물리적 카드를 연결해야만 액세스가 허용됩니다. PKI를 배포할 때 CA에서 클라이언트 인증서로 스마트 카드 인증서만 발급한 경우에는 사용자에게 스마트 카드 인증서만 제공됩니다. 사용자가 인증서를 선택하면 PIN을 묻는 메시지가 표시됩니다. 물리적 카드 및 인증서와 일치하는 PIN을 모두 가진 사용자만 로그인할 수 있습니다.

RSA SecurID 인증

RSA SecureID 인증을 사용하려면 올바르게 구성된 RSA Authentication Manager가 환경에 포함되어 있어야 합니다. Platform Services Controller가 RSA 서버를 가리키도록 구성되어 있고 RSA SecurID 인증이 사용되도록 설정되어 있으면 사용자는 자신의 사용자 이름 및 토큰을 사용하여 로그인할 수 있습니다.

참고 vCenter Single Sign-On은 네이티브 SecurID만 지원하며 RADIUS 인증은 지원하지 않습니다.

기본값이 아닌 인증 방법 지정

관리자는 Platform Services Controller 웹 인터페이스를 사용하거나 sso-config 스크립트(Windows에서는 sso-config.bat 및 장치에서는 sso-config.sh)를 사용하여 설정 작업을 수행할 수 있습니다.

- Common Access Card 인증의 경우 sso-config 스크립트를 사용하여 웹 브라우저를 설정해야 하며 Platform Services Controller 웹 인터페이스 또는 sso-config를 사용하여 vCenter Single Sign-On 설정을 수행할 수 있습니다. 설정에는 CAC 인증을 사용하도록 설정하고, 인증서 해지 정책을 구성하고 로그인 배너를 설정하는 작업이 포함됩니다.
- RSA SecureID의 경우 sso-config 스크립트를 사용하여 도메인의 RSA Authentication Manager를 구성하고 RSA 토큰 인증을 사용하도록 설정합니다. 이 인증 방법은 사용하도록 설정한 경우 Platform Services Controller 웹 인터페이스에 표시되지만, 웹 인터페이스에서 RSA SecureID 인증을 구성할 수는 없습니다.

여러 인증 방법 결합

sso-config를 사용하여 각 인증 방법을 개별적으로 사용하도록 설정하거나 사용하지 않도록 설정할 수 있습니다. 예를 들어 이중 인증 방법 중 하나를 테스트하는 동안에는 초기에 사용자 이름 및 암호 인증을 사용하도록 설정해 두었다가 나중에 인증 방법 중 하나만 사용하도록 설정할 수 있습니다.

vCenter Single Sign-On을 위한 스마트 카드 인증 구성

사용자가 vSphere Web Client에서 vCenter Server 또는 연결된 Platform Services Controller에 연결할 때 스마트 카드 인증이 필요하도록 환경을 설정할 수 있습니다.

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. Common Access Card는 각 시스템에 스마트 카드 판독기가 포함되어 있고, Common Access Card를 관리하는 스마트 카드 하드웨어 드라이버가 사전 설치되어 있는 환경에서 사용됩니다.

vCenter Single Sign-On에 대해 스마트 카드 인증을 구성할 경우, vCenter Server 또는 Platform Services Controller 시스템에 로그인하는 사용자에게는 다음과 같이 스마트 카드와 PIN 조합을 사용하여 인증하라는 메시지가 표시됩니다.

- 1 사용자가 스마트 카드를 스마트 카드 판독기에 넣으면 vCenter Single Sign-On이 카드에서 인증서를 읽습니다.
- 2 vCenter Single Sign-On은 인증서를 선택하라는 메시지를 표시한 후 해당 인증서의 PIN을 묻습니다.

- 3 vCenter Single Sign-On은 스마트 카드에 있는 인증서가 알려진 인증서인지 그리고 PIN이 올바른지 여부를 확인합니다. 해지 확인이 활성화되어 있으면 vCenter Single Sign-On은 인증서가 해지되었는지 여부도 확인합니다.
- 4 인증서가 알려진 인증서이고 해지되지 않았으면 사용자가 인증되고, 이 사용자는 자신에게 권한이 부여된 작업을 수행할 수 있습니다.

참고 대부분의 경우 테스트 중에는 사용자 이름 및 암호 인증을 사용하도록 설정해 두는 것이 좋습니다. 테스트가 완료된 후에는 사용자 이름 및 암호 인증을 사용하지 않도록 설정하고 스마트 카드 인증을 사용하도록 설정합니다. 이렇게 하면 vSphere Client에서 스마트 카드 로그인만 허용합니다. 시스템에서 루트 또는 관리자 권한을 가진 사용자만 Platform Services Controller에 직접 로그인하여 사용자 이름 및 암호를 다시 사용하도록 설정할 수 있습니다.

명령줄을 사용하여 스마트 카드 인증 구성

sso-config 유틸리티를 사용하면 명령줄에서 스마트 카드 인증을 구성할 수 있습니다. 이 유틸리티는 모든 스마트 카드 구성 작업을 지원합니다.

명령줄에서 스마트 카드 인증을 구성할 때는 항상 sso-config 명령을 먼저 사용하여 Platform Services Controller를 설정합니다. 그런 다음 Platform Services Controller 웹 인터페이스를 사용하여 다른 작업을 수행할 수 있습니다.

- 1 사용자가 로그인할 때 웹 브라우저가 스마트 카드 인증서 제출을 요청하도록 Platform Services Controller를 구성합니다.
- 2 인증 정책을 구성합니다. 정책은 sso-config 스크립트 또는 Platform Services Controller 웹 인터페이스를 사용하여 구성할 수 있습니다. 지원되는 인증 유형의 구성 및 해지 설정은 VMware Directory Service에 저장되며 vCenter Single Sign-On 도메인 내의 모든 Platform Services Controller 인스턴스에 복제됩니다.

스마트 카드 인증을 제외한 다른 모든 인증 방법을 사용하지 않도록 설정한 경우 사용자는 스마트 카드 인증을 사용하여 로그인해야 합니다.

vSphere Web Client에서 로그인할 수 없고 사용자 이름 및 암호 인증 기능이 해제되어 있는 경우 루트 사용자 또는 관리자는 다음 명령을 실행하여 Platform Services Controller 명령줄에서 사용자 이름 및 암호 인증을 다시 사용하도록 설정할 수 있습니다. 이 예제는 Windows에 해당하는 명령이며, Linux의 경우 sso-config.sh 명령을 사용하십시오.

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

다음 위치에서 sso-config 스크립트를 찾을 수 있습니다.

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

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

사전 요구 사항

- 환경에서 Platform Services Controller 버전 6.0 업데이트 2 이상을 사용하고, 현재 vCenter Server 버전 6.0 이상을 사용 중인지 확인합니다. 버전 5.5 노드를 버전 6.0으로 업그레이드합니다.
- 환경에 엔터프라이즈 PKI(공개 키 인프라)가 설정되어 있고 인증서가 다음과 같은 요구 사항을 충족하는지 확인합니다.
 - SAN(주체 대체 이름) 확장의 Active Directory 계정에 해당하는 UPN(사용자 계정 이름)이 있습니다.
 - 인증서의 [애플리케이션 정책] 또는 [고급 키 사용] 필드에 클라이언트 인증을 지정하지 않으면 브라우저에 해당 인증서가 표시되지 않습니다.
- 최종 사용자의 Workstation에서 Platform Services Controller 웹 인터페이스 인증서를 신뢰하는지 확인합니다. 신뢰하지 않는 인증서인 경우 브라우저는 인증을 시도하지 않습니다.
- Active Directory ID 소스를 구성하여 vCenter Single Sign-On에 ID 소스로 추가합니다.
- Active Directory ID 소스에 속한 사용자 한 명 이상에게 vCenter Server 관리자 역할을 할당합니다. 그러면 해당 사용자는 Active Directory 그룹에 속해 있고 vCenter Server 관리자 권한을 갖고 있으므로 인증할 수 있습니다. administrator@vsphere.local 사용자는 스마트 카드 인증을 수행할 수 없습니다.
- 환경에서 Platform Services Controller HA 솔루션을 사용하려면 스마트 카드 인증을 설정하기 전에 모든 HA 구성을 완료해야 합니다. VMware 기술 자료 문서 [2112085\(Windows\)](#) 또는 [2113315\(vCenter Server Appliance\)](#)를 참조하십시오.

절차

- 1 인증서를 가져온 후 sso-config 유틸리티에서 볼 수 있는 폴더에 복사합니다.

옵션	설명
Windows	Platform Services Controller Windows 설치 환경에 로그인한 후 WinSCP 또는 유사한 유틸리티를 사용하여 파일을 복사합니다.
장치	<ol style="list-style-type: none"> a 장치 콘솔에 직접 로그인하거나 SSH를 사용하여 로그인합니다. b 다음과 같이 장치 셸을 사용하도록 설정합니다. <pre>shell.set --enabled True shell chsh -s "/bin/bash" root csh -s "bin/appliance/sh" root</pre> c WinSCP 또는 유사한 유틸리티를 사용하여 인증서를 Platform Services Controller의 /usr/lib/vmware-sso/vmware-sts/conf에 복사합니다. d 필요한 경우 다음과 같이 장치 셸을 사용하지 않도록 설정합니다. <pre>chsh -s "bin/appliancesh" root</pre>

2 각 Platform Services Controller 노드에서 sso-config CLI를 사용하여 스마트 카드 인증 설정을 구성합니다.

- a sso-config 스크립트가 있는 디렉토리로 이동합니다.

옵션	설명
Windows	C:\Program Files\VMware\VCenter server\VMware Identity Services
장치	/opt/vmware/bin

- b 다음 명령을 실행합니다.

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

예:

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

- c 가상 시스템 또는 물리적 시스템을 다시 시작합니다.

```
service-control --stop vmware-stds
service-control --start vmware-stds
```

3 VMDIR(VMware Directory Service)에 대해 스마트 카드 인증을 사용하도록 설정하려면 다음 명령을 실행합니다.

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

예:

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

여러 인증서를 지정하는 경우 인증서 사이에 공백을 사용할 수 없습니다.

4 다른 모든 인증 방법을 사용하지 않도록 설정하려면 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
```

이러한 명령을 사용하면 필요에 따라 여러 인증 방법을 사용하거나 사용하지 않도록 설정할 수 있습니다.

5 (선택 사항) 인증서 정책 허용 목록을 설정하려면 다음 명령을 실행합니다.

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

정책을 여러 개 지정하려면 다음과 같이 각 정책을 명령으로 구분합니다.

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

이 허용 목록은 인증서의 인증서 정책 확장에서 허용되는 정책의 개체 ID를 지정합니다. X509 인증서는 인증서 정책 확장을 가질 수 있습니다.

6 (선택 사항) 구성 정보를 나열하려면 다음 명령을 실행합니다.

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

Platform Services Controller 웹 인터페이스를 사용하여 스마트 카드 인증 관리

Platform Services Controller 웹 인터페이스에서는 스마트 카드 인증의 사용 여부를 설정하고, 로그인 배너를 사용자 지정하고, 해지 정책을 설정할 수 있습니다.

명령줄에서 스마트 카드 인증을 구성할 때는 항상 sso-config 명령을 먼저 사용하여 Platform Services Controller를 설정합니다. 그런 다음 Platform Services Controller 웹 인터페이스를 사용하여 다른 작업을 수행할 수 있습니다.

- 1 사용자가 로그인할 때 웹 브라우저가 스마트 카드 인증서 제출을 요청하도록 Platform Services Controller를 구성합니다.
- 2 인증 정책을 구성합니다. 정책은 sso-config 스크립트 또는 Platform Services Controller 웹 인터페이스를 사용하여 구성할 수 있습니다. 지원되는 인증 유형의 구성 및 해지 설정은 VMware Directory Service에 저장되며 vCenter Single Sign-On 도메인 내의 모든 Platform Services Controller 인스턴스에 복제됩니다.

스마트 카드 인증을 제외한 다른 모든 인증 방법을 사용하지 않도록 설정한 경우 사용자는 스마트 카드 인증을 사용하여 로그인해야 합니다.

vSphere Web Client에서 로그인할 수 없고 사용자 이름 및 암호 인증 기능이 해제되어 있는 경우 루트 사용자 또는 관리자는 다음 명령을 실행하여 Platform Services Controller 명령줄에서 사용자 이름 및 암호 인증을 다시 사용하도록 설정할 수 있습니다. 이 예제는 Windows에 해당하는 명령이며, Linux의 경우 sso-config.sh 명령을 사용하십시오.

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

사전 요구 사항

- 환경에서 Platform Services Controller 버전 6.0 업데이트 2 이상을 사용하고, 현재 vCenter Server 버전 6.0 이상을 사용 중인지 확인합니다. 버전 5.5 노드를 버전 6.0으로 업그레이드합니다.
- 환경에 엔터프라이즈 PKI(공개 키 인프라)가 설정되어 있고 인증서가 다음과 같은 요구 사항을 충족하는지 확인합니다.
 - SAN(주체 대체 이름) 확장의 Active Directory 계정에 해당하는 UPN(사용자 계정 이름)이 있습니다.

- 인증서의 [애플리케이션 정책] 또는 [고급 키 사용] 필드에 클라이언트 인증을 지정하지 않으면 브라우저에 해당 인증서가 표시되지 않습니다.
- 최종 사용자의 Workstation에서 Platform Services Controller 웹 인터페이스 인증서를 신뢰하는지 확인합니다. 신뢰하지 않는 인증서인 경우 브라우저는 인증을 시도하지 않습니다.
- Active Directory ID 소스를 구성하여 vCenter Single Sign-On에 ID 소스로 추가합니다.
- Active Directory ID 소스에 속한 사용자 한 명 이상에게 vCenter Server 관리자 역할을 할당합니다. 그러면 해당 사용자는 Active Directory 그룹에 속해 있고 vCenter Server 관리자 권한을 갖고 있으므로 인증할 수 있습니다. administrator@vsphere.local 사용자는 스마트 카드 인증을 수행할 수 없습니다.
- 환경에서 Platform Services Controller HA 솔루션을 사용하려면 스마트 카드 인증을 설정하기 전에 모든 HA 구성을 완료해야 합니다. VMware 기술 자료 문서 [2112085\(Windows\)](#) 또는 [2113315\(vCenter Server Appliance\)](#)를 참조하십시오.

절차

- 1 인증서를 가져온 후 sso-config 유틸리티에서 볼 수 있는 폴더에 복사합니다.

옵션	설명
Windows	Platform Services Controller Windows 설치 환경에 로그인한 후 WinSCP 또는 유사한 유틸리티를 사용하여 파일을 복사합니다.
장치	<ol style="list-style-type: none"> a 장치 콘솔에 직접 로그인하거나 SSH를 사용하여 로그인합니다. b 다음과 같이 장치 셸을 사용하도록 설정합니다. <pre> shell.set --enabled True shell chsh -s "/bin/bash" root csh -s "bin/appliance/sh" root </pre> c WinSCP 또는 유사한 유틸리티를 사용하여 인증서를 Platform Services Controller의 /usr/lib/vmware-sso/vmware-sts/conf에 복사합니다. d 필요한 경우 다음과 같이 장치 셸을 사용하지 않도록 설정합니다. <pre> chsh -s "bin/appliancesh" root </pre>

- 2 각 Platform Services Controller 노드에서 sso-config CLI를 사용하여 스마트 카드 인증 설정을 구성합니다.

- a sso-config 스크립트가 있는 디렉토리로 이동합니다.

옵션	설명
Windows	C:\Program Files\VMware\VCenter server\VMware Identity Services
장치	/opt/vmware/bin

- b 다음 명령을 실행합니다.

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

예:

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

인증서가 여러 개인 경우 인증서를 쉼표로 구분하되 쉼표 사이에 공백을 사용하지 않습니다.

- c 가상 시스템 또는 물리적 시스템을 다시 시작합니다.

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

- 3 웹 브라우저에서 다음 URL을 지정하여 Platform Services Controller에 연결합니다.

https://psc_hostname_or_IP/psc

내장된 배포에서 Platform Services Controller 호스트 이름 또는 IP 주소는 vCenter Server 호스트 이름 또는 IP 주소와 동일합니다.

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

설치 시 다른 도메인을 지정한 경우에는 administrator@mydomain으로 로그인합니다.

- 5 **Single Sign-On > 구성**으로 이동합니다.

- 6 **스마트 카드 구성**을 클릭하고 **신뢰할 수 있는 CA 인증서** 탭을 선택합니다.

- 7 하나 이상의 신뢰할 수 있는 인증서를 추가하려면 **인증서 추가**를 클릭하고 **찾아보기**를 클릭하고 신뢰할 수 있는 CA에서 모든 인증서를 선택한 후 **확인**을 클릭합니다.

- 8 인증 구성을 지정하려면 **인증 구성** 옆의 **편집**을 클릭한 후 인증 방법을 선택하거나 선택 취소합니다.

RSA SecurID 인증은 이 웹 인터페이스에서 사용하도록 설정하거나 사용하지 않도록 설정할 수 없습니다. 그러나 RSA SecurID를 사용하도록 명령줄에서 설정한 경우에는 해당 상태가 웹 인터페이스에 표시됩니다.

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.

Platform Services Controller 웹 인터페이스를 사용하거나 `sso-config` 스크립트를 사용하여 동작을 사용자 지정할 수 있습니다. 선택하는 설정은 CA에서 지원하는 기능에 따라 부분적으로 달라집니다.

- 해지 확인을 사용하지 않도록 설정하면 vCenter Single Sign-On이 모든 CRL 또는 OCSP 설정을 무시합니다.
- 해지 확인을 사용하도록 설정하면 PKI 설정에 따라 권장되는 설정이 달라집니다.

OCSP 전용

발급하는 CA에서 OCSP 응답자를 지원하는 경우 OCSP를 사용하도록 설정하고 CRL을 페일오버로 사용하지 않도록 설정합니다.

CRL 전용

발급하는 CA에서 OCSP를 지원하지 않는 경우, CRL 확인을 사용하도록 설정하고 OCSP 확인을 사용하지 않도록 설정합니다.

OCSP 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 사용하도록 설정하고 CRL을 OCSP에 대한 페일오버로 사용하도록 설정합니다.

- 해지 확인을 사용하도록 설정하면 고급 사용자가 다음과 같은 추가 설정을 지정할 수 있습니다.

OCSP URL

기본적으로 vCenter Single Sign-On은 검증 중인 인증서에 정의된 OCSP 응답자의 위치를 확인합니다. 인증서에 기관 정보 액세스 확장의 위치가 없거나, 해당 확장을 재정의하려는 경우(예: 환경에서 사용할 수 없는 경우)에는 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 사용하지 않도록 설정하십시오.

CRL 위치

인증서의 CRL 사용 옵션을 사용하지 않도록 설정하고, CRL의 위치(파일 또는 HTTP URL)를 지정하려면 이 속성을 사용합니다.

또한 인증서 정책을 추가하여 vCenter Single Sign-On이 허용하는 인증서를 추가적으로 제한할 수 있습니다.

사전 요구 사항

- 환경에서 Platform Services Controller 버전 6.0 업데이트 2 이상을 사용하고, 현재 vCenter Server 버전 6.0 이상을 사용 중인지 확인합니다. 버전 5.5 노드를 버전 6.0으로 업그레이드합니다.
- 환경에 엔터프라이즈 PKI(공개 키 인프라)가 설정되어 있고 인증서가 다음과 같은 요구 사항을 충족하는지 확인합니다.
 - SAN(주체 대체 이름) 확장의 Active Directory 계정에 해당하는 UPN(사용자 계정 이름)이 있습니다.
 - 인증서의 [애플리케이션 정책] 또는 [고급 키 사용] 필드에 클라이언트 인증을 지정하지 않으면 브라우저에 해당 인증서가 표시되지 않습니다.
- 최종 사용자의 Workstation에서 Platform Services Controller 웹 인터페이스 인증서를 신뢰하는지 확인합니다. 신뢰하지 않는 인증서인 경우 브라우저는 인증을 시도하지 않습니다.
- Active Directory ID 소스를 구성하여 vCenter Single Sign-On에 ID 소스로 추가합니다.
- Active Directory ID 소스에 속한 사용자 한 명 이상에게 vCenter Server 관리자 역할을 할당합니다. 그러면 해당 사용자는 Active Directory 그룹에 속해 있고 vCenter Server 관리자 권한을 갖고 있으므로 인증할 수 있습니다. administrator@vsphere.local 사용자는 스마트 카드 인증을 수행할 수 없습니다.
- 환경에서 Platform Services Controller HA 솔루션을 사용하려면 스마트 카드 인증을 설정하기 전에 모든 HA 구성을 완료해야 합니다. VMware 기술 자료 문서 [2113085\(Windows\)](#) 또는 [2113315\(vCenter Server Appliance\)](#)를 참조하십시오.

절차

- 1 웹 브라우저에서 다음 URL을 지정하여 Platform Services Controller에 연결합니다.
`https://psc_hostname_or_IP/psc`
 내장된 배포에서 Platform Services Controller 호스트 이름 또는 IP 주소는 vCenter Server 호스트 이름 또는 IP 주소와 동일합니다.
- 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@mydomain으로 로그인합니다.
- 3 **Single Sign-On > 구성**으로 이동합니다.
- 4 **인증서 해지 설정**을 클릭하고 해지 확인을 사용하거나 사용하지 않도록 설정합니다.
- 5 현재 환경에 인증서 정책이 적용되어 있으면 **수락된 인증서 정책** 창에서 정책을 추가할 수 있습니다.

RSA SecurID 인증 설정

사용자가 암호 대신 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

- 환경에서 Platform Services Controller 버전 6.0 업데이트 2 이상을 사용하고, 현재 vCenter Server 버전 6.0 이상을 사용 중인지 확인합니다. 버전 5.5 노드를 버전 6.0으로 업그레이드합니다.
- 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](#)를 참조하십시오.
- RSA Authentication Manager 시스템에서 Platform Services Controller 호스트 이름을 확인할 수 있고 Platform Services Controller 시스템에서 RSA Authentication Manager 호스트 이름을 확인할 수 있는지 확인합니다.
- **액세스 > 인증 에이전트 > 구성 파일 생성**을 선택하여 RSA Manager에서 sdconf.rec 파일을 내보냅니다. 생성된 AM_Config.zip 파일의 압축을 해제하고 sdconf.rec 파일을 찾습니다.
- sdconf.rec 파일을 Platform Services Controller 노드에 복사합니다.

절차

- 1 sso-config 스크립트가 있는 디렉토리로 변경합니다.

옵션	설명
Windows	C:\Program Files\VMware\VCenter server\VMware Identity Services
장치	/opt/vmware/bin

- 2 RSA SecurID 인증을 사용하도록 설정하려면 다음 명령을 실행합니다.

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

*tenantName*은 vCenter Single Sign-On 도메인의 이름이며, 기본값은 vsphere.local입니다.

- 3 (선택 사항) 다른 인증 방법을 사용하지 않도록 설정하려면 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|bat] -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|bat] -set_rsa_config [-t tenantName] [-logLevel Level] [-logFileSize Size]
[-maxLogFileSize 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.

userID 특성은 RSA userID로 사용할 LDAP 특성을 결정합니다.

```
sso-config.[sh|bat] -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 이름과 암호 인증이 사용하지 않도록 설정되어 있고 SecurID 토큰 인증이 사용하도록 설정되어 있는 경우 사용자는 자신의 사용자 이름과 SecurID 토큰으로 로그인해야 합니다. 사용자 이름과 암호 로그인 은 더 이상 가능하지 않습니다.

로그인 배너 관리

vSphere 6.0 업데이트 2부터는 환경에 로그인 배너를 포함할 수 있습니다. 원하는 텍스트를 표시하거나, 사용자가 확인란을 클릭해야 하도록 설정할 수 있습니다(예: 약관에 동의함을 나타내는 확인란 선택). 로그인 배너를 사용하도록 설정하거나 사용하지 않도록 설정할 수 있으며, 사용자가 명시적 동의 확인란을 클릭해야 하도록 설정할 수도 있습니다.

절차

- 1 웹 브라우저에서 다음 URL을 지정하여 Platform Services Controller에 연결합니다.

https://psc_hostname_or_IP/psc

내장된 배포에서 Platform Services Controller 호스트 이름 또는 IP 주소는 vCenter Server 호스트 이름 또는 IP 주소와 동일합니다.

- 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@mydomain으로 로그인합니다.

- 3 Single Sign-On에서 **구성**을 선택하고 **로그인 배너** 탭을 클릭합니다.

- 4 **편집**을 클릭하고 로그인 배너를 구성합니다.

옵션	설명
상태	사용 확인란을 클릭하여 로그인 배너를 사용하도록 설정합니다. 이 확인란을 클릭해야 다른 필드를 변경할 수 있습니다.
명시적 동의	사용자가 로그인하기 전에 확인란을 클릭하도록 하려면 명시적 동의 확인란을 클릭합니다. 확인란 없이 메시지를 표시할 수도 있습니다.
제목	배너의 제목입니다. 기본적으로 로그인 배너 텍스트는 I agree to the입니다. 기본 텍스트에 텍스트를 추가할 수 있습니다(예: Terms and Conditions).
메시지	배너를 클릭했을 때 사용자에게 표시되는 메시지입니다. 예를 들어 약관 텍스트일 수 있습니다. 메시지는 명시적 동의 옵션을 사용할 경우에 필요합니다.

vCenter Single Sign-On을 다른 서비스 제공자의 ID 제공자로 사용

vSphere Web Client는 신뢰할 수 있는 SAML 2.0 SP(서비스 제공자)로 vCenter Single Sign-On에 자동으로 등록됩니다. vCenter Single Sign-On이 SAML IDP(ID 제공자) 역할을 하는 ID 페더레이션에 신뢰할 수 있는 다른 서비스 제공자를 추가할 수 있습니다. 서비스 제공자는 SAML 2.0 프로토콜 규정을 준수해야 합니다. 페더레이션이 설정되면 서비스 제공자는 vCenter Single Sign-On에서 인증할 수 있는 사용자에게 액세스 권한을 부여합니다.

참고 vCenter Single Sign-On은 다른 SP의 IDP가 될 수 있습니다.vCenter Single Sign-On은 다른 IDP를 사용하는 SP일 수 없습니다.

등록된 SAML 서비스 제공자는 라이브 세션을 이미 가진 사용자, 즉 ID 제공자에 로그인되어 있는 사용자에게 액세스 권한을 부여할 수 있습니다. 예를 들어 vRealize Automation 7.0 이상에서는 vCenter Single Sign-On을 ID 제공자로 지원합니다. vCenter Single Sign-On 및 vRealize Automation에서 페더레이션을 설정할 수 있습니다. 이렇게 하면 vCenter Single Sign-On에서는 사용자가 vRealize Automation에 로그인할 때 인증을 수행할 수 있습니다.

ID 페더레이션에 SAML 서비스 제공자를 가입하려면 SP와 IDP 사이에 메타데이터를 교환하여 둘 사이에 신뢰 관계를 설정해야 합니다.

vCenter Single Sign-On 및 vCenter Single Sign-On을 사용하는 서비스 둘 모두에서 통합 작업을 수행해야 합니다.

- 1 IDP 메타데이터를 파일로 내보낸 다음 SP로 가져옵니다.
- 2 SP 메타데이터를 내보내고 IDP로 가져옵니다.

vCenter Single Sign-On에 대한 vSphere Web Client 인터페이스를 사용하여 IDP 메타데이터를 내보내고 SP에서 메타데이터를 가져올 수 있습니다. vRealize Automation을 SP로 사용하는 경우, SP 메타데이터 내보내기 및 IDP 메타데이터 가져오기에 대한 자세한 내용을 보려면 vRealize Automation 설명서를 참조하십시오.

참고 서비스가 SAML 2.0 표준을 완전하게 지원하지 않으면 통합이 이루어지지 않습니다.

SAML 서비스 제공자 추가

SAML 서비스 제공자를 vCenter Single Sign-On에 추가하고, 해당 서비스에 vCenter Single Sign-On을 ID 제공자로 추가합니다. 이렇게 하면 나중에 사용자가 서비스 제공자에 로그인하면 서비스 제공자가 vCenter Single Sign-On을 사용하여 해당 사용자를 인증합니다.

VMware vRealize Automation 7.0 이상에 포함되어 있는 Single Sign-On 솔루션을 vCenter Single Sign-On ID 제공자와 통합하려는 경우 또는 다른 외부 SAML 서비스 제공자를 사용하는 경우에는 이 프로세스를 사용하십시오.

이 프로세스에는 메타데이터를 SAML 서비스 제공자에서 vCenter Single Sign-On으로 가져오고 vCenter Single Sign-On 메타데이터를 SAML 서비스 제공자로 가져와서 두 제공자가 모든 데이터를 공유하도록 하는 작업이 포함됩니다.

사전 요구 사항

대상 서비스에서 SAML 2.0 표준을 완벽하게 지원해야 합니다.

메타데이터가 SAML 2.0 메타데이터 스키마를 정확하게 준수하지 않을 경우 스키마를 가져오기 전에 편집해야 할 수 있습니다. 예를 들어 ADFS(Active Directory Federation Service) SAML 서비스 제공자를 사용하는 경우에 메타데이터를 가져오려면 먼저 편집해야 합니다. 다음의 비표준 요소를 제거합니다.

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

현재 vSphere Web Client에서 SAML IDP 메타데이터를 가져올 수 없습니다.

절차

- 1 서비스 제공자의 메타데이터를 파일로 내보냅니다.
- 2 서비스 제공자의 메타데이터를 vCenter Single Sign-On에 가져옵니다.
 - a administrator@vsphere.local 또는 vCenter Single Sign-On 관리자 권한을 가진 다른 사용자로 vSphere Web Client에 로그인합니다.
vCenter Single Sign-On 관리자 권한을 가진 사용자는 vsphere.local 도메인에서 Administrators 그룹에 있습니다.
 - b **Single Sign-On > 구성**으로 이동합니다.
 - c **SAML 서비스 제공자** 탭을 선택합니다.
 - d **SAML 서비스 제공자의 메타데이터** 필드에서 **가져오기**를 클릭하고 XML 문자열을 대화상자에 붙여 넣거나, **파일에서 가져오기**를 클릭하여 파일을 가져온 다음 **가져오기**를 클릭합니다.
- 3 vCenter Single Sign-On 메타데이터를 내보냅니다.
 - a **SAML 서비스 제공자의 메타데이터** 필드에서 **다운로드**를 클릭합니다.
 - b 파일 위치를 지정합니다.
- 4 SAML 서비스 제공자(예: VMware vRealize Automation 7.0 이상)로 이동한 후 SAML 서비스 제공자의 지침에 따라 vCenter Single Sign-On 메타데이터를 해당 서비스 제공자에 추가합니다.
메타데이터 가져오기에 대한 자세한 내용은 vRealize Automation 설명서를 참조하십시오.

STS(Security Token Service)

vCenter Single Sign-On STS(Security Token Service)는 보안 토큰을 발급, 검증 및 갱신하는 웹 서비스입니다.

사용자는 자신의 기본 자격 증명을 STS 인터페이스에 제공하여 SAML 토큰을 획득합니다. 기본 자격 증명 은 사용자 유형에 따라 다릅니다.

사용자

vCenter Single Sign-On ID 소스에서 사용할 수 있는 사용자 이름 및 암호

애플리케이션 사용자

유효한 인증서

STS는 기본 자격 증명에 기반하여 사용자를 인증하고 사용자 특성이 포함된 SAML 토큰을 구성합니다. STS는 STS 서명 인증서로 SAML 토큰을 서명한 다음 토큰을 사용자에게 할당합니다. 기본적으로 STS 서명 인증서는 VMCA를 통해 생성됩니다. vSphere Web Client에서 기본 STS 서명 인증서를 교체할 수 있습니다. 회사의 보안 정책에 따라 모든 인증서를 교체해야 하는 경우 이외에는 STS 서명 인증서를 교체하지 마십시오.

사용자가 SAML 토큰을 가진 후 SAML 토큰은 가능한 다양한 프록시를 통해 사용자의 HTTP 요청의 일부로 전송됩니다. 의도한 수신자(서비스 제공자)만 SAML 토큰에서 해당 정보를 사용할 수 있습니다.

장치에 새 STS 서명 인증서 생성

기본 vCenter Single Sign-On STS(Security Token Service) 서명 인증서를 교체하려면 새 인증서를 생성한 후 Java 키 저장소에 추가해야 합니다. 이 절차에서는 내장된 배포 장치 또는 외부 Platform Services Controller 장치에 대해 수행하는 단계를 설명합니다.

참고 이 인증서는 10년간 유효하며 외부를 대상으로 하는 인증서가 아닙니다. 회사의 보안 정책에서 요구하는 경우 이외에는 이 인증서를 교체하지 마십시오.

Platform Services Controller Windows 설치를 실행하는 경우에는 [vCenter Windows 설치에서 새 STS 서명 인증서 생성](#)을 참조하십시오.

절차

- 1 새 인증서를 저장할 최상위 디렉토리를 생성하고 디렉토리의 위치를 확인합니다.

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

- 2 certool.cfg 파일을 새 디렉토리에 복사합니다.

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

- 3 certool.cfg 파일 사본을 열고, 로컬 Platform Services Controller IP 주소와 호스트 이름을 사용하여도록 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
```

4 키를 생성합니다.

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

5 인증서를 생성합니다.

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

6 인증서를 PK12 형식으로 변환합니다.

```
openssl pkcs12 -export -in /root/newsts/newsts.cer -inkey /root/newsts/sts.key
-certfile /etc/vmware-sso/keys/ssoserverRoot.crt -name "newstssigning" -passout
pass:changeme -out newsts.p12
```

7 인증서를 JKS(Java 키 저장소)에 추가합니다.

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

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

8 메시지가 표시되면 **예**를 입력하여 키 저장소에 인증서를 수락합니다.

다음에 수행할 작업

이제 새 인증서를 가져올 수 있습니다. [보안 토큰 서비스 인증서 새로 고침](#)을 참조하십시오.

vCenter Windows 설치에서 새 STS 서명 인증서 생성

기본 STS 서명 인증서를 교체하려면 먼저 새 인증서를 생성하고 Java 키 저장소에 추가해야 합니다. 이 절차는 Windows 설치에서 수행할 단계를 설명합니다.

참고 이 인증서는 10년간 유효하며 외부 대상에 대한 인증서가 아닙니다. 회사의 보안 정책에서 요구하는 경우 이외에는 이 인증서를 교체하지 마십시오.

가상 장치를 사용 중인 경우 [장치에 새 STS 서명 인증서 생성](#) 항목을 참조하십시오.

절차

1 새 인증서를 유지할 새 디렉토리를 생성합니다.

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

- 2 certool.cfg 파일의 사본을 만들어서 새 디렉토리에 둡니다.

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

- 3 certool.cfg 파일 사본을 열고, 로컬 Platform Services Controller IP 주소와 호스트 이름을 사용하여도록 편집합니다.

국가는 필수 사항이며 2자여야 합니다. 다음 샘플은 이러한 내용을 보여줍니다.

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

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

- 4 키를 생성합니다.

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

- 5 인증서를 생성합니다.

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

- 6 인증서를 PK12 형식으로 변환합니다.

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

- 7 인증서를 JKS(Java 키 저장소)에 추가합니다.

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

다음에 수행할 작업

이제 새 인증서를 가져올 수 있습니다. [보안 토큰 서비스 인증서 새로 고침](#)을 참조하십시오.

보안 토큰 서비스 인증서 새로 고침

vCenter Single Sign-On 서버에는 STS(Security Token Service)가 포함됩니다. Security Token Service는 보안 토큰을 발급, 검증 및 갱신하는 웹 서비스입니다. 인증서가 만료되거나 변경된 경우 vSphere Web Client에서 기존 Security Token Service 인증서를 수동으로 새로 고칠 수 있습니다.

SAML 토큰을 획득하기 위해 사용자는 기본 자격 증명을 STS(Secure Token Server)에 제공합니다. 기본 자격 증명은 사용자 유형에 따라 다릅니다.

솔루션 사용자

유효한 인증서

기타 사용자

vCenter Single Sign-On ID 소스에서 사용할 수 있는 사용자 이름 및 암호

STS는 기본 자격 증명을 사용하여 사용자를 인증하고 사용자 특성이 포함된 SAML 토큰을 구성합니다. STS 서비스는 STS 서명 인증서로 SAML 토큰을 서명한 다음 토큰을 사용자에게 할당합니다. 기본적으로 STS 서명 인증서는 VMCA를 통해 생성됩니다.

사용자가 SAML 토큰을 가진 후 SAML 토큰은 가능한 다양한 프록시를 통해 사용자의 HTTP 요청의 일부로 전송됩니다. 의도한 수신자(서비스 제공자)만 SAML 토큰에서 해당 정보를 사용할 수 있습니다.

회사 정책에서 요구하거나 만료된 인증서를 업데이트하려는 경우 기존 STS 서명 인증서 vSphere Web Client를 교체할 수 있습니다.

경고 파일 시스템의 파일을 교체하지 마십시오. 교체할 경우 디버깅하기 어려운 예기치 않은 오류가 발생합니다.

참고 인증서를 교체한 다음 노드를 다시 시작하여 vSphere Web Client 서비스와 STS 서비스를 모두 다시 시작해야 합니다.

사전 요구 사항

Java 키 저장소에 추가한 인증서를 Platform Services Controller에서 로컬 워크스테이션으로 복사합니다.

Platform Services Controller 장치

`certificate_location/keys/root-trust.jks` For example: `/keys/root-trust.jks`

예:

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

Windows 설치

`certificate_location\root-trust.jks`

예:

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

절차

- 1 administrator@vsphere.local 또는 vCenter Single Sign-On 관리자 권한을 가진 다른 사용자로 vSphere Web Client에 로그인합니다.
vCenter Single Sign-On 관리자 권한을 가진 사용자는 vsphere.local 도메인에서 Administrators 그룹에 있습니다.
- 2 **인증서** 탭을 선택한 다음 **STS 서명** 하위 탭을 선택하고 **STS 서명 인증서 추가** 아이콘을 클릭합니다.
- 3 인증서를 추가합니다.
 - a **찾아보기**를 클릭하여 새 인증서가 포함된 키 저장소 JKS 파일을 찾고 **열기**를 클릭합니다.
 - b 메시지가 표시되면 암호를 입력합니다.
 - c STS 별칭 체인의 맨 위를 클릭하고 **확인**을 클릭합니다.
 - d 메시지가 표시되면 암호를 다시 입력합니다.
- 4 **확인**을 클릭합니다.
- 5 Platform Services Controller 노드를 다시 시작하여 STS 서비스와 vSphere Web Client를 모두 다시 시작합니다.

다시 시작하기 전까지는 인증이 제대로 작동하지 않으니 반드시 다시 시작해야 합니다.

LDAPS SSL 인증서의 만료 날짜 확인

Active Directory LDAP 서버 및 OpenLDAP 서버 ID 소스를 선택하고 LDAPS를 사용하기로 결정한 경우 LDAP 트래픽에 대해 SSL 인증서를 업로드할 수 있습니다. SSL 인증서는 미리 지정한 기간이 지나면 만료됩니다. 인증서가 만료되는 시기를 알아 두면 만료 날짜 이전에 인증서를 교체하거나 갱신할 수 있습니다.

Active Directory LDAP 서버 및 OpenLDAP 서버를 사용하고 서버에 대해 **ldaps://** URL을 지정하는 경우에만 인증서 만료 정보가 표시됩니다. [ID 소스 신뢰 저장소] 탭은 다른 유형의 ID 소스 또는 **ldap://** 트래픽에 대해 비어 있습니다.

절차

- 1 administrator@vsphere.local 또는 vCenter Single Sign-On 관리자 권한을 가진 다른 사용자로 vSphere Web Client에 로그인합니다.
vCenter Single Sign-On 관리자 권한을 가진 사용자는 vsphere.local 도메인에서 Administrators 그룹에 있습니다.
- 2 **관리 > Single Sign-On > 구성**을 찾습니다.
- 3 **인증서** 탭을 클릭한 다음 **ID 소스 신뢰 저장소** 하위 탭을 클릭합니다.

4 인증서를 찾아 **유효 기간 종료** 텍스트 상자의 만료 날짜를 확인합니다.

탭 위쪽에 인증서의 만료가 임박했음을 나타내는 경고가 표시될 수도 있습니다.

vCenter Single Sign-On 정책 관리

vCenter Single Sign-On 정책은 환경에 보안 규칙을 적용합니다. 기본 vCenter Single Sign-On 암호, 잠금 정책 및 토큰 정책을 보고 편집할 수 있습니다.

vCenter Single Sign-On 암호 정책 편집

vCenter Single Sign-On 암호 정책은 vCenter Single Sign-On 사용자 암호의 형식 및 만료에 대한 규칙 및 제한 모음입니다. 암호 정책은 vCenter Single Sign-On 도메인(vsphere.local)의 사용자에게만 적용됩니다.

기본적으로 vCenter Single Sign-On 암호는 90일 후에 만료됩니다. vSphere Web Client는 암호가 만료 되려고 할 때 미리 알려 줍니다.

절차

- 1 administrator@vsphere.local 또는 vCenter Single Sign-On 관리자 권한을 가진 다른 사용자로 vSphere Web Client에 로그인합니다.

vCenter Single Sign-On 관리자 권한을 가진 사용자는 vsphere.local 도메인에서 Administrators 그룹에 있습니다.

- 2 **관리 > Single Sign-On > 구성**으로 이동합니다.
- 3 **정책** 탭을 클릭하고 **암호 정책**을 선택합니다.
- 4 **편집**을 클릭합니다.
- 5 암호 정책 매개 변수를 편집합니다.

옵션	설명
설명	암호 정책 설명입니다.
최대 수명	사용자가 변경해야 될 때까지 암호가 존재할 수 있는 최대 일수입니다.
재사용 제한	사용자의 이전 암호 수로, 선택할 수 없습니다. 예를 들어 사용자가 최근 6개의 암호를 다시 사용할 수 없는 경우 6을 입력합니다.
최대 길이	암호에 허용되는 최대 문자 수입니다.
최소 길이	암호에 요구되는 최소 문자 수입니다. 최소 길이는 영문자, 숫자 및 특수 문자 결합의 최소 요구 사항을 충족해야 합니다.

옵션	설명
문자 요구 사항	<p>암호에 요구되는 다양한 문자 유형의 최소 수입니다. 각 문자 유형의 수를 다음과 같이 지정할 수 있습니다.</p> <ul style="list-style-type: none"> ■ 특수 문자: & # % ■ 영문자: A b c D ■ 대문자: A B C ■ 소문자: a b c ■ 숫자: 1 2 3 <p>영문자의 최소 수는 대소문자 결합 요구 사항을 충족해야 합니다.</p> <p>vSphere 6.0 이상에서는 암호에서 ASCII가 아닌 문자를 지원합니다. vCenter Single Sign-On 이전 버전에서는 지원되는 문자에 대한 제한이 있습니다.</p>
인접한 동일 문자 수	<p>암호에 허용되는 인접한 동일 문자의 최대 수입니다. 숫자가 0보다 커야 합니다. 예를 들면 1을 입력하면 p@\$word와 같은 암호가 허용되지 않습니다.</p>

6 확인을 클릭합니다.

vCenter Single Sign-On 잠금 정책 편집

vCenter Single Sign-On 잠금 정책은 사용자가 잘못된 자격 증명으로 로그인을 시도할 때 vCenter Single Sign-On 계정이 잠기는 조건을 지정합니다. 잠금 정책은 편집 가능합니다.

사용자가 잘못된 암호로 vsphere.local에 로그인하려고 여러 번 시도하면 해당 사용자가 잠깁니다. 잠금 정책을 사용하면 실패한 최대 로그인 시도 횟수와 실패 사이의 허용되는 경과 시간을 지정할 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 administrator@vsphere.local 또는 vCenter Single Sign-On 관리자 권한을 가진 다른 사용자로 vSphere Web Client에 로그인합니다.
vCenter Single Sign-On 관리자 권한을 가진 사용자는 vsphere.local 도메인에서 Administrators 그룹에 있습니다.
- 2 **관리 > Single Sign-On > 구성**을 찾습니다.
- 3 **정책** 탭을 클릭하고 **잠금 정책**을 선택합니다.
- 4 **편집**을 클릭합니다.
- 5 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.

옵션	설명
실패 시간 간격	잠금을 트리거하기 위해 실패한 로그인 시도가 발생해야 하는 기간입니다.
잠금 해제 시간	계정이 잠금 상태로 유지되는 기간입니다. 0을 입력하면 관리자가 해당 계정을 명시적으로 잠금 해제해야 합니다.

6 확인을 클릭합니다.

vCenter Single Sign-On 토큰 정책 편집

vCenter Single Sign-On 토큰 정책은 클럭 허용 오차, 갱신 횟수 및 기타 토큰 속성을 지정합니다. 토큰 사양이 회사의 보안 표준에 맞도록 vCenter Single Sign-On 토큰 정책을 편집할 수 있습니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **관리 > Single Sign-On**을 선택하고 **구성**을 선택합니다.
- 3 **정책** 탭을 클릭하고 **토큰 정책**을 선택합니다.

vSphere Web Client에 현재 구성 설정이 표시됩니다. 기본 설정을 수정하지 않은 경우 vCenter Single Sign-On은 기본 설정을 사용합니다.

- 4 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.
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 시스템 사용자 대신 위임된 토큰을 가져오고 해당 토큰을 사용하여 작업을 수행합니다. 이 값은 토큰이 잘못된 것으로 표시되기 전까지의 키 소유자 토큰 수명을 결정합니다.

5 확인을 클릭합니다.

vCenter Single Sign-On 사용자 및 그룹 관리

vCenter Single Sign-On 관리자는 vSphere Web Client에서 vsphere.local 도메인의 사용자 및 그룹을 관리할 수 있습니다.

vCenter Single Sign-On 관리자는 다음 작업을 수행할 수 있습니다.

■ vCenter Single Sign-On 사용자 추가

vSphere Web Client의 **사용자** 탭에 나열된 사용자는 vsphere.local 도메인에 속한 vCenter Single Sign-On 내부 사용자입니다.

■ vCenter Single Sign-On 사용자 사용 안 함/사용

vCenter Single Sign-On 사용자 계정을 사용하지 않도록 설정한 경우 사용자는 관리자가 해당 계정을 사용하도록 설정하기 전까지 vCenter Single Sign-On 서버에 로그인할 수 없습니다. vSphere Web Client 인터페이스에서 사용자를 사용하거나 사용하지 않도록 설정할 수 있습니다.

■ vCenter Single Sign-On 사용자 삭제

vsphere.local 도메인에 있는 사용자를 vCenter Single Sign-On에서 삭제할 수 있습니다. 로컬 운영 체제 사용자나 다른 도메인의 사용자는 vSphere Web Client에서 삭제할 수 없습니다.

■ vCenter Single Sign-On 사용자 편집

vSphere Web Client에서 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.

■ vCenter Single Sign-On 그룹 추가

vCenter Single Sign-On에서 **그룹** 탭에 나열되는 그룹은 vCenter Single Sign-On 내부 그룹입니다. 그룹을 사용하여 그룹 멤버(주체)의 모음에 대한 컨테이너를 생성할 수 있습니다.

■ 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 Web Client에서 새 멤버를 추가할 수 있습니다.

■ vCenter Single Sign-On 그룹에서 멤버 제거

vSphere Web Client에서 vCenter Single Sign-On 그룹의 멤버를 제거할 수 있습니다. 로컬 그룹에서 멤버(사용자 또는 그룹)를 제거하는 경우 해당 멤버는 시스템에서 삭제되지 않습니다.

■ vCenter Single Sign-On 솔루션 사용자 삭제

vCenter Single Sign-On은 솔루션 사용자를 표시합니다. 솔루션 사용자는 서비스 모음입니다. 여러 vCenter Server 솔루션 사용자가 미리 정의되고 설치의 일부로 vCenter Single Sign-On에 인증됩니다. 제거가 완전하게 완료되지 않은 경우와 같은 문제 해결 상황에서는 vSphere Web Client에서 개별 솔루션 사용자를 삭제할 수 있습니다.

■ vCenter Single Sign-On 암호 변경

로컬 도메인 vsphere.local에 속해 있는 사용자는 기본적으로 웹 인터페이스에서 자신의 vCenter Single Sign-On 암호를 변경할 수 있습니다. 다른 도메인의 사용자는 해당 도메인의 규칙에 따라 자신의 암호를 변경할 수 있습니다.

vCenter Single Sign-On 사용자 추가

vSphere Web Client의 **사용자** 탭에 나열된 사용자는 vsphere.local 도메인에 속한 vCenter Single Sign-On 내부 사용자입니다.

vSphere Web Client의 vCenter Single Sign-On 관리 인터페이스에서 다른 도메인을 선택하고 해당 도메인의 사용자에 대한 정보를 볼 수는 있지만 사용자를 다른 도메인에 추가할 수는 없습니다.

절차

- 1 administrator@vsphere.local 또는 vCenter Single Sign-On 관리자 권한을 가진 다른 사용자로 vSphere Web Client에 로그인합니다.

vCenter Single Sign-On 관리자 권한을 가진 사용자는 vsphere.local 도메인에서 Administrators 그룹에 있습니다.
- 2 **홈**을 클릭하고 **관리 > Single Sign-On > 사용자 및 그룹**으로 이동합니다.
- 3 현재 선택된 도메인이 vsphere.local이 아닌 경우 드롭다운 메뉴에서 vsphere.local을 선택합니다.

다른 도메인에는 사용자를 추가할 수 없습니다.
- 4 **사용자** 탭에서 **새 사용자** 아이콘을 클릭합니다.
- 5 새 사용자의 사용자 이름과 암호를 입력합니다.

사용자를 생성한 후에는 사용자 이름을 변경할 수 없습니다.

암호는 시스템의 암호 정책 요구 사항을 충족해야 합니다.
- 6 (선택 사항) 새 사용자의 성과 이름을 입력합니다.
- 7 (선택 사항) 사용자의 이메일 주소 및 설명을 입력합니다.
- 8 **확인**을 클릭합니다.

결과

사용자를 추가하면 처음에는 해당 사용자에게 관리 작업을 수행할 수 있는 권한이 없습니다.

다음에 수행할 작업

사용자를 vsphere.local domain의 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 추가**를 참조하십시오.

vCenter Single Sign-On 사용자 사용 안 함/사용

vCenter Single Sign-On 사용자 계정을 사용하지 않도록 설정한 경우 사용자는 관리자가 해당 계정을 사용하도록 설정하기 전까지 vCenter Single Sign-On 서버에 로그인할 수 없습니다. vSphere Web Client 인터페이스에서 사용자를 사용하거나 사용하지 않도록 설정할 수 있습니다.

사용하지 않도록 설정된 사용자 계정은 vCenter Single Sign-On 시스템에서 사용할 수 있는 상태로 유지되지만 사용자는 로그인하거나 서버에서 작업을 수행할 수 없습니다. 관리자 권한이 있는 사용자는 vCenter 사용자 및 그룹 페이지에서 사용자를 사용하거나 사용하지 않도록 설정할 수 있습니다.

사전 요구 사항

vCenter Single Sign-On 사용자를 사용하거나 사용하지 않도록 설정하려면 vCenter Single Sign-On 관리자 그룹의 멤버여야 합니다.

절차

- 1 administrator@vsphere.local 또는 vCenter Single Sign-On 관리자 권한을 가진 다른 사용자로 vSphere Web Client에 로그인합니다.
vCenter Single Sign-On 관리자 권한을 가진 사용자는 vsphere.local 도메인에서 Administrators 그룹에 있습니다.
- 2 홈을 클릭하고 **관리 > Single Sign-On > 사용자 및 그룹**으로 이동합니다.
- 3 사용자를 선택하고 **사용 안 함** 아이콘을 클릭한 다음 메시지가 표시되면 **예**를 클릭합니다.
- 4 사용자를 다시 사용하도록 설정하려면 사용자를 마우스 오른쪽 버튼으로 클릭하고 **사용**을 선택한 다음 메시지가 표시되면 **예**를 클릭합니다.

vCenter Single Sign-On 사용자 삭제

vsphere.local 도메인에 있는 사용자를 vCenter Single Sign-On에서 삭제할 수 있습니다. 로컬 운영 체제 사용자나 다른 도메인의 사용자는 vSphere Web Client에서 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 administrator@vsphere.local 또는 vCenter Single Sign-On 관리자 권한을 가진 다른 사용자로 vSphere Web Client에 로그인합니다.
vCenter Single Sign-On 관리자 권한을 가진 사용자는 vsphere.local 도메인에서 Administrators 그룹에 있습니다.
- 2 홈을 클릭하고 **관리 > Single Sign-On > 사용자 및 그룹**으로 이동합니다.
- 3 **사용자** 탭을 선택하고 vsphere.local 도메인을 선택합니다.

- 4 사용자 목록에서 삭제할 사용자를 선택하고 **삭제** 아이콘을 클릭합니다.

주의해서 진행하십시오. 이 작업은 실행 취소할 수 없습니다.

vCenter Single Sign-On 사용자 편집

vSphere Web Client에서 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.

vSphere Web Client에서 vCenter Single Sign-On 암호 정책을 검토할 수 있습니다.

administrator@vsphere.local로 로그인하고 **구성 > 정책 > 암호 정책**을 선택합니다.

절차

- 1 administrator@vsphere.local 또는 vCenter Single Sign-On 관리자 권한을 가진 다른 사용자로 vSphere Web Client에 로그인합니다.

vCenter Single Sign-On 관리자 권한을 가진 사용자는 vsphere.local 도메인에서 Administrators 그룹에 있습니다.
- 2 **홈**을 클릭하고 **관리 > Single Sign-On > 사용자 및 그룹**으로 이동합니다.
- 3 **사용자** 탭을 클릭합니다.
- 4 사용자를 마우스 오른쪽 버튼으로 클릭하고 **사용자 편집**을 선택합니다.
- 5 필요에 맞게 사용자를 변경합니다.

사용자의 사용자 이름은 변경할 수 없습니다.

암호는 시스템의 암호 정책 요구 사항을 충족해야 합니다.
- 6 **확인**을 클릭합니다.

vCenter Single Sign-On 그룹 추가

vCenter Single Sign-On에서 **그룹** 탭에 나열되는 그룹은 vCenter Single Sign-On 내부 그룹입니다. 그룹을 사용하여 그룹 멤버(주체)의 모음에 대한 컨테이너를 생성할 수 있습니다.

vSphere Web Client 관리 인터페이스에서 vCenter Single Sign-On 그룹을 추가하면 해당 그룹이 vsphere.local 도메인에 추가됩니다.

절차

- 1 administrator@vsphere.local 또는 vCenter Single Sign-On 관리자 권한을 가진 다른 사용자로 vSphere Web Client에 로그인합니다.

vCenter Single Sign-On 관리자 권한을 가진 사용자는 vsphere.local 도메인에서 Administrators 그룹에 있습니다.

- 2 **홈**을 클릭하고 **관리 > Single Sign-On > 사용자 및 그룹**으로 이동합니다.
- 3 **그룹** 탭을 선택하고 **새 그룹** 아이콘을 클릭합니다.
- 4 그룹의 이름과 설명을 입력합니다.

그룹을 생성한 후에는 그룹 이름을 변경할 수 없습니다.

- 5 **확인**을 클릭합니다.

다음에 수행할 작업

- 그룹에 멤버를 추가합니다.

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 Web Client에서 새 멤버를 추가할 수 있습니다.

Microsoft Active Directory 또는 OpenLDAP 그룹의 멤버를 vCenter Single Sign-On 그룹에 추가할 수 있습니다. 외부 ID 소스의 그룹은 vCenter Single Sign-On 그룹에 추가할 수 없습니다.

vSphere Web Client의 **그룹** 탭에 나열된 그룹은 vsphere.local 도메인에 속합니다. [vsphere.local 도메인의 그룹](#)을 참조하십시오.

절차

- 1 administrator@vsphere.local 또는 vCenter Single Sign-On 관리자 권한을 가진 다른 사용자로 vSphere Web Client에 로그인합니다.

vCenter Single Sign-On 관리자 권한을 가진 사용자는 vsphere.local 도메인에서 Administrators 그룹에 있습니다.
- 2 **홈**을 클릭하고 **관리 > Single Sign-On > 사용자 및 그룹**으로 이동합니다.
- 3 **그룹** 탭을 클릭하고 관리자 등의 그룹을 클릭합니다.
- 4 그룹 멤버 영역에서 **멤버 추가** 아이콘을 클릭합니다.
- 5 그룹에 추가할 멤버가 포함된 ID 소스를 선택합니다.
- 6 (선택 사항) 검색어를 입력하고 **검색**을 클릭합니다.
- 7 멤버를 선택하고 **추가**를 클릭합니다.

여러 멤버를 동시에 추가할 수 있습니다.
- 8 **확인**을 클릭합니다.

vCenter Single Sign-On 그룹에서 멤버 제거

vSphere Web Client에서 vCenter Single Sign-On 그룹의 멤버를 제거할 수 있습니다. 로컬 그룹에서 멤버(사용자 또는 그룹)를 제거하는 경우 해당 멤버는 시스템에서 삭제되지 않습니다.

절차

- 1 administrator@vsphere.local 또는 vCenter Single Sign-On 관리자 권한을 가진 다른 사용자로 vSphere Web Client에 로그인합니다.

vCenter Single Sign-On 관리자 권한을 가진 사용자는 vsphere.local 도메인에서 Administrators 그룹에 있습니다.
- 2 홈을 클릭하고 **관리 > Single Sign-On > 사용자 및 그룹**으로 이동합니다.
- 3 **그룹** 탭을 선택하고 그룹을 클릭합니다.
- 4 그룹 멤버 목록에서 제거할 사용자 또는 그룹을 선택하고 **멤버 제거** 아이콘을 클릭합니다.
- 5 **확인**을 클릭합니다.

결과

사용자가 그룹에서는 제거되지만 시스템에는 남아 있습니다.

vCenter Single Sign-On 솔루션 사용자 삭제

vCenter Single Sign-On은 솔루션 사용자를 표시합니다. 솔루션 사용자는 서비스 모음입니다. 여러 vCenter Server 솔루션 사용자가 미리 정의되고 설치의 일부로 vCenter Single Sign-On에 인증됩니다. 제거가 완전하게 완료되지 않은 경우와 같은 문제 해결 상황에서는 vSphere Web Client에서 개별 솔루션 사용자를 삭제할 수 있습니다.

환경에서 vCenter Server 솔루션 사용자 또는 타사 솔루션 사용자와 연결된 서비스 집합을 제거할 때 해당 솔루션 사용자가 vSphere Web Client 표시에서 제거됩니다. 애플리케이션을 강제로 제거하거나 솔루션 사용자가 아직 시스템에 있는 동안 시스템이 복구할 수 없는 상태가 되는 경우 vSphere Web Client에서 솔루션 사용자를 명시적으로 제거할 수 있습니다.

중요 솔루션 사용자를 삭제하는 경우 해당 서비스가 더 이상 vCenter Single Sign-On에 인증할 수 없습니다.

절차

- 1 administrator@vsphere.local 또는 vCenter Single Sign-On 관리자 권한을 가진 다른 사용자로 vSphere Web Client에 로그인합니다.

vCenter Single Sign-On 관리자 권한을 가진 사용자는 vsphere.local 도메인에서 Administrators 그룹에 있습니다.
- 2 홈을 클릭하고 **관리 > Single Sign-On > 사용자 및 그룹**으로 이동합니다.
- 3 **솔루션 사용자** 탭을 클릭하고 솔루션 사용자 이름을 클릭합니다.
- 4 **솔루션 사용자 삭제** 아이콘을 클릭합니다.
- 5 **예**를 클릭합니다.

결과

솔루션 사용자와 연결된 서비스가 더 이상 vCenter Server에 액세스할 수 없으며 vCenter Server 서비스로 작동할 수 없습니다.

vCenter Single Sign-On 암호 변경

로컬 도메인 vsphere.local에 속해 있는 사용자는 기본적으로 웹 인터페이스에서 자신의 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 사용자 암호는 90일 후 만료되지만 administrator@vsphere.local에 대한 암호와 같은 관리자 암호는 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 웹 브라우저에서 다음 URL을 지정하여 Platform Services Controller에 연결합니다.

https://psc_hostname_or_IP/psc

내장된 배포에서 Platform Services Controller 호스트 이름 또는 IP 주소는 vCenter Server 호스트 이름 또는 IP 주소와 동일합니다.

- 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@mydomain으로 로그인합니다.

- 3 위쪽 탐색 창에서 도움말 메뉴 왼쪽에 있는 사용자의 사용자 이름을 클릭하여 풀다운 메뉴를 표시합니다.

또는 **Single Sign-On > 사용자 및 그룹**을 선택하고 마우스 오른쪽 버튼 메뉴에서 **사용자 편집**을 선택할 수 있습니다.

- 4 **암호 변경**을 선택하고 현재 암호를 입력합니다.
- 5 새 암호를 입력하고 확인을 위해 한 번 더 입력합니다.
암호는 암호 정책을 준수해야 합니다.
- 6 **확인**을 클릭합니다.

vCenter Single Sign-On 보안 모범 사례

vCenter Single Sign-On 보안 모범 사례를 따라 vSphere 환경을 보호합니다.

vSphere 6.0 인증 및 인증서 인프라는 vSphere 환경의 보안을 향상합니다. 인프라가 손상되지 않도록 하려면 vCenter Single Sign-On 모범 사례를 따릅니다.

암호 만료 확인

기본 vCenter Single Sign-On 암호 정책의 암호 지속 시간은 90일입니다. 90일 후에는 암호가 만료되고 로그 기능이 손상됩니다. 만료를 확인하고 적시에 암호를 새로 고칩니다.

NTP 구성

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.

vCenter Single Sign-On 문제 해결

vCenter Single Sign-On 구성은 복잡한 과정일 수 있습니다.

다음 항목에서는 vCenter Single Sign-On의 문제 해결을 위한 시작 지점을 제공합니다. 이 설명서 센터와 VMware 기술 자료 시스템에서 추가 포인터를 검색하십시오.

Lookup Service 오류의 원인 확인

vCenter Single Sign-On 설치에 vCenter Server 또는 vSphere Web Client와 관련된 오류가 표시됩니다.

문제

vCenter Server 및 Web Client 설치 관리자에 Lookup Service에 연결할 수 없습니다.

VM_ssoreg.log를 참조하십시오. 라는 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. 등록 공급자를 초기화하는 중...이라고 표시된 마지막 메시지를 찾습니다.

메시지	원인 및 해결 방법
java.net.ConnectException: 연결 시간 초과: 연결	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 확인하고, vCenter Single Sign-On이 설치되어 있는 시스템에 사용 가능한 CPU, I/O 및 RAM 용량이 충분한지 확인합니다.
java.net.ConnectException: 연결 거부: 연결	IP 주소 또는 FQDN이 잘못되었고 vCenter Single Sign-On 서비스가 아직 시작되지 않았거나, 시작된 지 1분이 지나지 않은 경우입니다. vCenter Single Sign-On 서비스(Windows) 및 vmware-ssd 데몬(Linux)의 상태를 확인하여 vCenter Single Sign-On이 작동 중인지 확인합니다. 서비스를 다시 시작합니다. 이렇게 해서 문제를 해결할 수 없으면 vSphere 문제 해결 가이드의 복구 섹션을 참조하십시오.
예기치 않은 상태 코드: 404. 초기화하는 동안 SSO Server에서 오류가 발생함	vCenter Single Sign-On을 다시 시작합니다. 이렇게 해서 문제를 해결할 수 없으면 "vSphere 문제 해결 가이드"의 복구 섹션을 참조하십시오.
UI에 나와 있는 오류가 vCenter Single Sign-On에 연결할 수 없습니다.로 시작하는 경우입니다.	또한 SslHandshakeFailed라는 반환 코드도 표시됩니다. 이는 일반적으로 발생하지 않는 오류로, vCenter Single Sign-On 호스트에서 확인하도록 지정한 IP 주소나 FQDN이 vCenter Single Sign-On을 설치할 때 사용한 것과 다르다는 것을 나타냅니다. %TEMP%\VM_ssoreg.log에서 다음 메시지가 포함된 줄을 찾습니다. 인증서에 포함된 호스트 이름이 일치하지 않습니다. <구성된 FQDN 또는 IP> != <A>, 또는 <C>를 설치하십시오. 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 Web 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).

vCenter Server Appliance를 사용하는 경우에는 다른 문제가 발생할 수도 있습니다.

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 [2070433](#)을 참조하십시오. 기본적으로 통합 Windows 인증은 Active Directory 포리스트의 루트 도메인을 사용합니다.

vCenter Server Appliance를 사용하며 기본 ID 소스를 변경한 후에도 문제가 해결되지 않으면 다음과 같은 추가 문제 해결 단계를 수행합니다.

- 1 vCenter Server Appliance와 Active Directory 도메인 컨트롤러 간에 클럭을 동기화합니다.
- 2 각 도메인 컨트롤러의 PTR(포인터 레코드)가 Active Directory 도메인 DNS 서비스에 있으며 PTR 레코드 정보가 컨트롤러의 DNS 이름과 일치하는지 확인합니다. vCenter Server Appliance를 사용하는 경우 다음 명령을 실행하여 작업을 수행할 수 있습니다.
 - 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 Server Appliance를 Active Directory 도메인에서 제거한 후 도메인에 다시 가입합니다. "vCenter Server Appliance 구성" 설명서를 참조하십시오.
- 4 vCenter Server Appliance에 연결된 모든 브라우저 세션을 닫고 모든 서비스를 다시 시작합니다.

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

사용자 계정 잠김으로 인한 vCenter Server 로그인 실패

vSphere Web Client 로그인 페이지에서 vCenter Server에 로그인할 때 계정이 잠겨 있다는 오류가 발생합니다.

문제

몇 차례의 로그인 시도가 실패하면 vCenter Single Sign-On을 사용하여 vSphere Web Client에 로그인할 수 없습니다. 이 경우 계정이 잠겼다는 메시지가 표시됩니다.

원인

실패한 최대 로그인 시도 횟수를 초과한 것입니다.

해결책

- ◆ 시스템 도메인(vsphere.local)의 사용자로 로그인하는 경우 vCenter Single Sign-On 관리자에게 계정 잠금 해제를 요청하십시오. 아니면 암호 정책에서 잠금이 만료되도록 설정되어 있는 경우 계정의 잠금이 해제될 때까지 기다릴 수도 있습니다. vCenter Single Sign-On 관리자는 CLI 명령을 사용하여 계정의 잠금을 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 여러 개의 Platform Services Controller 인스턴스가 있으면 Platform Services Controller 인스턴스 중 하나를 사용할 수 없더라도 환경은 계속 작동합니다. Platform Services Controller이 다시 사용 가능한 상태가 되면 사용자 데이터 및 기타 정보는 일반적으로 60초 내에 복제됩니다. 하지만 특별한 상황에서는 복제에 시간이 많이 걸릴 수 있습니다.

문제

환경 내 여러 위치에 여러 개의 Platform Services Controller 인스턴스가 있을 때 Platform Services Controller 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 Platform Services Controller 인스턴스에 새 사용자를 추가한 경우 복제 완료 전까지는 새 사용자가 표시되지 않습니다.

원인

정상 작동 중에는 한 Platform Services Controller 인스턴스(노드)의 vmdir(VMware Directory Service) 인스턴스를 변경하면 이 변경 내용은 약 60초 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 라이선스 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.

vSphere 보안 인증서

3

vSphere 구성 요소는 SSL을 사용하여 서로 간에 그리고 ESXi와 보안 통신을 합니다. SSL 통신을 사용하면 데이터 기밀성과 무결성이 보장됩니다. 또한 데이터가 보호되며 전송 중 감지되지 않은 채로 수정될 수 없습니다.

인증서는 vCenter Single Sign-On에 대한 초기 인증을 위해 vSphere Web Client와 같은 vCenter Server 서비스에서도 사용됩니다. vCenter Single Sign-On은 구성 요소가 향후 인증에 사용하는 SAML 토큰으로 각 구성 요소를 프로비저닝합니다.

vSphere 6.0 이상에서 VMCA(VMware Certificate Authority)는 각 ESXi 호스트와 각 vCenter Server 서비스에 VMCA 서명이 있는 인증서를 기본적으로 할당합니다.

기존 인증서를 새 VMCA 서명 인증서로 교체하거나, VMCA를 하위 CA로 지정하거나, 모든 인증서를 사용자 지정 인증서로 교체할 수 있습니다. 다음과 같이 여러 가지 옵션이 있습니다.

표 3-1. 여러 가지 인증서 교체 방법

옵션	자세한 내용은
Platform Services Controller 웹 인터페이스(vSphere 6.0 업데이트 1 이상)를 사용합니다.	Platform Services Controller 웹 인터페이스를 사용하여 인증서 관리
명령줄에서 vSphere Certificate Manager 유틸리티를 사용합니다.	vSphere Certificate Manager 유틸리티를 사용하여 인증서 관리
CLI 명령을 사용하여 수동으로 인증서를 교체합니다.	CLI 명령으로 인증서 및 서비스 관리



vSphere 인증서 관리

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

본 장은 다음 항목을 포함합니다.

- 다양한 솔루션 경로에 대한 인증서 요구 사항
- 인증서 관리 개요
- Platform Services Controller 웹 인터페이스를 사용하여 인증서 관리
- vSphere Certificate Manager 유틸리티를 사용하여 인증서 관리
- 수동 인증서 교체

- CLI 명령으로 인증서 및 서비스 관리
- vSphere Web Client를 사용하여 vCenter 인증서 보기
- vCenter 인증서 만료 경고의 임계값 설정

다양한 솔루션 경로에 대한 인증서 요구 사항

인증서 요구 사항은 VMCA를 중간 CA로 사용하는지, 아니면 사용자 지정 인증서를 사용하는지에 따라 달라집니다. 또한 시스템 인증서와 솔루션 사용자 인증서 간에 요구 사항이 다릅니다.

시작하기 전에 환경의 모든 노드에서 시간이 동기화되는지 확인합니다.

가져온 모든 인증서에 대한 요구 사항

- 키 크기: 2048비트 이상(PEM 인코딩)
- 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, 부인 방지, 키 암호화
- 고급 키 사용에 클라이언트 인증과 서버 인증을 포함하면 안 됩니다.

VMCA는 다음 인증서를 지원하지 않습니다.

- 와일드카드가 있는 인증서
- 알고리즘 md2WithRSAEncryption 1.2.840.113549.1.1.2, md5WithRSAEncryption 1.2.840.113549.1.1.4 및 sha1WithRSAEncryption 1.2.840.113549.1.1.5는 권장되지 않습니다.
- 또한 RSASSA-PSS(OID 1.2.840.113549.1.1.10) 알고리즘은 지원되지 않습니다.

인증서의 RFC 2253 규정 준수

인증서는 RFC 2253 규정을 준수해야 합니다.

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

문자열	X.500 AttributeType
CN	commonName
L	localityName
ST	stateOrProvinceName
O	organizationName
OU	organizationalUnitName

문자열	X.500 AttributeType
C	countryName
STREET	streetAddress
DC	domainComponent
UID	userid

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

- 연결하는 vCenter Single Sign-On 도메인의 관리자 또는 administrator@vsphere.local 사용자의 암호
- 외부 Platform Services Controller가 있는 환경에서 CSR을 생성할 경우 Platform Services Controller의 호스트 이름 또는 IP 주소를 입력하라는 메시지가 표시됩니다.
- Certificate Manager가 certtool.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.
 - vCenter Server (관리) 노드에서 명령을 실행하는 경우 Platform Services Controller의 IP 주소

VMCA를 중간 CA로 사용하는 경우의 요구 사항

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

인증서 유형	인증서 요구 사항
루트 인증서	<ul style="list-style-type: none"> ■ vSphere Certificate Manager를 사용하여 CSR을 생성할 수 있습니다. vSphere 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. <ul style="list-style-type: none"> ■ 키 크기: 2048비트 이상 ■ PEM 형식. VMware는 PKCS8 및 PKCS1(RSA 키)을 지원합니다. 키가 VECS에 추가되면 추가된 키가 PKCS8로 변환됩니다. ■ x509 버전 3 ■ 사용자 지정 인증서를 사용하는 경우 CA 확장을 루트 인증서에 대해 true로 설정해야 하며 인증서 서명이 요구 사항 목록에 있어야 합니다. ■ CRL 서명을 사용하도록 설정해야 합니다. ■ 고급 키 사용에 클라이언트 인증 또는 서버 인증을 포함하면 안 됩니다. ■ 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. <p>Microsoft CA(인증 기관)를 사용하는 예는 VMware 기술 자료 문서 2112009, Creating a Microsoft Certificate Authority Template for SSL certificate creation in vSphere 6.0(vSphere 6.0에서 SSL 인증서 생성에 사용할 Microsoft CA(인증 기관) 템플릿 생성)을 참조하십시오.</p>
시스템 SSL 인증서	<p>vSphere Certificate Manager를 사용하여 CSR을 생성하거나 수동으로 CSR을 생성할 수 있습니다.</p> <p>CSR을 수동으로 생성하는 경우 위의 "가져온 모든 인증서에 대한 요구 사항" 목록에 나온 요구 사항을 충족해야 합니다. 또한 호스트의 FQDN을 지정해야 합니다.</p>
솔루션 사용자 인증서	<p>vSphere Certificate Manager를 사용하여 CSR을 생성하거나 수동으로 CSR을 생성할 수 있습니다.</p> <p>참고 각 솔루션 사용자의 이름에 다른 값을 사용해야 합니다. 인증서를 수동으로 생성하는 경우 사용하는 도구에 따라 주체 아래에 CN으로 표시될 수 있습니다.</p> <p>vSphere Certificate Manager를 사용하는 경우 각 솔루션 사용자에 대한 인증서 정보를 입력하라는 메시지가 표시됩니다. vSphere Certificate Manager가 이 정보를 certool.cfg에 저장합니다. "Certificate Manager에서 요청하는 정보"를 참조하십시오.</p>

사용자 지정 인증서에 대한 요구 사항

사용자 지정 인증서를 사용하려면 인증서가 다음 요구 사항을 충족해야 합니다.

인증서 유형	인증서 요구 사항
시스템 SSL 인증서	<p>각 노드의 시스템 SSL 인증서는 타사 또는 엔터프라이즈 CA에서 받은 별도의 인증서를 가져야 합니다.</p> <ul style="list-style-type: none"> ■ vSphere Certificate Manager를 사용하여 CSR을 생성하거나 수동으로 생성할 수 있습니다. CSR은 위의 "가져온 모든 인증서에 대한 요구 사항" 목록에 나온 요구 사항을 충족해야 합니다. ■ vSphere Certificate Manager를 사용하는 경우 각 솔루션 사용자에게 인증서 정보를 입력하라는 메시지가 표시됩니다. vSphere Certificate Manager가 이 정보를 certool.cfg에 저장합니다. "Certificate Manager에서 요청하는 정보"를 참조하십시오. ■ 대부분의 필드에서 기본값을 수락하거나 사이트별 값을 제공할 수 있습니다. 시스템의 FQDN은 필수 항목입니다.
솔루션 사용자 인증서	<p>각 노드의 각 솔루션 사용자는 타사 또는 엔터프라이즈 CA에서 받은 별도의 인증서를 가져야 합니다.</p> <ul style="list-style-type: none"> ■ vSphere Certificate Manager를 사용하여 CSR을 생성하거나 직접 준비할 수 있습니다. CSR은 위의 "가져온 모든 인증서에 대한 요구 사항" 목록에 나온 요구 사항을 충족해야 합니다. ■ vSphere Certificate Manager를 사용하는 경우 각 솔루션 사용자에게 인증서 정보를 입력하라는 메시지가 표시됩니다. vSphere Certificate Manager가 이 정보를 certool.cfg에 저장합니다. "Certificate Manager에서 요청하는 정보"를 참조하십시오. <p>참고 각 솔루션 사용자의 이름에 다른 값을 사용해야 합니다. 인증서를 수동으로 생성하는 경우 사용하는 도구에 따라 주제 아래에 CN으로 표시될 수 있습니다.</p> <p>이후에 솔루션 사용자 인증서를 사용자 지정 인증서로 교체하는 경우 타사 CA의 전체 서명 인증서 체인을 제공해야 합니다.</p>

참고 사용자 지정 인증서에는 CRL 배포 지점, 기관 정보 액세스 또는 인증서 템플릿 정보를 사용하지 않습니다.

인증서 관리 개요

새 인증서 인프라가 미치는 영향은 환경의 요구 사항, 새로 설치 중인지 업그레이드 중인지, ESXi 또는 vCenter Server 중 무엇을 고려 중인지에 따라 달라집니다.

VMware 인증서를 교체하지 않는 관리자

현재 VMware 인증서를 교체 중이지 않은 관리자인 경우 VMCA가 모든 인증서 관리를 처리할 수 있습니다. VMCA는 VMCA를 루트 인증 기관으로 사용하는 인증서로 vCenter Server 구성 요소와 ESXi 호스트를 프로비저닝합니다. 이전 버전의 vSphere에서 vSphere 6로 업그레이드 중인 경우에는 자체 서명된 모든 인증서가 VMCA에 의해 서명된 인증서로 교체됩니다.

VMware 인증서를 사용자 지정 인증서로 교체하는 관리자

새로 설치 시 관리자는 회사 정책에 따라 타사 또는 엔터프라이즈 인증 기관이 서명한 인증서가 필요하거나 사용자 지정 인증서 정보가 필요한 경우 다음 중에서 선택할 수 있습니다.

- VMCA 루트 인증서를 CA 서명된 인증서로 교체합니다. 이 시나리오에서 VMCA 인증서는 이 타사 CA의 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 교체해야 합니다. vSphere Certificate Manager 유틸리티를 사용하거나 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 VECS의 TRUSTED_ROOTS 저장소에 추가해야 합니다.

vCenter Server 업그레이드 후에는 관리자가 인증서 모드를 사용자 지정으로 설정할 수 있습니다([인증서 모드 변경](#) 참조). 인증서 모드가 기본값인 VMCA일 때 사용자가 vSphere Web Client에서 인증서 새로 고침을 수행하면 VMCA 서명 인증서가 사용자 지정 인증서로 교체됩니다.

- vCenter Server 구성 요소의 경우 수행되는 작업은 기존 환경에 따라 달라집니다.
 - 단순 설치를 내장된 배포로 업그레이드하는 경우에는 vCenter Server 사용자 지정 인증서가 유지됩니다. 업그레이드 후 환경은 이전처럼 작동합니다.
 - vCenter Single Sign-On과 vCenter Server 구성 요소가 서로 다른 시스템에 있는 다중 사이트 배포를 업그레이드하는 경우, 업그레이드 프로세스에서는 Platform Services Controller 노드와 하나 이상의 관리 노드가 포함된 다중 노드 배포를 생성합니다.

이 시나리오에서는 기존 vCenter Server 및 vCenter Single Sign-On 인증서가 유지되며 시스템 SSL 인증서로 사용됩니다. VMCA는 VMCA 서명 인증서를 각 솔루션 사용자(vCenter 서비스 모음)에게 할당합니다. 솔루션 사용자는 이 인증서를 vCenter Single Sign-On에 인증하는 용도로만 사용하므로 솔루션 사용자 인증서를 교체할 필요가 없을 수 있습니다.

새로운 아키텍처로 인해 서비스 배포와 교체가 달라졌기 때문에 vSphere 5.5 설치에 사용 가능했던 vSphere 5.5 인증서 교체 도구를 더 이상 사용할 수 없습니다. 대부분의 인증서 관리 작업에 새로운 명령줄 유틸리티인 vSphere Certificate Manager를 사용할 수 있습니다.

vCenter 인증서 인터페이스

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

vSphere Certificate Manager 유틸리티

일반적인 인증서 교체 작업 모두를 명령줄에서 수행합니다.

인증서 관리 CLI

`dir-cli`, `certool` 및 `vecs-cli`를 사용하여 모든 인증서 관리 작업을 수행합니다.

vSphere Web Client 인증서 관리

만료 정보를 포함하여 인증서를 봅니다.

ESXi의 경우 vSphere Web Client에서 인증서 관리를 수행합니다. 인증서는 VMCA에 의해 프로비저닝되며 `vmdir` 또는 `VECS`가 아니라 ESXi 호스트에만 로컬로 저장됩니다. [ESXi 호스트에 대한 인증서 관리를 참조하십시오.](#)

지원되는 vCenter 인증서

vCenter Server, Platform Services Controller, 관련 시스템 및 서비스의 경우 다음 인증서가 지원됩니다.

- VMCA(VMware 인증 기관)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.

인증서 교체 개요

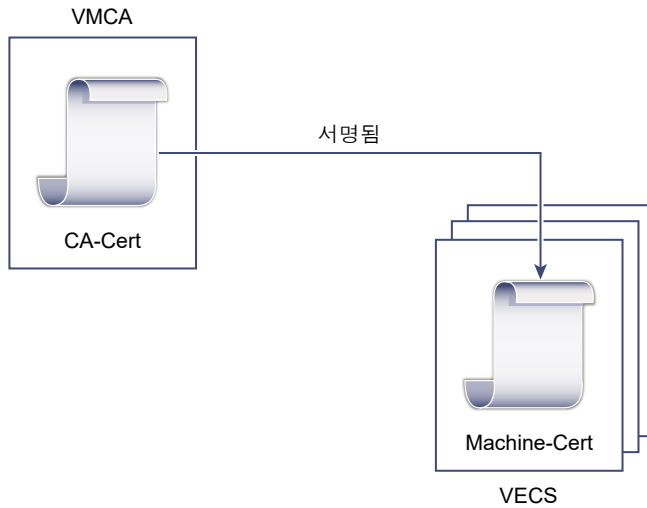
구성하는 시스템에 대한 요구 사항과 회사 정책에 따라 다양한 유형의 인증서 교체를 수행할 수 있습니다. vSphere Certificate Manager 유틸리티를 사용하거나 설치에 포함된 CLI를 사용하여 수동으로 각각의 교체를 수행할 수 있습니다.

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

VMCA에서 서명한 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 3-1. VMCA에서 서명한 인증서가 VECS에 저장됨

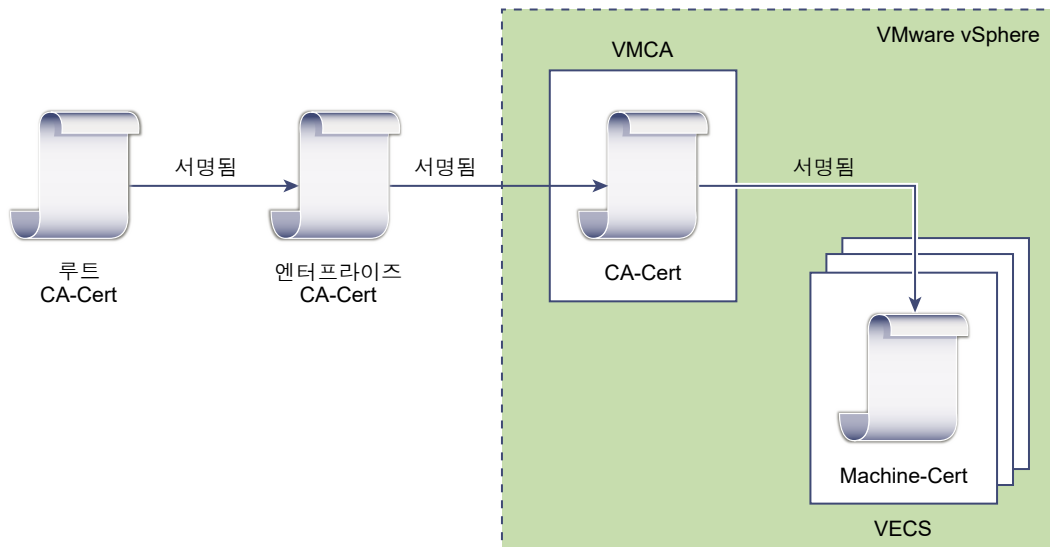


VMCA를 중간 CA로 만들기

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

참고 외부 Platform Services Controller가 포함된 새로 설치를 수행하는 경우 먼저 Platform Services Controller를 설치한 다음 VMCA 루트 인증서를 교체합니다. 다음으로 다른 서비스를 설치하거나 환경에 ESXi 호스트를 추가합니다. 내장된 Platform Services Controller로 새로 설치를 수행하는 경우 ESXi 호스트를 추가하기 전에 VMCA 루트 인증서를 교체합니다. 그렇게 하면 모든 인증서가 전체 체인에 의해 서명되고 새 인증서를 생성하지 않아도 됩니다.

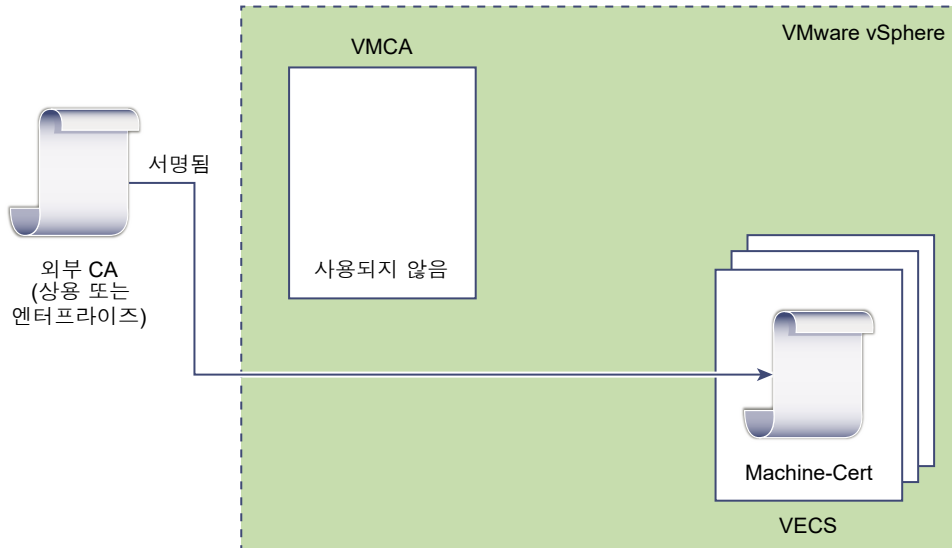
그림 3-2. 타사 또는 엔터프라이즈 CA에서 서명한 인증서가 VMCA를 중간 CA로 사용



VMCA 사용 안 함, 사용자 지정 인증서로 프로비저닝

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

그림 3-3. 외부 인증서가 VECS에 직접 저장됨



하이브리드 배포

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.

ESXi 인증서 교체

ESXi 호스트의 경우 vSphere Web Client에서 인증서 프로비저닝 동작을 변경할 수 있습니다.

VMware 인증 기관 모드(기본값)

vSphere Web 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.

vSphere 6.0에서 인증서를 사용하는 위치

vSphere 6.0 이상에서는 VMCA(VMware 인증 기관)가 인증서로 사용자 환경을 프로비저닝합니다. 여기에는 보안 연결을 위한 시스템 SSL 인증서, vCenter Single Sign-On에 인증하기 위한 솔루션 사용자 인증서 및 vCenter Server에 추가된 ESXi 호스트용 인증서가 포함됩니다.

다음의 인증서가 사용됩니다.

표 3-2. vSphere 6.0의 인증서

인증서	프로비저닝 주체	저장 위치
ESXi 인증서	VMCA(기본값)	ESXi 호스트에 로컬로
시스템 SSL 인증서	VMCA(기본값)	VECS
솔루션 사용자 인증서	VMCA(기본값)	VECS
vCenter Single Sign-On SSL 서명 인증서	설치 도중 프로비저닝됩니다.	vSphere Web Client에서 이 인증서를 관리합니다. 경고 파일 시스템에서 이 인증서를 변경하지 마십시오. 변경할 경우 예기치 않은 동작이 발생합니다.
vmdir(VMware 디렉토리 서비스) SSL 인증서	설치 도중 프로비저닝됩니다.	예외적 경우 이 인증서를 교체해야 할 수 있습니다. VMware 디렉토리 서비스 인증서 교체 를 참조하십시오.

ESXi

ESXi 인증서는 각 호스트의 `/etc/vmware/ssl` 디렉터리에 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.

시스템 SSL 인증서

각 노드의 시스템 SSL 인증서는 SSL 클라이언트가 연결하는 서버측에서 SSL 소켓을 만드는 데 사용됩니다. 인증서는 서버 확인 및 HTTPS나 LDAPS와 같은 보안 통신에 사용됩니다.

모든 서비스는 역방향 프록시를 통해 통신합니다. 호환성을 위해 이전 버전의 vSphere에서 사용 가능하던 서비스도 특정 포트를 사용할 수 있습니다. 예를 들어 vpxd 서비스는 MACHINE_SSL_CERT를 사용하여 끝점을 제공합니다.

모든 노드(내장된 배포, 관리 노드 또는 Platform Services Controller)에 자체 시스템 SSL 인증서가 있습니다. 해당 노드에서 실행 중인 모든 서비스는 이 시스템 SSL 인증서를 사용하여 SSL 끝점을 제공합니다.

시스템 SSL 인증서는 다음과 같은 방식으로 사용됩니다.

- 각 Platform Services Controller 노드의 역방향 프록시 서비스에 의해, 개별 vCenter 서비스로의 SSL 연결은 항상 역방향 프록시로 이동합니다. 트래픽이 서비스 자체로 이동하지 않습니다.
- 관리 노드 및 포함된 노드의 vCenter 서비스(vpxd)에 의해.
- 인프라 노드 및 포함된 노드의 vmdir(VMware 디렉토리 서비스)에 의해.

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

솔루션 사용자 인증서

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

솔루션 사용자 인증서는 vCenter Single Sign-On에 인증하는 용도로 사용됩니다. 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 Web Client에서 설정할 수 있으며 기본값은 2592000초(30일)입니다.

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

각 관리 노드 및 각 내장된 배포의 VECS에 다음의 솔루션 사용자 인증서 저장소가 포함되어 있습니다.

- machine: 구성 요소 관리자, 라이선스 서버 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: 관리 노드 및 내장된 배포의 vCenter 서비스 대문(vpxd) 저장소. vpxd는 이 저장소에 저장된 솔루션 사용자 인증서를 사용하여 vCenter Single Sign-On에 인증합니다.
- vpxd-extensions: vCenter 확장 저장소. Auto Deploy 서비스, Inventory Service를 비롯해 다른 솔루션 사용자의 일부가 아닌 기타 서비스가 포함됩니다.
- vsphere-webclient: vSphere Web Client 저장소. 성능 차트 서비스와 같은 일부 추가 서비스도 포함됩니다.

시스템 저장소는 각 Platform Services Controller 노드에도 포함됩니다.

vCenter Single Sign-On 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.

vCenter Single Sign-On은 솔루션 사용자에게 키 소유자 SAML 토큰을 사용자 이름과 암호로 로그인하는 다른 사용자에게 보유자 토큰을 발급합니다.

vSphere Web Client에서 이 인증서를 교체할 수 있습니다. [보안 토큰 서비스 인증서 새로 고침](#)을 참조하십시오.

VMware 디렉토리 서비스 SSL 인증서

사용자 지정 인증서를 사용하는 경우 VMware Directory Service SSL 인증서를 명시적으로 교체해야 할 수 있습니다. [VMware 디렉토리 서비스 인증서 교체](#)를 참조하십시오.

VMCA 및 VMware 핵심 ID 서비스

핵심 ID 서비스는 모든 내장된 배포와 모든 플랫폼 서비스 노드의 일부입니다. VMCA는 모든 VMware 핵심 ID 서비스 그룹에 속합니다. 이러한 서비스와 상호 작용하려면 관리 CLI 및 vSphere Web Client를 사용합니다.

VMware 핵심 ID 서비스에는 몇 개의 구성 요소가 포함됩니다.

표 3-3. 핵심 ID 서비스

서비스	설명	포함된 위치
VMware 디렉토리 서비스(vmdir)	vCenter Single Sign-On과 함께 인증하기 위한 SAML 인증서 관리를 처리합니다.	Platform Services Controller 내장된 배포
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.	Platform Services Controller 내장된 배포
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.	Platform Services Controller vCenter Server 내장된 배포

VMware Endpoint 인증서 저장소 개요

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 인증 프레임워크 대몬)의 일부로 실행됩니다. VECS는 모든 내장된 배포, Platform Services Controller 노드 및 관리 노드에서 실행되며 인증서와 키가 포함된 키 저장소를 포함합니다.

VECS는 TRUSTED_ROOTS 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 참조](#)를 참조하십시오.

VECS에는 다음과 같은 저장소가 포함됩니다.

표 3-4. VECS의 저장소

저장소	설명
시스템 SSL 저장소(MACHINE_SSL_CERT)	<ul style="list-style-type: none"> 모든 vSphere 노드의 역방향 프록시 서비스에서 사용됩니다. 내장된 배포 및 각 Platform Services Controller 노드의 VMware 디렉토리 서비스(vmdir)에서 사용합니다. <p>vSphere 6.0에서 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 아직 자체 포트를 열어둡니다.</p>
신뢰할 수 있는 루트 저장소(TRUSTED_ROOTS)	모든 신뢰할 수 있는 루트 인증서가 포함됩니다.
솔루션 사용자 저장소 <ul style="list-style-type: none"> machine vpxd vpxd-extensions vsphere-webclient 	<p>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.</p> <p>솔루션 사용자 인증서는 vCenter Single Sign-On을 사용한 인증에 사용됩니다. vCenter Single Sign-On은 인증서가 올바른지 확인하지만 다른 인증서 특성은 확인하지 않습니다. 포함된 배포에서 모든 솔루션 사용자 인증서는 같은 시스템에 있습니다.</p> <p>각 관리 노드 및 각 내장된 배포의 VECS에 다음의 솔루션 사용자 인증서 저장소가 포함되어 있습니다.</p> <ul style="list-style-type: none"> machine: 구성 요소 관리자, 라이선스 서버 및 로깅 서비스에서 사용됩니다. <p>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.</p> <ul style="list-style-type: none"> vpxd: 관리 노드 및 내장된 배포의 vCenter 서비스 대몬(vpxd) 저장소. vpxd는 이 저장소에 저장된 솔루션 사용자 인증서를 사용하여 vCenter Single Sign-On에 인증합니다. vpxd-extensions: vCenter 확장 저장소. Auto Deploy 서비스, Inventory Service를 비롯해 다른 솔루션 사용자의 일부가 아닌 기타 서비스가 포함됩니다. vsphere-webclient: vSphere Web Client 저장소. 성능 차트 서비스와 같은 일부 추가 서비스도 포함됩니다. <p>시스템 저장소는 각 Platform Services Controller 노드에도 포함됩니다.</p>

표 3-4. VECS의 저장소 (계속)

저장소	설명
vSphere Certificate Manager 유틸리티 백업 저장소 (BACKUP_STORE)	VMCA(VMware Certificate Manager)에서 인증서 복구를 지원하기 위해 사용됩니다. 최근 상태만 백업으로 저장되며 한 단계까지만 되돌아갈 수 있습니다.
기타 저장소	솔루션을 통해 기타 저장소가 추가될 수 있습니다. 예를 들어 가상 볼륨 솔루션은 SMS 저장소를 추가합니다. VMware 설명서 또는 VMware 기술 자료 문서에서 그렇게 하라고 지시하지 않는 이상 이러한 저장소의 인증서를 수정하지 마십시오. 참고 CRLS는 vSphere 6.0에서 지원되지 않지만 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.

vSphere Web Client에서 토큰 서명 인증서를 변경할 수 있습니다.

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

일부 인증서는 시작 도중 임시로 또는 영구적으로 파일 시스템에 저장됩니다. 파일 시스템의 인증서를 변경하지 마십시오. VECS에 저장된 인증서에 대한 작업을 수행하려면 `vecs-cli`를 사용합니다.

인증서 해지 관리

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

vSphere 6.0는 인증서 교체를 지원하지만 ESXi 호스트 또는 vCenter Server 시스템에 대한 인증서 해지는 적용하지 않습니다.

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

대규모 배포에서 인증서 교체

여러 관리 노드와 하나 이상의 Platform Services Controller 노드가 내장된 배포에서의 인증서 교체는 내장된 배포에서의 교체와 비슷합니다. 두 경우 모두 vSphere Certificate Management 유틸리티를 사용하여 인증서를 교체하거나 수동으로 교체할 수 있습니다. 교체 프로세스의 지침이 되는 몇 가지 모범 사례가 있습니다.

로드 밸런서가 포함된 고가용성 환경에서 인증서 교체

vCenter Server 시스템이 8개 미만인 환경에서는 일반적으로 하나의 Platform Services Controller 인스턴스 및 연관된 vCenter Single Sign-On 서비스를 권장합니다. 대규모 환경인 경우, 네트워크 로드 밸런서로 보호되는 여러 Platform Services Controller 인스턴스를 사용하는 것을 고려해 보십시오. VMware 웹 사이트의 "vCenter Server 6.0 배포 가이드" 백서에는 이 설정에 대한 설명이 있습니다.

관리 노드가 여러 개인 환경에서 시스템 SSL 인증서 교체

환경에 여러 개의 관리 노드와 하나의 Platform Services Controller가 포함된 경우 vSphere Certificate Manager 유틸리티를 사용하여 인증서를 교체하거나 vSphere CLI 명령을 사용하여 수동으로 교체할 수 있습니다.

vSphere Certificate Manager

각 시스템에서 vSphere Certificate Manager를 실행합니다. 관리 노드에서 Platform Services Controller의 IP 주소를 입력하라는 메시지가 표시됩니다. 수행하는 작업에 따라 인증서 정보를 묻는 메시지도 표시됩니다.

수동 인증서 교체

수동으로 인증서를 교체할 때는 각 시스템에서 인증서 교체 명령을 실행합니다. 관리 노드에서 --server 매개변수를 사용하여 Platform Services Controller를 지정합니다. 자세한 내용은 다음 항목을 참조하십시오.

- [VMCA 서명된 인증서로 시스템 SSL 인증서 교체](#)
- [시스템 SSL 인증서 교체\(중간 CA\)](#)
- [시스템 SSL 인증서를 사용자 지정 인증서로 교체](#)

관리 노드가 여러 개인 환경에서 솔루션 사용자 인증서 교체

환경에 여러 개의 관리 노드와 하나의 Platform Services Controller가 포함된 경우 인증서 교체 시 다음 단계를 따르십시오.

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

vSphere Certificate Manager

각 시스템에서 vSphere Certificate Manager를 실행합니다. 관리 노드에서 Platform Services Controller의 IP 주소를 입력하라는 메시지가 표시됩니다. 수행하는 작업에 따라 인증서 정보를 묻는 메시지도 표시됩니다.

수동 인증서 교체

- 1 인증서를 생성하거나 요청합니다. 다음 인증서가 필요합니다.
 - Platform Services Controller의 시스템 솔루션 사용자용 인증서.
 - 각 관리 노드의 시스템 솔루션 사용자용 인증서.
 - 각 관리 노드에서 다음 솔루션 사용자 각각을 위한 인증서:
 - vpxd 솔루션 사용자
 - vpxd-extension 솔루션 사용자
 - vsphere-webclient 솔루션 사용자
- 2 각 노드에서 인증서를 교체합니다. 정확한 프로세스는 수행 중인 인증서 교체의 유형에 따라 다릅니다. **vSphere Certificate Manager** 유틸리티를 사용하여 인증서 관리 항목을 참조하십시오.

자세한 내용은 다음 항목을 참조하십시오.

- 새 VMCA 서명된 인증서로 솔루션 사용자 인증서 교체
- 솔루션 사용자 인증서 교체(중간 CA)
- 솔루션 사용자 인증서를 사용자 지정 인증서로 교체

회사 정책에 따라 모든 인증서를 교체해야 하는 경우에는 Platform Services Controller에서 vmdir(VMware 디렉토리 서비스) 인증서도 교체해야 합니다. **VMware 디렉토리 서비스 인증서 교체**를 참조하십시오.

외부 솔루션이 포함된 환경에서 인증서 교체

VMware vCenter Site Recovery Manager 또는 VMware vSphere Replication과 같은 일부 솔루션은 vCenter Server 시스템 또는 Platform Services Controller가 아닌 다른 시스템에 항상 설치됩니다. vCenter Server 시스템 또는 Platform Services Controller에서 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. 자세한 내용은 **VMware 기술 자료 문서 2109074**를 참조하십시오.

Platform Services Controller 웹 인터페이스를 사용하여 인증서 관리

Platform Services Controller 웹 인터페이스에 로그인하여 인증서를 보고 관리할 수 있습니다. vSphere Certificate Manager 유틸리티를 사용하거나 이 웹 인터페이스를 사용하여 여러 가지 인증서 관리 작업을 수행할 수 있습니다.

Platform Services Controller 웹 인터페이스에서는 다음과 같은 관리 작업을 수행할 수 있습니다.

- 현재 인증서 저장소를 보고 인증서 저장소 항목을 추가 및 제거
- 이 Platform Services Controller에 연결된 VMCA(VMware Certificate Authority) 보기
- VMware Certificate Authority에서 생성한 인증서 보기
- 기존 인증서 갱신 또는 인증서 교체

인증서 교체 워크플로우 대부분은 Platform Services Controller 웹 인터페이스에서 완벽하게 지원됩니다. CSR은 vSphere 인증서 관리자 유틸리티를 사용하여 생성할 수 있습니다.

지원되는 워크플로우

Platform Services Controller를 설치하면 해당 노드의 VMware Certificate Authority가 환경에 포함된 다른 모든 노드에 기본적으로 인증서를 프로비저닝합니다. 다음의 워크플로우 중 하나를 사용하여 인증서를 갱신하거나 교체할 수 있습니다.

인증서 갱신

VMCA에서 새 루트 인증서를 생성한 후 Platform Services Controller 웹 인터페이스에서 환경 내의 모든 인증서를 갱신할 수 있습니다.

VMCA를 중간 CA로 만들기

vSphere Certificate Manager 유틸리티를 사용하여 CSR을 생성하고, CSR에서 수신한 인증서를 편집하여 VMCA를 체인에 추가한 다음 인증서 체인과 개인 키를 환경에 추가할 수 있습니다. 모든 인증서를 갱신하면 VMCA는 전체 체인에서 서명한 인증서를 모든 시스템과 솔루션 사용자에게 프로비저닝합니다.

인증서를 사용자 지정 인증서로 교체

VMCA를 사용하지 않으려는 경우, 교체하려는 모든 인증서에 대해 CSR을 생성할 수 있습니다. CA에서는 각 CSR에 대해 루트 인증서와 서명된 인증서를 반환합니다. 루트 인증서와 사용자 지정 인증서는 Platform Services Controller에서 업로드할 수 있습니다.

VMware Directory Service(vmdir) 루트 인증서를 교체해야 하거나 회사 정책으로 인해 혼합 모드 환경에서 vCenter Single Sign-On 인증서를 교체해야 할 경우에는 CLI 명령을 사용하여 다른 인증서를 교체한 후 해당 인증서를 교체할 수 있습니다. [VMware 디렉토리 서비스 인증서 교체](#) 및 [혼합 모드 환경에서 VMware 디렉토리 서비스 인증서 교체](#) 항목을 참조하십시오.

Platform Services Controller 웹 인터페이스에서 인증서 저장소 탐색

VECS(VMware Endpoint 인증서 저장소) 인스턴스는 각 Platform Services Controller 노드와 각 vCenter Server 노드에 포함됩니다. Platform Services Controller 웹 인터페이스에서 VMware Endpoint 인증서 저장소 내의 여러 저장소를 탐색할 수 있습니다.

VECS 내의 여러 저장소에 대한 자세한 내용은 [VMware Endpoint 인증서 저장소 개요](#)를 참조하십시오.

사전 요구 사항

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

절차

- 1 웹 브라우저에서 다음 URL을 지정하여 Platform Services Controller에 연결합니다.

`https://psc_hostname_or_IP/psc`

내장된 배포에서 Platform Services Controller 호스트 이름 또는 IP 주소는 vCenter Server 호스트 이름 또는 IP 주소와 동일합니다.

- 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] 아래에서 **인증서 저장소**를 클릭하고 저장소를 탐색합니다.

- 4 탐색할 VECS(VMware Endpoint 인증서 저장소) 내의 저장소를 풀다운 메뉴에서 선택합니다.

VMware Endpoint 인증서 저장소 개요에서는 개별 저장소에 포함된 내용에 대해 설명합니다.

- 5 인증서의 세부 정보를 보려면 인증서를 선택하고 **세부 정보 표시** 아이콘을 클릭합니다.

- 6 선택한 저장소에서 항목을 삭제하려면 **항목 삭제** 아이콘을 클릭합니다.

예를 들어 기존 인증서를 교체하면 나중에 이전 루트 인증서를 제거할 수 있습니다. 인증서는 더 이상 사용되지 않는 것이 확실한 경우에만 제거하십시오.

Platform Services Controller 웹 인터페이스에서 인증서를 새로운 VMCA 서명 인증서로 교체

모든 VMCA 서명된 인증서를 새로운 VMCA 서명된 인증서로 교체할 수 있습니다. 이 프로세스를 인증서 갱신이라고 합니다. Platform Services Controller 웹 인터페이스에서 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 웹 브라우저에서 다음 URL을 지정하여 Platform Services Controller에 연결합니다.

`https://psc_hostname_or_IP/psc`

내장된 배포에서 Platform Services Controller 호스트 이름 또는 IP 주소는 vCenter Server 호스트 이름 또는 IP 주소와 동일합니다.

- 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@mydomain으로 로그인합니다.

- 3 [인증서] 아래에서 **인증서 관리**를 선택하고 Platform Services Controller의 IP 주소나 호스트 이름 및 로컬 도메인 관리자(기본적으로 administrator@vsphere.local)의 사용자 이름과 암호를 지정한 다음 **제출**을 클릭합니다.

- 4 로컬 시스템의 시스템 SSL 인증서를 갱신합니다.

- a **시스템 인증서** 탭을 클릭합니다.

- b 인증서를 선택하고 **갱신**을 클릭한 다음 표시되는 메시지에 대해 **예**를 선택합니다.

- 5 (선택 사항) 로컬 시스템의 솔루션 사용자 인증서를 갱신합니다.

- a **솔루션 사용자 인증서** 탭을 클릭합니다.

- b 인증서를 선택하고 **갱신**을 클릭하여 선택한 개별 인증서를 갱신하거나 **모두 갱신**을 클릭하여 모든 솔루션 사용자 인증서를 갱신합니다.

- c 표시되는 메시지에 대해 **예**를 선택합니다.

- 6 환경에 외부 Platform Services Controller가 있는 경우에는 각 vCenter Server 시스템의 인증서를 갱신할 수 있습니다.

- a [인증서 관리] 패널에서 **로그아웃** 버튼을 클릭합니다.

- b 메시지가 표시되면 vCenter Server 시스템의 IP 주소나 FQDN 및 vCenter Single Sign-On에 인증될 수 있는 vCenter Server 관리자의 사용자 이름과 암호를 지정합니다.

- c vCenter Server의 시스템 SSL 인증서를 갱신하고, 필요한 경우 각 솔루션 사용자 인증서를 갱신합니다.

- d 환경에 vCenter Server 시스템이 여러 개 있는 경우에는 각 시스템에 대해 이 프로세스를 반복합니다.

다음에 수행할 작업

Platform Services Controller에서 서비스를 다시 시작합니다. Platform Services Controller를 다시 시작하거나, 명령줄에서 다음 명령을 실행할 수 있습니다.

Windows

Windows에서 service-control 명령은 `VCENTER_INSTALL_PATH\bin`에 있습니다.

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

vCenter Server Appliance

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

Platform Services Controller 웹 인터페이스에서 WMCA를 중간 인증 기관으로 만들기

VMCA 인증서를 다른 CA에서 서명하도록 하여 해당 VMCA를 중간 CA로 설정할 수 있습니다. 이렇게 하면 이 VMCA가 생성하는 모든 인증서에 전체 체인이 포함됩니다.

이 설정은 vSphere Certificate Manager 유틸리티를 사용하거나, CLI를 사용하거나 Platform Services Controller 웹 인터페이스에서 수행할 수 있습니다.

사전 요구 사항

- 1 CSR을 생성합니다.
- 2 수신하는 인증서를 편집하고 현재 VMCA 루트 인증서를 맨 아래에 배치합니다.

vSphere Certificate Manager를 사용하여 CSR 생성 및 루트 인증서(중간 CA) 준비에서는 이 두 단계에 대해 설명합니다.

절차

- 1 웹 브라우저에서 다음 URL을 지정하여 Platform Services Controller에 연결합니다.

`https://psc_hostname_or_IP/psc`

내장된 배포에서 Platform Services Controller 호스트 이름 또는 IP 주소는 vCenter Server 호스트 이름 또는 IP 주소와 동일합니다.

- 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@mydomain으로 로그인합니다.

3 기존 인증서를 체인 인증서로 교체하려면 다음 단계를 수행하십시오.

- a 인증서 아래에서 **인증 기관**을 클릭하고 **루트 인증서** 탭을 선택합니다.
- b **인증서 교체**를 클릭합니다. 개인 키 파일과 인증서 파일(전체 체인)을 추가한 후 **확인**을 클릭합니다.
- c **루트 인증서 교체** 대화상자에서 **찾아보기**를 클릭하여 개인 키를 선택하고, 다시 **찾아보기**를 클릭하여 인증서를 선택한 후 **확인**을 클릭합니다.

이렇게 하면 VMCA는 발급하는 모든 인증서를 새로운 체인 루트 인증서를 사용하여 서명합니다.

4 로컬 시스템의 시스템 SSL 인증서를 갱신합니다.

- a 인증서 아래에서 **인증서 관리**를 클릭하고 **시스템 인증서** 탭을 클릭합니다.
- b 인증서를 선택하고 **갱신**을 클릭한 다음 표시되는 메시지에 대해 **예**를 선택합니다.

VMCA가 시스템 SSL 인증서를 새 CA가 서명한 인증서로 교체합니다.

5 (선택 사항) 로컬 시스템의 솔루션 사용자 인증서를 갱신합니다.

- a **솔루션 사용자 인증서** 탭을 클릭합니다.
- b 인증서를 선택하고 **갱신**을 클릭하여 선택한 개별 인증서를 갱신하거나, **모두 갱신**을 클릭하여 모든 인증서를 교체한 후, 메시지가 표시되면 **예**를 선택합니다.

VMCA가 솔루션 사용자 인증서 또는 모든 솔루션 사용자 인증서를 새 CA가 서명한 인증서로 교체합니다.

6 환경에 외부 Platform Services Controller가 있는 경우에는 각 vCenter Server 시스템의 인증서를 갱신할 수 있습니다.

- a [인증서 관리] 패널에서 **로그아웃** 버튼을 클릭합니다.
- b 메시지가 표시되면 vCenter Server 시스템의 IP 주소나 FQDN 및 vCenter Single Sign-On에 인증될 수 있는 vCenter Server 관리자의 사용자 이름과 암호를 지정합니다.
- c vCenter Server의 시스템 SSL 인증서를 갱신하고, 필요한 경우 각 솔루션 사용자 인증서를 갱신합니다.
- d 환경에 vCenter Server 시스템이 여러 개 있는 경우에는 각 시스템에 대해 이 프로세스를 반복합니다.

다음에 수행할 작업

Platform Services Controller에서 서비스를 다시 시작합니다. Platform Services Controller를 다시 시작하거나, 명령줄에서 다음 명령을 실행할 수 있습니다.

Windows

Windows에서 service-control 명령은 `VCENTER_INSTALL_PATH\bin`에 있습니다.

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

vCenter Server Appliance

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

사용자 지정 인증서를 사용하도록 Platform Services Controller에서 시스템 설정

Platform Services Controller를 사용하면 사용자 지정 인증서를 사용하도록 환경을 설정할 수 있습니다.

인증서 관리자 유틸리티를 사용하여 각 시스템 및 각 솔루션 사용자에게 대해 CSR(인증서 서명 요청)을 생성할 수 있습니다. CSR을 내부 또는 타사 CA에 제출하면 CA는 서명된 인증서와 루트 인증서를 반환합니다. 루트 인증서와 서명된 인증서 둘 모두 Platform Services Controller UI에서 업로드할 수 있습니다.

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

vSphere Certificate Manager를 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.

다음과 같이 명령줄에서 인증서 관리자 도구를 실행할 수 있습니다.

Windows

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

Linux

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

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.
- 외부 Platform Services Controller가 있는 환경에서 CSR을 생성할 경우 Platform Services Controller의 호스트 이름 또는 IP 주소를 입력하라는 메시지가 표시됩니다.

- 시스템 SSL 인증서에 대한 CSR을 생성하는 경우 certtool.cfg 파일에 저장되는 인증서 속성을 묻습니다. 대부분의 필드에서 기본값을 수락하거나 사이트별 값을 제공할 수 있습니다. 시스템의 FQDN은 필수 항목입니다.

절차

- 1 사용자 환경의 각 시스템에서 vSphere Certificate Manager를 시작하고 옵션 1을 선택합니다.
- 2 메시지가 표시되면 암호 및 Platform Services Controller IP 주소 또는 호스트 이름을 제공합니다.
- 3 옵션 1을 선택하여 CSR을 생성하고 질문에 대답하고 인증서 관리자를 종료합니다.
해당 프로세스의 일부로, 디렉토리를 제공해야 합니다. 인증서 관리자가 디렉토리에 인증서 및 키 파일을 배치합니다.
- 4 또한 모든 솔루션 사용자 인증서를 교체하려면 인증서 관리자를 다시 시작합니다.
- 5 옵션 5를 선택합니다.
- 6 메시지가 표시되면 암호 및 Platform Services Controller IP 주소 또는 호스트 이름을 제공합니다.
- 7 옵션 1을 선택하여 CSR을 생성하고 질문에 대답하고 인증서 관리자를 종료합니다.
해당 프로세스의 일부로, 디렉토리를 제공해야 합니다. 인증서 관리자가 디렉토리에 인증서 및 키 파일을 배치합니다.

각각의 Platform Services Controller 노드에서 인증서 관리자가 한 개의 인증서와 키 쌍을 생성합니다. 각각의 vCenter Server 노드에서 인증서 관리자가 네 개의 인증서와 키 쌍을 생성합니다.

다음에 수행할 작업

인증서 교체를 수행합니다.

신뢰할 수 있는 루트 인증서를 인증서 저장소에 추가

환경에서 타사 인증서를 사용하려면 신뢰할 수 있는 루트 인증서를 인증서 저장소에 추가해야 합니다.

사전 요구 사항

타사 CA 또는 내부 CA에서 사용자 지정 루트 인증서를 가져옵니다.

절차

- 1 웹 브라우저에서 다음 URL을 지정하여 Platform Services Controller에 연결합니다.
https://psc_hostname_or_IP/psc
내장된 배포에서 Platform Services Controller 호스트 이름 또는 IP 주소는 vCenter Server 호스트 이름 또는 IP 주소와 동일합니다.
- 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@mydomain으로 로그인합니다.

- 3 [인증서] 아래에서 **인증서 관리**를 선택하고 Platform Services Controller의 IP 주소나 호스트 이름 및 로컬 도메인 관리자(기본적으로 `dministrator@vsphere.local`)의 사용자 이름과 암호를 지정한 다음 **제출**을 클릭합니다.
- 4 **신뢰할 수 있는 루트 인증서**를 선택하고 **인증서 추가**를 클릭합니다.
- 5 **찾아보기**를 클릭하고 인증서 체인의 위치를 선택합니다.
CER, PEM 또는 CRT 유형의 파일을 사용할 수 있습니다.

다음에 수행할 작업

시스템 SSL 인증서 및 필요한 경우 솔루션 사용자 인증서를 이 CA에서 서명한 인증서로 교체합니다.

Platform Services Controller에서 사용자 지정 인증서 추가

Platform Services Controller에서 사용자 지정 시스템 SSL 인증서와 사용자 지정 솔루션 사용자 인증서를 인증서 저장소에 추가할 수 있습니다.

대개는 각 구성 요소의 시스템 SSL 인증서를 교체하는 것으로도 충분합니다. 솔루션 사용자 인증서는 프록시 뒤에 남아 있습니다.

사전 요구 사항

교체할 각 인증서에 대해 CSR(인증서 서명 요청)을 생성합니다. CSR은 인증서 관리자 유틸리티를 사용하여 생성할 수 있습니다. 인증서와 개인 키를 Platform Services Controller에서 액세스할 수 있는 위치에 배치합니다.

절차

- 1 웹 브라우저에서 다음 URL을 지정하여 Platform Services Controller에 연결합니다.
`https://psc_hostname_or_IP/psc`
내장된 배포에서 Platform Services Controller 호스트 이름 또는 IP 주소는 vCenter Server 호스트 이름 또는 IP 주소와 동일합니다.
- 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] 아래에서 **인증서 관리**를 선택하고 Platform Services Controller의 IP 주소나 호스트 이름 및 로컬 도메인 관리자(기본적으로 `dministrator@vsphere.local`)의 사용자 이름과 암호를 지정한 다음 **제출**을 클릭합니다.
- 4 시스템 인증서를 교체하려면 다음 단계를 수행하십시오.
 - a **시스템 인증서** 탭을 선택하고 교체하려는 인증서를 클릭합니다.
 - b **교체**를 클릭하고 **찾아보기**를 클릭하여 인증서 체인을 교체한 다음 **찾아보기**를 클릭하여 개인 키를 교체합니다.

5 솔루션 사용자 인증서를 교체하려면 다음 단계를 수행하십시오.

- a **솔루션 사용자 인증서** 탭을 선택하고 구성 요소의 인증서 네 개 중 첫 번째 인증서(예: **시스템**)를 클릭합니다.
- b **교체**를 클릭하고 **찾아보기**를 클릭하여 인증서 체인을 교체한 다음 **찾아보기**를 클릭하여 개인 키를 교체합니다.
- c 같은 구성 요소의 나머지 인증서 세 개에 대해 동일한 과정을 반복합니다.

다음에 수행할 작업

Platform Services Controller에서 서비스를 다시 시작합니다. Platform Services Controller를 다시 시작하거나, 명령줄에서 다음 명령을 실행할 수 있습니다.

Windows

Windows에서 service-control 명령은 `VCENTER_INSTALL_PATH\bin`에 있습니다.

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

vCenter Server Appliance

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

vSphere Certificate Manager 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.

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

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.

다음과 같이 명령줄에서 도구를 실행할 수 있습니다.

Windows

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

Linux

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

절차

1 이전 인증서를 다시 게시하여 직전에 수행한 작업 되돌리기

vSphere Certificate Manager를 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.

2 모든 인증서 재설정

기존 vCenter 인증서 모두를 VMCA에서 서명한 인증서로 교체하려면 모든 인증서 재설정 옵션을 사용합니다.

3 새 VMCA 루트 인증서 다시 생성 및 모든 인증서 교체

VMCA 루트 인증서를 다시 생성하고, 로컬 시스템 SSL 인증서 및 로컬 솔루션 사용자 인증서를 VMCA 서명 인증서로 교체할 수 있습니다. 다중 노드 배포에서는 Platform Services Controller에서 이 옵션을 사용하여 vSphere Certificate Manager를 실행한 다음 다른 모든 노드에서 다시 유틸리티를 실행하고 시스템 SSL 인증서를 VMCA 인증서로 교체 및 솔루션 사용자 인증서를 VMCA 인증서로 교체를 선택합니다.

4 VMCA를 중간 CA(인증 기관)로 만들기(인증서 관리자)

인증서 관리자 유틸리티의 안내 메시지에 따라 VMCA를 중간 CA(인증 기관)로 만들 수 있습니다. 해당 프로세스를 완료한 후 VMCA가 전체 체인으로 모든 새 인증서에 서명합니다. 원하는 경우 인증서 관리자를 사용하여 모든 기존 인증서를 새 VMCA 서명 인증서로 교체할 수 있습니다.

5 모든 인증서를 사용자 지정 인증서로 교체(인증서 관리자)

vSphere Certificate Manager 유틸리티를 사용하여 모든 인증서를 사용자 지정 인증서로 교체할 수 있습니다. 프로세스를 시작하기 전에 CSR을 CA로 보내야 합니다. 인증서 관리자를 사용하여 CSR을 생성할 수 있습니다.

이전 인증서를 다시 게시하여 직전에 수행한 작업 되돌리기

vSphere Certificate Manager를 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 되돌리기됩니다.

모든 인증서 재설정

기존 vCenter 인증서 모두를 VMCA에서 서명한 인증서로 교체하려면 모든 인증서 재설정 옵션을 사용합니다.

이 옵션을 사용하면 현재 VECS에 있는 모든 사용자 지정 인증서를 덮어씁니다.

- Platform Services Controller 노드에서 vSphere Certificate Manager는 루트 인증서를 다시 생성하고 시스템 SSL 인증서 및 시스템 솔루션 사용자 인증서를 교체할 수 있습니다.
- 관리 노드에서 vSphere Certificate Manager는 시스템 SSL 인증서 및 모든 솔루션 사용자 인증서를 교체할 수 있습니다.
- 내장된 배포에서 vSphere Certificate Manager는 모든 인증서를 교체할 수 있습니다.

교체되는 인증서는 선택하는 옵션에 따라 달라집니다.

새 VMCA 루트 인증서 다시 생성 및 모든 인증서 교체

VMCA 루트 인증서를 다시 생성하고, 로컬 시스템 SSL 인증서 및 로컬 솔루션 사용자 인증서를 VMCA 서명 인증서로 교체할 수 있습니다. 다중 노드 배포에서는 Platform Services Controller에서 이 옵션을 사용하여 vSphere Certificate Manager를 실행한 다음 다른 모든 노드에서 다시 유틸리티를 실행하고 시스템 SSL 인증서를 VMCA 인증서로 교체 및 솔루션 사용자 인증서를 VMCA 인증서로 교체를 선택합니다.

이 명령을 실행하면 vSphere Certificate Manager가 암호 및 인증서 정보를 요청하고 암호를 제외한 모든 정보를 certtool.cfg 파일에 저장합니다. 그런 후의 서비스 중지, 모든 인증서 교체 및 프로세스 다시 시작은 자동으로 수행됩니다. 다음 정보를 묻는 메시지가 나타납니다.

- 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
- 관리 노드에서 명령을 실행하는 경우 Platform Services Controller의 IP 주소

사전 요구 사항

새 VMCA 서명 인증서를 생성할 시스템의 FQDN을 알아야 합니다. 다른 모든 속성은 사전 정의된 값을 기본값으로 사용합니다. IP 주소는 선택 사항입니다.

다음에 수행할 작업

다중 노드 배포에서 루트 인증서를 교체한 후에는 외부 Platform Services Controller 노드가 포함된 모든 vCenter Server에서 서비스를 다시 시작해야 합니다.

VMCA를 중간 CA(인증 기관)로 만들기(인증서 관리자)

인증서 관리자 유틸리티의 안내 메시지에 따라 VMCA를 중간 CA(인증 기관)로 만들 수 있습니다. 해당 프로세스를 완료한 후 VMCA가 전체 체인으로 모든 새 인증서에 서명합니다. 원하는 경우 인증서 관리자를 사용하여 모든 기존 인증서를 새 VMCA 서명 인증서로 교체할 수 있습니다.

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

vSphere Certificate Manager를 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.
- CSR을 수동으로 생성하려는 경우에는 서명을 위해 보내는 인증서가 다음 요구 사항을 충족해야 합니다.
 - 키 크기: 2048비트 이상
 - PEM 형식. VMware는 PKCS8 및 PKCS1(RSA 키)을 지원합니다. 키가 VECS에 추가되면 추가된 키가 PKCS8로 변환됩니다.
 - x509 버전 3
 - 사용자 지정 인증서를 사용하는 경우 CA 확장을 루트 인증서에 대해 true로 설정해야 하며 인증서 서명이 요구 사항 목록에 있어야 합니다.
 - CRL 서명을 사용하도록 설정해야 합니다.
 - 고급 키 사용에 클라이언트 인증 또는 서버 인증을 포함하면 안 됩니다.
 - 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 2112009, Creating a Microsoft Certificate Authority Template for SSL certificate creation in vSphere 6.0(vSphere 6.0에서 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 vSphere Certificate Manager를 시작하고 옵션 2를 선택합니다.

처음에는 이 옵션을 인증서를 교체하지 않고 CSR을 생성하는 데 사용합니다.

- 2 메시지가 표시되면 암호 및 Platform Services Controller IP 주소 또는 호스트 이름을 제공합니다.

- 3 옵션 1을 선택하여 CSR을 생성하고 질문에 대답합니다.

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

- 4 서명을 위해 인증서를 엔터프라이즈 CA 또는 외부 CA에 보내고 파일의 이름을 root_signing_cert.cer로 지정합니다.

- 5 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-----
```

