vSphere 보안

업데이트 3
수정 날짜: 2022년 11월 23일
VMware vSphere 7.0
VMware ESXi 7.0
vCenter Server 7.0

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

목차

vSphere 보안 정보 14

업데이트된 정보 17

1 vSphere 환경의 보안 20

ESXi 하이퍼바이저 보안 20

vCenter Server 시스템 및 관련 서비스 보안 22

가상 시스템 보안 23

가상 네트워킹 계층 보호 25

vSphere 환경의 암호 26

보안 모범 사례 및 리소스 27

2 vSphere 사용 권한 및 사용자 관리 작업 29

vSphere의 권한 부여 이해 30

사용 권한의 계층적 상속 34

여러 가지 사용 권한 설정 37

예1: 여러 그룹의 사용 권한 상속 37

예 2: 상위 사용 권한을 재정의하는 하위 사용 권한 38

예 3: 그룹 역할을 재정의하는 사용자 역할 39

vCenter 구성 요소에 대한 사용 권한 관리 39

인벤토리 개체에 사용 권한 추가 40

사용 권한 변경 또는 제거 40

사용자 검증 설정 변경 41

글로벌 사용 권한 42

글로벌 사용 권한 추가 42

태그 개체에 대한 사용 권한 43

역할을 사용하여 권한 할당 45

vCenter Server 사용자 지정 역할 생성 46

vCenter Server 시스템 역할 47

역할 및 권한에 대한 모범 사례 48

일반 작업에 필요한 권한 49

3 ESXi 호스트 보안 53

일반 ESXi 보안 권장 사항 54

고급 시스템 설정 55

호스트 프로파일을 사용하여 ESXi 호스트 구성 58

스크립트를 사용하여 호스트 구성 설정 관리 58
ESXi 암호 및 계정 잠금 60
암호화 키 생성 62
SSH 보안 63
ESXi SSH 키 63
PCI와 PCIe 디바이스 및 ESXi 65
MOB(Managed Object Browser) 사용 안 함 66
ESXi 네트워킹 보안 권장 사항 66
ESXi 웹 프록시 설정 수정 67
vSphere Auto Deploy 보안 고려 사항 68
CIM 기반 하드웨어 모니터링 도구에 대한 액세스 제어 68
ESXi 호스트에 대한 인증서 관리 70
호스트 업그레이드 및 인증서 72
인증서 모드 전환 워크플로 72
ESXi 인증서 기본 설정 74
인증서 기본 설정 변경 75
여러 ESXi 호스트에 대한 인증서 만료 정보 보기 76
단일 ESXi 호스트에 대한 인증서 세부 정보 보기 77
ESXi 인증서 갱신 또는 새로 고침 77
인증서 모드 변경 78
ESXi SSL 인증서 및 키 교체 79
ESXi 인증서 서명 요청에 대한 요구 사항 80
ESXi Shell에서 기본 인증서 및 키 교체 81
vifs 명령을 사용하여 기본 인증서 및 키 교체 81
HTTPS PUT를 사용하여 기본 인증서 교체 82
vCenter Server TRUSTED_ROOTS 스토어 업데이트(사용자 지정 인증서) 83
Auto Deploy와 함께 사용자 지정 인증서 사용 84
ESXi 인증서 및 키 파일 복원 85
보안 프로파일을 사용하여 호스트 사용자 지정 86
ESXi 방화벽 구성 86
ESXi 방화벽 설정 관리 87
ESXi 호스트에 대해 허용되는 IP 주소 추가 88
ESXi 호스트에 대해 들어오고 나가는 방화벽 포트 89
NFS 클라이언트 방화벽 동작 89
ESXi ESXCLI 방화벽 명령 90
보안 프로파일에서 ESXi 서비스 사용자 지정 91
서비스 사용 또는 사용 안 함 92
잠금 모드 93
잠금 모드 동작 94
잠금 모드 사용 95

잠금 모드 사용 안 함 95
Direct Console User Interface에서 정상 잠금 모드 사용 또는 사용 안 함 96
잠금 모드에서 액세스 권한을 가진 계정 지정 97
VIB를 사용하여 보안 업데이트 수행 98
호스트 및 VIB의 수락 수준 관리 99
ESXi 호스트에 대한 권한 할당 101
Active Directory를 통해 ESXi 사용자 관리 103
Active Directory를 사용하도록 호스트 구성 103
디렉토리 서비스 도메인에 호스트 추가 105
디렉토리 서비스 설정 보기 105
vSphere Authentication Proxy 사용 106
vSphere Authentication Proxy를 사용하도록 설정 107
vSphere Client를 사용하여 vSphere Authentication Proxy에 도메인 추가 107
camconfig 명령을 사용하여 vSphere Authentication Proxy에 도메인 추가 108
vSphere Authentication Proxy를 사용하여 도메인에 호스트 추가 109
vSphere Authentication Proxy에 대한 클라이언트 인증을 사용하도록 설정 110
ESXi 호스트에 vSphere Authentication Proxy 인증서 가져오기 110
vSphere Authentication Proxy용 새 인증서 생성 111
사용자 지정 인증서를 사용하도록 vSphere Authentication Proxy 설정 112
ESXi에 대한 스마트 카드 인증 구성 113
스마트 카드 인증 사용 114
스마트 카드 인증 사용 안 함 115
연결 문제 발생 시 사용자 이름과 암호를 사용하여 인증 115
잠금 모드에서 스마트 카드 인증 사용 115
ESXi Shell 사용 116
ESXi Shell에 대한 액세스를 사용하도록 설정 116
ESXi Shell 가용성에 대한 시간 초과 설정 생성 117
유휴 ESXi Shell 세션에 대한 시간 초과 설정 생성 118
Direct Console User Interface를 사용하여 ESXi Shell에 액세스할 수 있도록 설정 118
ESXi Shell에 대한 가용성 시간 초과 또는 유휴 시간 초과 설정 119
문제 해결을 위해 ESXi Shell에 로그인 120
ESXi 호스트를 위한 UEFI 보안 부팅 120
업그레이드된 ESXi 호스트에서 보안 부팅 유효성 검사 스크립트 실행 122
신뢰할 수 있는 플랫폼 모듈을 통한 ESXi 호스트 보안 123
ESXi 호스트 증명 상태 보기 124
ESXi 호스트 무결성 문제 해결 125
ESXi 로그 파일 125
ESXi 호스트의 Syslog 구성 126
ESXi 로그 파일 위치 127
Fault Tolerance 로깅 트래픽 보안 128

Fault Tolerance 암호화 사용 128
ESXi 감사 레코드 관리 129
ESXi 구성 보호 130
ESXi 구성 보호 개요 130
TPM 봉인 정책 개요 132
보안 ESXi 구성 관리 133
보안 ESXi 구성 복구 키의 컨텐츠 나열 133
보안 ESXi 구성 복구 키 순환 133
보안 ESXi 구성 문제 해결 및 복구 134
보안 ESXi 구성 복구 134
보안 ESXi 구성에 대한 보안 부팅 적용 사용 또는 사용 안 함 135
보안 ESXi 구성에 대한 execInstalledOnly 적용 사용 또는 사용 안 함 138

4 vCenter Server 시스템 보안 142
vCenter Server 보안 모범 사례 142
vCenter Server 액세스 제어에 대한 모범 사례 142
vCenter Server 암호 정책 설정 144
실패한 설치에서 만료되거나 해지된 인증서 및 로그 제거 144
vCenter Server 네트워크 연결 제한 145
CLI 및 SDK와 함께 Linux 클라이언트 사용 평가 145
클라이언트 플러그인 검사 146
vCenter Server 보안 모범 사례 146
vCenter 암호 요구 사항 및 잠금 동작 147
기존 ESXi 호스트 지문 확인 148
vCenter Server의 필수 포트 148

5 가상 시스템 보안 150
가상 시스템에 대해 UEFI 보안 부팅 사용 또는 사용 안 함 150
가상 시스템에서 VMX 파일로의 정보 메시지 제한 152
가상 시스템 보안 모범 사례 152
일반 가상 시스템 보호 153
템플릿을 사용하여 가상 시스템 배포 154
가상 시스템 콘솔 사용 최소화 154
가상 시스템의 리소스 대체 방지 155
가상 시스템 내의 불필요한 기능 사용 안 함 155
불필요한 하드웨어 디바이스 제거 156
사용되지 않는 표시 기능 사용 안 함 157
표시되지 않는 기능 사용 안 함 157
가상 시스템에 호스트 파일을 공유하는 VMware 공유 폴더를 사용하지 않도록 설정 158
게스트 운영 체제와 원격 콘솔 간에 복사하여 붙여넣기 작업 사용 안 함 159

클립보드에 복사된 중요한 데이터의 노출 제한 159
사용자가 가상 시스템 내에서 명령을 실행하지 못하도록 제한 160
가상 시스템 사용자 또는 프로세스가 디바이스와 연결이 끊어지지 않도록 방지 161
게스트 운영 체제 프로세스가 호스트에 구성 메시지를 보내지 않도록 방지 161
독립형 비영구 디스크 사용 방지 162
Intel Software Guard Extensions를 사용하여 가상 시스템 보호 162
vSGX 개요 163
가상 시스템에서 vSGX 사용 164
기존 가상 시스템에서 vSGX 사용 164
가상 시스템에서 vSGX 제거 165
AMD Secure Encrypted Virtualization-Encrypted State를 사용하여 가상 시스템 보호 166
AMD SEV-ES(Secure Encrypted Virtualization-Encrypted State) 개요 166
vSphere Client를 사용하여 가상 시스템에 AMD SEV-ES(Secure Encrypted Virtualization-Encrypted State) 추가 167
가상 시스템에 AMD SEV-ES(Secure Encrypted Virtualization-Encrypted State) 추가 168
vSphere Client를 사용하여 기존 가상 시스템에서 AMD SEV-ES(Secure Encrypted Virtualization-Encrypted State)를 사용하도록 설정 169
기존 가상 시스템에서 AMD SEV-ES(Secure Encrypted Virtualization-Encrypted State) 사용 170
vSphere Client를 사용하여 가상 시스템에 AMD SEV-ES(Secure Encrypted Virtualization-Encrypted State)를 사용하지 않도록 설정 172
가상 시스템에서 AMD SEV-ES(Secure Encrypted Virtualization-Encrypted State) 사용 안 함 172

6 가상 시스템 암호화 174
vSphere 키 제공자 비교 175
vSphere 가상 시스템 암호화를 통해 환경을 보호하는 방법 177
vSphere 가상 시스템 암호화 구성 요소 181
암호화 프로세스 흐름 183
가상 디스크 암호화 186
가상 시스템 암호화 오류 187
암호화 작업의 사전 요구 사항 및 필요한 권한 187
vSphere vMotion 암호화 189
암호화 모범 사례, 주의 사항 및 상호 운용성 192
가상 시스템 암호화 모범 사례 192
가상 시스템 암호화 주의 사항 195
가상 시스템 암호화 상호 운용성 196
키 지속성 개요 199

7 표준 키 제공자 구성 및 관리 201
표준 키 제공자 개요 201

표준 키 제공자 설정 202
vSphere Client를 사용하여 표준 키 제공자 추가 202
인증서를 교환하여 표준 키 제공자 신뢰할 수 있는 연결 설정 204
루트 CA 인증서 옵션을 사용하여 표준 키 제공자 신뢰할 수 있는 연결 설정 204
인증서 옵션을 사용하여 표준 키 제공자 신뢰할 수 있는 연결 설정 205
인증서 및 개인 키 업로드 옵션을 사용하여 표준 키 제공자 신뢰할 수 있는 연결 설정 206
새 인증서 서명 요청 옵션을 사용하여 표준 키 제공자 신뢰할 수 있는 연결 설정 206
기본 키 제공자 설정 207
표준 키 제공자에 대한 신뢰 설정 완료 207
서로 다른 사용자를 위해 별도의 키 제공자 설정 208

8 vSphere Native Key Provider 구성 및 관리 210
vSphere Native Key Provider 개요 210
vSphere Native Key Provider 프로세스 흐름 213
vSphere Native Key Provider 구성 214
vSphere Native Key Provider 백업 215
고급 연결 모드 구성에서 vSphere Native Key Provider 가져오기 216
vSphere Native Key Provider 복구 217
vSphere Client를 사용하여 vSphere Native Key Provider 복원 218
vSphere Native Key Provider 업데이트 219
vSphere Native Key Provider 삭제 220

9 vSphere 신뢰 기관 221
vSphere 신뢰 기관 개념 및 기능 221
vSphere 신뢰 기관에서 환경을 보호하는 방식 221
신뢰할 수 있는 인프라 개요 225
vSphere 신뢰 기관 프로세스 흐름 227
vSphere 신뢰 기관 토폴로지 230
vSphere 신뢰 기관에 대한 사전 요구 사항 및 필요한 권한 231
vSphere 신뢰 기관 모범 사례, 주의 사항 및 상호 운용성 233
vSphere 신뢰 기관 수명 주기 234
vSphere 신뢰 기관 구성 236
Workstation 설정 238
신뢰 기관 관리자 사용 239
신뢰 기관 상태 사용 240
신뢰할 수 있는 ESXi 호스트 및 vCenter Server에 대한 정보 수집 241
TPM 승인 키 인증서 내보내기 및 가져오기 246
신뢰 기관 클러스터로 신뢰할 수 있는 호스트 정보 가져오기 251
신뢰 기관 클러스터에서 키 제공자 생성 254
클라이언트 인증서를 업로드하여 신뢰할 수 있는 키 제공자가 신뢰할 수 있는 연결 설정 259

인증서 및 개인 키를 업로드하여 신뢰할 수 있는 키 제공자가 신뢰할 수 있는 연결 설정 261
인증서 서명 요청을 생성하여 신뢰할 수 있는 키 제공자가 신뢰할 수 있는 연결 설정 262
신뢰 기관 클러스터 정보 내보내기 264
신뢰할 수 있는 호스트로 신뢰 기관 클러스터 정보 가져오기 266
vSphere Client를 사용하여 신뢰할 수 있는 호스트를 위한 신뢰할 수 있는 키 제공자 구성 271
명령줄을 사용하여 신뢰할 수 있는 호스트를 위한 신뢰할 수 있는 키 제공자 구성 272
vSphere 환경에서 vSphere 신뢰 기관 관리 273
vSphere 신뢰 기관 서비스 시작, 중지 및 다시 시작 274
신뢰 기관 호스트 보기 274
vSphere 신뢰 기관 클러스터 상태 보기 274
신뢰할 수 있는 호스트 서비스 다시 시작 275
vSphere 신뢰 기관 호스트 추가 및 제거 275
vSphere Client를 사용하여 신뢰할 수 있는 클러스터에 호스트 추가 275
CLI를 사용하여 신뢰할 수 있는 클러스터에 호스트 추가 276
신뢰할 수 있는 클러스터에서 신뢰할 수 있는 호스트 서비스 해제 277
vSphere 신뢰 기관 구성 백업 279
키 제공자의 기본 키 변경 279
신뢰할 수 있는 호스트 증명 보고 개요 280
신뢰할 수 있는 클러스터 증명 상태 보기 281
신뢰할 수 있는 호스트 증명 문제 해결 282
신뢰할 수 있는 클러스터 상태 확인 및 업데이트 적용 282
신뢰할 수 있는 클러스터 상태 및 업데이트 적용 개요 283
신뢰할 수 있는 클러스터 상태 확인 284
신뢰할 수 있는 클러스터에 업데이트 적용 285

10 vSphere 환경에서 암호화 사용 286

암호화 스토리지 정책 생성 286
호스트 암호화 모드를 사용하도록 명시적으로 설정 287
API를 사용하여 호스트 암호화 모드 사용 안 함 287
암호화된 가상 시스템 생성 289
암호화된 가상 시스템 복제 290
기존 가상 시스템 또는 가상 디스크 암호화 292
암호화된 가상 시스템 또는 가상 디스크 암호 해독 293
가상 디스크에 대한 암호화 정책 변경 294
없는 키 문제 해결 295
잠긴 가상 시스템의 잠금 해제 296
ESXi 호스트 암호화 모드 문제 해결 297
ESXi 호스트 암호화 모드를 다시 사용하도록 설정 298
키 관리 서버 인증서 만료 임계값 설정 298
vSphere 가상 시스템 암호화 및 코어 덤프 299

암호화를 사용하는 ESXi 호스트에 대해 vm-support 패키지 수집 300
암호화된 코어 덤프 암호 해독 또는 다시 암호화 301
ESXi 호스트에서 키 지속성 사용 및 사용 안 함 302
vSphere Client를 사용하여 암호화된 가상 시스템 키 재생성 303

11 신뢰할 수 있는 가상 플랫폼 모듈로 가상 시스템 보호 305
신뢰할 수 있는 가상 플랫폼 모듈 개요 305
신뢰할 수 있는 가상 플랫폼 모듈을 사용하여 가상 시스템 생성 307
기존 가상 시스템에 신뢰할 수 있는 가상 플랫폼 모듈을 사용하도록 설정 308
가상 시스템에서 신뢰할 수 있는 가상 플랫폼 모듈 제거 309
신뢰할 수 있는 가상 플랫폼 모듈이 사용되도록 설정된 가상 시스템 식별 310
신뢰할 수 있는 가상 플랫폼 모듈 디바이스 인증서 보기 310
신뢰할 수 있는 가상 플랫폼 모듈 디바이스 인증서 내보내기 및 교체 311

12 가상화 기반 보안을 사용한 Windows 게스트 운영 체제 보호 313
가상화 기반 보안 모범 사례 313
가상 시스템에서 가상화 기반 보안을 사용하도록 설정 315
기존 가상 시스템에서 가상화 기반 보안을 사용하도록 설정 316
게스트 운영 체제에서 가상화 기반 보안을 사용하도록 설정 317
가상화 기반 보안을 사용하지 않도록 설정 317
VBS를 사용하는 가상 시스템 식별 318

13 vSphere 네트워킹 보호 319
vSphere 네트워크 보안 소개 319
방화벽으로 네트워크 보호 321
vCenter Server 구성을 위한 방화벽 321
방화벽을 통해 vCenter Server에 연결 322
방화벽을 통해 ESXi 호스트 연결 322
vCenter Server가 없는 구성을 위한 방화벽 323
방화벽을 통해 가상 시스템 콘솔에 연결 323
물리적 스위치 보호 324
보안 정책으로 표준 스위치 포트 보호 325
vSphere 표준 스위치 보안 325
MAC 주소 변경 사항 326
위조 전송 327
비규칙(Promiscuous) 모드 작업 327
표준 스위치 보호 및 VLAN 327
vSphere Distributed Switch 및 분산 포트 그룹 보안 329
VLAN으로 가상 시스템 보호 330
VLAN에 대한 보안 고려 사항 331

VLAN 보호 331
단일 ESXi 호스트 내에 여러 네트워크 생성 332
인터넷 프로토콜 보안 334
사용 가능한 보안 연결 나열 334
IPsec 보안 연결 추가 334
IPsec 보안 연결 제거 335
사용 가능한 IPsec 보안 정책 나열 336
IPSec 보안 정책 생성 336
IPsec 보안 정책 제거 337
적절한 SNMP 구성 확인 338
vSphere 네트워킹 보안 모범 사례 338
일반 네트워킹 보안 권장 사항 339
네트워킹 구성 요소 레이블 지정 340
vSphere VLAN 환경 문서화 및 확인 340
네트워크 분리 방식 채택 341
필요한 경우에만 vSphere Network Appliance API의 가상 스위치 사용 342

14 여러 vSphere 구성 요소와 관련된 모범 사례 344
vSphere 네트워크에서 클럭 동기화 344
네트워크 시간 서버와 ESXi 클럭 동기화 345
vCenter Server에서 시간 동기화 설정 구성 346
VMware Tools 시간 동기화 사용 346
vCenter Server 구성에서 NTP 서버 추가 또는 바꾸기 346
NTP 서버와 vCenter Server의 시간 동기화 347
스토리지 보안 모범 사례 348
iSCSI 스토리지 보안 348
iSCSI 장치 보안 348
iSCSI SAN 보호 349
SAN 리소스 마스킹 및 영역 설정 350
NFS 4.1에 Kerberos 사용 350
게스트로 호스트 성능 데이터 보내기가 사용하지 않도록 설정되었는지 확인 351
ESXi Shell 및 vSphere Client에 대한 시간 제한 설정 352

15 TLS 구성 유틸리티를 사용하여 TLS 프로토콜 구성 관리 353
TLS 버전을 사용하지 않도록 설정 가능한 포트 353
vSphere에서 TLS 버전을 사용하거나 사용하지 않도록 설정 354
선택적 수동 백업 수행 355
vCenter Server 시스템에서 TLS 버전을 사용하거나 사용하지 않도록 설정 356
ESXi 호스트에서 TLS 버전을 사용하거나 사용하지 않도록 설정 356
vCenter Server에서 사용하도록 설정된 TLS 프로토콜 검색 358

TLS 구성 변경 내용 되돌리기 359

16 정의된 권한 360

경보 권한 362
Auto Deploy 및 이미지 프로파일 권한 363
인증서 권한 363
인증 기관 권한 364
인증서 관리 권한 364
Cns 권한 364
컨텐츠 라이브러리 권한 365
암호화 작업 권한 367
dvPort 그룹 권한 369
Distributed Switch 권한 369
데이터 센터 권한 370
데이터스토어 권한 371
데이터스토어 클러스터 권한 372
ESX Agent Manager 권한 372
확장 권한 373
외부 통계 제공자 권한 373
폴더 권한 373
글로벌 권한 373
상태 업데이트 제공자 권한 375
호스트 CIM 권한 375
호스트 구성 권한 375
호스트 인벤토리 376
호스트 로컬 작업 권한 377
호스트 vSphere 복제 권한 378
호스트 프로파일 권한 378
vSphere with Tanzu 권한 378
네트워크 권한 379
성능 권한 380
사용 권한에 대한 권한 380
프로파일 기반 스토리지 권한 380
리소스 권한 381
스케줄링된 작업 권한 382
세션 권한 382
스토리지 보기 권한 382
작업 권한 383
전송 서비스 권한 383
VcTrusts/VcIdentity 권한 383