- 6 파일을 root_signing_chain.cer로 저장합니다.

다음에 수행할 작업

기존 루트 인증서를 체인 루트 인증서로 교체합니다. 사용자 지정 서명 인증서로 VMCA 루트 인증서 교체 및 모든 인증서 교체를 참조하십시오.

사용자 지정 서명 인증서로 VMCA 루트 인증서 교체 및 모든 인증서 교체

VMCA 루트 인증서를 인증서 체인에 VMCA가 중간 인증서로 포함된 CA 서명 인증서로 교체할 수 있습니다. 그러면 VMCA가 생성하는 모든 인증서에 전체 체인이 포함됩니다.

포함된 설치 또는 외부 Platform Services Controller에서 vSphere Certificate Manager를 실행하여 VMCA 루트 인증서를 사용자 지정 서명 인증서로 교체합니다.

vSphere Certificate Manager는 사용자에게 다음 정보를 묻습니다.

사전 요구 사항

- CSR을 생성합니다.
 - vSphere Certificate Manager를 사용하여 CSR을 생성할 수 있습니다. vSphere Certificate Manager를 사용하여 CSR 생성 및 루트 인증서(중간 CA) 준비 항목을 참조하십시오.

- CSR을 수동으로 생성하려는 경우에는 서명을 위해 보내는 인증서는 다음 요구 사항을 충족해야 합니다.
 - 키 크기: 2048비트 이상
 - PEM 형식. VMware는 PKCS8 및 PKCS1(RSA 키)을 지원합니다. 키가 VECS에 추가되면 추가된 키가 PKCS8로 변환됩니다.
 - x509 버전 3
 - 사용자 지정 인증서를 사용하는 경우 CA 확장을 루트 인증서에 대해 true로 설정해야 하며 인증서 서명이 요구 사항 목록에 있어야 합니다.
 - CRL 서명을 사용하도록 설정해야 합니다.
 - 고급 키 사용에 클라이언트 인증 또는 서버 인증을 포함하면 안 됩니다.
 - 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 2112009, Creating a Microsoft Certificate Authority Template for SSL certificate creation in vSphere 6.0(vSphere 6.0에서 SSL 인증서 생성에 사용할 Microsoft CA(인증 기관) 템플릿 생성)을 참조하십시오.

- 타사 또는 기업 CA로부터 인증서를 수신한 후에는 이 인증서를 초기 VMCA 루트 인증서와 결합하여, 맨 아래에 VMCA 루트 인증서가 있는 전체 체인을 생성합니다. [vSphere Certificate Manager](#)를 사용하여 CSR 생성 및 루트 인증서(중간 CA) 준비를 참조하십시오.
- 필요한 정보를 수집합니다.
 - administrator@vsphere.local의 암호
 - 루트에 대한 유효한 사용자 지정 인증서(.crt 파일)
 - 루트에 유효한 사용자 지정 키(.key 키).

절차

- 1 내장된 설치 환경 또는 외부 Platform Services Controller에서 vSphere Certificate Manager를 시작하고 옵션 2를 선택합니다.
- 2 옵션 2를 선택하여 인증서 교체를 시작하고 프롬프트에 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.

- 3 다중 노드 배포에서 루트 인증서를 교체하는 경우에는 모든 vCenter Server에서 서비스를 다시 시작해야 합니다.
- 4 다중 노드 배포의 경우 옵션 3(VMCA 인증서로 시스템 SSL 인증서 교체)과 옵션 6(VMCA 인증서로 솔루션 사용자 인증서 교체)을 사용하여 각 vCenter Server 인스턴스에 있는 모든 인증서를 다시 생성합니다.

인증서를 교체하면 VMCA가 전체 체인으로 서명합니다.

다음에 수행할 작업

사용자 환경에 따라 추가 인증서를 명시적으로 교체해야 할 수 있습니다.

- 회사 정책에 따라 모든 인증서를 교체해야 하는 경우 vmdir 루트 인증서를 교체합니다. [VMware 디렉토리 서비스 인증서 교체](#) 항목을 참조하십시오.
- vSphere 5.x 환경에서 업그레이드하는 경우 vmdir 내에서 vCenter Single Sign-On 인증서를 교체해야 할 수 있습니다. [혼합 모드 환경에서 VMware 디렉토리 서비스 인증서 교체](#) 항목을 참조하십시오.

VMCA 인증서로 시스템 SSL 인증서 교체(중간 CA)

VMCA를 중간 CA로 사용하는 다중 노드 배포에서는 시스템 SSL 인증서를 명시적으로 교체해야 합니다. 먼저 Platform Services Controller 노드에서 VMCA 루트 인증서를 교체합니다. 그런 다음 vCenter Server 노드에서 인증서를 교체하여 인증서가 전체 체인에 의해 서명되도록 할 수 있습니다. 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 Platform Services Controller의 암호와 IP 주소를 제외한 모든 값을 certtool.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.
- 관리 노드에서 명령을 실행하는 경우 Platform Services Controller의 IP 주소

사전 요구 사항

- 다중 노드 배포에서 VMCA 루트 인증서를 교체한 경우 명시적으로 모든 vCenter Server 노드를 다시 시작합니다.
- 이 옵션으로 인증서 관리자를 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.
 - 외부 Platform Services Controller를 사용하여 vCenter Server 시스템에서 실행 중인 경우 Platform Services Controller의 호스트 이름 또는 IP 주소

절차

- 1 vSphere Certificate Manager를 시작하고 옵션 3를 선택합니다.
- 2 프롬프트에 응답합니다.

인증서 관리자가 certtool.cfg 파일에 정보를 저장합니다.

결과

vSphere Certificate Manager가 시스템 SSL 인증서를 교체합니다.

VMCA 인증서로 솔루션 사용자 인증서 교체(중간 CA)

VMCA를 중간 CA로 사용하는 다중 노드에서는 솔루션 사용자 인증서를 명시적으로 교체해야 합니다. 먼저 Platform Services Controller 노드에서 VMCA 루트 인증서를 교체합니다. 그런 다음 vCenter Server 노드에서 인증서를 교체하여 인증서가 전체 체인에 의해 서명되도록 할 수 있습니다. 또한 이 옵션을 사용하여 손상되거나 만료되려고 하는 솔루션 사용자 인증서를 교체할 수 있습니다.

사전 요구 사항

- 다중 노드 배포에서 VMCA 루트 인증서를 교체한 경우 명시적으로 모든 vCenter Server 노드를 다시 시작합니다.
- 이 옵션으로 인증서 관리자를 실행하려면 다음 정보를 알고 있어야 합니다.
 - administrator@vsphere.local의 암호
 - 외부 Platform Services Controller를 사용하여 vCenter Server 시스템에서 실행 중인 경우 Platform Services Controller의 호스트 이름 또는 IP 주소

절차

- 1 vSphere Certificate Manager를 시작하고 옵션 6를 선택합니다.
- 2 프롬프트에 응답합니다.

결과

vSphere Certificate Manager가 모든 솔루션 사용자 인증서를 교체합니다.

모든 인증서를 사용자 지정 인증서로 교체(인증서 관리자)

vSphere Certificate Manager 유틸리티를 사용하여 모든 인증서를 사용자 지정 인증서로 교체할 수 있습니다. 프로세스를 시작하기 전에 CSR을 CA로 보내야 합니다. 인증서 관리자를 사용하여 CSR을 생성할 수 있습니다.

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

사용자 지정 인증서를 사용하는 경우 사용자는 사용자 지정 인증서를 사용하여 해당 환경에 추가하는 각 노드를 프로비저닝할 책임이 있습니다. VMCA는 계속 VMCA 서명 인증서를 사용하여 프로비저닝하며, 사용자는 해당 인증서를 교체할 책임이 있습니다. vSphere Certificate Manager 유틸리티를 사용하거나 수동 인증서 교체에 CLI를 사용할 수 있습니다. 인증서는 VECS에 저장됩니다.

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

vSphere Certificate Manager를 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.

다음과 같이 명령줄에서 인증서 관리자 도구를 실행할 수 있습니다.

Windows

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

Linux

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

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.
- 외부 Platform Services Controller가 있는 환경에서 CSR을 생성할 경우 Platform Services Controller의 호스트 이름 또는 IP 주소를 입력하라는 메시지가 표시됩니다.
- 시스템 SSL 인증서에 대한 CSR을 생성하는 경우 certtool.cfg 파일에 저장되는 인증서 속성을 묻습니다. 대부분의 필드에서 기본값을 수락하거나 사이트별 값을 제공할 수 있습니다. 시스템의 FQDN은 필수 항목입니다.

절차

- 1 사용자 환경의 각 시스템에서 vSphere Certificate Manager를 시작하고 옵션 1을 선택합니다.
- 2 메시지가 표시되면 암호 및 Platform Services Controller IP 주소 또는 호스트 이름을 제공합니다.

- 3 옵션 1을 선택하여 CSR을 생성하고 질문에 대답하고 인증서 관리자를 종료합니다.

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

- 4 또한 모든 솔루션 사용자 인증서를 교체하려면 인증서 관리자를 다시 시작합니다.

- 5 옵션 5를 선택합니다.

- 6 메시지가 표시되면 암호 및 Platform Services Controller IP 주소 또는 호스트 이름을 제공합니다.

- 7 옵션 1을 선택하여 CSR을 생성하고 질문에 대답하고 인증서 관리자를 종료합니다.

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

각각의 Platform Services Controller 노드에서 인증서 관리자가 한 개의 인증서와 키 쌍을 생성합니다. 각각의 vCenter Server 노드에서 인증서 관리자가 네 개의 인증서와 키 쌍을 생성합니다.

다음에 수행할 작업

인증서 교체를 수행합니다.

시스템 SSL 인증서를 사용자 지정 인증서로 교체

시스템 SSL 인증서는 모든 관리 노드, Platform Services Controller 및 내장된 배포에서 역방향 프록시 서비스가 사용합니다. 각 시스템마다 다른 서비스와의 보안 통신을 위한 시스템 SSL 인증서가 있어야 합니다. 각 노드의 인증서를 사용자 지정 인증서로 교체할 수 있습니다.

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 [vSphere Certificate Manager를 사용하여 인증서 서명 요청 생성\(사용자 지정 인증서\)](#)을(를) 참조하십시오.
- 2 명시적으로 CSR을 생성하려면 타사 또는 엔터프라이즈 CA에 각 시스템용 인증서를 요청합니다. 인증서는 다음 요구 사항을 충족해야 합니다.
 - 키 크기: 2048비트 이상(PEM 인코딩)
 - CRT 형식
 - x509 버전 3
 - SubjectAltName에는 DNS Name=<machine_FQDN>이 포함되어야 합니다.
 - 다음과 같은 키 사용이 포함되어 있습니다. 디지털 서명, 부인 방지, 키 암호화

VMware 기술 자료 문서 [2112014](#), [Microsoft Certificate Authority](#)에서 vSphere 인증서 가져오기를 참조하십시오.

절차

- 1 vSphere Certificate Manager를 시작하고 옵션 1을 선택합니다.
- 2 옵션 2를 선택하여 인증서 교체를 시작하고 프롬프트에 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 file).
- 다중 노드 배포의 관리 노드에서 명령을 실행할 경우 Platform Services Controller의 IP 주소.

다음에 수행할 작업

사용자 환경에 따라 추가 인증서를 명시적으로 교체해야 할 수 있습니다.

- 회사 정책에 따라 모든 인증서를 교체해야 하는 경우 vmdir 루트 인증서를 교체합니다. [VMware 디렉토리 서비스 인증서 교체](#) 항목을 참조하십시오.
- vSphere 5.x 환경에서 업그레이드하는 경우 vmdir 내에서 vCenter Single Sign-On 인증서를 교체해야 할 수 있습니다. [혼합 모드 환경에서 VMware 디렉토리 서비스 인증서 교체](#) 항목을 참조하십시오.

솔루션 사용자 인증서를 사용자 지정 인증서로 교체

대부분의 회사에서는 외부에서 액세스할 수 있는 서비스의 인증서만 교체하면 됩니다. 하지만 Certificate Manager는 솔루션 사용자 인증서를 교체하는 기능도 지원합니다. 솔루션 사용자는 서비스의 모음(예: vSphere Web Client와 연결된 모든 서비스)입니다. 다중 노드 배포에서는 Platform Services Controller에 있는 시스템 솔루션 사용자 인증서 및 각 관리 노드에 있는 솔루션 사용자 전체 집합을 교체합니다.

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

형식은 다음과 비슷해야 합니다.

```
-----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 [vSphere Certificate Manager를 사용하여 인증서 서명 요청 생성\(사용자 지정 인증서\)](#)을(를) 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 이상(PEM 인코딩)
 - CRT 형식
 - x509 버전 3
 - SubjectAltName에는 DNS Name=<machine_FQDN>이 포함되어야 합니다.
 - 각 솔루션 사용자 인증서마다 Subject가 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, 부인 방지, 키 암호화

VMware 기술 자료 문서 [2112014, Microsoft Certificate Authority](#)에서 vSphere 인증서 가져오기를 참조하십시오.

절차

- 1 vSphere Certificate Manager를 시작하고 옵션 5를 선택합니다.
- 2 옵션 2를 선택하여 인증서 교체를 시작하고 프롬프트에 응답합니다.

vSphere Certificate Manager는 사용자에게 다음 정보를 묻습니다.

- administrator@vsphere.local의 암호
- 시스템 솔루션 사용자의 인증서 및 키.
- Platform Services Controller 노드에서 vSphere Certificate Manager를 실행하는 경우 시스템 솔루션 사용자의 인증서와 키(vpxd.crt와 vpxd.key)를 요청하는 메시지가 나타납니다.
- 관리 노드 또는 내장된 배포에서 vSphere Certificate Manager를 실행할 경우에는 모든 솔루션 사용자의 전체 인증서 및 키(vpxd.crt 및 vpxd.key) 집합을 요청하는 메시지가 나타납니다.

다음에 수행할 작업

vSphere 5.x 환경에서 업그레이드하는 경우 vmmdir 내에서 vCenter Single Sign-On 인증서를 교체해야 할 수 있습니다. 혼합 모드 환경에서 [VMware 디렉토리 서비스 인증서 교체](#)의 내용을 참조하십시오.

수동 인증서 교체

일부 특별한 경우, 예를 들어 한 가지 유형의 솔루션 사용자 인증서만 교체하려는 경우에는 vSphere Certificate Manager 유틸리티를 사용할 수 없습니다. 이 경우 설치에 포함된 CLI를 인증서 교체에 사용할 수 있습니다.

서비스의 시작 및 중지 이해

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

다음 규칙을 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. 호스트와의 문제를 방지하기 위해 루트 인증서를 추가한 후 모든 서비스를 중지했다 즉시 다시 시작하십시오.
- 환경에 관리자가 여러 명 있는 경우 새 루트 인증서를 추가하기 전에 서비스를 중지하고 새 인증서 추가 후 서비스를 다시 시작하십시오.
- 다음 작업을 수행하기 직전에 서비스를 중지하십시오.
 - 시스템 SSL 인증서 또는 모든 솔루션 사용자 인증서를 VECS에서 삭제합니다.
 - vmdir(VMware 디렉토리 서비스)에서 솔루션 사용자 인증서를 교체합니다.

새 VMCA 서명된 인증서로 기존 VMCA 서명된 인증서 교체

VMCA 루트 인증서가 곧 만료되거나 다른 이유로 이를 교체하려는 경우, 새 루트 인증서를 생성하여 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 추가를 참조하십시오.

절차

1 새 VMCA 서명 루트 인증서 생성

certool CLI를 사용하여 새 VMCA 서명 인증서를 생성하고 이를 vmdir에 게시합니다.

2 VMCA 서명된 인증서로 시스템 SSL 인증서 교체

새 VMCA 서명 루트 인증서를 생성한 후에는 환경의 모든 시스템 SSL 인증서를 교체할 수 있습니다.

3 새 VMCA 서명된 인증서로 솔루션 사용자 인증서 교체

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

4 혼합 모드 환경에서 VMware 디렉토리 서비스 인증서 교체

업그레이드 도중 환경에 vCenter Single Sign-On 버전 5.5와 vCenter Single Sign-On 버전 6.x 모두가 임시로 포함될 수 있습니다. 이런 경우 vCenter Single Sign-On 서비스가 실행 중인 노드의 SSL 인증서를 교체한다면 VMware Directory Service SSL 인증서를 교체하기 위한 추가적인 단계를 수행해야 합니다.

새 VMCA 서명 루트 인증서 생성

certool CLI를 사용하여 새 VMCA 서명 인증서를 생성하고 이를 vmdir에 게시합니다.

다중 노드 배포에서는 Platform Services Controller에서 루트 인증서 생성 명령을 실행합니다.

절차

1 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.

서비스 이름은 Windows와 vCenter Server Appliance에서 서로 다릅니다.

Windows

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

vCenter Server Appliance

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

4 (선택 사항) 새 루트 인증서를 vmdir에 게시합니다.

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

이 명령을 실행하면 vmdir의 모든 인스턴스가 즉시 업데이트됩니다. 그렇지 않은 경우에는 모든 인스턴스로 전파하는 데 약간의 시간이 걸릴 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) VMCA 루트 인증서를 나열하여 인증서 저장소에 있는지 확인합니다.

- Platform Services Controller 노드 또는 포함된 설치의 경우:

```
C:\>"C:\Program Files\VMware\VMware vCenter Server\vmcad\"certool --getrootca
```

- 관리 노드의 경우(외부 설치):

```
C:\>"C:\Program Files\VMware\VMware vCenter Server\vmcad\"certool --getrootca --server=<psc-ip-or-fqdn>
```

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.

VECS가 vmdir을 폴링하므로 이 명령은 Platform Services Controller와 관리 노드 모두에서 작동합니다.

```
"C:\Program Files\VMware\VMware vCenter Server\vmafdd\"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. 인증서가 VECS 및 vmdir(VMware 디렉토리 서비스)의 TRUSTED_ROOTS 저장소에 추가됩니다.

```
C:\>"C:\Program Files\VMware\VMware vCenter Server\vmcad\"certool --selfca --config="C:\Program Files\VMware\VMware vCenter Server\vmcad\certool.cfg"
```

Windows에서는 명령이 기본적으로 certool.cfg 파일을 사용하므로 --config는 선택 사항입니다.

VMCA 서명된 인증서로 시스템 SSL 인증서 교체

새 VMCA 서명 루트 인증서를 생성한 후에는 환경의 모든 시스템 SSL 인증서를 교체할 수 있습니다.

각 시스템마다 다른 서비스와의 보안 통신을 위한 시스템 SSL 인증서가 있어야 합니다. 다중 노드 배포에서는 각 노드에서 시스템 SSL 인증서 생성 명령을 실행해야 합니다. --server 매개 변수를 사용하여 외부 Platform Services Controller가 포함된 vCenter Server에서 Platform Services Controller를 가리킵니다.

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.

다음 위치에서 certool.cfg를 찾을 수 있습니다.

운영 체제	경로
Windows	C:\Program Files\VMware\VMware vCenter Server\vmcad
Linux	/usr/lib/vmware-vmca/share/config/

- 2 해당 시스템의 FDQN을 포함하도록 각 시스템의 사용자 지정 구성 파일을 편집합니다.

시스템의 IP 주소에 대해 NSLookup을 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
```

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

서비스 이름은 Windows와 vCenter Server Appliance에서 서로 다릅니다.

Windows

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

vCenter Server Appliance

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

- 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
```

- 모든 서비스를 다시 시작합니다.

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

예제: 시스템 인증서를 VMCA 서명 인증서로 교체

- SSL 인증서에 대한 구성 파일을 만들고 이를 현재 디렉토리에 ssl-config.cfg로 저장합니다.

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

- 시스템 SSL 인증서에 대한 키 쌍을 생성합니다. 이 명령을 각 관리 노드 및 Platform Services Controller 노드에서 실행합니다. --server 옵션은 필요 없습니다.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"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.

- Platform Services Controller 노드 또는 포함된 설치의 경우:

```
C:\>"C:\Program Files\VMware\VMware vCenter Server\vmcad\"certool --gencert --cert=new-vmca-ssl.crt --privkey=ssl-key.priv --config=ssl-config.cfg
```

- vCenter Server의 경우(외부 설치):

```
C:\>"C:\Program Files\VMware\VMware vCenter Server\vmcad\"certool --gencert --cert=new-vmca-ssl.crt --privkey=ssl-key.priv --config=ssl-config.cfg --server=<psc-ip-or-fqdn>
```

new-vmca-ssl.crt 파일이 현재 디렉터리에 생성됩니다.

- 4 (선택 사항) VECS의 내용을 나열합니다.

```
"C:\Program Files\VMware\VMware vCenter Server\vmafdd\"vecs-cli store list
```

- Platform Services Controller에서의 출력:

```
MACHINE_SSL_CERT
TRUSTED_ROOTS
TRUSTED_ROOT_CRLS
machine
```

- vCenter Server에서의 출력:

```
output (on vCenter):
MACHINE_SSL_CERT
TRUSTED_ROOTS
TRUSTED_ROOT_CRLS
machine
vpxd
vpxd-extension
vsphere-webclient
sms
```

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

- Platform Services Controller에서 다음 명령을 실행하여 MACHINE_SSL_CERT 저장소의 시스템 SSL 인증서를 업데이트합니다.

```
C:\>"C:\Program Files\VMware\VMware vCenter Server\vmafdd\"vecs-cli entry delete --store MACHINE_SSL_CERT --alias __MACHINE_CERT
C:\>"C:\Program Files\VMware\VMware vCenter Server\vmafdd\"vecs-cli entry create --store MACHINE_SSL_CERT --alias __MACHINE_CERT --cert new-vmca-ssl.crt --key ssl-key.priv
```

- 각 관리 노드 또는 내장된 배포에서는 다음 명령을 실행하여 MACHINE_SSL_CERT 저장소의 시스템 SSL 인증서를 업데이트합니다. FQDN이 서로 다르므로 각 시스템용 인증서를 개별적으로 업데이트해야 합니다.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store
MACHINE_SSL_CERT --alias __MACHINE_CERT
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store
MACHINE_SSL_CERT --alias __MACHINE_CERT --cert new-vmca-ssl.crt --key ssl-key.priv
```

다음에 수행할 작업

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

다중 노드 배포에서 루트 인증서를 교체한 후에는 외부 Platform Services Controller 노드가 포함된 모든 vCenter Server에서 서비스를 다시 시작해야 합니다.

새 VMCA 서명된 인증서로 솔루션 사용자 인증서 교체

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

각 관리 노드 및 각 Platform Services Controller 노드에서 시스템 솔루션 사용자 인증서를 교체합니다. 다른 솔루션 사용자 인증서는 각 관리 노드에서만 교체합니다. 외부 Platform Services Controller를 사용하는 관리 노드에서 명령을 실행할 때는 --server 매개 변수를 사용하여 Platform Services Controller를 가리킵니다.

참고 대규모 배포의 솔루션 사용자 인증서를 나열할 경우 dir-cli list의 출력에는 모든 노드의 모든 솔루션 사용자가 포함됩니다. 각 호스트의 로컬 시스템 ID를 찾으려면 vmafd-cli get-machine-id --server-name localhost를 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 사용자에게 대한 인증서를 생성하고 직전에 사용자 지정한 구성 파일을 사용하여 전달합니다.

예:

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

- 3 각 솔루션 사용자의 이름을 찾습니다.

```
dir-cli service list
```

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

```
C:\Program Files\VMware\vCenter Server\vmafdd>dir-cli service list
Enter password for administrator@vsphere.local:
1. machine-1d364500-4b45-11e4-96c2-020011c98db3
2. vpzd-1d364500-4b45-11e4-96c2-020011c98db3
3. vpzd-extension-1d364500-4b45-11e4-96c2-020011c98db3
4. vsphere-webclient-1d364500-4b45-11e4-96c2-020011c98db3
```

다중 노드 배포의 솔루션 사용자 인증서를 나열할 경우 `dir-cli`의 출력에는 모든 노드의 모든 솔루션 사용자가 포함됩니다. 각 호스트의 로컬 시스템 ID를 찾으려면 `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.

서비스 이름은 Windows와 vCenter Server Appliance에서 서로 다릅니다.

Windows

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

vCenter Server Appliance

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

- 5 각 솔루션 사용자에게 대해 **vmdir** 및 **VECS**에서 차례로 기존 인증서를 교체합니다.

다음 예는 **vpzd** 서비스에 대한 인증서를 교체하는 방법을 보여 줍니다.

```
dir-cli service update --name <vpzd-xxxx-xxx-7c7b769cd9f4> --cert ./vpzd.crt
vecs-cli entry delete --store vpzd --alias vpzd
vecs-cli entry create --store vpzd --alias vpzd --cert vpzd.crt --key vpzd.priv
```

참고 **vmdir**에서 인증서를 교체하지 않으면 솔루션 사용자가 **vCenter Single Sign-On**에 인증할 수 없습니다.

- 6 모든 서비스를 다시 시작합니다.

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

예제: VMCA 서명 솔루션 사용자 인증서 사용

- 1 각 솔루션 사용자에게 대한 공개/개인 키 쌍을 생성합니다. 여기에는 각 **Platform Services Controller**와 각 관리 노드의 시스템 솔루션 사용자용 쌍과 각 관리 노드의 각 추가 솔루션 사용자(**vpzd**, **vpzd-extension**, **vsphere-webclient**)용 쌍이 포함됩니다.

- a 내장된 배포의 시스템 솔루션 사용자 또는 **Platform Services Controller**의 시스템 솔루션 사용자를 위한 키 쌍을 생성합니다.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=machine-key.priv --pubkey=machine-key.pub
```

- b (선택 사항) 외부 **Platform Services Controller**가 있는 배포의 경우 각 관리 노드에서 시스템 솔루션 사용자를 위한 키 쌍을 생성합니다.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=machine-key.priv --pubkey=machine-key.pub
```

- c 각 관리 노드에서 **vpzd** 솔루션 사용자를 위한 키 쌍을 생성합니다.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=vpzd-key.priv --pubkey=vpzd-key.pub
```

- d 각 관리 노드에서 **vpzd-extension** 솔루션 사용자를 위한 키 쌍을 생성합니다.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=vpzd-extension-key.priv --pubkey=vpzd-extension-key.pub
```

- e 각 관리 노드에서 **vsphere-webclient** 솔루션 사용자를 위한 키 쌍을 생성합니다.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=vsphere-webclient-key.priv --pubkey=vsphere-webclient-key.pub
```

- 2 각 Platform Services Controller 및 각 관리 노드의 시스템 솔루션 사용자 그리고 각 관리 노드의 추가적인 각 솔루션 사용자(vpxd, vpxd-extension, vsphere-webclient)에 대해 새 VMCA 루트 인증서로 서명된 솔루션 사용자 인증서를 생성합니다.

참고 --Name 매개 변수는 고유해야 합니다. vpxd 또는 vpxd-extension과 같은 솔루션 사용자 저장소의 이름을 포함하면 각 인증서가 매핑된 솔루션 사용자를 쉽게 확인할 수 있습니다.

- a Platform Services Controller 노드에서 다음 명령을 실행하여 해당 노드의 시스템 솔루션 사용자에 대한 솔루션 사용자 인증서를 생성합니다.

```
C:\>"C:\Program Files\VMware\VMware vCenter Server\vmcad\"certool --gencert --cert=new-machine.crt --privkey=machine-key.priv --Name=machine
```

- b 각 관리 노드에서 시스템 솔루션 사용자용 인증서를 생성합니다.

```
C:\>"C:\Program Files\VMware\VMware vCenter Server\vmcad\"certool --gencert --cert=new-machine.crt --privkey=machine-key.priv --Name=machine --server=<psc-ip-or-fqdn>
```

- c 각 관리 노드에서 vpxd 솔루션 사용자용 인증서를 생성합니다.

```
C:\>"C:\Program Files\VMware\VMware vCenter Server\vmcad\"certool --gencert --cert=new-vpxd.crt --privkey=vpxd-key.priv --Name=vpxd --server=<psc-ip-or-fqdn>
```

- d 각 관리 노드에서 vpxd-extensions 솔루션 사용자용 인증서를 생성합니다.

```
C:\>"C:\Program Files\VMware\VMware vCenter Server\vmcad\"certool --gencert --cert=new-vpxd-extension.crt --privkey=vpxd-extension-key.priv --Name=vpxd-extension --server=<psc-ip-or-fqdn>
```

- e 다음 명령을 실행하여 각 관리 노드에서 vsphere-webclient 솔루션 사용자용 인증서를 생성합니다.

```
C:\>"C:\Program Files\VMware\VMware vCenter Server\vmcad\"certool --gencert --cert=new-vsphere-webclient.crt --privkey=vsphere-webclient-key.priv --Name=vsphere-webclient --server=<psc-ip-or-fqdn>
```

- 3 VECS의 솔루션 사용자 인증서를 새 솔루션 사용자 인증서로 교체합니다.

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

- a Platform Services Controller 노드에서 다음 명령을 실행하여 시스템 솔루션 사용자 인증서를 교체합니다.

```
C:\>"C:\Program Files\VMware\VMware vCenter Server\vmadfs\"vecs-cli entry delete --store machine --alias machine
C:\>"C:\Program Files\VMware\VMware vCenter Server\vmadfs\"vecs-cli entry create --store machine --alias machine --cert new-machine.crt --key machine-key.priv
```

- b 각 관리 노드에서 시스템 솔루션 사용자 인증서를 교체합니다.

```
C:\>"C:\Program Files\VMware\VMware vCenter Server\vmafdd\"vecs-cli entry delete --store machine --alias machine
C:\>"C:\Program Files\VMware\VMware vCenter Server\vmafdd\"vecs-cli entry create --store machine --alias machine --cert new-machine-vc.crt --key machine-vc-key.priv
```

- c 각 관리 노드에서 vpxd 솔루션 사용자 인증서를 교체합니다.

```
C:\>"C:\Program Files\VMware\VMware vCenter Server\vmafdd\"vecs-cli entry delete --store vpxd --alias vpxd
C:\>"C:\Program Files\VMware\VMware vCenter Server\vmafdd\"vecs-cli entry create --store vpxd --alias vpxd --cert new-vpxd.crt --key vpxd-key.priv
```

- d 각 관리 노드에서 vpxd-extension 솔루션 사용자 인증서를 교체합니다.

```
C:\>"C:\Program Files\VMware\VMware vCenter Server\vmafdd\"vecs-cli entry delete --store vpxd-extension --alias vpxd-extension
C:\>"C:\Program Files\VMware\VMware vCenter Server\vmafdd\"vecs-cli entry create --store vpxd-extension --alias vpxd-extension --cert new-vpxd-extension.crt --key vpxd-extension-key.priv
```

- e 각 관리 노드에서 vsphere-webclient 솔루션 사용자 인증서를 교체합니다.

```
C:\>"C:\Program Files\VMware\VMware vCenter Server\vmafdd\"vecs-cli entry delete --store vsphere-webclient --alias vsphere-webclient
C:\>"C:\Program Files\VMware\VMware vCenter Server\vmafdd\"vecs-cli entry create --store vsphere-webclient --alias vsphere-webclient --cert new-vsphere-webclient.crt --key vsphere-webclient-key.priv
```

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

- a dir-cli service list를 실행하여 각 솔루션 사용자에게 고유한 서비스 ID 접미사를 가져옵니다. 이 명령은 Platform Services Controller 또는 vCenter Server 시스템에서 실행할 수 있습니다.

```
C:\>"C:\Program Files\VMware\VMware vCenter Server\vmafdd\"dir-cli>dir-cli service list
output:
1. machine-29a45d00-60a7-11e4-96ff-00505689639a
2. machine-6fd7f140-60a9-11e4-9e28-005056895a69
3. vpxd-6fd7f140-60a9-11e4-9e28-005056895a69
4. vpxd-extension-6fd7f140-60a9-11e4-9e28-005056895a69
5. vsphere-webclient-6fd7f140-60a9-11e4-9e28-005056895a69
```

참고 대규모 배포의 솔루션 사용자 인증서를 나열할 경우 dir-cli list의 출력에는 모든 노드의 모든 솔루션 사용자가 포함됩니다. 각 호스트의 로컬 시스템 ID를 찾으려면 vmafd-cli get-machine-id --server-name localhost를 실행하십시오. 각 솔루션 사용자 이름에 시스템 ID가 포함되어 있습니다.

- b Platform Services Controller에서 vmdir의 시스템 인증서를 교체합니다. 예를 들어 machine-29a45d00-60a7-11e4-96ff-00505689639a가 Platform Services Controller의 시스템 솔루션 사용자인 경우 다음 명령을 실행하십시오.

```
C:\>"C:\Program Files\VMware\vmCenter Server\vmafdd\"dir-cli service update --name machine-29a45d00-60a7-11e4-96ff-00505689639a --cert new-machine-1.crt
```

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

```
C:\>"C:\Program Files\VMware\vmCenter Server\vmafdd\"dir-cli service update --name machine-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-machine-2.crt
```

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

```
C:\>"C:\Program Files\VMware\vmCenter Server\vmafdd\"dir-cli service update --name vpxd-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vpxd.crt
```

- e 각 관리 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.

```
C:\>"C:\Program Files\VMware\vmCenter Server\vmafdd\"dir-cli service update --name vpxd-extension-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vpxd-extension.crt
```

- f 각 관리 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.

```
C:\>"C:\Program Files\VMware\vmCenter Server\vmafdd\"dir-cli service update --name vsphere-webclient-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vsphere-webclient.crt
```

다음에 수행할 작업

각 Platform Services Controller 노드 및 각 관리 노드에서 모든 서비스를 다시 시작합니다.

혼합 모드 환경에서 VMware 디렉토리 서비스 인증서 교체

업그레이드 도중 환경에 vCenter Single Sign-On 버전 5.5와 vCenter Single Sign-On 버전 6.x 모두가 임시로 포함될 수 있습니다. 이런 경우 vCenter Single Sign-On 서비스가 실행 중인 노드의 SSL 인증서를 교체한다면 VMware Directory Service SSL 인증서를 교체하기 위한 추가적인 단계를 수행해야 합니다.

VMware Directory Service SSL 인증서는 vmdir에서 vCenter Single Sign-On 복제를 수행하는 Platform Services Controller 노드 간에 핸드셰이크를 수행하는 데 사용됩니다.

이 단계는 vSphere 6.0 및 vSphere 6.5 노드를 포함하는 혼합 모드 환경에 필요하지 않습니다. 다음의 경우에만 이 단계가 필요합니다.

- 환경에 vCenter Single Sign-On 5.5와 vCenter Single Sign-On 6.x 서비스가 모두 포함되어 있습니다.
- vCenter Single Sign-On 서비스가 vmdir 데이터를 복제하도록 설정되었습니다.
- vCenter Single Sign-On 6.x 서비스가 실행되는 노드에 대해 기본 VMCA 서명 인증서를 사용자 지정 인증서로 교체할 계획입니다.

참고 서비스를 다시 시작하기 전에 전체 환경을 업그레이드하는 것이 가장 좋습니다. VMware Directory Service 인증서 교체는 일반적으로 권장되지 않습니다.

절차

- 1 vCenter Single Sign-On 6.x 서비스가 실행되는 노드에서 vmdird SSL 인증서 및 키를 교체합니다.
[VMware 디렉토리 서비스 인증서 교체](#)의 내용을 참조하십시오.
- 2 vCenter Single Sign-On 5.5 서비스가 실행되는 노드에서 vCenter Single Sign-On 6.x 서비스가 인식되도록 환경을 설정합니다.
 - a 모든 파일 C:\ProgramData\VMware\CIS\cfg\vmdird를 백업합니다.
 - b 6.x 노드에서 vmdircert.pem 파일의 사본을 만들고 이름을 <sso_node2.domain.com>.pem 으로 바꿉니다. 여기서 <sso_node2.domain.com>은 6.x 노드의 FQDN입니다.
 - c 이름을 바꾼 인증서를 C:\ProgramData\VMware\CIS\cfg\vmdird에 복사하여 기존 복제 인증서를 교체합니다.
- 3 인증서를 교체한 모든 시스템에서 VMware 디렉토리 서비스를 다시 시작합니다.
 vSphere Web Client에서 또는 service-control 명령을 사용하여 서비스를 다시 시작할 수 있습니다.

중간 CA(인증 기관)로 VMCA 사용

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. 이는 타사 CA 서명 인증서의 보안과 자동화된 인증서 관리의 편의성을 결합하는 접근 방식입니다.

절차

1 루트 인증서 교체(중간 CA)

VMCA 인증서를 사용자 지정 인증서로 교체하는 첫 번째 단계에서는 CSR을 생성하고 VMCA에 루트 인증서로 반환된 인증서를 추가합니다.

2 시스템 SSL 인증서 교체(중간 CA)

CA에서 서명된 인증서를 받아 VMCA 루트 인증서로 만든 후에는, 모든 시스템 SSL 인증서를 교체할 수 있습니다.

3 솔루션 사용자 인증서 교체(중간 CA)

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

4 VMware 디렉토리 서비스 인증서 교체

새 VMCA 루트 인증서를 사용하기로 결정하고 환경을 프로비저닝할 때 사용하던 VMCA 루트 인증서를 게시 취소한 경우, 시스템 SSL 인증서, 솔루션 사용자 인증서 및 일부 내부 서비스용 인증서를 교체해야 합니다.

5 혼합 모드 환경에서 VMware 디렉토리 서비스 인증서 교체

업그레이드 도중 환경에 vCenter Single Sign-On 버전 5.5와 vCenter Single Sign-On 버전 6.x 모두가 임시로 포함될 수 있습니다. 이런 경우 vCenter Single Sign-On 서비스가 실행 중인 노드의 SSL 인증서를 교체한다면 VMware Directory Service SSL 인증서를 교체하기 위한 추가적인 단계를 수행해야 합니다.

루트 인증서 교체(중간 CA)

VMCA 인증서를 사용자 지정 인증서로 교체하는 첫 번째 단계에서는 CSR을 생성하고 VMCA에 루트 인증서로 반환된 인증서를 추가합니다.

서명을 위해 보내는 인증서는 다음 요구 사항을 충족해야 합니다.

- 키 크기: 2048비트 이상
- PEM 형식. VMware는 PKCS8 및 PKCS1(RSA 키)을 지원합니다. 키가 VECS에 추가되면 추가된 키가 PKCS8로 변환됩니다.
- x509 버전 3
- 사용자 지정 인증서를 사용하는 경우 CA 확장을 루트 인증서에 대해 true로 설정해야 하며 인증서 서명이 요구 사항 목록에 있어야 합니다.
- CRL 서명을 사용하도록 설정해야 합니다.
- 고급 키 사용에 클라이언트 인증 또는 서버 인증을 포함하면 안 됩니다.
- 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 2112009, Creating a Microsoft Certificate Authority Template for SSL certificate creation in vSphere 6.0(vSphere 6.0에서 SSL 인증서 생성에 사용할 Microsoft CA(인증 기관) 템플릿 생성)을 참조하십시오.

VMCA는 사용자가 루트 인증서를 교체할 때 다음의 인증서 특성을 확인합니다.

- 키 크기 2048비트 이상
- 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.crt와 같은 이름으로 파일을 저장합니다.

이렇게 하려면 PEM 형식의 모든 CA 인증서를 하나의 파일로 복사합니다. VMCA 인증서 루트부터 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.

서비스 이름은 Windows와 vCenter Server Appliance에서 서로 다릅니다.

Windows

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

vCenter Server Appliance

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

- 4 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.

예:

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

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.

```
C:\>"C:\Program Files\VMware\VMware Server\vmcad\certool" --rootca --cert=C:\custom-  
certs\root.pem --privkey=C:\custom-certs\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. 이렇게 할 경우 다음의 내부 인증서를 새로 고쳐야 합니다.

- vCenter Single Sign-On 서명 인증서를 교체합니다. [보안 토큰 서비스 인증서 새로 고침](#)을 참조하십시오.
- VMware 디렉토리 서비스 인증서를 교체합니다. [VMware 디렉토리 서비스 인증서 교체](#)를 참조하십시오.

시스템 SSL 인증서 교체(중간 CA)

CA에서 서명된 인증서를 받아 VMCA 루트 인증서로 만든 후에는, 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. 다중 노드 배포에서는 각 노드에서 시스템 SSL 인증서 생성 명령을 실행해야 합니다. `--server` 매개 변수를 사용하여 외부 Platform Services Controller가 포함된 vCenter Server에서 Platform Services Controller를 가리킵니다.

사전 요구 사항

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

절차

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

다음 위치에서 `certtool.cfg`를 찾을 수 있습니다.

Windows

`C:\Program Files\VMware\vCenter Server\vmcad`

Linux

`/usr/lib/vmware-vmca/share/config/`

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

시스템의 IP 주소에 대해 NSLookup을 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:

```
certtool --genkey --privkey=machine1.priv --pubkey=machine1.pub
certtool --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.

서비스 이름은 Windows와 vCenter Server Appliance에서 서로 다릅니다.

Windows

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

vCenter Server Appliance

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

- 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.cfg로 저장합니다.

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

- 2 시스템 SSL 인증서에 대한 키 쌍을 생성합니다. 이 명령을 각 관리 노드 및 Platform Services Controller 노드에서 실행합니다. --server 옵션은 필요 없습니다.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"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.

- Platform Services Controller 노드 또는 포함된 설치의 경우:

```
C:\>"C:\Program Files\VMware\VMware vCenter Server\vmcad\"certool --gencert --cert=new-vmca-ssl.crt --privkey=ssl-key.priv --config=ssl-config.cfg
```

- vCenter Server의 경우(외부 설치):

```
C:\>"C:\Program Files\VMware\VMware vCenter Server\vmcad\"certool --gencert --cert=new-vmca-ssl.crt --privkey=ssl-key.priv --config=ssl-config.cfg --server=<psc-ip-or-fqdn>
```

new-vmca-ssl.crt 파일이 현재 디렉터리에 생성됩니다.

- 4 (선택 사항) VECS의 내용을 나열합니다.

```
"C:\Program Files\VMware\VMware vCenter Server\vmaddd\"vecs-cli store list
```

- Platform Services Controller에서의 출력:

```
MACHINE_SSL_CERT
TRUSTED_ROOTS
TRUSTED_ROOT_CRLS
machine
```

- vCenter Server에서의 출력:

```
output (on vCenter):
MACHINE_SSL_CERT
TRUSTED_ROOTS
TRUSTED_ROOT_CRLS
machine
vpxd
vpxd-extension
vsphere-webclient
sms
```

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

- Platform Services Controller에서 다음 명령을 실행하여 MACHINE_SSL_CERT 저장소의 시스템 SSL 인증서를 업데이트합니다.

```
C:\>"C:\Program Files\VMware\VMware vCenter Server\vmaddd\"vecs-cli entry delete --store MACHINE_SSL_CERT --alias __MACHINE_CERT
C:\>"C:\Program Files\VMware\VMware vCenter Server\vmaddd\"vecs-cli entry create --store MACHINE_SSL_CERT --alias __MACHINE_CERT --cert new-vmca-ssl.crt --key ssl-key.priv
```

- 각 관리 노드 또는 내장된 배포에서는 다음 명령을 실행하여 MACHINE_SSL_CERT 저장소의 시스템 SSL 인증서를 업데이트합니다. FQDN이 서로 다르므로 각 시스템용 인증서를 개별적으로 업데이트해야 합니다.

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store MACHINE_SSL_CERT --alias __MACHINE_CERT
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store MACHINE_SSL_CERT --alias __MACHINE_CERT --cert new-vmca-ssl.crt --key ssl-key.priv
```

다음에 수행할 작업

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

다중 노드 배포에서 루트 인증서를 교체한 후에는 외부 Platform Services Controller 노드가 포함된 모든 vCenter Server에서 서비스를 다시 시작해야 합니다.

솔루션 사용자 인증서 교체(중간 CA)

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

각 관리 노드 및 각 Platform Services Controller 노드에서 시스템 솔루션 사용자 인증서를 교체합니다. 다른 솔루션 사용자 인증서는 각 관리 노드에서만 교체합니다. 외부 Platform Services Controller를 사용하는 관리 노드에서 명령을 실행할 때는 --server 매개 변수를 사용하여 Platform Services Controller를 가리킵니다.

참고 대규모 배포의 솔루션 사용자 인증서를 나열할 경우 dir-cli list의 출력에는 모든 노드의 모든 솔루션 사용자가 포함됩니다. 각 호스트의 로컬 시스템 ID를 찾으려면 vmafd-cli get-machine-id --server-name localhost를 실행하십시오. 각 솔루션 사용자 이름에 시스템 ID가 포함되어 있습니다.

사전 요구 사항

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

절차

- 1 certtool.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 사용자에게 대한 인증서를 생성하고 직전에 사용자 지정한 구성 파일을 사용하여 전달합니다.

예:

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

- 3 각 솔루션 사용자의 이름을 찾습니다.

```
dir-cli service list
```

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

```
C:\Program Files\VMware\vCenter Server\vmafdd>dir-cli service list
Enter password for administrator@vsphere.local:
1. machine-1d364500-4b45-11e4-96c2-020011c98db3
2. vpzd-1d364500-4b45-11e4-96c2-020011c98db3
3. vpzd-extension-1d364500-4b45-11e4-96c2-020011c98db3
4. vsphere-webclient-1d364500-4b45-11e4-96c2-020011c98db3
```

다중 노드 배포의 솔루션 사용자 인증서를 나열할 경우 `dir-cli`의 출력에는 모든 노드의 모든 솔루션 사용자가 포함됩니다. 각 호스트의 로컬 시스템 ID를 찾으려면 `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.

서비스 이름은 Windows와 vCenter Server Appliance에서 서로 다릅니다.

Windows

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

vCenter Server Appliance

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


5 vmdir과 VECS에서 차례로 기존 인증서를 교체합니다.

솔루션 사용자의 경우 이 순서대로 인증서를 추가해야 합니다. 예:

```
dir-cli service update --name <vpzd-xxxx-xxx-7c7b769cd9f4> --cert ./vpzd.crt
vecs-cli entry delete --store vpzd --alias vpzd
vecs-cli entry create --store vpzd --alias vpzd --cert vpzd.crt --key vpzd.priv
```

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 각 솔루션 사용자에 대한 공개/개인 키 쌍을 생성합니다. 여기에는 각 Platform Services Controller와 각 관리 노드의 시스템 솔루션 사용자용 쌍과 각 관리 노드의 각 추가 솔루션 사용자(vpzd, vpzd-extension, vsphere-webclient)용 쌍이 포함됩니다.

- a 내장된 배포의 시스템 솔루션 사용자 또는 Platform Services Controller의 시스템 솔루션 사용자를 위한 키 쌍을 생성합니다.

```
C:\>"C:\Program Files\VMware\VCenter Server\vmcad\"certool --genkey --privkey=machine-key.priv --pubkey=machine-key.pub
```

- b (선택 사항) 외부 Platform Services Controller가 있는 배포의 경우 각 관리 노드에서 시스템 솔루션 사용자를 위한 키 쌍을 생성합니다.

```
C:\>"C:\Program Files\VMware\VCenter Server\vmcad\"certool --genkey --privkey=machine-key.priv --pubkey=machine-key.pub
```

- c 각 관리 노드에서 vpzd 솔루션 사용자를 위한 키 쌍을 생성합니다.

```
C:\>"C:\Program Files\VMware\VCenter Server\vmcad\"certool --genkey --privkey=vpzd-key.priv --pubkey=vpzd-key.pub
```

- d 각 관리 노드에서 vpzd-extension 솔루션 사용자를 위한 키 쌍을 생성합니다.

```
C:\>"C:\Program Files\VMware\VCenter Server\vmcad\"certool --genkey --privkey=vpzd-extension-key.priv --pubkey=vpzd-extension-key.pub
```

- e 각 관리 노드에서 vsphere-webclient 솔루션 사용자를 위한 키 쌍을 생성합니다.

```
C:\>"C:\Program Files\VMware\VCenter Server\vmcad\"certool --genkey --privkey=vsphere-webclient-key.priv --pubkey=vsphere-webclient-key.pub
```

- 2 각 Platform Services Controller 및 각 관리 노드의 시스템 솔루션 사용자 그리고 각 관리 노드의 추가적인 각 솔루션 사용자(vpxd, vpxd-extension, vsphere-webclient)에 대해 새 VMCA 루트 인증서로 서명된 솔루션 사용자 인증서를 생성합니다.

참고 --Name 매개 변수는 고유해야 합니다. vpxd 또는 vpxd-extension과 같은 솔루션 사용자 저장소의 이름을 포함하면 각 인증서가 매핑된 솔루션 사용자를 쉽게 확인할 수 있습니다.

- a Platform Services Controller 노드에서 다음 명령을 실행하여 해당 노드의 시스템 솔루션 사용자에 대한 솔루션 사용자 인증서를 생성합니다.

```
C:\>"C:\Program Files\VMware\VCenter Server\vmcad\"certool --gencert --cert=new-machine.crt --privkey=machine-key.priv --Name=machine
```

- b 각 관리 노드에서 시스템 솔루션 사용자용 인증서를 생성합니다.

```
C:\>"C:\Program Files\VMware\VCenter Server\vmcad\"certool --gencert --cert=new-machine.crt --privkey=machine-key.priv --Name=machine --server=<psc-ip-or-fqdn>
```

- c 각 관리 노드에서 vpxd 솔루션 사용자용 인증서를 생성합니다.

```
C:\>"C:\Program Files\VMware\VCenter Server\vmcad\"certool --gencert --cert=new-vpxd.crt --privkey=vpxd-key.priv --Name=vpxd --server=<psc-ip-or-fqdn>
```

- d 각 관리 노드에서 vpxd-extensions 솔루션 사용자용 인증서를 생성합니다.

```
C:\>"C:\Program Files\VMware\VCenter Server\vmcad\"certool --gencert --cert=new-vpxd-extension.crt --privkey=vpxd-extension-key.priv --Name=vpxd-extension --server=<psc-ip-or-fqdn>
```

- e 다음 명령을 실행하여 각 관리 노드에서 vsphere-webclient 솔루션 사용자용 인증서를 생성합니다.

```
C:\>"C:\Program Files\VMware\VCenter Server\vmcad\"certool --gencert --cert=new-vsphere-webclient.crt --privkey=vsphere-webclient-key.priv --Name=vsphere-webclient --server=<psc-ip-or-fqdn>
```

- 3 VECS의 솔루션 사용자 인증서를 새 솔루션 사용자 인증서로 교체합니다.

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

- a Platform Services Controller 노드에서 다음 명령을 실행하여 시스템 솔루션 사용자 인증서를 교체합니다.

```
C:\>"C:\Program Files\VMware\VCenter Server\vmaddd\"vecs-cli entry delete --store machine --alias machine
C:\>"C:\Program Files\VMware\VCenter Server\vmaddd\"vecs-cli entry create --store machine --alias machine --cert new-machine.crt --key machine-key.priv
```

- b 각 관리 노드에서 시스템 솔루션 사용자 인증서를 교체합니다.

```
C:\>"C:\Program Files\VMware\VMware vCenter Server\vmadfs\vecs-cli entry delete --store machine --alias machine
C:\>"C:\Program Files\VMware\VMware vCenter Server\vmadfs\vecs-cli entry create --store machine --alias machine --cert new-machine-vc.crt --key machine-vc-key.priv
```

- c 각 관리 노드에서 vpxd 솔루션 사용자 인증서를 교체합니다.

```
C:\>"C:\Program Files\VMware\VMware vCenter Server\vmadfs\vecs-cli entry delete --store vpxd --alias vpxd
C:\>"C:\Program Files\VMware\VMware vCenter Server\vmadfs\vecs-cli entry create --store vpxd --alias vpxd --cert new-vpxd.crt --key vpxd-key.priv
```

- d 각 관리 노드에서 vpxd-extension 솔루션 사용자 인증서를 교체합니다.

```
C:\>"C:\Program Files\VMware\VMware vCenter Server\vmadfs\vecs-cli entry delete --store vpxd-extension --alias vpxd-extension
C:\>"C:\Program Files\VMware\VMware vCenter Server\vmadfs\vecs-cli entry create --store vpxd-extension --alias vpxd-extension --cert new-vpxd-extension.crt --key vpxd-extension-key.priv
```

- e 각 관리 노드에서 vsphere-webclient 솔루션 사용자 인증서를 교체합니다.

```
C:\>"C:\Program Files\VMware\VMware vCenter Server\vmadfs\vecs-cli entry delete --store vsphere-webclient --alias vsphere-webclient
C:\>"C:\Program Files\VMware\VMware vCenter Server\vmadfs\vecs-cli entry create --store vsphere-webclient --alias vsphere-webclient --cert new-vsphere-webclient.crt --key vsphere-webclient-key.priv
```

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

- a dir-cli service list를 실행하여 각 솔루션 사용자에게 고유한 서비스 ID 접미사를 가져옵니다. 이 명령은 Platform Services Controller 또는 vCenter Server 시스템에서 실행할 수 있습니다.

```
C:\>"C:\Program Files\VMware\VMware vCenter Server\vmadfs\dir-cli>dir-cli service list
output:
1. machine-29a45d00-60a7-11e4-96ff-00505689639a
2. machine-6fd7f140-60a9-11e4-9e28-005056895a69
3. vpxd-6fd7f140-60a9-11e4-9e28-005056895a69
4. vpxd-extension-6fd7f140-60a9-11e4-9e28-005056895a69
5. vsphere-webclient-6fd7f140-60a9-11e4-9e28-005056895a69
```

참고 대규모 배포의 솔루션 사용자 인증서를 나열할 경우 dir-cli list의 출력에는 모든 노드의 모든 솔루션 사용자가 포함됩니다. 각 호스트의 로컬 시스템 ID를 찾으려면 vmadfs-cli get-machine-id --server-name localhost를 실행하십시오. 각 솔루션 사용자 이름에 시스템 ID가 포함되어 있습니다.

- b Platform Services Controller에서 vmdir의 시스템 인증서를 교체합니다. 예를 들어 machine-29a45d00-60a7-11e4-96ff-00505689639a가 Platform Services Controller의 시스템 솔루션 사용자인 경우 다음 명령을 실행하십시오.

```
C:\>"C:\Program Files\VMware\vmCenter Server\vmafdd\"dir-cli service update --name machine-29a45d00-60a7-11e4-96ff-00505689639a --cert new-machine-1.crt
```

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

```
C:\>"C:\Program Files\VMware\vmCenter Server\vmafdd\"dir-cli service update --name machine-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-machine-2.crt
```

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

```
C:\>"C:\Program Files\VMware\vmCenter Server\vmafdd\"dir-cli service update --name vpxd-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vpxd.crt
```

- e 각 관리 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.

```
C:\>"C:\Program Files\VMware\vmCenter Server\vmafdd\"dir-cli service update --name vpxd-extension-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vpxd-extension.crt
```

- f 각 관리 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.

```
C:\>"C:\Program Files\VMware\vmCenter Server\vmafdd\"dir-cli service update --name vsphere-webclient-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vsphere-webclient.crt
```

VMware 디렉토리 서비스 인증서 교체

새 VMCA 루트 인증서를 사용하기로 결정하고 환경을 프로비저닝할 때 사용하던 VMCA 루트 인증서를 게시 취소한 경우, 시스템 SSL 인증서, 솔루션 사용자 인증서 및 일부 내부 서비스용 인증서를 교체해야 합니다.

VMCA 루트 인증서를 게시 취소하는 경우 vCenter Single Sign-On이 사용하는 SSL 서명 인증서를 교체해야 합니다. [보안 토큰 서비스 인증서 새로 고침](#)을 참조하십시오. vmdir(VMware 디렉토리 서비스) 인증서도 교체해야 합니다.

사전 요구 사항

타사 또는 엔터프라이즈 CA에 vmdir용 인증서를 요청합니다.

절차

- 1 vmdir을 중지합니다.

Linux

```
service-control --stop vmdird
```

Windows

```
service-control --stop VMWareDirectoryService
```

- 2 생성한 인증서 및 키를 vmdir 위치에 복사합니다.

Linux

```
cp vmdir.crt /usr/lib/vmware-vmdir/share/config/vmdircert.pem
cp vmdir.priv /usr/lib/vmware-vmdir/share/config/vmdirkey.pem
```

Windows

```
copy vmdir.crt C:\programdata\vmware\vCenterServer\cfg\vmdird\vmdircert.pem
copy vmdir.priv C:\programdata\vmware\vCenterServer\cfg\vmdird\vmdirkey.pem
```

- 3 vSphere Web Client에서 또는 service-control 명령을 사용하여 vmdir을 다시 시작합니다.

Linux

```
service-control --start vmdird
```

Windows

```
service-control --start VMWareDirectoryService
```

혼합 모드 환경에서 VMware 디렉토리 서비스 인증서 교체

업그레이드 도중 환경에 vCenter Single Sign-On 버전 5.5와 vCenter Single Sign-On 버전 6.x 모두가 임시로 포함될 수 있습니다. 이런 경우 vCenter Single Sign-On 서비스가 실행 중인 노드의 SSL 인증서를 교체한다면 VMware Directory Service SSL 인증서를 교체하기 위한 추가적인 단계를 수행해야 합니다.

VMware Directory Service SSL 인증서는 vmdir에서 vCenter Single Sign-On 복제를 수행하는 Platform Services Controller 노드 간에 핸드셰이크를 수행하는 데 사용됩니다.

이 단계는 vSphere 6.0 및 vSphere 6.5 노드를 포함하는 혼합 모드 환경에 필요하지 않습니다. 다음의 경우에만 이 단계가 필요합니다.

- 환경에 vCenter Single Sign-On 5.5와 vCenter Single Sign-On 6.x 서비스가 모두 포함되어 있습니다.

- vCenter Single Sign-On 서비스가 vmdir 데이터를 복제하도록 설정되었습니다.
- vCenter Single Sign-On 6.x 서비스가 실행되는 노드에 대해 기본 VMCA 서명 인증서를 사용자 지정 인증서로 교체할 계획입니다.

참고 서비스를 다시 시작하기 전에 전체 환경을 업그레이드하는 것이 가장 좋습니다. VMware Directory Service 인증서 교체는 일반적으로 권장되지 않습니다.

절차

- 1 vCenter Single Sign-On 6.x 서비스가 실행되는 노드에서 vmdird SSL 인증서 및 키를 교체합니다.
VMware 디렉토리 서비스 인증서 교체의 내용을 참조하십시오.
- 2 vCenter Single Sign-On 5.5 서비스가 실행되는 노드에서 vCenter Single Sign-On 6.x 서비스가 인식되도록 환경을 설정합니다.
 - a 모든 파일 C:\ProgramData\VMware\CIS\cfg\vmdird을 백업합니다.
 - b 6.x 노드에서 vmdircert.pem 파일의 사본을 만들고 이름을 <sso_node2.domain.com>.pem으로 바꿉니다. 여기서 <sso_node2.domain.com>은 6.x 노드의 FQDN입니다.
 - c 이름을 바꾼 인증서를 C:\ProgramData\VMware\CIS\cfg\vmdird에 복사하여 기존 복제 인증서를 교체합니다.
- 3 인증서를 교체한 모든 시스템에서 VMware 디렉토리 서비스를 다시 시작합니다.
 vSphere Web Client에서 또는 service-control 명령을 사용하여 서비스를 다시 시작할 수 있습니다.

vSphere와 함께 타사 인증서 사용

회사 정책에서 요구하는 경우 vSphere에서 사용되는 모든 인증서를 타사 CA 서명 인증서로 교체할 수 있습니다. 이렇게 하면 VMCA가 인증서 체인에 포함되지 않으며 모든 vCenter 인증서를 VECS에 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 인증하는 용도로만 사용됩니다.

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

절차

- 1 **인증서 요청 및 사용자 지정 루트 인증서 가져오기**
 회사 정책에서 중간 CA를 허용하지 않는 경우에는 VMCA가 인증서를 생성할 수 없습니다. 엔터프라이즈 또는 타사 CA의 사용자 지정 인증서를 사용하십시오.

2 시스템 SSL 인증서를 사용자 지정 인증서로 교체

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

3 솔루션 사용자 인증서를 사용자 지정 인증서로 교체

시스템 SSL 인증서를 교체한 후에는 VMCA 서명 솔루션 사용자 인증서를 타사 또는 엔터프라이즈 인증서로 교체할 수 있습니다.

4 VMware 디렉토리 서비스 인증서 교체

새 VMCA 루트 인증서를 사용하기로 결정하고 환경을 프로비저닝할 때 사용하던 VMCA 루트 인증서를 게시 취소한 경우, 시스템 SSL 인증서, 솔루션 사용자 인증서 및 일부 내부 서비스용 인증서를 교체해야 합니다.

5 혼합 모드 환경에서 VMware 디렉토리 서비스 인증서 교체

업그레이드 도중 환경에 vCenter Single Sign-On 버전 5.5와 vCenter Single Sign-On 버전 6.x 모두가 임시로 포함될 수 있습니다. 이런 경우 vCenter Single Sign-On 서비스가 실행 중인 노드의 SSL 인증서를 교체한다면 VMware Directory Service SSL 인증서를 교체하기 위한 추가적인 단계를 수행해야 합니다.

인증서 요청 및 사용자 지정 루트 인증서 가져오기

회사 정책에서 중간 CA를 허용하지 않는 경우에는 VMCA가 인증서를 생성할 수 없습니다. 엔터프라이즈 또는 타사 CA의 사용자 지정 인증서를 사용하십시오.

사전 요구 사항

인증서는 다음 요구 사항을 충족해야 합니다.

- 키 크기: 2048비트 이상(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, 부인 방지, 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).

절차

1 다음 인증서에 대한 CSR을 엔터프라이즈 또는 타사 인증서 제공자에 보냅니다.

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

일반적으로 신뢰할 수 있는 체인에 대한 PEM 파일과 각 Platform Services Controller 또는 관리 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 확인하여 시스템 SSL 인증서와 일치하는지 확인합니다.

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

서비스 이름은 Windows와 vCenter Server Appliance에서 서로 다릅니다.

Windows

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

vCenter Server Appliance

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

4 타사 CA의 서명 인증서인 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 필요한 경우 원래 VMCA 루트 인증서를 인증서 저장소에서 제거할 수 있습니다. 이렇게 할 경우 다음의 내부 인증서를 새로 고쳐야 합니다.

- vCenter Single Sign-On 서명 인증서를 교체합니다. [보안 토큰 서비스 인증서 새로 고침](#)을 참조하십시오.
- VMware 디렉토리 서비스 인증서를 교체합니다. [VMware 디렉토리 서비스 인증서 교체](#)를 참조하십시오.

시스템 SSL 인증서를 사용자 지정 인증서로 교체

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

각 시스템마다 다른 서비스와의 보안 통신을 위한 시스템 SSL 인증서가 있어야 합니다. 다중 노드 배포에서는 각 노드에서 시스템 SSL 인증서 생성 명령을 실행해야 합니다. --server 매개 변수를 사용하여 외부 Platform Services Controller가 포함된 vCenter Server에서 Platform Services Controller를 가리킵니다.

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)
- 다중 노드 배포 환경에서 외부 Platform Services Controller가 포함된 vCenter Server에 대해 명령을 실행하는 경우 Platform Services Controller의 IP 주소

사전 요구 사항

타사 또는 엔터프라이즈 인증 기관에서 각 시스템에 대한 인증서를 받은 상태여야 합니다.

- 키 크기: 2048비트 이상(PEM 인코딩)
- CRT 형식
- x509 버전 3
- SubjectAltName에는 DNS Name=<machine_FQDN>이 포함되어야 합니다.
- 다음과 같은 키 사용이 포함되어 있습니다. 디지털 서명, 부인 방지, 키 암호화

절차

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

서비스 이름은 Windows와 vCenter Server Appliance에서 서로 다릅니다.

Windows

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

vCenter Server Appliance

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

- 2 각 노드에 로그인하여 CA에서 받은 새 시스템 인증서를 VECS에 추가합니다.

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

```
vecs-cli entry delete --store MACHINE_SSL_CERT --alias __MACHINE_CERT
vecs-cli entry create --store MACHINE_SSL_CERT --alias __MACHINE_CERT --cert <cert-file-path>
--key <key-file-path>
```

- 3 모든 서비스를 다시 시작합니다.

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

예제: 시스템 SSL 인증서를 사용자 지정 인증서로 교체

같은 방법으로 각 노드에서 시스템 SSL 인증서를 교체할 수 있습니다.

- 1 먼저 VECS에서 기존 인증서를 삭제합니다.