신뢰할 수 있는 인프라 관리자 권한 384
vApp 권한 385
VcIdentityProviders 권한 386
VMware vSphere Lifecycle Manager 구성 권한 386
VMware vSphere Lifecycle Manager ESXi 상태 관점 권한 387
VMware vSphere Lifecycle Manager 일반 권한 387
VMware vSphere Lifecycle Manager 하드웨어 호환성 권한 388
VMware vSphere Lifecycle Manager 이미지 권한 388
VMware vSphere Lifecycle Manager 이미지 업데이트 적용 권한 389
VMware vSphere Lifecycle Manager 설정 권한 390
VMware vSphere Lifecycle Manager 기준선 관리 권한 390
VMware vSphere Lifecycle Manager 패치 및 업그레이드 관리 권한 391
VMware vSphere Lifecycle Manager 파일 업로드 권한 391
가상 시스템 구성 권한 392
가상 시스템 게스트 작업 권한 394
가상 시스템 상호 작용 권한 395
가상 시스템 인벤토리 권한 397
가상 시스템 프로비저닝 권한 398
가상 시스템 서비스 구성 권한 399
가상 시스템 스냅샷 관리 권한 399
가상 시스템 vSphere 복제 권한 400
vServices 권한 400
vSphere 태그 지정 권한 401
vSphere Client 권한 402

17 vSphere 강화 및 규정 준수 이해 403
vSphere 환경의 보안 및 규정 준수 403
vSphere 보안 구성 가이드 이해 405
National Institute of Standards and Technology 정보 408
DISA STIG 정보 408
VMware 보안 개발 수명 주기 정보 409
감사 로깅 409
Single Sign-On 감사 이벤트 409
보안 및 규정 준수 이해 다음 단계 411
vCenter Server 및 FIPS 411
FIPS 모듈 412
vCenter Server Appliance에서 FIPS 사용 또는 사용 안 함 412
FIPS 사용 시 고려 사항 413

vSphere 보안 정보

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

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

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
사용 권한 및 사용자 관리	■ 사용 권한 모델(역할, 그룹, 개체) ■ 사용자 지정 역할 생성 ■ 사용 권한 설정 ■ 글로벌 사용 권한 관리
호스트 보안 기능	■ 잠금 모드 및 기타 보안 프로파일 기능 ■ 호스트 스마트 카드 인증 ■ vSphere Authentication Proxy ■ UEFI 보안 부팅 ■ TPM(신뢰할 수 있는 플랫폼 모듈) ■ VMware® vSphere 신뢰 기관™. ■ 보안 ESXi 구성 및 구성 봉인
가상 시스템 암호화	■ VMware vSphere® Native Key Provider™. ■ VM 암호화의 작동 방식 ■ KMS 설정 ■ VM 암호화 및 암호 해독 ■ 문제 해결 및 모범 사례
게스트 운영 체제 보안	■ vTPM(신뢰할 수 있는 가상 플랫폼 모듈) ■ VBS(가상화 기반 보안)
TLS 프로토콜 구성 관리	명령줄 유틸리티를 사용하여 TLS 프로토콜 구성 변경

표 1-1. "vSphere 보안" 하이라이트 (계속)

항목	컨텐츠 하이라이트
보안 모범 사례 및 강화	VMware 보안 전문가의 모범 사례 및 조언 ■ vCenter Server 보안 ■ 호스트 보안 ■ 가상 시스템 보안 ■ 네트워킹 보안
vSphere 권한	이 릴리스에서 지원되는 모든 vSphere 권한의 전체 목록

관련 설명서

함께 제공되는 문서인 "vSphere 인증" 에는 인증 서비스를 사용하여 vCenter Single Sign-On을 사용한 인증 관리 및 vSphere 환경의 인증서 관리와 같은 작업을 수행할 수 있는 방법이 설명되어 있습니다.

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

Platform Services Controller 변경 사항

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

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

대상 사용자

이 정보는 가상 시스템 기술과 데이터 센터 운영에 대해 잘 알고 있는 숙련된 시스템 관리자를 대상으로 작성되었습니다.

인증

VMware는 공통 조건 인증을 완료한 VMware 제품 공개 목록을 게시합니다. 특정 VMware 제품 버전이 인증되었는지 확인하려면 CCEVS(Common Criteria Evaluation and Validation) 웹 페이지(https://www.vmware.com/security/certifications/common-criteria.html)를 참조하십시오.

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 11월 23일	■ vCenter Server 시스템 역할에 대한 부분적 업데이트. ■ vSphere Native Key Provider에 대한 추가 정보로 키 지속성 개요 및 ESXi 호스트에서 키 지속성 사용 및 사용 안 함 항목이 업데이트되었습니다. ■ VLAN 보호에 대한 부분적 업데이트.
2022년 10월 13일	■ ESXi 감사 레코드 관리에 대한 부분적 업데이트. ■ vSphere Native Key Provider 업데이트에서 오타가 수정되었습니다. ■ 가상화 기반 보안 모범 사례, 가상 시스템에서 가상화 기반 보안을 사용하도록 설정 및 기존 가상 시스템에서 가상화 기반 보안을 사용하도록 설정에 대한 부분적인 업데이트가 있습니다. ■ `vifs` 명령에 대한 참조가 제거되었습니다. VMware 기술 자료 문서(https://kb.vmware.com/article/78473)를 참조하십시오.
2022년 8월 22일	■ ESXi 인증서 갱신 또는 새로 고침에 대한 부분적 업데이트. ■ vSphere Native Key Provider 삭제에 대한 부분적 업데이트. ■ 신뢰 기관 클러스터에서 키 제공자 생성의 예시가 수정되었습니다. ■ API를 사용하여 호스트 암호화 모드 사용 안 함 MOB(Managed Object Browser)를 사용하도록 vCenter Server 항목을 다시 작성했습니다. ■ 여러 VMware vSphere Lifecycle Manager 권한 항목이 부분적으로 업데이트되었습니다.
2022년 7월 28일	■ ESXi 인증서 서명 요청에 대한 요구 사항에 대한 부분적 업데이트. ■ 신뢰할 수 있는 가상 플랫폼 모듈 개요에 대한 부분적 업데이트. ■ MAC 주소 변경 사항에 대한 부분적 업데이트. ■ URL을 수락하는 VMware vSphere Lifecycle Manager API를 사용하는 권한은 관리자 또는 신뢰할 수 있는 사용자에게만 할당해야 한다는 점을 설명하기 위해 여러 항목이 업데이트되었습니다.
2022년 7월 12일	■ 사용자 검증 설정 변경에 대한 부분적 업데이트. ■ ESXi 인증서 갱신 또는 새로 고침에 대한 부분적 업데이트. ■ Fault Tolerance 암호화 사용에 대한 부분적 업데이트. ■ 보안 ESXi 구성에 대한 execInstalledOnly 적용 사용 또는 사용 안 함에서 ESXCLI 명령의 형식 문제가 수정되었습니다. ■ 사용되지 않는 표시 기능 사용 안 함에 대한 부분적 업데이트. ■ 표시되지 않는 기능 사용 안 함에서 이제 TRUE로 설정된 매개 변수가 제거되었습니다. ■ 암호화 스토리지 정책 생성의 단계가 수정되었습니다.

개정	설명
2022년 6월 15일	■ vCenter Server 및 암호화된 통신에 대한 정보가 vCenter Server 시스템 및 관련 서비스 보안에 추가되었습니다. ■ vSphere Distributed Switch에 대한 사용 권한 할당에 대한 정보가 사용 권한의 계층적 상속에 추가되었습니다. ■ ESXi 호스트를 위한 UEFI 보안 부팅에 대한 부분적 업데이트. ■ 암호화 고려 사항에 대한 정보가 가상 시스템 암호화 모범 사례에 추가되었습니다. ■ vSphere Native Key Provider 개요에 대한 부분적 업데이트. ■ `HostCryptoState`에 대한 정보가 API를 사용하여 호스트 암호화 모드 사용 안 함에 추가되었습니다. ■ 필수 권한인 **Cryptographic operations.Migrate**가 신뢰할 수 있는 가상 플랫폼 모듈을 사용하여 가상 시스템 생성 및 기존 가상 시스템에 신뢰할 수 있는 가상 플랫폼 모듈을 사용하도록 설정에 추가되었습니다. 이 권한을 사용하면 DRS가 다른 호스트에서 가상 시스템을 시작할 때 가상 시스템의 전원을 켤 수 있습니다. ■ 방화벽을 통해 가상 시스템 콘솔에 연결에 대한 부분적 업데이트. ■ ESXi 호스트에서 TLS 버전을 사용하거나 사용하지 않도록 설정에 대한 부분적 업데이트. ■ 사용 권한 설정에 대한 정보가 컨텐츠 라이브러리 권한에 추가되었습니다. ■ vSphere 태그 지정 권한에서 오타가 수정되었습니다.
2022년 4월 29일	■ ESXi 감사 레코드 관리에서 `viewAudit` 프로그램은 vSphere 7.0 업데이트 3d부터 `auditLogReader` 프로그램을 대체합니다. ■ 보안 ESXi 구성에 대한 보안 부팅 적용 사용 또는 사용 안 함 및 보안 ESXi 구성에 대한 execInstalledOnly 적용 사용 또는 사용 안 함에 대한 부분적인 업데이트. ■ vSphere 가상 시스템 암호화를 통해 환경을 보호하는 방법에 대한 사소한 업데이트가 있습니다. ■ 키 지속성 개요, vSphere Native Key Provider 백업 및 ESXi 호스트에서 키 지속성 사용 및 사용 안 함에서 vSphere Native Key Provider 및 키 지속성에 대한 정보가 업데이트되었습니다. ■ vSphere Native Key Provider 개요에 대한 부분적 업데이트. ■ vSphere Native Key Provider 업데이트에서 명령이 수정되었습니다. ■ 방화벽을 통해 ESXi 호스트 연결에 대한 부분적 업데이트. ■ 스토리지 보기 권한에 대한 부분적 업데이트.
2022년 3월 10일	■ 호스트 업그레이드 및 인증서에 대한 부분적 업데이트. ■ Auto Deploy와 함께 사용자 지정 인증서 사용의 4단계에서 잘못된 명령이 수정되었습니다. ■ vSphere Client를 사용하여 가상 시스템에 AMD SEV-ES(Secure Encrypted Virtualization-Encrypted State) 추가, 가상 시스템에 AMD SEV-ES(Secure Encrypted Virtualization-Encrypted State) 추가, vSphere Client를 사용하여 기존 가상 시스템에서 AMD SEV-ES(Secure Encrypted Virtualization-Encrypted State)를 사용하도록 설정, 기존 가상 시스템에서 AMD SEV-ES(Secure Encrypted Virtualization-Encrypted State) 사용에서 사전 요구 사항이 업데이트되었습니다. ■ 가상 시스템 암호화 상호 운용성에 대한 부분적 업데이트. ■ vSphere Native Key Provider에 TPM 2.0이 필요하지 않음을 설명하기 위해 vSphere Native Key Provider 개요 항목이 업데이트되었습니다. ■ vSphere Client를 사용하여 신뢰할 수 있는 호스트를 위한 신뢰할 수 있는 키 제공자 구성 및 명령줄을 사용하여 신뢰할 수 있는 호스트를 위한 신뢰할 수 있는 키 제공자 구성에서 vSphere Trust Authority 키 제공자를 추가하는 경우 키 제공자를 사용할 수 있게 되기까지 다소 시간이 소요된다는 점을 명확히 설명했습니다. ■ 신뢰할 수 있는 가상 플랫폼 모듈을 사용하여 가상 시스템 생성, 기존 가상 시스템에 신뢰할 수 있는 가상 플랫폼 모듈을 사용하도록 설정, 가상 시스템에서 신뢰할 수 있는 가상 플랫폼 모듈 제거에 필요한 권한이 추가되었습니다.

개정	설명
2022년 1월 19일	■ vSphere의 권한 부여 이해에 대한 부분적 업데이트. ■ ESXi 인증서 및 키 파일 복원에 대한 부분적 업데이트. ■ 독립형 ESXi 호스트의 경우 vCenter Server 시스템에서 `reconfigureEsx ESXiHost` 명령을 실행해야 한다는 점을 ESXi 호스트에서 TLS 버전을 사용하거나 사용하지 않도록 설정에서 명확히 설명했습니다. ■ FIPS 사용 시 고려 사항 항목이 vCenter Server 파일 기반 백업 및 복원에 대한 정보로 업데이트되었습니다.
2021년 12월 21일	■ vifs 명령을 사용하여 SSH Key 업로드에서 오타가 수정되었습니다. ■ TPM 봉인 정책 개요에 대한 부분적 업데이트. ■ 보안 ESXi 구성에 대한 보안 부팅 적용 사용 또는 사용 안 함에 대한 부분적 업데이트. ■ ESXi 호스트 암호화 모드 문제 해결에 대한 부분적 업데이트. ■ vSphere vMotion 암호화에 대한 부분적 업데이트.
2021년 12월 7일	■ vSphere 키 제공자 비교에 대한 부분적 업데이트. ■ 새 항목(고급 연결 모드 구성에서 vSphere Native Key Provider 가져오기)이 추가되었습니다. ■ vSphere 신뢰 기관 모범 사례, 주의 사항 및 상호 운용성에 대한 부분적 업데이트. ■ 새 항목(vSphere Client를 사용하여 암호화된 가상 시스템 키 재생성)이 추가되었습니다. ■ 컨텐츠 라이브러리 권한 항목이 새로운 권한으로 업데이트되었습니다. ■ vSphere with Tanzu 권한 항목이 새로운 권한으로 업데이트되었습니다.
2021년 11월 3일	■ 가상 네트워킹 계층 보호에 대한 부분적 업데이트. ■ 보안 ESXi 구성에 대한 execInstalledOnly 적용 사용 또는 사용 안 함에 대한 부분적 업데이트. ■ 열을 표시하고 숨기는 방법에 대한 사소한 UI 변경을 반영하기 위해 여러 ESXi 호스트에 대한 인증서 만료 정보 보기, 신뢰할 수 있는 가상 플랫폼 모듈이 사용되도록 설정된 가상 시스템 식별, 신뢰할 수 있는 가상 플랫폼 모듈 디바이스 인증서 보기, VBS를 사용하는 가상 시스템 식별 항목이 업데이트되었습니다. ■ 사소한 UI 변경을 반영하기 위해 ESXi 방화벽 설정 관리 및 ESXi 호스트에 대해 허용되는 IP 주소 추가 항목이 업데이트되었습니다. ■ 가상 시스템 암호화 상호 운용성에 암호화 관련 정보가 추가되었습니다. ■ 두 옵션의 기본값이 수락에서 거부로 변경되었음을 반영하기 위해 MAC 주소 변경 사항 및 위조 전송 항목이 업데이트되었습니다. ■ 가상 시스템 프로비저닝 권한에서 권한이 수정되었습니다. ■ Single Sign-On 감사 이벤트에 대한 부분적 업데이트.
2021년 10월 05일	최초 릴리스

vSphere 환경의 보안

1

vSphere 환경의 구성 요소는 기본적으로 인증, 권한 부여, 각 ESXi 호스트의 방화벽과 같은 몇 가지 기능에 의해 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. 예를 들어 vCenter Server 시스템, ESXi 호스트, 가상 시스템, 네트워크 및 스토리지 개체와 같은 vCenter 개체 계층의 여러 개체에 대해 보안 조치를 취할 수 있습니다.

주의가 필요한 vSphere의 여러 영역을 개괄적으로 파악하면 보안 전략을 계획하는 데 도움이 됩니다. 또한 VMware 웹 사이트에서 다른 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. 일관성을 위해 참조 호스트를 설정하고 모든 호스트가 참조 호스트의 호스트 프로파일과 동기화되도록 유지합니다. 또한 스크립트로 작성된 관리를 수행하여 환경을 보호할 수도 있습니다. 이렇게 하면 변경 내용이 모든 호스트에 적용됩니다.

다음 작업을 통해 vCenter Server로 관리되는 ESXi 호스트의 보호를 개선할 수 있습니다. 배경 및 세부 정보는 "VMware vSphere Hypervisor의 보안" 백서를 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 Server 시스템에서 호스트 개체에 대한 사용 권한을 설정합니다.

명명된 사용자 및 최소 권한 사용

기본적으로 루트 사용자는 여러 작업을 수행할 수 있습니다. 관리자가 루트 사용자 계정을 사용하여 ESXi 호스트에 로그인하도록 허용하지 마십시오. 대신, vCenter Server에서 명명된 관리자를 생성하고 해당 사용자에게 관리자 역할을 할당합니다. 또한 해당 사용자에게 사용자 지정 역할을 할당할 수 있습니다. vCenter Server 사용자 지정 역할 생성의 내용을 참조하십시오.

호스트에서 사용자를 직접 관리하는 경우 역할 관리 옵션이 제한됩니다. "vSphere 단일 호스트 관리 - VMware Host Client" 설명서를 참조하십시오.

열린 ESXi 방화벽 포트의 수 최소화

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

ESXi 방화벽 구성의 내용을 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. 호스트 프로파일을 스크립트로 작성된 관리 대신 사용할 수도 있습니다. 참조 호스트를 설정하고 호스트 프로파일을 내보내고 호스트 프로파일을 모든 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 "vCenter Server 설치 및 설정" 설명서를 참조하십시오.

잠금 모드 이용

잠금 모드에서 ESXi 호스트는 기본적으로 vCenter Server를 통해서만 액세스할 수 있습니다. 엄격 잠금 모드 또는 정상 잠금 모드를 선택할 수 있습니다. 백업 에이전트와 같은 서비스 계정에 직접 액세스할 수 있도록 예외 사용자를 정의할 수 있습니다.

잠금 모드의 내용을 참조하십시오.

VIB 패키지 무결성 검사

각 VIB 패키지에는 관련된 허용 수준이 있습니다. VIB 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 관리의 내용을 참조하십시오.

ESXi 인증서 관리

VMCA(VMware Certificate Authority)는 기본적으로 각 ESXi 호스트에 루트 인증 기관이 VMCA인 서명된 인증서를 프로비저닝합니다. 회사 정책에서 요구하는 경우 기존 인증서를 타사 또는 엔터프라이즈 CA에서 서명된 인증서로 교체할 수 있습니다.

ESXi 호스트에 대한 인증서 관리의 내용을 참조하십시오.

스마트 카드 인증 고려

ESXi는 사용자 이름 및 암호 인증 대신 스마트 카드 인증을 사용하도록 지원합니다. 보안 강화를 위해 스마트 카드 인증을 구성할 수 있습니다. vCenter Server에 2단계 인증도 지원됩니다. 사용자 이름 및 암호 인증과 스마트 카드 인증을 동시에 구성할 수 있습니다.

ESXi에 대한 스마트 카드 인증 구성의 내용을 참조하십시오.

ESXi 계정 잠금 고려

SSH 및 vSphere Web Services SDK를 통한 액세스에 대해 계정 잠금이 지원됩니다. 기본적으로, 계정이 잠기기 전에 최대 10번의 시도 실패가 허용되고 2분 후에는 계정에 대한 잠금이 해제됩니다.

참고 DCUI(Direct Console Interface) 및 ESXi Shell은 계정 잠금을 지원하지 않습니다.

ESXi 암호 및 계정 잠금의 내용을 참조하십시오.

관리 작업은 다를 수 있지만 독립형 호스트에 대한 보안 고려 사항은 유사합니다. "vSphere 단일 호스트 관리 - VMware Host Client" 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 수정할 수 있으며 환경에 대한 액세스를 제한하는 단계를 수행할 수 있습니다.

vSphere 환경을 보호할 때 vCenter Server 인스턴스와 관련된 모든 서비스가 보호되어야 한다는 것을 고려하십시오. 일부 환경에서는 여러 vCenter Server 인스턴스를 보호할 수 있습니다.

vCenter 및 암호화된 통신

기본적으로("즉시 사용 가능") vCenter Server와 다른 vSphere 구성 요소 간의 모든 데이터 통신은 암호화됩니다. 때로는 환경을 구성하는 방법에 따라 일부 트래픽이 암호화되지 않을 수 있습니다. 예를 들어 이메일 경고에는 암호화되지 않은 SMTP를 구성하고 모니터링에는 암호화되지 않은 SNMP를 구성할 수 있습니다. DNS 트래픽도 암호화되지 않습니다. vCenter Server는 포트 80(TCP) 및 포트 443(TCP)에서 수신 대기합니다. 포트 443(TCP)은 업계 표준 HTTPS(보안 HTTP) 포트이며 보호를 위해 TLS 1.2 암호화를 사용합니다. 포트 80(TCP)은 업계 표준 HTTP 포트이며 암호화를 사용하지 않습니다. 포트 80의 목적은 포트 80에서 안전한 포트 443으로 요청을 리디렉션하는 것입니다.

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 VMCA 서명이 있는 인증서를 사용하여 각 ESXi 호스트 및 환경의 각 시스템을 프로비저닝합니다. 회사 정책에 필요하면 기본 동작을 변경할 수 있습니다. 자세한 내용은 "vSphere 인증" 설명서를 참조하십시오.

추가로 보호하려면 만료되거나 해지된 인증서 및 실패한 설치를 명시적으로 제거합니다.

vCenter Single Sign-On 구성

vCenter Server 및 관련 서비스는 vCenter Single Sign-On 인증 프레임워크에 의해 보호됩니다. 처음 소프트웨어를 설치할 때 vCenter Single Sign-On 도메인(기본적으로 administrator@vsphere.local) 관리자의 암호를 지정합니다. 해당 도메인만 처음에 ID 소스로 사용할 수 있습니다. 페더레이션 인증을 위해 Microsoft AD FS(Active Directory Federation Services)와 같은 외부 ID 제공자를 추가할 수 있습니다. Active Directory 또는 LDAP를 사용하는 다른 ID 소스를 추가하고 기본 ID 소스를 설정할 수 있습니다. 이러한 ID 소스 중 하나에 인증할 수 있는 사용자는 권한이 부여된 경우 개체를 보고 작업을 수행할 수 있습니다. 자세한 내용은 "vSphere 인증" 설명서를 참조하십시오.

명명된 사용자 또는 그룹에 역할 할당

로깅을 향상시키기 위해 개체에 제공하는 각 사용 권한을 명명된 사용자 또는 그룹 및 사전 정의된 역할 또는 사용자 지정 역할과 연결합니다. vSphere 사용 권한 모델은 사용자 또는 그룹을 인증하는 다양한 방법을 통해 뛰어난 유연성을 제공합니다. vSphere의 권한 부여 이해 및 일반 작업에 필요한 권한 항목을 참조하십시오.

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

PTP 또는 NTP 설정

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

vSphere 네트워크에서 클럭 동기화의 내용을 참조하십시오.

가상 시스템 보안

가상 시스템을 보호하려면 게스트 운영 체제가 패치되도록 유지하고 환경을 물리적 시스템을 보호하는 것처럼 보호합니다. 불필요한 기능을 사용하지 않도록 설정하는 것을 고려하고 가상 시스템 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 가상 시스템과 원격 콘솔 간에 복사하여 붙여넣기와 같은 특정 기능을 사용하지 않도록 설정합니다.

가상 시스템 내의 불필요한 기능 사용 안 함의 내용을 참조하십시오.

템플릿 및 스크립트로 작성된 관리 기능 사용

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

초기 배포 후 가상 시스템 설정을 변경하려면 PowerCLI와 같은 스크립트 사용을 고려합니다. 이 설명서에서는 GUI를 사용하여 작업을 수행하는 방법을 설명합니다. 환경의 일관성을 유지하기 위해 GUI 대신 스크립트를 사용하는 것이 좋습니다. 대규모 환경에서는 스크립팅을 최적화하기 위해 가상 시스템을 폴더로 그룹화할 수 있습니다.

템플릿에 대한 자세한 내용은 템플릿을 사용하여 가상 시스템 배포 및 "vSphere 가상 시스템 관리" 설명서를 참조하십시오. PowerCLI에 대한 자세한 내용은 VMware PowerCLI 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 있습니다. 따라서 가상 시스템 콘솔 액세스로 인해 가상 시스템이 악의적인 공격을 받을 수 있습니다.

UEFI 보안 부팅 고려

UEFI 부팅을 사용하도록 가상 시스템을 구성할 수 있습니다. 운영 체제에서 UEFI 보안 부팅을 지원하는 경우 추가적인 보안을 위해 VM에 대해 해당 옵션을 선택할 수 있습니다. 가상 시스템에 대해 UEFI 보안 부팅 사용 또는 사용 안 함의 내용을 참조하십시오.

Carbon Black Cloud Workload 고려

Carbon Black Cloud Workload를 설치 및 사용하여 위험을 식별하고, 공격을 방지하고, 비정상적인 작업을 감지할 수 있습니다. Carbon Black Cloud Workload는 Carbon Black Cloud 플랫폼에 내장된 AppDefense 기능을 사용하는 AppDefense의 후속 제품입니다.

가상 네트워킹 계층 보호

가상 네트워킹 계층에는 가상 네트워크 어댑터, 가상 스위치, 분산 가상 스위치, 포트 및 포트 그룹이 포함됩니다. ESXi는 VM과 가상 시스템 사용자 간의 통신을 지원하기 위해 가상 네트워킹 계층에 의존합니다. 또한 ESXi는 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 어댑터와 같은 각 인프라 요소를 별도로 보호할 수 있습니다. 또한 장 13 vSphere 네트워킹 보호에서 보다 자세하게 논의된 다음 지침을 고려하십시오.

네트워크 트래픽 분리

ESXi 환경의 보안을 유지하기 위해서는 네트워크 트래픽을 분리하는 일이 필수적입니다. 필요한 액세스 및 분리 수준은 네트워크마다 다릅니다. 관리 네트워크에서는 클라이언트 트래픽, CLI(명령줄 인터페이스) 또는 API 트래픽, 타사 소프트웨어 트래픽을 일반적인 트래픽에서 분리합니다. 시스템, 네트워크 및 보안 관리자만 관리 네트워크에 액세스할 수 있는지 확인하십시오.

ESXi 네트워킹 보안 권장 사항의 내용을 참조하십시오.

방화벽을 사용하여 가상 네트워크 요소 보호

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

또한 vCenter Server 인스턴스의 포트를 명시적으로 열 수 있습니다.

vSphere 및 vSAN을 포함한 VMware 제품의 지원되는 모든 포트 및 프로토콜 목록은 https://ports.vmware.com/에서 VMware Ports and Protocols Tool™을 참조하십시오. VMware 제품별로 포트를 검색하고, 사용자 지정된 포트 목록을 생성하고, 포트 목록을 인쇄하거나 저장할 수 있습니다.

네트워크 보안 정책 고려

네트워크 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.

VM 네트워킹 보호

VM 네트워킹을 보호하기 위해 사용하는 방법은 다음을 비롯한 다양한 요소에 따라 결정됩니다.

- 설치된 게스트 운영 체제
- VM이 신뢰할 수 있는 환경에서 작동하는지 여부

가상 스위치 및 분산 가상 스위치는 방화벽 설치와 같은 다른 공통적인 보안 모범 사례와 함께 사용할 경우 높은 수준의 보호를 제공합니다.

장 13 vSphere 네트워킹 보호의 내용을 참조하십시오.

환경 보호에 VLAN 고려

ESXi는 IEEE 802.1q VLAN을 지원합니다. VLAN을 사용하면 물리적 네트워크를 세그먼트로 나눌 수 있습니다. VLAN을 사용하여 VM 네트워크나 스토리지 구성을 추가적으로 보호할 수 있습니다. VLAN을 사용하는 경우 동일한 물리적 네트워크에 있는 두 VM이 동일한 VLAN에 속하지 않는 한 서로 패킷을 주고받을 수 없습니다.

VLAN으로 가상 시스템 보호의 내용을 참조하십시오.

가상화된 스토리지에 대한 연결 보호

VM은 운영 체제 파일, 애플리케이션 파일 및 기타 데이터를 가상 디스크에 저장합니다. 각 가상 디스크는 VM에 SCSI 컨트롤러에 연결된 SCSI 드라이브로 표시됩니다. VM은 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 사용하는 경우 CHAP를 사용하도록 환경을 설정할 수 있습니다. 회사 정책에 따라 필요한 경우 상호 CHAP를 설정할 수 있습니다. CHAP를 설정하려면 vSphere Client 또는 CLI를 사용합니다.

스토리지 보안 모범 사례의 내용을 참조하십시오.

IPSec의 사용 평가

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

인터넷 프로토콜 보안의 내용을 참조하십시오.

vSphere 환경의 암호

vSphere 환경의 암호 제한, 암호 만료 및 계정 잠금은 사용자의 대상 시스템이 무엇인지, 사용자가 누구인지, 정책이 어떻게 설정되었는지에 따라 달라집니다.

ESXi 암호

ESXi 암호 제한은 특정 요구 사항에 의해 결정됩니다. ESXi 암호 및 계정 잠금의 내용을 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, 암호 만료 및 계정 잠금은 사용자의 도메인과 사용자가 누구인지에 따라 달라집니다.

vCenter Single Sign-On 관리자

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. 자세한 내용은 "vSphere 인증" 항목을 참조하십시오.

이 사용자의 암호를 잊은 경우 VMware 기술 자료 시스템에서 암호 재설정에 대한 정보를 찾아보십시오. 재설정하려면 vCenter Server 시스템에 대한 루트 액세스 권한과 같은 추가적인 권한이 필요합니다.

vCenter Single Sign-On 도메인의 다른 사용자

다른 vsphere.local 사용자 또는 설치 중 지정한 도메인의 사용자에 대한 암호는 vCenter Single Sign-On 암호 정책 및 잠금 정책에 의해 설정된 제한을 따라야 합니다. 자세한 내용은 "vSphere 인증" 항목을 참조하십시오. 이러한 암호는 기본적으로 90일 후에 만료되지만 관리자가 암호 정책의 일부로 만료 날짜를 변경할 수 있습니다.

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

기타 사용자

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

vCenter Single Sign-On은 하나의 기본 ID 소스를 지원합니다. 사용자는 vSphere Client에서 자신의 사용자 이름을 사용하여 해당 도메인에 로그인할 수 있습니다. 사용자가 기본값이 아닌 도메인에 로그인하려는 경우에는 도메인 이름을 포함할 수 있습니다. 즉, *user*@*domain* 또는 *domain**user*를 지정합니다. 도메인 암호 매개 변수는 각 도메인에 적용됩니다.

vCenter Server Direct Console User Interface 사용자의 암호

vCenter Server Appliance는 vCenter Server와 관련 서비스를 실행하는 데 최적화된 미리 구성된 가상 시스템입니다.

vCenter Server를 배포할 때 다음 암호를 지정합니다.

- 루트 사용자의 암호
- vCenter Single Sign-On 도메인(기본적으로 administrator@vsphere.local) 관리자의 암호

vCenter Server 관리 인터페이스에서 루트 사용자 암호를 변경하고 기타 vCenter Server 로컬 사용자 관리 작업을 수행할 수 있습니다. "vCenter Server 구성" 의 내용을 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	장 3 ESXi 호스트 보안
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 사용해야 하는 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
보안 구성과 하이퍼바이저 보안을 포함하여 ESXi와 vCenter Server의 보안 및 작업에 대한 정보	https://core.vmware.com/security
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. 업계에서는 VMware가 테스트할 수 있는 것보다 훨씬 많은 제품과 구성을 제공합니다. VMware의 호환성 가이드에 없는 제품이나 구성인 경우 기술 지원에서 문제 해결에 도움을 주려고 노력하지만 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	https://core.vmware.com/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
vSphere 및 기타 VMware 제품의 여러 버전에 대한 보안 구성 가이드(이전 명칭: 강화 지침)	https://core.vmware.com/security
"VMware vSphere Hypervisor의 보안" 백서	http://www.vmware.com/files/pdf/techpaper/vmw-wp-secrty-vsphr-hyprvsr-uslet-101.pdf

vSphere 사용 권한 및 사용자 관리 작업

2

인증 및 권한 부여를 통해 액세스가 제어됩니다. vCenter Single Sign-On은 인증을 지원합니다. 즉, 사용자가 vSphere 구성 요소에 로그인할 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 섹션에서는 vCenter Server 사용 권한 모델의 작동 방식과 사용자 관리 작업을 수행하는 방법에 대해 중점적으로 설명합니다.

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 vCenter Single Sign-On 도메인의 관리자만 vCenter Server 시스템에 로그인할 수 있습니다. 기본 도메인은 vsphere.local 이고 기본 관리자는 administrator@vsphere.local입니다. vSphere 설치 중에 기본 도메인을 변경할 수 있습니다.

관리자는 다음과 같이 진행할 수 있습니다.

1 vCenter Single Sign-On에 대해 사용자 및 그룹이 정의되는 ID 소스를 추가합니다. "vSphere 인증" 설명서를 참조하십시오.

2 가상 시스템 또는 vCenter Server 시스템과 같은 개체를 선택하고 사용자 또는 그룹에 이 개체에 대한 역할을 할당하여 사용자 또는 그룹에 권한을 부여합니다.

 (vSphere Client를 사용하여 역할 및 사용 권한 할당)

본 장은 다음 항목을 포함합니다.

- vSphere의 권한 부여 이해
- 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

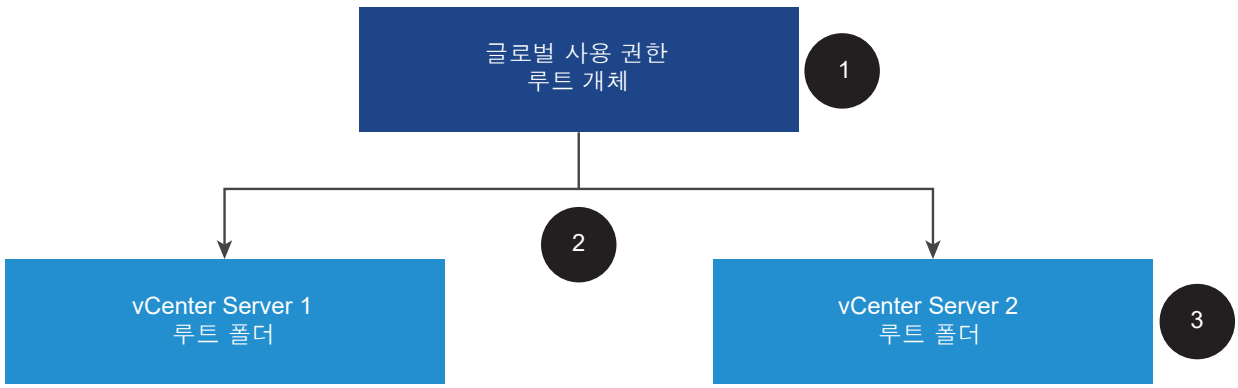
vSphere는 사용자가 작업을 수행할 수 있는지 여부를 결정하기 위한 여러 모델을 지원합니다. vCenter Single Sign-On 그룹의 그룹 멤버 자격은 사용자가 수행할 수 있는 작업을 결정합니다. 개체에 대한 역할 또는 글로벌 사용 권한에 따라 다른 작업을 수행할 수 있는지 여부가 결정됩니다.

권한 부여 개요

vSphere에서는 권한이 있는 사용자가 다른 사용자에게 작업을 수행할 수 있는 사용 권한을 할당할 수 있습니다. 글로벌 사용 권한을 사용하거나, 로컬 vCenter Server 사용 권한을 사용하여 개별 vCenter Server 인스턴스에 대한 권한을 다른 사용자에게 부여할 수 있습니다.

다음 그림은 글로벌 사용 권한과 로컬 사용 권한의 작동 방식에 대해 설명합니다.

그림 2-1. 글로벌 사용 권한 및 로컬 사용 권한



이 그림에서:

1 [하위 항목으로 전파]를 선택한 상태로 루트 개체 수준에서 글로벌 사용 권한을 할당합니다.

2 vCenter Server가 환경의 vCenter Server 1 및 vCenter Server 2 개체 계층에 사용 권한을 전파합니다.

3 vCenter Server 2의 루트 폴더에 대한 로컬 사용 권한이 글로벌 사용 권한을 재정의합니다.

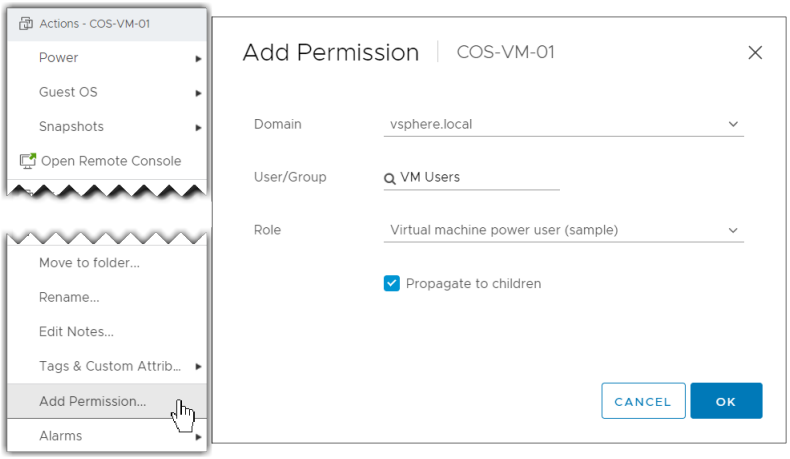
vCenter Server 사용 권한

vCenter Server 시스템의 사용 권한 모델은 개체 계층의 계체에 대한 사용 권한 할당을 사용합니다. 사용자는 다음과 같은 방법으로 사용 권한을 가져옵니다.

- 사용자에 대한 특정 사용 권한에서 또는 사용자가 멤버로 있는 그룹에서
- 개체에 대한 사용 권한에서 또는 상위 개체의 사용 권한 상속을 통해

각 사용 권한은 하나의 사용자 또는 그룹에 일련의 권한, 즉 선택된 개체에 대한 역할을 부여합니다. vSphere Client를 사용하여 사용 권한을 추가할 수 있습니다. 예를 들어 가상 시스템을 마우스 오른쪽 버튼으로 클릭하고 **사용 권한 추가**를 선택한 다음 대화상자를 완료하면 사용자 그룹에 역할을 추가할 수 있습니다. 이 역할을 통해 해당 사용자에게 해당 가상 시스템에 대한 권한이 부여됩니다.

그림 2-2. vSphere Client를 사용하여 가상 시스템에 사용 권한 추가



글로벌 사용 권한

글로벌 사용 권한은 배포 내 솔루션의 각 인벤토리 계층에 있는 모든 개체를 보거나 관리할 수 있는 권한을 사용자 또는 그룹에 부여합니다. 즉, 글로벌 사용 권한은 솔루션 인벤토리 계층에 걸쳐 있는 글로벌 루트 개체에 적용됩니다. (솔루션에는 vCenter Server, vRealize Orchestrator 등이 포함됩니다.) 글로벌 사용 권한은 태그 및 컨텐츠 라이브러리와 같은 글로벌 개체에도 적용됩니다. 예를 들어 vCenter Server 및 vRealize Orchestrator의 두 개 솔루션으로 구성된 배포를 고려합니다. 글로벌 사용 권한을 사용하여 vCenter Server 및 vRealize Orchestrator 개체 계층의 모든 개체에 대해 읽기 전용 권한이 있는 사용자 그룹에 역할을 할당할 수 있습니다.

글로벌 사용 권한은 vCenter Single Sign-On 도메인(기본적으로 vsphere.local) 전체에 복제됩니다. 글로벌 사용 권한은 vCenter Single Sign-On 도메인 그룹을 통해 관리되는 서비스에 대해 권한 부여를 제공하지 않습니다. 글로벌 사용 권한의 내용을 참조하십시오.

vCenter Single Sign-On 그룹의 그룹 멤버 자격

vCenter Single Sign-On 도메인 그룹의 멤버는 특정 작업을 수행할 수 있습니다. 예를 들어 LicenseService.Administrators 그룹의 멤버인 경우 라이센스 관리를 수행할 수 있습니다. "vSphere 인증" 설명서를 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 단일 호스트 관리 - VMware Host Client" 설명서를 참조하십시오.

관리 호스트의 경우 역할을 vCenter Server 인벤토리의 ESXi 호스트 개체에 할당합니다.

개체 수준 사용 권한 모델 이해

개체에 대한 사용 권한을 사용하여 vCenter Server 개체에 대한 작업 수행 권한을 사용자 또는 그룹에 부여합니다. 프로그래밍 관점에서 사용자가 작업을 수행하려고 하면 API 메서드가 실행됩니다. vCenter Server는 해당 메서드에 대한 사용 권한을 검사하여 사용자에게 작업을 수행할 권한이 있는지 확인합니다. 예를 들어 사용자가 호스트를 추가하려고 하면 `AddStandaloneHost_Task` 메소드가 호출됩니다. 이 메소드를 사용하려면 사용자 역할에 **Host.Inventory.Add standalone host** 권한이 있어야 합니다. 검사에서 이 권한을 찾지 못하면 사용자는 호스트를 추가할 수 있는 사용 권한이 거부됩니다.

다음 개념이 중요합니다.

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 사용자에 대해 지정됩니다. 사용 권한은 하위 개체에 전파될 수 있습니다.

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-On이 인증하는 데 사용하는 ID 소스에 사용자 및 그룹을 정의해야 합니다. Active Directory와 같은 ID 소스에서 도구를 사용하여 사용자 및 그룹을 정의합니다.