```
"C:\Program Files\VMware\VMware Server\vmaddd\"vecs-cli entry delete --store
MACHINE_SSL_CERT --alias __MACHINE_CERT
```

- 2 그런 다음 교체 인증서를 추가합니다.

```
"C:\Program Files\VMware\VMware Server\vmaddd\"vecs-cli entry create --store
MACHINE_SSL_CERT --alias __MACHINE_CERT --cert E:\custom-certs\ms-ca\signed-ssl\custom-wl-
vim-cat-dhcp-094.eng.vmware.com.crt --key E:\custom-certs\ms-ca\signed-ssl\custom-x3-vim-
cat-dhcp-1128.vmware.com.priv
```

다음에 수행할 작업

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

다중 노드 배포에서 루트 인증서를 교체한 후에는 외부 Platform Services Controller 노드가 포함된 모든 vCenter Server에서 서비스를 다시 시작해야 합니다.

솔루션 사용자 인증서를 사용자 지정 인증서로 교체

시스템 SSL 인증서를 교체한 후에는 VMCA 서명 솔루션 사용자 인증서를 타사 또는 엔터프라이즈 인증서로 교체할 수 있습니다.

솔루션 사용자는 vCenter Single Sign-On에 인증할 때만 인증서를 사용합니다. 인증서가 유효하면 vCenter Single Sign-On이 SAML 토큰을 솔루션 사용자에게 할당하며 솔루션 사용자는 SAML 토큰을 사용하여 다른 vCenter 구성 요소에 인증합니다.

환경에서 솔루션 사용자 인증서의 교체가 필요한지 고려하십시오. 솔루션 사용자는 프록시 서버 뒤에 있고 시스템 SSL 인증서가 SSL 트래픽의 보안에 사용되므로, 솔루션 사용자 인증서는 보안의 우려가 적을 수 있습니다.

각 관리 노드 및 각 Platform Services Controller 노드에서 시스템 솔루션 사용자 인증서를 교체합니다. 다른 솔루션 사용자 인증서는 각 관리 노드에서만 교체합니다. 외부 Platform Services Controller를 사용하는 관리 노드에서 명령을 실행할 때는 --server 매개 변수를 사용하여 Platform Services Controller를 가리킵니다.

참고 대규모 배포의 솔루션 사용자 인증서를 나열할 경우 dir-cli list의 출력에는 모든 노드의 모든 솔루션 사용자가 포함됩니다. 각 호스트의 로컬 시스템 ID를 찾으려면 vmafd-cli get-machine-id --server-name localhost를 실행하십시오. 각 솔루션 사용자 이름에 시스템 ID가 포함되어 있습니다.

사전 요구 사항

- 키 크기: 2048비트 이상(PEM 인코딩)
- CRT 형식
- x509 버전 3
- SubjectAltName에는 DNS Name=<machine_FQDN>이 포함되어야 합니다.
- 각 솔루션 사용자 인증서마다 Subject가 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, 부인 방지, 키 암호화

절차

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

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

2 각 솔루션 사용자의 이름을 찾습니다.

```
dir-cli service list
```

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

```
C:\Program Files\VMware\vCenter Server\vmafdd>dir-cli service list
Enter password for administrator@vsphere.local:
1. machine-1d364500-4b45-11e4-96c2-020011c98db3
2. vpxd-1d364500-4b45-11e4-96c2-020011c98db3
3. vpxd-extension-1d364500-4b45-11e4-96c2-020011c98db3
4. vsphere-webclient-1d364500-4b45-11e4-96c2-020011c98db3
```

다중 노드 배포의 솔루션 사용자 인증서를 나열할 경우 dir-cli 의 출력에는 모든 노드의 모든 솔루션 사용자가 포함됩니다. 각 호스트의 로컬 시스템 ID를 찾으려면 vmafd-cli get-machine-id --server-name localhost를 실행하십시오. 각 솔루션 사용자 이름에 시스템 ID가 포함되어 있습니다.

3 각 솔루션 사용자에 대해 VECS 및 vmdir에서 차례로 기존 인증서를 교체합니다.

이 순서로 인증서를 추가해야 합니다.

```
vecs-cli entry delete --store vpxd --alias vpxd
vecs-cli entry create --store vpxd --alias vpxd --cert vpxd.crt --key vpxd.priv
dir-cli service update --name <vpxd-xxxx-xxx-xxxxxx> --cert vpxd.crt
```

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

4 모든 서비스를 다시 시작합니다.

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

VMware 디렉토리 서비스 인증서 교체

새 VMCA 루트 인증서를 사용하기로 결정하고 환경을 프로비저닝할 때 사용하던 VMCA 루트 인증서를 게시 취소한 경우, 시스템 SSL 인증서, 솔루션 사용자 인증서 및 일부 내부 서비스용 인증서를 교체해야 합니다.

VMCA 루트 인증서를 게시 취소하는 경우 vCenter Single Sign-On이 사용하는 SSL 서명 인증서를 교체해야 합니다. **보안 토큰 서비스 인증서 새로 고침**을 참조하십시오. vmdir(VMware 디렉토리 서비스) 인증서도 교체해야 합니다.

사전 요구 사항

타사 또는 엔터프라이즈 CA에 vmdir용 인증서를 요청합니다.

절차

- 1 vmdir을 중지합니다.

Linux

```
service-control --stop vmdird
```

Windows

```
service-control --stop VMWareDirectoryService
```

- 2 생성한 인증서 및 키를 vmdir 위치에 복사합니다.

Linux

```
cp vmdir.crt /usr/lib/vmware-vmdir/share/config/vmdircert.pem
cp vmdir.priv /usr/lib/vmware-vmdir/share/config/vmdirkey.pem
```

Windows

```
copy vmdir.crt C:\programdata\vmware\vCenterServer\cfg\vmdird\vmdircert.pem
copy vmdir.priv C:\programdata\vmware\vCenterServer\cfg\vmdird\vmdirkey.pem
```

- 3 vSphere Web Client에서 또는 service-control 명령을 사용하여 vmdir을 다시 시작합니다.

Linux

```
service-control --start vmdird
```

Windows

```
service-control --start VMWareDirectoryService
```

혼합 모드 환경에서 VMware 디렉토리 서비스 인증서 교체

업그레이드 도중 환경에 vCenter Single Sign-On 버전 5.5와 vCenter Single Sign-On 버전 6.x 모두가 임시로 포함될 수 있습니다. 이런 경우 vCenter Single Sign-On 서비스가 실행 중인 노드의 SSL 인증서를 교체한다면 VMware Directory Service SSL 인증서를 교체하기 위한 추가적인 단계를 수행해야 합니다.

VMware Directory Service SSL 인증서는 vmdir에서 vCenter Single Sign-On 복제를 수행하는 Platform Services Controller 노드 간에 핸드셰이크를 수행하는 데 사용됩니다.

이 단계는 vSphere 6.0 및 vSphere 6.5 노드를 포함하는 혼합 모드 환경에 필요하지 않습니다. 다음의 경우에만 이 단계가 필요합니다.

- 환경에 vCenter Single Sign-On 5.5와 vCenter Single Sign-On 6.x 서비스가 모두 포함되어 있습니다.

- vCenter Single Sign-On 서비스가 vmdir 데이터를 복제하도록 설정되었습니다.
- vCenter Single Sign-On 6.x 서비스가 실행되는 노드에 대해 기본 VMCA 서명 인증서를 사용자 지정 인증서로 교체할 계획입니다.

참고 서비스를 다시 시작하기 전에 전체 환경을 업그레이드하는 것이 가장 좋습니다. VMware Directory Service 인증서 교체는 일반적으로 권장되지 않습니다.

절차

- 1 vCenter Single Sign-On 6.x 서비스가 실행되는 노드에서 vmdird SSL 인증서 및 키를 교체합니다.
[VMware 디렉토리 서비스 인증서 교체](#)의 내용을 참조하십시오.
- 2 vCenter Single Sign-On 5.5 서비스가 실행되는 노드에서 vCenter Single Sign-On 6.x 서비스가 인식되도록 환경을 설정합니다.
 - a 모든 파일 C:\ProgramData\VMware\CIS\cfg\vmdird을 백업합니다.
 - b 6.x 노드에서 vmdircert.pem 파일의 사본을 만들고 이름을 <sso_node2.domain.com>.pem 으로 바꿉니다. 여기서 <sso_node2.domain.com>은 6.x 노드의 FQDN입니다.
 - c 이름을 바꾼 인증서를 C:\ProgramData\VMware\CIS\cfg\vmdird에 복사하여 기존 복제 인증서를 교체합니다.
- 3 인증서를 교체한 모든 시스템에서 VMware 디렉토리 서비스를 다시 시작합니다.
 vSphere Web Client에서 또는 service-control 명령을 사용하여 서비스를 다시 시작할 수 있습니다.

CLI 명령으로 인증서 및 서비스 관리

일련의 CLI를 사용하여 VMCA(VMware Certificate Authority), VECS(VMware Endpoint 인증서 저장소) 및 vmdir(VMware Directory Service)를 관리할 수 있습니다. vSphere Certificate Manager 유틸리티는 다양한 관련 작업도 지원하지만 수동 인증서 관리에는 CLI가 필요합니다.

표 3-5. 인증서와 연결된 서비스 관리를 위한 CLI 도구

CLI	설명	자세한 내용은
certool	인증서와 키를 생성하고 관리합니다. VMCA의 일부입니다.	certool 초기화 명령 참조
vecs-cli	VMware Certificate Store 인스턴스의 콘텐츠를 관리합니다. VMAFD의 일부입니다.	vecs-cli 명령 참조
dir-cli	VMware Directory Service에서 인증서를 만들고 업데이트합니다. VMAFD의 일부입니다.	dir-cli 명령 참조
service-control	예를 들면 인증서 교체 워크플로의 일부로 서비스를 시작 또는 중지합니다.	

인증서 관리 도구 위치

기본적으로 각 노드의 다음 위치에서 도구를 찾을 수 있습니다.

Windows

```
C:\Program Files\VMware\vCenter Server\vmafdd\vecs-cli.exe
C:\Program Files\VMware\vCenter Server\vmafdd\dir-cli.exe
C:\Program Files\VMware\vCenter Server\vmcad\certool.exe
VCENTER_INSTALL_PATH\bin\service-control
```

Linux

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

Linux에서는 service-control 명령에 경로를 지정하지 않아도 됩니다.

외부 Platform Services Controller가 있는 관리 노드에서 명령을 실행하는 경우 --server 매개 변수로 Platform Services Controller를 지정할 수 있습니다.

인증서 관리 작업에 필요한 권한

vCenter 인증서 관리 작업 대부분을 수행하기 위해서는 vsphere.local 도메인의 CAAdmins 그룹에 속해야 합니다. administrator@vsphere.local 사용자는 CAAdmins 그룹에 속합니다. 일부 작업은 모든 사용자에게 허용됩니다.

vCenter Certificate Manager 유틸리티를 실행하는 경우 administrator@vsphere.local의 암호를 묻는 메시지가 나타납니다. 인증서를 수동으로 교체하는 경우 각 인증서 관리 CLI의 각 옵션마다 서로 다른 권한이 필요합니다.

dir-cli

vsphere.local 도메인에서 CAAdmins 그룹의 구성원이어야 합니다. dir-cli 명령을 실행할 때마다 사용자 이름과 암호를 묻는 메시지가 나타납니다.

vecs-cli

초기에는 저장소 소유자만 저장소에 액세스할 수 있습니다. 저장소 소유자는 Windows 시스템의 관리자 사용자 및 Linux 시스템의 루트 사용자입니다. 저장소 소유자는 다른 사용자에게 액세스 권한을 제공할 수 있습니다.

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

certool

certool 명령 대부분을 실행하려면 사용자가 CAAdmins 그룹에 속해야 합니다.

administrator@vsphere.local 사용자는 CAAdmins 그룹에 속합니다. 다음 명령은 모든 사용자가 실행할 수 있습니다.

- gensefcacert
- initscr
- getdc
- waitVMDIR
- waitVMCA
- genkey
- viewcert

ESXi 호스트의 인증서를 관리하려면 **인증서. 인증서 관리** 권한이 있어야 합니다. 이 권한은 vSphere Web Client에서 설정할 수 있습니다.

certool 구성 변경

certool --gencert 및 특정한 다른 인증서 초기화 또는 관리 명령을 실행하면 CLI는 구성 파일에서 모든 값을 읽습니다. 기존 파일을 편집하거나, --config=<file name> 옵션을 사용하여 기본 구성 파일 (certool.cfg)을 재정의하거나, 명령줄에서 다른 값을 재정의할 수 있습니다.

구성 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
```

다음과 같이 구성의 값을 변경할 수 있습니다.

- 구성 파일을 백업한 다음 파일을 편집합니다. 기본 구성 파일을 사용 중인 경우에는 지정하지 않아도 됩니다. 그렇지 않고 예를 들어 구성 파일 이름을 변경한 경우에는 --config 명령줄 옵션을 사용합니다.
- 명령줄에서 구성 파일 값을 재정의합니다. 예를 들어 Locality를 재정의하려면 이 명령을 실행합니다.

```
certool --gencert --privkey=private.key --Locality="Mountain View"
```


인증서 주체 이름의 CN 필드를 교체하려면 `--Name`을 지정합니다.

- 솔루션 사용자 인증서의 경우 이름은 관례적으로 `<sol_user name>@<domain>`이지만 환경에 다른 관례가 사용되는 경우에는 이름을 변경할 수 있습니다.
- 시스템 SSL 인증서의 경우 시스템의 호스트 이름을 확인할 때 SSL 클라이언트가 인증서 주체 이름의 CN 필드를 확인하기 때문에 시스템의 FQDN이 사용됩니다. 시스템에는 별칭이 두 개 이상일 수 있기 때문에, 인증서에는 다른 이름(DNS 이름, IP 주소 등)을 지정할 수 있는 주체 대체 이름 필드 확장이 있습니다. 하지만 VMCA에서는 하나의 DNSName(Hostname 필드에서)만 허용하며 다른 별칭 옵션은 허용하지 않습니다. 사용자가 IP 주소를 지정하는 경우 이 주소도 SubAltName에 저장됩니다.

`--Hostname` 매개 변수는 인증서 SubAltName의 DNSName을 지정하는 데 사용됩니다.

certool 초기화 명령 참조

certool 초기화 명령을 사용하면 인증서 서명 요청을 생성하고 VMCA에서 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 변경](#)를 참조하십시오. 몇 가지 사용 예는 새 VMCA 서명된 인증서로 기존 VMCA 서명된 인증서 교체 항목을 참조하십시오.

certool --initcsr

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

옵션	설명
<code>--initcsr</code>	CSR 생성에 필요합니다.
<code>--privkey <key_file></code>	개인 키 파일의 이름입니다.
<code>--pubkey <key_file></code>	공용 키 파일의 이름입니다.
<code>--csrfile <csr_file></code>	CA 제공자에게 보낼 CSR 파일의 파일 이름입니다.
<code>--config <config_file></code>	구성 파일의 선택적 이름입니다. 기본적으로 <code>certool.cfg</code> 로 설정됩니다.

예:

```
certool --initcsr --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. [중간 CA\(인증 기관\)로 VMCA 사용](#)를 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.
--config <config_file>	구성 파일의 선택적 이름입니다. 기본적으로 certool.cfg로 설정됩니다.
--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 서명에 최신 루트 인증서를 사용하지만 다른 루트 인증서는 계속 사용할 수 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>	구성 파일의 선택적 이름입니다. 기본적으로 certool.cfg로 설정됩니다.
--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 디렉토리 서비스가 실행될 때까지 대기하거나 --wait에서 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. 기본값을 3으로 합니다.
--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. 기본값을 3으로 합니다.
--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. 인증서를 사용하여 시스템 또는 솔루션 사용자를 프로비저닝할 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.

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 선택적 이름입니다. 기본적으로 certool.cfg로 설정됩니다.
--server <server>	VMCA 서버의 선택적 이름입니다. 기본적으로 이 명령은 localhost를 사용합니다.

예:

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

certool --getrootca

사람이 읽을 수 있는 형식으로 현재 루트 CA 인증서를 인쇄합니다. 관리 노드에서 이 명령을 실행하는 경우 Platform Services Controller 노드의 시스템 이름을 사용하여 루트 CA를 검색합니다. 이 출력은 인증서로 사용할 수 없으며 사람이 읽을 수 있는 형식으로 변경됩니다.

옵션	설명
<code>--getrootca</code>	루트 인증서 인쇄에 필요합니다.
<code>--server <server></code>	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
<code>--viewcert</code>	인증서 보기에 필요합니다.
<code>--cert <certfile></code>	구성 파일의 선택적 이름입니다. 기본적으로 certool.cfg로 설정됩니다.

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
<code>--enumcert</code>	모든 인증서 나열에 필요합니다.
<code>--filter [all active]</code>	필수 필드입니다. 모두 또는 활성을 지정합니다. 해지됨 및 만료된 옵션은 현재 지원되지 않습니다.

예:

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

certool --status

인증서가 해지되었는지 여부를 확인하기 위해 지정된 인증서를 VMCA 서버로 전송합니다. 인증서가 해지된 경우 Certificate: REVOKED를 인쇄하고, 그렇지 않은 경우 Certificate: ACTIVE를 인쇄합니다.

옵션	설명
--status	인증서의 상태를 확인하는 데 필요합니다.
--cert <certfile>	구성 파일의 선택적 이름입니다. 기본적으로 certool.cfg로 설정됩니다.
--server <server>	VMCA 서버의 선택적 이름입니다. 기본적으로 이 명령은 localhost를 사용합니다.

예:

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

certool --genselfcert

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

옵션	설명
--genselfcert	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 선택적 이름입니다. 기본적으로 certool.cfg로 설정됩니다.

예:

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

vecs-cli 명령 참조

vecs-cli 명령 집합을 통해 VECS(VMware Certificate Store) 인스턴스를 관리할 수 있습니다. 다음 명령을 dir-cli 및 certool과 함께 사용하여 인증서 인프라를 관리합니다.

vecs-cli store create

인증서 저장소를 생성합니다.

옵션	설명
--name <name>	인증서 저장소의 이름입니다.

예:

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

vecs-cli store delete

인증서 저장소를 삭제합니다. 시스템이 사전 정의한 인증서 저장소는 삭제할 수 없습니다.

옵션	설명
<code>--name <name></code>	삭제할 인증서 저장소의 이름입니다.

예:

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

vecs-cli store list

인증서 저장소를 나열합니다.

VECS에는 다음과 같은 저장소가 포함됩니다.

표 3-6. VECS의 저장소

저장소	설명
시스템 SSL 저장소(MACHINE_SSL_CERT)	<ul style="list-style-type: none"> 모든 vSphere 노드의 역방향 프록시 서비스에서 사용됩니다. 내장된 배포 및 각 Platform Services Controller 노드의 VMware 디렉토리 서비스(vmdir)에서 사용합니다. <p>vSphere 6.0에서 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 아직 자체 포트를 열어둡니다.</p>
신뢰할 수 있는 루트 저장소(TRUSTED_ROOTS)	모든 신뢰할 수 있는 루트 인증서가 포함됩니다.

표 3-6. VECS의 저장소 (계속)

저장소	설명
솔루션 사용자 저장소 <ul style="list-style-type: none"> ■ machine ■ vpxd ■ vpxd-extensions ■ vsphere-webclient 	<p>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.</p> <p>솔루션 사용자 인증서는 vCenter Single Sign-On을 사용한 인증에 사용됩니다. vCenter Single Sign-On은 인증서가 올바른지 확인하지만 다른 인증서 특성은 확인하지 않습니다. 포함된 배포에서 모든 솔루션 사용자 인증서는 같은 시스템에 있습니다.</p> <p>각 관리 노드 및 각 내장된 배포의 VECS에 다음의 솔루션 사용자 인증서 저장소가 포함되어 있습니다.</p> <ul style="list-style-type: none"> ■ machine: 구성 요소 관리자, 라이선스 서버 및 로깅 서비스에서 사용됩니다. <p>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.</p> <ul style="list-style-type: none"> ■ vpxd: 관리 노드 및 내장된 배포의 vCenter 서비스 대몬(vpxd) 저장소. vpxd는 이 저장소에 저장된 솔루션 사용자 인증서를 사용하여 vCenter Single Sign-On에 인증합니다. ■ vpxd-extensions: vCenter 확장 저장소. Auto Deploy 서비스, Inventory Service를 비롯해 다른 솔루션 사용자의 일부가 아닌 기타 서비스가 포함됩니다. ■ vsphere-webclient: vSphere Web Client 저장소. 성능 차트 서비스와 같은 일부 추가 서비스도 포함됩니다. <p>시스템 저장소는 각 Platform Services Controller 노드에도 포함됩니다.</p>
vSphere Certificate Manager 유틸리티 백업 저장소 (BACKUP_STORE)	<p>VMCA(VMware Certificate Manager)에서 인증서 복구를 지원하기 위해 사용됩니다. 최근 상태만 백업으로 저장되며 한 단계까지만 되돌아갈 수 있습니다.</p>
기타 저장소	<p>솔루션을 통해 기타 저장소가 추가될 수 있습니다. 예를 들어 가상 볼륨 솔루션은 SMS 저장소를 추가합니다. VMware 설명서 또는 VMware 기술 자료 문서에서 그렇게 하라고 지시하지 않는 이상 이러한 저장소의 인증서를 수정하지 마십시오.</p> <p>참고 CRLS는 vSphere 6.0에서 지원되지 않지만 TRUSTED_ROOTS_CRLS 저장소를 삭제하면 인증서 인프라가 손상될 수 있습니다. TRUSTED_ROOTS_CRLS 저장소를 삭제하거나 수정하지 마십시오.</p>

예:

```
vecs-cli store list
```


vecs-cli store permissions

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

저장소의 소유자는 사용 권한 부여 및 취소를 비롯하여 해당 저장소에 대한 모든 제어를 가집니다. 관리자는 사용 권한 부여 및 취소를 비롯하여 모든 저장소에 대한 모든 권한을 가집니다.

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

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

vecs-cli entry create

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

옵션	설명
<code>--store <NameOfStore></code>	인증서 저장소의 이름입니다.
<code>--alias <Alias></code>	인증서에 대한 선택적 별칭입니다. 이 옵션은 신뢰할 수 있는 루트 저장소에 대해 무시됩니다.
<code>--cert <certificate_file_path></code>	인증서 파일의 전체 경로입니다.
<code>--key <key-file-path></code>	인증서에 해당하는 키의 전체 경로입니다. 선택 사항입니다.

vecs-cli entry list

지정된 저장소의 모든 항목을 나열합니다.

옵션	설명
<code>--store <NameOfStore></code>	인증서 저장소의 이름입니다.
<code>--text</code>	사람이 읽을 수 있는 인증서 버전을 표시합니다.

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.

vecs-cli entry getkey

VECS에 저장된 키를 검색합니다. 출력 파일에 인증서를 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.

vecs-cli entry delete

인증서 저장소에서 항목을 삭제합니다. VECS에서 항목을 삭제하는 경우 VECS에서 영구적으로 제거합니다. 유일한 예외는 현재 루트 인증서입니다. VECS는 vmdir에서 루트 인증서를 폴링합니다.

옵션	설명
--store <NameOfStore>	인증서 저장소의 이름입니다.
--alias <Alias>	삭제하려는 항목의 별칭입니다.

vecs-cli force-refresh

vecs-cli를 강제로 새로 고칩니다. 그럴 경우 vmdir의 최신 정보를 사용하도록 vecs-cli가 업데이트됩니다. 기본적으로 VECS는 5분 간격으로 vmdir을 폴링하여 새 루트 인증서 파일을 검색합니다. vmdir에서 VECS를 즉시 업데이트하려면 이 명령을 사용합니다.

dir-cli 명령 참조

dir-cli 유틸리티를 사용하면 솔루션 사용자를 생성 및 업데이트하고 다른 사용자 계정을 생성하고 vmdir에서 인증서 및 암호를 관리할 수 있습니다. 이 유틸리티를 vecs-cli 및 certool과 함께 사용하여 인증서 인프라를 관리합니다.

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.
--login <admin_user_id>	기본적으로 administrator@vsphere.local입니다. 이 관리자는 다른 사용자를 CAAadmins vCenter Single Sign-On 그룹에 추가하여 해당 사용자에게 관리자 권한을 부여할 수 있습니다.
--password <admin_password>	관리자의 암호입니다. 암호를 지정하지 않으면 메시지가 표시됩니다.

dir-cli service list

dir-cli가 알고 있는 솔루션 사용자를 나열합니다.

옵션	설명
--login <admin_user_id>	기본적으로 administrator@vsphere.local입니다. 이 관리자는 다른 사용자를 CAAadmins vCenter Single Sign-On 그룹에 추가하여 해당 사용자에게 관리자 권한을 부여할 수 있습니다.
--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 administrator@vsphere.local입니다. 이 관리자는 다른 사용자를 CAAadmins vCenter Single Sign-On 그룹에 추가하여 해당 사용자에게 관리자 권한을 부여할 수 있습니다.
--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 VECS가 5분 후 변경 사항을 선택하거나 vecs-cli force-refresh를 사용하여 강제로 새로 고침할 수 있습니다.

옵션	설명
--name <name>	업데이트할 솔루션 사용자의 이름입니다.
--cert <cert_file>	서비스에 할당할 인증서의 이름입니다.

옵션	설명
--login <admin_user_id>	기본적으로 administrator@vsphere.local입니다. 이 관리자는 다른 사용자를 CAAAdmins vCenter Single Sign-On 그룹에 추가하여 해당 사용자에게 관리자 권한을 부여할 수 있습니다.
--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 사용자에게 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 administrator@vsphere.local입니다. 이 관리자는 다른 사용자를 CAAAdmins vCenter Single Sign-On 그룹에 추가하여 해당 사용자에게 관리자 권한을 부여할 수 있습니다.
--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 administrator@vsphere.local입니다. 이 관리자는 다른 사용자를 CAAAdmins vCenter Single Sign-On 그룹에 추가하여 해당 사용자에게 관리자 권한을 부여할 수 있습니다.
--password <admin_password>	관리자의 암호입니다. 암호를 지정하지 않으면 메시지가 표시됩니다.

dir-cli group modify

사용자 또는 그룹을 이미 존재하는 그룹에 추가합니다.

옵션	설명
--name <name>	vmdir의 그룹 이름입니다.
--add <user_or_group_name>	추가할 사용자 또는 그룹의 이름입니다.
--login <admin_user_id>	기본적으로 administrator@vsphere.local입니다. 이 관리자는 다른 사용자를 CAAadmins vCenter Single Sign-On 그룹에 추가하여 해당 사용자에게 관리자 권한을 부여할 수 있습니다.
--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 그룹이 있는지 여부를 확인할 수 있습니다.
--login <admin_user_id>	기본적으로 administrator@vsphere.local입니다. 이 관리자는 다른 사용자를 CAAadmins vCenter Single Sign-On 그룹에 추가하여 해당 사용자에게 관리자 권한을 부여할 수 있습니다.
--password <admin_password>	관리자의 암호입니다. 암호를 지정하지 않으면 메시지가 표시됩니다.

dir-cli trustedcert publish

신뢰할 수 있는 루트 인증서를 vmdir에 게시합니다.

옵션	설명
--cert <file>	인증서 파일의 경로입니다.
--login <admin_user_id>	기본적으로 administrator@vsphere.local입니다. 이 관리자는 다른 사용자를 CAAadmins vCenter Single Sign-On 그룹에 추가하여 해당 사용자에게 관리자 권한을 부여할 수 있습니다.
--password <admin_password>	관리자의 암호입니다. 암호를 지정하지 않으면 메시지가 표시됩니다.

dir-cli trustedcert unpublsh

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.

옵션	설명
--cert-file <file>	게시를 취소할 인증서 파일의 경로입니다.
--crl <file>	이 인증서와 연결된 CRL 파일의 경로입니다. 현재 사용되지 않습니다.
--login <admin_user_id>	기본적으로 administrator@vsphere.local입니다. 이 관리자는 다른 사용자를 CAAAdmins vCenter Single Sign-On 그룹에 추가하여 해당 사용자에게 관리자 권한을 부여할 수 있습니다.
--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 get을 사용하여 인증서를 검색하려면 인증서 ID가 필요합니다.

옵션	설명
--login <admin_user_id>	기본적으로 administrator@vsphere.local입니다. 이 관리자는 다른 사용자를 CAAAdmins vCenter Single Sign-On 그룹에 추가하여 해당 사용자에게 관리자 권한을 부여할 수 있습니다.
--password <admin_password>	관리자의 암호입니다. 암호를 지정하지 않으면 메시지가 표시됩니다.

dir-cli trustedcert get

vmmdir에서 신뢰할 수 있는 루트 인증서를 검색하고 지정된 파일에 씁니다.

옵션	설명
--id <cert_ID>	검색할 인증서의 ID입니다. ID는 dir-cli trustedcert list 명령에 표시됩니다.
--outcert <path>	인증서 파일을 쓸 경로입니다.
--outcrl <path>	CRL 파일을 쓸 경로입니다. 현재 사용되지 않습니다.
--login <admin_user_id>	기본적으로 administrator@vsphere.local입니다. 이 관리자는 다른 사용자를 CAAAdmins vCenter Single Sign-On 그룹에 추가하여 해당 사용자에게 관리자 권한을 부여할 수 있습니다.
--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 administrator@vsphere.local입니다. 이 관리자는 다른 사용자를 CAAadmins vCenter Single Sign-On 그룹에 추가하여 해당 사용자에게 관리자 권한을 부여할 수 있습니다.
--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 change를 사용합니다.

옵션	설명
--account	새 암호를 할당할 계정의 이름입니다.
--new	지정된 사용자의 새 암호입니다.
--login <admin_user_id>	기본적으로 administrator@vsphere.local입니다. 이 관리자는 다른 사용자를 CAAadmins vCenter Single Sign-On 그룹에 추가하여 해당 사용자에게 관리자 권한을 부여할 수 있습니다.
--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 reset을 사용하여 암호를 재설정할 수 있습니다.

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

vSphere Web Client를 사용하여 vCenter 인증서 보기

VMCA(vCenter 인증 기관)에 알려진 인증서를 확인하여 활성 인증서의 만료가 다가오는지 확인하고, 만료된 인증서를 확인하고, 루트 인증서의 상태를 확인할 수 있습니다. 인증서 관리 CLI를 사용하여 모든 인증서 관리 작업을 수행할 수 있습니다.

내장된 배포 또는 Platform Services Controller에 포함된 VMCA 인스턴스와 연관된 인증서를 확인합니다. 인증서 정보는 vmdir(VMware 디렉토리 서비스)의 인스턴스 전체에 복제됩니다.

vSphere Web Client에서 인증서를 보려고 하면 사용자 이름과 암호를 묻는 메시지가 표시됩니다. VMware 인증 기관에 대한 권한을 가진 사용자, 즉 CAAdmins vCenter Single Sign-On 그룹에 속한 사용자의 사용자 이름과 암호를 지정하십시오.

절차

- 1 administrator@vsphere.local 또는 CAAdmins vCenter Single Sign-On 그룹의 다른 사용자로 vCenter Server에 로그인합니다.
- 2 **관리**를 선택하고 **배포**를 클릭하고 **시스템 구성**을 클릭합니다.
- 3 **노드**를 클릭하고 인증서를 보거나 관리할 노드를 선택합니다.
- 4 **관리** 탭을 클릭하고 **인증 기관**을 클릭합니다.
- 5 인증서 정보를 볼 인증서 유형을 클릭합니다.

옵션	설명
활성 인증서	유효성 확인 정보를 포함하여 활성 인증서를 표시합니다. 인증서 만료가 다가오면 녹색 유효 기간 종료 아이콘이 바뀝니다.
해지된 인증서	해지된 인증서의 목록을 표시합니다. 이 톨리스에서는 지원되지 않습니다.
만료된 인증서	만료된 인증서를 나열합니다.
루트 인증서	vCenter 인증 기관의 이 인스턴스에 사용 가능한 루트 인증서를 표시합니다.

- 6 인증서를 선택하고 **인증서 세부 정보 표시** 버튼을 클릭하여 인증서 세부 정보를 표시합니다.
세부 정보에는 주체 이름, 발급자, 유효성 및 알고리즘이 포함됩니다.

vCenter 인증서 만료 경고의 임계값 설정

vSphere 6.0부터는 vCenter Server가 VECS(VMware Endpoint 인증서 저장소)의 모든 인증서를 관리하고 인증서 만료까지 남은 기간이 30일 이하인 경우 경보를 표시합니다. vpxd.cert.threshold 고급 옵션을 사용하면 경고 표시 시기를 변경할 수 있습니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 vCenter Server 개체를 선택하고 **관리** 탭과 **설정** 하위 탭을 선택합니다.
- 3 **고급 설정**을 클릭하고 **편집**을 선택한 다음 임계값을 필터링합니다.
- 4 vpxd.cert.threshold의 설정을 원하는 값으로 변경하고 **확인**을 클릭합니다.

vSphere 사용 권한 및 사용자 관리 작업

4

vCenter Single Sign-On은 인증을 지원합니다. 즉, 사용자가 vSphere 구성 요소에 액세스할 수 있는지 여부를 결정합니다. 또한 각 사용자에게는 vSphere 개체를 보거나 조작할 수 있는 권한이 있어야 합니다.

vSphere에서는 vSphere의 권한 부여 이해에서 논의된 몇 가지의 서로 다른 권한 부여 메커니즘을 지원합니다. 이 섹션의 정보는 vCenter Server 사용 권한 모델과 사용자 관리 작업을 수행하는 방법에 초점을 맞추고 있습니다.

vCenter Server에서는 사용 권한 및 역할을 통해 권한 부여를 세부적으로 제어할 수 있습니다. vCenter Server 개체 계층의 개체에 사용 권한을 할당할 때 해당 개체에 대해 권한을 가질 사용자나 그룹 그리고 그 권한의 내용을 지정합니다. 권한을 지정하려면 일련의 권한으로 구성된 역할을 사용합니다.

처음에는 administrator@vsphere.local 사용자만 vCenter Server 시스템에 로그인할 수 있습니다. 이후 이 사용자는 다음과 같이 계속할 수 있습니다.

- 1 vCenter Single Sign-On에 대해 추가 사용자 및 그룹이 정의되는 ID 소스를 추가합니다. [vCenter Single Sign-On ID 소스 추가](#)의 내용을 참조하십시오.
- 2 가상 시스템 또는 vCenter Server 시스템과 같은 개체를 선택하고 사용자 또는 그룹에 이 개체에 대한 역할을 할당하여 사용자 또는 그룹에 권한을 부여합니다.



역할, 권한 및 사용 권한

(https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_8vla7txu/uiConfId/49694343/)

본 장은 다음 항목을 포함합니다.

- vSphere의 권한 부여 이해
- vCenter Server 권한 모델 이해
- 사용 권한의 계층적 상속
- 여러 가지 사용 권한 설정
- vCenter 구성 요소에 대한 사용 권한 관리
- 글로벌 사용 권한
- 역할을 사용하여 권한 할당
- 역할 및 권한에 대한 모범 사례

■ 일반 작업에 필요한 권한

vSphere의 권한 부여 이해

vSphere의 사용자 또는 그룹 권한 부여의 기본 방식은 vCenter Server 사용 권한입니다. 수행할 작업에 따라 기타 권한 부여가 필요할 수 있습니다.

vSphere 6.0 이상에서는 권한이 있는 사용자가 다른 사용자에게 다음과 같은 방식으로 작업을 수행할 수 있는 사용 권한을 부여할 수 있습니다. 이러한 접근 방식은 대개 상호 배타적이지는 않지만 글로벌 사용 권한을 할당하여 모든 솔루션에 대한 특정 사용자에게 권한을 부여하고 로컬 vCenter Server 사용 권한을 할당하여 개별 vCenter Server 시스템에 대한 기타 사용자에게 권한을 부여할 수 있습니다.

vCenter Server 사용 권한

vCenter Server 시스템의 사용 권한 모델은 해당 vCenter Server의 개체 계층의 개체에 대한 사용 권한 할당을 사용합니다. 각 사용 권한은 하나의 사용자 또는 그룹에 일련의 권한, 즉 선택된 개체에 대한 역할을 부여합니다. 예를 들어 ESXi 호스트를 선택하고 역할을 사용자 그룹에 할당하여 해당 사용자에게 해당 호스트에 해당하는 권한을 부여할 수 있습니다.

글로벌 사용 권한

글로벌 사용 권한은 여러 솔루션에 걸쳐 있는 글로벌 루트 개체에 적용됩니다. 예를 들어 vCenter Server와 vCenter Orchestrator가 모두 설치된 경우 글로벌 사용 권한을 사용하여 두 개체 계층의 모든 개체에 사용 권한을 부여할 수 있습니다.

글로벌 사용 권한은 vsphere.local 도메인 전체에 복제됩니다. 글로벌 사용 권한은 vsphere.local 그룹을 통해 관리되는 서비스에 대해 권한 부여를 제공하지 않습니다. [글로벌 사용 권한](#)을 참조하십시오.

vsphere.local 그룹의 그룹 멤버 자격

administrator@vsphere.local 사용자는 Platform Services Controller에 포함된 서비스와 연결된 작업을 수행할 수 있습니다. 또한 vsphere.local 그룹의 멤버는 해당 작업을 수행할 수 있습니다. 예를 들어 LicenseService.Administrators 그룹의 멤버인 경우 라이선스 관리를 수행할 수 있습니다.

[vsphere.local 도메인의 그룹](#)을 참조하십시오.

ESXi 로컬 호스트 사용 권한

vCenter Server 시스템을 통해 관리되지 않는 독립형 ESXi 호스트를 관리하는 경우 미리 정의된 역할 중 하나를 사용자에게 할당할 수 있습니다. "vSphere Client를 통한 vSphere 관리" 설명서를 참조하십시오.

vCenter Server 권한 모델 이해

vCenter Server 시스템의 권한 모델은 vSphere 개체 계층의 개체에 대한 권한 할당을 사용합니다. 각 권한(permission)은 하나의 사용자 또는 그룹에 일련의 권한(privilege), 즉 선택된 개체에 대한 역할을 부여합니다.

다음 개념을 이해해야 합니다.

사용 권한

vCenter Server 개체 계층의 각 개체에는 연결된 사용 권한이 있습니다. 각 사용 권한은 그룹 또는 사용자가 개체에 대한 권한을 가지고 있는 하나의 그룹 또는 사용자에게 지정됩니다.

사용자 및 그룹

vCenter Server 시스템에서, 인증된 사용자 또는 인증된 사용자의 그룹에만 권한을 할당할 수 있습니다. 사용자는 vCenter Single Sign-On을 통해 인증됩니다. vCenter Single Sign-On에서 인증하는 데 사용하는 ID 소스에서 사용자 및 그룹을 정의해야 합니다. Active Directory와 같은 ID 소스에서 도구를 사용하여 사용자 및 그룹을 정의합니다.

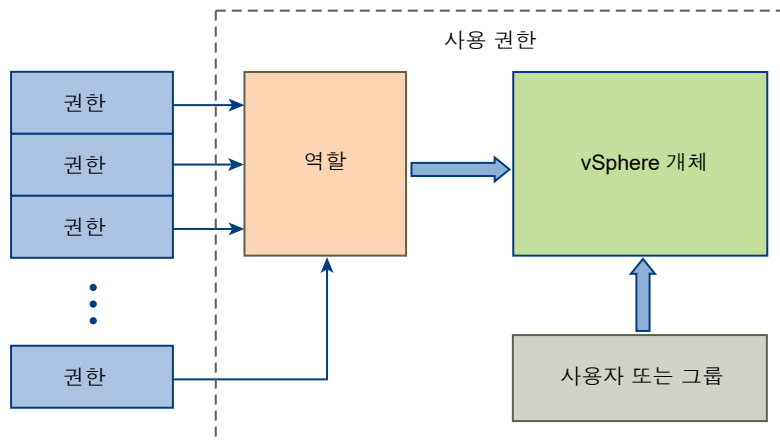
역할

역할을 사용하여 사용자가 수행하는 일련의 일반 작업을 기반으로 개체에 대한 사용 권한을 할당할 수 있습니다. 관리자와 같은 기본 역할은 vCenter Server에 미리 정의되어 있으며 변경할 수 없습니다. 리소스 풀 관리자와 같은 기타 역할은 미리 정의된 샘플 역할입니다. 사용자 지정 역할은 처음부터 생성하거나 샘플 역할을 복제 및 수정하여 생성할 수 있습니다.

권한

권한은 세분화된 액세스 제어입니다. 이러한 권한을 역할로 그룹화한 다음 사용자 또는 그룹에 매핑할 수 있습니다.

그림 4-1. vSphere 권한



개체에 권한을 할당하려면 다음 단계를 따르십시오.

- 1 vCenter 개체 계층에서 권한을 적용할 개체를 선택합니다.
- 2 개체에 대한 권한을 가져야 하는 그룹 또는 사용자를 선택합니다.
- 3 개체에 대해 그룹 또는 사용자가 가져야 하는 역할(일련의 권한)을 선택합니다. 기본적으로 권한은 전파됩니다. 즉 그룹 또는 사용자는 선택된 개체와 그 하위 개체에 대해 선택된 역할을 가집니다.

권한 모델을 사용하면 미리 정의된 역할을 활용하여 작업을 쉽고 빠르게 할 수 있습니다. 또한 권한을 결합하여 사용자 지정 역할을 생성할 수도 있습니다. 모든 권한 그리고 권한을 적용할 수 있는 개체에 대한 참조를 보려면 [장 11 정의된 권한](#)을 참조하십시오. 이러한 작업을 수행해야 하는 권한 집합의 일부 예는 [일반 작업에 필요한 권한](#)을 참조하십시오.

많은 경우, 소스 개체 및 대상 개체 모두에 대해 권한을 정의해야 합니다. 예를 들어, 가상 시스템을 이동하는 경우 가상 시스템에 대한 일부 권한이 필요하며 대상 데이터 센터에 대한 권한도 필요합니다.

독립형 ESXi 호스트에 대한 권한 모델은 더 간단합니다. [ESXi에 대한 사용 권한 할당](#) 항목을 참조하십시오.

vCenter Server 사용자 유효성 검사

디렉토리 서비스를 사용하는 vCenter Server 시스템은 정기적으로 사용자 디렉토리 도메인을 기준으로 사용자 및 그룹을 검증합니다. vCenter Server 설정에 지정된 간격마다 정기적으로 검증이 이루어집니다. 예를 들어, 사용자 Smith에게 몇 가지 개체에 대한 역할이 할당되었는데 도메인에서 사용자 이름이 Smith2로 변경된 경우 호스트는 Smith가 더 이상 존재하지 않는다고 단정하고 다음 유효성 검사가 수행될 때 해당 사용자와 연관된 권한을 vSphere 개체에서 제거합니다.

마찬가지로, 도메인에서 사용자 Smith가 제거되면 다음 유효성 검사가 수행될 때 해당 사용자와 연관된 모든 권한이 제거됩니다. 다음에 유효성 검사가 수행되기 전에 새 사용자 Smith가 도메인에 추가되면 새 사용자 Smith가 개체에 대한 권한에 있어 이전 사용자 Smith를 대체합니다.

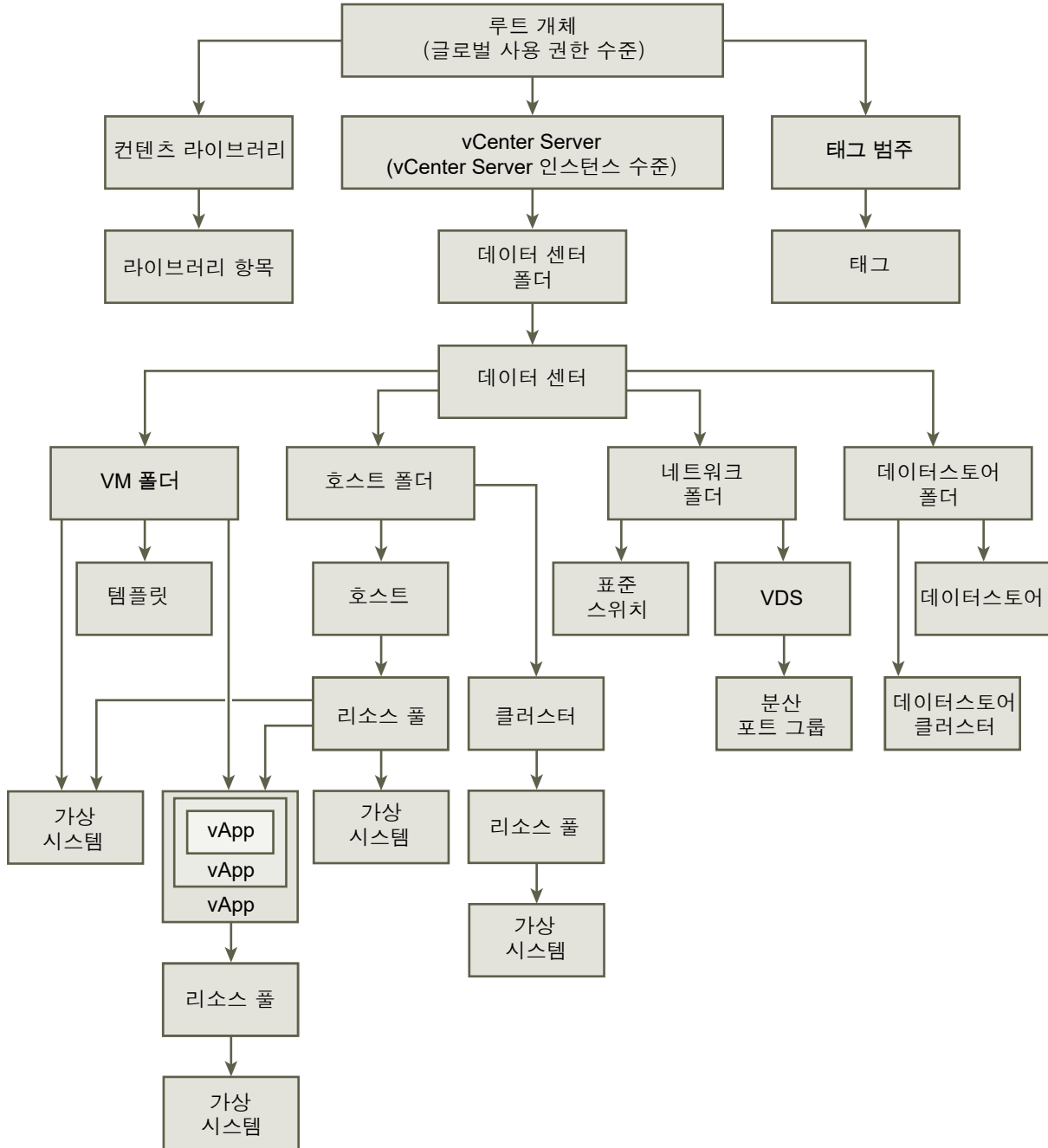
사용 권한의 계층적 상속

개체에 사용 권한을 할당할 때 사용 권한을 개체 계층의 하위 개체로 전파할지 여부를 선택할 수 있습니다. 각 사용 권한에 대한 전파를 설정합니다. 전파는 일괄 적용되지 않습니다. 하위 개체에 대해 정의된 사용 권한이 항상 상위 개체에서 전파된 사용 권한을 재정의합니다.

이 그림에서는 인벤토리 계층과 사용 권한을 전파할 수 있는 경로를 보여 줍니다.

참고 글로벌 사용 권한은 글로벌 루트 개체의 솔루션 전체에 대한 권한 할당을 지원합니다. [글로벌 사용 권한](#)을 참조하십시오.

그림 4-2. vSphere 인벤토리 계층 구조



대부분의 인벤토리 개체는 계층에 있는 단일 상위 개체로부터 사용 권한을 상속합니다. 예를 들어 데이터 스토어는 상위 데이터스토어 폴더 또는 상위 데이터 센터로부터 사용 권한을 상속합니다. 가상 시스템은 상위 가상 시스템 폴더 및 상위 호스트, 클러스터 또는 리소스 풀 모두로부터 동시에 사용 권한을 상속합니다.

예를 들어 폴더나 데이터 센터와 같은 상위 개체에 대한 사용 권한을 설정하여 Distributed Switch 및 그와 연결된 분산 포트 그룹에 대한 사용 권한을 설정할 수 있습니다. 또한 이 사용 권한을 하위 개체로 전파하는 옵션도 선택해야 합니다.

계층에는 다음 몇 가지 형식의 사용 권한이 있습니다.

관리 엔터티

권한 있는 사용자는 관리 엔터티에 대한 사용 권한을 정의할 수 있습니다.

- 클러스터
- 데이터 센터
- 데이터스토어
- 데이터스토어 클러스터
- 폴더
- 호스트
- 네트워크(vSphere Distributed Switch 제외)
- 분산 포트 그룹
- 리소스 풀
- 템플릿
- 가상 시스템
- vSphere vApp

글로벌 엔터티

루트 vCenter Server 시스템에서 사용 권한이 파생되는 엔터티에 대한 사용 권한을 수정할 수 없습니다.

- 사용자 지정 필드
- 라이선스
- 역할
- 통계 간격
- 세션

여러 가지 사용 권한 설정

개체에는 여러 권한이 있을 수 있지만 각 사용자나 그룹에는 사용 권한이 하나만 있을 수 있습니다. 예를 들어, 한 사용 권한에서 그룹 A가 개체에 대한 관리자 권한을 갖도록 지정할 수 있고 다른 사용 권한에서 그룹 B가 같은 개체에 대해 가상 시스템 관리자 권한을 갖도록 지정할 수 있습니다.

한 개체가 두 상위 개체로부터 사용 권한을 상속하면 한 개체의 사용 권한이 다른 개체의 사용 권한에 추가됩니다. 예를 들어, 한 가상 시스템이 가상 시스템 폴더에 있고 리소스 풀에도 속하는 경우 해당 가상 시스템은 가상 시스템 폴더와 리소스 풀 모두에서 모든 사용 권한 설정을 상속합니다.

하위 개체에 적용된 권한은 항상 상위 개체에 적용된 권한을 재정의합니다. [예 2: 상위 사용 권한을 재정의하는 하위 사용 권한](#)의 내용을 참조하십시오.

여러 그룹 사용 권한이 동일한 개체에 대해 정의되고 사용자가 이들 그룹 중 둘 이상에 속하게 되면 다음과 같은 두 가지 상황이 가능합니다.

- 해당 개체에 대해 사용자의 사용 권한이 정의되지 않은 경우 사용자는 해당 개체의 그룹에 할당된 권한 집합을 할당받습니다.
- 해당 개체에 대해 사용자의 권한이 정의된 경우에는 사용자의 사용 권한이 모든 그룹의 사용 권한보다 우선합니다.

예 1: 여러 사용 권한의 상속

이 예제에서는 상위 개체에 대한 사용 권한이 부여된 그룹에서 한 개체가 여러 사용 권한을 상속할 수 있는 방법을 보여 줍니다.

이 예제에서는 동일한 개체의 두 그룹에 대해 두 개의 사용 권한이 할당됩니다.

- 역할 1은 가상 시스템의 전원을 켤 수 있습니다.
- 역할 2는 가상 시스템의 스냅샷을 작성할 수 있습니다.
- 그룹 A에는 사용 권한이 하위 개체에 전파되도록 설정된 VM 폴더에 대한 역할 1이 부여됩니다.
- 그룹 B는 사용 권한이 하위 개체에 전파되도록 설정된 VM 폴더에 대한 역할 2가 부여됩니다.
- 사용자 1에는 특정 권한이 할당되지 않았습니다.

그룹 A 및 B에 속한 사용자 1이 로그인합니다. 사용자 1은 VM A와 VM B의 전원을 켜고 스냅샷을 작성할 수 있습니다.

그림 4-3. 예 1: 여러 사용 권한의 상속



예 2: 상위 사용 권한을 재정의하는 하위 사용 권한

이 예제에서는 하위 개체에 할당된 사용 권한이 상위 개체에 할당된 사용 권한을 재정의할 수 있는 방법을 보여 줍니다. 이 재정의 동작을 사용하여 사용자 액세스를 특정 인벤토리 영역으로 제한할 수 있습니다.

이 예에서는 사용 권한이 서로 다른 두 그룹의 다른 두 개체에서 정의됩니다.

- 역할 1은 가상 시스템의 전원을 켤 수 있습니다.
- 역할 2는 가상 시스템의 스냅샷을 작성할 수 있습니다.
- 그룹 A에는 사용 권한이 하위 개체에 전파되도록 설정된 VM 폴더에 대한 역할 1이 부여됩니다.

- 그룹 B에는 VM B에 대한 역할 2가 부여됩니다.

그룹 A 및 B에 속한 사용자 1이 로그인합니다. 역할 2는 계층에서 역할 1보다 낮은 지점에 할당되어 있으므로 VM B의 역할 1을 재정의합니다. 사용자 1은 VM A의 전원을 켤 수 있지만 VM A의 스냅샷을 작성할 수는 없습니다. 사용자 1은 VM B의 스냅샷을 작성할 수 있지만 VM B의 전원을 켤 수는 없습니다.

그림 4-4. 예 2: 상위 사용 권한을 재정의하는 하위 사용 권한



예 3: 그룹 역할을 재정의하는 사용자 역할

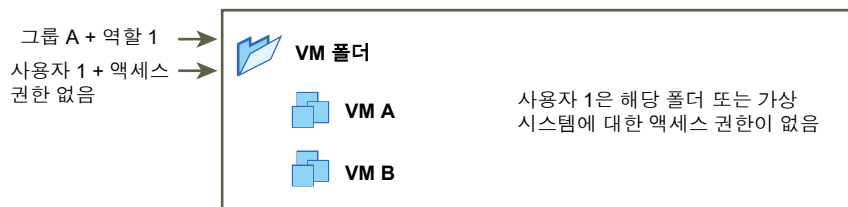
이 예제는 개별 사용자에게 직접 할당된 역할이 그룹에 할당된 역할과 연결된 권한을 재정의하는 방법을 보여줍니다.

이 예제에서 사용 권한은 동일한 개체에서 정의됩니다. 한 사용 권한은 그룹을 역할에 연결하고, 다른 사용 권한은 개별 사용자를 역할에 연결합니다. 사용자는 그룹의 멤버입니다.

- 역할 1은 가상 시스템의 전원을 켤 수 있습니다.
- 그룹 A에는 VM 폴더에 대한 역할 1이 부여됩니다.
- 사용자 1에는 VM 폴더에 대한 권한 없음 역할이 부여됩니다.

사용자 1(그룹 A에 속함)이 로그인합니다. VM 폴더에 대해 사용자 1에게 부여된 권한 없음 역할이 그룹에 할당된 역할을 재정의합니다. 사용자 1은 VM 폴더 또는 VM A 및 B에 액세스할 수 없습니다.

그림 4-5. 예 3: 그룹 사용 권한을 재정의하는 사용자 사용 권한



vCenter 구성 요소에 대한 사용 권한 관리

사용 권한은 vCenter 개체 계층의 개체에 설정됩니다. 각 사용 권한은 개체를 그룹 또는 사용자 그리고 그룹 또는 사용자의 액세스 역할과 연결시킵니다. 예를 들어 하나의 가상 시스템 개체를 선택한 후 그룹 1에 읽기 전용 역할을 제공하는 사용 권한 하나를 추가하고 사용자 2에 관리자 역할을 제공하는 두 번째 사용 권한을 추가할 수 있습니다.

여러 개체에 대한 각기 다른 역할을 사용자 그룹에 할당하여 해당 사용자가 vSphere 환경에서 수행할 수 있는 작업을 제어합니다. 예를 들어 그룹이 호스트의 메모리를 구성할 수 있도록 허용하려면 해당 호스트를 선택하고 해당 그룹에 **호스트.구성.메모리 구성** 권한이 포함된 역할을 부여하는 사용 권한을 추가합니다.

vSphere Web Client에서 사용 권한을 관리하려면 다음 개념을 이해해야 합니다.

사용 권한

vCenter Server 개체 계층의 각 개체에는 연결된 사용 권한이 있습니다. 각 사용 권한은 그룹 또는 사용자가 개체에 대한 권한을 가지고 있는 하나의 그룹 또는 사용자에게 대해 지정됩니다.

사용자 및 그룹

vCenter Server 시스템에서, 인증된 사용자 또는 인증된 사용자의 그룹에만 권한을 할당할 수 있습니다. 사용자는 vCenter Single Sign-On을 통해 인증됩니다. vCenter Single Sign-On에서 인증하는 데 사용하는 ID 소스에서 사용자 및 그룹을 정의해야 합니다. Active Directory와 같은 ID 소스에서 도구를 사용하여 사용자 및 그룹을 정의합니다.

역할

역할을 사용하여 사용자가 수행하는 일련의 일반 작업을 기반으로 개체에 대한 사용 권한을 할당할 수 있습니다. 관리자와 같은 기본 역할은 vCenter Server에 미리 정의되어 있으며 변경할 수 없습니다. 리소스 풀 관리자와 같은 기타 역할은 미리 정의된 샘플 역할입니다. 사용자 지정 역할은 처음부터 생성하거나 샘플 역할을 복제 및 수정하여 생성할 수 있습니다.

권한

권한은 세분화된 액세스 제어입니다. 이러한 권한을 역할로 그룹화한 다음 사용자 또는 그룹에 매핑할 수 있습니다.

계층의 다른 수준에 있는 개체에 사용 권한을 할당할 수 있습니다. 예를 들어, 사용 권한을 특정 호스트 개체에 할당하거나 모든 호스트 개체를 포함하는 폴더 개체에 할당할 수 있습니다. [사용 권한의 계층적 상속](#)을 참조하십시오. 또한 글로벌 루트 개체에 사용 권한을 할당하여 모든 솔루션에 있는 개체 전체에 사용 권한을 적용할 수도 있습니다. [글로벌 사용 권한](#)을 참조하십시오.

인벤토리 개체에 사용 권한 추가

사용자와 그룹을 생성하고 역할을 정의한 후에는 사용자와 그룹 및 해당 역할을 관련 인벤토리 개체에 할당해야 합니다. 개체를 폴더로 이동한 후 폴더에 사용 권한을 설정하여 동일한 사용 권한을 동시에 여러 개체에 할당할 수 있습니다.

vSphere Web Client에서 사용 권한을 할당할 때 사용자 및 그룹 이름이 대소문자를 포함하여 Active Directory와 정확하게 일치해야 합니다. 이전 버전의 vSphere에서 업그레이드한 경우 그룹과 관련된 문제가 발생하면 대소문자 불일치 여부를 확인합니다.

사전 요구 사항

수정하려는 사용 권한이 있는 개체에 대해 **사용 권한.사용 권한 수정** 권한을 포함하는 역할이 있어야 합니다.

절차

- 1 vSphere Web Client 개체 탐색기에서 사용 권한을 할당하려는 개체를 찾습니다.
- 2 **관리** 탭을 클릭하고 **사용 권한**을 선택합니다.
- 3 추가 아이콘을 클릭하고 **추가**를 클릭합니다.
- 4 선택된 역할에 따라 정의된 권한이 있는 사용자 또는 그룹을 식별합니다.
 - a **도메인** 드롭다운 메뉴에서 사용자 또는 그룹이 위치한 도메인을 선택합니다.
 - b 검색 상자에 이름을 입력하거나 목록에서 이름을 선택합니다.
사용자 이름, 그룹 이름 및 설명이 검색됩니다.
 - c 사용자 또는 그룹을 선택하고 **추가**를 클릭합니다.
사용자 또는 **그룹** 목록에 이름이 추가됩니다.
 - d (선택 사항) **이름 확인**을 클릭하여 ID 소스에 해당 사용자 또는 그룹이 있는지 확인합니다.
 - e **확인**을 클릭합니다.
- 5 **할당된 역할** 드롭다운 메뉴에서 역할을 선택합니다.
개체에 할당되어 있는 역할이 메뉴에 나타납니다. 역할에 포함된 권한은 역할 제목 아래의 섹션에 나열됩니다.
- 6 (선택 사항) 전파를 제한하려면 **하위 개체로 전파** 확인란을 선택 취소합니다.
선택한 개체에만 역할이 적용되고 하위 개체에는 전파되지 않습니다.
- 7 **확인**을 클릭하여 사용 권한을 추가합니다.

사용 권한 변경

인벤토리 개체에 대해 사용자나 그룹 및 역할 쌍을 설정한 후, 사용자나 그룹에 지정된 역할을 변경하거나 **전파** 확인란의 설정을 변경할 수 있습니다. 사용 권한 설정을 제거할 수도 있습니다.

절차

- 1 vSphere Web Client 개체 탐색기에서 개체를 찾습니다.
- 2 **관리** 탭을 클릭하고 **사용 권한**을 선택합니다.
- 3 행 항목을 클릭하여 사용자 또는 그룹과 역할 쌍을 선택합니다.
- 4 **사용 권한에 대한 역할 변경**을 클릭합니다.
- 5 **할당된 역할** 드롭다운 메뉴에서 사용자나 그룹의 역할을 선택합니다.

- 6 할당된 인벤토리 개체의 하위 항목에 권한을 전파하려면 **전파** 확인란을 클릭한 후 **확인**을 클릭합니다.

사용 권한 제거

개별 사용자 또는 그룹의 개체 계층에서 개체에 대한 사용 권한을 제거할 수 있습니다. 제거하면 사용자는 개체에 대한 역할과 관련된 권한을 더 이상 가질 수 없습니다.

절차

- 1 vSphere Web Client 개체 탐색기에서 개체를 찾습니다.
- 2 **관리** 탭을 클릭하고 **사용 권한**을 선택합니다.
- 3 적절한 행 항목을 클릭하여 사용자/그룹 및 역할 쌍을 선택합니다.
- 4 **사용 권한 제거**를 클릭합니다.

결과

vCenter Server가 사용 권한 설정을 제거합니다.

사용 권한 유효성 검사 설정 변경

vCenter Server에서는 사용자 디렉토리에 있는 사용자와 그룹을 기준으로 사용자 및 그룹 목록을 주기적으로 검사합니다. 그런 다음 도메인에 더 이상 존재하지 않는 사용자나 그룹을 제거합니다. 검증을 사용하지 않도록 설정하거나 검증 간격을 변경할 수 있습니다. 수천 명의 사용자나 그룹을 포함하는 도메인이 있는 경우 또는 검색을 완료하는 데 시간이 오래 걸리는 경우 검색 설정 조정을 고려합니다.

vCenter Server 5.0 이전 vCenter Server 버전의 경우 이러한 설정이 vCenter Server와 연결된 Active Directory에 적용됩니다. vCenter Server 5.0 이상의 경우 이러한 설정이 vCenter Single Sign-On ID 소스에 적용됩니다.

참고 이 절차는 vCenter Server 사용자 목록에만 적용됩니다. ESXi 사용자 목록은 같은 방법으로 검색할 수 없습니다.

절차

- 1 vSphere Web Client 개체 탐색기에서 vCenter Server 시스템을 찾습니다.
- 2 **관리** 탭을 선택하고 **설정**을 클릭합니다.
- 3 **일반**을 클릭하고 **편집**을 클릭합니다.
- 4 **사용자 디렉토리**를 선택합니다.

5 필요에 따라 값을 변경합니다.

옵션	설명
사용자 디렉토리 시간 초과	Active Directory 서버에 연결할 때 사용되는 시간 초과 간격(초 단위)입니다. 이 값은 vCenter Server에서 선택한 도메인에 대해 검색이 실행되도록 허용하는 최대 시간을 지정합니다. 대형 도메인을 검색하는 데는 오랜 시간이 걸릴 수 있습니다.
쿼리 제한	vCenter Server에서 표시하는 최대 사용자 및 그룹 수를 설정하려면 이 확인란을 선택합니다.
쿼리 제한 크기	사용자 또는 그룹 선택 대화상자의 선택된 도메인에서 vCenter Server가 표시하는 최대 사용자 및 그룹 수를 지정합니다. 0을 입력하면 모든 사용자 및 그룹이 표시됩니다.
검증	검증을 사용하지 않도록 설정하려면 이 확인란의 선택을 취소합니다.
검증 기간	vCenter Server에서 사용 권한을 검증하는 빈도(분)를 지정합니다.

6 확인을 클릭합니다.

글로벌 사용 권한

글로벌 사용 권한은 여러 솔루션에 걸쳐 있는 글로벌 루트 개체에 적용됩니다(예: vCenter Server 및 vCenter Orchestrator 둘 다). 사용자 또는 그룹에 전체 개체 계층의 모든 개체에 대한 권한을 부여하려면 글로벌 사용 권한을 사용하십시오.

각 솔루션의 고유한 개체 계층에는 루트 개체가 있습니다. 글로벌 루트 개체는 각 솔루션 개체에 대한 상위 개체 역할을 합니다. 사용자 또는 그룹에 글로벌 사용 권한을 할당하고 각 사용자 또는 그룹의 역할을 결정할 수 있습니다. 역할은 일련의 권한을 지정합니다. 미리 정의된 역할을 할당하거나 사용자 지정 역할을 생성할 수 있습니다. **역할을 사용하여 권한 할당**를 참조하십시오. vCenter Server 사용 권한과 글로벌 사용 권한을 구분하는 것이 중요합니다.

vCenter Server 사용 권한

대부분의 경우 ESXi 호스트 또는 가상 시스템과 같은 vCenter Server 인벤토리 개체에 사용 권한을 적용합니다. 그럴 경우 사용자 또는 그룹이 해당 개체에 대해 일련의 권한, 즉 역할을 가지도록 지정합니다.

글로벌 사용 권한

글로벌 사용 권한은 배포의 각 인벤토리 계층에 있는 모든 개체를 보거나 관리할 수 있는 권한을 사용자 또는 그룹에 부여합니다.

글로벌을 할당하고 전파를 선택하지 않으면 이 사용 권한과 연결된 사용자 또는 그룹에게 계층의 개체에 대한 액세스 권한이 부여되지 않습니다. 역할 생성과 같은 일부 글로벌 기능에 대한 액세스 권한만 부여됩니다.

중요 글로벌 사용 권한을 사용할 때에는 주의하십시오. 전체 인벤토리 계층의 모든 개체에 사용 권한을 할당하는 것이 맞는지 확인하십시오.

글로벌 사용 권한 추가

글로벌 사용 권한을 사용하여 배포 내 모든 인벤토리 계층의 개체 전체에 대한 권한을 사용자 또는 그룹에 제공할 수 있습니다.

글로벌 사용 권한을 사용할 때에는 주의하십시오. 전체 인벤토리 계층의 모든 개체에 사용 권한을 할당하는 것이 맞는지 확인하십시오.

사전 요구 사항

이 작업을 수행하려면 모든 인벤토리 계층의 루트 개체에 대한 **.사용 권한.사용 권한 수정** 권한이 있어야 합니다.

절차

- 1 **관리**를 클릭하고 액세스 제어 영역에서 **글로벌 사용 권한**을 선택합니다.
- 2 **관리**를 클릭하고 사용 권한 추가 아이콘을 클릭합니다.
- 3 선택된 역할에 따라 정의된 권한이 있는 사용자 또는 그룹을 식별합니다.
 - a **도메인** 드롭다운 메뉴에서 사용자 또는 그룹이 위치한 도메인을 선택합니다.
 - b 검색 상자에 이름을 입력하거나 목록에서 이름을 선택합니다.
사용자 이름, 그룹 이름 및 설명이 검색됩니다.
 - c 사용자 또는 그룹을 선택하고 **추가**를 클릭합니다.
사용자 또는 **그룹** 목록에 이름이 추가됩니다.
 - d (선택 사항) **이름 확인**을 클릭하여 ID 소스에 해당 사용자 또는 그룹이 있는지 확인합니다.
 - e **확인**을 클릭합니다.
- 4 **할당된 역할** 드롭다운 메뉴에서 역할을 선택합니다.
개체에 할당되어 있는 역할이 메뉴에 나타납니다. 역할에 포함된 권한은 역할 제목 아래의 섹션에 나열됩니다.
- 5 대개의 경우 하위 항목으로 전파 확인란을 선택된 상태로 둡니다.
글로벌을 할당하고 전파를 선택하지 않으면 이 사용 권한과 연결된 사용자 또는 그룹에게 계층의 개체에 대한 액세스 권한이 부여되지 않습니다. 역할 생성과 같은 일부 글로벌 기능에 대한 액세스 권한만 부여됩니다.
- 6 **확인**을 클릭합니다.

태그 개체에 대한 사용 권한

vCenter Server 개체 계층에서, 태그 개체는 vCenter Server의 하위 항목이 아니지만 vCenter Server 루트 수준에서 생성됩니다. 여러 vCenter Server 인스턴스가 있는 환경에서 태그 개체는 vCenter Server 인스턴스 간에 공유됩니다. 태그 개체에 대한 사용 권한은 vCenter Server 개체 계층의 다른 개체에 대한 사용 권한과 다른 방식으로 작동합니다.

글로벌 사용 권한 또는 태그 개체에 할당된 사용 권한만 적용됨

특정 사용자에게 ESXi 호스트 또는 가상 시스템과 같은 vCenter Server 인벤토리 개체에 대한 사용 권한을 부여하는 경우 사용자는 해당 개체에서 태그 작업을 수행할 수 없습니다.

예를 들어 사용자인 Dana에게 호스트 TPA에 대한 **vSphere 태그 할당** 권한을 부여하는 경우 해당 권한은 Dana가 호스트 TPA에서 태그를 할당할 수 있는지 여부에 영향을 주지 못합니다. Dana는 루트 수준에서 **vSphere 태그 할당** 권한이 있어야 합니다. 즉, 글로벌 사용 권한이나 태그 개체에 대한 권한이 있어야 합니다.

표 4-1. 글로벌 사용 권한 및 태그 개체 사용 권한이 사용자가 수행할 수 있는 작업에 영향을 미치는 방식

글로벌 사용 권한	태그 수준 사용 권한	vCenter Server 개체 수준 사용 권한	유효한 사용 권한
태그 지정 권한이 할당되지 않음	Dana에게 태그에 대한 vSphere 태그 할당 또는 할당 취소 권한이 있음	Dana에게 ESXi 호스트 TPA에 대한 vSphere 태그 삭제 권한이 있음	Dana에게 태그에 대한 vSphere 태그 할당 또는 할당 취소 권한이 있음
Dana에게 vSphere 태그 할당 또는 할당 취소 권한이 있음	태그에 대해 권한이 할당되지 않음	Dana에게 ESXi 호스트 TPA에 대한 vSphere 태그 삭제 권한이 있음	Dana에게 vSphere 태그 할당 또는 할당 취소 글로벌 권한이 있음. 여기에는 태그 수준에서의 권한이 포함됨
태그 지정 권한이 할당되지 않음	태그에 대해 권한이 할당되지 않음	Dana에게 ESXi 호스트 TPA에 대한 vSphere 태그 할당 또는 할당 취소 권한이 있음	Dana에게 호스트 TPA를 포함하여 모든 개체에 대한 태그 지정 권한이 없음

태그 개체 사용 권한을 보완하는 글로벌 사용 권한

글로벌 사용 권한, 즉 루트 개체에 할당되는 사용 권한은 태그 개체에 대한 사용 권한이 더 제한적일 때 태그 개체에 대한 사용 권한을 보완합니다. vCenter Server 사용 권한은 태그 개체에 영향을 미치지 않습니다.

예를 들어 **vSphere 태그 삭제** 권한을 루트 수준에서, 즉 글로벌 사용 권한을 사용하여 사용자 Robin에게 할당한다고 가정합니다. 태그 운영을 위해 **vSphere 태그 삭제** 권한은 Robin에게 할당하지 않습니다. 이 경우 Robin은 글로벌 사용 권한이 있으므로 태그 운영에 대한 권한도 가집니다. 글로벌 사용 권한을 수정하는 경우가 아니면 권한을 제한할 수 없습니다.

표 4-2. 태그 수준 사용 권한을 보완하는 글로벌 사용 권한

글로벌 사용 권한	태그 수준 사용 권한	유효한 사용 권한
Robin에게 vSphere 태그 삭제 권한이 있음	Robin에게 태그에 대한 vSphere 태그 삭제 권한이 없음	Robin에게 vSphere 태그 삭제 권한이 있음
태그 지정 권한이 할당되지 않음	Robin에게 태그에 대해 할당된 vSphere 태그 삭제 권한이 없음	Robin에게 vSphere 태그 삭제 권한이 없음

태그 수준 사용 권한이 글로벌 사용 권한을 확장할 수 있음

태그 수준 사용 권한을 사용하여 글로벌 사용 권한을 확장할 수 있습니다. 이것은 사용자가 하나의 태그에 대해 글로벌 사용 권한과 태그 수준 사용 권한을 모두 가질 수 있음을 의미합니다.

표 4-3. 태그 수준 사용 권한을 확장하는 글로벌 사용 권한

글로벌 사용 권한	태그 수준 사용 권한	유효한 사용 권한
Lee에게 vSphere 태그 할당 또는 할당 취소 권한이 있음	Lee에게 vSphere 태그 삭제 권한이 있음	Lee에게 태그에 대한 vSphere 태그 할당 권한 및 vSphere 태그 삭제 권한이 있음
태그 지정 권한이 할당되지 않음	Lee에게 태그에 대해 할당된 vSphere 태그 삭제 권한이 있음	Lee에게 태그에 대해 vSphere 태그 삭제 권한이 있음

역할을 사용하여 권한 할당

역할이란 미리 정의된 권한의 집합입니다. 권한은 작업을 수행하고 속성을 읽기 위한 권한을 정의합니다. 예를 들어 가상 시스템 관리자 역할은 읽기 속성과 작업을 수행하기 위한 권한 집합으로 구성되어 있습니다. 이 역할은 사용자가 가상 시스템 특성을 읽고 변경할 수 있도록 허용합니다.

사용 권한을 할당할 때 사용자 또는 그룹을 역할과 쌍으로 구성하고 해당 쌍을 인벤토리 개체와 연결합니다. 단일 사용자 또는 그룹은 인벤토리에 있는 서로 다른 개체에 대해 각기 다른 역할을 가질 수 있습니다.

예를 들어 인벤토리에 풀 A와 풀 B라는 2개의 리소스 풀이 있는 경우 특정 사용자에게 풀 A에는 가상 시스템 사용자 역할을 할당하고 풀 B에는 읽기 전용 역할을 할당할 수 있습니다. 이렇게 할당된 경우 해당 사용자는 풀 A에 있는 가상 시스템을 켤 수 있지만 풀 B에 있는 가상 시스템은 볼 수만 있습니다.

vCenter Server는 기본적으로 다음과 같은 시스템 역할 및 샘플 역할을 제공합니다.

시스템 역할

시스템 역할은 영구적입니다. 이러한 역할과 연결된 권한은 편집할 수 없습니다.

샘플 역할

VMware는 자주 수행되는 특정 작업 조합에 대한 샘플 역할을 제공합니다. 이러한 역할은 복제하거나 수정하거나 제거할 수 있습니다.

참고 샘플 역할의 미리 정의된 설정을 손실하지 않으려면 먼저 역할을 복제한 후 복제본을 수정합니다. 샘플을 기본 설정으로 재설정할 수 없습니다.

사용자는 작업이 생성되는 시점에 해당 작업을 수행할 있는 권한이 포함된 역할을 가지고 있는 작업만 스케줄링할 수 있습니다.

참고 역할 및 권한에 대한 변경 사항은 관련된 사용자가 로그인되어 있더라도 즉시 적용됩니다. 검색의 경우에는 예외이며, 이 경우에는 사용자가 로그아웃했다가 다시 로그인해야 변경 사항이 적용됩니다.

vCenter Server 및 ESXi의 사용자 지정 역할

vCenter Server 및 vCenter Server가 관리하는 모든 개체에 대한 사용자 지정 역할이나 개별 호스트에 대한 사용자 지정 역할을 생성할 수 있습니다.

vCenter Server 사용자 지정 역할(권장)

vSphere Web Client의 역할 편집 기능을 사용하여 사용자 지정 역할을 생성하면 사용자의 필요에 맞는 권한 집합을 생성할 수 있습니다.

ESXi 사용자 지정 역할

CLI 또는 vSphere Client를 사용하여 개별 호스트에 대한 사용자 지정 역할을 생성할 수 있습니다. "vSphere Client를 통한 vSphere 관리" 설명서를 참조하십시오. vCenter Server에서는 사용자 지정 호스트 역할에 액세스할 수 없습니다.

vCenter Server를 통해 ESXi 호스트를 관리하는 경우에 호스트와 vCenter Server에서 모두 사용자 지정 역할을 유지하면 충돌이 발생하고 역할이 잘못 사용될 수 있습니다. 대부분의 경우 vCenter Server 역할을 정의하는 것이 좋습니다.

vCenter Server를 사용하여 호스트를 관리할 때는 해당 호스트와 연결된 사용 권한이 vCenter Server를 통해 생성되고 vCenter Server에 저장됩니다. 호스트에 직접 연결할 경우에는 호스트에서 직접 생성된 역할만 사용할 수 있습니다.

참고 사용자 지정 역할을 추가한 후 역할에 권한을 할당하지 않으면 해당 역할은 시스템 정의된 세 가지 권한인 **System.Anonymous**, **System.View** 및 **System.Read**가 포함된 읽기 전용 역할로 생성됩니다.



vSphere Web Client에서 역할 생성

(https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_egsyxkp4/uiConfId/49694343/)

vCenter Server 시스템 역할

역할이란 미리 정의된 권한의 집합입니다. 사용 권한을 개체에 추가할 때 사용자 또는 그룹을 역할과 쌍으로 구성해야 합니다. vCenter Server에는 변경할 수 없는 여러 시스템 역할이 포함되어 있습니다.

vCenter Server 시스템 역할

vCenter Server는 소수의 기본 역할을 제공합니다. 기본 역할에 연결된 권한은 수정할 수 없습니다. 기본 역할은 계층으로 구성되며, 각 역할은 이전 역할의 권한을 상속합니다. 예를 들어 관리자 역할은 읽기 전용 역할의 권한을 상속합니다. 사용자가 생성하는 역할은 시스템 역할의 권한을 상속하지 않습니다.

관리자 역할

개체에 대한 관리자 역할이 할당된 사용자는 해당 개체에 대한 모든 작업을 보고 수행할 수 있습니다. 이 역할에는 읽기 전용 역할에 내재된 모든 권한도 포함됩니다. 개체에 대한 관리자 역할로 수행하는 경우 개별 사용자 및 그룹에 권한을 할당할 수 있습니다. vCenter Server에서 관리자 역할로 수행하는 경우 기본 vCenter Single Sign-On ID 소스의 사용자 및 그룹에 권한을 할당할 수 있습니다. 지원되는 ID 서비스에는 Windows Active Directory 및 OpenLDAP 2.4가 포함됩니다.

설치가 완료되면 기본적으로 administrator@vsphere.local 사용자는 vCenter Single Sign-On과 vCenter Server 모두에서 관리자 역할을 갖습니다. 그런 다음 해당 사용자는 다른 사용자를 vCenter Server에 대한 관리자 역할과 연결할 수 있습니다.

권한 없음 역할

개체에 대한 권한 없음 역할이 할당된 사용자는 어떠한 방법으로든 개체를 보거나 변경할 수 없습니다. 기본적으로 새 사용자 및 그룹은 이 역할이 할당됩니다. 개체별로 역할을 변경할 수 있습니다.

administrator@vsphere.local 사용자, 루트 사용자 및 vpxuser는 기본적으로 권한 없음 역할이 할당되지 않는 유일한 사용자입니다. 대신 이들은 관리자 역할이 할당됩니다. 먼저 관리자 역할로 루트 수준에서 교체용 사용 권한을 생성한 후 이 사용 권한을 다른 사용자와 연결할 경우 루트 사용자의 사용 권한을 제거하거나 루트 사용자의 역할을 권한 없음으로 변경할 수 있습니다.

읽기 전용 역할

개체에 대한 읽기 전용 역할이 할당된 사용자는 개체의 상태 및 개체에 대한 세부 정보를 볼 수 있습니다. 이 역할을 통해 사용자는 가상 시스템, 호스트 및 리소스 풀 특성을 볼 수 있습니다. 사용자는 호스트에 대한 원격 콘솔을 볼 수 없습니다. 메뉴 및 도구 모음을 통한 모든 작업은 허용되지 않습니다.

사용자 지정 역할 생성

환경의 액세스 제어 요구에 맞게 vCenter Server 사용자 지정 역할을 생성할 수 있습니다.

다른 vCenter Server 시스템과 동일한 vCenter Single Sign-On 도메인의 일부인 vCenter Server 시스템에서 역할을 생성하거나 편집하는 경우 VMware 디렉토리 서비스(vmdir)는 변경 내용을 그룹 내의 다른 모든 vCenter Server 시스템에 전파합니다. 특정 사용자 및 개체에 대한 역할 할당은 vCenter Server 시스템 간에 공유되지 않습니다.

사전 요구 사항

관리자 권한이 있는 사용자로 로그인했는지 확인합니다.

절차

- 1 vSphere Web Client로 vCenter Server에 로그인합니다.
- 2 홈을 선택하고 **관리**를 클릭하고 **역할**을 클릭합니다.
- 3 **역할 생성 작업 (+)** 버튼을 클릭합니다.
- 4 새 역할의 이름을 입력하십시오.
- 5 역할의 권한을 선택하고 **확인**을 클릭합니다.

역할 복제

기존 역할의 복사본을 생성하고, 이름을 변경하고, 기존 역할을 편집할 수 있습니다. 역할을 복사하면 새 역할은 사용자나 그룹 및 개체에 자동으로 적용되지 않으며 사용자나 그룹 및 개체에 직접 할당해야 합니다.

다른 vCenter Server 시스템과 동일한 vCenter Single Sign-On 도메인의 일부인 vCenter Server 시스템에서 역할을 생성하거나 편집하는 경우 VMware 디렉토리 서비스(vmdir)는 변경 내용을 그룹 내의 다른 모든 vCenter Server 시스템에 전파합니다. 특정 사용자 및 개체에 대한 역할 할당은 vCenter Server 시스템 간에 공유되지 않습니다.

사전 요구 사항

관리자 권한이 있는 사용자로 로그인했는지 확인합니다.

절차

- 1 vSphere Web Client로 vCenter Server에 로그인합니다.
- 2 홈을 선택하고 **관리**를 클릭하고 **역할**을 클릭합니다.
- 3 역할을 선택하고 **역할 복제 작업** 아이콘을 클릭합니다.
- 4 복제된 역할의 이름을 입력합니다.
- 5 역할의 권한을 선택하거나 선택 취소하고 **확인**을 클릭합니다.

역할 편집

역할을 편집할 때 이 역할에 선택된 권한을 변경할 수 있습니다. 작업이 완료되면 편집된 역할이 할당된 사용자 또는 그룹에 이러한 권한이 적용됩니다.

다른 vCenter Server 시스템과 동일한 vCenter Single Sign-On 도메인의 일부인 vCenter Server 시스템에서 역할을 생성하거나 편집하는 경우 VMware 디렉토리 서비스(vmdir)는 변경 내용을 그룹 내의 다른 모든 vCenter Server 시스템에 전파합니다. 특정 사용자 및 개체에 대한 역할 할당은 vCenter Server 시스템 간에 공유되지 않습니다.

사전 요구 사항

관리자 권한이 있는 사용자로 로그인했는지 확인합니다.

절차

- 1 vSphere Web Client로 vCenter Server에 로그인합니다.
- 2 홈을 선택하고 **관리**를 클릭하고 **역할**을 클릭합니다.
- 3 역할을 선택하고 **역할 편집 작업** 버튼을 클릭합니다.
- 4 역할의 권한을 선택하거나 선택 취소하고 **확인**을 클릭합니다.

역할 및 권한에 대한 모범 사례

역할 및 사용 권한에 대한 모범 사례를 활용하면 vCenter Server 환경의 보안을 강화하고 관리 용이성을 높일 수 있습니다.

vCenter Server 환경에서 역할 및 사용 권한을 구성할 때 다음의 모범 사례를 따르는 것이 좋습니다.

- 가능하면 개별 사용자보다는 그룹에 역할을 할당하여 해당 그룹에 권한을 부여합니다.
- 사용 권한이 필요한 개체에만 사용 권한을 부여하고, 권한이 반드시 있어야 하는 사용자 또는 그룹에만 해당 권한을 할당합니다. 사용 권한 수를 최소화하면 사용 권한 구조를 보다 쉽게 이해하고 관리할 수 있습니다.

- 그룹에 제한적인 역할을 할당할 경우에는 관리자 사용자나 관리 권한을 가진 사용자가 그룹에 포함되어 있지 않은지 확인합니다. 이러한 사용자가 만약 있으면 그룹에 제한적인 역할을 할당한 인벤토리 계층의 일부에서 관리자의 권한이 의도하지 않게 제한될 수 있습니다.
- 폴더를 사용하여 개체를 그룹화합니다. 예를 들어 한 호스트 집합에는 수정 권한을 부여하고 다른 호스트 집합에는 보기 권한을 부여하려는 경우 각 호스트 집합을 하나의 폴더에 배치합니다.
- 사용 권한을 루트 vCenter Server 개체에 추가할 때에는 주의합니다. 루트 수준의 권한을 가진 사용자는 vCenter Server 설정, 역할, 사용자 지정 특성과 같은 vCenter Server의 글로벌 데이터에 액세스할 수 있습니다.
- 대부분의 경우, 개체에 사용 권한을 할당할 때에는 전파 기능을 사용합니다. 이 기능을 사용하면 인벤토리 계층에 새 개체를 삽입했을 때 해당 개체에 사용 권한이 상속되어 사용자가 개체에 액세스할 수 있습니다.
- 특정 사용자 또는 그룹이 개체 계층의 특정 영역에 있는 개체에 액세스하지 못하도록 계층의 해당 영역을 숨기고 싶다면 권한 없음 역할을 사용합니다.
- 라이선스 변경 내용은 사용자에게 모든 vCenter Server 시스템에 대한 권한이 없는 경우에도 동일한 Platform Services Controller 또는 동일한 vCenter Single Sign-On 도메인의 Platform Services Controller에 연결된 모든 vCenter Server 시스템에 전파됩니다.

일반 작업에 필요한 권한

대부분 작업을 수행하려면 인벤토리에 있는 둘 이상의 개체에 대해 권한이 필요합니다. 작업 수행에 필요한 권한과 적합한 샘플 역할(적용 가능한 경우)을 검토해 볼 수 있습니다.

아래 표에는 둘 이상의 권한이 필요한 일반 작업이 나와 있습니다. 한 명의 사용자와 미리 정의된 역할 하나를 쌍으로 연결하여 인벤토리 개체에 사용 권한을 추가하거나 여러 번 사용할 것으로 예상하는 권한 집합으로 사용자 지정 역할을 생성할 수 있습니다.

수행하려는 작업이 이 표에 없는 경우 다음 규칙을 사용하면 특정 작업을 허용하기 위해 사용 권한을 할당해야 하는 위치를 결정하는 데 도움이 될 수 있습니다.

- 가상 디스크를 생성하거나 스냅샷을 생성하는 것처럼 스토리지 공간을 사용하는 모든 작업에는 대상 데이터스토어에 대한 **데이터스토어.공간 할당** 권한과 작업 자체를 수행할 수 있는 권한이 필요합니다.
- 인벤토리 계층에서 개체를 이동하기 위해서는 개체 자체, 소스 상위 개체(예: 폴더 또는 클러스터) 및 대상 상위 개체에 대한 적절한 권한이 필요합니다.
- 각 호스트와 개체에는 해당 호스트 또는 클러스터의 모든 리소스가 들어 있는 고유한 암시적 리소스 풀이 있습니다. 가상 시스템을 호스트나 클러스터에 직접 배포하려면 **리소스.리소스 풀에 가상 시스템 할당** 권한이 필요합니다.

표 4-4. 일반 작업에 필요한 권한

작업	필요한 권한	적용 가능한 역할
가상 시스템 생성	대상 폴더 또는 데이터 센터에서 다음을 수행: <ul style="list-style-type: none"> ■ 가상 시스템.인벤토리.새로 생성 ■ 가상 시스템.구성.새 디스크 추가(새 가상 디스크를 생성하는 경우) ■ 가상 시스템.구성.기존 디스크 추가(기존 가상 디스크를 사용하는 경우) ■ 가상 시스템.구성.원시 디바이스(RDM 또는 SCSI 패스스루 디바이스를 사용하는 경우) 	관리자
	대상 호스트, 클러스터 또는 리소스 풀에서 다음을 수행: 리소스.리소스 풀에 가상 시스템 할당	리소스 풀 관리자 또는 관리자
	대상 데이터스토어 또는 데이터스토어를 포함한 폴더에서 다음을 수행: 데이터스토어.공간 할당	데이터스토어 소비자 또는 관리자
	가상 시스템이 할당될 네트워크에서 다음을 수행: 네트워크.네트워크 할당	네트워크 소비자 또는 관리자
템플릿에서 가상 시스템 배포	대상 폴더 또는 데이터 센터에서 다음을 수행: <ul style="list-style-type: none"> ■ 가상 시스템.인벤토리.기존 항목에서 생성 ■ 가상 시스템.구성.새 디스크 추가 	관리자
	템플릿 또는 템플릿의 폴더에서 다음을 수행: 가상 시스템.프로비저닝.템플릿 배포	관리자
	대상 호스트, 클러스터 또는 리소스 풀에서 다음을 수행: 리소스.리소스 풀에 가상 시스템 할당	관리자
	대상 데이터스토어 또는 데이터스토어의 폴더에서 다음을 수행: 데이터스토어.공간 할당	데이터스토어 소비자 또는 관리자
	가상 시스템이 할당될 네트워크에서 다음을 수행: 네트워크.네트워크 할당	네트워크 소비자 또는 관리자
가상 시스템 스냅샷 작성	가상 시스템 또는 가상 시스템의 폴더에서 다음을 수행: 가상 시스템.스냅샷 관리.스냅샷 생성	가상 시스템 고급 사용자 또는 관리자
가상 시스템을 리소스 풀로 이동	가상 시스템 또는 가상 시스템의 폴더에서 다음을 수행: <ul style="list-style-type: none"> ■ 리소스.리소스 풀에 가상 시스템 할당 ■ 가상 시스템.인벤토리.이동 	관리자
	대상 리소스 풀에서 다음을 수행: 리소스.리소스 풀에 가상 시스템 할당	관리자

표 4-4. 일반 작업에 필요한 권한 (계속)

작업	필요한 권한	적용 가능한 역할
가상 시스템에 게스트 운영 체제 설치	<p>가상 시스템 또는 가상 시스템의 폴더에서 다음을 수행:</p> <ul style="list-style-type: none"> ■ 가상 시스템.상호 작용.질문에 응답 ■ 가상 시스템.상호 작용.콘솔 상호 작용 ■ 가상 시스템.상호 작용.디바이스 연결 ■ 가상 시스템.상호 작용.전원 끄기 ■ 가상 시스템.상호 작용.전원 켜기 ■ 가상 시스템.상호 작용.재설정 ■ 가상 시스템.상호 작용.CD 미디어 구성(CD에서 설치하는 경우) ■ 가상 시스템.상호 작용.플로피 미디어 구성(플로피 디스크에서 설치하는 경우) ■ 가상 시스템.상호 작용.VMware Tools 설치 <p>설치 미디어 ISO 이미지가 들어 있는 데이터스토어에서 다음을 수행:</p> <p>데이터스토어.데이터스토어 찾아보기(데이터스토어의 ISO 이미지에서 설치하는 경우)</p> <p>설치 미디어 ISO 이미지를 업로드하는 데이터스토어에서 다음을 수행:</p> <ul style="list-style-type: none"> ■ 데이터스토어.데이터스토어 찾아보기 ■ 데이터스토어.하위 수준 파일 작업 	가상 시스템 고급 사용자 또는 관리자
vMotion으로 가상 시스템 마이그레이션	<p>가상 시스템 또는 가상 시스템의 폴더에서 다음을 수행:</p> <ul style="list-style-type: none"> ■ 리소스.전원이 켜진 가상 시스템 마이그레이션 ■ 리소스.리소스 풀에 가상 시스템 할당(대상이 소스와 다른 리소스 풀인 경우) <p>대상 호스트, 클러스터 또는 리소스 풀에서 다음을 수행(소스와 다른 경우):</p> <p>리소스.리소스 풀에 가상 시스템 할당</p>	리소스 풀 관리자 또는 관리자
가상 시스템 월드 마이그레이션(재배치)	<p>가상 시스템 또는 가상 시스템의 폴더에서 다음을 수행:</p> <ul style="list-style-type: none"> ■ 리소스.전원이 꺼진 가상 시스템 마이그레이션 ■ 리소스.리소스 풀에 가상 시스템 할당(대상이 소스와 다른 리소스 풀인 경우) <p>대상 호스트, 클러스터 또는 리소스 풀에서 다음을 수행(소스와 다른 경우):</p> <p>리소스.리소스 풀에 가상 시스템 할당</p> <p>대상 데이터스토어에서 다음을 수행(소스와 다른 경우):</p> <p>데이터스토어.공간 할당</p>	리소스 풀 관리자 또는 관리자
Storage vMotion을 사용하여 가상 시스템 마이그레이션	<p>가상 시스템 또는 가상 시스템의 폴더에서 다음을 수행:</p> <p>리소스.전원이 켜진 가상 시스템 마이그레이션</p> <p>대상 데이터스토어에서 다음을 수행:</p> <p>데이터스토어.공간 할당</p>	리소스 풀 관리자 또는 관리자
호스트를 클러스터로 이동	<p>호스트에서 다음을 수행:</p> <p>호스트.인벤토리.클러스터에 호스트 추가</p> <p>대상 클러스터에서 다음을 수행:</p> <p>호스트.인벤토리.클러스터에 호스트 추가</p>	관리자

ESXi 하이퍼바이저 아키텍처에는 CPU 분리, 메모리 분리 및 디바이스 분리와 같은 여러 내장 보안 기능이 있습니다. 향상된 보안을 위해 잠금 모드, 인증서 교체 및 스마트 카드 인증과 같은 추가 기능을 구성할 수 있습니다.

ESXi 호스트는 방화벽으로도 보호됩니다. 필요에 따라 송수신 트래픽을 위해 포트를 열 수 있지만 서비스 및 포트에 대한 액세스를 제한해야 합니다. ESXi 잠금 모드를 사용하고 ESXi Shell에 대한 액세스를 제한하면 해당 환경의 보안을 한층 더 강화할 수 있습니다. vSphere 6.0부터 ESXi 호스트는 인증서 인프라에 참여합니다. 기본적으로 VMCA(VMware 인증 기관)에서 서명된 인증서를 사용하여 호스트가 프로비저닝됩니다.

ESXi 보안에 대한 자세한 내용은 VMware 백서 "VMware vSphere Hypervisor 보안" 을 참조하십시오.

본 장은 다음 항목을 포함합니다.

- 스크립트를 사용하여 호스트 구성 설정 관리
- 호스트 프로파일을 사용하여 ESXi 호스트 구성
- 일반 ESXi 보안 권장 사항
- ESXi 호스트에 대한 인증서 관리
- 보안 프로파일을 사용하여 호스트 사용자 지정
- ESXi에 대한 사용 권한 할당
- Active Directory를 통해 ESXi 사용자 관리
- vSphere Authentication Proxy 사용
- ESXi 보안 모범 사례
- ESXi에 대한 스마트 카드 인증 구성
- ESXi SSH 키
- ESXi Shell 사용
- ESXi 웹 프록시 설정 수정
- vSphere Auto Deploy 보안 고려 사항
- ESXi 로그 파일 관리

스크립트를 사용하여 호스트 구성 설정 관리

다수의 호스트가 포함된 환경에서는 스크립트를 사용한 호스트 관리가 vSphere Web Client에서 호스트를 관리하는 것보다 빠르고 오류 발생률이 낮습니다.

vSphere에는 호스트 관리를 위한 여러 스크립팅 언어가 포함되어 있습니다. 참조 정보 및 프로그래밍 팁은 "vSphere 명령줄 설명서" 및 "vSphere API/SDK 설명서"를 참조하고 스크립트로 작성된 관리에 대한 추가 팁은 VMware 커뮤니티를 참조하십시오. vSphere 관리자 설명서는 관리를 위한 vSphere Web Client 사용을 중점적으로 다룹니다.

vSphere PowerCLI

VMware vSphere PowerCLI는 vSphere API에 대한 Windows PowerShell 인터페이스입니다.

vSphere PowerCLI에는 vSphere 구성 요소 관리를 위한 PowerShell cmdlet이 포함되어 있습니다.

vSphere PowerCLI에는 200개가 넘는 cmdlet, 샘플 스크립트 집합, 관리 및 자동화를 위한 기능 라이브러리가 포함되어 있습니다. "vSphere PowerCLI 설명서"를 참조하십시오.

vCLI(vSphere Command-Line Interface)

vCLI에는 ESXi 호스트 및 가상 시스템 관리를 위한 명령 집합이 포함되어 있습니다. vSphere SDK for Perl도 설치하는 설치 관리자는 Windows 또는 Linux 시스템을 실행하고 ESXCLI 명령, vicfg-명령 및 기타 vCLI 명령 집합을 설치합니다. "vSphere Command-Line Interface 설명서"를 참조하십시오.

vSphere 6.0부터는 vCloud Suite SDK for Python과 같은 vCloud Suite SDK에 대한 스크립팅 인터페이스 중 하나를 사용할 수도 있습니다.

절차

- 1 제한된 권한을 가진 사용자 지정 역할을 생성합니다.

예를 들어 호스트 관리를 위한 권한 집합을 가지고 있지만 가상 시스템, 스토리지 또는 네트워킹 관리를 위한 권한을 가지고 있지 않은 역할을 생성하는 것을 고려합니다. 사용할 스크립트가 정보를 추출하기만 하는 경우 호스트에 대한 읽기 전용 권한을 가진 역할을 생성할 수 있습니다.

- 2 vSphere Web Client에서 서비스 계정을 생성하고 사용자 지정 역할에 할당합니다.

특정 호스트에 대한 액세스 권한을 매우 제한하고자 하는 경우 각기 다른 수준의 액세스 권한을 가진 여러 사용자 지정 역할을 생성할 수 있습니다.

3 매개 변수 검사 또는 수정을 수행하는 스크립트를 작성한 후 실행합니다.

예를 들어 다음과 같이 호스트의 셸 대화형 시간 초과를 검사하거나 설정할 수 있습니다.

언어	명령
vCLI(ESXCLI)	<pre>esxcli <conn_options> system settings advanced get / UserVars/ESXiShellTimeout esxcli --formatter=csv --format-param=fields="Path,Int Value" system settings advanced list grep /UserVars/ ESXiShellTimeout</pre>
PowerCLI	<pre>#List UserVars.ESXiShellInteractiveTimeout for each host Get-VMHost Select Name, @{N="UserVars.ESXiShellInteractiveTimeout";E={\$_ Get-AdvancedSetting -Name UserVars.ESXiShellInteractiveTimeout Select -ExpandProperty Value}} # Set UserVars.ESXiShellTimeout to 900 on all hosts Get-VMHost Foreach { Get-AdvancedSetting -Entity \$_ -Name UserVars.ESXiShellInteractiveTimeout Set- AdvancedSetting -Value 900 }</pre>

4 대규모 환경에서 각기 다른 액세스 권한을 가진 역할을 생성하고 수행할 작업에 따라 호스트를 폴더로 그룹화합니다. 그런 다음 다양한 서비스 계정에서 다른 폴더를 통해 스크립트를 실행합니다.

5 명령을 실행한 후에 발생한 변경 내용을 확인합니다.

호스트 프로파일을 사용하여 ESXi 호스트 구성

호스트 프로파일을 통해 ESXi 호스트에 대해 표준 구성을 설정하고 이러한 구성 설정에 대한 규정 준수를 자동화할 수 있습니다. 호스트 프로파일을 통해 메모리, 스토리지, 네트워킹 등을 포함하여 호스트 구성의 다양한 측면을 제어할 수 있습니다.

vSphere Web Client에서 참조 호스트에 대한 호스트 프로파일을 구성하고 호스트 프로파일을 참조 호스트의 특징을 공유하는 모든 호스트에 적용할 수 있습니다. 또한 호스트 프로파일을 사용하여 호스트에서 호스트 구성 변경 내용을 모니터링할 수도 있습니다. "vSphere 호스트 프로파일" 설명서를 참조하십시오.

호스트 프로파일을 클러스터에 연결하여 클러스터의 모든 호스트에 적용할 수도 있습니다.

절차

- 1 규격에 맞게 참조 호스트를 설정하고 호스트 프로파일을 생성합니다.
- 2 프로파일을 호스트나 클러스터에 연결합니다.
- 3 참조 호스트의 호스트 프로파일을 다른 호스트나 클러스터에 적용합니다.

일반 ESXi 보안 권장 사항

인증되지 않은 침입 및 잘못된 이용으로부터 ESXi 호스트를 보호하기 위해 VMware는 몇 가지 매개 변수, 설정 및 작업에 제약을 가합니다. 구성 요구 사항을 충족하기 위해 이 제약 조건을 완화할 수 있습니다. 이 경우 신뢰할 수 있는 환경에서 작업 중이어야 하고 네트워크 전체 및 호스트에 연결된 디바이스를 보호하기 위한 다른 보안 대책을 충분히 적용한 상태여야 합니다.

기본 제공 보안 기능

호스트에 대한 위험이 다음과 같이 기본적으로 최소화됩니다.

- ESXi Shell 및 SSH는 기본적으로 사용하지 않도록 설정됩니다.
- 제한된 수의 방화벽 포트만 기본적으로 열립니다. 특정 서비스에 연결된 추가 방화벽 포트를 명시적으로 열 수 있습니다.
- ESXi는 해당 기능을 관리하는 데 필수적인 서비스만 실행합니다. 이 배포는 ESXi를 실행하는 데 필요한 기능에 제한됩니다.
- 기본적으로 호스트에 대한 관리 액세스에 필요하지 않은 모든 포트는 닫혀 있습니다. 추가 서비스가 필요한 경우에는 포트를 명시적으로 열어야 합니다.
- 기본적으로 보안에 취약한 암호화는 사용하지 않도록 설정되며 클라이언트로부터의 통신에는 SSL 보안이 적용됩니다. 채널의 보안 유지에서 사용되는 정확한 알고리즘은 SSL 핸드셰이크에 따라 다릅니다. ESXi에서 생성된 기본 인증서는 RSA 암호화가 적용된 PKCS#1 SHA-256을 서명 알고리즘으로 사용합니다.
- 웹 클라이언트의 액세스를 지원하기 위해 ESXi에서 내부적으로 사용하는 Tomcat 웹 서비스는 웹 클라이언트를 통한 관리 및 모니터링에 필요한 기능만 실행하도록 수정되었습니다. 따라서 ESXi는 다양한 용도로 Tomcat에 대해 보고되는 보안 문제에 취약하지 않습니다.
- VMware는 ESXi 보안에 영향을 미칠 수 있는 모든 보안 경고를 모니터링하고 필요한 경우 보안 패치를 실행합니다.
- FTP 및 Telnet과 같은 안전하지 않은 서비스는 설치되지 않으며 이러한 서비스용 포트는 기본적으로 닫혀 있습니다. SSH 및 SFTP와 같은 더 안전한 서비스를 쉽게 사용할 수 있으므로 안전한 서비스 대신에 이러한 안전하지 않은 서비스를 사용하지 마십시오. 예를 들어 SSH를 사용할 수 없지만 Telnet을 사용해야 하는 경우 SSL 기반 Telnet을 사용하여 가상 직렬 포트에 액세스합니다.

안전하지 않은 서비스를 사용해야 하고 호스트에 대한 충분한 보안 대책을 구현한 경우 이를 지원하기 위해 포트를 명시적으로 열 수 있습니다.

추가 보안 대책

호스트 보안 및 관리를 평가할 때는 다음 권장 사항을 고려하십시오.

액세스 제한

DCUI(Direct Console User Interface)에 대한 액세스를 사용하도록 설정한 경우 ESXi Shell 또는 SSH는 강한 액세스 보안 정책을 시행합니다.

ESXi Shell에는 호스트의 특정 부분에 대한 액세스 권한이 있습니다. ESXi Shell 로그인 액세스는 신뢰할 수 있는 사용자에게만 제공하십시오.

관리 호스트에 직접 액세스하지 않음

vSphere Web Client를 사용하여 vCenter Server로 관리되는 ESXi 호스트를 관리합니다. vSphere Client에서 관리 호스트에 직접 액세스해서는 안 되며, 호스트의 DCUI에서 관리 호스트를 변경해서는 안 됩니다.

스크립팅 인터페이스 또는 API를 사용하여 호스트를 관리하는 경우 호스트를 직접 대상으로 하지 마십시오. 대신 호스트를 관리하는 vCenter Server 시스템을 대상으로 하고 호스트 이름을 지정하십시오.

vSphere Client 또는 VMware CLI 또는 API를 사용하여 독립형 ESXi 호스트 관리

vSphere Client, VMware CLI 또는 API 중 하나를 사용하여 ESXi 호스트를 관리합니다. 문제 해결을 위해서만 DCUI 또는 ESXi Shell에서 루트 사용자로 호스트에 액세스하십시오. ESXi Shell을 사용하도록 결정한 경우 계정의 액세스를 제한하고 시간 제한을 설정하십시오.

ESXi 구성 요소를 업그레이드할 때는 VMware 소스만 사용합니다.

호스트는 관리 인터페이스 또는 수행해야 하는 작업을 지원하기 위해 다양한 타사 패키지를 실행합니다. VMware는 VMware가 아닌 소스를 통한 이러한 패키지의 업그레이드를 지원하지 않습니다. 다른 소스의 다운로드나 패치를 사용하면 관리 인터페이스 보안 또는 기능이 제대로 작동하지 않을 수 있습니다. 타사 벤더 사이트 및 VMware 기술 자료에서 보안 경고를 정기적으로 확인하십시오.

참고 VMware 보안 권고(<http://www.vmware.com/security/>)를 따르십시오.

ESXi 암호 및 계정 잠금

ESXi 호스트에 대해 미리 정의된 요구 사항이 있는 암호를 사용해야 합니다.

Security.PasswordQualityControl 고급 옵션을 사용하여 암호 문구를 허용하거나 필수 길이 및 문자 클래스 요구 사항을 변경할 수 있습니다.

ESXi에서는 암호 관리 및 제어를 위해 Linux PAM 모듈 pam_passwdqc를 사용합니다. 자세한 정보는 pam_passwdqc의 manpage를 참조하십시오.

참고 ESXi 암호에 대한 기본 요구 사항은 특정 릴리스에서 다음 릴리스로 변경될 수 있습니다.

Security.PasswordQualityControl 고급 옵션을 사용하여 기본 암호 제한을 확인 및 변경할 수 있습니다.

ESXi 암호

ESXi에서는 DCUI(Direct Console User Interface), ESXi Shell, SSH 또는 vSphere Client로부터의 액세스에 대해 암호 요구 사항을 적용합니다. 기본적으로 암호를 생성할 때 소문자, 대문자, 숫자 및 특수 문자(예: 밑줄 또는 대시)와 같은 4개의 문자 클래스의 문자 조합을 포함해야 합니다.

참고 암호를 시작할 때의 대문자는 사용된 문자 클래스 수에 포함되지 않습니다. 암호가 끝날 때의 숫자도 사용된 문자 클래스 수에 포함되지 않습니다.

사전에 나오는 단어 또는 사전에 나오는 단어의 일부를 암호에 사용할 수 없습니다.

ESXi 암호 예

다음 암호 후보는 옵션이 다음과 같이 설정되었을 때 설정 가능한 암호를 보여 줍니다.

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

이 설정에서는 처음 3개 항목이 사용되지 않도록 설정되기 때문에 1개 또는 2개의 문자 클래스 및 암호 문구가 있는 암호가 허용되지 않습니다. 3개 및 4개의 문자 클래스의 암호에는 7개의 문자가 필요합니다. 자세한 내용은 `pam_passwdqc manpage`를 참조하십시오.

이러한 설정에서는 다음 암호가 허용됩니다.

- xQaTEhb!: 세 가지 문자 클래스의 문자 8개를 포함합니다.
- xQaT3#A: 네 가지 문자 클래스의 문자 7개를 포함합니다.

다음 암호 후보는 요구 사항을 충족하지 않습니다.

- Xqat3hi: 대문자로 시작되기 때문에 유효한 문자 클래스 수가 2개로 줄어듭니다. 필수 문자 클래스의 수는 최소 3개입니다.
- xQaTEh2: 숫자로 끝나기 때문에 유효한 문자 클래스가 2개로 줄어듭니다. 필수 문자 클래스의 수는 최소 3개입니다.

ESXi 암호 문구

암호 대신 암호 문구를 사용할 수도 있지만 암호 문구는 기본적으로 사용되지 않도록 설정됩니다.

vSphere Web Client에서 `Security.PasswordQualityControl` 고급 옵션을 사용하여 이 설정 또는 다른 설정을 변경할 수 있습니다.

예를 들어 옵션을 다음으로 변경할 수 있습니다.