권한

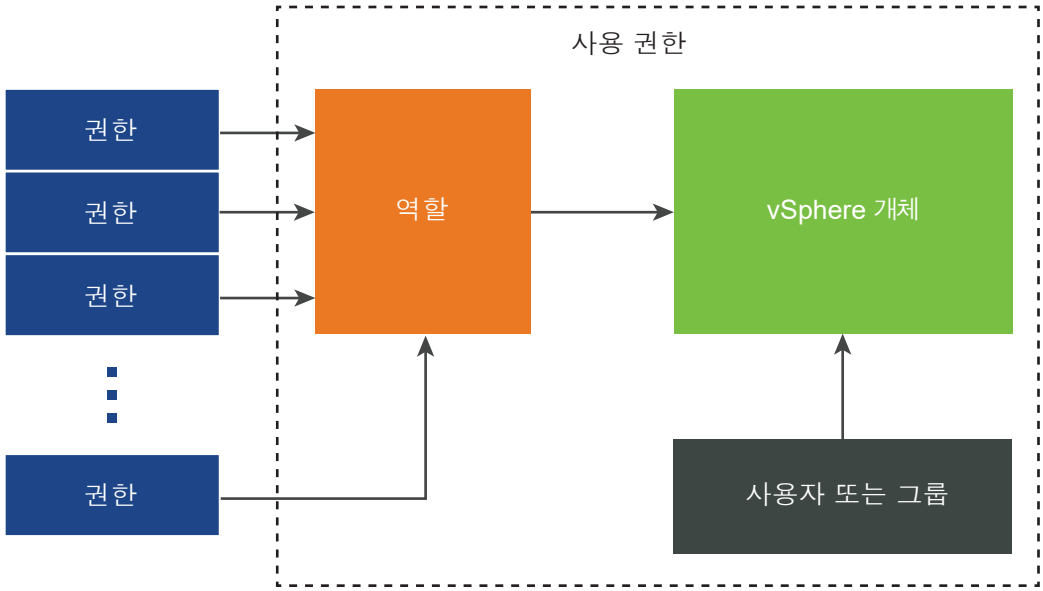
권한은 세분화된 액세스 제어입니다. 이러한 권한을 역할로 그룹화한 다음 사용자 또는 그룹에 매핑할 수 있습니다.

역할

역할은 권한의 집합입니다. 역할을 사용하여 사용자가 수행하는 일련의 일반 작업을 기반으로 개체에 대한 사용 권한을 할당할 수 있습니다. 관리자와 같은 시스템 역할은 vCenter Server에 미리 정의되어 있으며 변경할 수 없습니다. vCenter Server는 수정할 수 있는 몇 가지 기본 샘플 역할(예: 리소스 풀 관리자)도 제공합니다. 사용자 지정 역할은 처음부터 생성하거나 샘플 역할을 복제 및 수정하여 생성할 수 있습니다. vCenter Server 사용자 지정 역할 생성의 내용을 참조하십시오.

다음 그림은 권한 및 역할에서 사용 권한이 구성되고 vSphere 개체의 사용자 또는 그룹에 사용 권한이 할당되는 방식을 설명합니다.

그림 2-3. vSphere 사용 권한



개체에 권한을 할당하려면 다음 단계를 따르십시오.

1 vCenter Server 개체 계층에서 사용 권한을 적용할 개체를 선택합니다.

2 개체에 대한 권한을 가져야 하는 그룹 또는 사용자를 선택합니다.

3 개체에 대해 그룹 또는 사용자가 가져야 하는 개별 권한 또는 역할(일련의 권한)을 선택합니다.

   기본적으로 [하위 항목으로 전파]는 선택되지 않습니다. 해당 확인란을 선택해야 그룹 또는 사용자가 선택된 개체와 그 하위 개체에 대해 선택된 역할을 가집니다.

vCenter Server는 자주 사용되는 권한 집합이 결합된 샘플 역할을 제공합니다. 역할 집합을 결합하여 사용자 지정 역할을 생성할 수도 있습니다.

많은 경우 소스 개체 및 대상 개체 모두에 대해 사용 권한을 정의해야 합니다. 예를 들어, 가상 시스템을 이동하는 경우 가상 시스템에 대한 권한이 필요하며 대상 데이터 센터에 대한 권한도 필요합니다.

다음 정보를 참조하십시오.

참조 내용	참조 위치
사용자 지정 역할 생성	vCenter Server 사용자 지정 역할 생성
모든 권한 그리고 권한을 적용할 수 있는 개체	장 16 정의된 권한
다양한 작업을 위해 다양한 개체에 필요한 권한 집합	일반 작업에 필요한 권한

독립형 ESXi 호스트에 대한 권한 모델은 더 간단합니다. ESXi 호스트에 대한 권한 할당의 내용을 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 Smith라는 사용자에게 여러 개체에 대한 역할이 할당되어 있는 경우 도메인 관리자가 이름을 Smith2로 바꾼다면 다음번 검증 시 호스트에서 Smith가 더 이상 없다고 결론짓고 이 사용자에 연결된 사용 권한을 vSphere 개체에서 제거합니다.

마찬가지로, 도메인에서 사용자 Smith가 제거되면 다음 유효성 검사가 수행될 때 해당 사용자와 연관된 모든 권한이 제거됩니다. 다음에 검증이 수행되기 전에 새 사용자 Smith가 도메인에 추가되면 새 사용자 Smith가 개체에 대한 사용 권한에 있어 이전 사용자 Smith를 대체합니다.

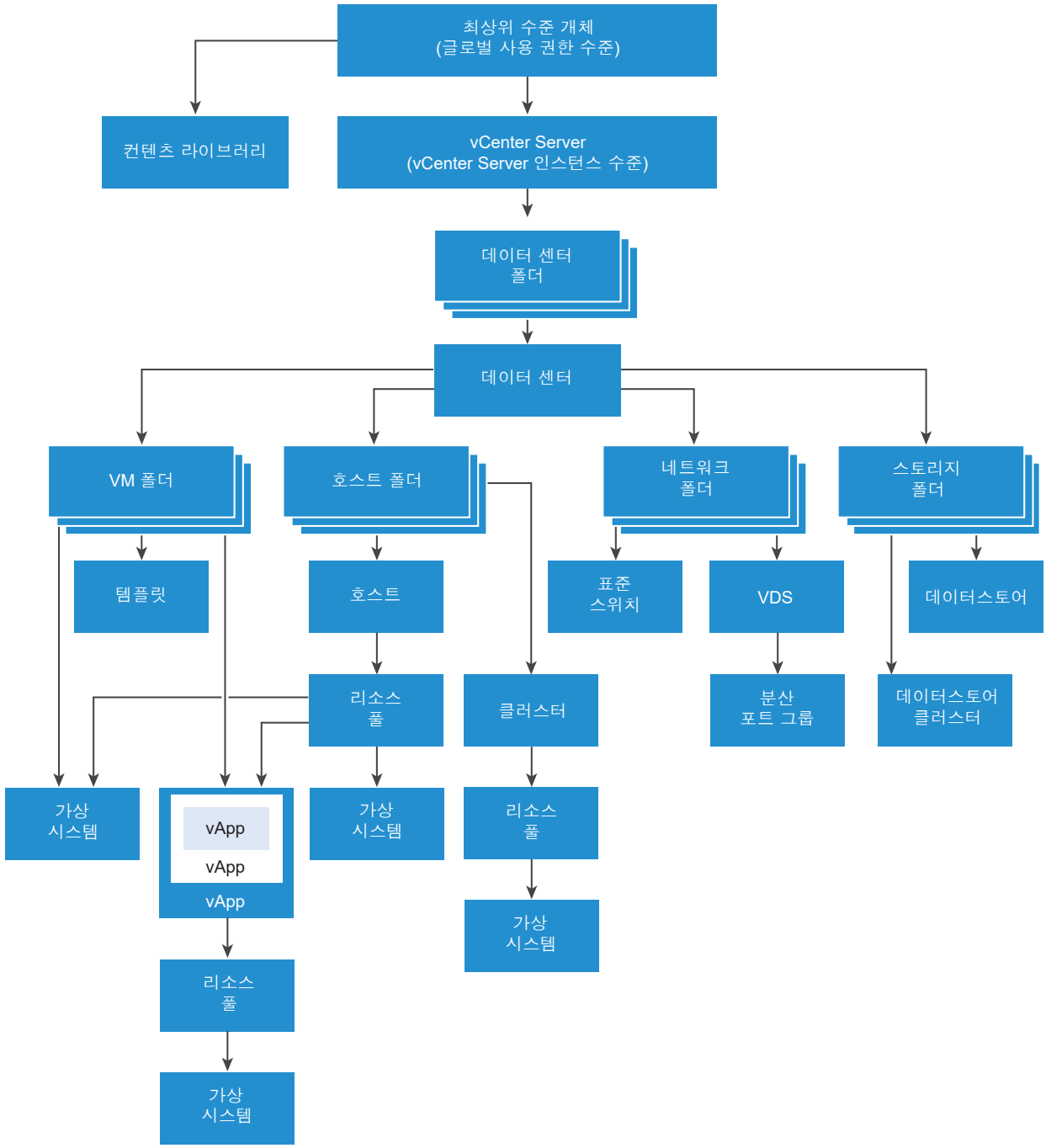
사용 권한의 계층적 상속

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.

다음 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 권한의 내용을 참조하십시오.

그림 2-4. vSphere 인벤토리 계층 구조



이 그림에 대한 설명:

- VM, 호스트, 네트워크 및 스토리지 폴더에 대한 직접 사용 권한을 설정할 수 없습니다. 즉, 이러한 폴더는 컨테이너로 작동하므로 사용자에게 표시되지 않습니다.

- 표준 스위치에 대한 사용 권한을 설정할 수 없습니다.

참고 사용 권한을 설정하고 VDS(vSphere Distributed Switch)의 하위 항목으로 전파하려면 스위치 개체가 데이터 센터에서 생성된 네트워크 폴더에 상주해야 합니다.

대부분의 인벤토리 개체는 계층에 있는 단일 상위 개체로부터 사용 권한을 상속합니다. 예를 들어 데이터스토어는 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 엔티티

관리 엔티티는 다음 vSphere 개체를 참조합니다. 관리 엔티티는 엔티티 유형에 따라 다른 특정 작업을 제공합니다. 권한 있는 사용자는 관리 엔티티에 대한 사용 권한을 정의할 수 있습니다. vSphere 개체, 속성 및 메서드에 대한 자세한 내용은 vSphere API 설명서를 참조하십시오.

- 클러스터
- 데이터 센터
- 데이터스토어
- 데이터스토어 클러스터
- 폴더
- 호스트
- 네트워크(vSphere Distributed Switch 제외)
- 분산 포트 그룹
- 리소스 풀
- 템플릿
- 가상 시스템
- vSphere vApp

글로벌 엔티티

루트 vCenter Server 시스템에서 사용 권한이 파생되는 엔티티에 대한 사용 권한을 수정할 수 없습니다.

- 사용자 지정 필드
- 라이센스

- 역할
- 통계 간격
- 세션

여러 가지 사용 권한 설정

개체에는 여러 권한이 있을 수 있지만 각 사용자나 그룹에는 권한이 하나만 있을 수 있습니다. 예를 들어, 한 사용 권한에서 GroupAdmin이 한 개체에 대해 관리자 역할을 갖도록 지정할 수 있고 다른 사용 권한에서 GroupVMAdmin이 동일한 개체에 대해 가상 시스템 관리자 역할을 갖도록 지정할 수 있습니다. 그러나 GroupVMAdmin 그룹은 이 개체의 동일한 GroupVMAdmin에 대해 다른 사용 권한을 가질 수 없습니다.

상위의 전파 속성이 true로 설정된 경우 하위 개체는 해당 상위의 사용 권한을 상속합니다. 하위 개체에 직접 설정된 사용 권한은 상위 개체의 사용 권한을 재정의합니다. 예 2: 상위 사용 권한을 재정의하는 하위 사용 권한의 내용을 참조하십시오.

여러 그룹 역할이 동일한 개체에 대해 정의되고 사용자가 이들 그룹 중 둘 이상에 속하게 되면 다음과 같은 두 가지 상황이 가능합니다.

- 해당 개체에 대한 사용자의 권한이 직접적으로 정의되지 않은 경우 사용자는 그룹이 개체에 대해 갖는 사용 권한의 결합체를 갖습니다.
- 해당 개체에 대한 사용자의 권한이 직접적으로 정의된 경우에는 사용자의 사용 권한이 모든 그룹 사용 권한보다 우선합니다.

예1: 여러 그룹의 사용 권한 상속

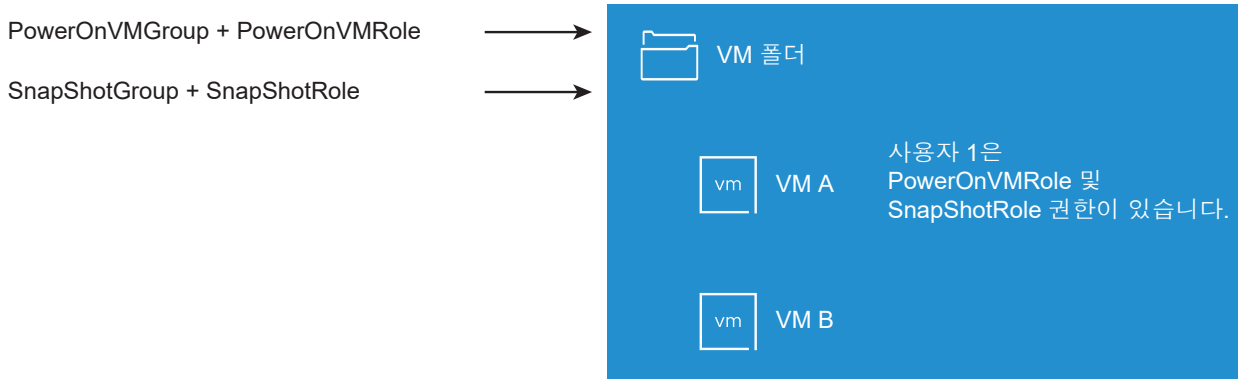
이 예제에서는 상위 개체에 대한 사용 권한이 부여된 그룹에서 한 개체가 여러 사용 권한을 상속할 수 있는 방법을 보여 줍니다.

이 예제에서는 동일한 개체의 두 그룹에 대해 두 개의 사용 권한이 할당됩니다.

- PowerOnVMRole은 가상 시스템의 전원을 켤 수 있습니다.
- SnapShotRole은 가상 시스템의 스냅샷을 생성할 수 있습니다.
- PowerOnVMGroup에는 VM 폴더에 대한 PowerOnVMRole이 부여되고, 사용 권한은 하위 개체로 전파되도록 설정됩니다.
- SnapShotGroup에는 VM 폴더에 대한 SnapShotRole이 부여되고, 사용 권한은 하위 개체에 전파되도록 설정됩니다.
- 사용자 1에는 특정 권한이 할당되지 않았습니다.

PowerOnVMGroup 및 SnapShotGroup에 모두 속한 사용자 1이 로그인합니다. 사용자 1은 VM A와 VM B의 전원을 모두 켜고 스냅샷을 생성할 수 있습니다.

그림 2-5. 예1: 여러 그룹의 사용 권한 상속



예 2: 상위 사용 권한을 재정의하는 하위 사용 권한

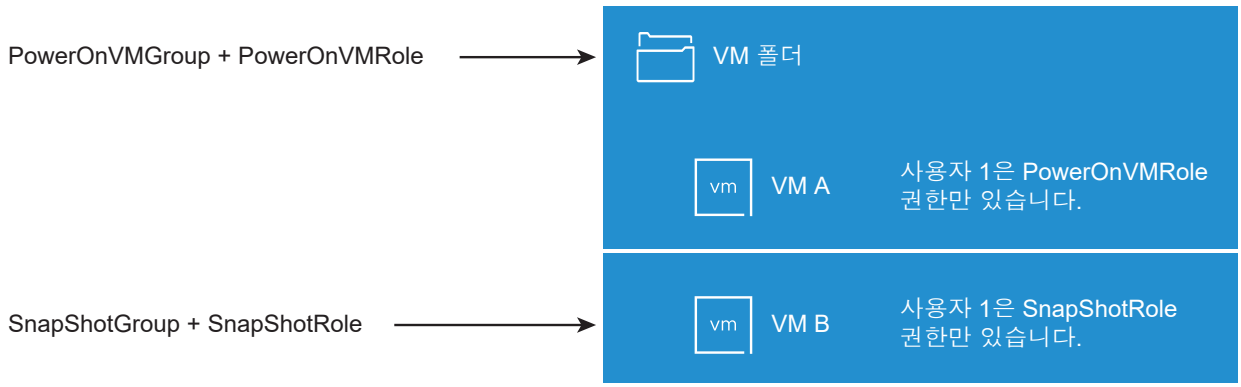
이 예제에서는 하위 개체에 할당된 사용 권한이 상위 개체에 할당된 사용 권한을 재정의할 수 있는 방법을 보여 줍니다. 이 재정의 동작을 사용하여 사용자 액세스를 특정 인벤토리 영역으로 제한할 수 있습니다.

이 예에서는 사용 권한이 서로 다른 두 그룹의 다른 두 개체에서 정의됩니다.

- PowerOnVMRole은 가상 시스템의 전원을 켤 수 있습니다.
- SnapShotRole은 가상 시스템의 스냅샷을 생성할 수 있습니다.
- PowerOnVMGroup에는 VM 폴더에 대한 PowerOnVMRole이 부여되고, 사용 권한은 하위 개체로 전파되도록 설정됩니다.
- SnapShotGroup에는 VM B에 대한 SnapShotRole이 부여됩니다.

PowerOnVMGroup 및 SnapShotGroup에 모두 속한 사용자 1이 로그인합니다. SnapShotRole은 계층에서 PowerOnVMRole보다 낮은 지점에 할당되어 있으므로 VM B에 대한 PowerOnVMRole을 재정의합니다. 사용자 1은 VM A의 전원을 켤 수 있지만 VM A의 스냅샷을 생성할 수는 없습니다. 사용자 1은 VM B의 스냅샷을 생성할 수 있지만 VM B의 전원을 켤 수는 없습니다.

그림 2-6. 예 2: 상위 사용 권한을 재정의하는 하위 사용 권한



예 3: 그룹 역할을 재정의하는 사용자 역할

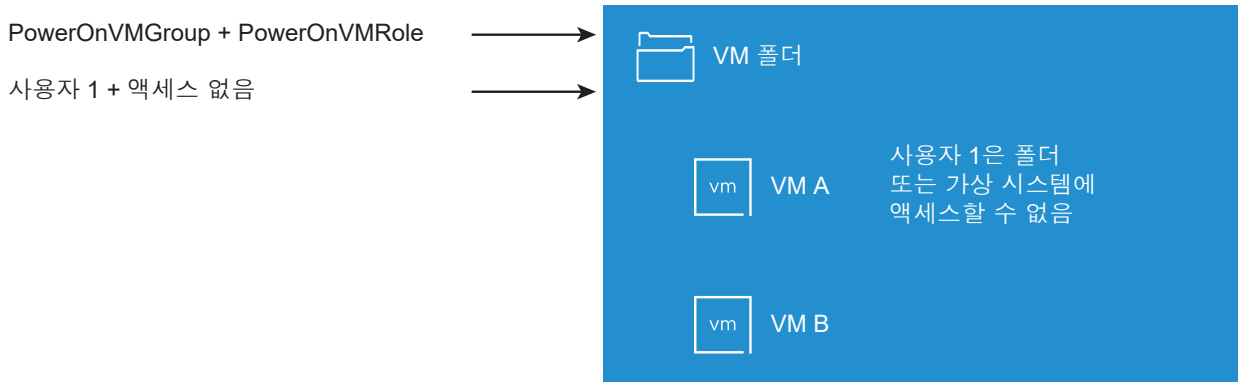
이 예제는 개별 사용자에게 직접 할당된 역할이 그룹에 할당된 역할과 연결된 권한을 재정의하는 방법을 보여줍니다.

이 예제에서 사용 권한은 동일한 개체에서 정의됩니다. 한 사용 권한은 그룹을 역할에 연결하고, 다른 사용 권한은 개별 사용자를 역할에 연결합니다. 사용자는 그룹의 멤버입니다.

- PowerOnVMRole은 가상 시스템의 전원을 켤 수 있습니다.
- PowerOnVMGroup에는 VM 폴더에 대한 PowerOnVMRole이 부여됩니다.
- 사용자 1에는 VM 폴더에 대한 NoAccess 역할이 부여됩니다.

PowerOnVMGroup에 속한 사용자 1이 로그인합니다. VM 폴더에 대해 사용자 1에게 부여된 NoAccess 역할이 그룹에 할당된 역할을 재정의합니다. 사용자 1은 VM 폴더 또는 VM A 및 B에 액세스할 수 없습니다. VM A 및 B는 계층에서 사용자 1에게 표시되지 않습니다.

그림 2-7. 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.

사용 권한에 대한 개념 정보는 개체 수준 사용 권한 모델 이해의 설명을 참조하십시오.

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 상속의 내용을 참조하십시오. 또한 글로벌 루트 개체에 전파 사용 권한을 할당하여 모든 솔루션에 있는 개체 전체에 사용 권한을 적용할 수도 있습니다. 글로벌 사용 권한의 내용을 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 전파 사용 권한을 동시에 여러 개체에 할당할 수 있습니다.

사용 권한을 할당할 때 사용자 및 그룹 이름이 대소문자를 포함하여 Active Directory와 정확하게 일치해야 합니다. 이전 버전의 vSphere에서 업그레이드한 경우 그룹과 관련한 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 Client 개체 탐색기에서 사용 권한을 할당하려는 개체를 찾습니다.
2. **사용 권한** 탭을 클릭합니다.
3. **추가**를 클릭합니다.
4. (선택 사항) 페더레이션된 인증을 위해 외부 ID 제공자를 구성한 경우, 해당 ID 제공자의 도메인을 **도메인** 드롭다운 메뉴에서 선택할 수 있습니다.
5. 선택된 역할에 따라 정의된 권한이 있는 사용자 또는 그룹을 선택합니다.
   a. **도메인** 드롭다운 메뉴에서 사용자 또는 그룹의 도메인을 선택합니다.
   b. 검색 상자에 이름을 입력합니다.

      시스템이 사용자 이름과 그룹 이름을 검색합니다.
   c. 사용자 또는 그룹을 선택합니다.
6. **역할** 드롭다운 메뉴에서 역할을 선택합니다.
7. (선택 사항) 사용 권한을 전파하려면 **하위 항목으로 전파** 확인란을 선택합니다.

   역할이 선택한 개체에 적용되고 하위 개체에 전파됩니다.
8. **확인**을 클릭합니다.

사용 권한 변경 또는 제거

인벤토리 개체에 대해 사용자나 그룹 및 역할 쌍을 설정한 후, 사용자나 그룹에 지정된 역할을 변경하거나 **하위 항목으로 전파** 확인란의 설정을 변경할 수 있습니다. 사용 권한 설정을 제거할 수도 있습니다.

절차

1. vSphere Client 개체 탐색기에서 개체를 찾습니다.
2. **사용 권한** 탭을 클릭합니다.

3 행을 클릭하여 사용 권한을 선택합니다.

작업	단계
사용 권한 변경	a **역할 변경** 아이콘을 클릭합니다. b **역할** 드롭다운 메뉴에서 사용자나 그룹의 역할을 선택합니다. c **하위 항목으로 전파** 확인란을 전환하여 사용 권한 상속을 변경합니다. d **확인**을 클릭합니다.
사용 권한 제거	**사용 권한 제거** 아이콘을 클릭합니다.

사용자 검증 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 목록을 동일한 방식으로 검색할 수 없습니다.

절차

1 vSphere Client 개체 탐색기에서 vCenter Server 시스템을 찾습니다.

2 **구성**을 선택하고 **설정 > 일반**을 클릭합니다.

3 **편집**을 클릭하고 **사용자 디렉토리**를 선택합니다.

4 필요에 따라 값을 변경하고 **저장**을 클릭합니다.

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 옵션을 켭니다.
쿼리 제한 크기	**사용자 또는 그룹 선택** 대화상자의 선택된 도메인에서 vCenter Server가 표시하는 최대 사용자 및 그룹 수입니다. 0을 입력하면 모든 사용자 및 그룹이 표시됩니다.

글로벌 사용 권한

글로벌 사용 권한은 여러 솔루션에 걸쳐 있는 글로벌 루트 개체에 적용됩니다. 온-프레미스 SDDC에서 글로벌 사용 권한은 vCenter Server 및 vRealize Orchestrator 모두에 걸쳐 있을 수 있습니다. 하지만 vSphere SDDC의 경우 글로벌 사용 권한은 태그 및 컨텐츠 라이브러리와 같은 글로벌 개체에 적용됩니다.

사용자 또는 그룹에 글로벌 사용 권한을 할당하고 각 사용자 또는 그룹의 역할을 결정할 수 있습니다. 이 역할은 사용자 또는 그룹이 계층의 모든 개체에 대해 가진 권한 집합을 결정합니다. 미리 정의된 역할을 할당하거나 사용자 지정 역할을 생성할 수 있습니다. 역할을 사용하여 권한 할당의 내용을 참조하십시오.

vCenter Server 사용 권한과 글로벌 사용 권한을 구분하는 것이 중요합니다.

vCenter Server 사용 권한

일반적으로 가상 시스템과 같은 vCenter Server 인벤토리 개체에 사용 권한을 적용합니다. 그럴 경우 사용자 또는 그룹이 해당 개체에 대해 특정 역할(일련의 권한)을 가지도록 지정합니다.

글로벌 사용 권한

글로벌 사용 권한은 배포의 각 인벤토리 계층에 있는 모든 개체를 보거나 관리할 수 있는 권한을 사용자 또는 그룹에 부여합니다. 글로벌 사용 권한은 태그 및 컨텐츠 라이브러리와 같은 글로벌 개체에도 적용됩니다. 태그 개체에 대한 사용 권한의 내용을 참조하십시오.

글로벌 사용 권한을 할당하고 [전파]를 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.

중요 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 vSphere Client를 사용하여 vCenter Server에 로그인합니다.

2 **관리**를 선택하고 액세스 제어 영역에서 **글로벌 사용 권한**을 클릭합니다.

3 **사용 권한 제공자** 드롭다운 메뉴에서 도메인을 선택합니다.

4 (선택 사항) 페더레이션된 인증을 위해 외부 ID 제공자를 구성한 경우, 해당 ID 제공자의 도메인을 **도메인** 드롭다운 메뉴에서 선택할 수 있습니다.

5 **추가**를 클릭합니다.

6 선택된 역할에 따라 정의된 권한이 있는 사용자 또는 그룹을 선택합니다.

   a **도메인** 드롭다운 메뉴에서 사용자 또는 그룹의 도메인을 선택합니다.

   b 검색 상자에 이름을 입력합니다.

      시스템이 사용자 이름과 그룹 이름을 검색합니다.

   c 사용자 또는 그룹을 선택합니다.

7 **역할** 드롭다운 메뉴에서 역할을 선택합니다.

8 **하위 항목으로 전파** 확인란을 선택하여 사용 권한을 전파할지 여부를 결정합니다.

   글로벌 사용 권한을 할당하고 **하위 항목으로 전파**를 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.

9 **확인**을 클릭합니다.

태그 개체에 대한 사용 권한

vCenter Server 개체 계층에서, 태그 개체는 vCenter Server의 하위 항목이 아니지만 vCenter Server 최상위 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

사용자에게 가상 시스템과 같은 vCenter Server 인벤토리 개체에 대한 사용 권한을 부여하는 경우 해당 사용자는 사용 권한과 연결된 작업을 수행할 수 있습니다. 하지만 사용자가 개체에 대한 태그 작업은 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 최상위 수준에서 **vSphere 태그 할당** 권한이 있어야 합니다. 즉, 글로벌 사용 권한이나 태그 개체에 대한 권한이 있어야 합니다.

표 2-1. 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 최상위 수준 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 최상위 수준에서 글로벌 사용 권한을 사용하여 사용자 Robin에게 할당한다고 가정합니다. 태그 운영을 위해 **vSphere 태그 삭제** 권한은 Robin에게 할당하지 않습니다. 이 경우 Robin은 최상위 수준에서 전파되는 글로벌 사용 권한이 있으므로 태그 운영에 대한 권한을 가집니다. 글로벌 사용 권한을 수정하는 경우가 아니면 권한을 제한할 수 없습니다.

표 2-2. 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.

참고 이 동작은 vCenter Server 권한이 상속되는 방식과 다릅니다. vCenter Server에서, 하위 개체에 대해 정의된 사용 권한이 항상 상위 개체에서 전파된 사용 권한을 재정의합니다.

표 2-3. 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 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 Sales 그룹에게 풀 A에는 가상 시스템 사용자 역할을 할당하고 풀 B에는 읽기 전용 역할을 할당할 수 있습니다. 이렇게 할당된 경우 Sales 그룹의 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 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 Client의 역할 편집 기능을 사용하여 사용자 지정 역할을 생성하면 사용자의 필요에 맞는 권한 집합을 생성할 수 있습니다.

ESXi 사용자 지정 역할

CLI 또는 VMware Host Client를 사용하여 개별 호스트에 대한 사용자 지정 역할을 생성할 수 있습니다. "vSphere 단일 호스트 관리 - VMware Host Client" 설명서를 참조하십시오. vCenter Server에서는 사용자 지정 호스트 역할에 액세스할 수 없습니다.

vCenter Server를 통해 ESXi 호스트를 관리하는 경우 호스트와 vCenter Server 모두에 사용자 지정 역할을 유지하지 마십시오. vCenter Server 수준에서 역할을 정의합니다.

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 추가하고 역할에 권한을 할당하지 않을 경우 해당 역할이 3가지 시스템 정의 권한(**시스템.익명**, **시스템.보기**, **시스템.읽기**)을 갖는 읽기 전용 역할로 생성됩니다. 이러한 권한은 vSphere Client에 표시되지 않지만 일부 관리 개체의 특정 속성을 읽는 데 사용됩니다. vCenter Server에 미리 정의된 모든 역할에는 이러한 3가지 시스템 정의 권한이 포함되어 있습니다. 자세한 내용은 "vSphere Web Services API" 설명서를 참조하십시오.

vCenter Server 사용자 지정 역할 생성

환경의 액세스 제어 요구에 맞게 vCenter Server 사용자 지정 역할을 생성할 수 있습니다. 역할을 생성하거나 기존 역할을 복제할 수 있습니다.

다른 vCenter Server 시스템과 동일한 vCenter Single Sign-On 도메인의 일부인 vCenter Server 시스템에서 역할을 생성 또는 편집할 수 있습니다. 이 경우 VMware Directory Service(vmdir)는 역할 변경 사항을 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 Client를 사용하여 vCenter Server에 로그인합니다.

2 **관리**를 선택하고 **액세스 제어** 영역에서 **역할**을 클릭합니다.

3 역할을 생성합니다.

옵션	설명
역할을 생성하려면	**새로 만들기**를 클릭합니다.
복제하여 역할을 생성하려면	역할을 선택하고 **복제**를 클릭합니다.

자세한 내용은 vCenter Server 시스템 역할의 내용을 참조하십시오.

4 새 역할의 이름을 입력합니다.

5 역할에 대한 권한을 선택하거나 선택 취소합니다.

권한 범주를 스크롤하고 해당 범주에 대한 모든 권한 또는 권한의 하위 집합을 선택합니다. 모든 범주, 선택된 범주 또는 선택되지 않은 범주를 표시할 수 있습니다. 모든 권한, 선택된 권한 또는 선택되지 않은 권한을 표시할 수도 있습니다.

자세한 내용은 장 16 정의된 권한의 내용을 참조하십시오.

참고 복제된 역할을 생성할 때는 권한을 변경할 수 없습니다. 권한을 변경하려면 복제된 역할을 선택하고 **편집**을 클릭합니다.

6 **추가**를 클릭합니다.

다음에 수행할 작업

이제 개체를 선택하고 해당 개체의 사용자 또는 그룹에 역할을 할당하여 사용 권한을 생성할 수 있습니다.

vCenter Server 시스템 역할

역할이란 미리 정의된 권한의 집합입니다. 개체에 사용 권한을 추가할 때 사용자 또는 그룹과 역할을 쌍으로 구성합니다. vCenter Server에는 변경할 수 없는 몇 가지 기본적인 시스템 역할이 포함되어 있습니다.

vCenter Server는 몇 가지 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.

기본 역할과 연결된 권한을 보려면 vSphere Client에서 해당 역할로 이동한 후(**메뉴 > 관리 > 역할**) **권한** 탭을 클릭합니다.

모든 vSphere 권한 및 설명을 보려면 장 16 정의된 권한 항목을 참조하십시오.

vCenter Server 역할 계층에는 다수의 샘플 역할도 포함되어 있습니다. 샘플 역할을 복제하여 유사한 역할을 생성할 수 있습니다.

역할을 생성하는 경우 시스템 역할의 권한을 상속하지 않습니다.

관리자 역할

개체에 대한 관리자 역할을 가진 사용자는 해당 개체에 대한 모든 작업을 보고 수행할 수 있습니다. 이 역할에는 읽기 전용 역할의 모든 권한도 포함됩니다. 개체에 대한 관리자 역할이 있는 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 서비스는 "vSphere 인증" 설명서를 참조하십시오.

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.

읽기 전용 역할

개체에 대해 읽기 전용 역할을 가진 사용자는 개체의 상태 및 개체에 대한 세부 정보를 볼 수 있습니다. 예를 들어 이 역할을 가진 사용자는 가상 시스템, 호스트 및 리소스 풀 특성을 볼 수 있지만 호스트의 원격 콘솔을 볼 수 없습니다. 메뉴 및 도구 모음을 통한 모든 작업은 허용되지 않습니다.

권한 없음 역할

개체에 대해 권한 없음 역할을 가진 사용자는 어떠한 방법으로든 개체를 보거나 변경할 수 없습니다. 기본적으로 새 사용자 및 그룹은 이 역할이 할당됩니다. 개체별로 역할을 변경할 수 있습니다.

vCenter Single Sign-On 도메인(기본적으로 administrator@vsphere.local)의 관리자, 루트 사용자 및 vpxuser에게는 기본적으로 관리자 역할이 할당됩니다. 다른 사용자에게는 기본적으로 권한 없음 역할이 할당됩니다.

가장 좋은 방법은 루트 수준에서 사용자를 생성하고 해당 사용자에게 관리자 역할을 할당하는 것입니다. 관리자 권한을 가진 명명된 사용자를 생성한 후 모든 사용 권한에서 루트 사용자를 제거하거나 해당 역할을 권한 없음으로 변경할 수 있습니다.

역할 및 권한에 대한 모범 사례

역할 및 사용 권한에 대한 모범 사례를 적용하여 vCenter Server 환경의 보안 및 관리 용이성을 극대화할 수 있습니다.

vCenter Server 환경에서 역할 및 사용 권한을 구성할 때 다음의 모범 사례를 따르십시오.

- 가능하면 개별 사용자보다는 그룹에 역할을 할당합니다.
- 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.
- 개체에 사용 권한을 할당할 때에는 전파 기능을 사용하는 것이 좋습니다. 전파 기능을 사용하면 개체 계층의 새 개체에 사용 권한을 상속할 수 있습니다. 예를 들어 가상 시스템 폴더에 사용 권한을 할당한 후 전파 기능을 사용하도록 설정하여 해당 폴더 내의 모든 VM에 이 사용 권한을 적용할 수 있습니다.
- 계층의 특정 영역을 마스킹하려면 권한 없음 역할을 사용합니다. 권한 없음 역할은 해당 역할이 있는 사용자 또는 그룹에 대한 액세스를 제한합니다.
- 라이센스 변경 사항은 같은 vCenter Single Sign-On 도메인 내의 연결된 모든 vCenter Server 시스템에 전파됩니다.

- 라이센스 전파는 사용자에게 모든 vCenter Server 시스템에 대한 권한이 없는 경우에도 이루어집니다.

일반 작업에 필요한 권한

대다수 작업을 수행하려면 인벤토리에 있는 여러 개체에 대해 권한이 필요합니다. 작업을 수행하려는 사용자에게 하나의 개체에 대한 권한만 있는 경우 작업을 성공적으로 완료할 수 없습니다.

다음 표에는 둘 이상의 권한이 필요한 일반 작업이 나와 있습니다. 한 명의 사용자와 미리 정의된 역할 중 하나 또는 여러 권한을 쌍으로 연결하여 인벤토리 개체에 사용 권한을 추가하거나 권한 집합을 여러 번 할당할 것으로 예상되는 경우 사용자 지정 역할을 생성합니다.

vSphere Client 사용자 인터페이스의 작업이 API 호출에 매핑되는 방법과 작업을 수행하는 데 필요한 권한에 대해 알아보려면 "vSphere Web Services API 참조" 설명서를 참조하십시오. 예를 들어 `AddHost_Task(addHost)` 메서드에 대한 API 설명서에서는 클러스터에 호스트를 추가하려면 **Host.Inventory.AddHostToCluster** 권한이 필요함을 지정합니다.

수행하려는 작업이 이 표에 없는 경우 다음 규칙을 사용하면 특정 작업을 허용하기 위해 사용 권한을 할당해야 하는 경우를 확인할 수 있습니다.

- 스토리지 공간을 사용하는 모든 작업에는 대상 데이터스토어에 대한 **데이터스토어.공간 할당** 권한과 작업 자체를 수행할 수 있는 권한이 필요합니다. 예를 들어 가상 디스크를 생성하거나 스냅샷을 생성하는 경우 이러한 권한이 있어야 합니다.
- 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 2-4. 일반 작업에 필요한 권한

작업	필요한 권한	적용 가능한 역할
가상 시스템 생성	대상 폴더 또는 데이터 센터에서 다음을 수행: ■ **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 구성**(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

표 2-4. 일반 작업에 필요한 권한 (계속)

작업	필요한 권한	적용 가능한 역할
가상 시스템 전원 켜기	가상 시스템이 배포되는 데이터 센터에서 다음을 수행: **가상 시스템.상호 작용.전원 켜기**	가상 시스템 고급 사용자 또는 관리자
	가상 시스템 또는 가상 시스템의 폴더에서 다음을 수행: **가상 시스템.상호 작용.전원 켜기**	
템플릿에서 가상 시스템 배포	대상 폴더 또는 데이터 센터에서 다음을 수행: ■ **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** ■ **vApp.가져오기**	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: ■ **리소스.리소스 풀에 가상 시스템 할당** ■ **가상 시스템.인벤토리.이동**	관리자
	대상 리소스 풀에서 다음을 수행: **리소스.리소스 풀에 가상 시스템 할당**	관리자
가상 시스템에 게스트 운영 체제 설치	가상 시스템 또는 가상 시스템의 폴더에서 다음을 수행: ■ **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**	가상 시스템 고급 사용자 또는 관리자

표 2-4. 일반 작업에 필요한 권한 (계속)

작업	필요한 권한	적용 가능한 역할
	설치 미디어 ISO 이미지가 들어 있는 데이터스토어에서 다음을 수행: **데이터스토어.데이터스토어 찾아보기**(데이터스토어의 ISO 이미지에서 설치하는 경우) 설치 미디어 ISO 이미지를 업로드하는 데이터스토어에서 다음을 수행: ■ **데이터스토어.데이터스토어 찾아보기** ■ **데이터스토어.하위 수준 파일 작업**	가상 시스템 고급 사용자 또는 관리자
vMotion으로 가상 시스템 마이그레이션	가상 시스템 또는 가상 시스템의 폴더에서 다음을 수행: ■ **리소스.전원이 켜진 가상 시스템 마이그레이션** ■ **리소스.리소스 풀에 가상 시스템 할당**(대상이 소스와 다른 리소스 풀인 경우)	리소스 풀 관리자 또는 관리자
	대상 호스트, 클러스터 또는 리소스 풀에서 다음을 수행(소스와 다른 경우): **리소스.리소스 풀에 가상 시스템 할당**	리소스 풀 관리자 또는 관리자
가상 시스템 콜드 마이그레이션(재배치)	가상 시스템 또는 가상 시스템의 폴더에서 다음을 수행: ■ **리소스.전원이 꺼진 가상 시스템 마이그레이션** ■ **리소스.리소스 풀에 가상 시스템 할당**(대상이 소스와 다른 리소스 풀인 경우)	리소스 풀 관리자 또는 관리자
	대상 호스트, 클러스터 또는 리소스 풀에서 다음을 수행(소스와 다른 경우): **리소스.리소스 풀에 가상 시스템 할당**	리소스 풀 관리자 또는 관리자
	대상 데이터스토어에서 다음을 수행(소스와 다른 경우): **데이터스토어.공간 할당**	데이터스토어 소비자 또는 관리자
Storage vMotion을 사용하여 가상 시스템 마이그레이션	가상 시스템 또는 가상 시스템의 폴더에서 다음을 수행: **리소스.전원이 켜진 가상 시스템 마이그레이션**	리소스 풀 관리자 또는 관리자
	대상 데이터스토어에서 다음을 수행: **데이터스토어.공간 할당**	데이터스토어 소비자 또는 관리자
호스트를 클러스터로 이동	호스트에서 다음을 수행: **호스트.인벤토리.클러스터에 호스트 추가**	관리자
	대상 클러스터에서 다음을 수행: ■ **호스트.인벤토리.클러스터에 호스트 추가** ■ **호스트.인벤토리.클러스터 수정**	관리자
vSphere Client를 사용하여 데이터 센터에 단일 호스트를 추가하거나 PowerCLI 또는 API(addHost API 활용)를 사용하여 클러스터에 단일 호스트 추가	호스트에서 다음을 수행: **호스트.인벤토리.클러스터에 호스트 추가**	관리자
	클러스터에서: ■ **호스트.인벤토리.클러스터 수정** ■ **호스트.인벤토리.클러스터에 호스트 추가**	관리자
	데이터 센터에서: **호스트.인벤토리.독립형 호스트 추가**	관리자
클러스터에 다중 호스트 추가	클러스터에서: ■ **호스트.인벤토리.클러스터 수정** ■ **호스트.인벤토리.클러스터에 호스트 추가**	관리자

표 2-4. 일반 작업에 필요한 권한 (계속)

작업	필요한 권한	적용 가능한 역할
	클러스터의 상위 데이터 센터에서(전파 포함): ■ **호스트.인벤토리.독립형 호스트 추가** ■ **호스트.인벤토리.호스트 이동** ■ **호스트.인벤토리.클러스터 수정** ■ **호스트.구성.유지 보수**	관리자
가상 시스템 암호화	암호화 작업은 vCenter Server가 포함된 환경에서만 가능합니다. 또한 ESXi 호스트에서 대부분의 암호화 작업에 대해 암호화 모드를 사용하도록 설정해야 합니다. 작업을 수행하는 사용자에게 적절한 권한이 있어야 합니다. **암호화 작업** 권한 집합을 통해 권한 부여를 세부적으로 제어할 수 있습니다. 암호화 작업의 사전 요구 사항 및 필요한 권한의 내용을 참조하십시오.	관리자

ESXi 호스트 보안

3

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. ESXi 호스트는 인증서 인프라에 참여합니다. 기본적으로 VMCA(VMware Certificate Authority)에서 서명된 인증서를 사용하여 호스트가 프로비저닝됩니다.

ESXi 보안에 대한 자세한 내용은 VMware 백서 "VMware vSphere Hypervisor 보안" 을 참조하십시오.

참고 ESXi는 Linux 커널 또는 상용 Linux 배포에 대해 빌드되지 않습니다. ESXi는 자체 포함 단위로 제공되는 고유한 VMware 전문의 독점적 커널 및 소프트웨어 도구를 사용합니다. Linux 배포의 애플리케이션 및 구성 요소는 여기에 포함되지 않습니다.

본 장은 다음 항목을 포함합니다.