```
retry=3 min=disabled,disabled,16,7,7
```

이 예에서는 공백으로 구분된 최소 16자 및 최소 3단어의 암호 문구를 허용합니다.

레거시 호스트의 경우 `/etc/pamd/passwd` 파일 변경이 계속 지원되지만 이후 릴리스에서는 더 이상 지원되지 않습니다. 대신 `Security.PasswordQualityControl` 고급 옵션을 사용합니다.

기본 암호 제한 변경

ESXi 호스트에 대해 Security.PasswordQualityControl 고급 옵션을 사용하여 암호 또는 암호 문구에 대한 기본 제한을 변경할 수 있습니다. ESXi 고급 옵션 설정에 대한 자세한 내용은 "vCenter Server 및 호스트 관리" 설명서를 참조하십시오.

예를 들어, 다음과 같이 최소 15개의 문자와 최소 4개의 단어가 필요하도록 기본값을 변경할 수 있습니다.

```
retry=3 min=disabled,disabled,15,7,7 passphrase=4
```

자세한 내용은 pam_passwdqc의 manpage를 참조하십시오.

참고 pam_passwdqc에 대한 가능한 모든 옵션의 조합이 테스트되지는 않았습니다. 기본 암호 설정을 변경한 후 추가 테스트를 수행합니다.

ESXi 계정 잠금 동작

vSphere 6.0부터 SSH 및 vSphere Web Services SDK를 통한 액세스에 대해 계정 잠금이 지원됩니다. DCUI(Direct Console Interface) 및 ESXi Shell은 계정 잠금을 지원하지 않습니다. 기본적으로, 계정이 잠기기 전에 최대 10번의 시도 실패가 허용되고 2분 후에는 계정에 대한 잠금이 해제됩니다.

로그인 동작 구성

다음 고급 옵션을 사용하여 ESXi 호스트에 대한 로그인 동작을 구성할 수 있습니다.

- Security.AccountLockFailures. 사용자 계정이 잠길 때까지 허용되는 최대 로그인 시도 실패 횟수입니다. 0으로 설정하면 계정 잠금 사용이 해제됩니다.
- Security.AccountUnlockTime. 사용자가 잠기게 되는 시간(초)입니다.

ESXi 고급 옵션 설정에 대한 자세한 내용은 "vCenter Server 및 호스트 관리" 설명서를 참조하십시오.

ESXi 네트워킹 보안 권장 사항

ESXi 환경의 보안을 유지하기 위해서는 네트워크 트래픽을 분리하는 일이 필수적입니다. 필요한 액세스 및 분리 수준은 네트워크마다 다릅니다.

ESXi 호스트에서는 여러 가지 네트워크를 사용합니다. 각각의 네트워크에 대해 적절한 보안 수단을 사용하고 특정 애플리케이션 및 기능에 대해 트래픽을 분리합니다. 예를 들어 vSphere vMotion 트래픽이 가상 시스템이 포함된 네트워크를 통해 이동하지 않도록 합니다. 분리 기능을 활용하면 스누핑이 방지됩니다. 분리된 네트워크를 유지하면 성능 측면에서도 도움이 됩니다.

- vSphere 인프라 네트워크는 VMware vSphere vMotion®, VMware vSphere Fault Tolerance, 스토리지 같은 기능에 사용됩니다. 이러한 네트워크는 해당 네트워크의 특정 기능에 대해 분리되는 것으로 간주되며 단일 물리적 서버 랙 집합 외부로 라우팅되지 않는 경우가 많습니다.

- 관리 네트워크에서는 클라이언트 트래픽, CLI(명령줄 인터페이스) 또는 API 트래픽, 타사 소프트웨어 트래픽을 일반적인 트래픽에서 분리합니다. 이 네트워크에는 시스템 관리자, 네트워크 관리자 및 보안 관리자만 액세스할 수 있어야 합니다. 관리 네트워크에 대한 액세스를 보호하려면 점프 박스(jump-box) 또는 VPN(Virtual Private Network)을 사용하십시오. 이 네트워크 내에서는 잠재적인 맬웨어의 원인을 엄격하게 제어할 수 있습니다.
- 가상 시스템 트래픽은 하나 또는 여러 개의 네트워크를 통해 이동할 수 있습니다. 가상 네트워크 컨트롤러에 방화벽 규칙을 설정하는 가상 방화벽 솔루션을 사용하여 가상 시스템의 분리 수준을 향상시킬 수 있습니다. 이러한 설정은 vSphere 환경 내에서 가상 시스템이 호스트 간에 마이그레이션될 때 가상 시스템과 함께 옮겨집니다.

MOB(Managed Object Browser) 사용 안 함

MOB(Managed Object Browser)에서는 VMkernel 개체 모델을 탐색할 수 있습니다. 그러나 OU가 MOB(Managed Object Browser)를 사용하여 호스트 구성을 변경할 수 있기 때문에 공격자는 이 인터페이스를 사용하여 악의적인 구성 변경이나 작업을 수행할 수 있습니다. 디버깅 목적에만 MOB(Managed Object Browser)를 사용하고 운영 시스템에서는 사용하지 않도록 설정하십시오.

vSphere 6.0부터 MOB는 기본적으로 사용하지 않도록 설정됩니다. 하지만 특정 태스크(예: 시스템에서 이전 인증서 추출)의 경우 MOB를 사용해야 합니다.

절차

- 1 vSphere Web Client에서 호스트를 선택하고 **고급 시스템 설정**으로 이동합니다.
- 2 **Config.HostAgent.plugins.solo.enableMob**의 값을 확인하고 필요한 경우 변경합니다.

ESXi Shell에서 vim-cmd 사용은 더 이상 권장되지 않습니다.

인증(SSH) 키 사용 안 함

인증 키를 사용하면 사용자 인증 요청 없이 SSH를 통해 ESXi 호스트에 액세스할 수 있습니다. 호스트의 보안을 강화하려면 사용자의 인증 키를 사용한 호스트 액세스를 허용하지 마십시오.

공용 키가 호스트의 /etc/ssh/keys-root/authorized_keys 파일에 있는 사용자는 신뢰할 수 있는 사용자로 간주됩니다. 신뢰할 수 있는 원격 사용자는 암호를 제공하지 않고 호스트에 액세스할 수 있습니다.

절차

- ◆ 일상적인 작업에 대해서는 ESXi 호스트에서 SSH를 사용하지 않도록 설정하십시오.
- ◆ SSH를 일시적으로라도 사용하도록 설정한 경우에는 /etc/ssh/keys-root/authorized_keys 파일의 내용을 모니터링하여 적절한 인증 없이 호스트 액세스가 허용된 사용자가 없는지 확인하십시오.
- ◆ /etc/ssh/keys-root/authorized_keys 파일을 모니터링하여 해당 파일이 비어 있고 파일에 SSH 키가 추가되지 않았는지 확인하십시오.

- ◆ `/etc/ssh/keys-root/authorized_keys` 파일이 비어 있지 않은 경우에는 모든 키를 제거하십시오.

결과

인증 키를 사용한 원격 액세스를 사용하지 않도록 설정하면 유효한 로그인을 제공하지 않고 호스트에서 명령을 원격으로 실행할 수 있는 기능이 제한될 수 있습니다. 예를 들어 자동 원격 스크립트를 실행하지 못할 수 있습니다.

ESXi 호스트에 대한 인증서 관리

vSphere 6.0 이상에서 VMCA(VMware Certificate Authority)는 기본적으로 VMCA를 루트 인증서로 가지고 있는 서명된 인증서로 새로운 각 ESXi 호스트를 프로비저닝합니다. 프로비저닝은 호스트가 vCenter Server에 명시적으로 추가되거나 ESXi 6.0 이상으로의 업그레이드 또는 설치의 일부로 추가될 때 발생합니다.

vSphere Web Client에서 그리고 vSphere Web Services SDK에서 `vim.CertificateManager` API를 사용하여 이러한 인증서를 보고 관리할 수 있습니다. vCenter Server 인증서 관리에 사용할 수 있는 인증서 관리 CLI를 사용하여 ESXi 인증서를 보거나 관리할 수 없습니다.

vSphere 5.5 및 vSphere 6.0의 인증서

ESXi 및 vCenter Server는 통신할 때 거의 모든 관리 트래픽에 SSL을 사용합니다.

vSphere 5.5 이하에서 SSL 끝점은 사용자 이름, 암호 및 지문의 조합을 통해서만 보호됩니다. 사용자는 해당하는 자체 서명된 인증서를 자신의 인증서로 교체할 수 있습니다. vSphere 5.5 설명서 센터를 참조하십시오.

vSphere 6.0 이상에서 vCenter Server는 ESXi 호스트에 대한 다음과 같은 인증서 모드를 지원합니다.

표 5-1. ESXi 호스트에 대한 인증서 모드

인증서 모드	설명
VMware Certificate Authority(기본값)	<p>VMCA가 모든 ESXi 호스트를 최상위 CA 또는 중간 CA로 프로비저닝하는 경우 이 모드를 사용합니다.</p> <p>기본적으로 VMCA는 인증서로 ESXi 호스트를 프로비저닝합니다.</p> <p>이 모드에서는 vSphere Web Client에서 인증서를 새로 고치거나 갱신할 수 있습니다.</p>
사용자 지정 인증 기관	<p>타사 CA가 서명한 사용자 지정 인증서만 사용하려는 경우 이 모드를 사용합니다.</p> <p>이 모드에서는 사용자가 인증서 관리에 대한 책임이 있습니다. vSphere Web Client에서 인증서를 새로 고치거나 갱신할 수 없습니다.</p> <p>참고 인증서 모드를 사용자 지정 인증 기관으로 변경하는 경우가 아니면 VMCA가 vSphere Web Client에서 갱신을 선택하는 경우와 같이 사용자 지정 인증서를 교체할 수도 있습니다.</p>
지문 모드	<p>vSphere 5.5에서는 지문 모드를 사용했으며 이 모드는 vSphere 6.0에 대한 폴백 옵션으로 아직 사용할 수 있습니다. 이 모드에서 vCenter Server는 인증서가 올바른 형식인지 검사하지만 인증서의 유효성은 검사하지 않습니다. 만료된 인증서도 수락됩니다.</p> <p>다른 두 모드 중 하나로 해결할 수 없는 문제가 발생하는 경우가 아니면 이 모드를 사용하지 마십시오. 일부 vCenter 6.0 이상 서비스는 지문 모드에서 올바르게 작동하지 않을 수 있습니다.</p>

인증서 만료

vSphere 6.0부터 vSphere Web Client에서 타사 CA 또는 VMCA가 서명한 인증서의 인증서 만료에 대한 정보를 볼 수 있습니다. vCenter Server를 통해 관리되는 모든 호스트 또는 개별 호스트에 대한 정보를 볼 수 있습니다. 인증서가 **곧 만료됨** 상태(8개월 미만)에 있는 경우 노란색 경보가 발생합니다. 인증서가 **만료 임박** 상태(2개월 미만)에 있는 경우 빨간색 경보가 발생합니다.

ESXi 프로비저닝 및 VMCA

설치 미디어에서 ESXi 호스트를 부팅할 때 호스트에는 처음에 자동 생성된 인증서가 있습니다. 호스트가 vCenter Server 시스템에 추가될 때 해당 호스트가 VMCA가 루트 CA로 서명한 인증서로 프로비저닝됩니다.

이 프로세스는 Auto Deploy로 프로비저닝된 호스트의 경우와 유사합니다. 그러나 이러한 호스트는 상태를 저장하지 않으므로 서명된 인증서가 Auto Deploy 서버에 의해 로컬 인증서 저장소에 저장됩니다. 이 인증서는 ESXi 호스트의 후속 부팅 시 재사용됩니다. Auto Deploy 서버는 내장된 배포 또는 관리 노드의 일부입니다.

Auto Deploy 호스트가 처음 부팅될 때 VMCA를 사용할 수 없는 경우 호스트가 첫 번째 연결을 시도한 다음 VMCA를 사용할 수 있게 되고 호스트를 서명된 인증서로 프로비저닝할 수 있을 때까지 종료 및 재부팅을 통한 주기를 수행합니다.

호스트 이름 및 IP 주소 변경 사항

vSphere 6.0 이상에서 호스트 이름 또는 IP 주소 변경은 vCenter Server가 호스트 인증서의 유효성을 고려하는지 여부에 영향을 미칠 수 있습니다. 호스트를 vCenter Server에 추가하는 방식은 수동 작업이 필요한지 여부에 영향을 미칩니다. 수동 작업은 호스트를 다시 연결하거나 vCenter Server에서 호스트를 제거한 후 다시 추가하는 것을 의미합니다.

표 5-2. 호스트 이름 또는 IP 주소 변경에 수동 작업이 필요한 경우

호스트가 다음을 사용하여 vCenter Server에 추가된 경우...	호스트 이름 변경	IP 주소 변경
호스트 이름	vCenter Server 연결 문제. 수동 작업이 필요합니다.	작업이 필요하지 않습니다.
IP 주소	작업이 필요하지 않습니다.	vCenter Server 연결 문제. 수동 작업이 필요합니다.



ESXi 인증서 관리

(https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_vkuyp3rf/uiConfId/49694343/)

호스트 업그레이드 및 인증서

ESXi 호스트를 ESXi 6.0 이상으로 업그레이드하는 경우 업그레이드 프로세스가 자체 서명된 인증서를 VMCA 서명된 인증서로 교체합니다. 사용자 지정 인증서는 만료되었거나 유효하지 않은 경우에도 해당 프로세스에서 유지됩니다.

권장되는 업그레이드 워크플로우는 현재 인증서에 따라 다릅니다.

지문 인증서로 프로비저닝된 호스트

호스트가 현재 지문 인증서를 사용 중인 경우 업그레이드 프로세스의 일부로 VMCA 인증서가 자동으로 할당됩니다.

참고 VMCA 인증서로 기존 호스트를 프로비저닝할 수 없습니다. ESXi 6.0 이상으로 업그레이드해야 합니다.

사용자 지정 인증서로 프로비저닝된 호스트

호스트가 일반적으로 타사 CA 서명된 인증서인 사용자 지정 인증서로 프로비저닝된 경우 이러한 인증서가 제자리에 유지됩니다. 인증서 모드를 사용자 지정으로 변경하여 인증서가 실수로 교체되지 않도록 합니다.

참고 환경이 VMCA 모드에 있으며 vSphere Web Client에서 인증서를 새로 고치는 경우 모든 기존 인증서가 VMCA에서 서명한 인증서로 교체됩니다.

앞으로 vCenter Server는 vSphere Web Client에서 인증서를 모니터링하고 인증서 만료 등에 대한 정보를 표시합니다.

호스트를 vSphere 6.0 이상으로 업그레이드하지 않는 경우 호스트는 호스트가 VMCA 인증서를 사용하는 vCenter Server 시스템을 통해 관리되는 경우에도 현재 사용하는 인증서를 유지합니다.

Auto Deploy를 통해 프로비저닝되는 호스트는 항상 ESXi 6.0 소프트웨어로 처음 부팅될 때 새 인증서가 할당됩니다. Auto Deploy를 통해 프로비저닝된 호스트를 업그레이드하는 경우 Auto Deploy 서버는 호스트에 대한 CSR(인증서 서명 요청)을 생성하고 이를 VMCA에 제출합니다. VMCA는 호스트에 대한 서명된 인증서를 저장합니다. Auto Deploy 서버가 호스트를 프로비저닝하는 경우 VMCA의 인증서를 검색한 후 프로비저닝 프로세스의 일부로 포함합니다.

사용자 지정 인증서로 Auto Deploy를 사용할 수 있습니다.

ESXi 인증서 기본 설정

vCenter Server가 ESXi 호스트의 CSR(인증서 서명 요청)을 요청하는 경우 기본 설정을 사용합니다. 대부분의 기본값은 여러 상황에 잘 적용되지만 회사별 정보는 변경할 수 있습니다.

조직 및 위치 정보 변경을 고려하십시오. vSphere Web Client를 사용하여 여러 가지 기본 설정을 변경할 수 있습니다. [인증서 기본 설정 변경](#)를 참조하십시오.

표 5-3. CSR 설정

매개 변수	기본값	고급 옵션
키 크기	2048	N.A.
키 알고리즘	RSA	N.A.
인증서 서명 알고리즘	sha256WithRSAEncryption	N.A.
일반 이름	호스트 이름으로 호스트가 vCenter Server에 추가된 경우 호스트의 이름입니다. IP 주소로 호스트가 vCenter Server에 추가된 경우 호스트의 IP 주소입니다.	N.A.
국가	USA	vpzd.certmgmt.certs.cn.country
이메일 주소	vmca@vmware.com	vpzd.certmgmt.certs.cn.email
구/군/시	Palo Alto	vpzd.certmgmt.certs.cn.localityName
조직 구성 단위 이름	VMware 엔지니어링	vpzd.certmgmt.certs.cn.organizationalUnitName
조직 이름	VMware	vpzd.certmgmt.certs.cn.organizationName
시/도	California	vpzd.certmgmt.certs.cn.state
인증서가 유효한 일 수입니다.	1825	vpzd.certmgmt.certs.cn.daysValid
인증서 만료의 하드 임계값입니다. 이 임계값에 도달하면 vCenter Server에서 빨간색 경보가 발생합니다.	30일	vpzd.certmgmt.certs.cn.hardThreshold

표 5-3. CSR 설정 (계속)

매개 변수	기본값	고급 옵션
vCenter Server 인증서 유효성 검사에 대한 폴링 간격입니다.	5일	vpzd.certmgmt.certs.cn.pollIntervalDays
인증서 만료의 소프트 임계값입니다. 이 임계값에 도달하면 vCenter Server에서 이벤트가 발생합니다.	240일	vpzd.certmgmt.certs.cn.softThreshold
vCenter Server가 기존 인증서 교체 여부를 결정하기 위해 사용하는 모드입니다. 업그레이드 중 사용자 지정 인증서를 유지하려면 이 모드를 변경합니다. 호스트 업그레이드 및 인증서를 참조하십시오.	기본값은 vmca입니다. 또한 지문이나 사용자 지정으로 지정할 수 있습니다. 인증서 모드 변경 을 참조하십시오.	vpzd.certmgmt.mode

여러 ESXi 호스트에 대한 인증서 만료 정보 보기

ESXi 6.0 이상을 사용하는 경우 vCenter Server 시스템에서 관리되는 모든 호스트의 인증서 상태를 볼 수 있습니다. 표시되는 화면에서 곧 만료되는 인증서가 있는지 확인할 수 있습니다.

vSphere Web Client에서 사용자 지정 모드를 사용하는 호스트 및 VMCA 모드를 사용하는 호스트의 인증서 상태 정보를 볼 수 있습니다. 지문 모드를 사용하는 호스트의 인증서 상태 정보는 볼 수 없습니다.

절차

- 1 vSphere Web Client 인벤토리 계층에서 호스트를 찾습니다.

기본적으로 호스트 표시에는 인증서 상태가 포함되어 있지 않습니다.

- 2 [이름] 필드를 마우스 오른쪽 버튼으로 클릭하고 **열 표시/숨기기**를 선택합니다.

- 3 **인증서 유효 기간 종료**를 선택하고 **확인**을 클릭한 다음 필요한 경우 오른쪽으로 스크롤합니다.

인증서 정보에 인증서가 만료되는 시기가 표시됩니다.

호스트가 vCenter Server에 추가되거나 연결이 끊긴 후 다시 연결된 경우 상태가 [만료됨], [만료], [곧 만료됨] 또는 [만료 임박]이면 vCenter Server가 인증서를 갱신합니다. 인증서 유효 기간이 8개월 미만이면 [만료] 상태이고, 인증서 유효 기간이 2개월 미만이면 [곧 만료됨] 상태이며, 인증서 유효 기간이 1개월 미만이면 [만료 임박] 상태입니다.

- 4 (선택 사항) 다른 열을 선택 취소하면 관심 있는 내용을 좀 더 쉽게 볼 수 있습니다.

다음에 수행할 작업

만료되는 인증서를 갱신합니다. [ESXi 인증서 갱신](#) 또는 [새로 고침](#)을 참조하십시오.

단일 ESXi 호스트에 대한 인증서 세부 정보 보기

VMCA 모드 또는 사용자 지정 모드에 있는 ESXi 6.0 이상 호스트의 경우 vSphere Web Client에서 인증서 세부 정보를 볼 수 있습니다. 인증서에 대한 정보는 디버깅에 유용할 수 있습니다.

절차

- 1 vSphere Web Client 인벤토리에서 호스트를 찾습니다.
- 2 **관리** 탭을 클릭하고 **설정**을 클릭합니다.
- 3 **시스템**을 선택하고 **인증서**를 클릭합니다.

다음 정보를 검토할 수 있습니다. 이 정보는 단일 호스트 보기에서만 사용할 수 있습니다.

필드	설명
제목	인증서 생성 동안 사용되는 제목입니다.
발급자	인증서의 발급자입니다.
유효 기간 시작	인증서가 생성된 날짜입니다.
유효 기간 종료	인증서가 만료되는 날짜입니다.
상태	인증서의 상태로 다음 중 하나입니다. <div> <div>정상</div> <div>정상 작업입니다.</div> <div>만료</div> <div>인증서가 곧 만료됩니다.</div> <div>곧 만료됨</div> <div>인증서가 8개월 이내에 만료됩니다(기본값).</div> <div>만료 임박</div> <div>인증서가 2개월 이내에 만료됩니다(기본값).</div> <div>만료됨</div> <div>인증서가 만료되었으므로 유효하지 않습니다.</div> </div>

ESXi 인증서 갱신 또는 새로 고침

VMCA가 인증서를 ESXi 호스트(6.0 이상)에 할당하는 경우 vSphere Web Client에서 해당 인증서를 갱신할 수 있습니다. vCenter Server와 연결된 TRUSTED_ROOTS 스토어에서 모든 인증서를 새로 고칠 수도 있습니다.

인증서가 곧 만료되는 경우 또는 다른 이유로 새 인증서로 호스트를 프로비저닝하려는 경우 인증서를 갱신할 수 있습니다. 인증서가 이미 만료된 경우 호스트의 연결을 끊고 다시 연결해야 합니다.

기본적으로 vCenter Server는 호스트가 인벤토리에 추가되거나 다시 연결될 때마다 상태가 만료됨, 곧 만료됨 또는 만료인 호스트의 인증서를 갱신합니다.

절차

- 1 vSphere Web Client 인벤토리에서 호스트를 찾습니다.
- 2 **관리** 탭을 클릭하고 **설정**을 클릭합니다.

3 시스템을 선택하고 인증서를 클릭합니다.

선택한 호스트의 인증서에 대한 자세한 내용을 볼 수 있습니다.

4 갱신 또는 CA 인증서 새로 고침을 클릭합니다.

옵션	설명
갱신	VMCA에서 호스트의 새로 서명된 인증서를 검색합니다.
CA 인증서 새로 고침	vCenter Server VECS 스토어의 TRUSTED_ROOTS 스토어에 있는 모든 인증서를 호스트로 푸시합니다.

5 예를 클릭하여 확인합니다.

인증서 기본 설정 변경

호스트가 vCenter Server 시스템에 추가되면 vCenter Server가 호스트에 대한 CSR(인증서 서명 요청)을 VMCA에 보냅니다. vSphere Web Client의 vCenter Server 고급 설정을 사용하여 CSR의 일부 기본 설정을 변경할 수 있습니다.

회사별 기본 인증서 설정을 변경합니다. 전체 기본 설정 목록은 [ESXi 인증서 기본 설정](#) 항목을 참조하십시오. 일부 기본값은 변경할 수 없습니다.

절차

- 1 vSphere Web Client에서 호스트를 관리하는 vCenter Server 시스템을 선택합니다.
- 2 **관리** 탭을 클릭하고 **설정**을 클릭합니다.
- 3 **고급 설정**을 클릭하고 **편집**을 클릭합니다.
- 4 필터 상자에서 **certmgmt**를 입력하여 인증서 관리 매개 변수만 표시합니다.
- 5 회사 정책을 따르도록 기존 매개 변수의 값을 변경하고 **확인**을 클릭합니다.

다음에 호스트를 vCenter Server에 추가할 때 vCenter Server가 VMCA에 보내는 CSR과 호스트에 할당된 인증서에서 새로운 설정이 사용됩니다.

다음에 수행할 작업

인증서 메타데이터의 변경 사항은 새 인증서에만 영향을 미칩니다. vCenter Server 시스템을 통해 이미 관리되는 호스트의 인증서를 변경하려면 호스트의 연결을 끊었다가 다시 연결합니다.

인증서 모드 전환 이해

vSphere 6.0부터는 ESXi 호스트가 기본적으로 VMCA를 통해 인증서로 프로비저닝됩니다. 대신 사용자 지정 인증서 모드를 사용하거나 디버깅 목적으로 지문 모드를 사용할 수 있습니다. 대부분의 경우 모드 전환은 지장을 주며 필요하지 않습니다. 모드 전환이 꼭 필요한 경우에는 시작하기 전에 잠재적 영향을 검토하십시오.

vSphere 6.0 이상에서 vCenter Server는 ESXi 호스트에 대한 다음과 같은 인증서 모드를 지원합니다.

표 5-4. ESXi 호스트에 대한 인증서 모드

인증서 모드	설명
VMware Certificate Authority(기본값)	기본적으로 VMware Certificate Authority가 ESXi 호스트 인증서의 CA로 사용됩니다. VMCA는 기본적으로 루트 CA지만 다른 CA에 대한 중간 CA로 설정될 수 있습니다. 이 모드에서는 사용자가 vSphere Web Client에서 인증서를 관리할 수 있습니다. VMCA가 하위 인증서인 경우에도 사용됩니다.
사용자 지정 인증 기관	일부 고객은 자신의 외부 인증 기관을 관리하는 것을 선호할 수 있습니다. 이 모드에서는 고객이 인증서 관리에 대한 책임이 있으며 vSphere Web Client에서 인증서를 관리할 수 없습니다.
지문 모드	vSphere 5.5에서는 지문 모드를 사용했으며 이 모드는 vSphere 6.0에 대한 폴백 옵션으로 계속 사용할 수 있습니다. 다른 두 모드 중 하나에 해결할 수 없는 문제가 발생한 경우에만 이 모드를 사용하십시오. 일부 vCenter 6.0 이상 서비스는 지문 모드에서 올바르게 작동하지 않을 수 있습니다.

사용자 지정 ESXi 인증서 사용

회사 정책에 따라 VMCA가 아닌 다른 루트 CA를 사용해야 하는 경우 신중한 계획 후 환경에서 인증서 모드를 전환할 수 있습니다. 권장되는 워크플로우는 다음과 같습니다.

- 1 사용할 인증서를 가져옵니다.
- 2 호스트를 유지 보수 모드로 설정하고 vCenter Server와의 연결을 끊습니다.
- 3 사용자 지정 CA의 루트 인증서를 VECS에 추가합니다.
- 4 사용자 지정 CA 인증서를 각 호스트에 배포한 후 해당 호스트에서 서비스를 다시 시작합니다.
- 5 사용자 지정 CA 모드로 전환합니다. [인증서 모드 변경](#)의 내용을 참조하십시오.
- 6 호스트를 vCenter Server 시스템에 연결합니다.

사용자 지정 CA 모드에서 VMCA 모드로 전환

사용자 지정 CA 모드를 사용 중이며 VMCA 사용이 환경에서 더욱 효과적으로 작동함을 확인하는 경우 신중한 계획 후 모드 전환을 수행할 수 있습니다. 권장되는 워크플로우는 다음과 같습니다.

- 1 vCenter Server 시스템에서 모든 호스트를 제거합니다.
- 2 vCenter Server 시스템의 VECS에서 타사 CA의 루트 인증서를 제거합니다.
- 3 VMCA 모드로 전환합니다. [인증서 모드 변경](#)의 내용을 참조하십시오.
- 4 호스트를 vCenter Server 시스템에 추가합니다.

참고 이 모드 전환에 대한 다른 워크플로우는 예기치 않은 동작을 초래할 수 있습니다.

업그레이드 동안 지문 모드 인증서 유지

VMCA 모드에서 지문 모드로의 전환은 VMCA 인증서와 관련된 문제가 발생하는 경우에 필요할 수 있습니다. 지문 모드에서는 vCenter Server 시스템이 인증서가 존재하고 올바르게 포맷되었는지 여부만 검사하며 인증서가 유효한지 여부는 검사하지 않습니다. 자세한 내용은 [인증서 모드 변경](#)의 내용을 참조하십시오.

지문 모드에서 VMCA 모드로 전환

지문 모드를 사용하며 VMCA 서명된 인증서를 사용하기 시작하려는 경우 전환에 약간의 계획이 필요합니다. 권장되는 워크플로우는 다음과 같습니다.

- 1 vCenter Server 시스템에서 모든 호스트를 제거합니다.
- 2 VMCA 인증서 모드로 전환합니다. [인증서 모드 변경](#)의 내용을 참조하십시오.
- 3 호스트를 vCenter Server 시스템에 추가합니다.

참고 이 모드 전환에 대한 다른 워크플로우는 예기치 않은 동작을 초래할 수 있습니다.

사용자 지정 CA 모드에서 지문 모드로 전환

사용자 지정 CA와 관련된 문제가 발생하는 경우 일시적으로 지문 모드로 전환하는 것을 고려하십시오. [인증서 모드 변경](#)의 지침을 따르면 전환이 원활하게 진행됩니다. 모드 전환 후 vCenter Server 시스템은 인증서의 형식만 검사하며 인증서 자체의 유효성은 더 이상 검사하지 않습니다.

지문 모드에서 사용자 지정 CA 모드로 전환

문제 해결 동안 환경을 지문 모드로 설정하고 사용자 지정 CA 모드를 사용하기 시작하려는 경우 먼저 필요한 인증서를 생성해야 합니다. 권장되는 워크플로우는 다음과 같습니다.

- 1 vCenter Server 시스템에서 모든 호스트를 제거합니다.
- 2 사용자 지정 CA 루트 인증서를 vCenter Server 시스템에 있는 VECS의 TRUSTED_ROOTS 저장소에 추가합니다. [vCenter Server TRUSTED_ROOTS 스토어 업데이트\(사용자 지정 인증서\)](#)의 내용을 참조하십시오.
- 3 각 ESXi 호스트에 대해 다음을 수행합니다.
 - a 사용자 지정 CA 인증서 및 키를 배포합니다.
 - b 호스트에서 서비스를 다시 시작합니다.
- 4 사용자 지정 모드로 전환합니다. [인증서 모드 변경](#)의 내용을 참조하십시오.
- 5 호스트를 vCenter Server 시스템에 추가합니다.

인증서 모드 변경

대부분의 경우 VMCA를 사용한 환경의 ESXi 호스트 프로비저닝이 최상의 솔루션입니다. 회사 정책에 따라 루트 CA가 다른 사용자 지정 인증서를 사용해야 하는 경우 vCenter Server 고급 옵션을 편집하여 인증

서를 새로 고칠 때 호스트가 VMCA 인증서로 자동으로 프로비저닝되지 않도록 할 수 있습니다. 그런 다음 환경의 인증서 관리를 담당합니다.

vCenter Server 고급 설정을 사용하여 지문 모드 또는 사용자 지정 CA 모드로 변경할 수 있습니다. 지문 모드를 폴백 옵션으로만 사용하십시오.

절차

- 1 호스트를 관리하는 vCenter Server를 선택하고 **설정**을 클릭합니다.
- 2 **고급 설정**을 클릭하고 **편집**을 클릭합니다.
- 3 필터 상자에서 **certmgmt**를 입력하여 인증서 관리 키만 표시합니다.
- 4 vpxd.certmgmt.mode의 값을 **custom**으로 변경하거나(자신의 인증서를 관리하려는 경우) **thumbprint**로 변경하고(일시적으로 지문 모드를 사용하려는 경우) **확인**을 클릭합니다.
- 5 vCenter Server 서비스를 다시 시작합니다.

ESXi SSL 인증서 및 키 교체

회사의 보안 정책에 따라 각 호스트에서 기본 ESXi SSL 인증서를 타사의 CA 서명된 인증서로 교체해야 할 수도 있습니다.

기본적으로 vSphere 구성 요소는 설치 중 생성된 VMCA 서명된 인증서와 키를 사용합니다. 잘못해서 VMCA 서명된 인증서를 삭제하는 경우 해당 vCenter Server 시스템에서 호스트를 제거하고 다시 추가합니다. 호스트를 추가할 때 vCenter Server는 VMCA에서 새 인증서를 요청하고 이 인증서를 사용하여 호스트를 프로비저닝합니다.

회사 정책에 따라 필요한 경우 VMCA 서명된 인증서를 신뢰할 수 있는 CA(상업용 CA 또는 조직 CA)에서 발급한 인증서로 교체하십시오.

기본 인증서는 vSphere 5.5 인증서와 동일한 위치에 있습니다. 기본 인증서를 신뢰할 수 있는 인증서로 교체하는 방법에는 여러 가지가 있습니다.

참고 vSphere Web Services SDK의 `vim.CertificateManager` 및 `vim.host.CertificateManager` 관리 개체를 사용할 수도 있습니다. vSphere Web Services SDK 설명서를 참조하십시오.

인증서를 교체한 다음 vCenter Server와 ESXi 호스트가 신뢰 관계를 가질 수 있도록 호스트를 관리하는 vCenter Server 시스템의 VECS에서 TRUSTED_ROOTS 스토어를 업데이트해야 합니다.

■ ESXi 인증서 서명 요청에 대한 요구 사항

하위 기관 VMCA의 타사 CA 서명된 인증서 또는 사용자 지정 인증 기관의 타사 CA 서명된 인증서를 사용하려면 CSR(인증서 서명 요청)을 CA에 보내야 합니다.

■ ESXi Shell에서 기본 인증서 및 키 교체

ESXi Shell에서 기본 VMCA 서명 ESXi 인증서를 교체할 수 있습니다.

■ vifs 명령을 사용하여 기본 인증서 및 키 교체

vifs 명령을 사용하여 기본 VMCA 서명 ESXi 인증서를 교체할 수 있습니다.

■ HTTPS PUT를 사용하여 기본 인증서 교체

타사 애플리케이션을 사용하여 인증서 및 키를 업로드할 수 있습니다. HTTPS PUT 작업을 지원하는 애플리케이션은 ESXi에 포함된 HTTPS 인터페이스와 연동이 가능합니다.

■ vCenter Server TRUSTED_ROOTS 스토어 업데이트(사용자 지정 인증서)

사용자 지정 인증서를 사용하도록 ESXi 호스트를 설정하는 경우 호스트를 관리하는 vCenter Server 시스템에서 TRUSTED_ROOTS 스토어를 업데이트해야 합니다.

ESXi 인증서 서명 요청에 대한 요구 사항

하위 기관 VMCA의 타사 CA 서명된 인증서 또는 사용자 지정 인증 기관의 타사 CA 서명된 인증서를 사용하려면 CSR(인증서 서명 요청)을 CA에 보내야 합니다.

이러한 특성의 CSR을 사용합니다.

- 2048비트
- PKCS1
- 와일드카드 없음
- 현재 시간 하루 전 시작 시간
- ESXi 호스트가 vCenter Server 인벤토리에 가지고 있는 호스트 이름(또는 IP 주소)으로 설정된 CN (및 SubjectAltName).

ESXi Shell에서 기본 인증서 및 키 교체

ESXi Shell에서 기본 VMCA 서명 ESXi 인증서를 교체할 수 있습니다.

사전 요구 사항

- 타사 CA 서명된 인증서를 사용하려는 경우 인증서 요청을 생성하고 인증 기관에 보낸 다음 각 ESXi 호스트에 인증서를 저장합니다.
- 필요한 경우 ESXi Shell을 사용하도록 설정하거나, vSphere Web Client에서 SSH 트래픽을 사용하도록 설정합니다. ESXi Shell에 대한 액세스 사용 설정에 대한 정보는 "vSphere 보안" 자료를 참조하십시오.
- 모든 파일 전송과 그 밖의 통신은 보안 HTTPS 세션을 통해 이루어집니다. 세션을 인증하는 데 사용되는 사용자는 호스트에 대한 **Host.Config.AdvancedConfig** 권한이 있어야 합니다. 역할을 통한 권한 할당에 대한 정보는 "vSphere 보안" 자료를 참조하십시오.

절차

- 1 DCUI에서 직접 또는 SSH 클라이언트에서 관리자 권한이 있는 사용자로 ESXi Shell에 로그인합니다.
- 2 `/etc/vmware/ssl` 디렉토리에서 다음 명령을 사용하여 기존 인증서의 이름을 변경합니다.

```
mv rui.crt orig.rui.crt
mv rui.key orig.rui.key
```


- 3 사용할 인증서를 /etc/vmware/ssl에 복사합니다.
- 4 새 인증서와 키의 이름을 각각 rui.crt와 rui.key로 변경합니다.
- 5 새로운 인증서를 설치한 후에 호스트를 다시 시작하십시오.

아니면 호스트를 유지 보수 모드에 두고 새로운 인증서를 설치한 다음 DCUI(Direct Console User Interface)를 사용하여 관리 에이전트를 다시 시작하고 호스트가 유지 보수 모드를 종료하도록 설정할 수 있습니다.

다음에 수행할 작업

vCenter Server TRUSTED_ROOTS 저장소를 업데이트합니다. [vCenter Server TRUSTED_ROOTS 스토어 업데이트\(사용자 지정 인증서\)](#)를 참조하십시오.

vifs 명령을 사용하여 기본 인증서 및 키 교체

vifs 명령을 사용하여 기본 VMCA 서명 ESXi 인증서를 교체할 수 있습니다.

사전 요구 사항

- 타사 CA 서명된 인증서를 사용하려는 경우 인증서 요청을 생성하고 인증 기관에 보낸 다음 각 ESXi 호스트에 인증서를 저장합니다.
- 필요한 경우 ESXi Shell을 사용하도록 설정하거나, vSphere Web Client에서 SSH 트래픽을 사용하도록 설정합니다. ESXi Shell에 대한 액세스 사용 설정에 대한 정보는 "vSphere 보안" 자료를 참조하십시오.
- 모든 파일 전송과 그 밖의 통신은 보안 HTTPS 세션을 통해 이루어집니다. 세션을 인증하는 데 사용되는 사용자는 호스트에 대한 **Host.Config.AdvancedConfig** 권한이 있어야 합니다. 역할을 통한 권한 할당에 대한 정보는 "vSphere 보안" 자료를 참조하십시오.

절차

- 1 기존 인증서를 백업합니다.
- 2 인증 기관으로부터 받은 지침에 따라 인증서 요청을 생성합니다.
- 3 인증서가 있는 경우 vifs 명령을 사용하여 SSH 연결에서 호스트로 인증서를 호스트의 적절한 위치에 업로드합니다.

```
vifs --server hostname --username username --put rui.crt /host/ssl_cert
vifs --server hostname --username username --put rui.key /host/ssl_key
```

- 4 호스트를 다시 시작합니다.

다음에 수행할 작업

vCenter Server TRUSTED_ROOTS 스토어를 업데이트합니다. [vCenter Server TRUSTED_ROOTS 스토어 업데이트\(사용자 지정 인증서\)](#)를 참조하십시오.

HTTPS PUT를 사용하여 기본 인증서 교체

타사 애플리케이션을 사용하여 인증서 및 키를 업로드할 수 있습니다. HTTPS PUT 작업을 지원하는 애플리케이션은 ESXi에 포함된 HTTPS 인터페이스와 연동이 가능합니다.

사전 요구 사항

- 타사 CA 서명된 인증서를 사용하려는 경우 인증서 요청을 생성하고 인증 기관에 보낸 다음 각 ESXi 호스트에 인증서를 저장합니다.
- 필요한 경우 ESXi Shell을 사용하도록 설정하거나, vSphere Web Client에서 SSH 트래픽을 사용하도록 설정합니다. ESXi Shell에 대한 액세스 사용 설정에 대한 정보는 "vSphere 보안" 자료를 참조하십시오.
- 모든 파일 전송과 그 밖의 통신은 보안 HTTPS 세션을 통해 이루어집니다. 세션을 인증하는 데 사용되는 사용자는 호스트에 대한 **Host.Config.AdvancedConfig** 권한이 있어야 합니다. 역할을 통한 권한 할당에 대한 정보는 "vSphere 보안" 자료를 참조하십시오.

절차

- 1 기존 인증서를 백업합니다.
- 2 업로드 애플리케이션에서 각 파일을 다음과 같이 처리합니다.
 - a 파일을 엽니다.
 - b 파일을 이들 위치 중 하나로 게시합니다.

옵션	설명
인증서	https://hostname/host/ssl_cert
키	https://hostname/host/ssl_key

/host/ssl_cert 및 host/ssl_key 위치는 /etc/vmware/ssl에 있는 인증서 파일에 연결됩니다.

- 3 호스트를 다시 시작합니다.

다음에 수행할 작업

vCenter Server TRUSTED_ROOTS 저장소를 업데이트합니다. [vCenter Server TRUSTED_ROOTS 스토어 업데이트\(사용자 지정 인증서\)](#)를 참조하십시오.

vCenter Server TRUSTED_ROOTS 스토어 업데이트(사용자 지정 인증서)

사용자 지정 인증서를 사용하도록 ESXi 호스트를 설정하는 경우 호스트를 관리하는 vCenter Server 시스템에서 TRUSTED_ROOTS 스토어를 업데이트해야 합니다.

사전 요구 사항

각 호스트의 인증서를 사용자 지정 인증서로 바꿉니다.

절차

- 1 ESXi 호스트를 관리하는 vCenter Server 시스템에 로그인합니다.

소프트웨어를 설치한 Windows 시스템에 로그인하거나 vCenter Server Appliance 셸에 로그인합니다.

- 2 `vecs-cli`를 실행하여 새 인증서를 TRUSTED_ROOTS 스토어에 추가합니다. 예:

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store TRUSTED_ROOTS --alias custom1.crt
--cert /etc/vmware/ssl/custom1.crt
```

옵션	설명
Linux	<code>/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store TRUSTED_ROOTS --alias custom1.crt --cert /etc/vmware/ssl/custom1.crt</code>
Windows	<code>C:\Program Files\VMware\vCenter Server\vmafdd\vecs-cli entry create --store TRUSTED_ROOTS --alias custom1.crt --cert c:\ssl\custom1.crt</code>

다음에 수행할 작업

인증서 모드를 사용자 지정으로 설정합니다. 인증서 모드가 기본값인 VMCA인 상태에서 인증서 새로 고침을 수행하는 경우 사용자 지정 인증서가 VMCA 서명된 인증서로 바뀝니다. [인증서 모드 변경](#)을 참조하십시오.

Auto Deploy와 함께 사용자 지정 인증서 사용

기본적으로 Auto Deploy 서버는 VMCA에서 서명한 인증서로 각 호스트를 프로비저닝합니다. Auto Deploy 서버가 VMCA에서 서명하지 않은 사용자 지정 인증서로 모든 호스트를 프로비저닝하도록 설정할 수 있습니다. 이 시나리오에서 Auto Deploy 서버는 타사 CA의 하위 인증 기관이 됩니다.

사전 요구 사항

- CA의 요구 사항을 충족하는 인증서를 요청합니다.
 - 키 크기: 2048비트 이상(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, 부인 방지, 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).
- 인증서 및 키 파일을 rbd-ca.crt 및 rbd-ca.key로 명명합니다.

절차

- 1 기본 ESXi 인증서를 백업합니다.

인증서는 /etc/vmware-rbd/ssl/에 있습니다.

- 2 vSphere Web Client에서 Auto Deploy 서비스를 중지합니다.

- a **관리**를 선택하고 **배포** 아래에서 **시스템 구성**을 클릭합니다.
- b **서비스**를 클릭합니다.
- c 중지할 서비스를 마우스 오른쪽 버튼으로 클릭하고 **중지**를 선택합니다.

- 3 Auto Deploy 서비스가 실행되는 시스템에서 /etc/vmware-rbd/ssl/의 rbd-ca.crt 및 rbd-ca.key를 사용자 지정 인증서 및 키 파일로 교체합니다.

- 4 Auto Deploy 서비스가 실행되는 시스템에서 새 인증서를 사용하도록 VECS의 TRUSTED_ROOTS 저장소를 업데이트합니다.

```
vecs-cli entry delete --store TRUSTED_ROOTS --alias
    rbd_cert
vecs-cli entry create --store TRUSTED_ROOTS --alias
    rbd_cert --cert /etc/vmware-rbd/ssl/rbd-ca.crt
```

Windows

C:\Program Files\VMware\vCenter Server\vmafdd\vecs-cli.exe

Linux

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

- 5 TRUSTED_ROOTS의 내용물이 포함된 castore.pem 파일을 생성하고 해당 파일을 /etc/vmware-rbd/ssl/ 디렉토리에 배치합니다.

사용자 지정 모드에서는 사용자에게 이 파일을 관리할 책임이 있습니다.

- 6 vCenter Server 시스템의 인증서 모드를 **사용자 지정**으로 변경합니다.

[인증서 모드 변경](#)를 참조하십시오.

- 7 vCenter Server 서비스를 다시 시작하고 Auto Deploy 서비스를 시작합니다.

결과

다음에 Auto Deploy를 사용하도록 설정된 호스트를 프로비저닝하면 Auto Deploy 서버가 TRUSTED_ROOTS 저장소에 추가한 루트 인증서를 사용하여 인증서를 생성합니다.

ESXi 인증서 및 키 파일 복원

vSphere Web Services SDK를 사용하여 ESXi 호스트에서 인증서를 바꾸는 경우 이전 인증서 및 키가 .bak 파일에 추가됩니다. .bak 파일의 정보를 현재 인증서 및 키 파일로 이동하면 이전 인증서를 복원할 수 있습니다.

호스트 인증서 및 키는 /etc/vmware/ssl/rui.crt 및 /etc/vmware/ssl/rui.key에 있습니다.

vSphere Web Services SDK vim.CertificateManager 관리 개체를 사용하여 호스트 인증서 및 키를 바꾸는 경우 이전 키 및 인증서가 /etc/vmware/ssl/rui.bak 파일에 추가됩니다.

참고 HTTP PUT, vifs를 사용하거나 ESXi Shell에서 인증서를 바꾸는 경우에는 기존 인증서가 .bak 파일에 추가되지 않습니다.

절차

- 1 ESXi 호스트에서 /etc/vmware/ssl/rui.bak 파일을 찾습니다.

파일의 형식은 다음과 같습니다.

```
#
# Host private key and certificate backup from 2014-06-20 08:02:49.961
#

-----BEGIN PRIVATE KEY-----
previous key
-----END PRIVATE KEY-----

-----BEGIN CERTIFICATE-----
previous cert
-----END CERTIFICATE-----
```

- 2 -----BEGIN PRIVATE KEY-----로 시작하고 -----END PRIVATE KEY-----로 끝나는 텍스트를 /etc/vmware/ssl/rui.key 파일에 복사합니다.

-----BEGIN PRIVATE KEY----- 및 -----END PRIVATE KEY-----를 포함합니다.

- 3 -----BEGIN CERTIFICATE-----와 -----END CERTIFICATE----- 사이의 텍스트를 /etc/vmware/ssl/rui.crt 파일에 복사합니다.

-----BEGIN CERTIFICATE----- 및 -----END CERTIFICATE-----를 포함합니다.

- 4 호스트를 다시 시작하거나 ssl_reset 이벤트를 키를 사용하는 모든 서비스에 보냅니다.

```
for s in /etc/init.d/*; do $s | grep ssl_reset > /dev/null; if [ $? == 0 ]; then $s
ssl_reset; fi; done
```

보안 프로파일을 사용하여 호스트 사용자 지정

vSphere Web Client의 보안 프로파일 패널을 통해 호스트에 대한 여러 필수 보안 설정을 사용자 지정할 수 있습니다. 보안 프로파일은 단일 호스트 관리에 특히 유용합니다. 여러 개의 호스트를 관리 중인 경우에는 CLI나 SDK를 사용하고 사용자 지정을 자동화하는 것을 고려해 보십시오.

ESXi 방화벽 구성

ESXi에는 기본적으로 활성화되는 방화벽이 포함됩니다.

설치 시 ESXi 방화벽은 호스트 보안 프로파일에서 활성화된 서비스의 트래픽을 제외하고 들어오고 나가는 트래픽을 차단하도록 구성됩니다.

방화벽에서 포트를 열 때 ESXi 호스트에서 실행되는 서비스에 대한 제한되지 않은 액세스로 인해 외부 공격 및 인증되지 않은 액세스에 호스트가 노출될 수 있는지 고려하십시오. 인증된 네트워크에서만 액세스를 허용하도록 ESXi 방화벽을 구성하여 위험을 줄이십시오.

참고 방화벽을 사용하여 ICMP(Internet Control Message Protocol) ping과 DHCP 및 DNS(UDP만 해당) 클라이언트와의 통신을 허용할 수도 있습니다.

ESXi 방화벽 포트는 다음과 같이 관리할 수 있습니다.

- vSphere Web Client의 각 호스트에서 보안 프로파일을 사용합니다. [ESXi 방화벽 설정 관리](#)의 내용을 참조하십시오.
- 명령줄 또는 스크립트에서 ESXCLI 명령을 사용합니다. [ESXi ESXCLI 방화벽 명령](#)의 내용을 참조하십시오.
- 열려는 포트가 보안 프로파일에 포함되어 있지 않은 경우 사용자 지정 VIB를 사용합니다.

사용자 지정 VIB는 VMware Labs에서 제공되는 vibauthor 도구를 사용하여 생성합니다. 사용자 지정 VIB를 설치하려면 ESXi 호스트의 허용 수준을 CommunitySupported로 변경해야 합니다. VMware 기술 자료 문서 [2007381](#)을 참조하십시오.

참고 VMware 기술 지원을 이용하여 CommunitySupported VIB가 설치된 ESXi 호스트에 발생한 문제를 조사하는 경우 VMware 지원팀에서는 이 CommunitySupported VIB가 조사하는 문제와 관련이 있는지 여부를 확인하기 위해 문제 해결 단계의 일환으로 해당 VIB를 제거하도록 요청할 수도 있습니다.



ESXi 방화벽 개념

(https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_8qp59yqe/uiConfId/49694343/)

NFS Client 규칙 집합(nfsClient)의 동작은 다른 규칙 집합의 동작과 다릅니다. NFS Client 규칙 집합이 사용되는 경우 허용되는 IP 주소 목록의 대상 호스트에 대해 모든 아웃바운드 TCP 포트가 열립니다. 자세한 내용은 [NFS 클라이언트 방화벽 동작](#)의 내용을 참조하십시오.

ESXi 방화벽 설정 관리

vSphere Web Client 또는 명령줄에서 서비스나 관리 에이전트에 대해 들어오는 방화벽 연결과 나가는 방화벽 연결을 구성할 수 있습니다.

참고 서로 다른 서비스에 포트 규칙이 겹치는 경우, 특정 서비스를 사용하도록 설정했을 때 다른 서비스도 사용 가능하도록 암시적으로 설정될 수 있습니다. 이 문제를 방지하려면 호스트의 각 서비스에 액세스하도록 허용된 IP 주소를 지정하면 됩니다.

절차

1 vSphere Web Client 인벤토리에서 호스트를 찾습니다.

2 **관리** 탭을 클릭하고 **설정**을 클릭합니다.

3 **보안 프로파일**을 클릭합니다.

vSphere Web Client에는 활성 상태의 들어오는 연결과 나가는 연결 및 해당 방화벽 포트의 목록이 표시됩니다.

4 방화벽 섹션에서 **편집**을 클릭합니다.

화면에 규칙 이름 및 연관된 정보가 포함된 방화벽 규칙 집합이 표시됩니다.

5 사용할 규칙 집합을 선택하거나, 사용하지 않을 규칙 집합을 선택 취소합니다.

열	설명
들어오는 포트 및 나가는 포트	서비스를 사용하도록 vSphere Web Client에서 여는 포트
프로토콜	서비스에서 사용하는 프로토콜
대문	서비스와 연결된 대문의 상태

6 일부 서비스의 경우 서비스 세부 정보를 관리할 수 있습니다.

- **시작, 중지 또는 다시 시작** 버튼을 사용하여 서비스의 상태를 일시적으로 변경합니다.
- 서비스가 호스트 또는 포트 사용과 함께 시작되도록 시작 정책을 변경합니다.

7 일부 서비스의 경우 연결이 허용되는 IP 주소를 명시적으로 지정할 수 있습니다.

[ESXi 호스트에 대해 허용되는 IP 주소 추가](#)를 참조하십시오.

8 **확인**을 클릭합니다.

ESXi 호스트에 대해 허용되는 IP 주소 추가

기본적으로 각 서비스의 방화벽은 모든 IP 주소에 대한 액세스를 허용합니다. 트래픽을 제한하려면 관리 서브넷에서만 트래픽을 허용하도록 각 서비스를 변경합니다. 환경에서 사용하지 않는 경우 일부 서비스를 선택 취소할 수도 있습니다.

vSphere Web Client, vCLI 또는 PowerCLI를 사용하여 서비스에 허용된 IP 목록을 업데이트할 수 있습니다. 기본적으로 서비스에 대해 모든 IP 주소가 허용됩니다.



ESXi 방화벽에 허용되는 IP 주소 추가

(https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_Ougsspa2/uiConfId/49694343/)

절차

- 1 vSphere Web Client 인벤토리에서 호스트를 찾습니다.
- 2 **관리** 탭을 클릭하고 **설정**을 클릭합니다.
- 3 시스템 아래에서 **보안 프로파일**을 클릭합니다.
- 4 방화벽 섹션에서 **편집**을 클릭하고 목록에서 서비스를 선택합니다.
- 5 허용된 IP 주소 섹션에서 **모든 IP 주소의 연결 허용**을 선택 취소하고 호스트에 연결할 수 있도록 허용할 네트워크의 IP 주소를 입력합니다.

여러 개의 IP 주소는 쉼표로 구분합니다. 다음과 같은 주소 형식을 사용할 수 있습니다.

- 192.168.0.0/24
- 192.168.1.2, 2001::1/64
- fd3e:29a6:0a81:e478::/64

- 6 **확인**을 클릭합니다.

ESXi 호스트에 대해 들어오고 나가는 방화벽 포트

vSphere Web Client를 사용하면 각 서비스에 대한 방화벽 포트를 열고 닫거나 선택된 IP 주소의 트래픽을 허용할 수 있습니다.

다음 표에는 일반적으로 설치된 서비스에 대한 방화벽이 나열되어 있습니다. 호스트에 다른 VIB를 설치하는 경우 추가 서비스 및 방화벽 포트를 사용하게 될 수 있습니다.

표 5-5. 수신 방화벽 연결

서비스	포트	설명
CIM 서버	5988(TCP)	CIM(Common Information Model)을 위한 서버입니다.
CIM 보안 서버	5989(TCP)	CIM을 위한 보안 서버입니다.
CIM SLP	427(TCP, UDP)	CIM 클라이언트에서는 CIM 서버를 찾는 데 SLPv2(Service Location Protocol 버전 2)를 사용합니다.
DHCPv6	546(TCP, UDP)	IPv6을 위한 DHCP 클라이언트입니다.
DVSSync	8301, 8302(UDP)	DVSSync 포트는 VMware FT 기록/재생이 사용할 수 있도록 설정된 호스트 간의 분산 가상 포트의 상태를 동기화하는 데 사용됩니다. 기본 또는 백업 가상 시스템을 실행하는 호스트만 이러한 포트가 반드시 열려 있어야 합니다. VMware FT를 사용 중이지 않은 호스트에서는 이러한 포트가 열려 있지 않아도 됩니다.

표 5-5. 수신 방화벽 연결 (계속)

서비스	포트	설명
NFC	902(TCP)	NFC(Network File Copy)는 vSphere 구성 요소를 위한 파일 형식 인식 FTP 서비스를 제공합니다. ESXi에서는 데이터스토어 간의 데이터 복사 및 이동 등의 작업에 기본적으로 NFC를 사용합니다.
Virtual SAN 클러스터링 서비스	12345, 23451(UDP)	Virtual SAN 클러스터 모니터링 및 멤버 자격 디렉토리 서비스입니다. UDP 기반 IP 멀티캐스트를 사용하여 클러스터 멤버를 설정하고 Virtual SAN 메타데이터를 모든 클러스터 멤버에 분산합니다. 사용하지 않도록 설정하는 경우 Virtual SAN이 작동하지 않습니다.
DHCP 클라이언트	68(UDP)	IPv4를 위한 DHCP 클라이언트입니다.
DNS 클라이언트	53(UDP)	DNS 클라이언트입니다.
Fault Tolerance	8200, 8100, 8300(TCP, UDP)	vSphere FT(Fault Tolerance)용 호스트 간의 트래픽입니다.
NSX 논리적 분산 라우터 서비스	6999(UDP)	NSX Virtual Distributed Router 서비스입니다. NSX VIB가 설치되고 VDR 모듈이 생성될 때 이 서비스와 연결된 방화벽 포트가 열려 있습니다. 호스트와 연결된 VDR 인스턴스가 없는 경우에는 포트가 열려 있지 않아도 됩니다. 이 서비스는 이전 버전의 제품에서 NSX 논리적 분산 라우터라고 불렸습니다.
Virtual SAN 전송	2233(TCP)	Virtual SAN의 신뢰할 수 있는 데이터그램 전송입니다. TCP를 사용하며 Virtual SAN 스토리지 IO에 사용됩니다. 사용하지 않도록 설정하는 경우 Virtual SAN이 작동하지 않습니다.
SNMP 서버	161(UDP)	호스트가 SNMP 서버에 연결할 수 있도록 허용합니다.
SSH 서버	22(TCP)	SSH 액세스에 필요합니다.
vMotion	8000(TCP)	vMotion을 사용한 가상 시스템 마이그레이션에 필요합니다.
vSphere Web Client	902, 443(TCP)	클라이언트 연결
vsanvp	8080(TCP)	VSAN VASA 벤더 제공자입니다. vCenter의 일부인 SMS(스토리지 관리 서비스)에서 Virtual SAN 스토리지 프로파일, 기능 및 규정 준수에 대한 정보에 액세스하는 데 사용됩니다. 사용하지 않도록 설정하는 경우 Virtual SAN SPBM(스토리지 프로파일 기반 관리)이 작동하지 않습니다.
vSphere Web Access	80(TCP)	다양한 인터페이스에 대한 다운로드 링크가 포함된 시작 페이지입니다.
RFB 프로토콜	5900-5964(TCP)	VNC 같은 관리 도구에서 사용합니다.

표 5-6. 송신 방화벽 연결

서비스	포트	설명
CIM SLP	427(TCP, UDP)	CIM 클라이언트에서는 CIM 서버를 찾는 데 SLPv2(Service Location Protocol 버전 2)를 사용합니다.
DHCPv6	547(TCP, UDP)	IPv6을 위한 DHCP 클라이언트입니다.
DVSSync	8301, 8302(UDP)	DVSSync 포트는 VMware FT 기록/재생이 사용할 수 있도록 설정된 호스트 간의 분산 가상 포트의 상태를 동기화하는 데 사용됩니다. 기본 또는 백업 가상 시스템을 실행하는 호스트만 이러한 포트가 반드시 열려 있어야 합니다. VMware FT를 사용 중이지 않은 호스트에서는 이러한 포트가 열려 있지 않아도 됩니다.
HBR	44046, 31031(TCP)	vSphere Replication 및 VMware Site Recovery Manager의 송신 복제 트래픽에 사용됩니다.
NFC	902(TCP)	NFC(Network File Copy)는 vSphere 구성 요소를 위한 파일 형식 인식 FTP 서비스를 제공합니다. ESXi에서는 데이터스토어 간의 데이터 복사 및 이동 등의 작업에 기본적으로 NFC를 사용합니다.
WOL	9(UDP)	Wake on LAN에서 사용.
Virtual SAN 클러스터링 서비스	12345 23451(UDP)	Virtual SAN에 의해 사용되는 클러스터 모니터링, 멤버 자격 및 디렉토리 서비스입니다.
DHCP 클라이언트	68(UDP)	DHCP 클라이언트입니다.
DNS 클라이언트	53(TCP, UDP)	DNS 클라이언트입니다.
Fault Tolerance	80, 8200, 8100, 8300(TCP, UDP)	VMware Fault Tolerance를 지원합니다.
소프트웨어 iSCSI 클라이언트	3260(TCP)	소프트웨어 iSCSI를 지원합니다.
NSX 논리적 분산 라우터 서비스	6999(UDP)	NSX VIB가 설치되고 VDR 모듈이 생성될 때 이 서비스와 연결된 방화벽 포트가 열려 있습니다. 호스트와 연결된 VDR 인스턴스가 없는 경우에는 포트가 열려 있지 않아도 됩니다.
rabbitmqproxy	5671(TCP)	ESXi 호스트에서 실행 중인 프로시저, 가상 시스템 내부에서 실행 중인 애플리케이션이 vCenter 네트워크 도메인에서 실행 중인 AMQP 브로커에 전달하도록 허용합니다. 가상 시스템은 네트워크에 있지 않아도 됩니다. 즉, NIC가 필요하지 않습니다. 프로시저는 vCenter 네트워크 도메인의 브로커에 연결됩니다. 따라서 송신 연결 IP 주소에 최소한 사용 중인 현재 브로커 또는 이후 브로커가 포함되어야 합니다. 고객이 스케일 업하려는 경우 브로커를 추가할 수 있습니다.
Virtual SAN 전송	2233(TCP)	Virtual SAN 노드 간의 RDT 트래픽(유니캐스트 피어-피어 통신)에 사용됩니다.
vMotion	8000(TCP)	vMotion을 사용한 가상 시스템 마이그레이션에 필요합니다.

표 5-6. 송신 방화벽 연결 (계속)

서비스	포트	설명
VMware vCenter 에이전트	902(UDP)	vCenter Server 에이전트입니다.
vsanvmp	8080(TCP)	Virtual SAN 벤더 제공자 트래픽에 사용됩니다.

NFS 클라이언트 방화벽 동작

NFS 클라이언트 방화벽 규칙 집합은 다른 ESXi 방화벽 규칙 집합과는 다르게 동작합니다. ESXi에서는 NFS 데이터스토어를 마운트하거나 마운트 해제할 때 NFS 클라이언트 설정을 구성합니다. 동작은 NFS의 버전별로 다릅니다.

NFS 데이터스토어를 추가, 마운트 또는 마운트 해제할 때 결과 동작은 NFS의 버전에 따라 다릅니다.

NFS v3 방화벽 동작

NFS v3 데이터스토어를 추가하거나 마운트할 때 ESXi에서는 NFS 클라이언트(nfsClient) 방화벽 규칙 집합의 상태를 확인합니다.

- nfsClient 규칙 집합이 사용하지 않도록 설정된 경우 ESXi에서는 해당 규칙 집합을 사용하도록 설정하고 allowedAll 플래그를 FALSE로 설정하여 모든 IP 주소 허용 정책을 사용하지 않도록 설정합니다. NFS 서버의 IP 주소는 허용된 송신 IP 주소 목록에 추가됩니다.
- nfsClient 규칙 집합이 사용하도록 설정된 경우 이 규칙 집합의 상태와 허용된 IP 주소 정책은 변경되지 않습니다. NFS 서버의 IP 주소는 허용된 송신 IP 주소 목록에 추가됩니다.

참고 NFS v3 데이터스토어를 시스템에 추가하기 전 또는 그 후에 nfsClient 규칙 집합을 수동으로 사용하도록 설정하거나 모든 IP 주소 허용 정책을 수동으로 설정하면 마지막 NFS v3 데이터스토어가 마운트 해제될 때 설정이 재정의됩니다. 모든 NFS v3 데이터스토어가 마운트 해제되면 nfsClient 규칙 집합은 사용하지 않도록 설정됩니다.

NFS v3 데이터스토어를 제거하거나 마운트 해제할 때 ESXi에서는 다음 작업 중 하나를 수행합니다.

- 나머지 NFS v3 데이터스토어 중에서 마운트 해제되는 데이터스토어 서버에서 마운트된 데이터스토어가 없으면 ESXi에서는 송신 IP 주소의 목록에서 서버의 IP 주소를 제거합니다.
- 마운트 해제 작업 후 마운트된 NFS v3 데이터스토어가 남아 있지 않으면 ESXi에서는 nfsClient 방화벽 규칙 집합을 사용하지 않도록 설정합니다.

NFS v4.1 방화벽 동작

첫 번째 NFS v4.1 데이터스토어를 마운트하면 ESXi에서는 nfs41client 규칙 집합을 사용하도록 설정하고 allowedAll 플래그를 TRUE로 설정합니다. 이 작업은 모든 IP 주소에 대해 포트 2049를 엽니다. NFS v4.1 데이터스토어 마운트 해제는 방화벽 상태에 영향을 주지 않습니다. 즉, 첫 번째 NFS v4.1 마운트는 포트 2049를 열고 해당 포트는 명시적으로 닫지 않는 한 사용하도록 설정된 상태로 유지됩니다.

ESXi ESXCLI 방화벽 명령

환경에 여러 ESXi 호스트가 포함된 경우 ESXCLI 명령 또는 vSphere Web Services SDK를 사용한 방화벽 구성 자동화가 권장됩니다.

ESXi Shell 또는 vSphere CLI 명령을 사용하여 명령줄에서 ESXi를 구성하여 방화벽 구성을 자동화할 수 있습니다. 소개는 "vSphere Command-Line Interface 시작" 항목을 참조하고 방화벽 및 방화벽 규칙 조작을 위한 ESXCLI 사용 예는 "vSphere 명령줄 인터페이스 개념 및 예"를 참조하십시오.

표 5-7. 방화벽 명령

명령	설명
<code>esxcli network firewall get</code>	방화벽의 사용 여부 상태를 반환하고 기본 작업을 나열합니다.
<code>esxcli network firewall set --default-action</code>	기본 작업을 '통과'로 설정하려면 true 로 설정하고 기본 작업을 '삭제'로 설정하려면 false 로 설정합니다.
<code>esxcli network firewall set --enabled</code>	ESXi 방화벽을 사용하거나 사용하지 않도록 설정합니다.
<code>esxcli network firewall load</code>	방화벽 모듈 및 규칙 집합 구성 파일을 로드합니다.
<code>esxcli network firewall refresh</code>	방화벽 모듈이 로드된 경우 규칙 집합 파일을 읽어 방화벽 구성을 새로 고칩니다.
<code>esxcli network firewall unload</code>	필터를 제거하고 방화벽 모듈을 언로드합니다.
<code>esxcli network firewall ruleset list</code>	규칙 집합 정보를 나열합니다.
<code>esxcli network firewall ruleset set --allowed-all</code>	모든 IP에 대한 모든 액세스를 허용하려면 true 로 설정하고 허용된 IP 주소 목록을 사용하려면 false 로 설정합니다.
<code>esxcli network firewall ruleset set --enabled --ruleset-id=<string></code>	지정된 규칙 집합을 사용하거나 사용하지 않도록 설정하려면 enabled 를 true 또는 false 로 설정합니다.
<code>esxcli network firewall ruleset allowedip list</code>	지정된 규칙 집합의 허용되는 IP 주소를 나열합니다.
<code>esxcli network firewall ruleset allowedip add</code>	지정된 IP 주소 또는 IP 주소 범위에서 규칙 집합에 액세스할 수 있도록 합니다.
<code>esxcli network firewall ruleset allowedip remove</code>	지정된 IP 주소 또는 IP 주소 범위에서 규칙 집합에 액세스할 수 없도록 합니다.
<code>esxcli network firewall ruleset rule list</code>	방화벽의 각 규칙 집합에 있는 규칙을 나열합니다.

보안 프로파일에서 ESXi 서비스 사용자 지정

ESXi 호스트에는 기본적으로 실행되는 여러 서비스가 포함됩니다. SSH와 같은 기타 서비스는 호스트의 보안 프로파일에 포함되어 있습니다. 회사 정책에서 허용하는 경우 필요에 따라 이러한 서비스를 사용하도록 설정하거나 사용하지 않도록 설정할 수 있습니다.

vSphere Web Client를 사용하여 ESXi Shell에 액세스할 수 있도록 설정 항목은 서비스를 사용하도록 설정하는 방법의 예입니다.

참고 서비스를 사용하도록 설정하는 것은 호스트의 보안에 영향을 미칩니다. 엄격하게 필요한 경우가 아니면 서비스를 사용하도록 설정하지 마십시오.

사용 가능한 서비스는 ESXi 호스트에 설치된 VIB에 따라 다릅니다. VIB를 설치하지 않고 서비스를 추가할 수 없습니다. vSphere HA와 같은 일부 VMware 제품은 호스트에 VIB를 설치하고 서비스와 해당 방화벽 포트를 사용할 수 있게 합니다.

기본 설치에서는 vSphere Web Client에서 다음과 같은 서비스의 상태를 수정할 수 있습니다.

표 5-8. 보안 프로파일의 ESXi 서비스

서비스	기본값	설명
직접 콘솔 UI	실행 중	DCUI(Direct Console User Interface) 서비스를 사용하면 텍스트 기반 메뉴를 통해 로컬 콘솔 호스트에서 ESXi 호스트와 상호 작용할 수 있습니다.
ESXi Shell	중지됨	ESXi Shell은 Direct Console User Interface에서 사용할 수 있으며 완전히 지원되는 명령 집합과 문제 해결 및 업데이트 적용을 위한 명령 집합을 포함합니다. 각 시스템의 직접 콘솔에서 ESXi Shell에 대한 액세스를 사용하도록 설정해야 합니다. 로컬 ESXi Shell에 대한 액세스를 사용하도록 설정하거나 SSH를 사용하여 ESXi Shell에 대한 액세스를 사용하도록 설정할 수 있습니다.
SSH	중지됨	보안 셸을 통한 원격 연결을 허용하는 호스트의 SSH 클라이언트 서비스입니다.
로드 기반 팀 구성 대몬	실행 중	로드 기반 팀 구성입니다.
로컬 보안 인증 서버(Active Directory 서비스)	중지됨	Active Directory 서비스의 일부입니다. Active Directory에 대한 ESXi를 구성할 때 이 서비스가 시작됩니다.
I/O 리더랙터(Active Directory 서비스)	중지됨	Active Directory 서비스의 일부입니다. Active Directory에 대한 ESXi를 구성할 때 이 서비스가 시작됩니다.
네트워크 로그인 서버(Active Directory 서비스)	중지됨	Active Directory 서비스의 일부입니다. Active Directory에 대한 ESXi를 구성할 때 이 서비스가 시작됩니다.
NTP 대몬	중지됨	네트워크 시간 프로토콜 대몬입니다.
CIM 서버	실행 중	CIM(Common Information Model) 애플리케이션에서 사용할 수 있는 서비스입니다.
SNMP 서버	중지됨	SNMP 대몬입니다. SNMP v1, v2 및 v3 구성에 대한 자세한 내용은 "vSphere 모니터링 및 성능" 항목을 참조하십시오.
Syslog 서버	중지됨	Syslog 대몬입니다. vSphere Web Client의 고급 시스템 설정에서 syslog를 사용하도록 설정해야 합니다. "vSphere 설치 및 설정"을 참조하십시오.
vSphere HA 에이전트	중지됨	vSphere High Availability 기능을 지원합니다.