- 일반 ESXi 보안 권장 사항
- ESXi 호스트에 대한 인증서 관리
- 보안 프로파일을 사용하여 호스트 사용자 지정
- ESXi 호스트에 대한 권한 할당
- Active Directory를 통해 ESXi 사용자 관리
- vSphere Authentication Proxy 사용
- ESXi에 대한 스마트 카드 인증 구성
- ESXi Shell 사용
- ESXi 호스트를 위한 UEFI 보안 부팅
- 신뢰할 수 있는 플랫폼 모듈을 통한 ESXi 호스트 보안
- ESXi 로그 파일
- ESXi 감사 레코드 관리
- ESXi 구성 보호

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. 그렇게 할 경우 신뢰할 수 있는 환경에서 작업 중인지 확인한 후 다른 보안 조치를 취합니다.

기본 제공 보안 기능

호스트에 대한 위험은 다음과 같이 완화됩니다.

- ESXi Shell 및 SSH 인터페이스는 기본적으로 사용하지 않도록 설정됩니다. 문제 해결 또는 지원 작업을 수행하지 않는 한 이러한 인터페이스를 사용하지 않도록 설정해 두어야 합니다. 일상적인 작업의 경우 vSphere Client를 사용합니다. 여기서 작업은 역할 기반 액세스 제어 및 최신 액세스 제어 방법을 따릅니다.
- 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 경우 포트를 엽니다.
- 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.
- 내부 웹 서비스는 웹 클라이언트의 액세스를 지원하기 위해 ESXi에 의해 사용됩니다. 이 서비스는 웹 클라이언트가 관리 및 모니터링을 위해 필요로 하는 기능만 실행하도록 수정되었습니다. 따라서 ESXi는 다양한 용도에 대해 보고되는 보안 문제에 취약하지 않습니다.
- VMware는 ESXi 보안에 영향을 미칠 수 있는 모든 보안 경고를 모니터링하고 필요한 경우 보안 패치를 실행합니다. VMware 보안 권고 및 보안 경고 메일 그룹을 구독하여 보안 경고를 수신할 수 있습니다. http://lists.vmware.com/mailman/listinfo/security-announce 웹 페이지를 참조하십시오.
- FTP 및 Telnet과 같은 안전하지 않은 서비스는 설치되지 않으며 이러한 서비스용 포트는 기본적으로 닫혀 있습니다.
- 암호화된 서명이 없는 드라이버 및 애플리케이션을 로드하지 않도록 호스트를 보호하려면 UEFI 보안 부팅을 사용하십시오. 보안 부팅은 시스템 BIOS에서 사용하도록 설정합니다. ESXi 호스트(예: 디스크 파티션)에는 추가적인 구성 변경이 필요하지 않습니다. ESXi 호스트를 위한 UEFI 보안 부팅의 내용을 참조하십시오.
- ESXi 호스트에 TPM 2.0 칩이 있는 경우, 시스템 BIOS에서 칩을 사용하도록 설정하고 구성하십시오. TPM 2.0은 보안 부팅과 함께 작동하여 하드웨어의 보안 및 신뢰 보증을 강화합니다. 신뢰할 수 있는 플랫폼 모듈을 통한 ESXi 호스트 보안의 내용을 참조하십시오.

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 엄격한 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 Client를 사용하여 vCenter Server로 관리되는 ESXi 호스트를 관리합니다. VMware Host Client를 통해 직접 관리 호스트에 액세스하지 말고 DCUI에서 관리 호스트를 변경하지 마십시오.

스크립팅 인터페이스 또는 API를 사용하여 호스트를 관리하는 경우 호스트를 직접 대상으로 하지 마십시오. 대신 호스트를 관리하는 vCenter Server 시스템을 대상으로 하고 호스트 이름을 지정하십시오.

문제 해결을 위해서만 DCUI 사용

문제 해결을 위해서만 DCUI 또는 ESXi Shell에서 루트 사용자로 호스트에 액세스하십시오. ESXi 호스트를 관리하려면 GUI 클라이언트 중 하나 또는 VMware CLI나 API 중 하나를 사용합니다. https://code.vmware.com/에서 "ESXCLI 개념 및 예제" 를 참조하십시오. ESXi Shell 또는 SSH를 사용하는 경우 액세스 권한이 있는 계정을 제한하고 시간 초과를 설정합니다.

ESXi 구성 요소를 업그레이드할 때는 VMware 소스만 사용합니다.

호스트는 관리 인터페이스 또는 수행해야 하는 작업을 지원하기 위해 다양한 타사 패키지를 실행합니다. VMware는 VMware 소스에서 전송되는 이러한 패키지로의 업그레이드만 지원합니다. 다른 소스의 다운로드나 패치를 사용하면 관리 인터페이스 보안 또는 기능이 제대로 작동하지 않을 수 있습니다. 타사 벤더 사이트 및 VMware 기술 자료에서 보안 경고를 확인합니다.

참고 VMware 보안 권고(http://www.vmware.com/security/)를 따르십시오.

고급 시스템 설정

고급 시스템 설정은 로깅, 시스템 리소스, 보안과 같은 ESXi 동작의 측면을 제어합니다.

다음 표에는 보안을 위한 몇 가지 중요한 ESXi 고급 시스템 설정이 제공됩니다. 모든 고급 시스템 설정을 보려면 vSphere Client(**호스트 > 구성 > 시스템 > 고급 시스템 설정**) 또는 해당 릴리스의 API를 참조하십시오.

표 3-1. 보안 고급 시스템 설정의 일부 목록

고급 시스템 설정	설명	기본값
Annotations.WelcomeMessage	로그인하기 전에 Host Client에 또는 기본 화면의 DCUI에 시작 메시지를 표시합니다. DCUI에서 시작 메시지는 호스트 IP 주소와 같은 일부 텍스트를 대체합니다.	(비어 있음)
Config.Etc.issue	SSH 로그인 세션 중에 배너를 표시합니다. 최상의 결과를 얻으려면 후행 줄 바꿈을 사용합니다.	(비어 있음)
Config.Etc.motd	SSH 로그인 시 오늘의 메시지를 표시합니다.	(비어 있음)
Config.HostAgent.vmacore.soap.sessionTimeout	시스템이 VIM API에서 자동으로 로그아웃될 때까지의 유휴 시간(분)을 설정합니다. 값이 0이면 유휴 시간을 사용하지 않도록 설정됩니다. 이 설정은 새 세션에만 적용됩니다.	30(분)
Mem.MemEagerZero	가상 시스템이 종료된 후 VMkernel 운영 체제(VMM 프로세스 포함)에서 사용자 월드 및 게스트 메모리 페이지 비우기를 활성화합니다. 기본값(0)은 느리게 비우기를 사용합니다. 값이 1이면 빠르게 비우기가 사용됩니다.	0(비활성화됨)
Security.AccountLockFailures	시스템에서 사용자 계정이 잠길 때까지 허용되는 최대 로그인 시도 실패 횟수를 설정합니다. 예를 들어 다섯 번째 로그인 실패 시 계정을 잠그려면 이 값을 4로 설정합니다. 값이 0이면 계정 잠금이 비활성화됩니다. 구현상의 이유로 일부 로그인 메커니즘이 예기치 않게 계산됩니다. ■ VIM 로그인(VMware Host Client 포함) 및 ESXCLI는 실패한 로그인의 정확한 수를 반영합니다. ■ SSH 연결은 암호 프롬프트가 표시될 때 로그인 시도로 계산되고 로그인에 성공하면 해당 계산이 실행 취소됩니다. 이 동작은 시도 및 응답 통신에서 정상입니다. ■ CGI 로그인은 로그인 실패 횟수를 이중으로 계산합니다. **경고** 이 문제로 인해 CGI 인터페이스를 사용하는 경우 로그인 실패 횟수보다 빠르게 사용자가 잠길 수 있습니다.	5

표 3-1. 보안 고급 시스템 설정의 일부 목록 (계속)

고급 시스템 설정	설명	기본값
Security.AccountUnlockTime	사용자가 잠기게 되는 시간(초)을 설정합니다. 지정된 잠금 제한 시간 내에 로그인을 시도하면 잠금 제한 시간이 다시 시작됩니다.	900(15분)
Security.PasswordHistory	각 사용자에 대해 기억할 암호 수를 설정합니다. 이 설정은 중복되거나 유사한 암호를 방지합니다.	0
Security.PasswordMaxDays	암호 변경 간격의 최대 일수를 설정합니다.	99999

Security.PasswordQualityControl	필요한 길이와 문자 클래스 요구 사항을 변경하거나 `Pam_passwdqc` 구성에서 암호 문구를 허용합니다. 암호에 특수 문자를 사용할 수 있습니다. 암호 길이는 15자 이상일 수 있습니다. 기본 설정에는 세 가지 문자 클래스와 최소 길이로 7자가 필요합니다.
	DoD Annex를 구현하는 경우 `similar=deny` 옵션과 최소 암호 길이를 결합하여 암호가 충분히 달라야 한다는 요구 사항을 적용할 수 있습니다. 암호 기록 설정은 VIM `LocalAccountManager.changePassword` API를 통해 변경된 암호에만 적용됩니다. 암호를 변경하려면 사용자에게 관리자 권한이 있어야 합니다.
	PasswordQualityControl 설정은 PasswordMaxDays 설정과 함께 DoD Annex의 요구 사항을 충족합니다.
	`min=disabled,disabled,disabled,disabled,15`
	`similar=deny`
		retry=3
		min=disabled,disabled,disabled,7,7

UserVars.DcuiTimeOut	시스템이 DCUI에서 자동으로 로그아웃될 때까지의 유휴 시간(초)을 설정합니다. 값이 0이면 시간 초과가 비활성화됩니다.	600(10분)
UserVars.ESXiShellInteractiveTimeOut	시스템이 대화형 셸에서 자동으로 로그아웃될 때까지의 유휴 시간(초)을 설정합니다. 이 설정은 새 세션에만 적용됩니다. 값이 0이면 유휴 시간을 사용하지 않도록 설정됩니다. DCUI 및 SSH 셸 모두에 적용됩니다.	0
UserVars.ESXiShellTimeOut	로그인 셸이 로그인을 기다리는 시간(초)을 설정합니다. 값이 0이면 시간 초과가 비활성화됩니다. DCUI 및 SSH 셸 모두에 적용됩니다.	0

표 3-1. 보안 고급 시스템 설정의 일부 목록 (계속)

고급 시스템 설정	설명	기본값
UserVars.HostClientSessionTimeout	시스템이 Host Client에서 자동으로 로그아웃될 때까지의 유휴 시간(초)을 설정합니다. 값이 0이면 유휴 시간을 사용하지 않도록 설정됩니다.	900(15분)
UserVars.HostClientWelcomeMessage	로그인 시 Host Client에 시작 메시지를 표시합니다. 메시지는 로그인 후 "힌트"로 표시됩니다.	(비어 있음)

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 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.

스크립트를 사용하여 호스트 구성 설정 관리

다수의 호스트가 포함된 환경에서는 스크립트를 사용한 호스트 관리가 vSphere Client에서 호스트를 관리하는 것보다 빠르고 오류 발생률이 낮습니다.

vSphere에는 호스트 관리를 위한 여러 스크립팅 언어가 포함되어 있습니다. 참조 정보 및 프로그래밍 팁은 "ESXCLI 설명서" 및 "vSphere API/SDK 설명서"를 참조하고 스크립트로 작성된 관리에 대한 추가 팁은 VMware 커뮤니티를 참조하십시오. vSphere 관리자 설명서는 관리를 위한 vSphere Client 사용을 중점적으로 다룹니다.

VMware PowerCLI

VMware PowerCLI는 vSphere API에 대한 Windows PowerShell 인터페이스입니다. VMware PowerCLI에는 vSphere 구성 요소 관리를 위한 PowerShell cmdlet이 포함되어 있습니다.

VMware PowerCLI에는 수백 개의 cmdlet, 샘플 스크립트 집합, 관리 및 자동화를 위한 기능 라이브러리가 포함되어 있습니다. https://developer.vmware.com/powercli의 내용을 참조하십시오.

ESXCLI

ESXCLI에는 ESXi 호스트 및 가상 시스템 관리를 위한 명령 집합이 포함되어 있습니다. "ESXCLI 설명서" 를 참조하십시오.

vSphere Automation SDK for Python과 같은 vSphere Automation 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 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

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

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

4 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.

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. `Security.PasswordHistory` 고급 옵션을 사용하여 각 사용자에 대해 기억할 암호 수도 설정할 수 있습니다.

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 VMware Host Client로부터의 액세스에 대해 암호 요구 사항을 적용합니다.

- 기본적으로 암호를 생성할 때는 소문자, 대문자, 숫자, 특수 문자(예: 밑줄 또는 대시)의 네 가지 문자 클래스 중 세 가지 이상을 혼합하여 포함해야 합니다.
- 기본적으로 암호 길이는 7자 이상 40자 미만입니다.
- 암호에는 사전에 나오는 단어 또는 사전에 나오는 단어의 일부를 포함하면 안 됩니다.

참고 암호를 시작할 때의 대문자는 사용된 문자 클래스 수에 포함되지 않습니다. 암호가 끝날 때의 숫자도 사용된 문자 클래스 수에 포함되지 않습니다. 암호 내에 사전 단어가 사용되면 전반적인 암호 강도가 감소됩니다.

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 설정을 사용하면 암호가 충분히 강력하지 않거나 암호가 올바르게 두 번 입력되지 않은 경우 새 암호를 입력하라는 메시지가 사용자에게 최대 세 번(retry=3) 표시됩니다. 처음 3개 항목이 사용되지 않도록 설정되기 때문에 1개 또는 2개의 문자 클래스 및 암호 문구가 있는 암호는 허용되지 않습니다. 3개 및 4개의 문자 클래스의 암호에는 7개의 문자가 필요합니다. 다른 옵션(예: `max`, `passphrase` 등)에 대한 자세한 내용은 `pam_passwdqc` man 페이지를 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 있습니다. 단, 암호 문구는 기본적으로 사용하지 않도록 설정되어 있습니다. vSphere Client에서 `Security.PasswordQualityControl` 고급 옵션을 사용하여 기본 설정 및 기타 설정을 변경할 수 있습니다.

예를 들어 옵션을 다음으로 변경할 수 있습니다.

```
retry=3 min=disabled,disabled,16,7,7
```

이 예에서는 최소 16자 및 최소 3개 단어의 암호 문구를 허용합니다.

레거시 호스트의 경우 `/etc/pam.d/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(`passphrase=4`) 단어가 필요하도록 기본값을 변경할 수 있습니다.

```
retry=3 min=disabled,disabled,15,7,7 passphrase=4
```

자세한 내용은 `pam_passwdqc`의 매뉴얼 페이지를 참조하십시오.

참고 가능한 모든 암호 옵션의 조합이 테스트되지는 않았습니다. 기본 암호 설정을 변경한 후에는 테스트를 수행하십시오.

이 예에서는 암호 복잡성 요구 사항에 상당한 암호 차이를 적용하는 네 가지 문자 클래스의 8개 문자, 5개 암호 기록 기억, 90일 순환 정책을 요구하도록 설정합니다.

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

`Security.PasswordHistory` 옵션을 5로 설정하고 `Security.PasswordMaxDays` 옵션을 90으로 설정합니다.

ESXi 계정 잠금 동작

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 5번의 시도 실패가 허용되고 15분 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. 0은 계정 잠금을 비활성화합니다.
- `Security.AccountUnlockTime`. 사용자가 잠기게 되는 시간(초)입니다.
- `Security.PasswordHistory`. 각 사용자에 대해 기억할 암호 수입니다. 0은 암호 기록을 비활성화합니다.

ESXi 고급 옵션 설정에 대한 자세한 내용은 "vCenter Server 및 호스트 관리" 설명서를 참조하십시오.

암호화 키 생성

ESXi는 정상적인 작업을 위한 여러 비대칭 키를 생성합니다. TLS(Transport Layer Security) 키는 TLS 프로토콜을 사용하여 ESXi 호스트와의 통신을 보호합니다. SSH 키는 SSH 프로토콜을 사용하여 ESXi 호스트와의 통신을 보호합니다.

TLS(Transport Layer Security) 키

TLS(Transport Layer Security) 키는 TLS 프로토콜을 사용하여 호스트와의 통신을 보호합니다. 처음 부팅하면 ESXi 호스트가 TLS 키를 2048비트 RSA 키로 생성합니다. 현재 ESXi는 TLS에 대한 ECDSA 키의 자동 생성을 구현하지 않습니다. TLS 개인 키는 관리자가 서비스하기 위한 것이 아닙니다.

TLS 키는 다음과 같은 비영구적 위치에 상주합니다.

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

TLS 공용 키(중간 인증 기관 포함)는 다음과 같은 비영구적 위치에 X.509 v3 인증서로 상주합니다.

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

ESXi 호스트에서 vCenter Server를 사용하면 vCenter Server는 CSR을 자동으로 생성하고 VMCA(VMware Certificate Authority)를 사용하여 서명한 후 인증서를 생성합니다. ESXi 호스트를 vCenter Server에 추가하면 vCenter Server가 결과 인증서를 ESXi 호스트에 설치합니다.

기본 TLS 인증서는 설치 시 호스트 이름과 일치하는 subjectAltName 필드를 사용하여 자체 서명됩니다. 예를 들어 다른 인증서를 설치하여 다른 subjectAltName을 사용하거나 확인 체인에 특정 CA(인증 기관)를 포함할 수 있습니다. ESXi SSL 인증서 및 키 교체의 내용을 참조하십시오.

VMware Host Client를 사용하여 인증서를 교체할 수도 있습니다. "vSphere 단일 호스트 관리 - VMware Host Client" 의 내용을 참조하십시오.

SSH 키

SSH 키는 SSH 프로토콜을 사용하여 ESXi 호스트와의 통신을 보호합니다. 처음 부팅하면 시스템에서 nistp256 ECDSA 키와 SSH 키가 2048비트 RSA 키로 생성됩니다. SSH 서버는 기본적으로 비활성화되어 있습니다. SSH 액세스는 주로 문제 해결을 위한 것입니다. SSH 키는 관리자가 서비스하기 위한 것이 아닙니다. SSH를 통해 로그인하려면 전체 호스트 제어와 동등한 관리 권한이 필요합니다. SSH 액세스를 사용하도록 설정하려면 ESXi Shell에 대한 액세스를 사용하도록 설정 항목을 참조하십시오.

SSH 공용 키는 다음 위치에 있습니다.

`/etc/ssh/ssh_host_rsa_key.pub`

`/etc/ssh/ssh_host_ecdsa_key.pub`

SSH 개인 키는 다음 위치에 상주합니다.

`/etc/ssh/ssh_host_rsa_key`

`/etc/ssh/ssh_host_ecdsa_key`

TLS 암호화 키 설정

TLS 암호화 키 설정 구성은 TLS 암호 그룹 선택에 따라 결정되며, 이것은 일시적 ECDH(Ecliptic Curve Diffie Hellman)(NIST Special Publication 800-56A에 명시됨)를 사용하는 ECC 기반 키 계약 또는 RSA 기반 키 전송(NIST Special Publication 800-56B에 명시됨) 중 하나를 선택합니다.

SSH 암호화 키 설정

SSH 암호화 키 설정의 구성은 SSHD 구성에 따라 결정됩니다. ESXi는 RSA 기반 키 전송(NIST Special Publication 800-56B에 명시됨), 일시적 DH(DH)(NIST Special Publication 800-56A에 명시됨) 키 계약, 일시적 ECDH(Ecliptic Curve Diffie Hellman)(NIST Special Publication 800-56A에 명시됨)를 허용하는 기본 구성을 제공합니다. SSHD 구성은 관리자가 서비스하기 위한 것이 아닙니다.

SSH 보안

ESXi Shell 및 SSH 인터페이스는 기본적으로 사용하지 않도록 설정됩니다. 문제 해결 또는 지원 작업을 수행하지 않는 한 이러한 인터페이스를 사용하지 않도록 설정해 두어야 합니다. 일상적인 작업의 경우 vSphere Client를 사용합니다. 여기서 작업은 역할 기반 액세스 제어 및 최신 액세스 제어 방법을 따릅니다.

ESXi의 SSH 구성에서는 다음 설정을 사용합니다.

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.

ESXi SSH 키

SSH 키로 ESXi 호스트에 대한 액세스를 제한, 제어 및 보호할 수 있습니다. SSH 키를 사용하면 신뢰할 수 있는 사용자 또는 스크립트가 암호를 입력하지 않고 호스트에 로그인하도록 허용할 수 있습니다.

vifs 명령을 사용하여 SSH 키를 호스트에 복사할 수 있습니다. 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(http://kb.vmware.com/kb/1002866)를 참조하십시오.

SSH를 사용하도록 설정하고 호스트에 SSH 키를 추가하면 위험이 수반됩니다. 사용자 이름 및 암호가 노출될 위험과 신뢰할 수 있는 키를 가진 사용자가 침입할 위험을 비교하여 판단하십시오.

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 사용자에 대한 인증된 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. 이렇게 하면 변경 사항을 호스트 데몬(hostd)에서 알지 못합니다.

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 사용자에 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 사용자에 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 엽니다.

2 파일을 다음 위치에 게시합니다.