표 5-8. 보안 프로파일의 ESXi 서비스 (계속)

서비스	기본값	설명
vProbe 대몬	중지됨	vProbe 대몬입니다.
VMware vCenter 에이전트	실행 중	vCenter Server 에이전트입니다. vCenter Server가 ESXi 호스트에 연결하도록 허용합니다. 특히 vpxa는 호스트 대몬에 대한 통신 통로로 이를 통해 ESXi 커널과 통신할 수 있습니다.
X.Org 서버	중지됨	X.Org 서버입니다. 이 선택적 기능은 가상 시스템에 대한 3D 그래픽을 위해 내부적으로 사용됩니다.

보안 프로파일에서 서비스 사용 또는 사용 안 함

vSphere Web Client에서 보안 프로파일에 나열된 서비스 중 하나를 사용하거나 사용하지 않도록 설정할 수 있습니다.

설치 후 특정 서비스는 기본적으로 실행되지만 나머지는 중지됩니다. 일부 경우에 vSphere Web Client UI에서 서비스를 사용하려면 추가 설치가 필요합니다. 예를 들어 NTP 서비스를 사용하여 정확한 시간 정보를 가져올 수 있지만 이 서비스는 필수 포트를 방화벽에서 열어 놓은 경우에만 작동합니다.

사전 요구 사항

vSphere Web Client를 사용하여 vCenter Server에 연결합니다.

절차

- 1 vSphere Web Client 인벤토리에서 호스트를 찾은 후 호스트를 선택합니다.
- 2 **관리** 탭을 클릭하고 **설정**을 클릭합니다.
- 3 시스템 아래에서 **보안 프로파일**을 선택하고 **편집**을 클릭합니다.
- 4 변경할 서비스로 스크롤합니다.
- 5 [서비스 세부 정보] 창에서 호스트 상태의 일회성 변경을 위해 **시작**, **중지** 또는 **다시 시작**을 선택하거나 재부팅 후 호스트의 상태 변경을 위해 **시작 정책** 메뉴에서 선택합니다.
 - **포트가 열려 있는 경우 자동으로 시작하고 포트가 모두 닫힌 경우 중지** 이러한 서비스에 대한 기본 설정입니다. 열려 있는 포트가 있으면 클라이언트는 서비스에 대한 네트워크 리소스에 연결하려고 시도합니다. 일부 포트가 열려 있지만 특정 서비스에 대한 포트가 닫혀 있는 경우 해당 시도가 실패합니다. 적용 가능한 송신 포트가 다시 열리면 서비스가 시작 완료를 시작합니다.
 - **호스트와 함께 시작 및 중지** 서비스는 호스트가 시작된 후 곧바로 시작되어 호스트가 종료되기 바로 전에 종료됩니다. **포트가 열려 있는 경우 자동으로 시작하고 포트가 모두 닫힌 경우 중지**와 유사하게 이 옵션은 지정된 NTP 서버에 연결하는 것처럼 서비스가 정기적으로 작업 완료를 시도함을 의미합니다. 포트가 닫혔다가 나중에 열리면 클라이언트가 곧바로 작업을 완료하기 시작합니다.

- **수동으로 시작 및 중지** 호스트는 포트가 열려 있는지 여부에 관계없이 사용자가 결정한 서비스 설정을 유지합니다. 사용자가 NTP 서비스를 시작하면 이 서비스는 호스트 전원이 켜져 있는 동안 계속 실행됩니다. 서비스를 시작한 이후에 호스트 전원을 끄면 종료 프로세스의 일부로 서비스가 중지되지만 호스트 전원을 켜는 즉시 서비스가 다시 시작되어 사용자가 지정한 상태가 유지됩니다.

참고 이러한 설정은 vSphere Web Client를 통해 구성된 서비스 설정 또는 vSphere Web Services SDK를 사용하여 생성된 애플리케이션에만 적용됩니다. ESXi Shell 또는 구성 파일과 같이 다른 방법을 통해 설정한 구성은 이러한 설정의 영향을 받지 않습니다.

잠금 모드

ESXi 호스트의 보안 수준을 높이려면 호스트를 잠금 모드로 설정합니다. 잠금 모드에서는 기본적으로 작업을 vCenter Server를 통해 수행해야 합니다.

vSphere 6.0부터 정상 잠금 모드 또는 엄격 잠금 모드를 선택하여 다른 수준의 잠금을 제공할 수 있습니다. 또한 vSphere 6.0에서는 예외 사용자 목록이 도입되었습니다. 예외 사용자는 호스트가 잠금 모드에 들어갈 때 권한을 잃지 않습니다. 예외 사용자 목록을 사용하면 호스트가 잠금 모드에 있을 때 직접 호스트에 액세스해야 하는 외부 애플리케이션 및 타사 솔루션 계정을 추가할 수 있습니다. **잠금 모드 예외 사용자 지정**의 내용을 참조하십시오.



vSphere 6의 잠금 모드

(https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_zg4ylgu0/uiConfId/49694343/)

정상 잠금 모드 및 엄격 잠금 모드

vSphere 6.0부터 정상 잠금 모드 또는 엄격 잠금 모드를 선택하여 다른 수준의 잠금을 제공할 수 있습니다.

정상 잠금 모드

정상 잠금 모드에서는 DCUI 서비스가 중지되지 않습니다. vCenter Server 시스템에 대한 연결이 끊기고 vSphere Web Client를 통한 액세스가 더 이상 사용 가능하지 않은 경우 권한이 있는 계정은 ESXi 호스트의 직접 콘솔 인터페이스에 로그인하여 잠금 모드를 종료할 수 있습니다. 다음 계정만 DCUI(Direct Console User Interface)에 액세스할 수 있습니다.

- 호스트에 대한 관리 권한이 있는, 잠금 모드의 예외 사용자 목록 계정. 예외 사용자 목록은 매우 한정된 작업을 수행하는 서비스 계정을 위한 것입니다. ESXi 관리자를 이 목록에 추가하면 잠금 모드의 목적이 무효화됩니다.
- 호스트에 대해 DCUI.Access 고급 옵션에서 정의된 사용자. 이 옵션은 vCenter Server에 대한 연결이 끊긴 경우 직접 콘솔 인터페이스에 긴급하게 액세스하기 위한 것입니다. 이러한 사용자는 호스트에 대한 관리 권한이 필요하지 않습니다.

엄격 잠금 모드

vSphere 6.0에 새로 도입된 엄격 잠금 모드에서는 DCUI 서비스가 중지됩니다. vCenter Server에 대한 연결이 끊어지고 vSphere Web Client가 더 이상 사용 가능하지 않은 경우 ESXi Shell 및 SSH 서비스가 사용하도록 설정되어 있고 예외 사용자가 정의되어 있지 않는 한 ESXi 호스트가 사용할 수 없게 됩니다. vCenter Server 시스템에 대한 연결을 복원할 수 없는 경우 호스트를 다시 설치해야 합니다.

잠금 모드와 ESXi Shell 및 SSH 서비스

엄격 잠금 모드는 DCUI 서비스를 중지합니다. 그러나 ESXi Shell 및 SSH 서비스는 잠금 모드와 상관이 없습니다. 잠금 모드가 효율적인 보안 대책이 되려면 ESXi Shell 및 SSH 서비스도 사용하지 않도록 설정해야 합니다. 기본적으로 이 서비스는 사용하지 않도록 설정되어 있습니다.

호스트가 잠금 모드에 있을 때 예외 사용자 목록의 사용자에게 호스트에 대한 관리자 역할이 있는 경우 해당 사용자는 ESXi Shell 및 SSH를 통해 호스트에 액세스할 수 있습니다. 이 액세스는 엄격 잠금 모드에서도 가능합니다. ESXi Shell 서비스 및 SSH 서비스를 사용하지 않도록 설정한 상태로 유지하는 것이 가장 안전한 옵션입니다.

참고 예외 사용자 목록은 호스트 백업과 같은 한정된 작업을 수행하는 서비스 계정을 위한 것으로 관리자가 용이 아닙니다. 예외 사용자 목록에 관리자 사용자를 추가하면 잠금 모드의 존재 목적이 무효화됩니다.

잠금 모드 사용 및 사용 안 함

권한 있는 사용자는 여러 가지 방법으로 잠금 모드를 사용하도록 설정할 수 있습니다.

- **호스트 추가** 마법사를 사용하여 vCenter Server 시스템에 호스트를 추가할 때 설정합니다.
- vSphere Web Client를 사용합니다. [vSphere Web Client를 사용하여 잠금 모드 사용](#)의 내용을 참조하십시오. 사용자는 vSphere Web Client에서 정상 잠금 모드와 엄격 잠금 모드를 모두 사용하도록 설정할 수 있습니다.
- DCUI(Direct Console User Interface)를 사용합니다. [Direct Console User Interface에서 정상 잠금 모드 사용 또는 사용 안 함](#)의 내용을 참조하십시오.

권한 있는 사용자는 vSphere Web Client에서 잠금 모드를 사용하지 않도록 설정할 수 있습니다. 직접 콘솔 인터페이스에서 정상 잠금 모드를 사용하지 않도록 설정할 수 있지만 직접 콘솔 인터페이스에서 엄격 잠금 모드를 사용하지 않도록 설정할 수는 없습니다.

참고 DCUI(Direct Console User Interface)를 사용하여 잠금 모드를 사용하거나 사용하지 않도록 설정할 경우 호스트의 사용자 및 그룹에 대한 사용 권한은 무시됩니다. 이러한 사용 권한을 유지하기 위해 vSphere Web Client를 사용하여 잠금 모드를 사용하거나 사용하지 않도록 설정할 수 있습니다.

잠금 모드 동작

잠금 모드에서, 일부 서비스는 사용되지 않도록 설정되고 일부 서비스에는 특정 사용자만 액세스할 수 있습니다.

여러 사용자별 잠금 모드 서비스

호스트가 실행 중일 때 사용 가능한 서비스는 잠금 모드를 사용 설정했는지 여부 및 잠금 모드의 유형에 따라 달라집니다.

- 엄격 및 정상 잠금 모드에서, 권한 있는 사용자는 vCenter Server를 통해(vSphere Web Client에서 또는 vSphere Web Services SDK를 사용하여) 호스트에 액세스할 수 있습니다.
- DCUI(Direct Console Interface) 동작은 엄격 잠금 모드와 정상 잠금 모드에서 서로 다릅니다.
 - 엄격 잠금 모드에서 DCUI(Direct Console User Interface) 서비스는 사용되지 않도록 설정됩니다.
 - 정상 잠금 모드에서 관리자 권한이 있는 예외 사용자 목록의 계정과 DCUI.Access 고급 시스템 설정에서 지정된 사용자는 DCUI(Direct Console Interface)에 액세스할 수 있습니다.
- ESXi Shell 또는 SSH가 사용 설정되고 호스트가 엄격 또는 정상 잠금 모드로 설정된 경우 관리자 권한이 있는 예외 사용자 목록의 계정은 이러한 서비스를 사용할 수 있습니다. 기타 모든 사용자의 경우, ESXi Shell 또는 SSH 액세스가 사용되지 않도록 설정됩니다. vSphere 6.0부터 관리자 권한이 없는 사용자에게 대한 ESXi 또는 SSH 세션이 종료됩니다.

엄격 및 정상 잠금 모드 모두에 대해 모든 액세스가 기록됩니다.

표 5-9. 잠금 모드 동작

서비스	정상 모드	정상 잠금 모드	엄격 잠금 모드
vSphere Web Services API	모든 사용자, 권한 기반	vCenter(vpxuser) 예외 사용자, 권한 기반 vCloud Director(vslauser, 사용 가능한 경우)	vCenter(vpxuser) 예외 사용자, 권한 기반 vCloud Director(vslauser, 사용 가능한 경우)
CIM Providers	호스트에서 관리자 권한이 있는 사용자	vCenter(vpxuser) 예외 사용자, 권한 기반. vCloud Director(vslauser, 사용 가능한 경우)	vCenter(vpxuser) 예외, 권한 기반. vCloud Director(vslauser, 사용 가능한 경우)
DCUI(Direct Console User Interface)	호스트에서 관리자 권한이 있는 사용자, DCUI.Access 고급 옵션의 사용자	DCUI.Access 고급 옵션에서 정의된 사용자 호스트에서 관리자 권한이 있는 예외 사용자	DCUI 서비스가 중단됨
ESXi Shell (사용 설정된 경우)	호스트에서 관리자 권한이 있는 사용자	DCUI.Access 고급 옵션에서 정의된 사용자 호스트에서 관리자 권한이 있는 예외 사용자	DCUI.Access 고급 옵션에서 정의된 사용자 호스트에서 관리자 권한이 있는 예외 사용자
SSH (사용 설정된 경우)	호스트에서 관리자 권한이 있는 사용자	DCUI.Access 고급 옵션에서 정의된 사용자 호스트에서 관리자 권한이 있는 예외 사용자	DCUI.Access 고급 옵션에서 정의된 사용자 호스트에서 관리자 권한이 있는 예외 사용자

잠금 모드가 사용 설정되었을 때 ESXi Shell에 로그인한 사용자

잠금 모드가 사용 설정되기 전에 사용자가 ESXi Shell에 로그인했거나 SSH를 통해 호스트에 액세스한 경우 예외 사용자 목록에 있고 호스트에서 관리자 권한이 있는 사용자는 계속 로그인된 상태로 남아 있습니다. vSphere 6.0부터 기타 모든 사용자에게 대해 세션이 종료됩니다. 이것은 정상 및 엄격 잠금 모드에 모두 적용됩니다.

vSphere Web Client를 사용하여 잠금 모드 사용

모든 구성 변경 내용이 vCenter Server에 적용되지 않도록 하려면 잠금 모드를 사용합니다. vSphere 6.0 이상은 정상 잠금 모드와 엄격 잠금 모드를 지원합니다.

호스트에 대한 모든 직접 액세스를 완전하게 허용하지 않으려면 엄격 잠금 모드를 선택하면 됩니다. 엄격 잠금 모드는 vCenter Server를 사용할 수 없고 SSH와 ESXi Shell이 해제된 경우 호스트에 액세스할 수 없도록 합니다. [잠금 모드 동작](#)를 참조하십시오.

절차

- 1 vSphere Web Client 인벤토리에서 호스트를 찾습니다.
- 2 **관리** 탭을 클릭하고 **설정**을 클릭합니다.
- 3 시스템 아래에서 **보안 프로파일**을 선택합니다.
- 4 [잠금 모드] 패널에서 **편집**을 클릭합니다.
- 5 **잠금 모드**를 클릭하고 잠금 모드 옵션 중 하나를 선택합니다.

옵션	설명
일반	vCenter Server를 통해 호스트에 액세스할 수 있습니다. 예외 사용자 목록에 있고 관리자 권한을 가진 사용자만 DCUI(Direct Console User Interface)에 로그인할 수 있습니다. SSH 또는 ESXi Shell이 사용 설정된 경우 액세스가 가능할 수 있습니다.
엄격	vCenter Server를 통해서만 호스트에 액세스할 수 있습니다. SSH 또는 ESXi Shell이 사용 설정된 경우 DCUI.Access 고급 옵션의 계정 및 관리자 권한이 있는 예외 사용자 계정에 대해 실행 중인 세션은 사용 상태로 유지되고 기타 모든 세션은 종료됩니다.

- 6 **확인**을 클릭합니다.

vSphere Web Client를 사용하여 잠금 모드 사용 안 함

ESXi 호스트에 대한 직접 연결의 구성 변경 사항을 허용하도록 잠금 모드를 사용하지 않도록 설정합니다. 잠금 모드를 사용하도록 설정된 상태로 두면 보다 안전한 환경을 구현할 수 있습니다.

vSphere 6.0에서 다음과 같이 잠금 모드를 사용하지 않도록 설정할 수 있습니다.

vSphere Web Client에서

사용자는 vSphere Web Client에서 정상 잠금 모드와 엄격 잠금 모드를 모두 사용하지 않도록 설정할 수 있습니다.

DCUI(Direct Console User Interface)에서

ESXi 호스트의 DCUI(Direct Console User Interface)에 액세스할 수 있는 사용자는 정상 잠금 모드를 사용하지 않도록 설정할 수 있습니다. 엄격 잠금 모드에서는 DCUI(Direct Console Interface) 서비스가 중지됩니다.

절차

- 1 vSphere Web Client 인벤토리에서 호스트를 찾습니다.
- 2 **관리** 탭을 클릭하고 **설정**을 클릭합니다.
- 3 시스템 아래에서 **보안 프로파일**을 선택합니다.
- 4 [잠금 모드] 패널에서 **편집**을 클릭합니다.
- 5 **잠금 모드**를 클릭하고 **없음**을 선택하여 잠금 모드를 사용하지 않도록 설정합니다.

결과

시스템이 잠금 모드를 종료하고 vCenter Server가 정보를 표시하고 항목이 감사 로그에 추가됩니다.

Direct Console User Interface에서 정상 잠금 모드 사용 또는 사용 안 함

DCUI(Direct Console User Interface)에서 정상 잠금 모드를 사용 및 사용하지 않도록 설정할 수 있습니다. 엄격 잠금 모드는 vSphere Web Client에서만 사용 및 사용하지 않도록 설정할 수 있습니다.

호스트가 정상 잠금 모드에 있을 때 DCUI(Direct Console User Interface)에 액세스할 수 있는 계정은 다음과 같습니다.

- 호스트에 대한 관리자 권한을 가지고 있는 예외 사용자 목록의 계정. 예외 사용자 목록은 백업 에이전트와 같은 서비스 계정용입니다.
- 호스트에 대해 DCUI.Access 고급 옵션에서 정의된 사용자. 이 옵션을 사용하면 심각한 오류가 발생했을 때 액세스를 활성화할 수 있습니다.

ESXi 6.0 이상의 경우, 잠금 모드를 사용하도록 설정하면 사용자 권한이 보존되고 DCUI(Direct Console Interface)에서 잠금 모드를 사용하지 않도록 설정하면 사용자 권한이 복원됩니다.

참고 잠금 모드에 있는 호스트를 잠금 모드 종료 없이 ESXi 버전 6.0으로 업그레이드하고 업그레이드 후에 잠금 모드를 종료하면 호스트가 잠금 모드로 들어가기 전에 정의된 모든 사용 권한은 손실됩니다. 시스템에서는 호스트를 액세스 가능한 상태로 유지할 수 있도록 DCUI.Access 고급 옵션에 있는 모든 사용자에게 관리자 역할을 할당합니다.

사용 권한을 유지하려면 업그레이드하기 전에 vSphere Web Client에서 호스트에 대해 잠금 모드를 사용하지 않도록 설정하십시오.

절차

- 1 호스트의 DCUI(Direct Console User Interface)에서 F2 키를 누르고 로그인합니다.
- 2 **잠금 모드 구성** 설정으로 스크롤하고 Enter 키를 눌러 현재 설정을 전환합니다.
- 3 Direct Console User Interface의 기본 메뉴로 돌아갈 때까지 Esc 키를 누릅니다.

잠금 모드에서 액세스 권한을 가진 계정 지정

서비스 계정을 예외 사용자 목록에 추가하여 ESXi 호스트에 직접 액세스할 수 있는 서비스 계정을 지정할 수 있습니다. 심각한 vCenter Server 오류가 발생하는 경우 ESXi 호스트에 액세스할 수 있는 단일 사용자를 지정할 수 있습니다.

잠금 모드가 설정되었을 때 각 계정에서 기본적으로 수행할 수 있는 작업과 기본 동작을 변경할 수 있는 방법은 vSphere 환경의 버전에 따라 다릅니다.

- vSphere 5.1 이전 버전의 vSphere에서는 루트 사용자만 잠금 모드에 있는 ESXi 호스트의 DCUI(Direct Console User Interface)에 로그인할 수 있습니다.
- vSphere 5.1 이상에서는 각 호스트의 DCUI.Access 고급 시스템 설정에 사용자를 추가할 수 있습니다. 이 옵션은 vCenter Server에 심각한 오류가 발생하는 경우를 위한 것으로 일반적으로 이 액세스 권한이 있는 사용자의 암호가 안전하게 잠깁니다. DCUI.Access 목록의 사용자는 호스트에 대한 전체 관리 권한이 필요하지 않습니다.
- vSphere 6.0 이상에서 DCUI.Access 고급 시스템 설정은 계속 지원됩니다. 또한 vSphere 6.0 이상은 예외 사용자 목록을 지원하는데, 이는 호스트에 직접 로그인해야 하는 서비스 계정을 위한 것입니다. 예외 사용자 목록에 있는 관리자 권한을 가진 계정은 ESXi Shell에 로그인할 수 있습니다. 또한 그러한 사용자는 정상 잠금 모드에 있는 호스트의 DCUI에 로그인할 수 있으며 잠금 모드를 종료할 수 있습니다.

예외 사용자는 vSphere Web Client에서 지정합니다.

참고 예외 사용자는 ESXi 호스트에 대해 로컬로 정의된 권한을 가진 Active Directory 사용자 또는 호스트 로컬 사용자로서 호스트가 잠금 모드에 있는 경우 Active Directory 그룹의 멤버인 사용자가 자신의 사용 권한을 잃을 수 있습니다.

DCUI.Access 고급 옵션에 사용자 추가

DCUI.Access 고급 옵션의 주 목적은 vCenter Server에서 호스트에 액세스할 수 없을 때 심각한 오류가 발생하면 잠금 모드를 종료할 수 있도록 하는 것입니다. vSphere Web Client에서 호스트에 대한 고급 설정을 편집하여 사용자를 목록에 추가합니다.

참고 DCUI.Access 목록의 사용자는 권한과 관계없이 잠금 모드 설정을 변경할 수 있습니다. 이는 호스트의 보안에 영향을 미칠 수 있습니다. 호스트에 직접 액세스해야 하는 서비스 계정의 경우에는 사용자를 예외 사용자 목록에 추가하는 것을 고려하십시오. 예외 사용자는 권한이 있는 작업만 수행할 수 있습니다. [잠금 모드 예외 사용자 지정](#)을 참조하십시오.

절차

- 1 vSphere Web Client 개체 탐색기에서 호스트를 찾습니다.
- 2 **관리** 탭을 클릭하고 **설정**을 선택합니다.
- 3 **고급 시스템 설정**을 클릭하고 **DCUI.Access**를 선택합니다.

4 편집을 클릭하고 사용자 이름을 쉼표로 구분해 입력합니다.

기본적으로 루트 사용자가 포함됩니다. DCUI.Access 목록에서 루트를 제거하고 감사 가능성 향상을 위해 명명된 계정을 지정하는 것을 고려해 보십시오.

5 확인을 클릭합니다.

잠금 모드 예외 사용자 지정

vSphere 6.0 이상에서는 vSphere Web Client의 예외 사용자 목록에 사용자를 추가할 수 있습니다. 이러한 사용자는 호스트가 잠금 모드에 들어갈 때 권한을 잃지 않습니다. 예외 사용자 목록에 백업 에이전트와 같은 서비스 계정을 추가합니다.

예외 사용자는 호스트가 잠금 모드에 들어갈 때 권한을 잃지 않습니다. 보통 이러한 계정은 잠금 모드에서 계속 작동해야 하는 타사 솔루션과 외부 애플리케이션을 나타냅니다.

참고 예외 사용자 목록은 매우 한정된 작업을 수행하는 서비스 계정에 대한 것으로 관리자용이 아닙니다. 예외 사용자 목록에 관리자 사용자를 추가하면 잠금 모드의 존재 목적이 무효화됩니다.

예외 사용자는 ESXi 호스트에 대해 로컬로 정의된 권한을 가진 Active Directory 사용자 또는 호스트 로컬 사용자로서 Active Directory 그룹의 멤버가 아니며 vCenter Server 사용자가 아닙니다. 이러한 사용자는 해당 권한을 기반으로 호스트에서 작업을 수행할 수 있습니다. 이것은 예를 들어 읽기 전용 사용자가 호스트에서 잠금 모드를 사용하지 않도록 설정할 수 없음을 의미합니다.

절차

- 1 vSphere Web Client 인벤토리에서 호스트를 찾습니다.
- 2 **관리** 탭을 클릭하고 **설정**을 클릭합니다.
- 3 시스템 아래에서 **보안 프로파일**을 선택합니다.
- 4 [잠금 모드] 패널에서 **편집**을 클릭합니다.
- 5 **예외 사용자**를 클릭하고 더하기 아이콘을 클릭하여 예외 사용자를 추가합니다.

호스트 및 VIB의 수락 수준 확인

ESXi 호스트의 무결성을 보호하려면 사용자가 서명되지 않은(커뮤니티 지원) VIB를 설치하도록 허용하지 마십시오. 서명되지 않은 VIB에는 VMware 또는 VMware 파트너가 인증, 수락 또는 지원하지 않는 코드가 포함되어 있습니다. 커뮤니티 지원 VIB에는 디지털 서명이 없습니다.

ESXCLI 명령을 사용하여 호스트의 수락 수준을 설정할 수 있습니다. 호스트의 수락 수준은 호스트에 추가하려는 VIB의 수락 수준과 같거나 이보다 덜 제한적이어야 합니다. ESXi 호스트의 보안 및 무결성을 보호하려면 운영 시스템에 있는 호스트에 서명되지 않은(CommunitySupported) VIB를 설치하도록 허용하지 마십시오.

지원되는 수락 수준은 다음과 같습니다.

VMwareCertified

VMwareCertified 허용 수준은 요구 사항이 가장 엄격합니다. 이 수준이 지정된 VIB는 동일한 기술에 대한 VMware의 내부 품질 관리 테스트와 동등한 철저한 테스트 과정을 거칩니다. 현재는 IOVP 드라이버만 이 수준으로 게시됩니다. VMware에서는 이 허용 수준이 지정된 VIB에 대한 지원 문의를 받습니다.

VMwareAccepted

이 허용 수준이 지정된 VIB는 검증 테스트 과정을 거치지만 이 테스트는 소프트웨어의 기능 중 일부만 테스트합니다. 테스트는 파트너가 실행하고 VMware에서는 결과를 확인합니다. 현재 이 수준으로 게시되는 VIB로는 CIM 제공자와 PSA 플러그인이 있습니다. VMware는 이 허용 수준이 지정된 VIB에 대한 지원 문의를 파트너의 지원 조직에 전달합니다.

PartnerSupported

PartnerSupported 허용 수준이 지정된 VIB는 VMware에서 신뢰하는 파트너가 게시합니다. 모든 테스트는 파트너가 수행하며 VMware는 결과를 확인하지 않습니다. 이 수준은 파트너가 VMware 시스템에 제공하려고 하는 새로운 기술 또는 비주류 기술에 사용됩니다. 현재 Infiniband, ATAoE 및 SSD 같은 드라이버 VIB 기술이 비표준 하드웨어 드라이버와 함께 이 수준으로 설정됩니다. VMware는 이 허용 수준이 지정된 VIB에 대한 지원 문의를 파트너의 지원 조직에 전달합니다.

CommunitySupported

CommunitySupported 허용 수준은 VMware 파트너 프로그램과 관련 없는 개인이나 회사에서 생성한 VIB에 적용됩니다. 이 수준의 VIB는 VMware에서 승인한 테스트 프로그램을 거치지 않았으며 VMware 기술 지원이나 VMware 파트너가 지원하지 않습니다.

절차

- 1 각 ESXi 호스트에 연결하고, 다음 명령을 실행하여 수락 수준이 VMwareCertified 또는 VMwareAccepted로 설정되어 있는지 확인합니다.

```
esxcli software acceptance get
```

- 2 호스트의 수락 수준이 VMwareCertified 또는 VMwareAccepted가 아닌 경우 다음 명령을 실행하여 VMwareCertified 또는 VMwareAccepted 수준에 해당하지 않는 VIB가 있는지 확인합니다.

```
esxcli software vib list
esxcli software vib get -n vibname
```

- 3 다음 명령을 실행하여 PartnerSupported 또는 CommunitySupported 수준에 해당하는 VIB를 모두 제거합니다.

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

- 4 다음 명령을 실행하여 호스트의 수락 수준을 변경합니다.

```
esxcli software acceptance set --level acceptance_level
```

ESXi에 대한 사용 권한 할당

대부분의 경우 vCenter Server 시스템이 관리하는 ESXi 호스트 개체에 사용 권한을 할당하여 사용자에게 권한을 부여합니다. 독립형 ESXi 호스트를 사용하는 경우 권한을 직접 할당할 수 있습니다.

vCenter Server가 관리하는 ESXi 호스트에 사용 권한 할당

vCenter Server가 ESXi 호스트를 관리하는 경우 vSphere Web Client를 통해 관리 작업을 수행합니다.

vCenter Server 개체 계층에서 ESXi 호스트 개체를 선택하고 ESXi 호스트에서 직접 관리를 수행할 수 있는 제한된 수의 사용자에게 관리자 역할을 할당할 수 있습니다. [역할을 사용하여 권한 할당](#)의 내용을 참조하십시오.

가장 좋은 방법은 명명된 사용자 계정을 1개 이상 생성하고 호스트에 전체 관리 권한을 할당한 다음 이 계정을 루트 계정 대신 사용하는 것입니다. 루트 계정에 매우 복잡한 암호를 설정하며 루트 계정의 사용을 제한합니다. (루트 계정은 제거하지 마십시오.)

독립형 ESXi 호스트에 사용 권한 할당

환경에 vCenter Server 시스템이 포함되지 않는 경우 다음 사용자가 미리 정의됩니다.

- 루트 사용자. [루트 사용자 권한](#)의 내용을 참조하십시오.
- vpxuser. [vpxuser 권한](#)의 내용을 참조하십시오.
- dcui 사용자. [dcui 사용자 권한](#)의 내용을 참조하십시오.

로컬 사용자를 추가하고 vSphere Client의 관리 탭에서 사용자 지정 역할을 정의할 수 있습니다.

모든 ESXi 버전에 대해 미리 정의된 사용자 목록을 /etc/passwd 파일에서 볼 수 있습니다.

다음 역할이 미리 정의됩니다.

읽기 전용

사용자가 ESXi 호스트와 연결된 개체를 보지만 개체를 변경하지는 못하도록 합니다.

관리자

관리자 역할입니다.

권한 없음

권한이 없습니다. 이 옵션이 기본값입니다. 필요한 경우 기본값을 재정의할 수 있습니다.

ESXi 호스트에 직접 연결된 vSphere Client를 사용하여 로컬 사용자 및 그룹을 관리하고 로컬 사용자 지정 역할을 ESXi 호스트에 추가할 수 있습니다.

vSphere 6.0부터 ESXi 로컬 사용자 계정 관리에 ESXCLI 계정 관리 명령을 사용할 수 있습니다. Active Directory 계정(사용자 및 그룹)과 ESXi 로컬 계정(사용자만) 모두에 대한 사용 권한 설정 또는 제거에 ESXCLI 사용 권한 관리 명령을 사용할 수 있습니다.

참고 호스트에 직접 연결하여 ESXi 호스트에 대한 사용자를 정의하고 동일한 이름의 사용자가 vCenter Server에도 있는 경우 해당 사용자가 다릅니다. 사용자 중 한 명에게 역할을 할당하는 경우 다른 사용자에게는 동일한 역할이 할당되지 않습니다.

루트 사용자 권한

기본적으로 각 ESXi 호스트에는 관리자 역할이 있는 단일 루트 사용자 계정이 있습니다. 해당 루트 사용자 계정은 로컬 관리에 사용할 수 있으며 호스트를 vCenter Server에 연결하는 데 사용할 수 있습니다.

이 공통 루트 계정은 ESXi 호스트에 진입하기가 더욱 쉽게 하고 작업을 특정 관리자에게 일치시키기가 더욱 어렵게 할 수 있습니다.

루트 계정에 매우 복잡한 암호를 설정하고 vCenter Server에 호스트를 추가하는 등의 경우에 사용하기 위한 루트 계정의 사용을 제한합니다. 루트 계정은 제거하지 마십시오. vSphere 5.1 이상에서는 관리자 역할이 있는 다른 명명된 사용자가 아닌 루트 사용자만 vCenter Server에 호스트를 추가할 수 있습니다.

가장 좋은 방법은 ESXi 호스트에서 관리자 역할이 있는 계정이 명명된 계정이 있는 특정 사용자에게 할당되었는지 확인하는 것입니다. ESXi Active Directory 기능을 사용하여 가능한 경우 Active Directory 자격 증명을 관리합니다.

중요 루트 사용자용 액세스 권한을 제거하는 경우 우선 관리자 역할에 할당된 다른 사용자가 있는 루트 수준에서 또 다른 사용 권한을 생성해야 합니다.

vpxuser 권한

vCenter Server에서는 호스트의 작업을 관리할 때 vpxuser 권한을 사용합니다.

vCenter Server에는 관리하는 호스트에 대한 관리자 권한이 있습니다. 예를 들어 vCenter Server에서는 가상 시스템을 호스트 간에 이동하고 가상 시스템을 지원하는 데 필요한 구성 변경 작업을 수행할 수 있습니다.

vCenter Server 관리자는 호스트에서 루트 사용자와 동일한 작업을 대부분 수행할 수 있으며 작업을 스케줄링하고 템플릿 등과 관련된 작업도 수행할 수 있습니다. 그러나 vCenter Server 관리자는 호스트의 로컬 사용자 및 그룹을 직접 만들거나 삭제하거나 편집할 수 없습니다. 이러한 작업은 각 호스트에 대해 직접적인 관리자 사용 권한이 있는 사용자만 수행할 수 있습니다.

참고 Active Directory를 사용하여 vpxuser를 관리할 수는 없습니다.

경고 어떠한 방법으로도 vpxuser를 변경하지 마십시오. 암호 및 사용 권한을 변경하면 안 됩니다. 암호나 사용 권한을 변경하면 vCenter Server를 통해 호스트에 대한 작업을 수행할 때 문제가 발생할 수 있습니다.

dcui 사용자 권한

dcui 사용자는 관리자 권한으로 호스트에서 실행됩니다. 이 사용자는 기본적으로 DCUI(Direct Console User Interface)에서 호스트를 잠금 모드로 구성하기 위한 용도로 사용됩니다.

이 사용자는 직접 콘솔의 에이전트 역할을 하므로 대화형 사용자가 수정하거나 사용할 수 없습니다.

Active Directory를 통해 ESXi 사용자 관리

Active Directory와 같은 디렉토리 서비스를 사용하여 사용자를 관리하도록 ESXi를 구성할 수 있습니다.

각 호스트에서 로컬 사용자 계정을 생성하면 여러 호스트에서 계정 이름과 암호를 동기화해야 하는 번거로움이 있습니다. ESXi 호스트를 Active Directory 도메인에 가입하면 로컬 사용자 계정을 생성하고 유지할 필요가 없습니다. Active Directory를 사용하여 사용자를 인증하면 ESXi 호스트 구성이 간소화되고 무단 액세스가 발생할 수 있는 구성 문제의 위험이 줄어듭니다.

Active Directory를 사용할 경우 사용자는 도메인에 호스트를 추가할 때 자신의 Active Directory 자격 증명과 Active Directory 서버의 도메인 이름을 제공합니다.

vSphere Authentication Proxy 설치 또는 업그레이드

vSphere Authentication Proxy를 설치하면 ESXi 호스트가 Active Directory 자격 증명을 사용하지 않고 도메인에 가입할 수 있습니다. vSphere Authentication Proxy를 사용하면 호스트 구성에 Active Directory 자격 증명을 저장할 필요가 없으므로 Auto Deploy를 사용해 프로비저닝된 호스트 및 PXE 부팅 호스트에 대한 보안이 향상됩니다.

시스템에 이전 버전의 vSphere Authentication Proxy가 설치되어 있는 경우 이 절차에서는 vSphere Authentication Proxy를 현재 버전으로 업그레이드합니다.

연결된 vCenter Server와 동일한 시스템 또는 vCenter Server에 대한 네트워크 연결이 있는 다른 시스템에 vSphere Authentication Proxy를 설치할 수 있습니다. vSphere Authentication Proxy는 vCenter Server 버전 5.0 이상에서 지원됩니다.

vSphere Authentication Proxy 서비스는 vCenter Server와의 통신을 위해 IPv4 주소에 바인딩되지만 IPv6은 지원하지 않습니다. vCenter Server 인스턴스는 IPv4 전용, IPv4/IPv6 혼합 모드 또는 IPv6 전용 네트워크 환경의 호스트 시스템에 있을 수 있지만 vSphere Web Client를 통해 vCenter Server에 연결하는 시스템에는 IPv4 주소가 있어야 vSphere Authentication Proxy 서비스가 작동합니다.

사전 요구 사항

- vSphere Authentication Proxy를 설치하려는 시스템에 Microsoft .NET Framework 3.5를 설치합니다.
- 관리자 권한이 있는지 확인해야 합니다.
- 호스트 시스템에 지원되는 프로세서와 운영 체제가 있는지 확인합니다.
- 호스트 시스템에 유효한 IPv4 주소가 있는지 확인합니다. IPv4 전용 또는 IPv4/IPv6 혼합 모드 네트워크 환경의 시스템에 vSphere Authentication Proxy를 설치할 수 있지만 IPv6 전용 환경의 시스템에는 vSphere Authentication Proxy를 설치할 수 없습니다.

- Windows Server 2008 R2 호스트 시스템에 vSphere Authentication Proxy를 설치하는 경우 support.microsoft.com 웹 사이트에서 Windows KB 문서 981506에 설명되어 있는 Windows 핫픽스를 다운로드하여 설치합니다. 이 핫픽스를 설치하지 않으면 vSphere Authentication Proxy 어댑터가 초기화되지 않습니다. 이 문제가 발생하면 camadapter.log에 CTL을 사용한 CAM 웹 사이트 바인딩 실패 및 CAMAdapter 초기화 실패와 유사한 내용의 오류 메시지가 기록됩니다.

- vCenter Server 설치 관리자를 다운로드합니다.

다음과 같은 정보를 수집하여 설치 또는 업그레이드를 완료합니다.

- vSphere Authentication Proxy 설치 위치(기본 위치를 사용하지 않는 경우).
- vSphere Authentication Proxy가 연결할 vCenter Server의 주소 및 자격 증명: IP 주소 또는 이름, HTTP 포트, 사용자 이름 및 암호.
- 네트워크에서 vSphere Authentication Proxy를 식별하는 호스트 이름 또는 IP 주소.

절차

- 1 Authentication Proxy 서비스를 설치할 호스트 컴퓨터를 도메인에 추가합니다.
- 2 도메인 관리자 계정을 사용하여 호스트 컴퓨터에 로그인합니다.
- 3 소프트웨어 설치 관리자 디렉토리에서 autorun.exe 파일을 두 번 클릭하여 설치 관리자를 시작합니다.
- 4 VMware vSphere Authentication Proxy를 선택하고 **설치**를 클릭합니다.
- 5 마법사의 지시에 따라 설치 또는 업그레이드를 완료합니다.

설치하는 동안 Auto Deploy가 등록된 vCenter Server 인스턴스에 인증 서비스가 등록됩니다.

결과

vSphere Authentication Proxy 서비스를 설치할 때 설치 관리자는 Authentication Proxy 서비스를 실행할 수 있는 적절한 권한을 가진 도메인 계정을 생성합니다. 계정 이름은 접두사 CAM-으로 시작되며 계정과 연결된 임의의 생성 암호 32자를 포함합니다. 암호는 만료되지 않도록 설정됩니다. 계정 설정은 변경하지 마십시오.

Active Directory를 사용하도록 호스트 구성

Active Directory와 같은 디렉토리 서비스를 사용하여 사용자와 그룹을 관리하도록 호스트를 구성할 수 있습니다.

ESXi 호스트를 Active Directory에 추가할 때 DOMAIN 그룹 **ESX Admins**가 있으면 호스트에 대한 전체 관리자 액세스 권한이 이 그룹에 할당됩니다. 전체 관리자 액세스 권한을 부여하지 않으려면 VMware 기술 자료 문서 1025569에서 해결 방법을 참조하십시오.

호스트가 Auto Deploy를 사용하여 프로비저닝된 경우 Active Directory 자격 증명을 해당 호스트에 저장할 수 없습니다. vSphere Authentication Proxy를 사용하여 호스트를 Active Directory 도메인에 가입시킬 수 있습니다. vSphere Authentication Proxy와 호스트 간에 신뢰 체인이 있으므로 Authentication Proxy는 호스트를 Active Directory 도메인에 가입시킬 수 있습니다. [vSphere Authentication Proxy 사용](#)을 참조하십시오.

참고 Active Directory에서 사용자 계정 설정을 정의할 때 컴퓨터 이름을 기준으로 사용자가 로그인할 수 있는 컴퓨터를 제한할 수 있습니다. 기본적으로 사용자 계정에 이러한 제한이 설정되지 않습니다. 이 제한을 설정하면 해당 사용자 계정에 대한 LDAP 바인딩 요청이 실패하고 LDAP 바인딩 실패 메시지가 표시됩니다. 나열된 컴퓨터에서 요청하는 경우에도 마찬가지입니다. 사용자 계정이 로그인할 수 있는 컴퓨터 목록에 Active Directory 서버의 netBIOS 이름을 추가하여 이 문제를 방지할 수 있습니다.

사전 요구 사항

- Active Directory 도메인이 있는지 확인합니다. 디렉토리 서버 설명서를 참조하십시오.
- ESXi의 호스트 이름이 Active Directory 포리스트의 도메인 이름으로 정규화되어 있는지 확인합니다.

정규화된 도메인 이름 = host_name.domain_name

절차

- 1 NTP를 사용하여 ESXi와 디렉토리 서비스 시스템 간의 시간을 동기화합니다.

Microsoft 도메인 컨트롤러와 ESXi 시간을 동기화하는 방법에 대한 자세한 내용은 VMware 기술 자료의 [네트워크 시간 서버와 ESXi 클럭 동기화](#)를 참조하십시오.

- 2 호스트에 대해 구성된 DNS 서버에서 Active Directory 컨트롤러의 호스트 이름을 확인할 수 있는지 확인합니다.
 - a vSphere Web Client 개체 탐색기에서 호스트를 찾습니다.
 - b **관리** 탭을 클릭하고 **네트워킹**을 클릭합니다.
 - c DNS를 클릭하고 호스트에 대한 호스트 이름과 DNS 서버 정보가 올바른지 확인합니다.

다음에 수행할 작업

vSphere Web Client를 사용하여 디렉토리 서비스 도메인에 가입합니다. Auto Deploy를 사용하여 프로비저닝된 호스트의 경우 vSphere Authentication Proxy를 설정합니다. [vSphere Authentication Proxy 사용](#)을 참조하십시오.

디렉토리 서비스 도메인에 호스트 추가

호스트가 디렉토리 서비스를 사용하도록 하려면 호스트를 디렉토리 서비스 도메인에 가입시켜야 합니다. 두 가지 방법 중 하나로 도메인 이름을 입력할 수 있습니다.

- **name.tld**(예: **domain.com**): 계정이 기본 컨테이너 아래에 생성됩니다.
- **name.tld/container/path**(예: **domain.com/OU1/OU2**): 계정이 특정 OU(조직 구성 단위) 아래에 생성됩니다.

vSphere Authentication Proxy 서비스를 사용하려면 [vSphere Authentication Proxy 사용](#)을 참조하십시오.

절차

- 1 vSphere Web Client 인벤토리에서 호스트를 찾습니다.
- 2 **관리** 탭을 클릭하고 **설정**을 클릭합니다.
- 3 시스템 아래에서 **인증 서비스**를 선택합니다.
- 4 **도메인 가입**을 클릭합니다.
- 5 도메인을 입력합니다.

name.tld 또는 **name.tld/container/path** 형식을 사용합니다.
- 6 도메인에 호스트를 가입시킬 수 있는 사용 권한이 있는 디렉토리 서비스 사용자의 사용자 이름 및 암호를 입력하고 **확인**을 클릭합니다.
- 7 (선택 사항) 인증 프록시를 사용하려면 프록시 서버 IP 주소를 입력합니다.
- 8 **확인**을 클릭하여 [디렉토리 서비스 구성] 대화상자를 닫습니다.

디렉토리 서비스 설정 보기

호스트가 사용자를 인증하는 데 사용하는 디렉토리 서버(있는 경우)의 유형과 디렉토리 서버 설정을 볼 수 있습니다.

절차

- 1 vSphere Web Client 인벤토리에서 호스트를 찾습니다.
- 2 **관리** 탭을 클릭하고 **설정**을 클릭합니다.
- 3 시스템 아래에서 **인증 서비스**를 선택합니다.

[인증 서비스] 페이지에 디렉토리 서비스 및 도메인 설정이 표시됩니다.

vSphere Authentication Proxy 사용

vSphere Authentication Proxy를 사용하는 경우에는 Active Directory 자격 증명을 호스트로 전송하지 않아도 됩니다. 호스트를 도메인에 추가할 때 사용자가 Active Directory 서버의 도메인 이름과 인증 프록시 서버의 IP 주소를 제공합니다.

vSphere Authentication Proxy는 Auto Deploy와 함께 사용될 때 특히 유용합니다. Authentication Proxy를 가리키는 참조 호스트를 설정하고 참조 호스트의 프로파일을 Auto Deploy를 통해 프로비저닝된 모든 ESXi 호스트에 적용하는 규칙을 설정합니다. VMCA를 통해 프로비저닝된 인증서 또는 타사 인증서를 사용하는 환경에서 vSphere Authentication Proxy를 사용하더라도 Auto Deploy를 사용한 사용자 지정 인증서 사용에 대한 지침을 따르기만 하면 프로세스가 원활하게 작동합니다. [Auto Deploy와 함께 사용자 지정 인증서 사용](#)의 내용을 참조하십시오.

참고 IPv6만 지원하는 환경에서는 vSphere Authentication Proxy를 사용할 수 없습니다.

vSphere Authentication Proxy 설치 또는 업그레이드

vSphere Authentication Proxy를 설치하면 ESXi 호스트가 Active Directory 자격 증명을 사용하지 않고 도 도메인에 가입할 수 있습니다. vSphere Authentication Proxy를 사용하면 호스트 구성에 Active Directory 자격 증명을 저장할 필요가 없으므로 Auto Deploy를 사용해 프로비저닝된 호스트 및 PXE 부팅 호스트에 대한 보안이 향상됩니다.

시스템에 이전 버전의 vSphere Authentication Proxy가 설치되어 있는 경우 이 절차에서는 vSphere Authentication Proxy를 현재 버전으로 업그레이드합니다.

연결된 vCenter Server와 동일한 시스템 또는 vCenter Server에 대한 네트워크 연결이 있는 다른 시스템에 vSphere Authentication Proxy를 설치할 수 있습니다. vSphere Authentication Proxy는 vCenter Server 버전 5.0 이상에서 지원됩니다.

vSphere Authentication Proxy 서비스는 vCenter Server와의 통신을 위해 IPv4 주소에 바인딩되지만 IPv6은 지원하지 않습니다. vCenter Server 인스턴스는 IPv4 전용, IPv4/IPv6 혼합 모드 또는 IPv6 전용 네트워크 환경의 호스트 시스템에 있을 수 있지만 vSphere Web Client를 통해 vCenter Server에 연결하는 시스템에는 IPv4 주소가 있어야 vSphere Authentication Proxy 서비스가 작동합니다.

사전 요구 사항

- vSphere Authentication Proxy를 설치하려는 시스템에 Microsoft .NET Framework 3.5를 설치합니다.
- 관리자 권한이 있는지 확인해야 합니다.
- 호스트 시스템에 지원되는 프로세서와 운영 체제가 있는지 확인합니다.
- 호스트 시스템에 유효한 IPv4 주소가 있는지 확인합니다. IPv4 전용 또는 IPv4/IPv6 혼합 모드 네트워크 환경의 시스템에 vSphere Authentication Proxy를 설치할 수 있지만 IPv6 전용 환경의 시스템에는 vSphere Authentication Proxy를 설치할 수 없습니다.
- Windows Server 2008 R2 호스트 시스템에 vSphere Authentication Proxy를 설치하는 경우 support.microsoft.com 웹 사이트에서 Windows KB 문서 981506에 설명되어 있는 Windows 핫픽스를 다운로드하여 설치합니다. 이 핫픽스를 설치하지 않으면 vSphere Authentication Proxy 어댑터가 초기화되지 않습니다. 이 문제가 발생하면 camadapter.log에 CTL을 사용한 CAM 웹 사이트 바인딩 실패 및 CAMAdapter 초기화 실패와 유사한 내용의 오류 메시지가 기록됩니다.
- vCenter Server 설치 관리자를 다운로드합니다.

다음과 같은 정보를 수집하여 설치 또는 업그레이드를 완료합니다.

- vSphere Authentication Proxy 설치 위치(기본 위치를 사용하지 않는 경우).
- vSphere Authentication Proxy가 연결할 vCenter Server의 주소 및 자격 증명: IP 주소 또는 이름, HTTP 포트, 사용자 이름 및 암호.
- 네트워크에서 vSphere Authentication Proxy를 식별하는 호스트 이름 또는 IP 주소.

절차

- 1 Authentication Proxy 서비스를 설치할 호스트 컴퓨터를 도메인에 추가합니다.
- 2 도메인 관리자 계정을 사용하여 호스트 컴퓨터에 로그인합니다.
- 3 소프트웨어 설치 관리자 디렉토리에서 autorun.exe 파일을 두 번 클릭하여 설치 관리자를 시작합니다.
- 4 VMware vSphere Authentication Proxy를 선택하고 **설치**를 클릭합니다.
- 5 마법사의 지시에 따라 설치 또는 업그레이드를 완료합니다.

설치하는 동안 Auto Deploy가 등록된 vCenter Server 인스턴스에 인증 서비스가 등록됩니다.

결과

vSphere Authentication Proxy 서비스를 설치할 때 설치 관리자는 Authentication Proxy 서비스를 실행할 수 있는 적절한 권한을 가진 도메인 계정을 생성합니다. 계정 이름은 접두사 CAM-으로 시작되며 계정과 연결된 임의의 생성 암호 32자를 포함합니다. 암호는 만료되지 않도록 설정됩니다. 계정 설정은 변경하지 마십시오.

인증에 vSphere Authentication Proxy를 사용하도록 호스트 구성

vSphere Authentication Proxy 서비스(CAM 서비스)를 설치한 후에는 인증 프록시 서버를 사용하여 사용자를 인증하도록 호스트를 구성해야 합니다.

사전 요구 사항

호스트에 vSphere Authentication Proxy 서비스(CAM 서비스)를 설치합니다. [vSphere Authentication Proxy 설치 또는 업그레이드를 참조하십시오.](#)

절차

- 1 호스트의 IIS 관리자를 사용하여 DHCP 범위를 설정합니다.

범위를 설정하면 관리 네트워크에서 DHCP를 사용하는 호스트가 인증 프록시 서비스를 사용할 수 있습니다.

옵션	작업
IIS 6	<ol style="list-style-type: none"> a 컴퓨터 계정 관리 웹 사이트를 찾습니다. b 가상 디렉토리 CAM ISAPI를 마우스 오른쪽 버튼으로 클릭합니다. c 속성 > 디렉토리 보안 > IP 주소 및 도메인 이름 제한 편집 > 컴퓨터 그룹 추가를 선택합니다.
IIS 7	<ol style="list-style-type: none"> a 컴퓨터 계정 관리 웹 사이트를 찾습니다. b 왼쪽 창에서 CAM ISAPI 가상 디렉토리를 클릭하고 IPv4 주소 및 도메인 제한을 엽니다. c 허용 항목 추가 > IPv4 주소 범위를 선택합니다.

- 2 호스트가 Auto Deploy를 사용하여 프로비저닝되지 않은 경우 기본 SSL 인증서를 자체 서명된 인증서 또는 상용 CA(인증 기관)에서 서명한 인증서로 변경합니다.

옵션	설명
VMCA 인증서	<p>기본 VMCA 서명된 인증서를 사용하는 경우 인증 프록시 호스트가 VMCA 인증서를 신뢰하도록 해야 합니다.</p> <ol style="list-style-type: none"> a 수동으로 VMCA 인증서를 신뢰된 루트 인증 기관 인증서 저장소에 추가합니다. b VMCA 서명된 인증서(root.cer)를 인증 프록시 서비스가 설치된 시스템의 로컬 신뢰 인증서 저장소에 추가합니다. C:\ProgramData\VMware\CIS\data\vmca에서 파일을 찾을 수 있습니다. c vSphere Authentication Proxy 서비스를 다시 시작합니다.
타사 CA 서명된 인증서	<p>CA 서명된 인증서(DER로 인코딩)를 인증 프록시 서비스가 설치되어 있는 시스템의 로컬 신뢰 인증서 저장소에 추가한 후 vSphere Authentication Proxy 서비스를 다시 시작합니다.</p> <ul style="list-style-type: none"> ■ Windows 2003을 사용하는 경우에는 인증서 파일을 C:\Documents and Settings\All Users\Application Data\VMware\vsphere Authentication Proxy\trust에 복사하고, ■ Windows 2008을 사용하는 경우에는 인증서 파일을 C:\Program Data\VMware\vsphere Authentication Proxy\trust에 복사합니다.

vSphere Authentication Proxy 설정

Authentication Proxy 인증서 정보가 있는 경우 ESXi 호스트에서는 vSphere Authentication Proxy를 사용할 수 있습니다.

서버를 한 번만 인증하면 됩니다.

참고 ESXi 및 Authentication Proxy 서버는 인증할 수 있어야 합니다. 이 인증 기능을 항상 사용 가능하도록 유지해야 합니다. 인증을 사용 중지해야 하는 경우에는 고급 설정 대화상자를 사용하여 `UserVars.ActiveDirectoryVerifyCAMCertificate` 특성을 0으로 설정하면 됩니다.

vSphere Authentication Proxy 인증서 내보내기

vSphere Authentication Proxy를 ESXi에 대해 인증하려면 ESXi에 프록시 서버 인증서를 제공해야 합니다.

사전 요구 사항

호스트에 vSphere Authentication Proxy(CAM 서비스)를 설치합니다. [vSphere Authentication Proxy 설치 또는 업그레이드](#)를 참조하십시오.

절차

- 1 인증 프록시 서버 시스템에서 IIS 관리자를 사용하여 인증서를 내보냅니다.

옵션	작업
IIS 6	<ol style="list-style-type: none"> a 컴퓨터 계정 관리 웹 사이트를 마우스 오른쪽 버튼으로 클릭합니다. b 속성 > 디렉토리 보안 > 인증서 보기를 선택합니다.
IIS 7	<ol style="list-style-type: none"> a 왼쪽 창에서 컴퓨터 계정 관리 웹 사이트를 클릭합니다. b 바인딩을 선택하여 사이트 바인딩 대화상자를 엽니다. c https 바인딩을 선택합니다. d 편집 > SSL 인증서 보기를 선택합니다.

- 2 세부 정보 > 파일에 복사를 선택합니다.

- 3 개인 키를 내보내지 않습니다. 및 Base 64로 인코딩된 X.509(.CER) 옵션을 선택합니다.

다음에 수행할 작업

인증서를 ESXi로 가져옵니다.

프록시 서버 인증서를 ESXi로 가져오기

vSphere Authentication Proxy 서버를 ESXi에 대해 인증하려면 프록시 서버 인증서를 ESXi로 업로드합니다.

vSphere Web Client 사용자 인터페이스를 사용하여 vSphere Authentication Proxy 서버 인증서를 ESXi 호스트에 업로드합니다.

사전 요구 사항

호스트에 vSphere Authentication Proxy 서비스(CAM 서비스)를 설치합니다. [vSphere Authentication Proxy 설치 또는 업그레이드](#)를 참조하십시오.

vSphere Authentication Proxy 인증서 내보내기에 설명되어 있는 대로 vSphere Authentication Proxy 서버 인증서를 내보냅니다.

절차

- 1 호스트로 이동하여 **관리** 탭을 클릭하고 **설정**을 클릭한 다음 **인증 서비스**를 클릭합니다.
- 2 **인증서 가져오기**를 클릭합니다.
- 3 호스트에 있는 인증 프록시 서버 인증서 파일의 전체 경로와 인증 프록시 서버의 IP 주소를 입력합니다.

[데이터스토어 이름] 파일 경로 형식을 사용하여 프록시 서버에 대한 경로를 입력합니다.

- 4 **확인**을 클릭합니다.

vSphere Authentication Proxy를 사용하여 도메인에 호스트 추가

호스트를 디렉토리 서비스 도메인에 가입시킬 때 사용자 제공 Active Directory 자격 증명을 전송하는 대신 vSphere Authentication Proxy 서버를 인증에 사용할 수 있습니다.

두 가지 방법 중 하나로 도메인 이름을 입력할 수 있습니다.

- **name.tld**(예: **domain.com**): 계정이 기본 컨테이너 아래에 생성됩니다.
- **name.tld/container/path**(예: **domain.com/OU1/OU2**): 계정이 특정 OU(조직 구성 단위) 아래에 생성됩니다.

사전 요구 사항

- vSphere Web Client를 사용하여 vCenter Server 시스템에 연결합니다.
- ESXi가 DHCP 주소를 사용하여 구성된 경우 DHCP 범위를 설정합니다.
- ESXi가 정적 IP 주소를 사용하여 구성된 경우에는 인증 프록시 서버가 ESXi IP 주소를 신뢰할 수 있도록 해당 프로파일이 vSphere Authentication Proxy 서비스를 사용하여 도메인에 가입하도록 구성되어 있는지 확인합니다.
- ESXi에서 VMCA 서명된 인증서를 사용하고 있는 경우 호스트가 vCenter Server에 추가되었는지 확인합니다. 이렇게 하면 인증 프록시 서버가 ESXi를 신뢰할 수 있습니다.
- ESXi에서 CA에서 서명한 인증서를 사용하고 있고 Auto Deploy를 사용하여 프로비저닝되지 않은 경우에는 인증에 vSphere Authentication Proxy를 사용하도록 호스트 구성에 설명되어 있는 대로 CA 인증서가 인증 프록시 서버의 로컬 신뢰 인증서 저장소에 추가되었는지 확인합니다.
- 호스트에 대해 vSphere Authentication Proxy 서버를 인증합니다.

절차

- 1 vSphere Web Client의 호스트로 이동하여 **관리** 탭을 클릭합니다.
- 2 **설정**을 클릭하고 **인증 서비스**를 선택합니다.
- 3 **도메인 가입**을 클릭합니다.

4 도메인을 입력합니다.

name.tld 또는 **name.tld/container/path** 형식을 사용합니다.

5 프록시 서버 사용을 선택합니다.

6 인증 프록시 서버의 IP 주소를 입력합니다.

7 확인을 클릭합니다.

ESXi 호스트의 인증 프록시 인증서 교체

vSphere Web Client에서 신뢰할 수 있는 인증 기관의 인증서를 가져올 수 있습니다.

사전 요구 사항

- 인증 프록시 인증서 파일을 ESXi 호스트에 업로드합니다.

절차

- 1 vSphere Web Client에서 ESXi 호스트를 선택합니다.
- 2 설정 탭의 시스템 영역에서 인증 서비스를 선택합니다.
- 3 인증서 가져오기를 클릭합니다.
- 4 SSL 인증서 경로 및 vSphere Authentication Proxy 서버를 입력합니다.

ESXi 보안 모범 사례

ESXi 보안 모범 사례를 따르면 vSphere 배포의 무결성을 보장할 수 있습니다. 추가 정보는 "강화 가이드"를 참조하십시오.

설치 미디어 확인

ISO, 오프라인 번들 또는 패치를 다운로드한 후에는 항상 파일의 해시를 확인하여 다운로드한 파일의 무결성과 신뢰성을 확인하십시오. VMware에서 받은 물리적 미디어의 보안 실(seal)이 파손된 경우 소프트웨어를 VMware에 반환하여 교체받으십시오.

미디어를 다운로드한 후에는 MD5 합계 값을 사용하여 다운로드의 무결성을 확인하십시오. MD5 합계 출력을 VMware 웹 사이트에 게시된 값과 비교합니다. 각 운영 체제마다 MD5 합계 값을 확인하는 방법과 도구가 다릅니다. Linux의 경우 "md5sum" 명령을 사용합니다. Microsoft Windows의 경우 추가 기능 제품을 다운로드할 수 있습니다.

수동으로 CRL 검사

기본적으로 ESXi 호스트는 CRL 검사를 지원하지 않습니다. 해지된 인증서를 수동으로 검색하여 제거해야 합니다. 이러한 인증서는 일반적으로 회사 CA 또는 타사 CA에서 생성한 사용자 지정 인증서입니다. 대부분의 회사에서는 스크립트를 사용하여 ESXi 호스트에서 해지된 SSL 인증서를 찾아서 교체합니다.

ESX Admins Active Directory 그룹 모니터링

vSphere에서 사용하는 Active Directory 그룹은 `plugins.hostsvc.esxAdminsGroup` 고급 시스템 설정을 통해 정의됩니다. 기본적으로 이 옵션은 ESX Admins로 설정되어 있습니다. ESX Admins 그룹의 모든 멤버에게는 도메인의 모든 ESXi 호스트에 대한 전체 관리 액세스 권한이 부여됩니다. Active Directory에서 이 그룹의 생성을 모니터링하고 매우 신뢰할 수 있는 사용자 및 그룹으로 멤버 자격을 제한하십시오.

구성 파일 모니터링

대부분의 ESXi 구성 설정이 API를 통해 제어되지만 제한된 수의 구성 파일은 호스트에 직접 영향을 미칩니다. 이러한 파일은 HTTPS를 사용하는 vSphere 파일 전송 API를 통해 제공됩니다. 이러한 파일을 변경하는 경우 구성 변경과 같은 해당 관리 작업도 수행해야 합니다.

참고 이 파일 전송 API를 통해 노출되지 않는 파일에 대한 모니터링은 시도하지 마십시오.

vmkfstools를 사용하여 중요 데이터 지우기

중요 데이터가 포함된 VMDK 파일을 삭제할 때는 가상 시스템을 종료하거나 중지한 다음 해당 파일에 대해 vCLI 명령 `vmkfstools --writezeros`를 실행합니다. 그런 다음 데이터스토어에서 파일을 삭제할 수 있습니다.

PCI와 PCIe 디바이스 및 ESXi

VMware DirectPath I/O 기능을 사용하여 PCI 또는 PCIe 디바이스를 가상 시스템에 전달하면 잠재적인 보안 취약성이 발생합니다. 게스트 OS에서 사용 권한이 있는 모드로 실행되는 디바이스 드라이버 등, 버그성 코드나 악성 코드에 의해 취약성이 트리거될 수 있습니다. 현재는 업계 표준 하드웨어 및 펌웨어에서 ESXi가 완전히 취약성을 막게 할 수 있는 충분한 오류 억제 지원이 되지 않고 있습니다.

신뢰할 수 있는 엔티티가 가상 시스템을 소유하고 관리하는 경우에만 가상 시스템에 대한 PCI 또는 PCIe 패스스루를 사용하는 것이 좋습니다. 이 엔티티가 가상 시스템에서 호스트를 충돌시키거나 악용하려고 시도하지 않는지 확인해야 합니다.

사용 중인 호스트가 다음 방법 중 하나로 손상될 수 있습니다.

- 게스트 OS가 복구할 수 없는 PCI 또는 PCIe 오류를 생성할 수 있습니다. 이러한 오류는 데이터를 손상시키지는 않지만 ESXi 호스트가 충돌되게 할 수 있습니다. 전달되고 있는 하드웨어 디바이스의 버그 또는 비호환성으로 인해서나 게스트 OS의 드라이버 관련 문제로 인해 이러한 오류가 발생할 수 있습니다.
- 예를 들어 DMA 작업이 가상 시스템의 메모리 외부 주소를 대상으로 하는 경우 게스트 OS가 ESXi 호스트에서 IOMMU 페이지 장애를 일으키는 DMA(Direct Memory Access) 작업을 생성할 수 있습니다. 일부 시스템에서 호스트 펌웨어는 NMI(Non-Maskable Interrupt)를 통해 치명적인 오류를 보고하도록 IOMMU 장애를 구성하고, 이로 인해 ESXi 호스트가 충돌하게 됩니다. 게스트 OS의 드라이버 관련 문제로 인해 이 문제가 발생할 수 있습니다.

- ESXi 호스트의 운영 체제가 인터럽트 재매핑을 사용하고 있지 않은 경우 게스트 OS가 벡터의 ESXi 호스트에 가상 인터럽트를 주입할 수 있습니다. 현재 ESXi는 인터럽트 재매핑이 사용 가능한 Intel 플랫폼에서 인터럽트 재매핑을 사용합니다. 인터럽트 매핑은 Intel VT-d 기능 세트의 일부입니다. ESXi는 AMD 플랫폼에서 인터럽트 매핑을 사용하지 않습니다. 가상 인터럽트는 ESXi 호스트의 충돌을 일으킬 가능성이 높지만 이론적으로는 이러한 인터럽트를 악용하는 다른 방법이 존재할 수 있습니다.

ESXi에 대한 스마트 카드 인증 구성

사용자 이름 및 암호에 대한 기본 프롬프트 대신 PIV(Personal Identity Verification), CAC(Common Access Card) 또는 SC650 스마트 카드를 통해 스마트 카드 인증을 사용하여 ESXi DCUI(Direct Console User Interface)에 로그인할 수 있습니다.

스마트 카드는 집적 회로 칩이 내장된 소형 플라스틱 카드입니다. 수많은 정부 기관과 대기업에서는 스마트 카드 기반의 이중 인증을 사용하여 시스템의 보안을 강화하고 보안 규정을 준수합니다.

스마트 카드 인증이 ESXi 호스트에서 사용하도록 설정된 경우 DCUI는 사용자 이름 및 암호에 대한 기본 프롬프트 대신 올바른 스마트 카드 및 PIN 조합을 확인하는 메시지를 표시합니다.

- 1 스마트 카드를 스마트 카드 판독기에 삽입하면 ESXi 호스트가 해당 스마트 카드의 자격 증명을 읽습니다.
- 2 ESXi DCUI는 로그인 ID를 표시하고 PIN을 묻는 메시지를 표시합니다.
- 3 PIN을 입력하면 ESXi 호스트가 스마트 카드에 저장된 PIN과 대조한 후 Active Directory를 통해 스마트 카드의 인증서를 확인합니다.
- 4 스마트 카드 인증서를 성공적으로 확인하면 ESXi가 사용자를 DCUI에 로그인시킵니다.

F3을 눌러 DCUI에서 사용자 이름 및 암호 인증으로 전환할 수 있습니다.

스마트 카드의 칩은 PIN 항목을 연속해서 잘못 입력하면 잠깁니다(일반적으로 세 번임). 스마트 카드가 잠기면 선택된 담당자만 잠금 해제할 수 있습니다.

스마트 카드 인증 사용

ESXi DCUI에 로그인하려면 스마트 카드 및 PIN 조합을 요구하도록 스마트 카드 인증을 사용합니다.

사전 요구 사항

- Active Directory 도메인의 계정, 스마트 카드 판독기 및 스마트 카드와 같이 스마트 카드 인증을 처리하는 인프라를 설정합니다.
- 스마트 카드 인증을 지원하는 Active Directory 도메인에 가입하도록 ESXi를 구성합니다. 자세한 내용은 [Active Directory를 통해 ESXi 사용자 관리](#)를 참조하십시오.
- vSphere Web Client를 사용하여 루트 인증서를 추가합니다. [ESXi 호스트에 대한 인증서 관리](#)를 참조하십시오.

절차

- 1 vSphere Web Client에서 호스트를 찾습니다.

- 2 **관리** 탭을 클릭하고 **설정**을 클릭합니다.
- 3 시스템 아래에서 **인증 서비스**를 선택합니다.
현재 스마트 카드 인증 상태와 가져온 인증서가 포함된 목록이 표시됩니다.
- 4 스마트 카드 인증 패널에서 **편집**을 클릭합니다.
- 5 [스마트 카드 인증 편집] 대화상자에서 [인증서] 페이지를 선택합니다.
- 6 신뢰할 수 있는 CA(인증 기관) 인증서(예: 루트 및 중간 CA 인증서)를 추가합니다.
- 7 [스마트 카드 인증] 페이지를 열고 **스마트 카드 인증 사용** 확인란을 선택한 다음 **확인**을 클릭합니다.

스마트 카드 인증 사용 안 함

스마트 카드 인증을 사용하지 않도록 설정하여 ESXi DCUI 로그인에 대한 기본 사용자 이름 및 암호 인증으로 돌아갑니다.

절차

- 1 vSphere Web Client에서 호스트를 찾습니다.
- 2 **관리** 탭을 클릭하고 **설정**을 클릭합니다.
- 3 시스템 아래에서 **인증 서비스**를 선택합니다.
현재 스마트 카드 인증 상태와 가져온 인증서가 포함된 목록이 표시됩니다.
- 4 스마트 카드 인증 패널에서 **편집**을 클릭합니다.
- 5 [스마트 카드 인증] 페이지에서 **스마트 카드 인증 사용** 확인란의 선택을 취소하고 **확인**을 클릭합니다.

연결 문제의 경우 사용자 자격 증명 인증

AD(Active Directory) 도메인 서버에 연결할 수 없는 경우 사용자 이름 및 암호 인증을 사용하여 ESXi DCUI에 로그인하면 호스트에서 긴급 작업을 수행할 수 있습니다.

예외적인 환경에서 연결 문제, 네트워크 운영 중단 또는 재해로 인해 스마트 카드에서 사용자 자격 증명을 인증하기 위해 AD 도메인 서버에 연결할 수 없습니다. AD 서버에 대한 연결이 끊어진 경우 로컬 ESXi 사용자의 자격 증명을 사용하여 ESXi DCUI에 로그인할 수 있습니다. 그러면 진단 또는 다른 긴급 작업을 수행할 수 있습니다. 사용자 이름 및 암호 로그인에 대한 폴백이 기록됩니다. AD에 대한 연결이 복원되는 경우 스마트 카드 인증을 다시 사용하도록 설정할 수 있습니다.

참고 AD(Active Directory) 도메인 서버를 사용할 수 있으면 vCenter Server에 대한 네트워크 연결이 끊어져도 스마트 카드 인증에는 영향을 주지 않습니다.

잠금 모드에서 스마트 카드 인증 사용

사용하도록 설정된 경우 ESXi 호스트의 잠금 모드는 호스트의 보안을 강화하고 DCUI에 대한 액세스를 제한합니다. 잠금 모드는 스마트 카드 인증 기능을 사용하지 않도록 설정할 수 있습니다.

정상 잠금 모드에서는 관리자 권한이 있는 예외 사용자 목록의 사용자만 DCUI에 액세스할 수 있습니다. 예외 사용자는 ESXi 호스트에 대해 로컬로 정의된 사용 권한이 있는 Active Directory 사용자 또는 호스트 로컬 사용자입니다. 정상 잠금 모드에서 스마트 카드 인증을 사용하려는 경우 vSphere Web Client에서 사용자를 예외 사용자 목록에 추가해야 합니다. 이러한 사용자는 호스트가 정상 잠금 모드로 전환될 때 사용 권한을 손실하지 않으며 DCUI에 로그인할 수 있습니다. 자세한 내용은 [잠금 모드 예외 사용자 지정](#)을 참조하십시오.

엄격 잠금 모드에서는 DCUI 서비스가 중지됩니다. 따라서 스마트 카드 인증을 사용하여 호스트에 액세스할 수 없습니다.

ESXi SSH 키

SSH 키를 사용하여 ESXi 호스트에 대한 액세스를 제한, 제어 및 보호할 수 있습니다. SSH 키를 사용하면 신뢰할 수 있는 사용자 또는 스크립트가 암호를 지정하지 않고 호스트에 로그인하도록 허용할 수 있습니다.

`vifs` vSphere CLI 명령을 사용하여 SSH 키를 호스트에 복사할 수 있습니다. vSphere CLI 명령 집합을 설치 및 사용하는 방법에 대한 자세한 내용은 ["vSphere 명령줄 인터페이스 시작"](#)을 참조하십시오. 또한 HTTPS PUT를 사용하여 호스트에 SSH 키를 복사할 수도 있습니다.

외부에서 키를 생성하여 업로드하는 대신 ESXi 호스트에서 키를 생성하고 다운로드할 수 있습니다. VMware 기술 자료 문서 [1002866](#)를 참조하십시오.

SSH를 사용하도록 설정하며 호스트에 SSH 키를 추가할 경우 위험이 수반되므로 확장된 환경에서는 권장되지 않습니다. [인증\(SSH\) 키 사용 안 함](#) 항목을 참조하십시오.

참고 ESXi 5.0 이전 버전의 경우 SSH 키가 있는 사용자는 호스트가 잠금 모드인 경우에도 호스트에 액세스할 수 있습니다. 이는 ESXi 5.1에서 수정되었습니다.

SSH 보안

SSH를 사용하여 ESXi Shell에 원격으로 로그인하고 호스트에 대한 문제 해결 작업을 수행할 수 있습니다. ESXi에서는 SSH 구성이 향상되어 보다 높은 수준의 보안이 제공됩니다.

버전 1 SSH 프로토콜 사용 안 함

VMware에서는 버전 1 SSH 프로토콜을 지원하지 않으며 버전 2 프로토콜만 사용합니다. 버전 2는 버전 1에서 발생하던 몇 가지 보안 문제를 해결하고 관리 인터페이스와 통신하는 안전한 방법을 제공합니다.

향상된 암호화 수준

SSH는 연결에 256비트 및 128비트 AES 암호화만 지원합니다.

이러한 설정은 SSH를 통해 관리 인터페이스로 전송하는 데이터를 강력하게 보호하기 위한 것입니다. 이러한 설정은 변경할 수 없습니다.

vifs 명령을 사용하여 SSH Key 업로드

SSH를 통해 인증된 키를 사용하여 호스트에 로그인하려는 경우 vifs 명령을 사용하여 인증된 키를 업로드해야 합니다.

참고 인증된 키를 사용하면 사용자 인증이 필요 없이 SSH 액세스가 가능하므로 환경에서 SSH 키를 사용할지 여부를 신중하게 고려해야 합니다.

인증 키를 통해 호스트에 대한 원격 액세스를 인증할 수 있습니다. 사용자 또는 스크립트가 SSH를 사용하여 호스트에 액세스하려고 할 때 키가 암호 없이 인증을 제공합니다. 인증 키를 사용하면 인증을 자동화할 수 있으므로 정기적인 작업을 수행할 스크립트를 작성할 때 유용합니다.

다음 유형의 SSH 키를 호스트에 업로드할 수 있습니다.

- 루트 사용자에게 대한 인증 키 파일
- RSA 키
- RSA 공용 키

vSphere 6.0 업데이트 2 릴리스부터 DSS/DSA 키가 더 이상 지원되지 않습니다.

중요 /etc/ssh/sshd_config 파일을 수정하지 마십시오.

절차

- ◆ 명령줄 또는 관리 서버에서 vifs 명령을 사용하여 SSH 키를 ESXi 호스트의 적절한 위치로 업로드합니다.

```
vifs --server hostname --username username --put filename /host/ssh_host_dsa_key_pub
```

키의 유형	위치
루트 사용자에게 대한 인증된 키 파일	/host/ssh_root_authorized_keys 이 파일을 업로드하려면 전체 관리자 권한이 있어야 합니다.
RSA 키	/host/ssh_host_rsa_key
RSA 공용 키	/host/ssh_host_rsa_key_pub

HTTPS PUT를 사용하여 SSH 키 업로드

SSH를 사용하여 인증 키로 호스트에 로그인할 수 있습니다. HTTPS PUT를 사용하여 인증된 키를 업로드할 수 있습니다.

인증 키를 통해 호스트에 대한 원격 액세스를 인증할 수 있습니다. 사용자 또는 스크립트가 SSH를 사용하여 호스트에 액세스하려고 할 때 키가 암호 없이 인증을 제공합니다. 인증 키를 사용하면 인증을 자동화할 수 있으므로 정기적인 작업을 수행할 스크립트를 작성할 때 유용합니다.

HTTPS PUT를 사용하여 다음 유형의 SSH 키를 호스트로 업로드할 수 있습니다.

- 루트 사용자에게 대한 인증 키 파일

- DSA 키
- DSA 공용 키
- RSA 키
- RSA 공용 키

중요 /etc/ssh/sshd_config 파일을 수정하지 마십시오.

절차

- 1 업로드 애플리케이션에서 키 파일을 업로드.
- 2 파일을 다음 위치에 게시합니다.

키의 유형	위치
루트 사용자에게 대한 인증된 키 파일	<code>https://hostname_or_IP_address/host/ssh_root_authorized_keys</code> 이 파일을 업로드하려면 호스트에 대한 전체 관리자 권한이 있어야 합니다.
DSA 키	<code>https://hostname_or_IP_address/host/ssh_host_dsa_key</code>
DSA 공용 키	<code>https://hostname_or_IP_address/host/ssh_host_dsa_key_pub</code>
RSA 키	<code>https://hostname_or_IP_address/host/ssh_host_rsa_key</code>
RSA 공용 키	<code>https://hostname_or_IP_address/host/ssh_host_rsa_key_pub</code>

ESXi Shell 사용

ESXi Shell은 기본적으로 ESXi 호스트에서 사용되지 않도록 설정됩니다. 필요한 경우 이 셸에 로컬 및 원격으로 액세스할 수 있도록 설정할 수 있습니다.

무단 액세스 위험을 줄이기 위해 문제 해결용으로만 ESXi Shell을 사용하도록 설정하십시오.

ESXi Shell은 잠금 모드에 영향을 받지 않습니다. 호스트가 잠금 모드에서 실행되더라도 사용하도록 설정되어 있으면 ESXi Shell에 로그인할 수 있습니다.

ESXi Shell

ESXi Shell에 로컬로 액세스하려면 이 서비스를 사용하도록 설정합니다.

SSH

SSH를 사용하여 ESXi Shell에 원격으로 액세스하려면 이 서비스를 사용하도록 설정합니다.

"vSphere 보안"의 내용을 참조하십시오.

루트 사용자와 관리자 역할이 할당된 사용자가 ESXi Shell에 액세스할 수 있습니다. Active Directory의 ESX Admins 그룹에 속한 사용자에게는 관리자 역할이 자동으로 할당됩니다. 기본적으로 루트 사용자만 ESXi Shell을 사용하여 시스템 명령(예: `vmware -v`)을 실행할 수 있습니다.

참고 실제로 액세스가 필요한 경우가 아니면 ESXi Shell을 사용하도록 설정하지 마십시오.

- **vSphere Web Client를 사용하여 ESXi Shell에 액세스할 수 있도록 설정**
vSphere Web Client를 사용하여 ESXi Shell에 대한 로컬 및 원격(SSH) 액세스를 사용하도록 설정하고 유효 시간 초과 및 가용성 시간 초과를 설정할 수 있습니다.
- **DCUI(Direct Console User Interface)를 사용하여 ESXi Shell에 액세스할 수 있도록 설정**
DCUI(Direct Console User Interface)에서 텍스트 기반 메뉴를 사용하여 로컬로 호스트와 상호 작용할 수 있습니다. 사용자 환경의 보안 요구 사항이 Direct Console User Interface의 사용을 지원하는지 신중하게 평가합니다.
- **문제 해결을 위해 ESXi Shell에 로그인**
vSphere Web Client, vSphere CLI 또는 vSphere PowerCLI를 사용하여 ESXi 구성 작업을 수행합니다. 문제 해결을 위해서만 ESXi Shell(이전의 Tech Support Mode 또는 TSM)에 로그인합니다.

vSphere Web Client를 사용하여 ESXi Shell에 액세스할 수 있도록 설정

vSphere Web Client를 사용하여 ESXi Shell에 대한 로컬 및 원격(SSH) 액세스를 사용하도록 설정하고 유효 시간 초과 및 가용성 시간 초과를 설정할 수 있습니다.

참고 vSphere Web Client, 원격 명령줄 도구(vCLI 및 PowerCLI) 및 게시된 API를 사용하여 호스트에 액세스합니다. 특별한 상황에서 SSH 액세스를 사용하도록 설정해야 하는 경우가 아니면 SSH를 사용하여 호스트에 원격으로 액세스하도록 설정하지 마십시오.

사전 요구 사항

인증된 SSH 키를 사용하려면 해당 SSH 키를 업로드할 수 있습니다. [ESXi SSH 키](#) 항목을 참조하십시오.

절차

- 1 vSphere Web Client 인벤토리에서 호스트를 찾습니다.
- 2 **관리** 탭을 클릭하고 **설정**을 클릭합니다.
- 3 시스템 아래에서 **보안 프로파일**을 선택합니다.
- 4 서비스 패널에서 **편집**을 클릭합니다.
- 5 목록에서 서비스를 선택합니다.
 - ESXi Shell
 - SSH
 - 직접 콘솔 UI

6 **서비스 세부 정보**를 클릭하고 시작 정책으로 **수동으로 시작 및 중지**를 선택합니다.

수동으로 시작 및 중지를 선택하면 호스트를 재부팅할 때 서비스가 시작되지 않습니다. 호스트를 재부팅할 때 서비스가 시작되도록 하려면 **호스트와 함께 시작 및 중지**를 선택합니다.

7 **시작**을 선택하여 서비스를 설정합니다.

8 **확인**을 클릭합니다.

다음에 수행할 작업

ESXi Shell에 대한 가용성 및 유휴 시간 초과를 설정합니다. 자세한 내용은 [vSphere Web Client에서 ESXi Shell 가용성에 대한 시간 초과 설정 생성](#) 및 [vSphere Web Client에서 유휴 ESXi Shell 세션에 대한 시간 초과 설정 생성](#) 항목을 참조하십시오.

vSphere Web Client에서 ESXi Shell 가용성에 대한 시간 초과 설정 생성

ESXi Shell은 기본적으로 사용하지 않도록 설정되어 있습니다. 셸을 사용하도록 설정할 경우 ESXi Shell의 가용성 시간 초과를 설정하여 보안을 강화할 수 있습니다.

가용성 시간 초과 설정은 ESXi Shell이 설정된 후 로그인할 때까지의 최대 대기 시간입니다. 시간 초과 기간이 끝나면 서비스가 사용되지 않도록 설정되고 사용자는 로그인할 수 없습니다.

절차

- 1 vSphere Web Client 인벤토리에서 호스트를 찾습니다.
- 2 **관리** 탭을 클릭하고 **설정**을 클릭합니다.
- 3 시스템 아래에서 **고급 시스템 설정**을 선택합니다.
- 4 UserVars.ESXiShellTimeOut을 선택하고 **편집** 아이콘을 클릭합니다.
- 5 유휴 시간 초과 설정을 입력합니다.

시간 초과를 적용하려면 SSH 서비스 및 ESXi Shell 서비스를 다시 시작해야 합니다.

6 **확인**을 클릭합니다.

결과

시간 초과 기간이 경과된 시점에 로그인되어 있으면 세션이 지속됩니다. 하지만 사용자가 로그아웃했거나 세션이 종료되면 사용자는 로그인할 수 없습니다.

vSphere Web Client에서 유휴 ESXi Shell 세션에 대한 시간 초과 설정 생성

사용자가 호스트에서 ESXi Shell을 사용하도록 설정하며 세션에서 로그아웃하는 것을 잊을 경우 유휴 세션이 무기한 연결 상태로 유지됩니다. 이 경우 열려 있는 연결에서 호스트에 대한 액세스 권한을 얻는 사용자가 늘어날 수 있습니다. 유휴 세션에 대한 시간 초과를 설정하여 이 문제를 방지할 수 있습니다.

유휴 시간 초과란 사용자가 유휴 대화형 세션에서 로그아웃할 때까지의 최대 대기 시간입니다.

DCUI(Direct Console Interface) 또는 vSphere Web Client에서 로컬 및 원격(SSH) 세션 모두에 대한 시간을 제어할 수 있습니다.

절차

- 1 vSphere Web Client 인벤토리에서 호스트를 찾습니다.
- 2 **관리** 탭을 클릭하고 **설정**을 클릭합니다.
- 3 시스템 아래에서 **고급 시스템 설정**을 선택합니다.
- 4 UserVars.ESXiShellInteractiveTimeOut을 선택하고 **편집** 아이콘을 클릭한 다음 시간 초과 설정을 입력합니다.
- 5 시간 초과를 적용하려면 ESXi Shell 서비스 및 SSH 서비스를 다시 시작합니다.

결과

세션이 유효 상태일 때 시간 초과 기간이 경과하면 사용자가 로그아웃됩니다.

DCUI(Direct Console User Interface)를 사용하여 ESXi Shell에 액세스할 수 있도록 설정

DCUI(Direct Console User Interface)에서 텍스트 기반 메뉴를 사용하여 로컬로 호스트와 상호 작용할 수 있습니다. 사용자 환경의 보안 요구 사항이 Direct Console User Interface의 사용을 지원하는지 신중하게 평가합니다.

Direct Console User Interface를 사용하여 ESXi Shell에 대한 로컬 및 원격 액세스가 가능하도록 설정할 수 있습니다.

참고 Direct Console User Interface, vSphere Web Client, ESXCLI 또는 다른 관리자 도구를 사용하여 호스트에 변경한 내용은 매시간 또는 정상 종료 시 영구 스토리지에 커밋됩니다. 변경 내용이 커밋되기 전에 호스트에서 오류가 발생하면 변경 내용이 손실될 수 있습니다.

절차

- 1 Direct Console User Interface에서 F2 키를 눌러 시스템 사용자 지정 메뉴에 액세스합니다.
- 2 **문제 해결 옵션**을 선택하고 Enter를 누릅니다.
- 3 문제 해결 모드 옵션 메뉴에서 사용하도록 설정할 서비스를 선택합니다.
 - ESXi Shell 사용
 - SSH 사용
- 4 Enter 키를 눌러 서비스를 사용하도록 설정합니다.
- 5 Direct Console User Interface의 기본 메뉴로 돌아갈 때까지 Esc 키를 누릅니다.

다음에 수행할 작업

ESXi Shell에 대한 가용성 및 유효 시간 초과를 설정합니다. [Direct Console User Interface에서 ESXi Shell 가용성에 대한 시간 초과 설정 생성](#) 및 [유효 ESXi Shell 세션에 대한 시간 제한 설정 생성](#)을 참조하십시오.

Direct Console User Interface에서 ESXi Shell 가용성에 대한 시간 초과 설정 생성

ESXi Shell은 기본적으로 사용하지 않도록 설정되어 있습니다. 셸을 사용하도록 설정할 경우 ESXi Shell에 대한 가용성 시간 초과를 설정하여 보안을 강화할 수 있습니다.

가용성 시간 초과 설정은 ESXi Shell이 설정된 후 로그인할 때까지의 최대 대기 시간입니다. 시간 초과 기간이 끝나면 서비스가 사용되지 않도록 설정되고 사용자는 로그인할 수 없습니다.

절차

- 1 문제 해결 모드 옵션 메뉴에서 **ESXi Shell 및 SSH 시간 초과 수정**을 선택하고 Enter 키를 누릅니다.
- 2 가용성 시간 초과를 입력합니다.
시간 초과를 적용하려면 SSH 서비스 및 ESXi Shell 서비스를 다시 시작해야 합니다.
- 3 Enter 키를 누르고 Direct Console User Interface의 기본 메뉴로 돌아갈 때까지 Esc 키를 누릅니다.
- 4 **확인**을 클릭합니다.

결과

시간 초과 기간이 경과될 때 로그인되어 있으면 세션이 지속됩니다. 하지만 사용자가 로그아웃했거나 세션이 종료되면 사용자는 로그인할 수 없습니다.

유휴 ESXi Shell 세션에 대한 시간 제한 설정 생성

사용자가 호스트에서 ESXi Shell을 사용하도록 설정하며 세션에서 로그아웃하는 것을 잊을 경우 유휴 세션이 무기한 연결 상태로 유지됩니다. 이 경우 열려 있는 연결에서 호스트에 대한 액세스 권한을 얻는 사용자가 늘어날 수 있습니다. 유휴 세션에 대한 시간 제한을 설정하여 이 문제를 방지할 수 있습니다.

유휴 시간 초과는 사용자가 유휴 대화형 세션에서 로그아웃할 때까지의 최대 대기 시간입니다. 유휴 시간 초과에 대한 변경 내용은 사용자가 다음에 ESXi Shell에 로그인할 때 적용되며 기존 세션에는 영향을 미치지 않습니다.

Direct Console User Interface에서 시간 제한을 초 단위로 지정하거나 vSphere Web Client에서 분 단위로 지정할 수 있습니다.

절차

- 1 문제 해결 모드 옵션 메뉴에서 **ESXi Shell 및 SSH 시간 초과 수정**을 선택하고 Enter 키를 누릅니다.
- 2 유휴 시간 제한을 초 단위로 입력합니다.
시간 제한을 적용하려면 SSH 서비스 및 ESXi Shell 서비스를 다시 시작해야 합니다.
- 3 Enter 키를 누르고 Direct Console User Interface의 기본 메뉴로 돌아갈 때까지 Esc 키를 누릅니다.

결과

세션이 유휴 상태일 때 시간 제한 기간이 경과하면 사용자가 로그아웃됩니다.

문제 해결을 위해 ESXi Shell에 로그인

vSphere Web Client, vSphere CLI 또는 vSphere PowerCLI를 사용하여 ESXi 구성 작업을 수행합니다. 문제 해결을 위해서만 ESXi Shell(이전의 Tech Support Mode 또는 TSM)에 로그인합니다.

절차

- 1 다음 방법 중 하나를 사용하여 ESXi Shell에 로그인합니다.
 - 호스트에 직접 액세스할 수 있으면 시스템의 물리적 콘솔에서 **Alt+F1**을 눌러 로그인 페이지를 엽니다.
 - 호스트에 원격으로 연결하려면 SSH 또는 다른 원격 콘솔 연결을 사용하여 호스트의 세션을 시작합니다.
- 2 호스트에서 인식하는 사용자 이름 및 암호를 입력합니다.

ESXi 웹 프록시 설정 수정

웹 프록시 설정을 수정할 때 고려해야 할 몇 가지 암호화 및 사용자 보안 지침이 있습니다.

참고 호스트 디렉토리 또는 인증 메커니즘을 변경한 후에는 호스트 프로세스를 다시 시작합니다.

- 암호 또는 암호 문구를 사용하는 인증서를 설정하지 마십시오. ESXi는 암호화된 키라고도 하는 암호 또는 암호 문구를 사용하는 웹 프록시를 지원하지 않습니다. 암호 또는 암호 문구가 필요한 웹 프록시를 설정하면 ESXi 프로세스가 올바르게 시작되지 않습니다.
- 사용자 이름, 암호 및 패킷에 대한 암호화를 지원하려면 vSphere Web Services SDK 연결에 대해 SSL을 기본적으로 사용하도록 설정해야 합니다. 이러한 연결이 전송을 암호화하지 않도록 구성하려면 HTTPS의 연결을 HTTP로 전환하여 vSphere Web Services SDK 연결에 대해 SSL을 사용하지 않도록 설정합니다.

이들 클라이언트에 대해 방화벽이 제대로 작동하고 호스트와의 전송이 완전히 분리되는 완전히 신뢰할 수 있는 환경을 만든 경우에만 SSL을 사용하지 않도록 설정해야 합니다. SSL을 사용하지 않도록 설정하면 암호화를 수행하는 데 필요한 오버헤드가 방지되므로 성능이 향상됩니다.

- ESXi 서비스가 잘못 사용되지 않도록 대부분의 내부 ESXi 서비스는 HTTPS 전송에서 사용되는 포트 443을 통해서만 액세스할 수 있습니다. 포트 443은 ESXi에 대해 역방향 프록시로 작동합니다. ESXi의 서비스 목록은 HTTP 시작 페이지를 통해 볼 수 있지만 적절한 권한 부여 없이는 스토리지 어댑터 서비스에 직접 액세스할 수 없습니다.

개별 서비스가 HTTP 연결을 통해 직접 액세스 가능하도록 이 구성을 변경할 수 있습니다. 완전히 신뢰할 수 있는 환경에서 ESXi를 사용하는 것이 아니라면 이러한 변경을 수행하지 마십시오.