키의 유형	위치
루트 사용자에 대한 인증된 키 파일	`https://hostname_or_IP_address/host/ssh_root_authorized_keys` 이 파일을 업로드하려면 호스트에 대한 전체 관리자 권한이 있어야 합니다.
DSA 키	`https://hostname_or_IP_address/host/ssh_host_dsa_key`
DSA 공용 키	`https://hostname_or_IP_address/host/ssh_host_dsa_key_pub`
RSA 키	`https://hostname_or_IP_address/host/ssh_host_rsa_key`
RSA 공용 키	`https://hostname_or_IP_address/host/ssh_host_rsa_key_pub`

PCI와 PCIe 디바이스 및 ESXi

VMware DirectPath I/O 기능을 사용하여 PCI 또는 PCIe 디바이스를 가상 시스템에 전달하면 잠재적인 보안 취약성이 발생합니다. 버그성 코드나 악성 코드(예: 디바이스 드라이버)가 게스트 운영 체제에서 권한이 있는 모드로 실행되면 취약성이 유발될 수 있습니다. 현재는 업계 표준 하드웨어 및 펌웨어에서 ESXi 호스트를 취약성으로부터 보호할 수 있는 충분한 오류 억제가 지원되지 않습니다.

신뢰할 수 있는 엔티티가 가상 시스템을 소유하고 관리하는 경우에만 가상 시스템에 대한 PCI 또는 PCIe 패스스루를 사용하십시오. 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. 통과하는 하드웨어 디바이스의 버그 또는 비호환성으로 인해서나 게스트 운영 체제의 드라이버 관련 문제로 인해 이러한 오류가 발생할 수 있습니다.
- 게스트 운영 체제가 ESXi 호스트에서 IOMMU 페이지 장애를 일으키는 DMA(Direct Memory Access) 작업을 생성할 수 있습니다. 예를 들어 DMA 작업이 가상 시스템의 메모리 외부 주소를 대상으로 하는 경우 이 작업이 생성될 수 있습니다. 일부 시스템에서 호스트 펌웨어는 IOMMU 장애가 NMI(Non-Maskable Interrupt)를 통해 치명적인 오류를 보고하도록 구성하고 이 치명적인 오류로 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 높으며 이론적으로는 이러한 가상 인터럽트를 악용하는 다른 방법이 존재할 수 있습니다.

MOB(Managed Object Browser) 사용 안 함

MOB(Managed Object Browser)에서는 VMkernel 개체 모델을 탐색할 수 있습니다. 그러나 MOB를 사용하여 호스트 구성을 변경할 수 있기 때문에 공격자는 이 인터페이스를 사용하여 악의적인 구성 변경이나 작업을 수행할 수 있습니다. 디버깅 목적에만 MOB를 사용하고 운영 시스템에서는 사용하지 않도록 설정합니다.

MOB는 기본적으로 사용하지 않도록 설정되어 있습니다. 하지만 특정 태스크(예: 시스템에서 이전 인증서 추출)의 경우 MOB를 사용해야 합니다. 다음과 같이 MOB를 사용하거나 사용하지 않도록 설정할 수 있습니다.

절차

1. vSphere Client 인벤토리에서 호스트를 찾습니다.
2. **구성**을 클릭합니다.
3. 시스템 아래에서 **고급 시스템 설정**을 클릭합니다.
4. **Config.HostAgent.plugins.solo.enableMob**의 값을 확인하고 **편집**을 클릭하여 적절히 변경합니다.

   ESXi Shell에서는 `vim-cmd`를 사용하지 마십시오.

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 VMware vSphere® vMotion® 트래픽이 가상 시스템이 있는 네트워크를 통해 이동하지 않도록 합니다. 분리 기능을 활용하면 스누핑이 방지됩니다. 분리된 네트워크를 사용하면 성능 측면에서도 도움이 됩니다.

- vSphere 인프라 네트워크는 vSphere vMotion, VMware vSphere Fault Tolerance, VMware vSAN, 스토리지 같은 기능에 사용됩니다. 해당하는 특정 기능에 맞게 이러한 네트워크를 분리합니다. 이러한 네트워크를 단일 물리적 서버 랙 외부로 라우팅할 필요는 거의 없습니다.
- 관리 네트워크에서는 클라이언트 트래픽, CLI(명령줄 인터페이스) 또는 API 트래픽 및 타사 소프트웨어 트래픽을 다른 트래픽으로부터 분리합니다. 일반적으로 관리 네트워크는 시스템, 네트워크 및 보안 관리자만 액세스할 수 있습니다. 관리 네트워크에 대한 액세스를 보호하려면 배스천 호스트 또는 VPN(Virtual Private Network)을 사용합니다. 이 네트워크 내의 액세스는 엄격하게 제어합니다.
- 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.

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

vSphere Auto Deploy를 사용할 때는 네트워킹 보안, 부팅 이미지 보안 및 호스트 프로파일을 통한 암호 노출 가능성에 주의를 기울여서 환경을 보호해야 합니다.

네트워킹 보안

다른 PXE 기반 배포 방법을 사용할 때 네트워크를 보호하는 것과 마찬가지로 네트워크를 보호해야 합니다. 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 이미지에는 다음과 같은 구성 요소가 포함될 수 있습니다.

- 이미지 프로파일을 구성하는 VIB 패키지는 항상 부팅 이미지에 포함됩니다.
- 호스트 프로파일 또는 호스트 사용자 지정을 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 SHA-512로 해싱됩니다.
  - 프로파일과 연결된 다른 암호는 암호화되지 않습니다. 호스트 프로파일을 사용하여 Active Directory를 설정하는 경우에는 암호가 보호되지 않습니다.

    Active Directory 암호의 노출을 방지하기 위해 vSphere Authentication Proxy를 사용합니다. 호스트 프로파일을 사용하여 Active Directory를 설정하면 암호가 보호되지 않습니다.
- 호스트의 공용 및 개인 SSL 키와 인증서가 부팅 이미지에 포함됩니다.

CIM 기반 하드웨어 모니터링 도구에 대한 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 원격 애플리케이션에 필요한 최소한의 액세스 권한만 제공합니다. 루트 또는 관리자 계정으로 원격 애플리케이션을 프로비저닝하며 애플리케이션이 손상된 경우 가상 환경이 손상될 수 있습니다.

CIM은 ESXi 호스트의 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 드라이브 및 기본 하드웨어에 대한 관리 액세스를 지원합니다. 서버 제조업체 및 하드웨어 디바이스 벤더를 포함한 하드웨어 벤더는 디바이스를 모니터링 및 관리하는 제공자를 쓸 수 있습니다. VMware는 서버 하드웨어, ESXi 스토리지 인프라 및 가상화 관련 리소스를 모니터링하는 제공자를 씁니다. 이러한 제공자는 ESXi 호스트 내부에서 실행되며 경량이고 특정 관리 작업에 초점을 맞춥니다. CIM 브로커는 모든 CIM 제공자로부터 정보를 가져오고 표준 API를 사용하여 이를 외부에 표시합니다. 가장 일반적인 API는 WS-MAN입니다.

원격 애플리케이션에는 CIM 인터페이스에 액세스하기 위한 루트 자격 증명을 제공하지 마십시오. 대신 이러한 애플리케이션에 권한이 낮은 vSphere 사용자 계정을 만들고 VIM API 티켓 기능을 사용하여 권한이 낮은 사용자 계정에 sessionId("티켓"이라고 함)를 발행하여 CIM에 인증합니다. 계정에 CIM 티켓을 얻을 수 있는 권한이 부여되면 VIM API는 티켓을 CIM에 제공할 수 있습니다. 이러한 티켓은 CIM-XML API 호출에 대해 사용자 ID와 암호로 제공됩니다. 자세한 내용은 `AcquireCimServicesTicket()` 메서드를 참조하십시오.

CIM 서비스는 타사 CIM VIB를 설치할 때, 예를 들어 `esxcli software vib install -n VIBname` 명령을 실행할 때 시작됩니다.

CIM 서비스를 수동으로 사용하도록 설정해야 하는 경우에는 다음 명령을 실행합니다.

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

필요한 경우 CIM 서비스만 실행되도록 wsman(WSManagement 서비스)를 사용하지 않도록 설정할 수 있습니다.

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

wsman이 사용하지 않도록 설정되었는지 확인하려면 다음 명령을 실행 합니다.

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

ESXCLI 명령에 대한 자세한 내용은 "ESXCLI 설명서" 를 참조하십시오. CIM 서비스를 사용하도록 설정하는 방법에 대한 자세한 내용은 https://kb.vmware.com/kb/1025757에서 VMware 기술 자료 문서를 참조하십시오.

절차

1 CIM 애플리케이션에 대해 루트가 아닌 vSphere 사용자 계정을 생성합니다.

"vSphere 인증" 에서 vCenter Single Sign-On 사용자 추가에 대한 항목을 참조하십시오. 사용자 계정에 필요한 vSphere 권한은 **Host.CIM.Interaction**입니다.

2 원하는 vSphere API SDK를 사용하여 vCenter Server에 사용자 계정을 인증합니다. 그런 다음, `AcquireCimServicesTicket()`을 호출하여 티켓을 반환하고 CIM-XML 포트 5989 또는 WS-Man 포트 433 API를 사용하여 ESXi를 관리자 수준 계정으로 인증합니다.

자세한 내용은 "vSphere Web Services API 참조" 를 참조하십시오.

3 필요에 따라 2분마다 티켓을 갱신합니다.

ESXi 호스트에 대한 인증서 관리

VMCA(VMware Certificate Authority)는 기본적으로 각 ESXi 호스트에 루트 인증 기관이 VMCA인 서명된 인증서를 프로비저닝합니다. 프로비저닝은 호스트가 vCenter Server에 명시적으로 추가되거나 ESXi 6.0 이상으로의 업그레이드 또는 설치의 일부로 추가될 때 발생합니다.

vSphere Client에서 그리고 vSphere Web Services SDK에서 `vim.CertificateManager` API를 사용하여 ESXi 인증서를 보고 관리할 수 있습니다. vCenter Server 인증서 관리에 사용할 수 있는 인증서 관리 CLI를 사용하여 ESXi 인증서를 보거나 관리할 수 없습니다.

vSphere 6.0 이상의 인증서

ESXi 및 vCenter Server는 통신할 때 거의 모든 관리 트래픽에 TLS를 사용합니다.

vSphere 6.0 이상에서 vCenter Server는 ESXi 호스트에 대한 다음과 같은 인증서 모드를 지원합니다.

표 3-2. ESXi 호스트에 대한 인증서 모드

인증서 모드	설명
VMware Certificate Authority(기본값)	VMCA가 모든 ESXi 호스트를 최상위 CA 또는 중간 CA로 프로비저닝하는 경우 이 모드를 사용합니다. 기본적으로 VMCA는 인증서로 ESXi 호스트를 프로비저닝합니다. 이 모드에서는 vSphere Client에서 인증서를 새로 고치거나 갱신할 수 있습니다.
사용자 지정 인증 기관	타사 또는 엔터프라이즈 CA가 서명한 사용자 지정 인증서만 사용하려는 경우 이 모드를 사용합니다. 이 모드에서는 사용자가 인증서 관리에 대한 책임이 있습니다. vSphere Client에서 인증서를 새로 고치거나 갱신할 수 없습니다. **참고** 인증서 모드를 사용자 지정 인증 기관으로 변경하는 경우가 아니면 VMCA가 vSphere Client에서 **갱신**을 선택하는 경우와 같이 사용자 지정 인증서를 교체할 수도 있습니다.
지문 모드	vSphere 5.5에서는 지문 모드를 사용했으며 이 모드는 vSphere 6.x에 대한 폴백 옵션으로 아직 사용할 수 있습니다. 이 모드에서 vCenter Server는 인증서가 올바른 형식인지 검사하지만 인증서의 유효성은 검사하지 않습니다. 만료된 인증서도 수락됩니다. 다른 두 모드 중 하나로 해결할 수 없는 문제가 발생하는 경우가 아니면 이 모드를 사용하지 마십시오. 일부 vCenter 6.x 이상 서비스는 지문 모드에서 올바르게 작동하지 않을 수 있습니다.

인증서 만료

vSphere 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 vCenter Server 시스템의 일부입니다.

Auto Deploy 호스트가 처음으로 부팅될 때 VMCA를 사용할 수 없는 경우 호스트에서 먼저 연결을 시도합니다. 연결할 수 없는 경우 호스트는 VMCA를 사용할 수 있게 되고 서명된 인증서를 사용하여 호스트를 프로비저닝할 수 있을 때까지 종료와 재부팅을 반복합니다.

ESXi 인증서 관리에 필요한 권한

ESXi 호스트의 인증서를 관리하려면 **인증서.인증서 관리** 권한이 있어야 합니다. 이 권한은 vSphere Client에서 설정할 수 있습니다.

호스트 이름 및 IP 주소 변경 사항

호스트 이름 또는 IP 주소 변경은 vCenter Server가 호스트 인증서를 유효한 인증서로 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 3-3. 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.

호스트 업그레이드 및 인증서

ESXi 호스트를 ESXi 6.5 이상으로 업그레이드하는 경우 업그레이드 프로세스가 자체 서명된 (지문) 인증서를 VMCA 서명된 인증서로 교체합니다. ESXi 호스트에서 사용자 지정 인증서를 사용하는 경우 해당 인증서가 만료되었거나 잘못된 경우에도 업그레이드 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. 해당 호스트를 ESXi 6.5 이상으로 업그레이드해야 합니다.

사용자 지정 인증서로 프로비저닝된 호스트

호스트가 일반적으로 타사 CA 서명된 인증서인 사용자 지정 인증서로 프로비저닝된 경우 업그레이드 중 이러한 인증서가 제자리에 유지됩니다. 인증서 모드를 **사용자 지정**으로 변경하여 나중에 인증서 새로 고침을 수행하는 동안 인증서가 실수로 교체되지 않도록 합니다.

참고 환경이 VMCA 모드에 있으며 vSphere Client에서 인증서를 새로 고치는 경우 모든 기존 인증서가 VMCA에서 서명한 인증서로 교체됩니다.

앞으로 vCenter Server는 vSphere Client에서 인증서를 모니터링하고 인증서 만료 등에 대한 정보를 표시합니다.

Auto Deploy를 사용하여 프로비저닝된 호스트

Auto Deploy를 통해 프로비저닝되는 호스트는 항상 ESXi 6.5 이상 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.

Auto Deploy와 함께 사용자 지정 인증서 사용의 내용을 참조하십시오.

인증서 모드 전환 워크플로

vSphere 6.0부터는 ESXi 호스트가 기본적으로 VMCA를 통해 인증서로 프로비저닝됩니다. 대신 사용자 지정 인증서 모드를 사용하거나 디버깅 목적으로 기존 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.

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 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 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. 워크플로는 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 변경의 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. 워크플로는 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 변경의 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 변경의 내용을 참조하십시오.

지문 모드에서 VMCA 모드로 전환

지문 모드를 사용하며 VMCA 서명된 인증서를 사용하기 시작하려는 경우 전환에 약간의 계획이 필요합니다. 워크플로는 다음과 같습니다.

1 vCenter Server 시스템에서 모든 호스트를 제거합니다.

2 VMCA 인증서 모드로 전환합니다. 인증서 모드 변경의 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 변경의 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. 워크플로는 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 변경의 내용을 참조하십시오.

5 호스트를 vCenter Server 시스템에 추가합니다.

ESXi 인증서 기본 설정

호스트가 vCenter Server 시스템에 추가되면 vCenter Server가 호스트에 대한 CSR(인증서 서명 요청)을 VMCA에 보냅니다. 대부분의 기본값은 여러 상황에 잘 적용되지만 회사별 정보는 변경할 수 있습니다.

vSphere Client를 사용하여 여러 가지 기본 설정을 변경할 수 있습니다. 조직 및 위치 정보 변경을 고려하십시오. 인증서 기본 설정 변경의 내용을 참조하십시오.

표 3-4. ESXi CSR 설정

매개 변수	기본값	고급 옵션
키 크기	2048	해당 없음
키 알고리즘	RSA	해당 없음
인증서 서명 알고리즘	sha256WithRSAEncryption	해당 없음
일반 이름	호스트 이름으로 호스트가 vCenter Server에 추가된 경우 호스트의 이름입니다. IP 주소로 호스트가 vCenter Server에 추가된 경우 호스트의 IP 주소입니다.	해당 없음
국가	USA	vpxd.certmgmt.certs.cn.country
이메일 주소	vmca@vmware.com	vpxd.certmgmt.certs.cn.email
구/군/시	Palo Alto	vpxd.certmgmt.certs.cn.localityName
조직 구성 단위 이름	VMware 엔지니어링	vpxd.certmgmt.certs.cn.organizationalUnitName
조직 이름	VMware	vpxd.certmgmt.certs.cn.organizationName
시/도	California	vpxd.certmgmt.certs.cn.state
인증서가 유효한 일 수입니다.	1825	vpxd.certmgmt.certs.daysValid
인증서 만료에 대한 하드 임계값입니다. 이 임계값에 도달하면 vCenter Server에서 빨간색 경보가 발생합니다.	30일	vpxd.certmgmt.certs.cn.hardThreshold
vCenter Server 인증서 유효성 검사에 대한 폴링 간격입니다.	5일	vpxd.certmgmt.certs.cn.pollIntervalDays
인증서 만료에 대한 소프트 임계값입니다. 이 임계값에 도달하면 vCenter Server에서 이벤트가 발생합니다.	240일	vpxd.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 인증서의 내용을 참조하십시오.	vmca 또한 지문이나 사용자 지정으로 지정할 수 있습니다. 인증서 모드 변경의 내용을 참조하십시오.	vpxd.certmgmt.mode

인증서 기본 설정 변경

호스트가 vCenter Server 시스템에 추가되면 vCenter Server가 호스트에 대한 CSR(인증서 서명 요청)을 VMCA에 보냅니다. vSphere Client의 vCenter Server 고급 설정을 사용하여 CSR의 일부 기본 설정을 변경할 수 있습니다.

기본 설정 목록은 ESXi 인증서 기본 설정 항목을 참조하십시오. 일부 기본값은 변경할 수 없습니다.

절차

1 vSphere Client에서 호스트를 관리하는 vCenter Server 시스템을 선택합니다.

2 **구성**을 클릭하고 **고급 설정**을 클릭합니다.

3 **설정 편집**을 클릭합니다.

4 [이름] 열에서 **필터** 아이콘을 클릭하고 [필터] 상자에 **`vpxd.certmgmt`**를 입력하여 인증서 관리 매개 변수만 표시합니다.

5 회사 정책을 따르도록 기존 매개 변수의 값을 변경하고 **저장**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. 이미 vCenter Server 시스템을 통해 관리되는 호스트의 인증서를 변경하려면 호스트의 연결을 끊었다가 다시 연결하거나 인증서를 갱신할 수 있습니다.

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 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 Client를 사용하여 vCenter Server에 로그인합니다.

2 인벤토리 목록을 찾아서 vCenter Server 인스턴스를 선택합니다.

3 **호스트 및 클러스터 > 호스트**를 선택합니다.

기본적으로 호스트 표시에는 인증서 상태가 포함되어 있지 않습니다.

4 열을 표시하거나 숨기려면 왼쪽 아래 모서리에 있는 세 개의 막대형 **열 선택기**를 클릭합니다.

5 **인증서 유효 기간 종료** 확인란을 선택하고 필요한 경우 오른쪽으로 스크롤하여 추가된 열을 봅니다.

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.

6 (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 고침의 내용을 참조하십시오.

단일 ESXi 호스트에 대한 인증서 세부 정보 보기

VMCA 모드 또는 사용자 지정 모드에 있는 ESXi 6.0 이상 호스트의 경우 vSphere Client에서 인증서 세부 정보를 볼 수 있습니다. 인증서에 대한 정보는 디버깅에 유용할 수 있습니다.

절차

1 vSphere Client 인벤토리에서 호스트를 찾습니다.

2 **구성**을 클릭합니다.

3 **시스템** 아래에서 **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. **정상** 정상 작업입니다. **만료** 인증서가 곧 만료됩니다. **곧 만료됨** 인증서가 8개월 이내에 만료됩니다(기본값). **만료 임박** 인증서가 2개월 이내에 만료됩니다(기본값). **만료됨** 인증서가 만료되었으므로 유효하지 않습니다.

ESXi 인증서 갱신 또는 새로 고침

VMCA가 인증서를 ESXi 호스트(6.0 이상)에 할당하는 경우 vSphere 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 만료되기 전에 갱신하지 않을 경우 호스트의 연결을 끊었다가 다시 연결하면 vCenter Server에서 인증서를 갱신합니다. 호스트를 vCenter Server에 다시 추가하여 신뢰가 다시 설정되고 vCenter Server가 갱신된 인증서를 무조건 발급할 수 있습니다.

기본적으로 vCenter Server는 호스트가 인벤토리에 추가되거나 다시 연결될 때마다 만료됨, 만료 임박 또는 곧 만료됨 상태인 호스트의 인증서를 갱신합니다.

사전 요구 사항

다음을 확인합니다.

- ESXi 호스트는 vCenter Server 시스템에 연결되어 있습니다.
- vCenter Server 시스템과 ESXi 호스트 간에 적절한 시간 동기화가 있습니다.
- DNS 확인은 vCenter Server 시스템과 ESXi 호스트 간에 작동합니다.
- vCenter Server 시스템의 MACHINE_SSL_CERT 및 Trusted_Root 인증서가 유효하며 만료되지 않았습니다. VMware 기술 자료 문서(https://kb.vmware.com/s/article/2111411)를 참조하십시오.
- ESXi 호스트가 유지 보수 모드로 설정되지 않았습니다.

절차

1. vSphere Client 인벤토리에서 호스트를 찾습니다.
2. **구성**을 클릭합니다.
3. **시스템** 아래에서 **인증서**를 클릭합니다.

   선택한 호스트의 인증서에 대한 자세한 내용을 볼 수 있습니다.
4. **갱신** 또는 **CA 인증서 새로 고침**을 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. **예**를 클릭하여 확인합니다.