- 환경을 업그레이드할 때 인증서는 그대로 유지됩니다.

vSphere Auto Deploy 보안 고려 사항

환경을 가장 효과적으로 보호하기 위해서는 호스트 프로파일과 함께 Auto Deploy를 사용할 때 발생할 수 있는 보안 위험을 알고 있어야 합니다.

네트워킹 보안

다른 PXE 기반 배포 방법을 보호하는 것과 마찬가지로 네트워크를 보호합니다. vSphere Auto Deploy는 SSL을 통해 데이터를 전송함으로써 일반적인 간섭 및 스누핑을 방지합니다. 그러나 PXE 부팅 동안에는 클라이언트나 Auto Deploy 서버에 대한 신뢰성이 확인되지 않습니다.

Auto Deploy가 사용되는 네트워크를 완전히 분리하면 Auto Deploy의 보안 위험을 대폭 줄일 수 있습니다.

부팅 이미지 및 호스트 프로파일 보안

vSphere Auto Deploy 서버에서 시스템에 다운로드하는 부팅 이미지는 다음과 같은 구성 요소가 포함될 수 있습니다.

- 이미지 프로파일을 구성하는 VIB 패키지는 항상 부팅 이미지에 포함됩니다.
 - 호스트 프로파일 또는 호스트 사용자 지정 설정을 사용하여 호스트를 프로비저닝하도록 Auto Deploy 규칙이 설정된 경우 호스트 프로파일 및 호스트 사용자 지정이 부팅 이미지에 포함됩니다.
 - 호스트 프로파일 및 호스트 사용자 지정과 함께 포함되는 관리자(루트) 암호와 사용자 암호는 MD5로 암호화됩니다.
 - 프로파일과 연결된 다른 암호는 암호화되지 않습니다. 호스트 프로파일을 사용하여 Active Directory를 설정하는 경우에는 암호가 보호되지 않습니다.
- Active Directory를 설정하는 데 vSphere Authentication Service를 사용하면 Active Directory 암호가 노출되는 것을 방지할 수 있습니다. 호스트 프로파일을 사용하여 Active Directory를 설정하면 암호가 보호되지 않습니다.
- 호스트의 공용 및 개인 SSL 키와 인증서가 부팅 이미지에 포함됩니다.

ESXi 로그 파일 관리

로그 파일은 공격 문제를 해결하고 호스트 보안의 침해에 대한 정보를 얻기 위한 중요한 구성 요소입니다. 안전한 중앙 집중식 로그 서버에 로그인하면 로그 변조를 방지할 수 있습니다. 원격 로깅 역시 장기적인 감사 기록을 제공합니다.

호스트의 보안을 강화하기 위해 다음 대책을 수행하십시오.

- 데이터스토어에 대한 영구적 로깅을 구성합니다. 기본적으로 ESXi 호스트의 로그는 메모리 내 파일 시스템에 저장됩니다. 따라서 호스트를 재부팅하면 로그가 손실되며 24시간의 로그 데이터만 저장됩니다. 영구적 로깅을 사용하도록 설정하면 호스트에 사용 가능한 전용 서버 활동 기록이 생성됩니다.

- 중앙 호스트로 원격 로깅하면 로그 파일을 중앙 호스트로 모을 수 있고 하나의 도구로 모든 호스트를 모니터링할 수 있습니다. 또한 집계 분석 및 로그 데이터의 검색도 가능하므로 여러 호스트에 대한 조정한 공격과 같은 상황에 대한 정보도 포착할 수 있습니다.
- vCLI 또는 PowerCLI와 같은 원격 명령줄 또는 API 클라이언트를 사용하여 ESXi 호스트에서 원격 보안 syslog를 구성하십시오.
- 그리고 syslog 구성을 쿼리하여 올바른 포트를 비롯한 적절한 syslog 서버가 구성되었는지 확인하십시오.

ESXi 호스트의 Syslog 구성

모든 ESXi 호스트는 VMkernel 및 다른 시스템 구성 요소에서 보낸 로그 메시지를 로그 파일에 기록하는 syslog 서비스(vmsyslogd)를 실행합니다.

vSphere Web Client나 `esxcli system syslog vCLI` 명령을 사용하여 syslog 서비스를 구성할 수 있습니다.

vCLI 명령에 대한 자세한 내용은 "vSphere Command-Line Interface 시작" 을 참조하십시오.

절차

- 1 vSphere Web Client 인벤토리에서 호스트를 선택합니다.
- 2 **관리** 탭을 클릭합니다.
- 3 시스템 패널에서 **고급 시스템 설정**을 클릭합니다.
- 4 고급 시스템 설정 목록의 **Syslog** 섹션을 찾습니다.
- 5 로깅을 전체적으로 설정하려면 변경할 설정을 선택하고 편집 아이콘을 클릭합니다.

옵션	설명
Syslog.global.defaultRotate	유지할 최대 아카이브 수를 설정합니다. 이 숫자는 전체적으로 설정할 수 있으며 개별 하위 로거에 대해 설정할 수도 있습니다.
Syslog.global.defaultSize	시스템에서 로그를 회전할 때까지의 기본 로그 크기(KB)를 설정합니다. 이 숫자는 전체적으로 설정할 수 있으며 개별 하위 로거에 대해 설정할 수도 있습니다.
Syslog.global.LogDir	로그가 저장된 디렉토리입니다. 디렉토리는 마운트된 NFS 또는 VMFS 볼륨에 위치할 수 있습니다. 로컬 파일 시스템의 /scratch 디렉토리만 여러 번 재부팅해도 영구적으로 유지됩니다. 디렉토리는 <code>[datastorename] path_to_file</code> 형식으로 지정해야 하며, 경로는 데이터스토어 백업 볼륨의 루트에 상대적입니다. 예를 들어 경로 <code>[storage1] /systemlogs</code> 는 경로 <code>/vmfs/volumes/storage1/systemlogs</code> 에 매핑됩니다.

옵션	설명
Syslog.global.logDirUnique	이 옵션을 선택하면 Syslog.global.LogDir 에서 지정한 디렉토리 아래에 ESXi 호스트의 이름을 가진 하위 디렉토리가 생성됩니다. 여러 ESXi 호스트에서 동일한 NFS 디렉토리를 사용하는 경우에는 고유한 디렉토리를 사용하는 것이 유용합니다.
Syslog.global.LogHost	syslog 메시지가 전달되는 원격 호스트 및 원격 호스트가 syslog 메시지를 수신하는 포트입니다. ssl://hostName:1514처럼 프로토콜과 포트를 포함할 수 있습니다. UDP(기본값), TCP 및 SSL이 지원됩니다. 전달된 syslog 메시지를 수신하려면 원격 호스트에 syslog가 설치되고 올바르게 구성되어 있어야 합니다. 자세한 구성 정보는 원격 호스트에 설치되어 있는 syslog 서비스에 대한 설명서를 참조하십시오.

6 (선택 사항) 로그의 기본 로그 크기와 로그 회전을 덮어쓰려면 다음을 수행합니다.

- 사용자 지정할 로그의 이름을 클릭합니다.
- 편집 아이콘을 클릭하고 원하는 회전 수와 로그 크기를 입력합니다.

7 **확인**을 클릭합니다.

결과

syslog 옵션에 대한 변경 내용이 즉시 적용됩니다.

ESXi 로그 파일 위치

ESXi에서는 syslog 기능을 사용하여 호스트 작업을 로그 파일에 기록합니다.

구성 요소	위치	용도
VMkernel	/var/log/vmkernel.log	가상 시스템 및 ESXi와 관련된 작업을 기록합니다.
VMkernel 주의	/var/log/vmkwarning.log	가상 시스템과 관련된 작업을 기록합니다.
VMkernel 요약	/var/log/vmksummary.log	ESXi의 가동 시간 및 가용성 통계를 확인하는 데 사용됩니다(섬표로 구분).
ESXi 호스트 에이전트 로그	/var/log/hostd.log	ESXi 호스트와 해당 가상 시스템을 관리하고 구성하는 에이전트에 대한 정보가 들어 있습니다.
vCenter 에이전트 로그	/var/log/vpxa.log	vCenter Server와 통신하는 에이전트에 대한 정보가 들어 있습니다(vCenter Server로 호스트를 관리하는 경우).
셸 로그	/var/log/shell.log	ESXi Shell에 입력한 모든 명령의 기록과 셸 이벤트(예: 셸이 사용하도록 설정된 시점)가 들어 있습니다.
인증	/var/log/auth.log	로컬 시스템의 인증과 관련된 모든 이벤트가 들어 있습니다.

구성 요소	위치	용도
시스템 메시지	<code>/var/log/syslog.log</code>	모든 일반 로그 메시지가 들어 있으며 이 메시지를 문제 해결에 이용할 수 있습니다. 기존에는 이 정보가 메시지 로그 파일에 있었습니다.
가상 시스템	영향을 받는 가상 시스템의 구성 파일과 같은 디렉토리에 있는 <code>vmware.log</code> 및 <code>vmware*.log</code> 파일. 예: <code>/vmfs/volumes/datastore/virtual machine/vmware.log</code>	가상 시스템 전원 이벤트, 시스템 오류 정보, 도구 상태 및 작업, 시간 동기화, 가상 하드웨어 변경, vMotion 마이그레이션, 시스템 복제 등이 들어 있습니다.

Fault Tolerance 로깅 트래픽 보안

FT(Fault Tolerance)를 사용하도록 설정한 경우 VMware vLockstep은 기본 VM에서 수행되는 입력 및 이벤트를 캡처하여 다른 호스트에서 실행 중인 보조 VM으로 보냅니다.

기본 VM과 보조 VM 간의 이 로깅 트래픽은 암호화되지 않으며, 게스트 운영 체제의 메모리 내용뿐만 아니라 게스트 네트워크 및 스토리지 I/O 데이터도 포함합니다. 이 트래픽에는 암호와 같은 중요한 데이터가 일반 텍스트로 포함될 수 있습니다. 이러한 데이터가 노출되지 않도록 하려면 이 네트워크가 보안되도록 하고 특히 "메시지 가로채기(man-in-the-middle)" 공격을 방지해야 합니다. 예를 들어 FT 로깅 트래픽에는 전용 네트워크를 사용합니다.

vCenter Server 시스템 보안

6

vCenter Server 보안에는 vCenter Server가 실행 중인 호스트의 보안을 보장하고, 권한 및 역할 할당을 위한 모범 사례를 따르고, vCenter Server에 연결하는 클라이언트의 무결성을 확인하는 작업이 포함됩니다.

본 장은 다음 항목을 포함합니다.

- vCenter Server 보안 모범 사례
- 기존 ESXi 호스트 지문 확인
- NFC(Network File Copy)를 통한 SSL 인증서 유효성 검사 사용 확인
- vCenter Server TCP 및 UDP 포트
- CIM 기반 하드웨어 모니터링 도구 액세스 제어

vCenter Server 보안 모범 사례

vCenter Server 보안 모범 사례를 따르면 vSphere 환경의 무결성을 보장할 수 있습니다.

vCenter Server 액세스 제어에 대한 모범 사례

다양한 vCenter Server 구성 요소에 대한 액세스를 엄격하게 제어하여 시스템의 보안을 향상시킵니다.

다음 지침은 환경의 보안을 강화하는 데 도움이 됩니다.

명명된 계정 사용

- 현재 로컬 Windows 관리자 계정에 vCenter Server에 대한 전체 관리 권한이 있는 경우 이러한 액세스 권한을 제거하고 해당 권한을 하나 이상의 명명된 vCenter Server 관리자 계정에 부여합니다. 전체 관리 권한은 필요한 관리자에게만 부여합니다. 구성원 자격이 엄격히 제어되지 않는 그룹에는 이 권한을 부여하지 마십시오.

참고 vSphere 6.0부터 로컬 관리자는 더 이상 기본적으로 vCenter Server에 대한 전체 관리 권한이 없습니다. 로컬 운영 체제 사용자 사용은 권장되지 않습니다.

- Windows 계정 대신 서비스 계정을 사용하여 vCenter Server를 설치합니다. 서비스 계정은 로컬 시스템의 관리자여야 합니다.
- vCenter Server 시스템에 연결할 때 애플리케이션이 고유한 서비스 계정을 사용해야 합니다.

액세스 최소화

사용자가 vCenter Server 호스트 시스템에 직접 로그인하지 않도록 합니다. vCenter Server에 로그인된 사용자는 설정을 변경하고 프로세스를 수정하여 의도적이든 의도적이지 않든 잠재적으로 피해를 끼칠 수 있습니다. 그들은 또한 SSL 인증서와 같은 vCenter 자격 증명에 액세스할 수도 있습니다. 수행할 정당한 작업이 있는 사용자만 시스템에 로그인할 수 있도록 하고 로그인 이벤트가 감사되도록 합니다.

vCenter Server 관리자의 권한 모니터링

모든 관리자에게 관리자 역할이 있어야 하는 것은 아닙니다. 대신 적절한 권한 집합이 있는 사용자 지정 역할을 생성하고 이를 다른 관리자에게 할당합니다.

vCenter Server 관리자 역할이 있는 사용자는 계층의 모든 개체에 대한 권한이 있습니다. 예를 들어 기본적으로 관리자 역할이 있는 사용자는 가상 시스템의 게스트 운영 체제 내에서 파일 및 프로그램과 상호 작용할 수 있습니다. 이러한 역할을 너무 많은 사용자에게 할당하면 가상 시스템 데이터 기밀성, 가용성 또는 무결성이 줄어들 수 있습니다. 관리자에게 필요한 권한을 부여하는 역할을 생성하되 가상 시스템 관리 권한의 일부를 제거합니다.

vCenter Server 데이터베이스 사용자에게 최소 권한 부여

데이터베이스 사용자에게는 데이터베이스 액세스와 관련된 일부 권한만 필요합니다. 또한 일부 권한은 설치 및 업그레이드의 경우에만 필요합니다. 이러한 권한은 제품 설치 또는 업그레이드 후 제거할 수 있습니다.

데이터스토어 브라우저 액세스 제한

데이터스토어 브라우저 기능은 적절한 권한을 가진 사용자가 웹 브라우저 또는 vSphere Web Client를 통해 vSphere 배포에 연결된 데이터스토어에서 파일을 보거나, 업로드하거나 다운로드할 수 있도록 지원합니다. **데이터스토어.데이터스토어 찾아보기** 권한은 해당 권한이 실제로 필요한 사용자 또는 그룹에만 할당합니다.

가상 시스템에서 사용자의 명령 실행 제한

기본적으로 vCenter Server 관리자 역할이 할당된 사용자는 가상 시스템의 게스트 운영 체제 내에서 파일 및 프로그램과 상호 작용할 수 있습니다. 게스트 기밀성, 가용성 또는 무결성이 침해될 위험을 줄이려면 **게스트 작업** 권한이 없는 게스트가 아닌 액세스 역할을 생성해야 합니다. **사용자가 가상 시스템 내에서 명령을 실행하지 못하도록 제한**을 참조하십시오.

vpxuser의 암호 정책 확인

기본적으로 vCenter Server는 자동으로 30일마다 vpxuser 암호를 변경합니다. 이 설정이 정책을 준수하는지 확인하거나 회사의 암호 사용 기간 정책을 준수하도록 정책을 구성합니다. **vCenter Server 암호 정책 설정**를 참조하십시오.

참고 암호 사용 기간 정책이 너무 짧지 않아야 합니다.

vCenter Server 다시 시작 후 권한 확인

vCenter Server를 다시 시작할 때는 권한 재할당을 확인합니다. 루트 폴더에서 관리자 역할이 할당된 사용자 또는 사용자 그룹이 다시 시작 동안 유효한 사용자 또는 그룹으로 확인되지 않는 경우 해당 사용자 또는 그룹에서 역할이 제거됩니다. 그 대신 vCenter Server는 vCenter Single Sign-On 계정 administrator@vsphere.local에 관리자 역할을 부여합니다. 그러면 이 계정이 관리자 역할을 수행할 수 있습니다.

명명된 관리자 계정을 다시 설정하고 관리자 역할을 해당 계정에 할당하여 익명 administrator@vsphere.local 계정 사용을 방지합니다.

높은 수준의 RDP 암호화 사용

인프라의 각 Windows 컴퓨터에서 원격 데스크톱 호스트 구성 설정이 환경에 적합한 최고 수준의 암호화를 보장하도록 설정되었는지 확인합니다.

vSphere Web Client 인증서 확인

vSphere Web Client 또는 다른 클라이언트 애플리케이션 장치 중 하나의 사용자가 인증서 확인 경고를 절대 무시하지 않도록 지시해야 합니다. 인증서가 확인되지 않으면 사용자가 MITM 공격의 대상이 될 수 있습니다.

vCenter Server 암호 정책 설정

기본적으로 vCenter Server는 30일마다 자동으로 vpxuser 암호를 변경합니다. vSphere Web Client에서 해당 값을 변경할 수 있습니다.

절차

- 1 vSphere Web Client 개체 계층에서 vCenter Server를 선택합니다.
- 2 **관리** 탭을 클릭하고 **설정** 하위 탭을 클릭합니다.
- 3 **고급 설정**을 클릭하고 필터 상자에 **VimPasswordExpirationInDays**를 입력합니다.
- 4 요구 사항에 맞게 VirtualCenter.VimPasswordExpirationInDays를 설정합니다.

vCenter Server Windows 호스트 보호

호스트 환경의 보안을 최대한 유지하여 vCenter Server가 실행 중인 Windows 호스트를 취약성 및 공격으로부터 보호합니다.

- vCenter Server 시스템에서 지원하는 운영 체제, 데이터베이스 및 하드웨어를 유지합니다. vCenter Server가 지원되는 운영 체제에서 실행되고 있지 않으면 적절하게 실행되지 않아서 vCenter Server가 공격에 취약해질 수 있습니다.
- vCenter Server 시스템에 패치를 적절하게 적용합니다. 최신 운영 체제 패치를 적용하면 공격에 대한 서버의 취약성을 줄일 수 있습니다.
- vCenter Server 호스트에서 운영 체제를 보호합니다. 보호에는 안티바이러스 및 안티멀웨어 소프트웨어가 포함됩니다.

- 인프라의 각 Windows 컴퓨터에서 RDP(원격 데스크톱) 호스트 구성 설정이 업계 표준 지침 또는 내부 지침에 따라 최고 수준의 암호화를 보장하도록 설정되어 있는지 확인합니다.

운영 체제 및 데이터베이스 호환성 정보에 대해서는 "vSphere 호환성 매트릭스"를 참조하십시오.

실패한 설치에서 만료되거나 해지된 인증서 및 로그 제거

vCenter Server 시스템에 만료되거나 해지된 인증서를 그대로 두거나, 설치에 실패한 vCenter Server 설치 로그를 그대로 두면 사용 환경의 성능이 저하될 수 있습니다.

만료되거나 해지된 인증서를 제거해야 하는 이유는 다음과 같습니다.

- 만료되거나 해지된 인증서를 vCenter Server 시스템에서 제거하지 않으면 환경이 MiTM 공격의 대상이 될 수 있습니다.
- vCenter Server 설치에 실패하면 일반 텍스트의 데이터베이스 암호가 포함된 로그 파일이 시스템에 생성되는 경우도 있습니다. vCenter Server 시스템에 침입하는 공격자는 이 암호에 액세스하는 동시에 vCenter Server 데이터베이스에 액세스할 수 있습니다.

vCenter Server 네트워크 연결 제한

보안을 강화하기 위해 vCenter Server 시스템을 관리 네트워크가 아닌 다른 네트워크에 배치해서는 안 되며, vSphere 관리 트래픽이 제한된 네트워크에 있어야 합니다. 네트워크 연결을 제한하면 특정 유형의 공격을 제한할 수 있습니다.

vCenter Server에는 관리 네트워크에 대한 액세스만 필요합니다. vCenter Server 시스템을 운영 네트워크, 스토리지 네트워크 등의 다른 네트워크 또는 인터넷에 대한 액세스 권한이 있는 네트워크에 배치하지 마십시오. vCenter Server는 vMotion이 작동하는 네트워크에 액세스할 필요가 없습니다.

vCenter Server에는 다음 시스템에 대한 네트워크 연결이 필요합니다.

- 모든 ESXi 호스트
- vCenter Server 데이터베이스
- 기타 vCenter Server 시스템(vCenter Server 시스템이 태그, 사용 권한 등의 복제를 위한 공통 vCenter Single Sign-On 도메인의 일부인 경우).
- 관리 클라이언트 실행 권한이 부여된 시스템. 예를 들어 PowerCLI 또는 다른 모든 SDK 기반 클라이언트를 사용하는 Windows 시스템인 vSphere Web Client가 있습니다.
- VMware vSphere Update Manager와 같은 추가 기능 구성 요소를 실행하는 시스템
- DNS, Active Directory 및 NTP와 같은 인프라 서비스
- vCenter Server 시스템의 기능에 필수적인 구성 요소를 실행하는 기타 시스템

vCenter Server 시스템이 실행 중인 Windows 시스템의 로컬 방화벽을 사용하거나 네트워크 방화벽을 사용합니다. 필요한 구성 요소만 vCenter Server 시스템과 통신할 수 있도록 IP 기반 액세스 제한을 포함합니다.

Linux 클라이언트 사용 제한 고려

클라이언트 구성 요소와 vCenter Server 시스템 또는 ESXi 호스트 간의 통신은 기본적으로 SSL 기반 암호화를 통해 보호됩니다. Linux 버전의 이러한 구성 요소는 인증서 검증을 수행하지 않습니다. 이러한 클라이언트 사용 제한을 고려하십시오.

vCenter Server 시스템 및 ESXi 호스트의 VMCA 서명된 인증서를 타사 CA에서 서명한 인증서로 교체하더라도 Linux 클라이언트와의 특정 통신이 계속해서 메시지 가로채기(man-in-the-middle) 공격에 취약할 수 있습니다. 다음 구성 요소는 Linux 운영 체제에서 실행될 때 취약성이 드러납니다.

- vCLI 명령
- Perl용 vSphere SDK 스크립트
- vSphere Web Services SDK를 사용하여 작성한 프로그램

적절한 제어를 적용하는 경우 Linux 클라이언트에 대한 제한을 다소 완화할 수 있습니다.

- 인증된 시스템만 관리 네트워크에 액세스할 수 있도록 제한합니다.
- 방화벽을 사용하여 인증된 호스트만 vCenter Server에 액세스하도록 허용합니다.
- 점프 박스(jump-box) 시스템을 사용하여 Linux 클라이언트를 점프 뒤에 배치합니다.

설치된 플러그인 검사

vSphere Web Client 확장은 로그인한 사용자와 동일한 권한 수준에서 실행됩니다. 따라서 악성 확장이 유용한 플러그인으로 가장하고 자격 증명을 도용하거나 시스템 구성을 변경하는 등의 유해한 작업을 수행할 수 있습니다. 보안을 강화하려면 신뢰할 수 있는 소스의 인증된 확장만 포함하는 vSphere Web Client 설치를 사용합니다.

vCenter 설치에 포함된 vSphere Web Client 확장성 프레임워크에서는 vCenter 추가 기능 구성 요소 또는 외부 웹 기반 기능에 액세스할 수 있는 메뉴 선택이나 도구 모음 아이콘을 사용하여 vSphere Web Client를 확장하는 기능을 제공합니다. 이와 같은 유연성 때문에 의도하지 않는 기능이 도입될 위험이 있습니다. 예를 들어 관리자가 vSphere Web Client의 인스턴스에 플러그인을 설치하면 이 플러그인을 사용하여 해당 관리자의 권한 수준으로 임의의 명령을 실행할 수 있습니다.

vSphere Web Client의 잠재적인 손상을 방지하려면 설치된 모든 플러그인을 정기적으로 검사하고 모든 플러그인이 신뢰할 수 있는 소스에서 전송되었는지 확인해야 합니다.

사전 요구 사항

vCenter Single Sign-On 서비스에 액세스할 수 있는 권한이 있어야 합니다. 이러한 권한은 vCenter Server 권한과는 다릅니다.

절차

- 1 administrator@vsphere.local 또는 vCenter Single Sign-On 권한을 보유한 사용자로 vSphere Web Client에 로그인합니다.
- 2 홈 페이지에서 **관리**를 선택한 후 **솔루션** 아래에서 **클라이언트 플러그인**을 선택합니다.
- 3 클라이언트 플러그인 목록을 검토합니다.

vCenter Server Appliance 보안 모범 사례

vCenter Server 시스템을 보호하기 위한 모든 모범 사례를 준수하여 vCenter Server Appliance를 보호합니다. 추가 단계는 환경을 더욱 안전하게 보호하는 데 도움이 됩니다.

NTP 구성

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 인증서 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. [NTP 서버와 vCenter Server Appliance의 시간 동기화](#)를 참조하십시오.

vCenter Server Appliance 네트워크 액세스 제한

vCenter Server Appliance와 통신하는 데 필요한 해당 필수 구성 요소로만 액세스를 제한합니다. 불필요한 시스템의 액세스 차단은 운영 체제에 대한 일반적인 공격의 가능성을 줄입니다. 해당 필수 구성 요소로만 액세스를 제한하는 것은 위험을 최소화합니다.

기존 ESXi 호스트 지문 확인

vSphere 6 이상에서는 기본적으로 호스트에 VMCA 인증서가 할당됩니다. 인증서 모드를 지문으로 변경하는 경우 기존 호스트에 대해 계속해서 지문 모드를 사용할 수 있습니다. vSphere Web Client에서 지문을 확인할 수 있습니다.

참고 기본적으로 인증서는 업그레이드 동안 보존됩니다.

절차

- 1 vSphere Web Client 개체 탐색기에서 vCenter Server 시스템을 찾습니다.
- 2 **관리** 탭을 선택하고 **설정**을 클릭하고 **일반**을 클릭합니다.
- 3 **편집**을 클릭합니다.
- 4 **SSL 설정**을 클릭합니다.
- 5 ESXi 5.5 이하 호스트 중 수동 검증이 필요한 호스트가 있는 경우 호스트에 대해 나열된 지문을 호스트 콘솔의 지문과 비교합니다.

호스트 지문을 가져오려면 DCUI(Direct Console User Interface)를 사용합니다.

- a 직접 콘솔에 로그인하고 F2 키를 눌러 시스템 사용자 지정 메뉴에 액세스합니다.
- b **지원 정보 보기**를 선택합니다.

호스트 지문이 오른쪽 열에 나타납니다.

- 6 지문이 일치하면 호스트 옆의 **확인** 확인란을 선택합니다.
선택되지 않은 호스트는 **확인**을 클릭한 후 연결 해제됩니다.

7 확인을 클릭합니다.

NFC(Network File Copy)를 통한 SSL 인증서 유효성 검사 사용 확인

NFC(Network File Copy)는 vSphere 구성 요소를 위한 파일 형식 인식 FTP 서비스를 제공합니다.

vSphere 5.5부터 ESXi는 기본적으로 데이터스토어 간 데이터 복사 및 이동과 같은 작업을 위해 NFC를 사용하지만 NFC가 사용되지 않도록 설정된 경우 사용되도록 설정해야 할 수 있습니다.

NFC를 통한 SSL을 사용하도록 설정하면 NFC를 통한 vSphere 구성 요소 간의 연결에 보안이 적용됩니다. 이 연결은 데이터 센터 내의 메시지 가로채기 공격을 방지하는 데 도움이 될 수 있습니다.

NFC를 통한 SSL을 사용하면 약간의 성능 저하가 발생하기 때문에 일부 개발 환경에서는 이 고급 설정을 사용하지 않도록 설정해야 할 수도 있습니다.

참고 값을 확인하기 위해 스크립트를 사용할 경우 명시적으로 이 값을 `true`로 설정합니다.

절차

- 1 vSphere Web Client를 사용하여 vCenter Server에 연결합니다.
- 2 **설정** 탭을 선택하고 **고급 설정**을 클릭합니다.
- 3 **편집**을 클릭합니다.
- 4 대화 상자 아래쪽에 다음과 같은 키와 값을 입력합니다.

필드	값
키	config.nfc.useSSL
값	true

- 5 **확인**을 클릭합니다.

vCenter Server TCP 및 UDP 포트

vCenter Server는 사전 결정된 TCP 및 UDP 포트를 통해 액세스됩니다. 방화벽 외부에서 네트워크 구성 요소를 관리하는 경우 적절한 포트에 액세스할 수 있도록 방화벽을 다시 구성해야 할 수 있습니다.

다음 표에는 TCP 및 UDP 포트와 각 포트의 용도 및 유형이 나와 있습니다. 설치 시 기본적으로 열리는 포트는 (기본값)으로 표시되어 있습니다. 다양한 vSphere 버전의 모든 vSphere 구성 요소에 대한 최신 포트 목록은 [VMware 기술 자료 문서 1012382](#)를 참조하십시오.

표 6-1. vCenter Server TCP 및 UDP 포트

포트	용도
80(기본값)	HTTP 액세스 vCenter Server에서는 직접 HTTP 연결에 포트 80이 필요합니다. 포트 80은 요청을 HTTPS 포트 443으로 리디렉션합니다. 이 리디렉션은 https://server 대신 실수로 http://server 를 사용하는 경우에 유용합니다. WS 관리(포트 443도 열려 있어야 함)
88, 2013	Kerberos용 제어 인터페이스 RPC(vCenter Single Sign-On에서 사용)
123	NTP 클라이언트
135(기본값)	vCenter Server Appliance의 경우 이 포트는 Active Directory 인증용으로 지정됩니다. vCenter Server Windows 설치의 경우 이 포트는 연결 모드에 사용되며 포트 88이 Active Directory 인증에 사용됩니다.
161(기본값)	SNMP 서버. ESXi 호스트와 vCenter Server Appliance 모두의 기본 포트입니다.
389	vCenter Single Sign-On LDAP(6.0 이상)
636	vCenter Single Sign-On LDAPS(6.0 이상)
443(기본값)	vCenter Server 시스템은 포트 443을 사용하여 SDK 클라이언트의 데이터 전송을 모니터링합니다. 이 포트는 다음 서비스에도 사용됩니다. <ul style="list-style-type: none"> ■ WS 관리(포트 80도 열려 있어야 함) ■ 타사 네트워크 관리 클라이언트에서 vCenter Server에 연결할 때 ■ 타사 네트워크 관리 클라이언트에서 호스트에 액세스할 때
2012	VMware Directory Service(vmdir)의 RPC 포트
2014	VMCA(VMware Certificate Authority) 서비스의 RPC 포트.
2020	VMware Authentication Framework Service(vmafd)의 RPC 포트
31031, 44046(기본값)	vSphere Replication
7444	vCenter Single Sign-On HTTPS
8093	클라이언트 통합 플러그인은 로컬 루프백 호스트 이름을 사용하며 포트 8093과 50100-60099 범위 내의 임의의 포트를 사용합니다. 클라이언트 통합 플러그인은 포트 8093을 로컬 통신용으로만 사용합니다. 이 포트는 방화벽으로 차단되어 있을 수 있습니다.
8109	VMware Syslog Collector
9443	vSphere Web Client에서 ESXi 호스트에 대해 HTTP 액세스를 수행할 때 사용
10080	Inventory Service
11711	vCenter Single Sign-On LDAP(vSphere 5.5에서 업그레이드된 환경)
11712	vCenter Single Sign-On LDAPS(vSphere 5.5에서 업그레이드된 환경)
12721	VMware Identity Management Service

표 6-1. vCenter Server TCP 및 UDP 포트 (계속)

포트	용도
15005	EAM(ESX Agent Manager). ESX Agent는 가상 시스템이거나 선택적 VIB일 수 있습니다. 이 에이전트는 ESXi 호스트의 기능을 확장하여 NSX-v 또는 vRealize Automation 등의 vSphere 솔루션에 필요한 추가 서비스를 제공합니다.
15007	VSM(vService Manager). 이 서비스는 vCenter Server 확장을 등록합니다. 사용하려는 확장에서 필요한 경우에만 이 포트를 엽니다.
50100-60099	클라이언트 통합 플러그인은 로컬 루프백 호스트 이름을 사용하며 포트 8093과 50100-60099 범위 내의 임의의 포트를 사용합니다. 클라이언트 통합 플러그인은 이 포트 범위를 로컬 통신용으로만 사용합니다. 이 포트는 방화벽으로 차단되어 있을 수 있습니다.

이러한 포트 외에도 필요에 따라 다른 포트를 구성할 수 있습니다.

CIM 기반 하드웨어 모니터링 도구 액세스 제어

CIM(공통 정보 모형, Common Information Model) 시스템에서는 표준 API 집합을 사용하여 원격 애플리케이션에서 하드웨어 수준 관리를 사용할 수 있게 해 주는 인터페이스를 제공합니다. CIM 인터페이스의 보안을 유지하려면 이러한 애플리케이션에 필요한 최소한의 액세스 권한만 제공합니다. 애플리케이션이 루트 또는 전체 관리자 계정으로 프로비저닝된 경우 애플리케이션이 손상되면 전체 가상 환경이 손상될 수 있습니다.

CIM은 ESXi의 하드웨어 리소스를 에이전트 없이 표준에 따라 모니터링하기 위한 프레임워크를 정의하는 개방형 표준입니다. 이 프레임워크는 CIM 개체 관리자(CIM 브로커라고도 함)와 일련의 CIM 제공자로 구성됩니다.

CIM 제공자는 디바이스 드라이버와 기본 하드웨어에 대한 관리 액세스 권한을 제공하기 위한 메커니즘으로 사용됩니다. 서버 제조업체와 특정 하드웨어 디바이스 벤더를 비롯한 하드웨어 벤더는 특정 디바이스의 모니터링 및 관리 기능을 제공하기 위한 제공자를 작성할 수 있습니다. VMware에서도 서버 하드웨어, ESXi 스토리지 인프라 및 가상화 관련 리소스의 모니터링을 구현하는 제공자를 작성합니다. 이러한 제공자는 ESXi 시스템 내부에서 실행되므로 매우 경량으로 설계되어 특정 관리 작업에 초점을 맞춥니다. CIM 브로커는 모든 CIM 제공자로부터 정보를 받고, 표준 API(WS-MAN이 가장 일반적)를 통해 이를 외부에 표시합니다.

원격 애플리케이션에는 CIM 인터페이스에 액세스하기 위한 루트 자격 증명을 제공하지 마십시오. 대신 해당 애플리케이션에 특정한 서비스 계정을 생성하고, ESXi 시스템에 정의된 모든 로컬 계정과 vCenter Server에 정의된 모든 역할에 CIM 정보에 대한 읽기 전용 액세스 권한을 부여하십시오.

절차

- 1 CIM 애플리케이션에 특정한 서비스 계정 생성
- 2 ESXi 시스템에 정의된 모든 로컬 계정과 vCenter Server에 정의된 모든 역할에 CIM 정보에 대한 읽기 전용 액세스 권한을 부여합니다.

- 3 (선택 사항) 애플리케이션에 CIM 인터페이스에 대한 쓰기 액세스 권한이 필요한 경우 다음 두 개의 권한만 포함하여 서비스 계정에 적용할 역할을 생성합니다.

- **Host.Config.SystemManagement**

- **Host.CIM.CIMInteraction**

이 역할은 모니터링 애플리케이션의 작동 방식에 따라 호스트에 대해 로컬로 존재하거나 vCenter Server 중앙에서 정의될 수 있습니다.

결과

CIM 애플리케이션을 위해 생성한 서비스 계정으로 호스트에 로그인하는 사용자는 **SystemManagement** 및 **CIMInteraction** 권한이나 읽기 전용 액세스 권한만 갖게 됩니다.

가상 시스템 보안

7

가상 시스템에서 실행되는 게스트 운영 체제에는 물리적 시스템과 동일한 보안 위험이 따릅니다. 물리적 시스템을 보호하는 것과 마찬가지로 가상 시스템을 보호합니다.

본 장은 다음 항목을 포함합니다.

- 가상 시스템에서 **VMX** 파일로의 정보 메시지 제한
- 가상 디스크 축소 방지
- 가상 시스템 보안 모범 사례

가상 시스템에서 VMX 파일로의 정보 메시지 제한

데이터스토어가 가득 차서 DoS(서비스 거부)가 발생하는 것을 방지하기 위해 가상 시스템의 정보 메시지를 **VMX** 파일로 제한할 수 있습니다. 가상 시스템의 **VMX** 파일 크기를 제어하지 않고 정보의 양이 데이터스토어의 용량을 초과하면 서비스 거부 발생 가능성이 있습니다.

정보 이름-값 쌍이 포함된 구성 파일은 기본적으로 크기가 **1MB**로 제한됩니다. 대부분의 경우 이 용량으로 충분하지만 필요한 경우 이 값을 변경할 수 있습니다. 예를 들어 대량의 사용자 지정 정보가 구성 파일에 저장되는 경우에는 제한을 늘릴 수 있습니다.

참고 필요한 정보의 분량을 신중하게 고려합니다. 정보량이 데이터스토어의 용량을 초과하면 서비스가 거부될 수 있습니다.

`tools.setInfo.sizeLimit` 매개 변수가 고급 옵션에 나열되지 않더라도 **1MB**의 기본 제한이 적용됩니다.

절차

- 1 vSphere Web Client 인벤토리에서 가상 시스템을 찾습니다.
 - a 데이터 센터, 폴더, 클러스터, 리소스 풀 또는 호스트를 선택합니다.
 - b **관련 항목** 탭을 클릭하고 **가상 시스템**을 클릭합니다.
- 2 가상 시스템을 마우스 오른쪽 버튼으로 클릭한 후 **설정 편집**을 클릭합니다.
- 3 **VM 옵션**을 선택합니다.
- 4 **고급**을 클릭하고 **구성 편집**을 클릭합니다.

5 `tools.setInfo.sizeLimit` 매개 변수를 추가하거나 편집합니다.

가상 디스크 축소 방지

게스트 운영 체제에서 관리 권한이 없는 사용자가 가상 디스크를 축소할 수 있습니다. 가상 디스크를 축소하면 디스크의 사용되지 않는 공간이 회수됩니다. 하지만 디스크를 반복적으로 축소하면 디스크를 사용할 수 없게 되고 서비스 거부가 발생할 수 있습니다. 이를 방지하려면 가상 디스크 축소 기능을 사용할 수 없도록 설정하십시오.

사전 요구 사항

- 가상 시스템을 끕니다.
- 가상 시스템에 대한 루트 또는 관리자 권한이 있는지 확인합니다.

절차

- 1 vSphere Web Client 인벤토리에서 가상 시스템을 찾습니다.
 - a 데이터 센터, 폴더, 클러스터, 리소스 풀 또는 호스트를 선택합니다.
 - b **관련 항목** 탭을 클릭하고 **가상 시스템**을 클릭합니다.
- 2 가상 시스템을 마우스 오른쪽 버튼으로 클릭한 후 **설정 편집**을 클릭합니다.
- 3 **VM 옵션**을 선택합니다.
- 4 **고급**을 클릭하고 **구성 편집**을 클릭합니다.
- 5 다음 매개 변수를 추가하거나 편집합니다.

이름	값
<code>isolation.tools.diskWiper.disable</code>	TRUE
<code>isolation.tools.diskShrink.disable</code>	TRUE

- 6 **확인**을 클릭합니다.

결과

이 기능을 사용하지 않도록 설정할 때 데이터스토어에 공간이 부족하면 가상 시스템 디스크를 축소할 수 없습니다.

가상 시스템 보안 모범 사례

가상 시스템 보안 모범 사례를 따르면 vSphere 배포의 무결성을 보장할 수 있습니다.

■ 일반 가상 시스템 보호

가상 시스템은 대부분의 측면에서 물리적 서버와 동일합니다. 물리적 시스템에서와 동일한 보안 대책을 가상 시스템에 적용합니다.

■ 템플릿을 사용하여 가상 시스템 배포

가상 시스템에서 게스트 운영 체제 및 애플리케이션을 수동으로 설치하는 경우 구성이 잘못될 위험이 있습니다. 애플리케이션이 설치되지 않은 확장된 기본 운영 체제 이미지를 템플릿을 사용하여 캡처하면 모든 가상 시스템이 알려진 기준선 보안 수준으로 생성되었는지 확인할 수 있습니다.

■ 가상 시스템 콘솔 사용 최소화

가상 시스템 콘솔은 물리적 서버의 모니터가 제공하는 가상 시스템에 동일한 기능을 제공합니다. 가상 시스템 콘솔에 대한 액세스 권한이 있는 사용자는 가상 시스템 전원 관리 및 이동식 디바이스 연결 제어에 대한 액세스 권한이 있어 가상 시스템이 악의적인 공격을 받을 수 있습니다.

■ 가상 시스템의 리소스 대체 방지

가상 시스템 하나가 호스트 리소스를 너무 많이 사용하여 호스트의 다른 가상 시스템이 원하는 기능을 수행할 수 없으면 DoS(서비스 거부)가 발생할 수 있습니다. 가상 시스템에서 DoS가 발생하는 것을 방지하려면 공유 설정 및 리소스 풀 사용과 같은 호스트 리소스 관리 기능을 사용합니다.

■ 가상 시스템 내의 불필요한 기능 사용 안 함

가상 시스템에서 실행되는 모든 서비스는 공격을 받을 가능성이 있습니다. 시스템에서 실행 중인 애플리케이션이나 서비스를 지원하는 데 필요하지 않은 시스템 구성 요소를 사용하지 않도록 설정하면 공격 받을 가능성이 있는 구성 요소의 수를 줄일 수 있습니다.

일반 가상 시스템 보호

가상 시스템은 대부분의 측면에서 물리적 서버와 동일합니다. 물리적 시스템에서와 동일한 보안 대책을 가상 시스템에 적용합니다.

가상 시스템을 보호하려면 다음 모범 사례를 따르십시오.

패치 및 다른 보호

모든 보안 대책은 적절한 패치의 적용을 포함하여 항상 최신 상태로 유지해야 합니다. 특히 간과하기 쉬운 전원이 꺼진 유휴 가상 시스템의 업데이트도 적절하게 관리해야 합니다. 예를 들어 가상 인프라의 모든 가상 시스템에서 바이러스 백신 소프트웨어, 스파이웨어 차단, 침입 탐지 및 기타 보호 기능을 설정해야 합니다. 또한 가상 시스템 로그를 저장할 공간이 충분한지 확인해야 합니다.

바이러스 백신 검색

각 가상 시스템에서는 표준 운영 체제를 호스트하므로 바이러스 백신 소프트웨어를 설치하여 바이러스로부터 보호해야 합니다. 가상 시스템을 사용하는 방식에 따라 소프트웨어 방화벽을 설치해야 할 수도 있습니다.

특히 가상 시스템의 수가 많은 배포에서는 바이러스 검사 일정이 서로 겹치지 않도록 하십시오. 모든 가상 시스템을 동시에 검사하면 환경의 시스템 성능이 크게 저하됩니다. 소프트웨어 방화벽과 바이러스 백신 소프트웨어는 가상화 리소스를 많이 사용할 수 있으므로, 특히 가상 시스템의 환경이 완전히 신뢰할 수 있는 수준이라고 생각하는 경우에는, 가상 시스템의 성능과 이 두 보안 대책의 필요성을 함께 고려해야 합니다.

직렬 포트

직렬 포트는 주변 디바이스를 가상 시스템에 연결하기 위한 인터페이스입니다. 서버 콘솔에 하위 수준의 직접 연결을 제공하기 위해 종종 사용되며, 가상 직렬 포트는 가상 시스템에 동일한 액세스를 허용합니다. 직렬 포트는 하위 수준의 액세스를 허용하며 로깅 또는 권한과 같은 강력한 제어는 없는 경우가 많습니다.

템플릿을 사용하여 가상 시스템 배포

가상 시스템에서 게스트 운영 체제 및 애플리케이션을 수동으로 설치하는 경우 구성이 잘못될 위험이 있습니다. 애플리케이션이 설치되지 않은 확장된 기본 운영 체제 이미지를 템플릿을 사용하여 캡처하면 모든 가상 시스템이 알려진 기준선 보안 수준으로 생성되었는지 확인할 수 있습니다.

패치가 적용되고 올바르게 구성된 확장된 운영 체제를 포함하는 템플릿을 사용하여 다른 애플리케이션별 템플릿을 생성하거나, 애플리케이션 템플릿을 사용하여 가상 시스템을 배포할 수 있습니다.

절차

- ◆ 패치가 적용되고 올바르게 구성된 확장된 운영 체제 배포를 포함하는 가상 시스템을 생성하기 위한 템플릿을 제공합니다.

가능하면 애플리케이션도 템플릿으로 배포합니다. 애플리케이션이 배포할 가상 시스템과 관련된 정보에 종속되지 않아야 합니다.

다음에 수행할 작업

템플릿에 대한 자세한 내용은 "vSphere 가상 시스템 관리" 설명서를 참조하십시오.

가상 시스템 콘솔 사용 최소화

가상 시스템 콘솔은 물리적 서버의 모니터가 제공하는 가상 시스템에 동일한 기능을 제공합니다. 가상 시스템 콘솔에 대한 액세스 권한이 있는 사용자는 가상 시스템 전원 관리 및 이동식 디바이스 연결 제어에 대한 액세스 권한이 있어 가상 시스템이 악의적인 공격을 받을 수 있습니다.

절차

- 1 터미널 서비스 및 SSH와 같은 네이티브 원격 관리 서비스를 사용하여 가상 시스템과 상호 작용합니다.

가상 시스템 콘솔에 대한 액세스 권한은 필요한 경우에만 부여합니다.

- 2 필요한 경우 콘솔에 대한 연결을 소수의 연결로 제한합니다.

예를 들어 보안 수준이 높은 환경에서 연결을 하나로 제한합니다. 일부 환경에서는 정상 작업을 수행하는 데 필요한 동시 연결 수에 따라 제한을 늘릴 수 있습니다.

가상 시스템의 리소스 대체 방지

가상 시스템 하나가 호스트 리소스를 너무 많이 사용하여 호스트의 다른 가상 시스템이 원하는 기능을 수행할 수 없으면 DoS(서비스 거부)가 발생할 수 있습니다. 가상 시스템에서 DoS가 발생하는 것을 방지하려면 공유 설정 및 리소스 풀 사용과 같은 호스트 리소스 관리 기능을 사용합니다.

기본적으로 ESXi 호스트의 모든 가상 시스템이 동등하게 리소스를 공유합니다. 공유 및 리소스 풀을 사용하면 한 개의 가상 시스템이 호스트의 리소스를 너무 많이 사용하여 동일한 호스트의 다른 가상 시스템이 의도한 기능을 수행할 수 없게 하는 서비스 거부 공격을 방지할 수 있습니다.

어떤 영향을 미치는지 완전히 이해하지 못한 경우 제한을 사용하지 마십시오.

절차

- 1 제대로 작동하게 하려면 각 가상 시스템에 충분한 리소스(CPU 및 메모리)를 프로비저닝합니다.
- 2 중요한 가상 시스템이 리소스를 사용할 수 있도록 보장하려면 공유를 사용합니다.
- 3 유사한 요구 사항을 가진 가상 시스템을 리소스 풀로 그룹화합니다.
- 4 각 리소스 풀에서 공유 설정을 기본값으로 유지하여 풀의 각 가상 시스템이 거의 동일한 리소스 우선 순위를 받도록 합니다.

이 설정을 사용하면 단일 가상 시스템이 리소스 풀의 다른 가상 시스템보다 많이 사용할 수 없습니다.

다음에 수행할 작업

공유 및 제한에 대한 자세한 내용은 "vSphere 리소스 관리" 설명서를 참조하십시오.

가상 시스템 내의 불필요한 기능 사용 안 함

가상 시스템에서 실행되는 모든 서비스는 공격을 받을 가능성이 있습니다. 시스템에서 실행 중인 애플리케이션이나 서비스를 지원하는 데 필요하지 않은 시스템 구성 요소를 사용하지 않도록 설정하면 공격 받을 가능성이 있는 구성 요소의 수를 줄일 수 있습니다.

가상 시스템에는 일반적으로 물리적 서버만큼 많은 서비스나 기능이 필요하지 않습니다. 시스템을 가상화할 때는 특정 서비스나 기능이 필요한지 여부를 평가하십시오.

절차

- ◆ 그리고 사용되지 않는 서비스는 운영 체제에서 사용하지 않도록 설정하십시오.
예를 들어 시스템에서 파일 서버를 실행하는 경우에는 웹 서비스를 중지하십시오.
- ◆ CD/DVD 드라이브, 플로피 드라이브 및 USB 어댑터와 같은 사용하지 않는 물리적 디바이스는 연결을 끊으십시오.
- ◆ 사용하지 않는 포시 기능 또는 HGFS(Host Guest File System)와 같은 사용하지 않는 기능을 사용하지 않도록 설정하십시오.
- ◆ 화면 보호기를 끄십시오.
- ◆ 꼭 필요한 경우 이외에는 Linux, BSD 또는 Solaris 게스트 운영 체제에서 X Window 시스템을 실행하지 마십시오.

불필요한 하드웨어 디바이스 제거

사용하도록 설정되거나 연결된 디바이스는 잠재적인 공격 채널이 될 수 있습니다. 가상 시스템에 대한 권한이 없는 사용자 및 프로세스도 네트워크 어댑터 및 CD-ROM 드라이브와 같은 하드웨어 디바이스에 연

결하거나 연결을 끊을 수 있습니다. 공격자는 이 기능을 사용하여 가상 시스템의 보안을 침해할 수 있습니다. 불필요한 하드웨어 디바이스를 제거하면 공격을 방지하는 데 도움이 됩니다.

가상 시스템에 대한 액세스 권한이 있는 공격자가 연결이 끊어진 하드웨어 디바이스에 연결하여 드라이브에 남아 있는 미디어의 중요 정보에 액세스하거나 네트워크 어댑터의 연결을 끊어 가상 시스템을 네트워크에서 격리하여 서비스 거부를 유발할 수 있습니다.

- 인증되지 않은 디바이스가 연결되지 않도록 하고 불필요하거나 사용되지 않는 하드웨어 디바이스는 모두 제거합니다.
- 불필요한 가상 디바이스는 가상 시스템 내에서 사용되지 않도록 설정합니다.
- 꼭 필요한 경우가 아니면 디바이스가 가상 시스템에 연결되지 않도록 합니다. 데이터 센터의 가상 시스템에서는 직렬 및 병렬 포트가 거의 사용되지 않으며 CD/DVD 드라이브는 일반적으로 소프트웨어를 설치할 때만 일시적으로 연결됩니다.

절차

- 1 vSphere Web Client를 사용하여 vCenter Server 시스템에 로그인합니다.
- 2 가상 시스템을 마우스 오른쪽 버튼으로 클릭한 후 **설정 편집**을 클릭합니다.
- 3 각 하드웨어 디바이스를 확인하고 연결 상태를 확인합니다.

다음 디바이스에 대한 확인이 포함됩니다.

- 플로피 드라이브
- 직렬 포트
- 병렬 포트
- USB 컨트롤러
- CD-ROM 드라이브

사용되지 않는 표시 기능 사용 안 함

공격자들은 사용되지 않는 표시 기능을 사용자 환경에 악성 코드를 삽입하기 위한 벡터로 사용할 수 있습니다. 환경에서 사용되지 않는 기능을 사용하지 않도록 설정합니다.

절차

- 1 vSphere Web Client 인벤토리에서 가상 시스템을 찾습니다.
 - a 데이터 센터, 폴더, 클러스터, 리소스 풀 또는 호스트를 선택합니다.
 - b **관련 항목** 탭을 클릭하고 **가상 시스템**을 클릭합니다.
- 2 가상 시스템을 마우스 오른쪽 버튼으로 클릭한 후 **설정 편집**을 클릭합니다.
- 3 **VM 옵션**을 선택합니다.
- 4 **고급**을 클릭하고 **구성 편집**을 클릭합니다.

5 적합한 경우 다음 매개 변수를 추가하거나 편집하여 설정합니다.

옵션	설명
<code>svga.vgaonly</code>	이 매개 변수를 TRUE로 설정할 경우 고급 그래픽 기능이 작동하지 않습니다. 문자 셀 콘솔 모드만 사용할 수 있게 됩니다. 이 설정을 사용하는 경우 <code>mks.enable3d</code> 에 영향을 미치지 않습니다. 참고 이 설정은 가상화된 비디오 카드가 필요하지 않은 가상 시스템에만 적용합니다.
<code>mks.enable3d</code>	3D 기능이 필요하지 않은 가상 시스템에서 이 매개 변수를 FALSE로 설정합니다.

표시되지 않는 기능 사용 안 함

VMware 가상 시스템은 Workstation 및 Fusion 같은 호스팅되는 가상화 플랫폼과 vSphere 시스템 모두에서 작동하도록 설계되었습니다. 가상 시스템을 vSphere 시스템에서 실행할 때는 특정 가상 시스템 매개 변수를 사용하도록 설정할 필요가 없습니다. 이러한 매개 변수를 사용하지 않도록 설정하면 취약점이 노출될 가능성이 낮아집니다.

사전 요구 사항

가상 시스템을 끕니다.

절차

- 1 vSphere Web Client 인벤토리에서 가상 시스템을 찾습니다.
 - a 데이터 센터, 폴더, 클러스터, 리소스 풀 또는 호스트를 선택합니다.
 - b **관련 항목** 탭을 클릭하고 **가상 시스템**을 클릭합니다.
- 2 가상 시스템을 마우스 오른쪽 버튼으로 클릭한 후 **설정 편집**을 클릭합니다.
- 3 **VM 옵션**을 선택합니다.
- 4 **고급**을 클릭하고 **구성 편집**을 클릭합니다.
- 5 다음 매개 변수를 추가하거나 편집하여 TRUE로 설정합니다.
 - `isolation.tools.unity.push.update.disable`
 - `isolation.tools.ghi.launchmenu.change`
 - `isolation.tools.memSchedFakeSampleStats.disable`
 - `isolation.tools.getCreds.disable`
 - `isolation.tools.ghi.autologon.disable`
 - `isolation.bios.bbs.disable`
 - `isolation.tools.hgfsServerSet.disable`
- 6 **확인**을 클릭합니다.

HGFS 파일 전송 사용 안 함

자동화된 도구 업그레이드와 같은 특정 작업은 하이퍼바이저에서 HGFS(호스트 게스트 파일 시스템)라고 하는 구성 요소를 사용합니다. 보안 수준이 높은 환경에서는 이 구성 요소를 사용하지 않도록 설정하여, 공격자가 HGFS를 사용하여 게스트 운영 체제 내에서 파일을 전송할 수 있는 위험을 최소화할 수 있습니다.

절차

- 1 vSphere Web Client 인벤토리에서 가상 시스템을 찾습니다.
 - a 데이터 센터, 폴더, 클러스터, 리소스 풀 또는 호스트를 선택합니다.
 - b **관련 항목** 탭을 클릭하고 **가상 시스템**을 클릭합니다.
- 2 가상 시스템을 마우스 오른쪽 버튼으로 클릭한 후 **설정 편집**을 클릭합니다.
- 3 **VM 옵션**을 선택합니다.
- 4 **고급**을 클릭하고 **구성 편집**을 클릭합니다.
- 5 `isolation.tools.hgfsServerSet.disable` 매개 변수가 TRUE로 설정되었는지 확인합니다.

결과

이러한 변경을 수행할 때 VMX 프로세스는 도구 프로세스의 명령에 더 이상 응답하지 않습니다. 일부 VIX 명령 또는 VMware Tools 자동 업그레이드 유틸리티처럼 HGFS를 사용하여 게스트 운영 체제와 파일을 주고받는 API가 더 이상 작동하지 않습니다.

게스트 운영 체제와 원격 콘솔 간에 복사하여 붙여넣기 작업 사용 안 함

게스트 운영 체제와 원격 콘솔 간의 복사하여 붙여넣기 작업은 기본적으로 사용하지 않도록 설정되어 있습니다. 보안 환경의 경우 기본 설정을 유지하십시오. 복사하여 붙여넣기 작업이 필요한 경우 vSphere Web Client를 사용하여 해당 작업을 사용하도록 설정해야 합니다.

이러한 옵션은 권장되는 값으로 기본 설정됩니다. 하지만 설정이 올바른지 확인하기 위해 감사 도구를 사용하도록 설정하려면 명시적으로 값을 `true`로 설정해야 합니다.

사전 요구 사항

가상 시스템을 끕니다.

절차

- 1 vSphere Web Client를 사용하여 vCenter Server 시스템에 로그인합니다.
- 2 가상 시스템을 마우스 오른쪽 버튼으로 클릭한 후 **설정 편집**을 클릭합니다.
- 3 **VM 옵션**을 클릭하고 **구성 편집**을 클릭합니다.

- 4 이름 및 값 열에서 다음 값을 확인하거나 **행 추가**를 클릭하여 추가합니다.

이름	권장되는 값
isolation.tools.copy.disable	참
isolation.tools.paste.disable	참
isolation.tools.setGUIOptions.enable	false

이 옵션은 게스트 운영 체제의 VMware Tools 제어판에서 지정된 설정을 모두 재정의합니다.

- 5 **확인**을 클릭합니다.

- 6 (선택 사항) 구성 매개 변수를 변경한 경우 가상 시스템을 다시 시작합니다.

클립보드에 복사된 중요한 데이터의 노출 제한

클립보드에 복사된 중요한 데이터의 노출을 방지하기 위해 호스트에서는 복사/붙여넣기 작업이 기본적으로 사용되지 않도록 설정되어 있습니다.

VMware Tools를 실행하는 가상 시스템에서 복사/붙여넣기가 사용되도록 설정된 경우에는 게스트 운영 체제와 원격 콘솔 간에 복사/붙여넣기를 수행할 수 있습니다. 콘솔 창으로 포커스가 이동하면 가상 시스템에서 실행 중인 프로세스 및 권한 없는 사용자가 가상 시스템 콘솔의 클립보드에 액세스할 수 있습니다. 콘솔을 사용하기 전에 사용자가 클립보드에 중요한 정보를 복사한 경우에는 사용자도 모르게 중요한 데이터가 가상 시스템에 노출됩니다. 이 문제를 방지하기 위해 게스트 운영 체제에 대한 복사/붙여넣기 작업은 기본적으로 사용되지 않도록 설정되어 있습니다.

필요한 경우 가상 시스템에 대해 복사/붙여넣기 작업이 사용되도록 설정할 수 있습니다.

사용자가 가상 시스템 내에서 명령을 실행하지 못하도록 제한

기본적으로 vCenter Server 관리자 역할이 할당된 사용자는 가상 시스템의 게스트 운영 체제 내에서 파일 및 프로그램과 상호 작용할 수 있습니다. 게스트 기밀성, 가용성 또는 무결성이 침해될 위험을 줄이려면 **게스트 작업** 권한이 없는 게스트가 아닌 액세스 역할을 생성해야 합니다.

보안을 위해 물리적 데이터 센터와 마찬가지로 가상 데이터 센터에 대한 액세스도 제한적으로 허용하십시오. 사용자에게 전체 관리자 액세스 권한을 부여하지 않으려면 관리자 권한이 필요하지만 게스트 운영 체제 내의 파일 및 프로그램과 상호 작용할 권한이 없는 사용자에게 게스트 액세스를 사용하지 않도록 설정하는 사용자 지정 역할을 생성하여 해당 역할을 적용합니다.

예를 들어 구성에는 중요한 정보가 들어 있는 인프라의 가상 시스템이 포함될 수 있습니다. vMotion 및 Storage vMotion을 사용한 마이그레이션 등의 작업을 수행하려면 IT 역할이 가상 시스템에 액세스해야 합니다. 이 경우 게스트 OS 내에서 일부 원격 작업을 사용하지 않도록 설정하여 IT 역할이 중요한 정보에 액세스하지 못하게 합니다.

사전 요구 사항

역할을 생성하는 vCenter Server 시스템에서 **관리자** 권한이 있는지 확인합니다.

절차

- 1 역할을 생성할 vCenter Server 시스템에서 **관리자** 권한을 가진 사용자로 vSphere Web Client에 로그인합니다.
- 2 **관리**를 클릭하고 **역할**을 선택합니다.
- 3 **역할 생성 작업** 아이콘을 클릭하고 역할의 이름을 입력합니다.
예를 들어 **Administrator No Guest Access**를 입력합니다.
- 4 **모든 권한**을 선택합니다.
- 5 **모든 권한.가상 시스템.게스트 작업**을 선택 취소하여 게스트 작업 권한 집합을 제거합니다.
- 6 **확인**을 클릭합니다.

다음에 수행할 작업

vCenter Server 시스템 또는 호스트를 선택하고 새 권한이 있어야 하는 사용자 또는 그룹과 쌍이 되는 사용 권한을 새로 생성된 역할에 할당합니다. 기본 관리자 역할에서 해당 사용자를 제거합니다.

가상 시스템 사용자 또는 프로세스가 디바이스와 연결이 끊어지지 않도록 방지

가상 시스템 내에서 루트 또는 관리자 권한이 없는 사용자와 프로세스는 네트워크 어댑터와 CD-ROM 드라이브 등의 디바이스를 연결하거나 연결을 끊을 수 있고 디바이스 설정을 수정할 수 있습니다. 가상 시스템의 보안을 강화하려면 이러한 디바이스를 제거하십시오. 디바이스가 영구적으로 제거되는 것을 원하지 않는 경우 게스트 운영 체제 내에서 가상 시스템 사용자나 프로세스가 디바이스와 연결되거나 연결이 끊어지지 않도록 방지할 수 있습니다.

사전 요구 사항

가상 시스템을 끕니다.

절차

- 1 vSphere Web Client 인벤토리에서 가상 시스템을 찾습니다.
 - a 데이터 센터, 폴더, 클러스터, 리소스 풀 또는 호스트를 선택합니다.
 - b **관련 항목** 탭을 클릭하고 **가상 시스템**을 클릭합니다.
- 2 가상 시스템을 마우스 오른쪽 버튼으로 클릭한 후 **설정 편집**을 클릭합니다.
- 3 **VM 옵션**을 선택합니다.
- 4 **고급**을 클릭하고 **구성 편집**을 클릭합니다.
- 5 이름 및 값 열에서 다음 값을 확인하거나 **행 추가**를 클릭하여 추가합니다.

이름	값
isolation.device.connectable.disable	참
isolation.device.edit.disable	참

이 옵션은 게스트 운영 체제의 VMware Tools 제어판에서 지정된 설정을 모두 재정의합니다.

6 확인을 클릭하여 구성 매개 변수 대화상자를 닫고 **확인**을 다시 클릭합니다.

게스트 운영 체제 가변 메모리 제한 수정

구성 파일에 많은 양의 사용자 지정 정보가 저장되는 경우 게스트 운영 체제 가변 메모리 제한을 늘릴 수 있습니다.

사전 요구 사항

가상 시스템을 끕니다.

절차

- 1 vSphere Web Client 인벤토리에서 가상 시스템을 찾습니다.
 - a 데이터 센터, 폴더, 클러스터, 리소스 풀 또는 호스트를 선택합니다.
 - b **관련 항목** 탭을 클릭하고 **가상 시스템**을 클릭합니다.
- 2 가상 시스템을 마우스 오른쪽 버튼으로 클릭한 후 **설정 편집**을 클릭합니다.
- 3 **VM 옵션 > 고급**을 선택하고 **구성 편집**을 클릭합니다.
- 4 매개 변수 `tools.setInfo.sizeLimit`를 추가 또는 편집하고 값을 바이트 수로 설정합니다.
- 5 **확인**을 클릭합니다.

게스트 운영 체제 프로세스가 호스트에 구성 메시지를 보내지 않도록 방지

게스트가 이름-값 쌍을 구성 파일에 쓰지 못하도록 할 수 있습니다. 이것은 게스트 운영 체제가 구성 설정을 수정하지 못하도록 해야 하는 경우에 적합합니다.

사전 요구 사항

가상 시스템을 끕니다.

절차

- 1 vSphere Web Client 인벤토리에서 가상 시스템을 찾습니다.
 - a 데이터 센터, 폴더, 클러스터, 리소스 풀 또는 호스트를 선택합니다.
 - b **관련 항목** 탭을 클릭하고 **가상 시스템**을 클릭합니다.
- 2 가상 시스템을 마우스 오른쪽 버튼으로 클릭한 후 **설정 편집**을 클릭합니다.
- 3 **VM 옵션**을 선택합니다.
- 4 **고급**을 클릭하고 **구성 편집**을 클릭합니다.
- 5 **행 추가**를 클릭하고 이름 및 값 열에 다음 값을 입력합니다.
 - 이름 열: `isolation.tools.setinfo.disable`
 - [값] 열: 참

6 **확인**을 클릭하여 구성 매개 변수 대화상자를 닫고 **확인**을 다시 클릭합니다.

독립형 비영구 디스크 사용 방지

독립형 비영구 디스크를 사용하는 경우 성공적인 공격자는 시스템을 종료하거나 재부팅하여 시스템이 손상되었다는 모든 증거를 제거할 수 있습니다. 가상 시스템 활동에 대한 영구 기록이 없으면 관리자가 공격을 알지 못할 수 있습니다. 따라서 독립형 비영구 디스크를 사용하지 말아야 합니다.

절차

- ◆ 가상 시스템 활동이 Syslog 서버나 동일한 Windows 기반 이벤트 수집기와 같은 별도의 서버에서 원격으로 로깅되는지 확인합니다.

이벤트 및 활동의 원격 로깅이 게스트에 대해 구성되어 있지 않은 경우 scsiX:Y.mode가 다음 설정 중 하나여야 합니다.

- 존재하지 않음
- 독립형 비영구로 설정되지 않음

결과

비영구 모드가 사용되도록 설정되어 있지 않은 경우 시스템을 재부팅할 때 가상 시스템을 알려진 상태로 롤백할 수 없습니다.

vSphere 네트워킹 보호

8

환경을 보호하려면 vSphere 네트워킹을 반드시 보호해야 합니다. 다양한 방식으로 여러 vSphere 구성 요소를 보호할 수 있습니다. vSphere 환경의 네트워킹에 대한 자세한 내용은 "vSphere 네트워킹" 설명서를 참조하십시오.

본 장은 다음 항목을 포함합니다.

- vSphere 네트워크 보안 소개
- 방화벽으로 네트워크 보호
- 물리적 스위치 보호
- 보안 정책으로 표준 스위치 포트 보호
- vSphere 표준 스위치 보안
- vSphere Distributed Switch 및 분산 포트 그룹 보안
- VLAN으로 가상 시스템 보호
- 단일 ESXi 호스트에 네트워크 DMZ 생성
- 단일 ESXi 호스트 내에 여러 네트워크 생성
- 인터넷 프로토콜 보안
- 적절한 SNMP 구성 확인
- 필요한 경우에만 vSphere Network Appliance API의 가상 스위치 사용
- vSphere 네트워킹 보안 모범 사례

vSphere 네트워크 보안 소개

vSphere 환경의 네트워크 보안은 물리적 네트워크 환경을 보호하는 여러 가지 특성을 공유하지만 포함된 일부 특성은 가상 시스템에만 적용됩니다.

방화벽

일부 또는 전체 가상 시스템에서 호스트 기반 방화벽을 설치하고 구성하여 가상 네트워크에 방화벽 보호 기능을 추가합니다.

효율성을 위해 전용 가상 시스템 이더넷 네트워크 또는 가상 네트워크를 설정할 수 있습니다. 가상 시스템을 구성하는 경우, 가상 네트워크의 맨 앞에 있는 가상 시스템에 호스트 기반 방화벽을 설치합니다. 이 방화벽이 물리적 네트워크 어댑터와 가상 네트워크의 나머지 가상 시스템 사이에서 보호 완충 지대 역할을 하게 됩니다.

호스트 기반 방화벽은 성능을 저하시킬 수 있으므로 가상 네트워크 내의 다른 곳에 위치한 가상 시스템에 호스트 기반 방화벽을 설치하기 전에 먼저 보안 요구 사항과 성능 목표 간의 균형을 고려해야 합니다.

[방화벽으로 네트워크 보호](#) 항목을 참조하십시오.

세분화

세분화를 통해 호스트 내에서 서로 다른 네트워크 세그먼트에 서로 다른 가상 시스템 영역을 유지할 수 있습니다. 각 가상 시스템 영역을 고유한 네트워크 세그먼트로 분리하면 한 가상 시스템 영역에서 다른 가상 시스템 영역으로 데이터가 누출될 위험이 최소화됩니다. 세그먼트화는 다양한 위협을 방지합니다. 여기에는 공격자가 ARP(주소 분석 프로토콜) 테이블을 조작하여 MAC 및 IP 주소를 다시 매핑함으로써 호스트에서 들어오고 나가는 네트워크 트래픽에 액세스할 수 있는 ARP 스푸핑 위협이 포함됩니다. 공격자는 ARP 스푸핑을 사용하여 메시지 가로채기(MITM: man-in-the-middle) 공격을 일으키고 DoS(서비스 거부) 공격을 수행하며 대상 시스템을 강탈하고 가상 네트워크를 중단시킵니다.

세그먼트를 세심하게 계획하면 가상 시스템 영역 간의 패킷 전송을 최소화함으로써 공격 대상에 네트워크 트래픽을 보내야 하는 스니핑 공격을 방지할 수 있습니다. 또한 공격자가 한 가상 시스템 영역의 비보안 서비스를 사용하여 호스트 내의 다른 가상 시스템 영역에 액세스할 수 없게 됩니다. 세분화는 두 가지 방식 중 하나로 구현할 수 있으며 각 방식에는 고유한 이점이 있습니다.

- 가상 시스템 영역에 대해 별도의 물리적 네트워크 어댑터를 사용하여 영역이 분리되도록 합니다. 대개 가상 시스템 영역에 대해 별도의 물리적 네트워크 어댑터를 유지하는 것이 가장 안전한 방법이며 초기 세그먼트 생성 후의 구성 오류를 줄일 수 있는 방법입니다.
- VLAN(Virtual Local Area Network)을 설정하여 네트워크를 보호할 수 있습니다. VLAN은 물리적으로 분리된 네트워크를 구현하여 얻을 수 있는 거의 모든 보안 이점을 하드웨어 오버헤드 없이 제공하므로 추가 디바이스의 배포 및 유지와 케이블 작업 등에 필요한 비용을 절감할 수 있는 실용적인 솔루션입니다. [VLAN으로 가상 시스템 보호](#) 항목을 참조하십시오.

무단 액세스 방지

가상 시스템 네트워크가 물리적 네트워크에 연결되어 있는 경우 물리적 시스템으로 구성된 네트워크와 동일한 침입 위험에 노출될 수 있습니다. 가상 시스템 네트워크가 물리적 네트워크에서 분리된 경우에도 네트워크에 속한 가상 시스템이 네트워크의 다른 가상 시스템으로부터 공격을 받을 수 있습니다. 가상 시스템을 보호하기 위한 요구 사항은 물리적 시스템을 보호하기 위한 요구 사항과 동일한 경우가 많습니다.

가상 시스템은 서로 분리되어 있습니다. 가상 시스템은 다른 가상 시스템에 있는 메모리를 읽거나 쓸 수 없고 데이터에 액세스할 수 없으며 애플리케이션을 사용할 수 없습니다. 하지만 네트워크 내에서는 모든 가상 시스템이나 가상 시스템 그룹이 다른 가상 시스템을 통한 무단 액세스의 대상이 될 수 있으므로 외부적인 수단을 통한 추가적인 보호가 필요할 수 있습니다.

방화벽으로 네트워크 보호

보안 관리자는 방화벽을 사용하여 네트워크나 네트워크의 선택적 구성 요소를 침입으로부터 보호합니다.

방화벽은 관리자가 명시적이거나 묵시적으로 승인한 포트를 제외한 모든 포트를 차단하여 방화벽 경계 안에 포함된 디바이스에 대한 액세스를 제어합니다. 관리자가 연 포트를 통해 방화벽 외부에 있는 디바이스와의 트래픽이 허용됩니다.

중요 ESXi 5.5 이상의 ESXi 방화벽에서는 vMotion 트래픽의 네트워크별 필터링을 허용하지 않습니다. 따라서 외부 방화벽에 규칙을 설치하여 vMotion 소켓으로 들어오는 연결이 없도록 해야 합니다.

가상 시스템 환경에서 다음과 같은 구성 요소 사이에 방화벽을 배치하도록 계획할 수 있습니다.

- vCenter Server 시스템, ESXi 호스트 등의 물리적 시스템 사이에 방화벽 배치
- 가상 시스템 사이에 방화벽 배치(예: 외부 웹 서버 역할을 하는 가상 시스템과 회사의 내부 네트워크에 연결된 가상 시스템 사이)
- 물리적 시스템과 가상 시스템 사이에 방화벽 배치(예: 물리적 네트워크 어댑터 카드와 가상 시스템 사이에 방화벽을 배치하는 경우)

ESXi 구성에서 방화벽을 사용하는 방법은 네트워크 사용 계획과 지정된 구성 요소의 필요한 보안 수준에 따라 달라집니다. 예를 들어 한 부서의 여러 벤치마크 테스트 집합 각각을 별도의 전용 가상 시스템에서 실행하는 가상 네트워크를 생성하면 한 가상 시스템에서 다른 가상 시스템으로의 무단 액세스 위험을 최소화할 수 있습니다. 이 경우 가상 시스템 사이에 방화벽을 두는 구성이 필요하지 않습니다. 대신 호스트 외부에서 테스트 실행을 중단하지 못하도록 가상 네트워크의 진입점에서 방화벽을 구성하여 전체 가상 시스템 집합을 보호할 수 있습니다.

방화벽 포트의 다이어그램은 VMware 기술 자료 문서 [2131180](#)을 참조하십시오.

vCenter Server 구성을 위한 방화벽

vCenter Server를 통해 ESXi 호스트에 액세스하는 경우에는 일반적으로 방화벽을 사용하여 vCenter Server를 보호합니다. 이 방화벽은 네트워크에 대한 기본적인 보호 기능을 제공합니다.

방화벽은 클라이언트와 vCenter Server 사이에 있을 수 있습니다. 또는 배포에 따라 vCenter Server와 클라이언트가 모두 방화벽 뒤에 있을 수도 있습니다. 중요한 점은 방화벽이 시스템의 진입점이 되는 위치에 있어야 한다는 것입니다.

vSphere vMotion™ 및 vSphere Fault Tolerance-용을 비롯한 전체 TCP 및 UDP 포트 목록은 [vCenter Server TCP 및 UDP 포트](#)를 참조하십시오.

vCenter Server로 구성된 네트워크는 vSphere Web Client를 통하거나 SDK를 사용하여 호스트와 상호 작용하는 타사 네트워크 관리 클라이언트를 통해 통신을 받을 수 있습니다. 정상적인 작업 중 vCenter Server는 지정된 포트에서 관리 호스트 및 클라이언트의 데이터를 수신합니다. 또한 vCenter Server는 관리 호스트가 지정된 포트에서 vCenter Server의 데이터를 수신한다고 가정합니다. 방화벽이 이러한 요소 사이에 있으면 방화벽에 데이터 전송을 지원하기 위해 열려 있는 포트가 있는지 확인해야 합니다.

계획한 네트워크 사용 방법과 다양한 디바이스에 필요한 보안 수준에 따라 네트워크의 다른 여러 액세스 지점에도 방화벽을 포함할 수 있습니다. 네트워크 구성에서 식별한 보안 위협을 기반으로 방화벽의 위치를 선택해야 합니다. ESXi 구현 시 일반적인 방화벽 위치는 다음과 같습니다.

- vSphere Web Client 또는 타사 네트워크 관리 클라이언트와 vCenter Server 사이
- 사용자가 웹 브라우저를 통해 가상 시스템에 액세스하는 경우, 웹 브라우저와 ESXi 호스트 사이
- 사용자가 vSphere Web Client를 통해 가상 시스템에 액세스하는 경우, vSphere Web Client와 ESXi 호스트 사이. 이 연결은 vSphere Web Client와 vCenter Server 간의 연결 외에 추가적인 연결로, 여기에는 다른 포트가 필요합니다.
- vCenter Server와 ESXi 호스트 사이
- 네트워크의 ESXi 호스트 사이. 호스트 간 트래픽은 일반적으로 신뢰할 수 있는 것으로 간주되지만 시스템 간 보안 침해가 우려되는 경우에는 호스트 사이에 방화벽을 추가할 수 있습니다.

ESXi 호스트 사이에 방화벽을 추가한 경우 서버 간에 가상 시스템을 마이그레이션하거나 복제를 수행하거나 vMotion을 사용하려면 소스와 대상이 통신할 수 있도록 소스 호스트를 대상 호스트에서 분리하는 방화벽에도 포트를 열어야 합니다.

- ESXi 호스트와 NFS 또는 iSCSI 스토리지 등의 네트워크 스토리지 사이. 이러한 포트는 VMware와 관련이 없으며 네트워크의 규격에 따라 이러한 포트를 구성합니다.

방화벽을 통해 vCenter Server에 연결

vCenter Server는 TCP 포트 443을 사용하여 클라이언트의 데이터 전송을 수신합니다. vCenter Server와 클라이언트 사이에 방화벽이 있는 경우 vCenter Server가 클라이언트로부터 데이터를 수신할 수 있는 연결을 구성해야 합니다.

방화벽에서 TCP 포트 443을 열어 vCenter Server가 vSphere Web Client에서 데이터를 받을 수 있도록 합니다. 방화벽 구성은 사이트에서 사용하는 방화벽에 따라 다르므로 자세한 내용은 로컬 방화벽 시스템 관리자에게 문의하십시오.

포트 443을 vSphere Web Client 대 vCenter Server 통신용 포트로는 사용하지 않으려면 vSphere Web Client에서 vCenter Server 설정을 변경하여 다른 포트에 전환할 수 있습니다. "vCenter Server 및 호스트 관리" 설명서를 참조하십시오.

아직 vSphere Client를 사용 중인 경우 "vSphere Client에서 vSphere 관리 설명서"를 참조하십시오.

vCenter Server가 없는 구성을 위한 방화벽

vCenter Server를 사용하는 대신 ESXi 네트워크에 클라이언트를 직접 연결할 수 있습니다.

vCenter Server 없이 구성된 네트워크는 vSphere Client, vSphere 명령줄 인터페이스 중 하나, vSphere Web Services SDK 또는 타사 클라이언트를 통해 통신을 받습니다. 대부분의 경우 vCenter Server가 있을 때와 동일하게 방화벽이 필요하지만 몇 가지 주요 차이점이 있습니다.

- vCenter Server가 포함된 구성과 마찬가지로, ESXi 계층(일부 구성에서는 클라이언트와 ESXi 계층)을 보호하기 위해 방화벽이 있어야 합니다. 이 방화벽은 네트워크에 대한 기본적인 보호 기능을 제공합니다.
- 이 구성 유형에서 라이선싱은 각 호스트에 설치하는 ESXi 패키지의 일부입니다. 라이선싱이 서버에 있으므로 별도의 라이선스 서버는 필요하지 않습니다. 따라서 라이선스 서버와 ESXi 네트워크 사이의 방화벽이 필요하지 않습니다.

ESXCLI, vSphere Client 또는 방화벽 규칙을 사용하여 방화벽 포트를 구성할 수 있습니다. [ESXi 방화벽 구성](#)를 참조하십시오.

방화벽을 통해 ESXi 호스트 연결

두 ESXi 호스트 사이에 방화벽이 있는 경우 호스트 간의 트랜잭션을 허용하거나 vCenter Server를 사용하여 vSphere HA(vSphere High Availability) 트래픽, 마이그레이션, 복제, vMotion 등의 소스 또는 대상 작업을 수행하려면 관리되는 호스트에서 데이터를 수신하는 데 사용할 수 있는 연결을 구성해야 합니다.

데이터를 수신하기 위한 연결을 구성하려면 vSphere High Availability, vMotion 및 vSphere Fault Tolerance와 같은 서비스에서 들어오는 트래픽을 위한 포트를 엽니다. 구성 파일, vSphere Web Client 액세스 및 방화벽 명령에 대한 자세한 내용은 [ESXi 방화벽 구성](#) 항목을 참조하십시오. 포트 목록은 [ESXi 호스트에 대해 들어오고 나가는 방화벽 포트](#) 항목을 참조하십시오. 포트 구성에 대한 자세한 내용은 방화벽 시스템 관리자에게 문의하십시오.

방화벽을 통해 가상 시스템 콘솔에 연결

사용자와 관리자가 가상 시스템 콘솔과 통신하기 위해서는 특정 포트가 열려 있어야 합니다. 어떤 포트가 열려 있어야 하는지는 가상 시스템 콘솔의 유형 및 vSphere Web Client를 사용하여 vCenter Server를 통해 연결하는지 아니면 vSphere Client에서 ESXi 호스트에 직접 연결하는지에 따라 다릅니다.

vSphere Web Client를 통해 브라우저 기반의 가상 시스템 콘솔에 연결

vSphere Web Client를 사용하여 연결하는 경우에는 ESXi 호스트를 관리하는 vCenter Server 시스템에 항상 연결한 후 여기에서 가상 시스템 콘솔에 액세스합니다.

vSphere Web Client를 사용하여 브라우저 기반 가상 시스템 콘솔에 연결하는 경우에는 다음과 같은 액세스가 가능해야 합니다.

- 방화벽이 포트 9443에서 vSphere Web Client의 vCenter Server 액세스를 허용해야 합니다.
- 방화벽이 포트 902에서 vCenter Server의 ESXi 호스트 액세스를 허용해야 합니다.

vSphere Web Client를 통해 독립 실행형 가상 시스템 콘솔에 연결

vSphere Web Client를 사용하여 독립 실행형 가상 시스템 콘솔에 연결하는 경우에는 다음과 같은 액세스가 가능해야 합니다.

- 방화벽이 포트 9443에서 vSphere Web Client의 vCenter Server 액세스를 허용해야 합니다.
- 방화벽이 포트 9443에서 독립 실행형 가상 시스템 콘솔의 vCenter Server 액세스를 허용하고 포트 902에서 독립 실행형 가상 시스템 콘솔의 ESXi 호스트에 대한 액세스를 허용해야 합니다.

vSphere Client를 사용하여 ESXi 호스트에 직접 연결

ESXi 호스트에 직접 연결하면 vSphere Client 가상 시스템 콘솔을 사용할 수 있습니다.

참고 vCenter Server 시스템에 의해 관리되는 호스트에 직접 연결할 때는 vSphere Client를 사용하지 마십시오. vSphere Client에서 해당 호스트를 변경하는 경우 환경이 불안정해질 수 있습니다.

방화벽은 포트 443과 902에서 ESXi 호스트에 대한 액세스를 허용해야 합니다.

vSphere Client는 포트 902를 사용하여 가상 시스템의 게스트 운영 체제 MKS 작업에 대한 연결을 제공합니다. 사용자가 이 포트를 통해 가상 시스템의 게스트 운영 체제 및 애플리케이션과 상호 작용할 수 있습니다. VMware는 다른 포트를 이 기능에 구성하는 것을 지원하지 않습니다.

물리적 스위치 보호

각 ESXi 호스트의 물리적 스위치를 보호하여 공격자가 호스트 및 해당 가상 시스템에 액세스하지 못하게 방지할 수 있습니다.

호스트를 최대한 보호하려면 스페닝 트리를 사용하지 않도록 설정한 상태에서 물리적 스위치 포트를 구성하고 외부 물리적 스위치와 VST(Virtual Switch Tagging) 모드의 가상 스위치 간 트렁크 링크에 대해 비협상 옵션을 구성해야 합니다.

절차

- 1 물리적 스위치에 로그인한 후 스페닝 트리 프로토콜이 사용하지 않도록 설정되어 있거나 ESXi 호스트에 연결된 모든 물리적 스위치 포트에 대해 PortFast가 구성되어 있는지 확인합니다.
- 2 브리징 또는 라우팅을 수행하는 가상 시스템에서 첫 번째 업스트림 물리적 스위치 포트가 BPDU 가드 및 PortFast를 사용하지 않고 스페닝 트리 프로토콜을 사용하도록 구성되어 있는지 주기적으로 확인합니다.

vSphere 5.1 이상에서 물리적 스위치를 잠재적 DoS(서비스 거부) 공격으로부터 보호하려면 ESXi 호스트에서 게스트 BPDU 필터를 설정할 수 있습니다.
- 3 물리적 스위치에 로그인한 후 ESXi 호스트에 연결된 물리적 스위치 포트에서 DTP(Dynamic Trunking Protocol)가 사용하지 않도록 설정되어 있는지 확인합니다.
- 4 물리적 스위치 포트를 정기적으로 검사하여 가상 스위치 VLAN 트렁킹 포트에 연결되어 있는 경우 트렁크 포트가 올바르게 구성되어 있는지 확인합니다.

보안 정책으로 표준 스위치 포트 보호

물리적 네트워크 어댑터와 마찬가지로 가상 시스템 네트워크 어댑터는 다른 시스템에서 온 것으로 보이는 프레임을 보내거나 다른 시스템으로 가장하여 해당 시스템으로 보내려 하는 네트워크 프레임을 받을 수 있습니다. 또한 물리적 네트워크 어댑터와 마찬가지로 다른 시스템을 대상으로 하는 프레임을 받도록 가상 시스템 네트워크 어댑터를 구성할 수 있습니다. 두 시나리오에는 모두 보안 위험이 있습니다.

네트워크의 표준 스위치를 생성할 때 vSphere Web Client에서 포트 그룹을 추가하여 스위치에 연결된 시스템 트래픽에 VMkernel 어댑터와 가상 시스템에 대한 정책을 적용합니다.

VMkernel 포트 그룹 또는 가상 시스템 포트 그룹을 표준 스위치에 추가하는 과정에서 ESXi는 포트에 대한 보안 정책을 그룹으로 구성합니다. 이 보안 정책을 사용하여 호스트에 있는 가상 시스템의 게스트 운영 체제가 네트워크의 다른 시스템으로 가장하지 못하게 방지할 수 있습니다. 이 보안 기능은 가장을 초래한 게스트 운영 체제가 가장이 금지된 것을 감지하지 못하도록 구현됩니다.

보안 정책은 가상 시스템의 가장 및 가로채기 공격에 대한 보호 적용 강도를 결정합니다. 보안 프로파일의 설정을 올바르게 사용하려면 가상 시스템 네트워크 어댑터가 전송을 제어하는 방식과 이 수준에서 공격이 이루어지는 방식을 이해해야 합니다. 자세한 내용은 "vSphere 네트워킹" 설명서의 보안 정책 섹션을 참조하십시오.

vSphere 표준 스위치 보안

스위치의 보안 설정을 사용하여 일부 MAC 주소 모드를 제한하여 표준 스위치 트래픽을 계층 2 공격으로부터 보호할 수 있습니다.

각 가상 시스템 네트워크 어댑터에는 초기 MAC 주소와 유효 MAC 주소가 있습니다.

초기 MAC 주소

초기 MAC 주소는 어댑터를 생성할 때 할당됩니다. 초기 MAC 주소는 게스트 운영 체제 외부에서 다시 구성할 수 있지만 게스트 운영 체제가 변경할 수는 없습니다.

유효 MAC 주소

각 어댑터에는 유효 MAC 주소가 있으며, 대상 MAC 주소가 이 유효 MAC 주소와 일치하지 않는 들어오는 네트워크 트래픽은 필터링됩니다. 유효 MAC 주소를 설정하는 것은 게스트 운영 체제가 책임지며 대개 유효 MAC 주소는 초기 MAC 주소와 일치합니다.

가상 시스템 네트워크 어댑터를 생성할 때 유효 MAC 주소와 초기 MAC 주소는 동일합니다. 게스트 운영 체제에서 언제든지 유효 MAC 주소를 다른 값으로 변경할 수 있습니다. 운영 체제가 유효 MAC 주소를 변경할 경우 네트워크 어댑터는 새 MAC 주소로 향하는 네트워크 트래픽을 수신합니다.

네트워크 어댑터를 통해 패킷을 보낼 때 게스트 운영 체제는 일반적으로 자체 어댑터의 유효 MAC 주소를 이더넷 프레임의 소스 MAC 주소 필드에 삽입합니다. 또한 대상 MAC 주소 필드에 수신 네트워크 어댑터의 MAC 주소를 삽입합니다. 수신 어댑터는 패킷의 대상 MAC 주소가 자체 유효 MAC 주소와 일치하는 경우에만 패킷을 수락합니다.

운영 체제는 가장된 소스 MAC 주소를 사용하여 프레임을 보낼 수 있습니다. 이것은 운영 체제가 수신 네트워크에 의해 인증된 네트워크 어댑터를 가장하여 네트워크의 디바이스에 악의적인 공격을 피할 수 있다는 의미입니다.

포트 그룹 또는 포트에 보안 정책을 구성하여 가상 트래픽을 가장 및 가로채기 계층 2 공격으로부터 보호합니다.

분산 포트 그룹 및 포트의 보안 정책에는 다음 옵션이 포함됩니다.

- 비규칙 모드(비규칙(Promiscuous) 모드 작업 참조)
- MAC 주소 변경(MAC 주소 변경 사항 참조)
- 위조 전송(위조 전송 참조)

vSphere Web Client에서 호스트와 연결된 가상 스위치를 선택하여 기본 설정을 보고 변경할 수 있습니다. "vSphere 네트워킹" 설명서를 참조하십시오.

MAC 주소 변경 사항

가상 스위치의 보안 정책에는 **MAC 주소 변경** 옵션이 포함됩니다. 이 옵션은 가상 시스템이 수신하는 트래픽에 적용됩니다.

MAC 주소 변경 옵션이 **수락**으로 설정되면 ESXi는 유효 MAC 주소를 초기 MAC 주소가 아닌 다른 주소로 변경하려는 요청을 수락합니다.

MAC 주소 변경 옵션이 **거부**로 설정되면 ESXi는 유효 MAC 주소를 초기 MAC 주소가 아닌 다른 주소로 변경하려는 요청을 수락하지 않습니다. 이 설정을 통해 MAC 가장으로부터 호스트가 보호됩니다. 유효 MAC 주소가 초기 MAC 주소와 일치할 때까지는 가상 시스템 어댑터가 요청을 보내는 데 사용한 포트가 사용되지 않도록 설정되고 가상 시스템 어댑터가 더 이상 프레임을 받지 않습니다. 게스트 운영 체제는 MAC 주소 변경 요청이 수락되지 않은 것을 감지하지 못합니다.

참고 iSCSI 이니시에이터에는 특정 유형의 스토리지에서 MAC 주소 변경을 가져오는 기능이 필요합니다. iSCSI 스토리지가 포함된 ESXi iSCSI를 사용하는 경우 **MAC 주소 변경** 옵션을 **수락**으로 설정하십시오.

상황에 따라 둘 이상의 어댑터가 네트워크에서 동일한 MAC 주소를 가지도록 해야 할 경우가 있습니다. 유니캐스트 모드에서 Microsoft 네트워크 로드 밸런싱을 사용하는 경우를 예로 들 수 있습니다. Microsoft 네트워크 로드 밸런싱이 표준 유니캐스트 모드에서 사용되면 어댑터 간에 MAC 주소를 공유하지 않습니다.

위조 전송

위조 전송 옵션은 가상 시스템으로부터 전송되는 트래픽에 영향을 미칩니다.

위조 전송 옵션을 **동의**로 설정하면 ESXi가 소스 MAC 주소와 유효 MAC 주소를 비교하지 않습니다.

MAC 가장으로부터 보호하려면 **위조 전송** 옵션을 **거부**로 설정하면 됩니다. 이렇게 하면 호스트가 게스트 운영 체제에서 전송되는 소스 MAC 주소를 해당 가상 시스템 어댑터의 유효 MAC 주소와 비교하여 두 주소가 일치하는지 확인합니다. 주소가 일치하지 않으면 ESXi 호스트는 패킷을 삭제합니다.

게스트 운영 체제는 해당 가상 시스템 어댑터가 가장된 MAC 주소를 사용하여 패킷을 전송할 수 없음을 감지하지 못합니다. 주소가 가장된 모든 패킷이 배달되기 전에 ESXi 호스트가 이를 가로채며 게스트 운영 체제는 패킷이 버려진 것으로 가정할 수 있습니다.

비규칙(Promiscuous) 모드 작업

비규칙 모드는 게스트 운영 체제가 회선에서 발견한 모든 트래픽을 받을 수 있도록 가상 시스템 어댑터가 수행하는 모든 수신 필터링을 제거합니다. 기본적으로 가상 시스템 어댑터는 비규칙 모드로 작동할 수 없습니다.

비규칙 모드는 네트워크 작업을 추적하는 데 유용할 수 있지만 안전하지 않은 작업 모드입니다. 비규칙 모드인 어댑터는 특정 네트워크 어댑터에서만 수신하는 일부 패킷에 대해서도 액세스할 수 있기 때문입니다. 이것은 가상 시스템 내의 관리자 또는 루트 사용자가 다른 게스트 또는 호스트 운영 체제로 전송될 트래픽을 잠재적으로 볼 수 있음을 의미합니다.

참고 상황에 따라 비규칙 모드로 작동하는 표준 또는 분산 가상 스위치를 구성해야 하는 경우가 있습니다. 예를 들어 네트워크 침입 감지 소프트웨어 또는 패킷 스니퍼를 실행하는 경우가 이에 해당합니다.

vSphere Distributed Switch 및 분산 포트 그룹 보안

관리자는 여러 가지 옵션을 통해 vSphere 환경에서 vSphere Distributed Switch를 보호할 수 있습니다.

절차

- 1 정적 바인딩을 사용하는 분산 포트 그룹의 경우 자동 확장 기능이 사용하지 않도록 설정되었는지 확인합니다.

자동 확장은 vSphere 5.1 이상에서 기본적으로 사용하도록 설정되어 있습니다.

자동 확장을 사용하지 않도록 설정하려면 vSphere Web Services SDK 또는 명령줄 인터페이스를 사용하여 분산 포트 그룹 아래의 `autoExpand` 속성을 구성합니다. "vSphere Web Services SDK" 설명서를 참조하십시오.

- 2 vSphere Distributed Switch의 모든 전용 VLAN ID가 완전히 문서화되었는지 확인합니다.
- 3 dvPortgroup에서 VLAN 태그 지정을 사용하는 경우 VLAN ID가 외부 VLAN 인식 업스트림 스위치의 ID와 일치해야 합니다. VLAN ID가 완전하게 추적되지 않는 경우 잘못된 ID 재사용이 부적절한 물리적 시스템과 가상 시스템 간의 트래픽을 허용할 수 있습니다. 마찬가지로 VLAN ID가 잘못되었거나 누락된 경우 물리적 시스템과 가상 시스템 간에 트래픽이 통과하지 않을 수 있습니다.
- 4 vSphere Distributed Switch와 연결된 가상 포트 그룹에 사용되지 않는 포트가 없는지 확인합니다.
- 5 모든 vSphere Distributed Switch의 레이블을 지정합니다.

ESXi 호스트와 연결된 vSphere Distributed Switch는 스위치 이름을 위한 필드가 필요합니다. 이 레이블은 물리적 스위치에 연결된 호스트 이름과 마찬가지로 스위치의 기능 설명자 역할을 합니다.

vSphere Distributed Switch의 레이블은 스위치의 기능 또는 IP 서브넷을 나타냅니다. 예를 들어 스위치의 레이블을 내부로 지정하면 스위치가 물리적 네트워크 어댑터가 바인딩되지 않은 가상 시스템의 전용 가상 스위치 간 내부 네트워킹만을 위한 것이라는 것을 나타낼 수 있습니다.

- 6 현재 사용하지 않는 경우 vSphere Distributed Switch의 네트워크 상태 검사를 사용하지 않도록 설정합니다.

네트워크 상태 검사는 기본적으로 사용하지 않도록 설정되어 있습니다. 사용하도록 설정되면 상태 검사 패킷에 공격자가 잠재적으로 사용할 수 있는 호스트, 스위치 및 포트에 대한 정보가 포함됩니다. 문제 해결을 위해서만 네트워크 상태 검사를 사용하고 문제 해결이 완료되면 끄십시오.

- 7 포트 그룹 또는 포트에 보안 정책을 구성하여 가상 트래픽을 가장 및 가로채기 계층 2 공격으로부터 보호합니다.

분산 포트 그룹 및 포트의 보안 정책에는 다음 옵션이 포함됩니다.

- 비규칙 모드(비규칙(Promiscuous) 모드 작업 참조)
- MAC 주소 변경(MAC 주소 변경 사항 참조)
- 위조 전송(위조 전송 참조)

분산 스위치의 마우스 오른쪽 버튼 메뉴에서 **분산 포트 그룹 관리**를 선택하고 마법사에서 **보안**을 선택하여 현재 설정을 보고 변경할 수 있습니다. "vSphere 네트워킹" 설명서를 참조하십시오.

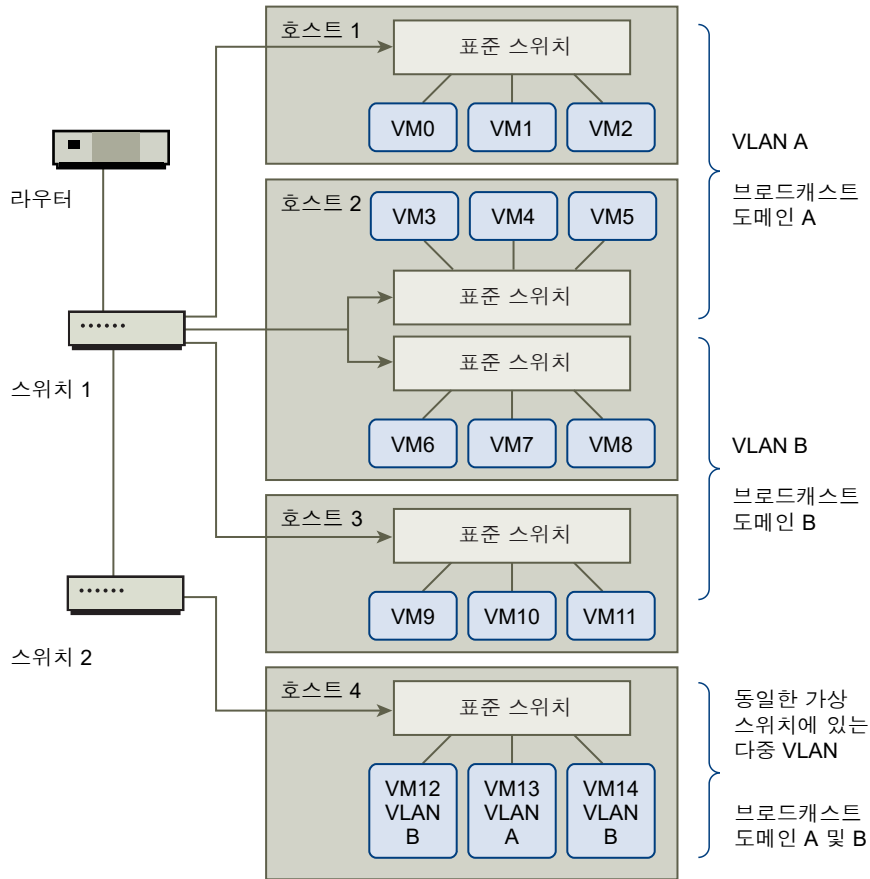
VLAN으로 가상 시스템 보호

네트워크는 시스템에서 가장 취약한 부분 중 하나일 수 있습니다. 가상 시스템 네트워크도 물리적 네트워크만큼 강력한 보호가 필요합니다. VLAN을 사용하면 해당 환경의 네트워크 보안 성능을 개선할 수 있습니다.

VLAN은 IEEE 표준 네트워킹 체계의 일종으로, VLAN에 속하는 포트로의 패킷 라우팅만 허용하는 특수한 태깅 방법을 포함하고 있습니다. 적절히 구성된 VLAN은 실수나 악의에 의한 침입으로부터 가상 시스템 집합을 보호할 수 있는 신뢰할 수 있는 수단을 제공합니다.

VLAN을 사용하면 물리적 네트워크를 세그먼트로 나눠 네트워크 내의 두 시스템이 동일한 VLAN에 속하지 않는 한 서로 패킷을 전송하지 못하게 만들 수 있습니다. 예를 들어 회계 레코드와 트랜잭션은 기업의 가장 민감한 내부 정보에 속합니다. 영업, 배송 및 회계 부서의 모든 직원이 동일한 물리적 네트워크 내의 가상 시스템을 사용하는 회사에서 VLAN을 설정하여 회계 부서의 가상 시스템을 보호할 수 있습니다.

그림 8-1. 샘플 VLAN 레이아웃



이 구성에서는 회계 부서의 모든 직원은 **VLAN A**의 가상 시스템을 사용하고 영업 부서의 직원은 **VLAN B**의 가상 시스템을 사용합니다.

라우터는 회계 데이터가 포함된 패킷을 스위치로 전달합니다. 이러한 패킷에는 **VLAN A**로만 배포하도록 제한하는 태그가 붙습니다. 따라서 회계 데이터는 브로드캐스트 도메인 **A**로 제한되고 라우터 구성을 따로 변경하지 않는 한 브로드캐스트 도메인 **B**로 라우팅될 수 없습니다.

이 **VLAN** 구성에서는 영업 부서의 사용자가 회계 부서로 향하는 패킷을 가로챌 수 없습니다. 또한 회계 부서에서 영업 그룹용으로 지정된 패킷을 받지 못하도록 방지합니다. 단일 가상 스위치에 의해 서비스를 제공하는 가상 시스템들이 서로 다른 **VLAN**에 속할 수 있습니다.

VLAN에 대한 보안 고려 사항

VLAN을 설정하여 네트워크의 각 부분을 보호하는 방식은 게스트 운영 체제, 네트워크 장비가 구성된 방식 등과 같은 요소에 따라 달라집니다.

ESXi는 완벽한 **IEEE 802.1q** 호환 **VLAN**을 구현합니다. **VLAN** 설정 방법에 대한 구체적인 권장 사항을 제공할 수는 없지만 보안 시행 정책의 일부로 **VLAN** 배포를 사용할 경우 고려해야 할 여러 가지 요소가 있습니다.

VLAN 보호

관리자는 vSphere 환경에서 여러 가지 옵션으로 VLAN을 보호할 수 있습니다.

절차

- 1 포트 그룹이 업스트림 물리적 스위치에 예약된 VLAN 값으로 구성되어 있지 않은지 확인합니다.
VLAN ID를 물리적 스위치에 예약된 값으로 설정하지 마십시오.
- 2 VGT(Virtual Guest Tagging)에 사용하는 경우를 제외하고 포트 그룹이 VLAN 4095로 구성되어 있지 않은지 확인합니다.

vSphere에는 세 가지 VLAN 태깅 유형이 있습니다.

- EST(External Switch Tagging)
- VST(Virtual Switch Tagging) - 가상 스위치는 연결된 가상 시스템에 들어오는 트래픽에 대해 구성된 VLAN ID로 태그를 지정하고, 가상 시스템에서 나가는 트래픽에서 VLAN 태그를 제거합니다. VST 모드를 설정하려면 VLAN ID를 1에서 4095 사이의 값으로 할당해야 합니다.
- VGT(Virtual Guest Tagging) - 가상 시스템이 VLAN 트래픽을 처리합니다. VGT 모드를 활성화하려면 VLAN ID를 4095로 설정합니다. Distributed Switch에서 **VLAN 트렁킹** 옵션을 사용하여 해당 VLAN을 기준으로 가상 시스템 트래픽을 허용할 수도 있습니다.

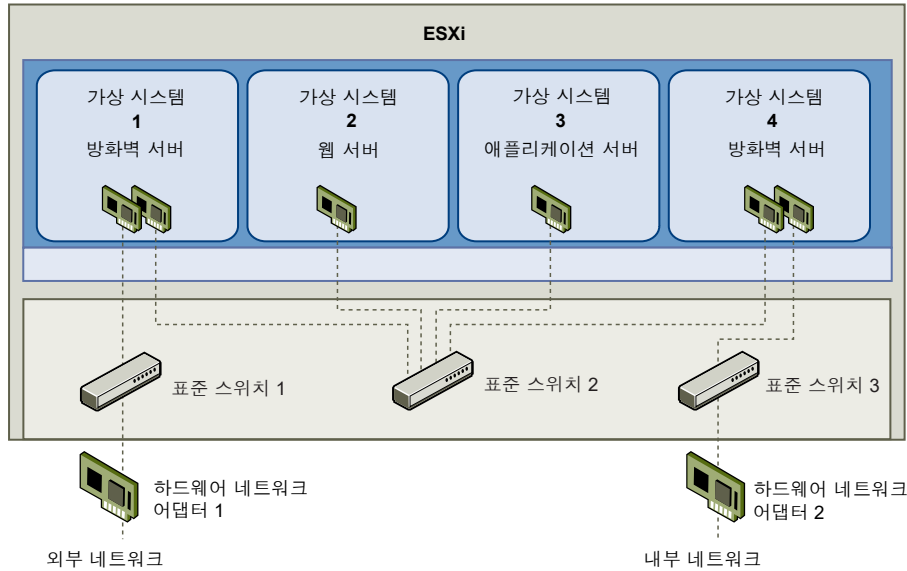
VLAN 네트워킹 모드는 표준 스위치의 경우 스위치 또는 포트 그룹 수준에서 구성할 수 있고, Distributed Switch의 경우 분산 포트 그룹 또는 포트 수준에서 구성할 수 있습니다.

- 3 각 가상 스위치의 모든 VLAN이 완전히 문서화되었는지 확인하고 각 가상 스위치에 필수 VLAN만 모두 있는지 확인합니다.

단일 ESXi 호스트에 네트워크 DMZ 생성

ESXi 분리 및 가상 네트워킹 기능을 사용하여 안전한 환경을 구성하는 방법의 한 가지 예로 단일 호스트에 네트워크 DMZ(완충 지역)를 생성하는 방법이 있습니다.

그림 8-2. DMZ가 단일 ESXi 호스트에 구성됨



이 예에서는 가상 시스템 네 개를 구성하여 표준 스위치 2에 가상 DMZ를 생성합니다.

- 가상 시스템 1과 가상 시스템 4는 방화벽을 실행하고 표준 스위치를 통해 물리적 네트워크 어댑터에 연결됩니다. 두 가상 시스템 모두 여러 스위치를 사용하고 있습니다.
- 가상 시스템 2는 웹 서버를 실행하고 가상 시스템 3은 애플리케이션 서버로 실행됩니다. 두 가상 시스템 모두 1개의 가상 스위치에 연결되어 있습니다.

웹 서버와 애플리케이션 서버는 두 방화벽 사이의 DMZ를 차지하며 이 두 요소 사이의 통로는 방화벽을 서버와 연결하는 표준 스위치 2입니다. 이 스위치는 DMZ 외부의 어떤 요소와도 직접 연결되지 않으며, 두 방화벽에 의해 외부 트래픽으로부터 분리됩니다.

작동 측면에서 보면 인터넷으로부터의 외부 트래픽은 하드웨어 네트워크 어댑터 1(표준 스위치 1에서 라우팅됨)을 통해 가상 시스템 1에 수신되며, 이 시스템에 설치된 방화벽을 통해 검증됩니다. 방화벽이 트래픽을 인증하면 트래픽은 DMZ의 표준 스위치인 표준 스위치 2로 라우팅됩니다. 웹 서버와 애플리케이션 서버도 이 스위치에 연결되어 있기 때문에 이 두 서버에서 외부 요청을 처리할 수 있습니다.

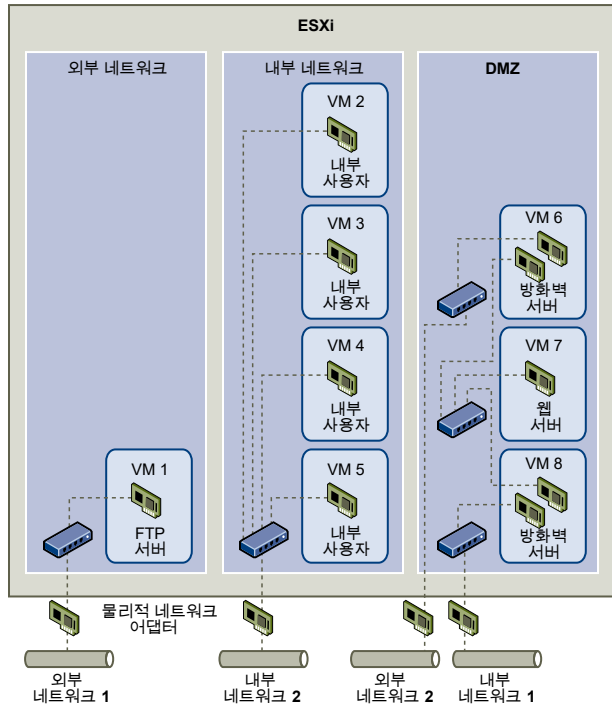
표준 스위치 2는 가상 시스템 4와도 연결되어 있으며, 이 가상 시스템은 DMZ와 내부 회사 네트워크 사이에 방화벽을 제공합니다. 이 방화벽은 웹 서버와 애플리케이션 서버에서 전송한 패킷을 필터링합니다. 패킷이 검증되면 해당 패킷은 표준 스위치 3을 통해 하드웨어 네트워크 어댑터 2로 라우팅되며 하드웨어 네트워크 어댑터 2는 내부 회사 네트워크에 연결됩니다.

단일 호스트에 DMZ를 생성하는 경우에는 경량 방화벽을 사용할 수 있습니다. 이 구성에서는 가상 시스템이 다른 가상 시스템을 직접적으로 제어하거나 해당 메모리에 액세스하지 못하지만 모든 가상 시스템은 가상 네트워크를 통해 연결되어 있습니다. 이 네트워크는 바이러스 전파에 사용되거나 다른 종류의 공격의 대상이 될 수 있습니다. DMZ에 있는 가상 시스템의 보안 수준은 같은 네트워크에 연결되어 있는 개별 물리적 시스템의 보안 수준과 동일합니다.

단일 ESXi 호스트 내에 여러 네트워크 생성

ESXi 시스템은 동일한 호스트에서 가상 시스템 중 일부 그룹은 내부 네트워크에 연결하고, 다른 일부 그룹은 외부 네트워크에 연결하며, 또 다른 그룹은 두 가지 네트워크에 모두 연결할 수 있도록 설계되었습니다. 이 기능은 기본적으로 가상 시스템을 분리하고 가상 네트워킹 기능을 효과적으로 활용함으로써 구현할 수 있습니다.

그림 8-3. 단일 ESXi 호스트에 외부 네트워크, 내부 네트워크 및 DMZ 구성



이 그림에서 시스템 관리자는 호스트를 세 가지 고유한 가상 시스템 영역인 FTP 서버, 내부 가상 시스템 및 DMZ로 구성했습니다. 각 영역은 하나의 고유한 기능을 제공합니다.

FTP 서버

가상 시스템 1은 FTP 소프트웨어를 사용하여 구성되었으며, 벤더가 지역화한 참고 자료 및 양식과 같이 외부 리소스와 주고 받는 데이터의 보관 영역 기능을 합니다.

이 가상 시스템은 외부 네트워크와만 연결되며, 고유한 가상 스위치와 물리적 네트워크 어댑터를 사용하여 외부 네트워크 1에 연결합니다. 외부 네트워크 1은 회사에서 외부 소스의 데이터를 수신하는 데 사용하는 서버의 전용 네트워크입니다. 예를 들어 회사에서는 외부 네트워크 1을 사용하여 벤더의 FTP 트래픽을 수신하고, 벤더는 FTP를 통해 외부에서 사용할 수 있는 서버에 저장된 데이터에 액세스할 수 있습니다. 외부 네트워크 1은 가상 시스템 1뿐 아니라 사이트 전체에서 다른 ESXi 호스트에 구성되어 있는 FTP 서버에도 서비스를 제공합니다.

가상 시스템 1은 호스트 내의 어떤 가상 시스템과도 가상 스위치나 물리적 네트워크 어댑터를 공유하지 않기 때문에 호스트의 다른 가상 시스템은 가상 시스템 1 네트워크와 패킷을 주고 받을 수 없습니다. 이러한 제한은 공격 대상에 네트워크 트래픽을 보내야 하는 스니핑 공격을 방지하는 역할을 합니다. 더

중요한 점은 공격자가 **FTP**의 기본적인 취약점을 악용하여 호스트의 다른 가상 시스템에 액세스하지 못한다는 것입니다.

내부 가상 시스템

가상 시스템 2부터 5까지는 내부 용도로 예약됩니다. 이러한 가상 시스템은 의료 기록, 법적 합의서 및 사기 조사와 같이 회사의 기밀 데이터를 처리하고 저장합니다. 따라서 시스템 관리자는 이러한 가상 시스템에 가장 강력한 수준의 보호 기능을 사용해야 합니다.

가상 시스템 각각은 고유한 가상 스위치와 네트워크 어댑터를 통해 내부 네트워크 2에 연결합니다. 내부 네트워크 2는 청구 담당자, 내부 변호사 또는 사정인과 같은 직원이 내부적으로 사용하도록 예약됩니다.

가상 시스템 2부터 5까지는 가상 스위치를 통해 서로 통신하며, 물리적 네트워크 어댑터를 통해 내부 네트워크 2의 다른 위치에 있는 내부 가상 시스템과 통신합니다. 그러나 외부로 대상으로 하는 시스템과는 통신할 수 없습니다. **FTP** 서버에서와 마찬가지로 이러한 가상 시스템은 다른 가상 시스템의 네트워크와 패킷을 주고받을 수 없습니다. 마찬가지로 호스트의 다른 가상 시스템은 가상 시스템 2부터 5까지와 패킷을 주고 받을 수 없습니다.

DMZ

가상 시스템 6부터 8까지는 마케팅 그룹이 회사의 외부 웹 사이트를 게시하는 데 사용하는 **DMZ**로 구성되어 있습니다.

이 가상 시스템 그룹은 외부 네트워크 2 및 내부 네트워크 1과 연결되어 있습니다. 회사에서는 외부 네트워크 2를 사용하여 마케팅 및 재무 부서가 회사 웹 사이트를 호스트하는 데 사용하는 웹 서버를 지원하고 외부 사용자를 위해 호스트하는 다른 웹 기능을 지원합니다. 내부 네트워크 1은 마케팅 부서가 회사 웹 사이트에 콘텐츠를 게시하고, 다운로드를 게시하고, 사용자 포럼과 같은 서비스를 유지 관리하는 데 사용하는 통로입니다.

이러한 네트워크는 외부 네트워크 1 및 내부 네트워크 2와는 별개이며 가상 시스템에도 이러한 네트워크에 대한 공유된 연결 지점(스위치나 어댑터)이 없기 때문에 **FTP** 서버나 내부 가상 시스템 그룹을 대상으로 하는 공격의 위험이 없습니다.

시스템 관리자는 가상 시스템 분리 기능을 활용하고, 가상 스위치를 올바르게 구성하고, 분리된 네트워크를 유지 관리하여 세 가지 가상 시스템 영역 모두를 **ESXi** 호스트 하나에 구성하여 데이터나 리소스 위반을 확실하게 방지할 수 있습니다.

회사에서는 가상 시스템 그룹 간의 분리를 확실히 하기 위해 여러 개의 내부/외부 네트워크를 사용하고 각 그룹마다 서로 완전히 다른 가상 스위치와 물리적 네트워크 어댑터를 사용하도록 합니다.

모든 가상 스위치가 하나의 가상 시스템 영역에만 사용되기 때문에 시스템 관리자는 영역 사이에 패킷 누수 위험을 방지할 수 있습니다. 가상 스위치는 다른 가상 스위치에 직접 패킷을 전송하지 못하도록 설계되었습니다. 가상 스위치 간의 패킷 전송은 다음과 같은 경우에만 가능합니다.

- 가상 스위치가 동일한 물리적 **LAN**에 연결된 경우
- 가상 스위치가 패킷 전송에 사용될 수 있는 공통의 가상 시스템에 연결된 경우

위의 샘플 구성에서는 이와 같은 경우는 해당되지 않습니다. 시스템 관리자가 공통의 가상 스위치 경로가 없는지 확인하려는 경우, vSphere Web Client에서 네트워크 스위치 레이어아웃을 검토하여 가능한 공유 연결 지점이 있는지 검사할 수 있습니다.

가상 시스템의 리소스를 보호하기 위해 시스템 관리자는 각 가상 시스템에 대해 리소스 예약 및 제한을 구성하여 DoS/DDos 공격의 위험을 줄입니다. 더 나아가 시스템 관리자는 DMZ의 프런트 엔드와 백 엔드에 소프트웨어 방화벽을 설치하여 호스트를 물리적 방화벽 안쪽에 배치하고 각각의 네트워킹 스토리지 리소스가 고유의 가상 스위치를 사용하도록 구성함으로써 ESXi 호스트와 가상 시스템을 보호합니다.

인터넷 프로토콜 보안

IPsec(Internet Protocol Security)은 호스트에서 주고받는 IP 통신에 보안을 적용합니다. ESXi 호스트는 IPv6을 사용하는 IPsec을 지원합니다.

호스트에서 IPsec을 설정할 때는 수신 및 송신 패킷에 대해 인증과 암호화가 사용되도록 설정해야 합니다. IP 트래픽이 암호화되는 시기와 방법은 시스템의 보안 연결과 보안 정책을 설정하는 방법에 따라 달라집니다.

보안 연결은 시스템에서 트래픽을 암호화하는 방법을 결정합니다. 보안 연결을 생성할 때는 소스와 대상, 암호화 매개 변수, 그리고 보안 연결의 이름을 지정해야 합니다.

보안 정책은 시스템에서 트래픽을 암호화해야 하는 시기를 결정합니다. 보안 정책에는 소스 및 대상 정보, 암호화할 트래픽의 프로토콜과 방향, 사용할 모드(전송 또는 터널)와 보안 연결이 포함됩니다.

사용 가능한 보안 연결 나열

ESXi는 보안 정책에 의해 사용할 수 있는 모든 보안 연결 목록을 제공할 수 있습니다. 이 목록에는 사용자가 생성한 보안 연결과 VMkernel이 IKE(Internet Key Exchange)를 통해 설치한 보안 연결이 모두 포함됩니다.

`esxcli vSphere CLI 명령을 통해 사용 가능한 보안 연결 목록을 가져올 수 있습니다.`

절차

- ◆ 명령 프롬프트에서 **`esxcli network ip ipsec sa list`** 명령을 입력합니다.

결과

ESXi가 사용 가능한 모든 보안 연결 목록을 표시합니다.

IPsec 보안 연결 추가

연결된 IP 트래픽의 암호화 매개 변수를 지정하기 위해 보안 연결을 추가합니다.

`esxcli vSphere CLI 명령을 사용하여 보안 연결을 추가할 수 있습니다.`

절차

- ◆ 명령 프롬프트에서 다음 옵션을 하나 이상 포함하여 **esxcli network ip ipsec sa add** 명령을 입력합니다.

옵션	설명
--sa-source= <i>source address</i>	필수. 소스 주소를 지정합니다.
--sa-destination= <i>destination address</i>	필수. 대상 주소를 지정합니다.
--sa-mode= <i>mode</i>	필수. transport 또는 tunnel 모드 중 하나를 지정합니다.
--sa-spi= <i>security parameter index</i>	필수. 보안 매개 변수 인덱스를 지정합니다. 보안 매개 변수 인덱스는 호스트에서 보안 연결을 식별하는 데 사용되며 0x 접두사로 시작하는 16진수여야 합니다. 생성하는 각 보안 연결에는 프로토콜과 보안 매개 변수 인덱스의 고유한 조합이 있어야 합니다.
--encryption-algorithm= <i>encryption algorithm</i>	필수. 다음 매개 변수 중 하나를 사용하여 암호화 알고리즘을 지정합니다. <ul style="list-style-type: none"> ■ 3des-cbc ■ aes128-cbc ■ null(암호화를 제공하지 않음)
--encryption-key= <i>encryption key</i>	암호화 알고리즘을 지정하는 경우 필수. 암호화 키를 지정합니다. ASCII 텍스트 또는 0x 접두사로 시작하는 16진수를 키로 입력할 수 있습니다.
--integrity-algorithm= <i>authentication algorithm</i>	필수. 인증 알고리즘을 hmac-sha1 또는 hmac-sha2-256으로 지정합니다.
--integrity-key= <i>authentication key</i>	필수. 인증 키를 지정합니다. ASCII 텍스트 또는 0x 접두사로 시작하는 16진수를 키로 입력할 수 있습니다.
--sa-name= <i>name</i>	필수. 보안 연결에 대한 이름을 제공합니다.

예제: 새 보안 연결 명령

다음 예에는 읽기 쉽도록 줄 바꿈이 추가로 포함되어 있습니다.

```
esxcli network ip ipsec sa add
--sa-source 3ffe:501:ffff:0::a
--sa-destination 3ffe:501:ffff:0001:0000:0000:0000:0001
--sa-mode transport
--sa-spi 0x1000
--encryption-algorithm 3des-cbc
--encryption-key 0x6970763672656164796c6f676f336465736362636f757432
--integrity-algorithm hmac-sha1
--integrity-key 0x6970763672656164796c6f67736861316f757432
--sa-name sal
```

IPsec 보안 연결 제거

ESXCLI vSphere CLI 명령을 사용하여 보안 연결을 제거할 수 있습니다.

사전 요구 사항

사용하려는 보안 연결이 현재 사용 중인지 확인합니다. 사용 중인 보안 연결을 제거하려고 시도하면 제거 작업이 실패합니다.

절차

- ◆ 명령 프롬프트에서

esxcli network ip ipsec sa remove --sa-name *security_association_name* 명령을 입력합니다.

사용 가능한 IPsec 보안 정책 나열

ESXCLI vSphere CLI 명령을 사용하여 사용 가능한 보안 정책을 나열할 수 있습니다.

절차

- ◆ 명령 프롬프트에서 **esxcli network ip ipsec sp list** 명령을 입력합니다.

결과

사용 가능한 모든 보안 정책의 목록이 표시됩니다.

IPSec 보안 정책 생성

보안 연결에 설정되어 있는 인증 및 암호화 매개 변수를 사용할 시점을 판단하기 위해 보안 정책을 생성합니다. ESXCLI vSphere CLI 명령을 사용하여 보안 정책을 추가할 수 있습니다.

사전 요구 사항

보안 정책을 생성하기 전에 **IPsec 보안 연결 추가**에 설명되어 있는 대로 적절한 인증 및 암호화 매개 변수가 설정된 보안 연결을 추가합니다.

절차

- ◆ 명령 프롬프트에서 다음 옵션을 하나 이상 포함하여 **esxcli network ip ipsec sp add** 명령을 입력합니다.

옵션	설명
--sp-source= <i>source address</i>	필수. 소스 IP 주소와 접두사 길이를 지정합니다.
--sp-destination= <i>destination address</i>	필수. 대상 주소 및 접두사 길이를 지정합니다.
--source-port= <i>port</i>	필수. 소스 포트를 지정합니다. 소스 포트는 0에서 65535 사이의 숫자여야 합니다.
--destination-port= <i>port</i>	필수. 대상 포트를 지정합니다. 소스 포트는 0에서 65535 사이의 숫자여야 합니다.

옵션	설명
--upper-layer-protocol= <i>protocol</i>	다음 매개 변수 중 하나를 사용하여 상위 계층 프로토콜을 지정합니다. <ul style="list-style-type: none"> ■ tcp ■ udp ■ icmp6 ■ 임의
--flow-direction= <i>direction</i>	in 또는 out을 사용하여 트래픽을 모니터링할 방향을 지정합니다.
--action= <i>action</i>	지정한 매개 변수를 사용하는 트래픽을 발견했을 때 수행할 작업을 지정합니다. 다음 매개 변수 중 하나를 사용할 수 있습니다. <ul style="list-style-type: none"> ■ 없음 어떤 작업도 수행하지 않습니다. ■ 삭제 데이터 수신 및 송신을 허용하지 않습니다. ■ ipsec: 보안 연결에 제공되는 인증 및 암호화 정보를 사용하여 데이터가 신뢰할 수 있는 소스로부터 전송되었는지 확인합니다.
--sp-mode= <i>mode</i>	tunnel 또는 transport으로 모드를 지정합니다.
--sa-name= <i>security association name</i>	필수. 보안 정책에 사용할 보안 연결의 이름을 제공합니다.
--sp-name= <i>name</i>	필수. 보안 정책에 대한 이름을 제공합니다.

예제: 새 보안 정책 명령

다음 예제에서는 가독성을 높이기 위해 추가로 줄 바꿈이 포함됩니다.

```
esxcli network ip ipsec add
--sp-source=2001:db8:1::/64
--sp-destination=2002:db8:1::/64
--source-port=23
--destination-port=25
--upper-layer-protocol=tcp
--flow-direction=out
--action=ipsec
--sp-mode=transport
--sa-name=sal
--sp-name=sp1
```

IPsec 보안 정책 제거

ESXCLI vSphere CLI 명령을 사용하여 ESXi 호스트에서 보안 정책을 제거할 수 있습니다.

사전 요구 사항

사용하려는 보안 정책이 현재 사용 중인지 확인합니다. 사용 중인 보안 정책을 제거하려고 하면 제거 작업이 실패합니다.

절차

◆ 명령 프롬프트에서

esxcli network ip ipsec sp remove --sa-name security policy name 명령을 입력합니다.

모든 보안 정책을 제거하려면 **esxcli network ip ipsec sp remove --remove-all** 명령을 입력합니다.

적절한 SNMP 구성 확인

SNMP가 적절하게 구성되지 않으면 모니터링 정보가 악의적인 호스트에 전송될 수 있습니다. 그러면 악의적인 호스트가 이 정보를 이용하여 공격을 계획할 수 있습니다.

절차

- 1 **esxcli system snmp get**을 실행하여 **SNMP**가 현재 사용되고 있는지 확인합니다.
- 2 시스템에 **SNMP**가 필요하면 **esxcli system snmp set --enable true** 명령을 실행하여 **SNMP**가 실행되고 있는지 확인합니다.
- 3 시스템에서 **SNMP**가 사용되는 경우에는 "모니터링 및 성능" 설명서에서 **SNMP 3**에 대한 설정 정보를 참조하십시오.

SNMP는 각 **ESXi** 호스트에서 구성되어야 합니다. **vCLI**, **PowerCLI** 또는 **vSphere Web Services SDK**를 사용하여 구성할 수 있습니다.

필요한 경우에만 vSphere Network Appliance API의 가상 스위치 사용

vSphere Network Appliance API(DvFilter)를 이용하는 제품을 사용하지 않는 경우에는 가상 시스템으로 네트워크 정보를 보내도록 호스트를 구성하지 마십시오. **vSphere Network Appliance API**가 사용하도록 설정된 경우 공격자가 가상 시스템을 필터에 연결하려고 시도할 수 있으며, 연결되는 경우 공격자가 호스트에 있는 다른 가상 시스템의 네트워크에 액세스할 수 있습니다.

이 **API**를 이용하는 제품을 사용하는 경우 호스트가 올바르게 구성되어 있는지 확인합니다. 자세한 내용은 "vSphere 솔루션, vService 및 ESX Agent 개발 및 배포"에서 **DvFilter** 섹션을 참조하십시오. 호스트가 이 **API**를 사용하도록 설정된 경우 **Net.DVFilterBindIpAddress** 매개 변수의 값이 이 **API**를 사용하는 제품과 일치하는지 확인해야 합니다.

절차

- 1 Net.DVFilterBindIpAddress 커널 매개 변수의 값이 올바른지 확인하려면 vSphere Web Client 를 사용하여 이 매개 변수를 찾습니다.
 - a 호스트를 선택하고 **관리** 탭을 클릭합니다.
 - b 시스템 아래에서 **고급 시스템 설정**을 선택합니다.
 - c 아래로 스크롤하여 Net.DVFilterBindIpAddress를 찾은 다음 매개 변수의 값이 비어 있는지 확인합니다.

매개 변수의 순서는 엄격히 사전순으로 정렬되어 있지 않습니다. 필터 필드에 **DVFilter**를 입력하여 모든 관련 매개 변수를 표시합니다.
- 2 DvFilter 설정을 사용하지 않는 경우 값이 비어 있는지 확인합니다.
- 3 DvFilter 설정을 사용하는 경우 이 매개 변수의 값이 DvFilter를 사용하는 제품에서 사용 중인 값과 일치하는지 확인합니다.

vSphere 네트워킹 보안 모범 사례

네트워킹 보안 모범 사례를 따르면 vSphere 배포의 무결성을 보장할 수 있습니다.

일반 네트워킹 보안 권장 사항

네트워킹 환경을 보호하기 위한 첫 번째 단계는 일반 네트워크 보안 권장 사항을 따르는 것입니다. 그런 다음 방화벽 또는 IPsec를 사용하는 네트워크 보안과 같은 특수 분야로 나아갈 수 있습니다.

- 스페닝 트리를 사용하도록 설정한 경우 물리적 스위치 포트가 **Portfast**로 구성되었는지 확인하십시오. VMware 가상 스위치는 STP를 지원하지 않기 때문에 물리적 스위치 네트워크에서 루프를 방지하기 위해 스페닝 트리를 사용하도록 설정한 경우 ESXi 호스트에 연결된 물리적 스위치 포트에 **Portfast**가 구성되어 있어야 합니다. **Portfast**가 설정되지 않은 경우 잠재적인 성능 및 연결 문제가 발생할 수 있습니다.
- Distributed Virtual Switch에 대한 Netflow 트래픽이 인증된 수집기 IP 주소로만 전송되는지 확인하십시오. Netflow 내보내기는 암호화되지 않고 가상 네트워크에 대한 정보를 포함할 수 있기 때문에 메시지 가로채기 공격이 성공할 가능성이 높아집니다. Netflow 내보내기가 필요한 경우 모든 Netflow 대상 IP 주소가 올바른지 확인하십시오.
- 인증된 관리자만 역할 기반 액세스 컨트롤을 사용하여 가상 네트워킹 구성 요소에 액세스할 수 있는지 확인하십시오. 예를 들어 가상 시스템 관리자는 해당 가상 시스템이 있는 포트 그룹에 대해서만 액세스 권한이 있어야 합니다. 네트워크 관리자는 모든 가상 네트워킹 구성 요소에 대한 사용 권한이 있어야 하지만 가상 시스템에 대한 액세스 권한은 없어야 합니다. 액세스를 제한하면 실수는 악의적이든 잘못된 구성에 대한 위험이 줄어들고 의무와 최소 권한의 분리라는 핵심 보안 개념이 적용됩니다.

- 포트 그룹이 네이티브 VLAN의 값으로 구성되어 있지 않은지 확인합니다. 물리적 스위치는 네이티브 VLAN으로 VLAN 1을 사용합니다. 네이티브 VLAN의 프레임은 태그가 1로 지정되지 않습니다. ESXi에는 네이티브 VLAN이 없습니다. VLAN이 포트 그룹에서 지정된 프레임에는 태그가 있지만 VLAN이 포트 그룹에서 지정되지 않은 프레임에는 태그가 지정되지 않습니다. 따라서 태그가 1로 지정된 가상 시스템이 물리적 스위치의 네이티브 VLAN에 속하게 되기 때문에 문제가 발생할 수 있습니다.

예를 들어 Cisco 물리적 스위치의 VLAN 1에 있는 프레임은 VLAN1이 해당 물리적 스위치에서 네이티브 VLAN이기 때문에 태그가 해제됩니다. 그런데 ESXi 호스트에서 VLAN 1로 지정된 프레임에는 태그가 1로 지정되었으므로 태그가 해제되는 대신 네이티브 VLAN으로 향하는 ESXi 호스트의 트래픽이 올바르게 라우팅되지 않습니다. 네이티브 VLAN에서 전송되는 물리적 스위치의 트래픽은 태그가 지정되지 않으므로 표시되지 않습니다. ESXi 가상 스위치 포트 그룹이 네이티브 VLAN ID를 사용하는 경우 가상 시스템의 이 포트에서 시작되는 트래픽은 스위치가 태그 해제된 트래픽을 예상하기 때문에 스위치의 네이티브 VLAN에 표시되지 않습니다.

- 포트 그룹이 업스트림 물리적 스위치에 예약된 VLAN 값으로 구성되어 있지 않은지 확인합니다. 물리적 스위치는 내부 용도로 특정 VLAN ID를 예약하며 대개 트래픽이 이러한 값으로 구성되지 못하도록 합니다. 예를 들어 Cisco Catalyst 스위치는 일반적으로 VLAN 1001 - 1024 및 4094를 예약합니다. 예약된 VLAN을 사용하면 네트워크에서 서비스 거부 발생할 수 있습니다.
- VGT(Virtual Guest Tagging)를 제외하고 포트 그룹이 VLAN 4095로 구성되어 있지 않은지 확인합니다. 포트 그룹을 VLAN 4095로 설정하면 VGT 모드가 활성화됩니다. 이 모드에서는 가상 스위치가 VLAN 태그를 수정하지 않은 채 가상 시스템이 처리하도록 두고 모든 네트워크 프레임을 가상 시스템에 전달합니다.
- Distributed Virtual Switch에서 포트 수준 구성 재정의의 제한합니다. 포트 수준 구성 재정의는 기본적으로 사용하지 않도록 설정됩니다. 사용하도록 설정하면 가상 시스템에 대해 포트 그룹 수준의 설정과 다른 보안 설정을 적용할 수 있습니다. 특정 가상 시스템에는 고유한 구성이 필요하지만 반드시 모니터링해야 합니다. 재정의의 모니터링하지 않을 경우 보안이 약한 Distributed Virtual Switch 구성을 사용하는 가상 시스템에 대한 액세스 권한을 획득한 모든 사람이 해당 액세스를 악용하려고 할 수 있습니다.
- Distributed Virtual Switch 포트 미러 트래픽이 권한이 있는 수집기 포트 또는 VLAN으로만 전송되는지 확인합니다. vSphere Distributed Switch는 한 포트에서 다른 포트로의 트래픽을 미러링할 수 있으므로 패킷 캡처 디바이스가 특정 트래픽 흐름을 수집할 수 있습니다. 포트 미러링은 모든 지정된 트래픽의 복사본을 암호화되지 않은 형식으로 전송합니다. 이러한 미러링된 트래픽은 캡처된 패킷의 전체 데이터를 포함하므로 잘못 전송될 경우 해당 데이터가 완전히 손상될 수 있습니다. 포트 미러링이 필요할 경우 모든 포트 미러 대상 VLAN, 포트 및 업링크 ID가 올바른지 확인하십시오.

네트워킹 구성 요소 레이블 지정

네트워킹 아키텍처의 여러 구성 요소 식별은 중요하며 네트워크가 늘어남에 따라 오류가 발생하지 않도록 보장하는 데 도움이 됩니다.

다음 모범 사례를 따르십시오.

- 포트 그룹이 명확한 네트워크 레이블로 구성되었는지 확인합니다. 이러한 레이블은 포트 그룹의 기능 설명자 역할을 하며 네트워크가 더욱 복잡해짐에 따라 각 포트 그룹의 기능을 식별하는 데 도움이 됩니다.
- 각각의 vSphere Distributed Switch에 스위치의 기능 또는 IP 서브넷을 나타내는 명확한 네트워크 레이블이 있는지 확인합니다. 이 레이블은 물리적 스위치에 호스트 이름이 필요한 것과 마찬가지로 스위치의 기능 설명자 역할을 합니다. 예를 들어 스위치의 레이블을 내부로 지정하여 내부 네트워킹용임을 표시할 수 있습니다. 표준 가상 스위치에 대한 레이블은 변경할 수 없습니다.

vSphere VLAN 환경 문서화 및 확인

VLAN 환경을 정기적으로 확인하여 주소 지정 문제를 방지합니다. VLAN 환경을 완전히 문서화하고 VLAN ID가 한 번만 사용되는지 확인합니다. 설명서는 문제 해결에 도움이 될 수 있으며 환경을 확장하려고 할 때 필수적입니다.

절차

- 1 모든 vSwitch 및 VLAN ID가 완전히 문서화되었는지 확인합니다.

가상 스위치에서 VLAN 태그 지정을 사용하는 경우 해당 ID가 외부 VLAN 인식 업스트림 스위치의 ID와 일치해야 합니다. VLAN ID가 완전하게 추적되지 않는 경우 잘못된 ID 재사용이 잘못된 물리적 시스템과 가상 시스템 간의 트래픽을 허용할 수 있습니다. 마찬가지로 VLAN ID가 잘못되었거나 누락된 경우 물리적 시스템과 가상 시스템 간의 트래픽이 통과하기를 원하는 곳에서 차단될 수 있습니다.

- 2 모든 분산 가상 포트 그룹(dvPortgroup 인스턴스)에 대한 VLAN ID가 완전히 문서화되었는지 확인합니다.

dvPortgroup에서 VLAN 태그 지정을 사용하는 경우 해당 ID가 외부 VLAN 인식 업스트림 스위치의 ID와 일치해야 합니다. VLAN ID가 완전하게 추적되지 않는 경우 잘못된 ID 재사용이 잘못된 물리적 시스템과 가상 시스템 간의 트래픽을 허용할 수 있습니다. 마찬가지로 VLAN ID가 잘못되었거나 누락된 경우 물리적 시스템과 가상 시스템 간의 트래픽이 통과하기를 원하는 곳에서 차단될 수 있습니다.

- 3 모든 Distributed Virtual Switch에 대한 전용 VLAN ID가 완전히 문서화되었는지 확인합니다.

Distributed Virtual Switch에 대한 PVLAN(전용 VLAN)은 기본 및 보조 VLAN ID를 필요로 합니다. 이러한 ID는 외부 PVLAN 인식 업스트림 스위치의 ID와 일치해야 합니다. VLAN ID가 완전하게 추적되지 않는 경우 잘못된 ID 재사용이 잘못된 물리적 시스템과 가상 시스템 간의 트래픽을 허용할 수 있습니다. 마찬가지로 PVLAN ID가 잘못되었거나 누락된 경우 물리적 시스템과 가상 시스템 간의 트래픽이 통과하기를 원하는 곳에서 차단될 수 있습니다.

- 4 VLAN 트렁크 링크가 트렁크 링크로 작동하는 물리적 스위치 포트에만 연결되었는지 확인합니다.

가상 스위치를 VLAN 트렁크 포트에 연결하는 경우 업링크 포트에서 가상 스위치와 물리적 스위치를 모두 적절한 구성해야 합니다. 물리적 스위치가 제대로 구성되지 않으면 VLAN 802.1q 헤더가 포함된 프레임이 도착을 예상하지 않은 스위치로 전달됩니다.

건전한 네트워크 분리 방식 채택

건전한 네트워크 분리 방식을 채택하면 vSphere 환경의 네트워크 보안이 크게 향상됩니다.

관리 네트워크 분리

vSphere 관리 네트워크는 각 구성 요소의 vSphere 관리 인터페이스에 대한 액세스를 제공합니다. 관리 인터페이스에서 실행 중인 서비스는 공격자가 해당 시스템에 대한 액세스 권한을 얻을 수 있는 기회를 제공합니다. 원격 공격은 이 네트워크에 대한 액세스 획득으로 시작될 가능성이 있습니다. 공격자가 관리 네트워크에 대한 액세스 권한을 얻는 경우 이후 침입을 위한 단계적 토대가 됩니다.

ESXi 호스트 또는 클러스터에서 실행되는 가장 안전한 가상 시스템의 보안 수준에서 보호함으로써 관리 네트워크에 대한 액세스를 엄격하게 제어합니다. 관리 네트워크가 제한되는 방식에 관계없이 관리자는 ESXi 호스트 및 vCenter Server 시스템을 구성하기 위해 이 네트워크에 대한 액세스 권한이 있어야 합니다.

공동 vSwitch의 전용 VLAN에 vSphere 관리 포트 그룹을 배치합니다. vSphere 관리 포트 그룹의 VLAN이 운영 가상 시스템에 의해 사용되지 않는 경우 vSwitch를 운영(가상 시스템) 트래픽과 공유할 수 있습니다. 예를 들어 vSphere Replication과 함께, 기타 관리 관련 엔터티가 발견된 네트워크 등을 제외하고, 네트워크 세그먼트가 라우팅되지 않았는지 확인합니다. 특히, 이 네트워크에 운영 가상 시스템 트래픽을 라우팅할 수 없는지 확인합니다.

다음 접근 방식 중 하나를 사용하여 엄격하게 제어되는 방식으로 관리 기능에 대한 액세스를 사용하도록 설정합니다.

- 특히 중요한 환경의 경우 관리 네트워크에 액세스하기 위한 제어되는 게이트웨이 또는 기타 제어되는 방법을 구성합니다. 예를 들어 관리자가 VPN을 통해 관리 네트워크에 연결하도록 요구하고 신뢰할 수 있는 관리자에게만 액세스를 허용합니다.
- 관리 클라이언트를 실행하는 점프 박스(jump box)를 구성합니다.

스토리지 트래픽 분리

IP 기반 스토리지 트래픽이 분리되었는지 확인합니다. IP 기반 스토리지에는 iSCSI 및 NFS가 포함됩니다. 가상 시스템은 IP 기반 스토리지 구성을 통해 가상 스위치 및 VLAN을 공유할 수 있습니다. 이러한 구성 유형은 IP 기반 스토리지 트래픽을 허용되지 않은 가상 시스템 사용자에게 노출할 수 있습니다.

IP 기반 스토리지는 대개 암호화되어 있지 않아 이 네트워크에 대한 액세스 권한이 있는 사용자면 누구든지 볼 수 있습니다. 허용되지 않은 사용자가 IP 기반 스토리지 트래픽을 보지 못하도록 제한하려면 IP 기반 스토리지 네트워크 트래픽을 운영 트래픽과 논리적으로 분리합니다. VMkernel 관리 네트워크와 분리된 VLAN 또는 네트워크 세그먼트에 IP 기반 스토리지 어댑터를 구성하여 허용되지 않은 사용자가 트래픽을 보지 못하도록 제한합니다.

VMotion 트래픽 분리

VMotion 마이그레이션 정보는 일반 텍스트로 전송됩니다. 이 정보가 전송되는 네트워크에 대한 액세스 권한이 있는 사용자면 누구든지 해당 정보를 볼 수 있습니다. 잠재적 공격자는 vMotion 트래픽을 가로채 가상 시스템의 메모리 콘텐츠를 얻을 수 있습니다. 또한 잠재적 공격자는 마이그레이션 동안 콘텐츠가 수정되는 MiTM 공격을 스테이징합니다.

VMotion 트래픽을 분리된 네트워크의 운영 트래픽과 분리합니다. 네트워크를 라우팅할 수 없도록 설정합니다. 즉, 네트워크에 대한 외부 액세스를 방지하기 위해 이 네트워크와 다른 네트워크를 확장하는 계층-3 라우터가 없도록 합니다.

VMotion 포트 그룹은 공통 vSwitch의 전용 VLAN에 있어야 합니다. VMotion 포트 그룹의 VLAN이 운영 가상 시스템에 의해 사용되지 않는 경우 vSwitch를 운영(가상 시스템) 트래픽과 공유할 수 있습니다.

여러 vSphere 구성 요소와 관련된 모범 사례

9

환경에서 NTP 설정과 같은 일부 보안 모범 사례는 둘 이상의 vSphere 구성 요소에 영향을 줍니다. 환경을 구성할 때 다음 권장 사항을 고려하십시오.

관련 정보는 [장 5 ESXi 호스트 보안](#) 및 [장 7 가상 시스템 보안](#)을 참조하십시오.

본 장은 다음 항목을 포함합니다.

- [vSphere 네트워크에서 클럭 동기화](#)
- [스토리지 보안 모범 사례](#)
- [게스트로 호스트 성능 데이터 보내기가 사용하지 않도록 설정되었는지 확인](#)
- [ESXi Shell 및 vSphere Web Client에 대한 시간 제한 설정](#)

vSphere 네트워크에서 클럭 동기화

vSphere 네트워크에 있는 모든 구성 요소의 클럭은 서로 동기화되어야 합니다. vSphere 네트워크에 있는 시스템의 클럭이 동기화되지 않으면 네트워크 시스템 간 통신에서 시간에 민감한 SSL 인증서가 유효한 인증서로 인식되지 않을 수 있습니다.

클럭이 동기화되지 않으면 인증 문제가 발생하여 설치가 실패하거나 vCenter Server Appliance vpxd 서비스를 시작하지 못할 수 있습니다.

vCenter 구성 요소가 실행되는 Windows 호스트 시스템이 NTP 서버와 동기화되는지 확인합니다. 자세한 내용은 기술 자료 문서(<http://kb.vmware.com/kb/1318>)를 참조하십시오.

■ [네트워크 시간 서버와 ESXi 클럭 동기화](#)

vCenter Server를 설치하거나 vCenter Server Appliance를 배포하기 전에 vSphere 네트워크의 모든 시스템에서 해당 클럭을 동기화해야 합니다.

■ [vCenter Server Appliance에서 시간 동기화 설정 구성](#)

배포 후에 vCenter Server Appliance에서 시간 동기화 설정을 변경할 수 있습니다.

네트워크 시간 서버와 ESXi 클럭 동기화

vCenter Server를 설치하거나 vCenter Server Appliance를 배포하기 전에 vSphere 네트워크의 모든 시스템에서 해당 클럭을 동기화해야 합니다.

이 작업은 vSphere Client에서 NTP를 설정하는 방법을 설명합니다. `vicfg-ntp` vCLI 명령을 대신 사용할 수도 있습니다. 자세한 내용은 "vSphere Command-Line Interface 참조" 를 참조하십시오.

절차

- 1 vSphere Client를 시작하고 ESXi 호스트에 연결합니다.
- 2 구성 탭에서 시간 구성을 클릭합니다.
- 3 속성을 클릭한 후 옵션을 클릭합니다.
- 4 NTP 설정을 선택합니다.
- 5 추가를 클릭합니다.
- 6 [NTP 서버 추가] 대화상자에서 동기화할 NTP 서버의 IP 주소나 정규화된 도메인 이름을 입력합니다.
- 7 확인을 클릭합니다.

호스트 시간이 NTP 서버와 동기화됩니다.

vCenter Server Appliance에서 시간 동기화 설정 구성

배포 후에 vCenter Server Appliance에서 시간 동기화 설정을 변경할 수 있습니다.

vCenter Server Appliance를 배포할 때 NTP 서버를 사용하거나 VMware Tools를 사용하는 것 중에 하나로 시간 동기화 방법을 선택할 수 있습니다. vSphere 네트워크의 시간 설정이 변경될 경우 장치 셸에 있는 명령을 사용하여 vCenter Server Appliance를 편집하고 시간 동기화 설정을 구성할 수 있습니다.

정기 시간 동기화 기능을 사용하도록 설정한 경우 VMware Tools는 게스트 운영 체제의 시간을 호스트의 시간과 동일하게 설정합니다.

시간을 동기화한 후 VMware Tools는 게스트 운영 체제와 호스트의 클럭이 일치하는지 1분 단위로 확인합니다. 시간이 일치하지 않으면 호스트의 클럭을 기준으로 게스트 운영 체제의 클럭을 동기화합니다.

일반적으로 NTP(Network Time Protocol)와 같은 기본적으로 제공되는 시간 동기화 소프트웨어가 VMware Tools의 정기 시간 동기화보다 정확하기 때문에 되도록이면 이러한 시간 동기화 소프트웨어를 사용하는 것이 좋습니다. vCenter Server Appliance에서 한 가지 형태의 정기 시간 동기화만 사용할 수 있습니다. 기본적으로 제공되는 시간 동기화 소프트웨어와 vCenter Server Appliance VMware Tools 정기 시간 동기화 중에서 하나를 사용하기로 결정하면 다른 하나는 해제됩니다.

VMware Tools 시간 동기화 사용

VMware Tools 시간 동기화를 사용하도록 vCenter Server Appliance를 설정할 수 있습니다.

절차

- 1 장치 셸에 액세스하고 관리자 또는 슈퍼 관리자 역할을 가진 사용자로 로그인합니다.

슈퍼 관리자 역할의 기본 사용자는 루트입니다.

- 명령을 실행하여 VMware Tools 시간 동기화를 사용하도록 설정합니다.

```
timesync.set --mode host
```

- (선택 사항) 해당 명령을 실행하여 VMware Tools 시간 동기화를 적용했는지 확인합니다.

```
timesync.get
```

이 명령은 시간 동기화가 호스트 모드에 있다고 반환합니다.

결과

장치 시간이 ESXi 호스트 시간과 동기화됩니다.

vCenter Server Appliance 구성에서 NTP 서버 추가 또는 바꾸기

NTP 기반 시간 동기화를 사용하도록 vCenter Server Appliance를 설정하려면 NTP 서버를 vCenter Server Appliance 구성에 추가해야 합니다.

절차

- 장치 셸에 액세스하고 관리자 또는 슈퍼 관리자 역할을 가진 사용자로 로그인합니다.
슈퍼 관리자 역할의 기본 사용자는 루트입니다.

- ntp.server.add 명령을 사용하여 NTP 서버를 vCenter Server Appliance 구성에 추가합니다.

예를 들어 다음 명령을 실행합니다.

```
ntp.server.add --servers IP-addresses-or-host-names
```

여기서 *IP-addresses-or-host-names*는 NTP 서버의 IP 주소 목록 및 호스트 이름에 대해 쉼표로 구분된 목록입니다.

이 명령은 NTP 서버를 구성에 추가합니다. 시간 동기화가 NTP 서버를 기반으로 하는 경우에는 새 NTP 서버를 다시 불러오기 위해 NTP 데몬이 다시 시작됩니다. 그 외의 경우 이 명령은 단지 새 NTP 서버를 기존 NTP 구성에 추가합니다.

- (선택 사항) 이전 NTP 서버를 삭제하고 새 NTP 서버를 vCenter Server Appliance 구성에 추가하려면 ntp.server.set 명령을 실행합니다.

예를 들어 다음 명령을 실행합니다.

```
ntp.server.set --servers IP-addresses-or-host-names
```

여기서 *IP-addresses-or-host-names*는 NTP 서버의 IP 주소 목록 및 호스트 이름에 대해 쉼표로 구분된 목록입니다.

이 명령은 이전 NTP 서버를 구성에서 삭제하고 입력 NTP 서버를 구성에 설정합니다. 시간 동기화가 NTP 서버를 기반으로 하는 경우에는 새 NTP 구성을 다시 불러오기 위해 NTP 데몬이 다시 시작됩니다. 그 외의 경우 이 명령은 단지 NTP 구성에 있는 서버를 입력된 서버로 바꿉니다.

- 4 (선택 사항) 해당 명령을 실행하여 새로운 NTP 구성 설정을 적용했는지 확인합니다.

```
ntp.get
```

이 명령은 NTP 동기화에 대해 구성된 서버의 공백으로 구분된 목록을 반환합니다. NTP 동기화가 사용되는 경우 이 명령은 NTP 구성이 작동 상태에 있다고 반환합니다. NTP 동기화가 사용되지 않는 경우 이 명령은 NTP 구성이 중단 상태에 있다고 반환합니다.

다음에 수행할 작업

NTP 동기화가 사용되지 않는 경우 vCenter Server Appliance에서 NTP 서버를 기반으로 하도록 시간 동기화 설정을 구성할 수 있습니다. [NTP 서버와 vCenter Server Appliance의 시간 동기화](#)를 참조하십시오.

NTP 서버와 vCenter Server Appliance의 시간 동기화

vCenter Server Appliance에서 NTP 서버를 기반으로 하도록 시간 동기화 설정을 구성할 수 있습니다.

사전 요구 사항

vCenter Server Appliance 구성에서 하나 이상의 NTP(네트워크 시간 프로토콜) 서버를 설정합니다. [vCenter Server Appliance 구성에서 NTP 서버 추가 또는 바꾸기](#)를 참조하십시오.

절차

- 1 장치 셸에 액세스하고 관리자 또는 슈퍼 관리자 역할을 가진 사용자로 로그인합니다.
슈퍼 관리자 역할의 기본 사용자는 루트입니다.
- 2 명령을 실행하여 NTP 기반 시간 동기화를 사용하도록 설정합니다.

```
timesync.set --mode NTP
```

- 3 (선택 사항) 해당 명령을 실행하여 NTP 동기화를 적용했는지 확인합니다.

```
timesync.get
```

이 명령은 시간 동기화가 NTP 모드에 있다고 반환합니다.

스토리지 보안 모범 사례

스토리지 보안 공급자에서 설명한 대로 스토리지 보안의 모범 사례를 따르십시오. 또한 CHAP 및 상호 CHAP를 이용하여 iSCSI 스토리지, 마스크 및 영역 SAN 리소스를 보호하고 NFS 4.1에 대한 Kerberos 자격 증명을 구성할 수 있습니다.

"VMware Virtual SAN 관리" 설명서도 참조하십시오.

iSCSI 스토리지 보안

호스트에 대해 구성하는 스토리지는 iSCSI를 사용하는 하나 이상의 SAN(Storage Area Network)을 포함할 수 있습니다. 호스트에서 iSCSI를 구성할 때 보안 위험을 최소화하는 여러 수단을 사용할 수 있습니다.

iSCSI는 SCSI 디바이스에 액세스하는 방법이며, SCSI 디바이스에 대한 직접 연결하는 대신 네트워크 포트를 통한 TCP/IP를 사용하여 데이터 레코드를 교환하는 방법입니다. iSCSI 트랜잭션에서 원시 SCSI 데이터 블록은 iSCSI 레코드 내에 캡슐화되어 요청한 디바이스나 사용자에게 전송됩니다.

iSCSI SAN을 사용하면 기존 이더넷 인프라를 효율적으로 사용하여 동적으로 공유할 수 있는 스토리지 리소스에 대한 호스트 액세스를 제공합니다. iSCSI SAN은 여러 사용자에게 서비스를 제공하는 공용 스토리지 풀에 기반한 환경에서 경제적인 스토리지 솔루션을 제공합니다. 네트워크로 연결된 다른 시스템과 마찬가지로 iSCSI SAN은 보안 침해의 대상이 될 수 있습니다.

참고 iSCSI SAN을 보호하기 위한 요구 사항 및 절차는 호스트에서 사용할 수 있는 하드웨어 iSCSI 어댑터와 호스트를 통해 직접 구성된 iSCSI에 대한 요구 사항 및 절차와 유사합니다.

iSCSI 장치 보안

무단 침입으로부터 iSCSI 디바이스를 보호하는 한 가지 방법은 호스트(또는 이니시에이터)가 대상 LUN의 데이터에 액세스하려고 할 때마다 대상(iSCSI 디바이스)으로 하여금 호스트를 인증하도록 요구하는 것입니다.

인증의 목표는 이니시에이터에게 대상에 액세스할 수 있는 권한이 있음을 입증하는 것으로, 이러한 권한은 인증을 구성할 때 부여합니다.

ESXi는 iSCSI에 대해 SRP(보안 원격 프로토콜) 또는 공용 키 인증 방법을 지원하지 않습니다. NFS 4.1에서만 Kerberos를 사용할 수 있습니다.

ESXi는 CHAP 및 상호 CHAP 인증을 모두 지원합니다. "vSphere 스토리지" 설명서에서 iSCSI 디바이스에 최선의 인증 방법을 선택하는 방법 및 CHAP를 설정하는 방법을 설명합니다.

CHAP 암호가 고유한지 확인합니다. 각 호스트의 상호 인증 암호는 서로 달라야 합니다. 가능한 경우 서버에 인증하는 각 클라이언트에 대해서도 암호가 달라야 합니다. 그러면 단일 호스트가 손상되어도 공격자가 다른 임의의 호스트를 생성하여 스토리지 디바이스에 인증할 수 없습니다. 단일 공유 암호를 사용하는 경우 하나의 호스트가 손상되면 공격자가 스토리지 디바이스에 인증할 수 있습니다.

iSCSI SAN 보호

iSCSI 구성을 계획할 때 iSCSI SAN의 전반적인 보안을 개선할 방법을 강구해야 합니다. iSCSI 구성에 대한 보안은 IP 네트워크의 보안에 비례하므로 네트워크를 설정할 때 적절한 보안 표준을 적용하면 iSCSI 스토리지를 보호하는 데 도움이 됩니다.

다음은 적절한 보안 표준을 적용하기 위한 몇 가지 세부 제안 사항입니다.

전송 데이터 보호

iSCSI SAN에서의 주된 보안 위협은 공격자가 전송된 스토리지 데이터를 스니핑할 수 있다는 것입니다.

공격자가 iSCSI 데이터를 쉽게 볼 수 없도록 하려면 추가 조치를 취해야 합니다. 하드웨어 iSCSI 어댑터와 ESXi iSCSI 이니시에이터는 대상과 주고받는 데이터를 암호화하지 않으므로 데이터가 스니핑 공격에 더 취약합니다.

가상 시스템에 대해 표준 스위치 및 VLAN을 iSCSI 구성과 공유할 수 있도록 허용하면 잠재적으로 iSCSI 트래픽이 노출되어 가상 시스템 공격자에 의해 남용될 수 있습니다. 침입자가 iSCSI 전송을 수신할 수 없도록 하려면 가상 시스템이 iSCSI 스토리지 네트워크를 볼 수 없도록 만들어야 합니다.

하드웨어 iSCSI 어댑터를 사용하는 경우에는 iSCSI 어댑터 및 ESXi 물리적 네트워크 어댑터가 스위치 공유나 기타 방법으로 인해 부주의하게 호스트 외부로 연결되지 않도록 함으로써 이를 달성할 수 있습니다. ESXi 호스트를 통해 직접 iSCSI를 구성하는 경우에는 가상 시스템에서 사용하는 것과는 다른 표준 스위치를 통해 iSCSI 스토리지를 구성하여 이를 달성할 수 있습니다.

전용 표준 스위치를 제공하여 iSCSI SAN을 보호하는 것 외에도 고유의 VLAN에 iSCSI SAN을 구성하여 성능 및 보안을 개선할 수 있습니다. iSCSI 구성을 별도의 VLAN에 배치하면 iSCSI 어댑터 이외의 디바이스는 iSCSI SAN 내에서의 전송을 볼 수 없습니다. 또한 다른 소스의 네트워크 정체는 iSCSI 트래픽을 방해할 수 없습니다.

iSCSI 포트 보안

iSCSI 디바이스를 실행할 때 ESXi는 네트워크 연결을 수신하는 포트를 열지 않습니다. 이렇게 하면 침입자가 여분의 포트를 통해 ESXi에 침입하여 호스트에 대한 제어를 얻을 수 있는 기회를 줄일 수 있습니다. 따라서 iSCSI를 실행해도 연결의 ESXi 끝에서 추가적인 보안 위험이 생기지 않습니다.

실행하는 모든 iSCSI 대상 디바이스는 iSCSI 연결을 수신할 TCP 포트를 하나 이상 가지고 있어야 합니다. iSCSI 디바이스 소프트웨어에 보안상 취약한 부분이 존재하면 ESXi에 아무 문제가 없어도 데이터가 위험해질 수 있습니다. 이러한 위험을 줄이려면 해당 스토리지 장비 제조업체에서 제공하는 모든 보안 패치를 설치하고 iSCSI 네트워크에 연결되는 디바이스를 제한합니다.

SAN 리소스 마스킹 및 영역 설정

영역 설정 및 LUN 마스킹을 사용하여 SAN 작업을 분리하고 스토리지 디바이스에 대한 액세스를 제한할 수 있습니다.

SAN 리소스에 영역 설정 및 LUN 마스킹을 사용하여 vSphere 환경의 스토리지에 대한 액세스를 보호할 수 있습니다. 예를 들어 SAN 내에서 테스트를 위해 별도로 정의된 영역을 관리하여 운영 영역의 작업을 방해하지 않도록 할 수 있습니다. 마찬가지로 부서마다 다른 영역을 설정할 수도 있습니다.

영역을 설정할 때는 SAN 디바이스에 설정된 호스트 그룹을 고려해야 합니다.

각 SAN 스위치/디스크 어레이에 대한 영역 설정 및 마스킹 기능과 LUN 마스킹 관리용 도구는 벤더마다 다릅니다.

SAN 벤더의 설명서 및 "vSphere 스토리지" 설명서를 참조하십시오.

NFS 4.1에 Kerberos 자격 증명 사용

NFS 버전 4.1에서 ESXi는 Kerberos 인증 메커니즘을 지원합니다.

Kerberos는 NFS 공유를 마운팅하기 전에 ESXi에 설치된 NFS 4.1 클라이언트가 NFS 서버에 대한 해당 ID를 입증할 수 있는 인증 서비스입니다. Kerberos는 안전하지 않은 네트워크 연결에서 작업하기 위해 암호화를 사용합니다. NFS 4.1에 대해 Kerberos를 vSphere에서 구현할 때 클라이언트 및 서버에 대한 ID 확인만 지원하고 데이터 무결성 또는 기밀 서비스를 제공하지 않습니다.

Kerberos 인증을 사용할 때 다음 고려 사항이 적용됩니다.

- ESXi는 Kerberos 버전 5를 Active Directory 도메인 및 KDC(키 배포 센터)와 함께 사용합니다.
- vSphere 관리자는 Active Directory 자격 증명을 지정하여 NFS 4.1 Kerberos 데이터스토어에 대한 액세스를 NFS 사용자에게 제공합니다. 해당 호스트에 마운트된 모든 Kerberos 데이터스토어에 액세스하기 위해 단일 자격 증명 집합이 사용됩니다.
- 여러 ESXi 호스트가 동일한 NFS 4.1 데이터스토어를 공유하는 경우, 공유 데이터스토어에 액세스하는 모든 호스트에 대해 동일한 Active Directory 자격 증명을 사용해야 합니다. 호스트 프로파일에서 사용자를 설정하고 해당 프로파일을 모든 ESXi 호스트에 적용하면 이 작업을 자동화할 수 있습니다.
- NFS 4.1은 동시 AUTH_SYS 및 Kerberos 마운트를 지원하지 않습니다.
- Kerberos를 사용하는 NFS 4.1은 IPv6을 지원하지 않습니다. IPv4만 지원됩니다.

게스트로 호스트 성능 데이터 보내기가 사용하지 않도록 설정되었는지 확인

vSphere에는 VMware Tools가 설치된 Windows 운영 체제에 대한 가상 시스템 성능 카운터가 포함되어 있습니다. 가상 시스템 소유자는 성능 카운터를 사용하여 게스트 운영 체제 내에서 정확한 성능 분석을 수행할 수 있습니다. 기본적으로 vSphere는 게스트 가상 시스템에 호스트 정보를 제공하지 않습니다.

호스트 성능 데이터를 게스트 가상 시스템에 보내는 기능은 기본적으로 사용하지 않도록 설정됩니다. 이 기본 설정에 따라 가상 시스템은 물리적 호스트에 대한 세부 정보를 가져올 수 없으며, 가상 시스템의 보안을 위반할 경우 호스트 데이터를 사용하지 못하게 됩니다.

참고 아래의 절차는 기본 프로세스를 보여 줍니다. vSphere를 사용하거나, vSphere 명령줄 인터페이스(vCLI, PowerCLI 등) 중 하나를 대신 사용하여 모든 호스트에서 이 작업을 동시에 수행할 수도 있습니다.

절차

- 1 가상 시스템을 호스트하는 ESXi 시스템에서 VMX 파일을 찾습니다.

가상 시스템 구성 파일은 /vmfs/volumes/datastore 디렉토리에 있습니다. 여기서 *datastore*는 가상 시스템 파일이 저장된 스토리지 디바이스의 이름입니다.

- 2 VMX 파일에서 다음 매개 변수가 설정되어 있는지 확인합니다.

```
tools.guestlib.enableHostInfo=FALSE
```

- 3 파일을 저장한 후 닫습니다.

결과

게스트 가상 시스템 내에서 호스트에 대한 성능 정보를 검색할 수 없습니다.

ESXi Shell 및 vSphere Web Client에 대한 시간 제한 설정

침입자가 유희 세션을 사용하지 못하도록 하려면 ESXi Shell 및 vSphere Web Client에 대한 제한 시간을 설정해야 합니다.

ESXi Shell 시간 제한

ESXi Shell의 경우 vSphere Web Client 및 DCUI(Direct Console User Interface)에서 다음 시간 제한을 설정할 수 있습니다.

가용성 시간 제한

가용성 시간 초과 설정은 ESXi Shell이 설정된 후 로그인할 때까지의 최대 대기 시간입니다. 시간 초과 기간이 끝나면 서비스가 사용되지 않도록 설정되고 사용자는 로그인할 수 없습니다.

유희 시간 제한

유희 시간 초과는 사용자가 유희 대화형 세션에서 로그아웃할 때까지의 최대 대기 시간입니다. 유희 시간 초과에 대한 변경 내용은 사용자가 다음에 ESXi Shell에 로그인할 때 적용되며 기존 세션에는 영향을 미치지 않습니다.

vSphere Web Client 시간 제한

vSphere Web Client 세션은 기본적으로 120분 후에 종료됩니다. "vCenter Server 및 호스트 관리" 설명서에 나와 있는 것처럼 `webclient.properties` 파일에서 이 기본값을 변경할 수 있습니다.

TLS 재구성 유틸리티를 사용하여 TLS 프로토콜 구성 관리

10

TLS 재구성 유틸리티를 사용하여 TLS 프로토콜 버전을 사용하거나 사용하지 않도록 설정할 수 있습니다. vSphere 환경 내에서 TLS 1.0을 사용하지 않도록 설정하거나, TLS 1.0과 TLS 1.1을 모두 사용하지 않도록 설정할 수 있습니다. vSphere 6.5부터 TLS 프로토콜 버전 1.0, 1.1 및 1.2가 기본적으로 사용하도록 설정됩니다.

재구성하려면 환경 내 vCenter Server, Platform Services Controller, vSphere Update Manager 및 ESXi 호스트에서 사용하지 않도록 설정 가능한 소프트웨어 버전을 실행해야 합니다. TLS 1.0을 사용하지 않도록 설정 가능한 VMware 제품 목록은 VMware 기술 자료 문서 [2145796](#)을 참조하십시오.

TLS 1.0을 사용하지 않도록 설정하기 전에, 다른 VMware 제품 및 타사 제품이 사용하도록 설정된 프로토콜을 지원하는지 확인해야 합니다. 구성에 따라 사용하도록 설정된 프로토콜은 TLS 1.2나 TLS 1.1과 TLS 1.2 모두가 될 수 있습니다.

본 장은 다음 항목을 포함합니다.

- TLS 버전을 사용하지 않도록 설정 가능한 포트
- vSphere에서 TLS 버전을 사용하지 않도록 설정
- TLS 구성 유틸리티 설치
- 선택적 수동 백업 수행
- vCenter Server 시스템에서 TLS 버전을 사용하지 않도록 설정
- ESXi 호스트에서 TLS 버전을 사용하지 않도록 설정
- Platform Services Controller 시스템에서 TLS 버전을 사용하지 않도록 설정
- TLS 구성 변경 내용 되돌리기
- vSphere Update Manager에서 TLS 버전을 사용하지 않도록 설정

TLS 버전을 사용하지 않도록 설정 가능한 포트

vSphere 환경에서 TLS 구성 유틸리티를 실행하는 경우 vCenter Server, Platform Services Controller 및 ESXi 호스트에서 TLS를 사용하는 포트 전반에 걸쳐 TLS를 사용하지 않도록 설정할 수 있습니다. TLS 1.0이나 TLS 1.0과 TLS 1.1 모두를 사용하지 않도록 설정할 수 있습니다.

다음 표에 이러한 포트가 정리되어 있습니다. 여기에 포함되지 않은 포트는 이 유틸리티의 영향을 받지 않습니다.

표 10-1. TLS 구성 유틸리티의 영향을 받는 vCenter Server 및 Platform Services Controller

서비스	Windows에서의 이름	Linux에서의 이름	포트
VMware HTTP Reverse Proxy	rhttpproxy	vmware-rhttpproxy	443
VMware Directory Service	VMwareDirectoryService	vmldird	636
VMware Syslog Collector(*)	vmwaresyslogcollector(*)	rsyslogd	1514
vSphere Auto Deploy Waiter	vmware-autodeploy-waiter	vmware-rbd-watchdog	6501 6502
VMware Secure Token Service	VMwareSTS	vmware-stsd	7444
vSphere Update Manager 서비스(**)	vmware-ufad-vci(**)	vmware-updatemgr	8084 9087
vSphere Web Client	vspherewebclientsvc	vsphere-client	9443
VMware Directory Service	VMwareDirectoryService	vmldird	11712

(*) TLS는 이러한 서비스에 대한 암호 목록으로 제어됩니다. 세부적인 관리는 불가능합니다. TLS 1.2만 지원되거나 모든 TLS 1.x 버전이 지원됩니다.

(**) vCenter Server Appliance에서는 vSphere Update Manager가 vCenter Server와 동일한 시스템에 있습니다. Windows의 vCenter Server에서는 구성 파일을 편집하여 TLS를 구성합니다. [vSphere Update Manager](#)에서 TLS 버전을 사용하지 않도록 설정의 내용을 참조하십시오.

표 10-2. TLS 구성 유틸리티의 영향을 받는 ESXi 포트

서비스	서비스 이름	포트
VMware HTTP Reverse Proxy 및 호스트 데몬	Hostd	443
VMware vSAN VASA 벤더 제공자	vSANVP	8080
VMware 장애 도메인 관리자	FDM	8182
IO 필터용 VMware vSphere API	ioFilterVPsServer	9080
VMware 인증 데몬	vmware-authd	902

참고 사항 및 주의 사항

- vCenter Server로 관리되는 기존 ESXi 호스트는 사용하도록 설정된 TLS 버전(TLS 1.1과 TLS 1.2 또는 TLS 1.2만)을 지원합니다. vCenter Server 6.5에서 TLS 버전을 사용하지 않도록 설정하면, vCenter Server에서 더 이상 기존 ESXi 호스트 5.x 및 6.0 호스트를 관리할 수 없습니다. 이러한 호스트를 TLS 1.1 또는 TLS 1.2를 지원하는 버전으로 업그레이드합니다.

- 외부 Microsoft SQL Server 또는 외부 Oracle 데이터베이스에는 TLS 1.2 단독 연결을 사용할 수 없습니다.
- Windows Server 2008에서 실행되는 vCenter Server 또는 Platform Services Controller 인스턴스에서는 TLS 1.0을 사용하지 않도록 설정하지 마십시오. Windows 2008은 TLS 1.0만 지원합니다. Microsoft TechNet 문서 "서버 역할 및 기술 가이드"의 "TLS/SSL 설정"을 참조하십시오.
- 다음과 같은 경우 TLS 구성 변경 내용을 적용한 후 호스트 서비스를 다시 시작해야 합니다.
 - ESXi 호스트에 변경 내용을 직접 적용하는 경우
 - 호스트 프로파일을 사용하여 클러스터 구성을 통해 변경 내용을 적용하는 경우

vSphere에서 TLS 버전을 사용하지 않도록 설정

TLS 버전을 사용하지 않도록 설정하는 프로세스는 여러 단계로 이루어집니다. 올바른 순서로 TLS 버전을 사용하지 않도록 설정하면 이 프로세스를 진행하는 동안 환경이 중단 없이 운영됩니다.

- 1 Windows 환경에서 vSphere Update Manager를 사용하고 vSphere Update Manager가 별도의 시스템에 있는 경우 구성 파일을 편집하여 프로토콜을 명시적으로 사용하지 않도록 설정합니다.
vSphere Update Manager에서 TLS 버전을 사용하지 않도록 설정의 내용을 참조하십시오.
vCenter Server Appliance의 vSphere Update Manager는 항상 vCenter Server 시스템에 포함되어 있으며 스크립트를 통해 해당 포트가 업데이트됩니다.
- 2 vCenter Server 및 Platform Services Controller에서 TLS 구성 유틸리티를 설치합니다. 내장된 Platform Services Controller를 환경에서 사용하는 경우 vCenter Server에만 유틸리티를 설치합니다.
- 3 vCenter Server에서 유틸리티를 실행합니다.
- 4 vCenter Server로 관리되는 각 ESXi 호스트에서 이 유틸리티를 실행합니다. 각 호스트 또는 클러스터의 모든 호스트에 대해 이 작업을 수행할 수 있습니다.
- 5 하나 이상의 Platform Services Controller 인스턴스를 환경에서 사용하는 경우 각 인스턴스에서 유틸리티를 실행합니다.

사전 요구 사항

이 구성은 vSphere 6.0 U3을 실행하는 시스템과 vSphere 6.5를 실행하는 시스템에서 수행합니다. 다음 두 가지 중에 선택할 수 있습니다.

- TLS 1.0을 사용하지 않도록 설정하고 TLS 1.1과 TLS 1.2를 사용하도록 설정
- TLS 1.0과 TLS 1.1을 사용하지 않도록 설정하고 TLS 1.2를 사용하도록 설정

TLS 구성 유틸리티 설치

MyVMware.com에서 TLS 구성 유틸리티를 다운로드하여 로컬 시스템에 설치할 수 있습니다. 설치 후에는 두 개의 스크립트를 사용할 수 있습니다. 스크립트 하나는 vCenter Server 및 Platform Services Controller 구성용이고 또 하나는 ESXi 구성용입니다.

vCenter Server Appliance에서 스크립트를 통해 vSphere Update Manager 포트가 업데이트됩니다. vCenter Server에서 vSphere Update Manager 구성 파일을 편집합니다. [vSphere Update Manager](#)에서 TLS 버전을 사용하지 않도록 설정의 내용을 참조하십시오.

사전 요구 사항

스크립트를 다운로드하려면 MyVMware 계정이 필요합니다.

절차

- 1 MyVMware 계정에 로그인하고 vSphere로 이동합니다.
- 2 라이선스가 있는 제품과 제품 버전을 찾아 VMware vCenter Server를 선택하고 **다운로드**로 이동을 클릭합니다.
- 3 VMware vSphere TLS Configurator를 선택하고 다음 파일을 다운로드합니다.

운영 체제	파일
Windows	VMware-vSphereTlsReconfigurator-version-build_number.x86_64.msi
Linux	VMware-vSphereTlsReconfigurator-version-build_number.x86_64.rpm

4 파일을 vCenter Server에 업로드하고 스크립트를 설치합니다.

외부 Platform Services Controller를 사용하는 환경에서는 Platform Services Controller에도 파일을 업로드합니다.

운영 체제	절차
Windows	<ol style="list-style-type: none"> 관리자 권한을 가진 사용자로 로그인합니다. 방금 다운로드한 VMware-vSphereTlsReconfigurator-version-build_number.x86_64.msi 파일을 복사합니다. MSI 파일을 설치합니다.
Linux	<ol style="list-style-type: none"> SSH를 사용하여 장치에 연결하고 스크립트를 실행할 수 있는 권한이 있는 사용자로 로그인합니다. SCP 클라이언트를 사용하여 VMware-vSphereTlsReconfigurator-version-build_number.x86_64.rpm 파일을 장치로 복사합니다. Bash 셸이 현재 사용되지 않는 경우 다음 명령을 실행합니다. <div style="background-color: #f0f0f0; padding: 5px; margin: 5px 0;"> <pre>shell.set --enabled true shell</pre> </div> 업로드된 rpm 파일이 있는 디렉토리로 이동하여 다음 명령을 실행합니다. <div style="background-color: #f0f0f0; padding: 5px; margin: 5px 0;"> <pre>rpm -Uvh VMware-vSphereTlsReconfigurator-version-build_number.x86_64.rpm</pre> </div>

결과

설치가 완료된 후 다음 위치에서 스크립트를 찾을 수 있습니다.

운영 체제	위치
Windows	<ul style="list-style-type: none"> ■ C:\Program Files\VMware\CIS\vSphereTlsReconfigurator\VcTlsReconfigurator ■ C:\Program Files\VMware\CIS\vSphereTlsReconfigurator\EsxTlsReconfigurator
Linux	<ul style="list-style-type: none"> ■ /usr/lib/vmware-vSphereTlsReconfigurator/VcTlsReconfigurator ■ /usr/lib/vmware-vSphereTlsReconfigurator/EsxTlsReconfigurator

선택적 수동 백업 수행

TLS 구성 유틸리티는 스크립트를 통해 vCenter Server, Platform Services Controller 또는 vSphere Update Manager가 수정될 때마다 백업을 수행합니다. 특정 디렉토리에 백업을 수행해야 할 경우 수동 백업을 수행할 수 있습니다.

기본 디렉토리는 Windows 및 장치에 따라 다릅니다.

운영 체제	백업 디렉토리
Windows	c:\users\current_user\appdata\local\temp\yearmonthdayTtime
Linux	/tmp/yearmonthdayTtime

절차

- 1 디렉토리를 vSphereTlsReconfigurator로 변경한 후 VcTlsReconfigurator 하위 디렉토리로 변경합니다.

운영 체제	명령
Windows	C:\Program Files\VMware\CIS\vsphereTlsReconfigurator\ cd VcTlsReconfigurator
Linux	cd /usr/lib/vmware-vSphereTlsReconfigurator/ cd VcTlsReconfigurator

- 2 특정 디렉토리에 백업을 수행하려면 다음 명령을 실행합니다.

운영 체제	명령
Windows	<i>directory_path</i> \VcTlsReconfigurator> reconfigureVc backup -d <i>backup_directory_path</i>
Linux	<i>directory_path</i> /VcTlsReconfigurator> ./ reconfigureVc backup -d <i>backup_directory_path</i>

- 3 백업이 성공적으로 완료되었는지 확인합니다.

백업에 성공하면 다음 예와 유사하게 표시됩니다.

```
vCenter Transport Layer Security reconfigurator, version=6.0.0, build=8482376
For more information, refer to the following article: https://kb.vmware.com/kb/2148819
Log file: "C:\ProgramData\VMware\vCenterServer\logs\vmware\vsphere-
TlsReconfigurator\VcTlsReconfigurator.log".
===== Backing up vCenter Server TLS configuration =====
Using backup directory: c:\users\admini~1\appdata\local\temp\1\20170202T054311
Backing up: vmsyslogcollector
Backing up: vspherewebclientsvc
Backing up: vmware-autodeploy-waiter
Backing up: rhttpproxy
Backing up: VMwareSTS
Backing up: VMWareDirectoryService
```

- 4 (선택 사항) 이후에 복원을 수행해야 할 경우 다음 명령을 실행할 수 있습니다.

```
reconfigure restore -d tmp directory or custom backup directory path
```

vCenter Server 시스템에서 TLS 버전을 사용하지 않도록 설정

TLS 구성 유틸리티를 사용하여 vCenter Server 시스템에서 TLS 버전을 사용하지 않도록 설정할 수 있습니다. 이 프로세스 중에 TLS 1.1과 TLS 1.2를 모두 사용하도록 설정하거나 TLS 1.2만 사용하도록 설정할 수 있습니다.

사전 요구 사항

vCenter Server에서 관리하는 호스트와 서비스가 사용하도록 설정되어 있는 TLS 버전을 사용하여 통신할 수 있는지 확인합니다. TLS 1.0만 사용하여 통신하는 제품의 경우 연결이 불가능합니다.

절차

- 1 스크립트를 실행할 수 있는 사용자로 vCenter Server 시스템에 로그인하고 스크립트가 있는 디렉토리로 이동합니다.

운영 체제	명령
Windows	<code>cd C:\Program Files\VMware\CIS\vsphereTlsReconfigurator\VcTlsReconfigurator</code>
Linux	<code>cd /usr/lib/vmware-vSphereTlsReconfigurator/VcTlsReconfigurator</code>

- 2 운영 체제와 사용할 TLS 버전에 따라 명령을 실행합니다.

- TLS 1.0을 사용하지 않도록 설정하고 TLS 1.1과 TLS 1.2를 모두 사용하도록 설정하려면 다음 명령을 실행합니다.

운영 체제	명령
Windows	<code>directory_path\VcTlsReconfigurator> reconfigureVc update -p TLSv1.1 TLSv1.2</code>
Linux	<code>directory_path/VcTlsReconfigurator> ./reconfigureVc update -p TLSv1.1 TLSv1.2</code>

- TLS 1.0과 TLS 1.1을 사용하지 않도록 설정하고 TLS 1.2만 사용하도록 설정하려면 다음 명령을 실행합니다.

운영 체제	명령
Windows	<code>directory_path\VcTlsReconfigurator> reconfigureVc update -p TLSv1.2</code>
Linux	<code>directory_path/VcTlsReconfigurator> ./reconfigureVc update -p TLSv1.2</code>

- 3 다른 vCenter Server 시스템이 환경에 포함되어 있는 경우 각 vCenter Server 시스템에서 이 프로세스를 반복합니다.
- 4 각 ESXi 호스트와 각 Platform Services Controller에서 이 구성을 반복합니다.

ESXi 호스트에서 TLS 버전을 사용하지 않도록 설정

TLS 구성 유틸리티를 사용하여 ESXi 호스트에서 TLS 버전을 사용하지 않도록 설정할 수 있습니다. 이 프로세스 중에 TLS 1.1과 TLS 1.2를 모두 사용하도록 설정하거나 TLS 1.2만 사용하도록 설정할 수 있습니다. ESXi 호스트의 경우 vSphere 환경의 나머지 구성 요소와 다른 스크립트를 사용합니다.

참고 이 스크립트는 -p 옵션을 지정하지 않는 한 TLS 1.0과 TLS 1.1을 모두 사용하지 않도록 설정합니다.

사전 요구 사항

ESXi 호스트와 연결된 모든 제품 또는 서비스가 TLS 1.1 또는 TLS 1.2를 사용하여 통신할 수 있는지 확인합니다. TLS 1.0만 사용하여 통신하는 제품의 경우 연결이 끊깁니다.

절차

- 1 스크립트를 실행할 수 있는 사용자로 vCenter Server 호스트에 로그인하고 스크립트가 있는 디렉토리로 이동합니다.

운영 체제	명령
Windows	C:\Program Files\VMware\CIS\vSphereTLSReconfigurator\EsxTlsReconfigurator
Linux	/usr/lib/vmware-vSphereTlsReconfigurator/EsxTlsReconfigurator

- 2 클러스터의 모든 호스트에서 TLS를 사용하지 않도록 설정하려면 다음 명령 중 하나를 실행합니다.

- 클러스터에 있는 모든 호스트에서 TLS 1.0을 사용하지 않도록 설정하고 TLS 1.1과 TLS 1.2를 모두 사용하도록 설정하려면 다음 명령을 실행합니다.

운영 체제	명령
Windows	reconfigureEsx vCenterCluster -c Cluster_Name -u Administrative_User -p TLSv1.1 TLSv1.2
Linux	./reconfigureEsx vCenterCluster -c Cluster_Name -u Administrative_User -p TLSv1.1 TLSv1.2

- 클러스터에 있는 모든 호스트에서 TLS 1.0과 TLS 1.1을 사용하지 않도록 설정하고 TLS 1.2만 사용하도록 설정하려면 다음 명령을 실행합니다.

운영 체제	명령
Windows	reconfigureEsx vCenterCluster -c Cluster_Name -u Administrative_User -p TLSv1.2
Linux	./reconfigureEsx vCenterCluster -c Cluster_Name -u Administrative_User -p TLSv1.2

3 개별 호스트에서 TLS를 사용하지 않도록 설정하려면 각 호스트에서 다음 명령 중 하나를 실행합니다.

- 각 호스트에서 TLS 1.0을 사용하지 않도록 설정하고 TLS 1.1과 TLS 1.2를 모두 사용하도록 설정하려면 다음 명령을 실행합니다.

운영 체제	명령
Windows	<code>reconfigureEsx vCenterHost -h <ESXi_Host_Name> -u Administrative_User -p TLSv1.1 TLSv1.2</code>
Linux	<code>./reconfigureEsx vCenterHost -h <ESXi_Host_Name> -u Administrative_User -p TLSv1.1 TLSv1.2</code>

- 각 호스트에서 TLS 1.0과 TLS 1.1을 사용하지 않도록 설정하고 TLS 1.2만 사용하도록 설정하려면 다음 명령을 실행합니다.

운영 체제	명령
Windows	<code>reconfigureEsx vCenterHost -h <ESXi_Host_Name> -u Administrative_User -p TLSv1.2</code>
Linux	<code>./reconfigureEsx vCenterHost -h <ESXi_Host_Name> -u Administrative_User -p TLSv1.2</code>

4 ESXi 호스트를 재부팅하여 TLS 프로토콜 변경을 완료합니다.

Platform Services Controller 시스템에서 TLS 버전을 사용하지 않도록 설정

하나 이상의 Platform Services Controller 시스템이 환경에 포함되어 있는 경우 TLS 구성 유틸리티를 사용하여 지원되는 TLS 버전을 변경할 수 있습니다.

환경에서 내장된 Platform Services Controller만 사용하는 경우 이 작업을 수행할 필요가 없습니다.

참고 각 vCenter Server 시스템이 호환되는 TLS 버전을 실행하는지 반드시 확인한 후에 이 작업을 진행하십시오. vCenter Server 6.0.x 또는 5.5.x 인스턴스가 vCenter Server에 연결되어 있는 경우 TLS 버전을 사용하지 않도록 설정하면 해당 인스턴스와 Platform Services Controller의 통신이 중지됩니다.

TLS 1.0 및 TLS 1.1을 사용하지 않도록 설정하고 TLS 1.2를 계속 사용하도록 설정하거나 TLS 1.0만 사용하지 않도록 설정하고 TLS 1.1과 TLS 1.2를 계속 사용하도록 설정할 수 있습니다.

사전 요구 사항

Platform Services Controller가 연결하는 호스트와 서비스가 지원되는 프로토콜을 사용하여 통신할 수 있는지 확인합니다. 인증과 인증서 관리가 Platform Services Controller에서 처리되기 때문에 영향을 받을 수 있는 서비스를 신중하게 고려해야 합니다. 지원되지 않는 프로토콜만 사용하여 통신하는 서비스의 경우 연결이 불가능합니다.

절차

- 1 스크립트를 실행할 수 있는 사용자로 Platform Services Controller에 로그인하고 스크립트가 있는 디렉토리로 이동합니다.

운영 체제 명령

Windows `cd C:\Program Files\VMware\CIS\vsphereTlsReconfigurator\VcTlsReconfigurator`

Linux `cd /usr/lib/vmware-vsphereTlsReconfigurator/VcTlsReconfigurator`

- 2 Platform Services Controller에 대한 작업은 Windows 또는 Platform Services Controller 장치에서 수행할 수 있습니다.

- TLS 1.0을 사용하지 않도록 설정하고 TLS 1.1과 TLS 1.2를 모두 사용하도록 설정하려면 다음 명령을 실행합니다.

운영 체제 명령

Windows `directory_path\VcTlsReconfigurator> reconfigureVc update -p TLSv1.1 TLSv1.2`

Linux `directory_path\VcTlsReconfigurator> ./reconfigureVc update -p TLSv1.1 TLSv1.2`

- TLS 1.0과 TLS 1.1을 사용하지 않도록 설정하고 TLS 1.2만 사용하도록 설정하려면 다음 명령을 실행합니다.

운영 체제 명령

Windows `directory_path\VcTlsReconfigurator> reconfigureVc update -p TLSv1.2`

Linux `directory_path\VcTlsReconfigurator> ./reconfigureVc update -p TLSv1.2`

- 3 다른 Platform Services Controller 시스템이 환경에 포함되어 있는 경우 이 프로세스를 반복합니다.

TLS 구성 변경 내용 되돌리기

TLS 구성 유틸리티를 사용하여 구성 변경 내용을 되돌릴 수 있습니다. 변경 내용을 되돌리면, 시스템에서 TLS 구성 유틸리티를 통해 사용하지 않도록 설정한 프로토콜이 사용하도록 설정됩니다.

이전에 구성을 백업한 경우에만 복구를 수행할 수 있습니다. ESXi 호스트에는 변경 내용 되돌리기가 지원되지 않습니다.

다음 순서로 복구를 수행합니다.

- 1 vSphere Update Manager.

Windows 시스템에서 별도의 vSphere Update Manager 인스턴스를 실행하는 환경에서는 먼저 vSphere Update Manager를 업데이트해야 합니다.

- 2 vCenter Server

3 Platform Services Controller

절차

- 1 Windows 시스템 또는 장치에 연결합니다.
- 2 변경 내용을 되돌리려는 시스템에 로그인합니다.

운영 체제 절차

- Windows
- 1 관리자 권한을 가진 사용자로 로그인합니다.
 - 2 VcTlsReconfigurator 디렉토리로 이동합니다.

```
cd C:\Program Files\VMware\CIS\vsphereTlsReconfigurator\VcTlsReconfigurator
```

- Linux
- 1 SSH를 사용하여 장치에 연결하고 스크립트를 실행할 수 있는 권한이 있는 사용자로 로그인합니다.
 - 2 Bash 셸이 현재 사용되지 않는 경우 다음 명령을 실행합니다.

```
shell.set --enabled true
shell
```

- 3 VcTlsReconfigurator 디렉토리로 이동합니다.

```
cd /usr/lib/vmware-vSphereTlsReconfigurator/VcTlsReconfigurator
```

- 3 이전 백업을 검토합니다.

운영 체제 절차

Windows

```
C:\ProgramData\VMware\vCenterServer\logs\vsphere-  
TlsReconfigurator\VcTlsReconfigurator.log
```

출력은 다음 예와 비슷합니다.

```
c:\users\username\appdata\local\temp\20161108T161539  
c:\users\username\appdata\local\temp\20161108T171539
```

Linux

```
grep "backup directory" /var/log/vmware/vSphere-TlsReconfigurator/  
VcTlsReconfigurator.log
```

출력은 다음 예와 비슷합니다.

```
2016-11-17T17:29:20.950Z INFO Using backup directory: /tmp/20161117T172920  
2016-11-17T17:32:59.019Z INFO Using backup directory: /tmp/20161117T173259
```

- 4 복원을 수행하려면 다음 명령 중 하나를 실행합니다.

운영 체제 절차

Windows `reconfigureVc restore -d Directory_path_from_previous_step`

예:

```
reconfigureVc restore -d c:\users\username\appdata\local\temp\20161108T171539
```

Linux `reconfigureVc restore -d Directory_path_from_previous_step`

예:

```
reconfigureVc restore -d /tmp/20161117T172920
```

- 5 다른 vCenter Server 인스턴스에서 이 절차를 반복합니다.
- 6 다른 Platform Services Controller 인스턴스에서 이 절차를 반복합니다.

vSphere Update Manager에서 TLS 버전을 사용하지 않도록 설정

vSphere Update Manager 6.0 업데이트 3 이상에서는 기본적으로 TLS 프로토콜 버전 1.0, 1.1 및 1.2가 모두 사용하도록 설정되어 있습니다. TLS 버전 1.0 및 TLS 버전 1.1은 사용하지 않도록 설정할 수 있지만 TLS 버전 1.2는 사용하지 않도록 설정할 수 없습니다.

TLS 구성 유틸리티를 사용하여 다른 서비스에 대한 TLS 프로토콜 구성을 관리할 수 있습니다. 그러나 vSphere Update Manager에 대해서는 TLS 프로토콜을 수동으로 재구성해야 합니다.

TLS 프로토콜 구성을 수정하려면 다음 작업을 수행해야 할 수 있습니다.

- TLS 버전 1.1 및 TLS 버전 1.2는 계속 사용하도록 설정하고 TLS 버전 1.0을 사용하지 않도록 설정
- TLS 버전 1.2는 계속 사용하도록 설정하고 TLS 버전 1.0 및 TLS 버전 1.1을 사용하지 않도록 설정
- 사용하지 않도록 설정된 TLS 프로토콜 버전을 다시 사용하도록 설정

Update Manager 포트 9087에 대해 이전 TLS 버전을 사용하지 않도록 설정

jetty-vum-ssl.xml 구성 파일을 수정하여 포트 9087에 대해 이전 TLS 버전을 사용하지 않도록 설정할 수 있습니다. 포트 8084의 경우 프로세스가 이와 다릅니다.

참고 특정 TLS 버전을 사용하지 않도록 설정하기 전에, vSphere Update Manager와 통신하는 서비스에 서 해당 버전을 사용하지 않는지 확인합니다.

사전 요구 사항

vSphere Update Manager 서비스를 중지합니다. "VMware vSphere Update Manager 설치 및 관리" 설명서를 참조하십시오.

절차

- 1 vSphere Update Manager 서비스를 중지합니다.
- 2 Update Manager 설치 디렉토리로 이동합니다. 이는 vSphere 6.0과 vSphere 6.5에서 서로 다릅니다.

버전	위치
vSphere 6.0	C:\Program Files (x86)\VMware\Infrastructure\Update Manager
vSphere 6.5	C:\Program Files\VMware\Infrastructure\Update Manager

- 3 jetty-vum-ssl.xml 파일의 백업을 생성하고 백업 파일을 엽니다.
- 4 파일을 변경하여 이전 TLS 버전을 사용하지 않도록 설정합니다.

옵션	설명
TLS 1.0을 사용하지 않도록 설정하고 TLS 1.1 및 TLS 1.2를 계속 사용하도록 설정합니다.	<pre><Set name="ExcludeProtocols"> <Array type="java.lang.String"> <Item>TLSv1</Item> </Array> </Set></pre>
TLS 1.0과 TLS 1.1을 사용하지 않도록 설정하고 TLS 1.2를 계속 사용하도록 설정합니다.	<pre><Set name="ExcludeProtocols"> <Array type="java.lang.String"> <Item>TLSv1</Item> <Item>TLSv1.1</Item> </Array> </Set></pre>

- 5 파일을 저장합니다.
- 6 vSphere Update Manager 서비스를 다시 시작합니다.

Update Manager 포트 8084에 대해 이전 TLS 버전을 사용하지 않도록 설정

vci-integrity.xml 구성 파일을 수정하여 포트 8084에 대해 이전 TLS 버전을 사용하지 않도록 설정할 수 있습니다. 포트 9087의 경우 프로세스가 이와 다릅니다.

참고 특정 TLS 버전을 사용하지 않도록 설정하기 전에, vSphere Update Manager와 통신하는 서비스에 해당 버전을 사용하지 않는지 확인합니다.

사전 요구 사항

vSphere Update Manager 서비스를 중지합니다. "VMware vSphere Update Manager 설치 및 관리" 설명서를 참조하십시오.

절차

- 1 vSphere Update Manager 서비스를 중지합니다.

- 2 Update Manager 설치 디렉토리로 이동합니다. 이는 6.0과 6.5에서 서로 다릅니다.

버전	위치
vSphere 6.0	C:\Program Files (x86)\VMware\Infrastructure\Update Manager
vSphere 6.5	C:\Program Files\VMware\Infrastructure\Update Manager

- 3 vci-integrity.xml 파일의 백업을 생성하고 백업 파일을 엽니다.

- 4 <sslOptions> 태그를 vci-integrity.xml 파일에 추가합니다.

```
<ssl>
  <handshakeTimeoutMs>120000</handshakeTimeoutMS>
  <sslOptions>sslOptions_value</sslOptions>
</ssl>

<ssl>
  <privateKey>ssl/rui.key</privateKey>
  <certificate>ssl/rui.crt</certificate>
  <sslOptions>sslOptions_value</sslOptions>
</ssl>
```

- 5 사용하지 않도록 설정할 TLS 버전에 따라 <sslOptions> 태그에 다음 십진수 값 중 하나를 사용합니다.

- TLSv1.0만 사용하지 않도록 설정하려면 십진수 값 117587968을 사용합니다.
- TLSv1.0 및 TLSv1.1을 사용하지 않도록 설정하려면 십진수 값 386023424를 사용합니다.

- 6 파일을 저장합니다.

- 7 vSphere Update Manager 서비스를 다시 시작합니다.

Update Manager 포트 9087에 대해 사용하지 않도록 설정된 TLS 버전을 다시 사용하도록 설정

Update Manager 포트 9087에 TLS 버전을 사용하지 않도록 설정하였는데 문제가 발생할 경우 해당 버전을 다시 사용하도록 설정할 수 있습니다. 포트 8084를 다시 사용하도록 설정하는 프로세스는 이와 다릅니다.

이전 버전의 TLS를 다시 사용하도록 설정하면 보안에 영향을 미칩니다.

절차

- 1 vSphere Update Manager 서비스를 중지합니다.
- 2 Update Manager 설치 디렉토리로 이동합니다. 이는 6.0과 6.5에서 서로 다릅니다.

버전	위치
vSphere 6.0	C:\Program Files (x86)\VMware\Infrastructure\Update Manager
vSphere 6.5	C:\Program Files\VMware\Infrastructure\Update Manager

- 3 jetty-vum-ssl.xml 파일의 백업을 생성하고 백업 파일을 엽니다.
- 4 사용하도록 설정할 TLS 프로토콜 버전에 해당하는 TLS 태그를 제거합니다.
예를 들어 TLSv1.1을 사용하도록 설정하려면 jetty-vum-ssl.xml 파일에서 <Item>TLSv1.1</Item>을 제거합니다.
- 5 파일을 저장합니다.
- 6 vSphere Update Manager 서비스를 다시 시작합니다.

Update Manager 포트 8084에 대해 사용하지 않도록 설정된 TLS 버전을 다시 사용하도록 설정

Update Manager 포트 8084에 TLS 버전을 사용하지 않도록 설정하였는데 문제가 발생할 경우 해당 버전을 다시 사용하도록 설정할 수 있습니다. 포트 9087의 경우 프로세스가 이와 다릅니다.

이전 버전의 TLS를 다시 사용하도록 설정하면 보안에 영향을 미칩니다.

절차

- 1 vSphere Update Manager 서비스를 중지합니다.
- 2 Update Manager 설치 디렉토리로 이동합니다. 이는 6.0과 6.5에서 서로 다릅니다.

버전	위치
vSphere 6.0	C:\Program Files (x86)\VMware\Infrastructure\Update Manager
vSphere 6.5	C:\Program Files\VMware\Infrastructure\Update Manager

- 3 vci-integrity.xml 파일의 백업을 생성하고 백업 파일을 엽니다.
- 4 <sslOptions> 태그에 사용되는 십진수 값을 변경하거나 이 태그를 삭제하여 모든 TLS 버전을 허용합니다.
 - TLS 1.1을 사용하도록 설정하고 TLS 1.0은 계속 사용하지 않도록 설정하려면 십진수 값 117587968을 사용합니다.
 - TLS 1.1과 TLS 1.0을 모두 다시 사용하도록 설정하려면 태그를 제거합니다.
- 5 파일을 저장합니다.
- 6 vSphere Update Manager 서비스를 다시 시작합니다.

다음 표에는 기본 권한이 나와 있으며, 이러한 권한이 역할에 대해 선택되면 사용자와 쌍을 이루어 개체에 할당될 수 있습니다. 이 부록의 표에서 VC는 vCenter Server를 나타내고 HC는 호스트 클라이언트, 독립형 ESXi 또는 Workstation 호스트를 나타냅니다.

사용 권한을 설정할 때는 모든 개체 유형이 각 특정 작업에 적절한 권한으로 설정되어 있는지 확인합니다. 일부 작업에는 조작할 개체에 대한 액세스 권한 외에도 루트 폴더나 상위 폴더 수준의 액세스 권한이 필요합니다. 또한 상위 폴더 및 관련 개체 수준의 액세스 또는 성능 권한이 필요한 작업도 있습니다.

vCenter Server 확장을 통해 여기에 나열되어 있지 않은 추가 권한을 정의할 수도 있습니다. 이러한 권한에 대한 자세한 내용은 확장 설명서를 참조하십시오.

본 장은 다음 항목을 포함합니다.

- 정보 권한
- Auto Deploy 및 이미지 프로파일 권한
- 인증서 권한
- 콘텐츠 라이브러리 권한
- 데이터 센터 권한
- 데이터스토어 권한
- 데이터스토어 클러스터 권한
- Distributed Switch 권한
- ESX Agent Manager 권한
- 확장 권한
- 폴더 권한
- 글로벌 권한
- 호스트 CIM 권한
- 호스트 구성 권한
- 호스트 인벤토리
- 호스트 로컬 작업 권한

- 호스트 vSphere 복제 권한
- 호스트 프로파일 권한
- Inventory Service 제공자 권한
- Inventory Service 태그 지정 권한
- 네트워크 권한
- 성능 권한
- 사용 권한에 대한 권한
- 프로파일 기반 스토리지 권한
- 리소스 권한
- 스케줄링된 작업 권한
- 세션 권한
- 스토리지 보기 권한
- 작업 권한
- 전송 서비스 권한
- VRM 정책 권한
- 가상 시스템 구성 권한
- 가상 시스템 게스트 작업 권한
- 가상 시스템 상호 작용 권한
- 가상 시스템 인벤토리 권한
- 가상 시스템 프로비저닝 권한
- 가상 시스템 서비스 구성 권한
- 가상 시스템 스냅샷 관리 권한
- 가상 시스템 vSphere 복제 권한
- dvPort 그룹 권한
- vApp 권한
- vServices 권한

경보 권한

경보 권한은 인벤토리 개체에 대한 경보를 생성하고 수정하고 응답하는 기능을 제어합니다.

계층의 서로 다른 수준에서 이 권한을 설정할 수 있습니다. 예를 들어 폴더 수준에서 권한을 설정하는 경우 폴더 내 하나 이상의 개체로 권한을 전파할 수 있습니다. 필수 열에 나열된 개체에는 직접 또는 상속을 통해 권한이 설정되어 있어야 합니다.

표 11-1. 경보 권한

권한 이름	설명	필수
경보.경보 승인	트리거된 모든 경보에 대한 경보 작업을 모두 표시하지 않을 수 있습니다.	경보가 정의된 개체
경보.경보 생성	새 경보를 생성할 수 있습니다. 사용자 지정 작업을 포함하는 경보를 만드는 경우 사용자가 경보를 만들 때 해당 작업을 수행할 수 있는 권한이 확인됩니다.	경보가 정의된 개체
경보.경보 작업 사용 안 함	경보가 트리거된 후에 경보 작업의 발생을 중지할 수 있습니다. 경보를 사용하지 않도록 설정하지는 않습니다.	경보가 정의된 개체
경보.경보 수정	경보의 속성을 변경할 수 있습니다.	경보가 정의된 개체
경보.경보 제거	경보를 삭제할 수 있습니다.	경보가 정의된 개체
경보.경보 상태 설정	구성된 이벤트 경보의 상태를 변경할 수 있습니다. 상태는 정상 , 주의 또는 경고 로 변경될 수 있습니다.	경보가 정의된 개체

Auto Deploy 및 이미지 프로파일 권한

Auto Deploy 권한은 Auto Deploy 규칙에 대해 서로 다른 작업을 수행할 수 있는 사람과 호스트를 연결할 수 있는 사람을 제어합니다. 또한 Auto Deploy 권한을 사용하여 이미지 프로파일을 생성하거나 편집할 수 있는 사람을 제어할 수도 있습니다.

아래 표에서는 Auto Deploy 규칙과 규칙 집합을 관리할 수 있는 사람과 이미지 프로파일을 생성하고 편집할 수 있는 사람을 결정하는 권한을 설명합니다. "vSphere 설치 및 설정"의 내용을 참조하십시오.

계층의 서로 다른 수준에서 이 권한을 설정할 수 있습니다. 예를 들어 폴더 수준에서 권한을 설정하는 경우 폴더 내 하나 이상의 개체로 권한을 전파할 수 있습니다. 필수 열에 나열된 개체에는 직접 또는 상속을 통해 권한이 설정되어 있어야 합니다.

표 11-2. Auto Deploy 권한

권한 이름	설명	필수
Auto Deploy.호스트.시스템 연결	사용자가 호스트와 시스템을 연결할 수 있습니다.	vCenter Server
Auto Deploy.이미지 프로파일 .생성	이미지 프로파일을 생성할 수 있습니다.	vCenter Server
Auto Deploy.이미지 프로파일 .편집	이미지 프로파일을 편집할 수 있습니다.	vCenter Server
Auto Deploy.규칙 .생성	Auto Deploy 규칙을 생성할 수 있습니다.	vCenter Server
Auto Deploy.규칙 .삭제	Auto Deploy 규칙을 삭제할 수 있습니다.	vCenter Server
Auto Deploy.규칙.편집	Auto Deploy 규칙을 편집할 수 있습니다.	vCenter Server
Auto Deploy.규칙 집합 .활성화	Auto Deploy 규칙 집합을 활성화할 수 있습니다.	vCenter Server
Auto Deploy.규칙 집합 .편집	Auto Deploy 규칙 집합을 편집할 수 있습니다.	vCenter Server

인증서 권한

인증서 권한은 ESXi 인증서를 관리할 수 있는 사용자를 제어합니다.

이 권한은 ESXi 호스트에 대한 인증서 관리를 수행할 수 있는 사용자를 결정합니다. vCenter Server 인증서 관리에 대한 자세한 내용은 [인증서 관리 작업에 필요한 권한](#)을 참조하십시오.

계층의 서로 다른 수준에서 이 권한을 설정할 수 있습니다. 예를 들어 폴더 수준에서 권한을 설정하는 경우 폴더 내 하나 이상의 개체로 권한을 전파할 수 있습니다. 필수 열에 나열된 개체에는 직접 또는 상속을 통해 권한이 설정되어 있어야 합니다.

표 11-3. 호스트 인증서 권한

권한 이름	설명	필수
인증서. 인증서 관리	ESXi 호스트에 대한 인증서 관리를 허용합니다.	vCenter Server

컨텐츠 라이브러리 권한

컨텐츠 라이브러리를 통해 가상 시스템 템플릿 및 vApp을 간단하고 효율적으로 관리할 수 있습니다. 컨텐츠 라이브러리 권한은 컨텐츠 라이브러리의 여러 기능을 누가 보고 관리할 수 있는지 제어합니다.

계층의 서로 다른 수준에서 이 권한을 설정할 수 있습니다. 예를 들어 폴더 수준에서 권한을 설정하는 경우 폴더 내 하나 이상의 개체로 권한을 전파할 수 있습니다. 필수 열에 나열된 개체에는 직접 또는 상속을 통해 권한이 설정되어 있어야 합니다.

표 11-4. 컨텐츠 라이브러리 권한

권한 이름	설명	필수
컨텐츠 라이브러리.라이브러리 항목 추가	라이브러리의 항목을 추가할 수 있습니다.	라이브러리
컨텐츠 라이브러리.로컬 라이브러리 생성	지정된 vCenter Server 시스템에 로컬 라이브러리를 생성할 수 있습니다.	vCenter Server
컨텐츠 라이브러리.구독 라이브러리 생성	구독 라이브러리를 생성할 수 있습니다.	vCenter Server
컨텐츠 라이브러리.라이브러리 항목 삭제	라이브러리 항목을 삭제할 수 있습니다.	라이브러리. 모든 라이브러리 항목에 전파하기 위한 이 사용 권한을 설정합니다.
컨텐츠 라이브러리.로컬 라이브러리 삭제	로컬 라이브러리를 삭제할 수 있습니다.	라이브러리
컨텐츠 라이브러리.구독 라이브러리 삭제	구독 라이브러리를 삭제할 수 있습니다.	라이브러리
컨텐츠 라이브러리.파일 다운로드	컨텐츠 라이브러리에서 파일을 다운로드할 수 있습니다.	라이브러리
컨텐츠 라이브러리.라이브러리 항목 편집	항목을 제거할 수 있습니다. 구독 라이브러리의 컨텐츠는 캐시되거나 캐시되지 않을 수 있습니다. 컨텐츠가 캐시된 경우 이 권한이 있으면 라이브러리 항목을 제거하여 릴리스할 수 있습니다.	라이브러리. 모든 라이브러리 항목에 전파하기 위한 이 사용 권한을 설정합니다.

표 11-4. 콘텐츠 라이브러리 권한 (계속)

권한 이름	설명	필수
콘텐츠 라이브러리.구독 라이브러리 제거	구독 라이브러리를 제거할 수 있습니다. 구독 라이브러리의 콘텐츠는 캐시되거나 캐시되지 않을 수 있습니다. 콘텐츠가 캐시된 경우 이 권한이 있으면 라이브러리를 제거하여 릴리스할 수 있습니다.	라이브러리
콘텐츠 라이브러리.스토리 지 가져오기	소스 파일 URL이 <code>ds://</code> 또는 <code>file://</code> 로 시작하는 경우 사용자가 라이브러리 항목을 가져올 수 있습니다. 콘텐츠 라이브러리 관리자에 대해서는 기본적으로 이 권한이 사용되지 않도록 설정되어 있습니다. 스토리지 URL에서 가져오기는 콘텐츠 가져오기를 의미하기 때문에 필요한 경우 및 현재 가져오기를 수행하는 사용자에게 대해 보안이 엄려되는 경우에만 이 권한을 사용하도록 설정합니다.	라이브러리
콘텐츠 라이브러리.구독 정보 검색	이 권한을 통해 솔루션 사용자 및 API는 URL, SSL 인증서 및 암호를 포함하여 원격 라이브러리의 구독 정보를 검색할 수 있습니다. 그 결과로 나타나는 구조에서 구독 구성이 성공적인지 SSL 오류와 같은 문제가 있는지 설명합니다.	라이브러리
콘텐츠 라이브러리.스토리 지 읽기	콘텐츠 라이브러리 스토리지를 읽을 수 있습니다.	라이브러리
콘텐츠 라이브러리.라이브러리 항목 동기화	라이브러리 항목을 동기화할 수 있습니다.	라이브러리. 모든 라이브러리 항목에 전파하기 위한 이 사용 권한을 설정합니다.
콘텐츠 라이브러리.구독 라이브러리 동기화	구독 라이브러리를 동기화할 수 있습니다.	라이브러리
콘텐츠 라이브러리.유형 검사	솔루션 사용자 또는 API는 콘텐츠 라이브러리 서비스의 유형 지원 플러그인을 검사할 수 있습니다.	라이브러리
콘텐츠 라이브러리.구성 설정 업데이트	구성 설정을 업데이트할 수 있습니다. 이 권한과 연결된 vSphere Web Client 사용자 인터페이스 요소는 없습니다.	라이브러리
콘텐츠 라이브러리.파일 업데이트	컨텐츠를 콘텐츠 라이브러리로 업로드할 수 있습니다. 또한 라이브러리 항목에서 파일을 제거할 수 있습니다.	라이브러리
콘텐츠 라이브러리.라이브러리 업데이트	콘텐츠 라이브러리를 업데이트할 수 있습니다.	라이브러리
콘텐츠 라이브러리.라이브러리 항목 업데이트	라이브러리 항목을 업데이트할 수 있습니다.	라이브러리. 모든 라이브러리 항목에 전파하기 위한 이 사용 권한을 설정합니다.
콘텐츠 라이브러리.로컬 라이브러리 업데이트	로컬 라이브러리를 업데이트할 수 있습니다.	라이브러리
콘텐츠 라이브러리.구독 라이브러리 업데이트	구독 라이브러리 속성을 업데이트할 수 있습니다.	라이브러리
콘텐츠 라이브러리.구성 설정 업데이트 보기	구성 설정을 볼 수 있습니다. 이 권한과 연결된 vSphere Web Client 사용자 인터페이스 요소는 없습니다.	라이브러리

데이터 센터 권한

데이터 센터 권한은 vSphere Web Client 인벤토리에서 데이터 센터를 생성하고 편집하는 기능을 제어합니다.

모든 데이터 센터 권한은 vCenter Server에서만 사용됩니다. **데이터 센터 생성** 권한은 데이터 센터 폴더나 루트 개체에 정의되어 있습니다. 다른 모든 데이터 센터 권한은 데이터 센터, 데이터 센터 폴더 또는 루트 개체와 쌍으로 구성되어 있습니다.

계층의 서로 다른 수준에서 이 권한을 설정할 수 있습니다. 예를 들어 폴더 수준에서 권한을 설정하는 경우 폴더 내 하나 이상의 개체로 권한을 전파할 수 있습니다. 필수 열에 나열된 개체에는 직접 또는 상속을 통해 권한이 설정되어 있어야 합니다.

표 11-5. 데이터 센터 권한

권한 이름	설명	필수
데이터 센터.데이터 센터 생성	새 데이터 센터를 생성할 수 있습니다.	데이터 센터 폴더 또는 루트 개체
데이터 센터.데이터 센터 이동	데이터 센터를 이동할 수 있습니다. 권한은 소스와 대상에 모두 있어야 합니다.	데이터 센터, 소스 및 대상
데이터 센터.네트워크 프로토콜 프로파일 구성	데이터 센터의 네트워크 프로파일을 구성할 수 있습니다.	데이터 센터
데이터 센터.IP 풀 할당 쿼리	IP 주소의 풀을 구성할 수 있도록 합니다.	데이터 센터
데이터 센터.데이터 센터 재구성	데이터 센터를 재구성할 수 있습니다.	데이터 센터
데이터 센터.IP 할당 해제	데이터 센터에 할당된 IP 할당을 해제할 수 있습니다.	데이터 센터
데이터 센터.데이터 센터 제거	데이터 센터를 제거할 수 있습니다. 이 작업을 수행하기 위한 권한을 얻으려면 개체와 상위 개체 모두에 이 권한이 할당되어야 합니다.	데이터 센터 및 상위 개체
데이터 센터.데이터 센터 이름 바꾸기	데이터 센터의 이름을 변경할 수 있습니다.	데이터 센터

데이터스토어 권한

데이터스토어 권한은 데이터스토어의 공간을 찾아보고, 관리하고, 할당하는 기능을 제어합니다.

계층의 서로 다른 수준에서 이 권한을 설정할 수 있습니다. 예를 들어 폴더 수준에서 권한을 설정하는 경우 폴더 내 하나 이상의 개체로 권한을 전파할 수 있습니다. 필수 열에 나열된 개체에는 직접 또는 상속을 통해 권한이 설정되어 있어야 합니다.

표 11-6. 데이터스토어 권한

권한 이름	설명	필수
데이터스토어.공간 할당	데이터스토어에서 가상 시스템, 스냅샷, 복제본 또는 가상 디스크를 위한 공간을 할당할 수 있습니다.	데이터스토어
데이터스토어.데이터스토어 찾아보기	데이터스토어의 파일을 찾아볼 수 있습니다.	데이터스토어
데이터스토어.데이터스토어 구성	데이터스토어를 구성할 수 있습니다.	데이터스토어
데이터스토어.하위 수준 파일 작업	데이터스토어 브라우저에서 읽기, 쓰기, 삭제 및 이름 변경 작업을 수행할 수 있습니다.	데이터스토어
데이터스토어.데이터스토어 이동	폴더 간에 데이터스토어를 이동할 수 있습니다. 권한은 소스와 대상에 모두 있어야 합니다.	데이터스토어, 소스 및 대상
데이터스토어.데이터스토어 제거	데이터스토어를 제거할 수 있습니다. 이 권한은 사용되지 않습니다. 이 작업을 수행하기 위한 권한을 얻으려면 사용자 또는 그룹이 개체와 상위 개체 모두에 이 권한을 할당해야 합니다.	데이터스토어
데이터스토어.파일 제거	데이터스토어에서 파일을 삭제할 수 있습니다. 이 권한은 사용되지 않습니다. 하위 수준 파일 작업 권한을 할당하십시오.	데이터스토어
데이터스토어.데이터스토어 이름 바꾸기	데이터스토어의 이름을 바꿀 수 있습니다.	데이터스토어
데이터스토어.가상 시스템 파일 업데이트	데이터스토어를 재서명하면 데이터스토어에 있는 가상 시스템 파일의 파일 경로를 업데이트할 수 있습니다.	데이터스토어
데이터스토어.가상 시스템 메타데이터 업데이트	데이터스토어와 연결된 가상 시스템 메타데이터를 업데이트할 수 있습니다.	데이터스토어

데이터스토어 클러스터 권한

데이터스토어 클러스터 권한은 Storage DRS에 대한 데이터스토어 클러스터의 구성을 제어합니다.

계층의 서로 다른 수준에서 이 권한을 설정할 수 있습니다. 예를 들어 폴더 수준에서 권한을 설정하는 경우 폴더 내 하나 이상의 개체로 권한을 전파할 수 있습니다. 필수 열에 나열된 개체에는 직접 또는 상속을 통해 권한이 설정되어 있어야 합니다.

표 11-7. 데이터스토어 클러스터 권한

권한 이름	설명	필수
데이터스토어 클러스터.데이터스토어 클러스터 구성	Storage DRS의 데이터스토어 클러스터에 대한 설정을 생성하고 구성할 수 있습니다.	데이터스토어 클러스터

Distributed Switch 권한

Distributed Switch 권한은 Distributed Switch 인스턴스의 관리와 관련된 작업을 수행하는 기능을 제어합니다.

계층의 서로 다른 수준에서 이 권한을 설정할 수 있습니다. 예를 들어 폴더 수준에서 권한을 설정하는 경우 폴더 내 하나 이상의 개체로 권한을 전파할 수 있습니다. 필수 열에 나열된 개체에는 직접 또는 상속을 통해 권한이 설정되어 있어야 합니다.

표 11-8. vSphere Distributed Switch 권한

권한 이름	설명	필수
Distributed Switch.생성	Distributed Switch를 생성할 수 있습니다.	데이터 센터, 네트워크 폴더
Distributed Switch.삭제	Distributed Switch를 제거할 수 있습니다. 이 작업을 수행하기 위한 권한을 얻으려면 사용자 또는 그룹이 개체와 상위 개체 모두에 이 권한을 할당해야 합니다.	Distributed Switch
Distributed Switch.호스트 작업	Distributed Switch의 호스트 멤버를 변경할 수 있습니다.	Distributed Switch
Distributed Switch.수정	Distributed Switch의 구성을 변경할 수 있습니다.	Distributed Switch
Distributed Switch.이동	vSphere Distributed Switch를 다른 폴더로 이동할 수 있습니다.	Distributed Switch
Distributed Switch.Network I/O Control 작업	vSphere Distributed Switch의 리소스 설정을 변경할 수 있습니다.	Distributed Switch
Distributed Switch.정책 작업	vSphere Distributed Switch의 정책을 변경할 수 있습니다.	Distributed Switch
Distributed Switch.포트 구성 작업	vSphere Distributed Switch에서 포트의 구성을 변경할 수 있습니다.	Distributed Switch
Distributed Switch.포트 설정 작업	vSphere Distributed Switch에서 포트의 설정을 변경할 수 있습니다.	Distributed Switch
Distributed Switch.VSPAN 작업	vSphere Distributed Switch의 VSPAN 구성을 변경할 수 있습니다.	Distributed Switch

ESX Agent Manager 권한

ESX Agent Manager 권한은 ESX Agent Manager 및 에이전트 가상 시스템과 관련된 작업을 제어합니다. ESX Agent Manager는 호스트에 연결되어 있으며 가상 시스템을 마이그레이션하는 VMware DRS 또는 다른 서비스의 영향을 받지 않는 관리 가상 시스템을 설치할 수 있게 해 주는 서비스입니다.

계층의 서로 다른 수준에서 이 권한을 설정할 수 있습니다. 예를 들어 폴더 수준에서 권한을 설정하는 경우 폴더 내 하나 이상의 개체로 권한을 전파할 수 있습니다. 필수 열에 나열된 개체에는 직접 또는 상속을 통해 권한이 설정되어 있어야 합니다.

표 11-9. ESX Agent Manager

권한 이름	설명	필수
ESX Agent Manager.구성	호스트 또는 클러스터에 에이전트 가상 시스템을 배포할 수 있습니다.	가상 시스템
ESX Agent Manager.수정	에이전트 가상 시스템에 대해 가상 시스템 전원 끄기 또는 삭제와 같은 수정 작업을 수행할 수 있습니다.	가상 시스템
ESX Agent 보기.보기	에이전트 가상 시스템을 볼 수 있습니다.	가상 시스템

확장 권한

확장 권한은 확장을 설치하고 관리하는 기능을 제어합니다.

계층의 서로 다른 수준에서 이 권한을 설정할 수 있습니다. 예를 들어 폴더 수준에서 권한을 설정하는 경우 폴더 내 하나 이상의 개체로 권한을 전파할 수 있습니다. 필수 열에 나열된 개체에는 직접 또는 상속을 통해 권한이 설정되어 있어야 합니다.

표 11-10. 확장 권한

권한 이름	설명	필수
확장.확장 등록	확장(플러그인)을 등록할 수 있습니다.	루트 vCenter Server
확장.확장 등록 취소	확장(플러그인)의 등록을 취소할 수 있습니다.	루트 vCenter Server
확장.확장 업데이트	확장(플러그인)을 업데이트할 수 있습니다.	루트 vCenter Server

폴더 권한

폴더 권한은 폴더를 생성하고 관리할 수 있는지 여부를 제어합니다.

계층의 서로 다른 수준에서 이 권한을 설정할 수 있습니다. 예를 들어 폴더 수준에서 권한을 설정하는 경우 폴더 내 하나 이상의 개체로 권한을 전파할 수 있습니다. 필수 열에 나열된 개체에는 직접 또는 상속을 통해 권한이 설정되어 있어야 합니다.

표 11-11. 폴더 권한

권한 이름	설명	필수
폴더.폴더 생성	새 폴더를 생성할 수 있습니다.	폴더
폴더.폴더 삭제	폴더를 삭제할 수 있습니다. 이 작업을 수행하기 위한 권한을 얻으려면 사용자 또는 그룹이 개체와 상위 개체 모두에 이 권한을 할당해야 합니다.	폴더
폴더.폴더 이동	폴더를 이동할 수 있습니다. 권한은 소스와 대상에 모두 있어야 합니다.	폴더
폴더.폴더 이름 바꾸기	폴더의 이름을 변경할 수 있습니다.	폴더

글로벌 권한

글로벌 권한은 작업, 스크립트 및 확장과 관련된 글로벌 작업을 제어합니다.

계층의 서로 다른 수준에서 이 권한을 설정할 수 있습니다. 예를 들어 폴더 수준에서 권한을 설정하는 경우 폴더 내 하나 이상의 개체로 권한을 전파할 수 있습니다. 필수 열에 나열된 개체에는 직접 또는 상속을 통해 권한이 설정되어 있어야 합니다.

표 11-12. 글로벌 권한

권한 이름	설명	필수
글로벌.vCenter Server로 작동	vMotion 전송 작업 또는 vMotion 수신 작업을 준비하거나 시작할 수 있습니다.	루트 vCenter Server
글로벌.작업 취소	실행 중이거나 대기열에 있는 작업을 취소할 수 있습니다.	작업과 관련된 인벤토리 개체
글로벌.용량 계획	물리적 시스템을 가상 시스템에 통합하려는 경우 용량 계획을 사용할 수 있습니다.	루트 vCenter Server
글로벌.진단	진단 파일, 로그 헤더, 이진 파일 또는 진단 번들의 목록을 검색할 수 있습니다. 잠재적인 보안 침해 문제를 방지하려면 이 권한을 vCenter Server 관리자 역할로 제한합니다.	루트 vCenter Server
글로벌.메서드 사용 안 함	vCenter Server 확장용 서버를 통해 vCenter Server가 관리하는 개체에 대한 특정 작업을 사용하지 않도록 설정할 수 있습니다.	루트 vCenter Server
글로벌.메서드 사용	vCenter Server 확장용 서버를 통해 vCenter Server가 관리하는 개체에 대한 특정 작업을 사용하도록 설정할 수 있습니다.	루트 vCenter Server
글로벌.글로벌 태그	글로벌 태그를 추가하거나 제거할 수 있습니다.	루트 호스트 또는 vCenter Server
글로벌.상태	vCenter Server 구성 요소의 상태를 볼 수 있습니다.	루트 vCenter Server
글로벌.라이선스	설치된 라이선스를 보고 라이선스를 추가하거나 제거할 수 있습니다.	루트 호스트 또는 vCenter Server
글로벌.이벤트 기록	특정 관리 엔티티에 대한 사용자 정의 이벤트를 로깅할 수 있습니다.	모든 개체
글로벌.사용자 지정 특성 관리	사용자 지정 필드 정의를 추가하거나, 제거하거나, 이름을 바꿀 수 있습니다.	루트 vCenter Server
글로벌.프록시	프록시에 끝점을 추가하거나 프록시에서 끝점을 제거하기 위해 내부 인터페이스에 액세스할 수 있습니다.	루트 vCenter Server
글로벌.스크립트 작업	경보와 함께 스크립트로 작성된 작업을 스케줄링할 수 있습니다.	모든 개체
글로벌.서비스 관리자	vSphere CLI에서 <code>resxstop</code> 명령을 사용할 수 있습니다.	루트 호스트 또는 vCenter Server
글로벌.사용자 지정 특성 설정	관리 개체의 사용자 지정 특성을 보거나 생성하거나 제거할 수 있습니다.	모든 개체
글로벌.설정	런타임 vCenter Server 구성 설정을 읽고 수정할 수 있습니다.	루트 vCenter Server
글로벌.시스템 태그	시스템 태그를 추가하거나 제거할 수 있습니다.	루트 vCenter Server

호스트 CIM 권한

호스트 CIM 권한은 호스트 상태 모니터링을 위한 CIM 사용을 제어합니다.

계층의 서로 다른 수준에서 이 권한을 설정할 수 있습니다. 예를 들어 폴더 수준에서 권한을 설정하는 경우 폴더 내 하나 이상의 개체로 권한을 전파할 수 있습니다. 필수 열에 나열된 개체에는 직접 또는 상속을 통해 권한이 설정되어 있어야 합니다.

표 11-13. 호스트 CIM 권한

권한 이름	설명	필수
호스트.CIM.CIM 상호 작용	클라이언트가 CIM 서비스에 사용할 티켓을 얻을 수 있습니다.	호스트

호스트 구성 권한

호스트 구성 권한은 호스트를 구성하는 기능을 제어합니다.

계층의 서로 다른 수준에서 이 권한을 설정할 수 있습니다. 예를 들어 폴더 수준에서 권한을 설정하는 경우 폴더 내 하나 이상의 개체로 권한을 전파할 수 있습니다. 필수 열에 나열된 개체에는 직접 또는 상속을 통해 권한이 설정되어 있어야 합니다.

표 11-14. 호스트 구성 권한

권한 이름	설명	필수
호스트.구성.고급 설정	고급 호스트 구성 옵션을 설정할 수 있습니다.	호스트
호스트.구성.인증 저장소	Active Directory 인증 저장소를 구성할 수 있습니다.	호스트
호스트.구성.PciPassthru 설정 변경	호스트에 대한 PciPassthru 설정을 변경할 수 있습니다.	호스트
호스트.구성.SNMP 설정 변경	호스트에 대한 SNMP 설정을 변경할 수 있습니다.	호스트
호스트.구성.날짜 및 시간 설정 변경	호스트의 날짜 및 시간 설정을 변경할 수 있습니다.	호스트
호스트.구성.설정 변경	ESXi 호스트에 잠금 모드를 설정할 수 있습니다.	호스트
호스트.구성.연결	호스트의 연결 상태(연결됨 또는 연결 끊김)를 변경할 수 있습니다.	호스트
호스트.구성.펌웨어	ESXi 호스트의 펌웨어를 업데이트할 수 있습니다.	호스트
호스트.구성.하이퍼스레딩	호스트 CPU 스케줄러에서 하이퍼스레딩을 사용하거나 사용하지 않도록 설정할 수 있습니다.	호스트
호스트.구성.이미지 구성	호스트에 연결된 이미지를 변경할 수 있습니다.	
호스트.구성.유지 보수	호스트를 유지 보수 모드로 설정 또는 해제하며, 호스트를 종료하고 다시 시작할 수 있습니다.	호스트
호스트.구성.메모리 구성	호스트 구성을 수정할 수 있습니다.	호스트
호스트.구성.네트워크 구성	네트워크, 방화벽 및 vMotion 네트워크를 구성할 수 있습니다.	호스트

표 11-14. 호스트 구성 권한 (계속)

권한 이름	설명	필수
호스트.구성.전원	호스트 전원 관리 설정을 구성할 수 있습니다.	호스트
호스트.구성.패치 쿼리	설치 가능한 패치를 쿼리하고 호스트에 패치를 설치할 수 있습니다.	호스트
호스트.구성.보안 프로파일 및 방화벽	인터넷 서비스(예: SSH, 텔넷, SNMP) 및 호스트 방화벽을 구성할 수 있습니다.	호스트
호스트.구성.스토리지 파티션 구성	VMFS 데이터스토어 및 진단 파티션을 관리할 수 있습니다. 이 권한을 가진 사용자는 새 스토리지 디바이스를 검사하고 iSCSI를 관리할 수 있습니다.	호스트
호스트.구성.시스템 관리	확장을 통해 호스트의 파일 시스템을 조작할 수 있습니다.	호스트
호스트.구성.시스템 리소스	시스템 리소스 계층의 구성을 업데이트할 수 있습니다.	호스트
호스트.구성.가상 시스템 자동 시작 구성	단일 호스트에서 가상 시스템의 자동 시작 및 자동 중지 순서를 변경할 수 있습니다.	호스트

호스트 인벤토리

호스트 인벤토리 권한은 인벤토리 및 클러스터에 호스트를 추가하고 인벤토리에서 호스트를 이동하는 기능을 제어합니다.

다음 표에서는 인벤토리에 호스트 및 클러스터를 추가하고 이동하는 데 필요한 권한을 설명합니다.

계층의 서로 다른 수준에서 이 권한을 설정할 수 있습니다. 예를 들어 폴더 수준에서 권한을 설정하는 경우 폴더 내 하나 이상의 개체로 권한을 전파할 수 있습니다. 필수 열에 나열된 개체에는 직접 또는 상속을 통해 권한이 설정되어 있어야 합니다.

표 11-15. 호스트 인벤토리 권한

권한 이름	설명	필수
호스트.인벤토리.클러스터에 호스트 추가	기존 클러스터에 호스트를 추가할 수 있습니다.	클러스터
호스트.인벤토리.독립형 호스트 추가	독립형 호스트를 추가할 수 있습니다.	호스트 폴더
호스트.인벤토리.클러스터 생성	새 클러스터를 생성할 수 있습니다.	호스트 폴더
호스트.인벤토리.클러스터 수정	클러스터의 속성을 변경할 수 있습니다.	클러스터
호스트.인벤토리.클러스터 또는 독립형 호스트 이동	폴더 간에 클러스터 또는 독립형 호스트를 이동할 수 있습니다. 권한은 소스와 대상에 모두 있어야 합니다.	클러스터
호스트.인벤토리.호스트 이동	기존 호스트 집합을 클러스터 내부 또는 외부로 이동할 수 있습니다. 권한은 소스와 대상에 모두 있어야 합니다.	클러스터

표 11-15. 호스트 인벤토리 권한 (계속)

권한 이름	설명	필수
호스트.인벤토리.클러스터 제거	클러스터 또는 독립형 호스트를 삭제할 수 있습니다. 이 작업을 수행하기 위한 권한을 얻으려면 사용자 또는 그룹이 개체와 상위 개체 모두에 이 권한을 할당해야 합니다.	클러스터, 호스트
호스트.인벤토리.호스트 제거	호스트를 제거할 수 있습니다. 이 작업을 수행하기 위한 권한을 얻으려면 사용자 또는 그룹이 개체와 상위 개체 모두에 이 권한을 할당해야 합니다.	호스트 및 상위 개체
호스트.인벤토리.클러스터 이름 바꾸기	클러스터의 이름을 바꿀 수 있습니다.	클러스터

호스트 로컬 작업 권한

호스트 로컬 작업 권한은 vSphere Client가 호스트에 직접 연결된 경우에 수행할 수 있는 작업을 제어합니다.

계층의 서로 다른 수준에서 이 권한을 설정할 수 있습니다. 예를 들어 폴더 수준에서 권한을 설정하는 경우 폴더 내 하나 이상의 개체로 권한을 전파할 수 있습니다. 필수 열에 나열된 개체에는 직접 또는 상속을 통해 권한이 설정되어 있어야 합니다.

표 11-16. 호스트 로컬 작업 권한

권한 이름	설명	필수
호스트.로컬 작업.vCenter 에 호스트 추가	호스트에 vpxa 및 aam과 같은 vCenter 에이전트를 설치하거나 제거할 수 있습니다.	루트 호스트
호스트.로컬 작업.가상 시스템 생성	호스트에 가상 시스템을 등록하지 않고 디스크에 새 가상 시스템을 처음부터 생성할 수 있습니다.	루트 호스트
호스트.로컬 작업.가상 시스템 삭제	디스크에서 가상 시스템을 삭제할 수 있습니다. 등록된 가상 시스템 및 등록되지 않은 가상 시스템에 대해 지원됩니다.	루트 호스트
호스트.로컬 작업.NVRAM 콘텐츠 추출	호스트의 NVRAM 콘텐츠를 추출할 수 있습니다.	
호스트.로컬 작업.사용자 그룹 관리	호스트의 로컬 계정을 관리할 수 있습니다.	루트 호스트
호스트.로컬 작업.가상 시스템 재구성	가상 시스템을 재구성할 수 있습니다.	루트 호스트
호스트.로컬 작업.스냅샷 데이터 레이아웃	가상 시스템의 스냅샷 레이아웃을 변경할 수 있습니다.	루트 호스트

호스트 vSphere 복제 권한

호스트 vSphere 복제 권한은 호스트에 대한 VMware vCenter Site Recovery Manager™를 통한 가상 시스템 복제 사용을 제어합니다.

계층의 서로 다른 수준에서 이 권한을 설정할 수 있습니다. 예를 들어 폴더 수준에서 권한을 설정하는 경우 폴더 내 하나 이상의 개체로 권한을 전파할 수 있습니다. 필수 열에 나열된 개체에는 직접 또는 상속을 통해 권한이 설정되어 있어야 합니다.

표 11-17. 호스트 vSphere 복제 권한

권한 이름	설명	필수
호스트.vSphere Replication.복제 관리	이 호스트에서 가상 시스템 복제를 관리할 수 있습니다.	호스트

호스트 프로파일 권한

호스트 프로파일 권한은 호스트 프로파일을 만들고 수정하는 데 관련된 작업을 제어합니다.

계층의 서로 다른 수준에서 이 권한을 설정할 수 있습니다. 예를 들어 폴더 수준에서 권한을 설정하는 경우 폴더 내 하나 이상의 개체로 권한을 전파할 수 있습니다. 필수 열에 나열된 개체에는 직접 또는 상속을 통해 권한이 설정되어 있어야 합니다.

표 11-18. 호스트 프로파일 권한

권한 이름	설명	필수
호스트 프로파일.지우기	프로파일 관련 정보를 지울 수 있습니다.	루트 vCenter Server
호스트 프로파일.생성	호스트 프로파일을 생성할 수 있습니다.	루트 vCenter Server
호스트 프로파일.삭제	호스트 프로파일을 삭제할 수 있습니다.	루트 vCenter Server
호스트 프로파일.편집	호스트 프로파일을 편집할 수 있습니다.	루트 vCenter Server
호스트 프로파일.내보내기	호스트 프로파일을 내보낼 수 있습니다.	루트 vCenter Server
호스트 프로파일.보기	호스트 프로파일을 볼 수 있습니다.	루트 vCenter Server

Inventory Service 제공자 권한

Inventory Service 제공자 권한은 내부 전용입니다. 사용하지 마십시오.

Inventory Service 태그 지정 권한

Inventory Service 태그 지정 권한은 태그 생성/삭제, 범주에 태그 지정, vSphere 인벤토리 개체에서 태그 할당/제거 등을 수행할 수 있는 기능을 제어합니다.

계층의 서로 다른 수준에서 이 권한을 설정할 수 있습니다. 예를 들어 폴더 수준에서 권한을 설정하는 경우 폴더 내 하나 이상의 개체로 권한을 전파할 수 있습니다. 필수 열에 나열된 개체에는 직접 또는 상속을 통해 권한이 설정되어 있어야 합니다.

표 11-19. vCenter Inventory Service 권한

권한 이름	설명	필수
Inventory Service.vSphere 태그 지정.vSphere 태그 할당 또는 할당 취소	vCenter Server 인벤토리의 개체에 대해 태그를 할당하거나 할당 취소할 수 있습니다.	모든 개체
Inventory Service.vSphere 태그 지정.vSphere 태그 생성	태그를 생성할 수 있습니다.	모든 개체
Inventory Service.vSphere 태그 지정.vSphere 태그 범주 생성	태그 범주를 생성할 수 있습니다.	모든 개체
Inventory Service.vSphere 태그 지정.vSphere 태그 범위 생성	태그 범위를 생성할 수 있습니다.	모든 개체
Inventory Service.vSphere 태그 지정.vSphere 태그 삭제	태그 범주를 삭제할 수 있습니다.	모든 개체
Inventory Service.vSphere 태그 지정.vSphere 태그 범주 삭제	태그 범주를 삭제할 수 있습니다.	모든 개체
Inventory Service.vSphere 태그 지정.vSphere 태그 범위 삭제	태그 범위를 삭제할 수 있습니다.	모든 개체
Inventory Service.vSphere 태그 지정.vSphere 태그 편집	태그를 편집할 수 있습니다.	모든 개체
Inventory Service.vSphere 태그 지정.vSphere 태그 범주 편집	태그 범주를 편집할 수 있습니다.	모든 개체
Inventory Service.vSphere 태그 지정.vSphere 태그 범위 편집	태그 범위를 편집할 수 있습니다.	모든 개체
Inventory Service.vSphere 태그 지정.범주의 UsedBy 필드 수정	태그 범주에 대한 사용자 필드를 변경할 수 있습니다.	모든 개체
Inventory Service.vSphere 태그 지정.태그의 UsedBy 필드 수정	태그에 대한 사용자 필드를 변경할 수 있습니다.	모든 개체

네트워크 권한

네트워크 권한은 네트워크 관리와 관련된 작업을 제어합니다.

계층의 서로 다른 수준에서 이 권한을 설정할 수 있습니다. 예를 들어 폴더 수준에서 권한을 설정하는 경우 폴더 내 하나 이상의 개체로 권한을 전파할 수 있습니다. 필수 열에 나열된 개체에는 직접 또는 상속을 통해 권한이 설정되어 있어야 합니다.

표 11-20. 네트워크 권한

권한 이름	설명	필수
네트워크.네트워크 할당	가상 시스템에 네트워크를 할당할 수 있습니다.	네트워크, 가상 시스템
네트워크.구성	네트워크를 구성할 수 있습니다.	네트워크, 가상 시스템

표 11-20. 네트워크 권한 (계속)

권한 이름	설명	필수
네트워크.네트워크 이동	폴더 간에 네트워크를 이동할 수 있습니다. 권한은 소스와 대상에 모두 있어야 합니다.	네트워크
네트워크.제거	네트워크를 제거할 수 있습니다. 이 권한은 사용되지 않습니다. 이 작업을 수행하기 위한 권한을 얻으려면 사용자 또는 그룹이 개체와 상위 개체 모두에 이 권한을 할당해야 합니다.	네트워크

성능 권한

성능 권한은 성능 통계 설정을 수정하는 기능을 제어합니다.

계층의 서로 다른 수준에서 이 권한을 설정할 수 있습니다. 예를 들어 폴더 수준에서 권한을 설정하는 경우 폴더 내 하나 이상의 개체로 권한을 전파할 수 있습니다. 필수 열에 나열된 개체에는 직접 또는 상속을 통해 권한이 설정되어 있어야 합니다.

표 11-21. 성능 권한

권한 이름	설명	필수
성능.간격 수정	성능 데이터 수집 간격을 생성, 제거 및 업데이트할 수 있습니다.	루트 vCenter Server

사용 권한에 대한 권한

사용 권한에 대한 권한은 역할과 사용 권한을 할당하는 기능을 제어합니다.

계층의 서로 다른 수준에서 이 권한을 설정할 수 있습니다. 예를 들어 폴더 수준에서 권한을 설정하는 경우 폴더 내 하나 이상의 개체로 권한을 전파할 수 있습니다. 필수 열에 나열된 개체에는 직접 또는 상속을 통해 권한이 설정되어 있어야 합니다.

표 11-22. 사용 권한에 대한 권한

권한 이름	설명	필수
사용 권한.권한 수정	엔티티에 대한 사용 권한 규칙을 하나 이상 정의하거나, 지정된 엔티티 사용자 또는 그룹에 대한 규칙이 이미 있는 경우 해당 규칙을 업데이트할 수 있습니다. 이 작업을 수행하기 위한 권한을 얻으려면 사용자 또는 그룹이 개체와 상위 개체 모두에 이 권한을 할당해야 합니다.	임의의 개체와 상위 개체
사용 권한.권한 수정	권한의 그룹 또는 설명을 수정할 수 있습니다. 이 권한과 연결된 vSphere Web Client 사용자 인터페이스 요소는 없습니다.	
사용 권한.역할 수정	역할의 이름 및 해당 역할과 연결된 권한을 업데이트할 수 있습니다.	모든 개체
사용 권한.역할 권한 다시 할당	역할의 모든 사용 권한을 다른 역할에 다시 할당할 수 있습니다.	모든 개체

프로파일 기반 스토리지 권한

프로파일 기반 스토리지 권한은 스토리지 프로파일과 관련된 작업을 제어합니다.

계층의 서로 다른 수준에서 이 권한을 설정할 수 있습니다. 예를 들어 폴더 수준에서 권한을 설정하는 경우 폴더 내 하나 이상의 개체로 권한을 전파할 수 있습니다. 필수 열에 나열된 개체에는 직접 또는 상속을 통해 권한이 설정되어 있어야 합니다.

표 11-23. 프로파일 기반 스토리지 권한

권한 이름	설명	필수
프로파일 기반 스토리지.프로파일 기반 스토리지 업데이트	스토리지 기능과 가상 시스템 스토리지 프로파일을 만들고 업데이트하는 등의 스토리지 프로파일 변경 작업을 수행할 수 있습니다.	루트 vCenter Server
프로파일 기반 스토리지.프로파일 기반 스토리지 보기	정의된 스토리지 기능 및 스토리지 프로파일을 볼 수 있습니다.	루트 vCenter Server

리소스 권한

리소스 권한은 가상 시스템의 마이그레이션뿐만 아니라 리소스 풀의 생성 및 관리도 제어합니다.

계층의 서로 다른 수준에서 이 권한을 설정할 수 있습니다. 예를 들어 폴더 수준에서 권한을 설정하는 경우 폴더 내 하나 이상의 개체로 권한을 전파할 수 있습니다. 필수 열에 나열된 개체에는 직접 또는 상속을 통해 권한이 설정되어 있어야 합니다.

표 11-24. 리소스 권한

권한 이름	설명	필수
리소스.권장 사항 적용	vMotion을 사용하여 마이그레이션을 수행하라는 서버의 제안을 수락할 수 있습니다.	클러스터
리소스.리소스 풀에 vApp 할당	리소스 풀에 vApp을 할당할 수 있습니다.	리소스 풀
리소스.리소스 풀에 가상 시스템 할당	리소스 풀에 가상 시스템을 할당할 수 있습니다.	리소스 풀
리소스.리소스 풀 생성	리소스 풀을 생성할 수 있습니다.	리소스 풀, 클러스터
리소스.전원이 꺼진 가상 시스템 마이그레이션	전원이 꺼진 가상 시스템을 다른 리소스 풀이나 호스트로 마이그레이션할 수 있습니다.	가상 시스템
리소스.전원이 켜진 가상 시스템 마이그레이션	vMotion을 사용하여 전원이 켜진 가상 시스템을 다른 리소스 풀이나 호스트로 마이그레이션할 수 있습니다.	
리소스.리소스 풀 수정	리소스 풀의 할당을 변경할 수 있습니다.	리소스 풀
리소스.리소스 풀 이동	리소스 풀을 이동할 수 있습니다. 권한은 소스와 대상에 모두 있어야 합니다.	리소스 풀
리소스.vMotion 쿼리	호스트 집합을 사용하여 가상 시스템의 일반적인 vMotion 호환성을 쿼리할 수 있습니다.	루트 vCenter Server

표 11-24. 리소스 권한 (계속)

권한 이름	설명	필수
리소스.리소스 풀 제거	리소스 풀을 삭제할 수 있습니다. 이 작업을 수행하기 위한 권한을 얻으려면 사용자 또는 그룹이 개체와 상위 개체 모두에 이 권한을 할당해야 합니다.	리소스 풀
리소스.리소스 풀 이름 바꾸기	리소스 풀 이름을 바꿀 수 있습니다.	리소스 풀

스케줄링된 작업 권한

스케줄링된 작업 권한은 스케줄링된 작업의 생성, 편집 및 제거를 제어합니다.

계층의 서로 다른 수준에서 이 권한을 설정할 수 있습니다. 예를 들어 폴더 수준에서 권한을 설정하는 경우 폴더 내 하나 이상의 개체로 권한을 전파할 수 있습니다. 필수 열에 나열된 개체에는 직접 또는 상속을 통해 권한이 설정되어 있어야 합니다.

표 11-25. 스케줄링된 작업 권한

권한 이름	설명	필수
스케줄링된 작업.작업 생성	작업을 스케줄링할 수 있습니다. 스케줄링 시간에 스케줄링된 작업을 수행할 수 있는 권한 외에 추가적으로 필요한 권한입니다.	모든 개체
스케줄링된 작업.작업 수정	스케줄링된 작업 속성을 재구성할 수 있습니다.	모든 개체
스케줄링된 작업.작업 제거	대기열에서 스케줄링된 작업을 제거할 수 있습니다.	모든 개체
스케줄링된 작업.작업 실행	스케줄링된 작업을 즉시 실행할 수 있습니다. 스케줄링된 작업을 만들고 실행하려면 관련 작업을 수행할 수 있는 사용 권한도 필요합니다.	모든 개체

세션 권한

세션 권한은 vCenter Server 시스템에서 세션을 열 수 있는 확장 기능을 제어합니다.

계층의 서로 다른 수준에서 이 권한을 설정할 수 있습니다. 예를 들어 폴더 수준에서 권한을 설정하는 경우 폴더 내 하나 이상의 개체로 권한을 전파할 수 있습니다. 필수 열에 나열된 개체에는 직접 또는 상속을 통해 권한이 설정되어 있어야 합니다.

표 11-26. 세션 권한

권한 이름	설명	필수
세션.사용자 가장	다른 사용자를 가장할 수 있습니다. 이 기능은 확장에 사용됩니다.	루트 vCenter Server
세션.메시지	글로벌 로그인 메시지를 설정할 수 있습니다.	루트 vCenter Server

표 11-26. 세션 권한 (계속)

권한 이름	설명	필수
세션.세션의 유효성 검사	세션의 유효성을 검사할 수 있습니다.	루트 vCenter Server
세션.세션 보기 및 중지	세션을 보고, 로그인한 사용자 한 명 이상을 강제 로그아웃할 수 있습니다.	루트 vCenter Server

스토리지 보기 권한

스토리지 보기 권한은 스토리지 모니터링 서비스 Storage Monitoring Service API에 대한 권한을 제어합니다.

계층의 서로 다른 수준에서 이 권한을 설정할 수 있습니다. 예를 들어 폴더 수준에서 권한을 설정하는 경우 폴더 내 하나 이상의 개체로 권한을 전파할 수 있습니다. 필수 열에 나열된 개체에는 직접 또는 상속을 통해 권한이 설정되어 있어야 합니다.

표 11-27. 스토리지 보기 권한

권한 이름	설명	필수
스토리지 보기.서비스 구성	권한 있는 사용자가 모든 Storage Monitoring Service API를 사용하도록 합니다. 읽기 전용 Storage Monitoring Service API에 대한 권한에 스토리지 보기. 보기 를 사용합니다.	루트 vCenter Server
스토리지 보기.보기	권한 있는 사용자가 읽기 전용 Storage Monitoring Service API를 사용하도록 합니다.	루트 vCenter Server

작업 권한

작업 권한은 vCenter Server에서 작업을 만들고 업데이트할 수 있는 확장 기능을 제어합니다.

계층의 서로 다른 수준에서 이 권한을 설정할 수 있습니다. 예를 들어 폴더 수준에서 권한을 설정하는 경우 폴더 내 하나 이상의 개체로 권한을 전파할 수 있습니다. 필수 열에 나열된 개체에는 직접 또는 상속을 통해 권한이 설정되어 있어야 합니다.

표 11-28. 작업 권한

권한 이름	설명	필수
작업.작업 생성	확장을 통해 사용자 정의 작업을 만들 수 있습니다. 이 권한과 연결된 vSphere Web Client 사용자 인터페이스 요소는 없습니다.	루트 vCenter Server
작업.작업 업데이트	확장을 통해 사용자 정의 작업을 업데이트할 수 있습니다. 이 권한과 연결된 vSphere Web Client 사용자 인터페이스 요소는 없습니다.	루트 vCenter Server

전송 서비스 권한

전송 서비스 권한은 VMware 내부입니다. 이러한 권한을 사용하지 마십시오.

VRM 정책 권한

VRM 정책 권한은 VMware 내부입니다. 이러한 권한을 사용하지 마십시오.

가상 시스템 구성 권한

가상 시스템 구성 권한은 가상 시스템 옵션 및 디바이스를 구성하는 기능을 제어합니다.

계층의 서로 다른 수준에서 이 권한을 설정할 수 있습니다. 예를 들어 폴더 수준에서 권한을 설정하는 경우 폴더 내 하나 이상의 개체로 권한을 전파할 수 있습니다. 필수 열에 나열된 개체에는 직접 또는 상속을 통해 권한이 설정되어 있어야 합니다.

표 11-29. 가상 시스템 구성 권한

권한 이름	설명	필수
가상 시스템.구성.기존 디스크 추가	가상 시스템에 기존 가상 디스크를 추가할 수 있습니다.	가상 시스템
가상 시스템.구성.새 디스크 추가	가상 시스템에 추가할 새 가상 디스크를 생성할 수 있습니다.	가상 시스템
가상 시스템.구성.디바이스 추가 또는 제거	디스크가 아닌 디바이스를 추가하거나 제거할 수 있습니다.	가상 시스템
가상 시스템.구성.고급	가상 시스템의 구성 파일에서 고급 매개 변수를 추가하거나 수정할 수 있습니다.	가상 시스템
가상 시스템.구성.CPU 수 변경	가상 CPU 수를 변경할 수 있습니다.	가상 시스템
가상 시스템.구성.리소스 변경	지정된 리소스 풀에 있는 가상 시스템 노드 집합에 대한 리소스 구성을 변경할 수 있습니다.	가상 시스템
가상 시스템.구성.managedBy 구성	확장 또는 솔루션을 통해 가상 시스템을 해당 확장 또는 솔루션에 의해 관리되는 것으로 표시할 수 있습니다.	가상 시스템
가상 시스템.구성.디스크 변경 내용 추적	가상 시스템 디스크에 대한 변경 내용 추적을 사용하거나 사용하지 않도록 설정할 수 있습니다.	가상 시스템
가상 시스템.구성.디스크 리스	가상 시스템에 대한 디스크 리스 작업을 허용합니다.	가상 시스템
가상 시스템.구성.연결 설정 표시	가상 시스템의 원격 콘솔 옵션을 구성할 수 있도록 합니다.	가상 시스템
가상 시스템.구성.가상 디스크 확장	가상 디스크의 크기를 확장할 수 있습니다.	가상 시스템
가상 시스템.구성.호스트 USB 디바이스	호스트 기반 USB 디바이스를 가상 시스템에 연결할 수 있습니다.	가상 시스템
가상 시스템.구성.메모리	가상 시스템에 할당된 메모리 크기를 변경할 수 있습니다.	가상 시스템

표 11-29. 가상 시스템 구성 권한 (계속)

권한 이름	설명	필수
가상 시스템.구성.디바이스 설정 수정	기존 디바이스의 속성을 변경할 수 있습니다.	가상 시스템
가상 시스템.구성.Fault Tolerance 호환성 쿼리	가상 시스템의 Fault Tolerance 호환성 여부를 확인할 수 있습니다.	가상 시스템
가상 시스템.구성.소유자가 없는 파일 쿼리	소유자가 없는 파일을 쿼리할 수 있습니다.	가상 시스템
가상 시스템.구성.원시 디바이스	원시 디스크 매핑 또는 SCSI 패스스루 디바이스를 추가하거나 제거할 수 있습니다. 이 매개 변수를 설정하면 연결 상태를 포함하여 원시 디바이스를 수정할 수 있는 다른 모든 권한이 재정의됩니다.	가상 시스템
가상 시스템.구성.경로에서 다시 로드	가상 시스템의 ID를 유지하면서 가상 시스템 구성 경로를 변경할 수 있습니다. VMware vCenter Site Recovery Manager와 같은 솔루션에서는 이 작업을 통해 페일오버 및 페일백 중 가상 시스템 ID를 유지합니다.	가상 시스템
가상 시스템.구성.디스크 제거	가상 디스크 디바이스를 제거할 수 있습니다.	가상 시스템
가상 시스템.구성.이름 바꾸기	가상 시스템의 이름을 변경하거나 가상 시스템의 관련 기록을 수정할 수 있습니다.	가상 시스템
가상 시스템.구성.게스트 정보 재설정	가상 시스템의 게스트 운영 체제 정보를 편집할 수 있습니다.	가상 시스템
가상 시스템.구성.주석 설정	가상 시스템 주석을 추가하거나 편집할 수 있도록 합니다.	가상 시스템
가상 시스템.구성.설정	일반적인 가상 시스템 설정을 변경할 수 있습니다.	가상 시스템
가상 시스템.구성.스왑 파일 배치	가상 시스템의 스왑 파일 배치 정책을 변경할 수 있습니다.	가상 시스템
가상 시스템.구성.가상 시스템 잠금 해제	가상 시스템의 암호를 해독할 수 있습니다.	가상 시스템
가상 시스템.구성.가상 시스템 호환성 업그레이드	가상 시스템의 가상 시스템 호환성 버전을 업그레이드할 수 있습니다.	가상 시스템

가상 시스템 게스트 작업 권한

가상 시스템 게스트 작업 권한은 API를 사용하는 가상 시스템의 게스트 운영 체제 내에서 파일 및 프로그램과 상호 작용하는 기능을 제어합니다.

이러한 작업에 대한 자세한 내용은 "VMware vSphere API 참조" 설명서를 참조하십시오.

계층의 서로 다른 수준에서 이 권한을 설정할 수 있습니다. 예를 들어 폴더 수준에서 권한을 설정하는 경우 폴더 내 하나 이상의 개체로 권한을 전파할 수 있습니다. 필수 열에 나열된 개체에는 직접 또는 상속을 통해 권한이 설정되어 있어야 합니다.

표 11-30. 가상 시스템 게스트 작업

권한 이름	설명	적용되는 개체
가상 시스템.게스트 작업.게스트 작업 별칭 수정	가상 시스템에 대한 별칭 수정을 수반하는 가상 시스템 게스트 작업을 허용합니다.	가상 시스템
가상 시스템.게스트 작업.게스트 작업 별칭 쿼리	가상 시스템에 대한 별칭 쿼리를 수반하는 가상 시스템 게스트 작업을 허용합니다.	가상 시스템
가상 시스템.게스트 작업.게스트 작업 수정	가상 시스템으로 파일을 전송하는 경우와 같이 가상 시스템에서의 게스트 운영 체제 수정을 수반하는 가상 시스템 게스트 작업을 허용합니다. 이 권한과 연결된 vSphere Web Client 사용자 인터페이스 요소는 없습니다.	가상 시스템
가상 시스템.게스트 작업.게스트 작업 프로그램 실행	가상 시스템에서의 프로그램 실행을 수반하는 가상 시스템 게스트 작업을 허용합니다. 이 권한과 연결된 vSphere Web Client 사용자 인터페이스 요소는 없습니다.	가상 시스템
가상 시스템.게스트 작업.게스트 작업 쿼리	게스트 운영 체제의 파일을 나열하는 경우와 같이 게스트 운영 체제에 대한 쿼리를 수반하는 가상 시스템 게스트 작업을 허용합니다. 이 권한과 연결된 vSphere Web Client 사용자 인터페이스 요소는 없습니다.	가상 시스템

가상 시스템 상호 작용 권한

가상 시스템 상호 작용 권한은 가상 시스템 콘솔과 상호 작용하고, 미디어를 구성하고, 전원 작업을 수행하고, VMware Tools를 설치하는 기능을 제어합니다.

계층의 서로 다른 수준에서 이 권한을 설정할 수 있습니다. 예를 들어 폴더 수준에서 권한을 설정하는 경우 폴더 내 하나 이상의 개체로 권한을 전파할 수 있습니다. 필수 열에 나열된 개체에는 직접 또는 상속을 통해 권한이 설정되어 있어야 합니다.

표 11-31. 가상 시스템 상호 작용

권한 이름	설명	필수
가상 시스템.상호 작용.질문에 응답	가상 시스템 상태 전환 또는 런타임 오류와 관련된 문제를 해결할 수 있습니다.	가상 시스템
가상 시스템.상호 작용.가상 시스템의 백업 작업	가상 시스템의 백업 작업을 수행할 수 있습니다.	가상 시스템
가상 시스템.상호 작용.CD 미디어 구성	가상 DVD 또는 CD-ROM 디바이스를 구성할 수 있습니다.	가상 시스템
가상 시스템.상호 작용.플로피 미디어 구성	가상 플로피 디바이스를 구성할 수 있습니다.	가상 시스템
가상 시스템.상호 작용.콘솔 상호 작용	가상 시스템의 가상 마우스, 키보드 및 화면과 상호 작용할 수 있습니다.	가상 시스템

표 11-31. 가상 시스템 상호 작용 (계속)

권한 이름	설명	필수
가상 시스템.상호 작용.스크린샷 생성	가상 시스템 스크린샷을 생성할 수 있습니다.	가상 시스템
가상 시스템.상호 작용.모든 디스크 조각 모음	가상 시스템의 모든 디스크에 대한 조각 모음 작업을 수행할 수 있습니다.	가상 시스템
가상 시스템.상호 작용.디바이스 연결	가상 시스템에 있는 연결 불가능한 가상 디바이스의 연결 상태를 변경할 수 있습니다.	가상 시스템
가상 시스템.상호 작용.Fault Tolerance 사용 안 함	Fault Tolerance를 사용하는 가상 시스템의 보조 가상 시스템을 사용하지 않도록 설정할 수 있습니다.	가상 시스템

표 11-31. 가상 시스템 상호 작용 (계속)

권한 이름	설명	필수
가상 시스템.상호 작용.끌어서 놓기	가상 시스템과 원격 클라이언트 간에 파일을 끌어서 놓을 수 있습니다.	가상 시스템
가상 시스템.상호 작용.Fault Tolerance 사용	Fault Tolerance를 사용하는 가상 시스템의 보조 가상 시스템을 사용하도록 설정할 수 있습니다.	가상 시스템
가상 시스템.상호 작용.VIX API를 통해 게스트 운영 체제 관리	VIX API를 통해 가상 시스템의 운영 체제를 관리할 수 있습니다.	가상 시스템
가상 시스템.상호 작용.USB HID 검색 코드 넣기	USB HID 검색 코드를 넣을 수 있습니다.	가상 시스템

표 11-31. 가상 시스템 상호 작용 (계속)

권한 이름	설명	필수
가상 시스템.상호 작용.일시 중지/일시 중지 해제	가상 시스템을 일시 중지하거나 일시 중지를 해제할 수 있습니다.	가상 시스템
가상 시스템.상호 작용.지우기 또는 축소 작업 수행	가상 시스템에서 지우기 또는 축소 작업을 수행할 수 있습니다.	가상 시스템
가상 시스템.상호 작용.전원 끄기	전원이 꺼진 가상 시스템의 전원을 끌 수 있습니다. 이 작업을 수행하면 게스트 운영 체제의 전원이 꺼집니다.	가상 시스템
가상 시스템.상호 작용.전원 켜기	전원이 꺼진 가상 시스템의 전원을 켜고 일시 중단된 가상 시스템을 재개할 수 있습니다.	가상 시스템

표 11-31. 가상 시스템 상호 작용 (계속)

권한 이름	설명	필수
가상 시스템.상호 작용.가상 시스템의 기록 세션	가상 시스템에 세션을 기록할 수 있습니다.	가상 시스템
가상 시스템.상호 작용.가상 시스템의 재생 세션	가상 시스템에 기록된 세션을 재생할 수 있습니다.	가상 시스템
가상 시스템.상호 작용.재설정	가상 시스템을 재설정하고 게스트 운영 체제를 재부팅할 수 있습니다.	가상 시스템
가상 시스템.상호 작용..Fault Tolerance 재개	가상 시스템에 대한 Fault Tolerance를 재개할 수 있습니다.	가상 시스템
가상 시스템.상호 작용.일시 중단	전원이 켜진 가상 시스템을 일시 중단할 수 있습니다. 이 작업을 수행하면 게스트가 대기 모드로 전환됩니다.	가상 시스템

표 11-31. 가상 시스템 상호 작용 (계속)

권한 이름	설명	필수
가상 시스템.상호 작용.Fault Tolerance 일시 중단	가상 시스템에 대한 Fault Tolerance를 일시 중단할 수 있습니다.	가상 시스템
가상 시스템.상호 작용.페일오버 테스트	보조 가상 시스템을 기본 가상 시스템으로 설정하여 Fault Tolerance 페일오버를 테스트할 수 있습니다.	가상 시스템
가상 시스템.상호 작용.보조 VM 다시 시작 테스트	Fault Tolerance를 사용하는 가상 시스템의 보조 가상 시스템을 종료할 수 있습니다.	가상 시스템
가상 시스템.상호 작용.Fault Tolerance 해제	가상 시스템에 대한 Fault Tolerance를 해제할 수 있습니다.	가상 시스템

표 11-31. 가상 시스템 상호 작용 (계속)

권한 이름	설명	필수
가상 시스템.상호 작용.Fault Tolerance 설정	가상 시스템에 대한 Fault Tolerance를 설정할 수 있습니다.	가상 시스템
가상 시스템.상호 작용.VMware Tools 설치	VMware Tools 설치 관리자를 게스트 운영 체제의 CD-ROM으로 마운트하거나 마운트 해제할 수 있습니다.	가상 시스템

가상 시스템 인벤토리 권한

가상 시스템 인벤토리 권한은 가상 시스템을 추가, 이동 및 제거하는 기능을 제어합니다.

계층의 서로 다른 수준에서 이 권한을 설정할 수 있습니다. 예를 들어 폴더 수준에서 권한을 설정하는 경우 폴더 내 하나 이상의 개체로 권한을 전파할 수 있습니다. 필수 열에 나열된 개체에는 직접 또는 상속을 통해 권한이 설정되어 있어야 합니다.

표 11-32. 가상 시스템 인벤토리 권한

권한 이름	설명	필수
가상 시스템.인벤토리.기존 항목에서 생성	템플릿에서 복제하거나 배포하는 방법으로 기존 가상 시스템 또는 템플릿을 기반으로 가상 시스템을 생성할 수 있습니다.	클러스터, 호스트, 가상 시스템 폴더
가상 시스템.인벤토리.새로 생성	가상 시스템을 생성하고 실행할 리소스를 할당할 수 있습니다.	클러스터, 호스트, 가상 시스템 폴더
가상 시스템.인벤토리.이동	계층에서 가상 시스템을 재배포할 수 있습니다. 권한은 소스와 대상에 모두 있어야 합니다.	가상 시스템

표 11-32. 가상 시스템 인벤토리 권한 (계속)

권한 이름	설명	필수
가상 시스템.인벤토리.등록	기존 가상 시스템을 vCenter Server 또는 호스트 인벤토리에 추가할 수 있습니다.	클러스터, 호스트, 가상 시스템 폴더
가상 시스템.인벤토리.제거	가상 시스템을 삭제할 수 있습니다. 가상 시스템을 삭제하면 디스크에서 가상 시스템의 기본 파일이 제거됩니다. 이 작업을 수행하기 위한 권한을 얻으려면 사용자 또는 그룹이 개체와 상위 개체 모두에 이 권한을 할당해야 합니다.	가상 시스템
가상 시스템.인벤토리.등록 취소	vCenter Server 또는 호스트 인벤토리에서 가상 시스템을 등록 취소할 수 있습니다. 이 작업을 수행하기 위한 권한을 얻으려면 사용자 또는 그룹이 개체와 상위 개체 모두에 이 권한을 할당해야 합니다.	가상 시스템

가상 시스템 프로비저닝 권한

가상 시스템 프로비저닝 권한은 가상 시스템 배포 및 사용자 지정과 관련된 작업을 제어합니다.

계층의 서로 다른 수준에서 이 권한을 설정할 수 있습니다. 예를 들어 폴더 수준에서 권한을 설정하는 경우 폴더 내 하나 이상의 개체로 권한을 전파할 수 있습니다. 필수 열에 나열된 개체에는 직접 또는 상속을 통해 권한이 설정되어 있어야 합니다.

표 11-33. 가상 시스템 프로비저닝 권한

권한 이름	설명	필수
가상 시스템.프로비저닝.디스크 액세스 허용	가상 시스템의 디스크를 열어 임의 읽기/쓰기에 액세스할 수 있습니다. 주로 원격 디스크를 마운트하는 데 사용됩니다.	가상 시스템
가상 시스템.프로비저닝.읽기 전용 디스크 액세스 허용	가상 시스템의 디스크를 열어 임의 읽기에 액세스할 수 있습니다. 주로 원격 디스크를 마운트하는 데 사용됩니다.	가상 시스템
가상 시스템.프로비저닝.가상 시스템 다운로드 허용	.vmx, .disk, .log 및 .nvram을 포함하여 가상 시스템과 연결된 파일을 읽을 수 있습니다.	루트 호스트 또는 vCenter Server
가상 시스템.프로비저닝.가상 시스템 파일 업로드 허용	.vmx, .disk, .log 및 .nvram을 포함하여 가상 시스템과 연결된 파일에 쓸 수 있습니다.	루트 호스트 또는 vCenter Server
가상 시스템.프로비저닝.템플릿 복제	템플릿을 복제할 수 있습니다.	템플릿
가상 시스템.프로비저닝.가상 시스템 복제	기존 가상 시스템을 복제하고 리소스를 할당할 수 있습니다.	가상 시스템
가상 시스템.프로비저닝.가상 시스템에서 템플릿 생성	가상 시스템에서 새 템플릿을 생성할 수 있습니다.	가상 시스템
가상 시스템.프로비저닝.사용자 지정	가상 시스템을 이동하지 않고 가상 시스템의 게스트 운영 체제를 사용자 지정할 수 있습니다.	가상 시스템
가상 시스템.프로비저닝.템플릿 배포	템플릿에서 가상 시스템을 배포할 수 있습니다.	템플릿

표 11-33. 가상 시스템 프로비저닝 권한 (계속)

권한 이름	설명	필수
가상 시스템.프로비저닝.템플릿으로 표시	기존의 전원이 꺼진 가상 시스템을 템플릿으로 표시할 수 있습니다.	가상 시스템
가상 시스템.프로비저닝.가상 시스템으로 표시	기존 템플릿을 가상 시스템으로 표시할 수 있습니다.	템플릿
가상 시스템.프로비저닝.사용자 지정 규격 수정	사용자 지정 규격을 생성하거나 수정하거나 삭제할 수 있습니다.	루트 vCenter Server
가상 시스템.프로비저닝.디스크 수준 올리기	가상 시스템의 디스크 수준을 올릴 수 있습니다.	가상 시스템
가상 시스템.프로비저닝.사용자 지정 규격 읽기	사용자 지정 규격을 읽을 수 있습니다.	가상 시스템

가상 시스템 서비스 구성 권한

가상 시스템 서비스 구성 권한은 서비스 구성에 대한 모니터링 및 관리 작업을 수행할 수 있는 사용자를 제어합니다.

계층의 서로 다른 수준에서 이 권한을 설정할 수 있습니다. 예를 들어 폴더 수준에서 권한을 설정하는 경우 폴더 내 하나 이상의 개체로 권한을 전파할 수 있습니다. 필수 열에 나열된 개체에는 직접 또는 상속을 통해 권한이 설정되어 있어야 합니다.

참고 vSphere 6.0에서는 vSphere Web Client를 사용하여 이 권한을 할당하거나 제거하지 마십시오.

표 11-34. 가상 시스템 서비스 구성 권한

권한 이름	설명
가상 시스템.서비스 구성.알림 허용	서비스 상태에 대한 알림을 생성 및 사용할 수 있습니다.
가상 시스템.서비스 구성.글로벌 이벤트 알림 폴링 허용	알림이 존재하는지 여부를 쿼리할 수 있습니다.
가상 시스템.서비스 구성.서비스 구성 관리	가상 시스템 서비스를 생성, 수정 및 삭제할 수 있습니다.
가상 시스템.서비스 구성.서비스 구성 수정	기존 가상 시스템 서비스 구성을 수정할 수 있습니다.
가상 시스템.서비스 구성.서비스 구성 쿼리	가상 시스템 서비스 목록을 검색할 수 있습니다.
가상 시스템.서비스 구성.서비스 구성 읽기	기존 가상 시스템 서비스 구성을 검색할 수 있습니다.

가상 시스템 스냅샷 관리 권한

가상 시스템 스냅샷 관리 권한은 스냅샷을 생성, 삭제, 복원하고 이름을 변경할 수 있는지 여부를 제어합니다.

계층의 서로 다른 수준에서 이 권한을 설정할 수 있습니다. 예를 들어 폴더 수준에서 권한을 설정하는 경우 폴더 내 하나 이상의 개체로 권한을 전파할 수 있습니다. 필수 열에 나열된 개체에는 직접 또는 상속을 통해 권한이 설정되어 있어야 합니다.

표 11-35. 가상 시스템 상태 권한

권한 이름	설명	필수
가상 시스템.스냅샷 관리.스냅샷 생성	가상 시스템의 현재 상태에서 스냅샷을 생성할 수 있습니다.	가상 시스템
가상 시스템.스냅샷 관리.스냅샷 제거	스냅샷 기록에서 스냅샷을 제거할 수 있습니다.	가상 시스템
가상 시스템.스냅샷 관리.스냅샷 이름 바꾸기	새 이름, 새 설명 또는 둘 모두를 사용하여 스냅샷의 이름을 변경할 수 있습니다.	가상 시스템
가상 시스템.스냅샷 관리.스냅샷으로 복구	가상 시스템을 지정된 스냅샷 시점의 상태로 설정할 수 있습니다.	가상 시스템

가상 시스템 vSphere 복제 권한

가상 시스템 vSphere 복제 권한은 가상 시스템에 대한 VMware vCenter Site Recovery Manager™를 통한 복제 사용을 제어합니다.

계층의 서로 다른 수준에서 이 권한을 설정할 수 있습니다. 예를 들어 폴더 수준에서 권한을 설정하는 경우 폴더 내 하나 이상의 개체로 권한을 전파할 수 있습니다. 필수 열에 나열된 개체에는 직접 또는 상속을 통해 권한이 설정되어 있어야 합니다.

표 11-36. 가상 시스템 vSphere 복제

권한 이름	설명	필수
가상 시스템.vSphere Replication.복제 구성	가상 시스템에 대한 복제를 구성할 수 있습니다.	가상 시스템
가상 시스템.vSphere Replication.복제 관리	복제 시 전체 동기화, 온라인 동기화 또는 오프라인 동기화를 트리거할 수 있습니다.	가상 시스템
가상 시스템.vSphere Replication.복제 모니터링	복제를 모니터링할 수 있습니다.	가상 시스템

dvPort 그룹 권한

분산 가상 포트 그룹 권한은 분산 가상 포트 그룹의 생성, 삭제 및 수정 기능을 제어합니다.

다음 표에서는 분산 가상 포트 그룹을 만들고 구성하는 데 필요한 권한을 설명합니다.

계층의 서로 다른 수준에서 이 권한을 설정할 수 있습니다. 예를 들어 폴더 수준에서 권한을 설정하는 경우 폴더 내 하나 이상의 개체로 권한을 전파할 수 있습니다. 필수 열에 나열된 개체에는 직접 또는 상속을 통해 권한이 설정되어 있어야 합니다.

표 11-37. 분산 가상 포트 그룹 권한

권한 이름	설명	필수
dvPort 그룹.생성	분산 가상 포트 그룹을 생성할 수 있습니다.	가상 포트 그룹
dvPort 그룹.삭제	분산 가상 포트 그룹을 삭제할 수 있습니다. 이 작업을 수행하기 위한 권한을 얻으려면 사용자 또는 그룹이 개체와 상위 개체 모두에 이 권한을 할당해야 합니다.	가상 포트 그룹
dvPort 그룹.수정	분산 가상 포트 그룹 구성을 수정할 수 있습니다.	가상 포트 그룹
dvPort 그룹.정책 작업	분산 가상 포트 그룹의 정책을 설정할 수 있습니다.	가상 포트 그룹
dvPort 그룹.범위 작업	분산 가상 포트 그룹의 범위를 설정할 수 있습니다.	가상 포트 그룹

vApp 권한

vApp 권한은 vApp 배포 및 구성과 관련된 작업을 제어합니다.

계층의 서로 다른 수준에서 이 권한을 설정할 수 있습니다. 예를 들어 폴더 수준에서 권한을 설정하는 경우 폴더 내 하나 이상의 개체로 권한을 전파할 수 있습니다. 필수 열에 나열된 개체에는 직접 또는 상속을 통해 권한이 설정되어 있어야 합니다.

표 11-38. vApp 권한

권한 이름	설명	필수
vApp.가상 시스템 추가	vApp에 가상 시스템을 추가할 수 있습니다.	vApp
vApp.리소스 풀 할당	vApp에 리소스 풀을 할당할 수 있습니다.	vApp
vApp.vApp 할당	다른 vApp에 vApp을 할당할 수 있습니다.	vApp
vApp.복제	vApp을 복제할 수 있습니다.	vApp
vApp.생성	vApp을 생성할 수 있습니다.	vApp
vApp.삭제	vApp을 삭제할 수 있습니다. 이 작업을 수행하기 위한 권한을 얻으려면 사용자 또는 그룹이 개체와 상위 개체 모두에 이 권한을 할당해야 합니다.	vApp
vApp.내보내기	vSphere에서 vApp을 내보낼 수 있습니다.	vApp
vApp.가져오기	vApp을 vSphere로 가져올 수 있습니다.	vApp
vApp.이동	vApp을 새 인벤토리 위치로 이동할 수 있습니다.	vApp
vApp.전원 끄기	vApp에서 전원 끄기 작업을 수행할 수 있습니다.	vApp

표 11-38. vApp 권한 (계속)

권한 이름	설명	필수
vApp.전원 켜기	vApp에서 전원 켜기 작업을 수행할 수 있습니다.	vApp
vApp.이름 바꾸기	vApp 이름을 변경할 수 있습니다.	vApp
vApp.일시 중단	vApp을 일시 중단할 수 있습니다.	vApp
vApp.등록 취소	vApp을 등록 취소할 수 있습니다. 이 작업을 수행하기 위한 권한을 얻으려면 사용자 또는 그룹이 개체와 상위 개체 모두에 이 권한을 할당해야 합니다.	vApp
vApp.OVF 환경 보기	vApp 내에서 전원이 켜진 가상 시스템의 OVF 환경을 볼 수 있습니다.	vApp
vApp.vApp 애플리케이션 구성	제품 정보 및 속성 같은 vApp의 내부 구조를 수정할 수 있습니다.	vApp
vApp.vApp 인스턴스 구성	정책 같은 vApp의 인스턴스 구성을 수정할 수 있습니다.	vApp
vApp.vApp managedBy 구성	확장 또는 솔루션을 통해 vApp을 해당 확장 또는 솔루션에서 관리하는 것으로 표시할 수 있습니다. 이 권한과 연결된 vSphere Web Client 사용자 인터페이스 요소는 없습니다.	vApp
vApp.vApp 리소스 구성	vApp의 리소스 구성을 수정할 수 있습니다. 이 작업을 수행하기 위한 권한을 얻으려면 사용자 또는 그룹이 개체와 상위 개체 모두에 이 권한을 할당해야 합니다.	vApp

vServices 권한

vServices 권한은 가상 시스템 및 vApp에 대한 vService 종속성을 만들고 구성하고 업데이트하는 기능을 제어합니다.

계층의 서로 다른 수준에서 이 권한을 설정할 수 있습니다. 예를 들어 폴더 수준에서 권한을 설정하는 경우 폴더 내 하나 이상의 개체로 권한을 전파할 수 있습니다. 필수 열에 나열된 개체에는 직접 또는 상속을 통해 권한이 설정되어 있어야 합니다.

표 11-39. vServices

권한 이름	설명	필수
vService.종속성 생성	가상 시스템이나 vApp에 대한 vService 종속성을 만들 수 있습니다.	vApp 및 가상 시스템
vService.종속성 제거	가상 시스템이나 vApp에 대한 vService 종속성을 제거할 수 있습니다.	vApp 및 가상 시스템
vService.종속성 재구성	종속성을 재구성하여 제공자 또는 바인딩을 업데이트할 수 있습니다.	vApp 및 가상 시스템
vService.종속성 업데이트	종속성을 업데이트하여 이름 또는 설명을 구성할 수 있습니다.	vApp 및 가상 시스템