인증서 모드 변경

회사 정책에 따라 사용자 지정 인증서를 사용해야 하는 경우가 아니라면 VMCA를 사용하여 ESXi 호스트를 프로비저닝합니다. 다른 루트 CA에 사용자 지정 인증서를 사용하려면 vCenter Server `vpxd.certmgmt.mode` 고급 옵션을 편집할 수 있습니다. 변경 후에는 인증서를 새로 고칠 때 호스트가 VMCA 인증서로 자동 프로비저닝되지 않습니다. 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 vSphere Client에서 호스트를 관리하는 vCenter Server 시스템을 선택합니다.

2 **구성**을 클릭하고 [설정] 아래에서 **고급 설정**을 클릭합니다.

3 **설정 편집**을 클릭합니다.

4 [이름] 열에서 **필터** 아이콘을 클릭하고 [필터] 상자에 **vpxd.certmgmt**를 입력하여 인증서 관리 매개 변수만 표시합니다.

5 vpxd.certmgmt.mode의 값을 **custom**으로 변경하거나(자신의 인증서를 관리하려는 경우) **thumbprint**로 변경하고(일시적으로 지문 모드를 사용하려는 경우) **저장**을 클릭합니다.

6 vCenter Server 서비스를 다시 시작합니다.

서비스 다시 시작에 대한 자세한 내용은 "vCenter Server 구성" 설명서를 참조하십시오.

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 필요한 경우 VMCA 서명 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 방법은 다양합니다.

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 호스트에 CA 서명된 인증서를 사용하는 방법에 대한 자세한 내용은 인증서 모드 전환 워크플로에서 참조하십시오.

참고 vSAN 클러스터의 일부인 ESXi 호스트에서 SSL 인증서를 교체하는 경우 https://kb.vmware.com/s/article/56441에서 VMware 기술 자료 문서에 나와 있는 단계를 수행하십시오.

- ESXi 인증서 서명 요청에 대한 요구 사항

  엔터프라이즈 또는 타사 CA 서명 인증서 또는 하위 CA 서명 인증서를 사용하려는 경우 CA에 CSR(인증서 서명 요청)을 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

엔터프라이즈 또는 타사 CA 서명 인증서 또는 하위 CA 서명 인증서를 사용하려는 경우 CA에 CSR(인증서 서명 요청)을 보내야 합니다.

이러한 특성의 CSR을 사용합니다.

- 키 크기: 2048비트(최소)~16384비트(최대)(PEM 인코딩)
- PEM 형식. VMware는 PKCS8 및 PKCS1(RSA 키)을 지원합니다. 키가 VECS에 추가되면 추가된 키가 PKCS8로 변환됩니다.
- x509 버전 3
- 루트 인증서의 경우 CA 확장을 true로 설정해야 하며 인증서 서명이 요구 사항 목록에 있어야 합니다.
- SubjectAltName에는 DNS Name=<machine_FQDN>이 포함되어야 합니다.
- CRT 형식
- 다음과 같은 키 사용이 포함되어 있습니다. 디지털 서명, 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).

vSphere는 다음 인증서를 지원하지 않습니다.

- 와일드카드가 있는 인증서.
- md2WithRSAEncryption, md5WithRSAEncryption, RSASSA-PSS, dsaWithSHA1, ecdsa_with_SHA1 및 sha1WithRSAEncryption 알고리즘은 지원되지 않습니다.

CSR 생성에 대한 자세한 내용은 https://kb.vmware.com/s/article/2113926에서 VMware 기술 자료 문서를 참조하십시오.

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 Client에서 SSH 트래픽을 사용하도록 설정합니다.
- 모든 파일 전송과 그 밖의 통신은 보안 HTTPS 세션을 통해 이루어집니다. 세션을 인증하는 데 사용되는 사용자는 호스트에 대한 **Host.Config.AdvancedConfig** 권한이 있어야 합니다.

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/ssl`에 복사합니다.

4 새 인증서와 키의 이름을 각각 `rui.crt`와 `rui.key`로 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 스토어를 업데이트합니다. vCenter Server TRUSTED_ROOTS 스토어 업데이트(사용자 지정 인증서)의 내용을 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 Client에서 SSH 트래픽을 사용하도록 설정합니다.
- 모든 파일 전송과 그 밖의 통신은 보안 HTTPS 세션을 통해 이루어집니다. 세션을 인증하는 데 사용되는 사용자는 호스트에 대한 **Host.Config.AdvancedConfig** 권한이 있어야 합니다.

절차

1 기존 인증서를 백업합니다.

2 인증 기관으로부터 받은 지침에 따라 인증서 요청을 생성합니다.

ESXi 인증서 서명 요청에 대한 요구 사항의 내용을 참조하십시오.

3 인증서가 있는 경우 `vifs` 명령을 사용하여 SSH 연결에서 호스트로 인증서를 호스트의 적절한 위치에 업로드합니다.

```
vifs --server 호스트 이름 --username 사용자 이름 --put rui.crt /host/ssl_cert
vifs --server 호스트 이름 --username 사용자 이름 --put rui.key /host/ssl_key
```

4 호스트를 다시 시작합니다.

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 스토어를 업데이트합니다. vCenter Server TRUSTED_ROOTS 스토어 업데이트(사용자 지정 인증서)의 내용을 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 Client에서 SSH 트래픽을 사용하도록 설정합니다.
- 모든 파일 전송과 그 밖의 통신은 보안 HTTPS 세션을 통해 이루어집니다. 세션을 인증하는 데 사용되는 사용자는 호스트에 대한 **Host.Config.AdvancedConfig** 권한이 있어야 합니다.

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/ssl`에 있는 인증서 파일에 연결됩니다.

3 호스트를 다시 시작합니다.

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 스토어를 업데이트합니다. vCenter Server TRUSTED_ROOTS 스토어 업데이트(사용자 지정 인증서)의 내용을 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.

참고 ESXi 호스트에 설치된 것과 동일한 CA에서 발급한 사용자 지정 인증서를 사용하여 vCenter Server 시스템을 실행하는 경우에는 이 단계가 필요하지 않습니다.

절차

1 ESXi 호스트를 관리하는 vCenter Server 시스템의 vCenter Server 셸에 로그인합니다.

2 `TRUSTED_ROOTS` 저장소에 새 인증서를 추가하려면 `dir-cli`를 실행합니다. 예를 들면 다음과 같습니다.

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

3 메시지가 표시되면 Single Sign-On 관리자 자격 증명을 제공합니다.

4 사용자 지정 인증서가 중간 CA에서 발급된 경우 vCenter Server의 TRUSTED_ROOTS 저장소에도 중간 CA를 추가해야 합니다. 예를 들면 다음과 같습니다.

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

다음에 수행할 작업

인증서 모드를 사용자 지정으로 설정합니다. 인증서 모드가 기본값인 VMCA인 상태에서 인증서 새로 고침을 수행하면 사용자 지정 인증서가 VMCA 서명된 인증서로 교체됩니다. 인증서 모드 변경의 내용을 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

- CA에서 인증서를 요청합니다. 인증서는 다음 요구 사항을 충족해야 합니다.
  - 키 크기: 2048비트(최소)~16384비트(최대)(PEM 인코딩)
  - PEM 형식. VMware는 PKCS8 및 PKCS1(RSA 키)을 지원합니다. 키가 VECS에 추가되면 추가된 키가 PKCS8로 변환됩니다.
  - x509 버전 3
  - 루트 인증서의 경우 CA 확장을 true로 설정해야 하며 인증서 서명이 요구 사항 목록에 있어야 합니다.
  - SubjectAltName에는 DNS Name=<machine_FQDN>이 포함되어야 합니다.
  - CRT 형식
  - 다음과 같은 키 사용이 포함되어 있습니다. 디지털 서명, 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/ 디렉토리에 있습니다.

2 vSphere Authentication Proxy 서비스를 중지합니다.

도구	단계
vCenter Server 관리 인터페이스	a 웹 브라우저에서 vCenter Server 관리 인터페이스 https://*vcenter-IP-address-or-FQDN*:5480으로 이동합니다. b 루트로 로그인합니다. 기본 루트 암호는 vCenter Server를 배포하는 중에 설정하는 암호입니다. c **서비스**를 클릭하고 **VMware vSphere Authentication Proxy 서비스**를 클릭합니다. d **중지**를 클릭합니다.
CLI	`service-control --stop vmcam`

3 Auto Deploy 서비스가 실행되는 시스템에서 `/etc/vmware-rbd/ssl/`의 `rbd-ca.crt` 및 `rbd-ca.key`를 사용자 지정 인증서 및 키 파일로 교체합니다.

4 Auto Deploy 서비스가 실행되는 시스템에서 다음 명령을 실행하여 새 인증서를 사용하도록 VECS 내의 TRUSTED_ROOTS 저장소를 업데이트합니다.

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

5 TRUSTED_ROOTS 저장소의 컨텐츠가 포함된 `castore.pem` 파일을 생성하여 `/etc/vmware-rbd/ssl/` 디렉토리에 배치합니다.

사용자 지정 모드에서는 사용자에게 이 파일을 관리할 책임이 있습니다.

6 vCenter Server 시스템의 ESXi 인증서 모드를 **사용자 지정**으로 변경합니다.

인증서 모드 변경의 내용을 참조하십시오.

7 vCenter Server 서비스를 다시 시작하고 Auto Deploy 서비스를 시작합니다.

결과

다음 번에 Auto Deploy를 사용하도록 설정된 호스트를 프로비저닝하면 Auto Deploy 서버에서 인증서를 생성합니다. TRUSTED_ROOTS 저장소에 추가한 루트 인증서가 Auto Deploy 서버에서 사용됩니다.

참고 인증서 교체 후 Auto Deploy 관련 문제가 발생하면 VMware 기술 자료 문서(http://kb.vmware.com/kb/2000988)를 참조하십시오.

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 ESXi 호스트를 다시 시작합니다.

아니면 호스트를 유지 보수 모드로 전환하고 DCUI(Direct Console User Interface)를 사용하여 관리 에이전트를 다시 시작하고 호스트가 유지 보수 모드를 종료하도록 설정할 수 있습니다.

보안 프로파일을 사용하여 호스트 사용자 지정

vSphere Client의 보안 프로파일, 서비스 및 방화벽 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 액세스가 가능하도록 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 Client의 각 호스트에 대해 **구성 > 방화벽**을 사용합니다. ESXi 방화벽 설정 관리의 내용을 참조하십시오.
- 명령줄 또는 스크립트에서 ESXCLI 명령을 사용합니다. ESXi ESXCLI 방화벽 명령의 내용을 참조하십시오.
- 열려는 포트가 보안 프로파일에 포함되어 있지 않은 경우 사용자 지정 VIB를 사용합니다.

  사용자 지정 VIB를 설치하려면 ESXi 호스트의 허용 수준을 CommunitySupported로 변경해야 합니다.

  참고 CommunitySupported VIB가 설치된 ESXi 호스트의 문제를 조사하기 위해 VMware 기술 지원을 이용하는 경우 VMware 지원팀이 VIB를 제거하도록 요청할 수 있습니다. 이러한 요청은 해당 VIB가 조사 중인 문제와 관련이 있는지 확인하기 위한 문제 해결 단계입니다.

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 동작의 내용을 참조하십시오.

ESXi 방화벽 설정 관리

vSphere Client 또는 명령줄에서 서비스나 관리 에이전트에 대해 들어오는 방화벽 연결과 나가는 방화벽 연결을 구성할 수 있습니다.

이 작업은 vSphere Client를 사용하여 ESXi 방화벽 설정을 구성하는 방법에 대해 설명합니다. ESXi Shell 또는 ESXCLI 명령을 사용하여 명령줄에서 ESXi를 구성하여 방화벽 구성을 자동화할 수 있습니다. vSphere CLI에 대한 소개 정보는 "ESXCLI 시작" 의 내용을, 방화벽 및 방화벽 규칙 조작을 위한 ESXCLI 사용 예는 "ESXCLI 개념 및 예제" 의 내용을 참조하십시오.

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 Client를 사용하여 vCenter Server에 로그인합니다.

2 인벤토리에서 호스트를 찾습니다.

3 **구성**을 클릭한 다음 **시스템**에서 **방화벽**을 클릭합니다.

수신 및 **송신**을 클릭하여 수신 연결과 송신 연결 간에 전환할 수 있습니다.

4 방화벽 섹션에서 **편집**을 클릭합니다.

5 **그룹 해제됨**, **보안 셸**, **SNMP(단순 네트워크 관리 프로토콜)**라는 세 가지 서비스 그룹 중 하나를 선택합니다.

6 사용할 규칙 집합을 선택하거나, 사용하지 않을 규칙 집합을 선택 취소합니다.

7 일부 서비스의 경우 시스템에서 **구성 > 서비스**로 이동하여 서비스 세부 정보를 관리할 수도 있습니다.

서비스 시작, 중지 및 다시 시작하는 방법에 대한 자세한 내용은 서비스 사용 또는 사용 안 함을 참조하십시오.

8 일부 서비스의 경우 연결이 허용되는 IP 주소를 명시적으로 지정할 수 있습니다.

ESXi 호스트에 대해 허용되는 IP 주소 추가의 내용을 참조하십시오.

9 **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.

서비스에 대해 허용된 IP 목록을 업데이트하려면 vSphere Client, ESXCLI 또는 PowerCLI를 사용하면 됩니다. 기본적으로 서비스에 대해 모든 IP 주소가 허용됩니다. 이 작업에서는 vSphere Client를 사용하는 방법을 설명합니다. ESXCLI 사용에 대한 지침은 https://code.vmware.com/의 "ESXCLI 개념 및 예" 에서 방화벽 관리에 관한 항목을 참조하십시오.

절차

1 vSphere Client를 사용하여 vCenter Server에 로그인합니다.

2 ESXi 호스트를 찾습니다.

3 **구성**을 클릭한 다음 **시스템**에서 **방화벽**을 클릭합니다.

수신 및 **송신**을 클릭하여 수신 연결과 송신 연결 간에 전환할 수 있습니다.

4 방화벽 섹션에서 **편집**을 클릭합니다.

5 **그룹 해제됨**, **보안 셸**, **SNMP(단순 네트워크 관리 프로토콜)**라는 세 가지 서비스 그룹 중 하나를 선택합니다.

6 허용된 IP 주소 섹션을 표시하려면 서비스를 확장합니다.

7 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

8 서비스 자체가 선택되어 있는지 확인합니다.

9 **확인**을 클릭합니다.

10 서비스에 대한 **허용된 IP 주소** 열의 변경 사항을 확인합니다.

ESXi 호스트에 대해 들어오고 나가는 방화벽 포트

vSphere Client 및 VMware Host Client를 사용하면 각 서비스에 대한 방화벽 포트를 열고 닫거나 선택된 IP 주소의 트래픽을 허용할 수 있습니다.

ESXi에는 기본적으로 활성화되는 방화벽이 포함됩니다. 설치 시 ESXi 방화벽은 호스트 보안 프로파일에서 활성화된 서비스의 트래픽을 제외하고 들어오고 나가는 트래픽을 차단하도록 구성됩니다. ESXi 방화벽에서 지원되는 포트 및 프로토콜 목록은 https://ports.vmware.com/에서 VMware Ports and Protocols Tool™을 참조하십시오.

VMware Ports and Protocols Tool은 기본적으로 설치되는 서비스에 대한 포트 정보를 나열합니다. 호스트에 다른 VIB를 설치하는 경우 추가 서비스 및 방화벽 포트를 사용하게 될 수 있습니다. 이 정보는 vSphere Client에서 볼 수 있는 서비스에 주로 사용되지만 VMware Ports and Protocols Tool에는 몇 가지 다른 포트도 포함되어 있습니다.

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 `FALSE`로 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 ESXi 호스트가 여러 개 포함된 경우 ESXCLI 명령 또는 vSphere Web Services SDK를 사용하여 방화벽 구성을 자동화합니다.

방화벽 명령 참조

ESXi Shell 또는 ESXCLI 명령을 사용하여 명령줄에서 ESXi를 구성하여 방화벽 구성을 자동화할 수 있습니다. 방화벽 및 방화벽 규칙을 조작하려면 "ESXCLI 시작" 에서 소개를 참조하고 "ESXCLI 개념 및 예" 에서 ESXCLI를 사용하는 예를 참조하십시오.

ESXi 7.0 이상에서는 사용자 지정 방화벽 규칙을 생성하는 데 사용되는 service.xml 파일에 대한 액세스가 제한됩니다. /etc/rc.local.d/local.sh 파일을 사용하여 사용자 지정 방화벽 규칙을 생성하는 방법에 대한 자세한 내용은 VMware 기술 자료 문서 2008226을 참조하십시오.

표 3-5. 방화벽 명령

명령	설명
esxcli network firewall get	방화벽의 사용 여부 상태를 반환하고 기본 작업을 나열합니다.
esxcli network firewall set --default-action	기본 작업을 '통과'로 설정하려면 true로 설정하고 기본 작업을 '삭제'로 설정하려면 false로 설정합니다.
esxcli network firewall set --enabled	ESXi 방화벽을 사용하거나 사용하지 않도록 설정합니다.
esxcli network firewall load	방화벽 모듈 및 규칙 집합 구성 파일을 로드합니다.

표 3-5. 방화벽 명령 (계속)

명령	설명
esxcli network firewall refresh	방화벽 모듈이 로드된 경우 규칙 집합 파일을 읽어 방화벽 구성을 새로 고칩니다.
esxcli network firewall unload	필터를 제거하고 방화벽 모듈을 언로드합니다.
esxcli network firewall ruleset list	규칙 집합 정보를 나열합니다.
esxcli network firewall ruleset set --allowed-all	모든 IP에 대한 모든 액세스를 허용하려면 true로 설정하고 허용된 IP 주소 목록을 사용하려면 false로 설정합니다.
esxcli network firewall ruleset set --enabled --ruleset-id=<string>	지정된 규칙 집합을 사용하도록 설정하려면 enabled를 true로 설정합니다. 지정된 규칙 집합을 사용하지 않도록 설정하려면 enabled를 false로 설정합니다.
esxcli network firewall ruleset allowedip list	지정된 규칙 집합의 허용되는 IP 주소를 나열합니다.
esxcli network firewall ruleset allowedip add	지정된 IP 주소 또는 IP 주소 범위에서 규칙 집합에 액세스할 수 있도록 합니다.
esxcli network firewall ruleset allowedip remove	지정된 IP 주소 또는 IP 주소 범위에서 규칙 집합에 액세스할 수 없도록 합니다.
esxcli network firewall ruleset rule list	방화벽의 각 규칙 집합에 있는 규칙을 나열합니다.

보안 프로파일에서 ESXi 서비스 사용자 지정

ESXi 호스트에는 기본적으로 실행되는 여러 서비스가 포함됩니다. 회사 정책에서 허용하는 경우 보안 프로파일의 서비스를 사용 또는 사용하지 않도록 설정할 수 있습니다.

서비스 사용 또는 사용 안 함 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 Client에서 다음과 같은 서비스의 상태를 수정할 수 있습니다.

표 3-6. 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.
attestd	중지됨	vSphere 신뢰 기관 증명 서비스.
kmxd	중지됨	vSphere 신뢰 기관 키 제공자 서비스.
Active Directory 서비스	중지됨	Active Directory에 대한 ESXi를 구성할 때 이 서비스가 시작됩니다.
NTP 대몬	중지됨	네트워크 시간 프로토콜 대몬입니다.
PC/SC 스마트 카드 대몬	중지됨	호스트에 스마트 카드 인증을 사용하도록 설정하면 이 서비스가 시작됩니다. ESXi에 대한 스마트 카드 인증 구성의 내용을 참조하십시오.
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 Client의 고급 시스템 설정에서 syslog를 사용하도록 설정해야 합니다. "vCenter Server 설치 및 설정" 의 내용을 참조하십시오.
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.

서비스 사용 또는 사용 안 함

vSphere Client에서 서비스를 사용하거나 사용하지 않도록 설정할 수 있습니다.

설치 후 특정 서비스는 기본적으로 실행되지만 나머지는 중지됩니다. 경우에 따라, UI에서 서비스를 사용하려면 추가 설정이 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 Client를 사용하여 vCenter Server에 연결합니다.

절차

1 인벤토리에서 호스트를 찾습니다.

2 **구성**을 클릭한 다음 [시스템]에서 **서비스**를 클릭합니다.

3 변경하려는 서비스를 선택합니다.

a 호스트 상태를 한 번 변경하려는 경우 **다시 시작**, **시작** 또는 **중지**를 선택합니다.

b 재부팅 시 호스트의 상태를 변경하려면 **시작 정책 편집**을 클릭하고 정책을 선택합니다.

- **호스트와 함께 시작 및 중지**: 이 서비스는 호스트가 시작된 후 곧바로 시작되어 호스트가 종료되기 바로 전에 종료됩니다. **포트의 사용 현황에 따라 시작 및 중지**와 마찬가지로 이 옵션은 서비스가 정기적으로 작업(예: 지정된 NTP 서버에 연결)을 완료하려고 시도한다는 것을 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 경우 계속 실행됩니다. 서비스가 시작되고 호스트의 전원이 꺼지면 서비스가 종료 프로세스의 일부로 중지됩니다. 호스트의 전원이 켜지면 서비스가 다시 시작되고 사용자가 결정한 상태가 유지됩니다.
- **포트의 사용 현황에 따라 시작 및 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.

참고 이러한 설정은 UI를 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.

4 **확인**을 클릭합니다.

잠금 모드

ESXi 호스트의 보안 수준을 높이려면 호스트를 잠금 모드로 설정합니다. 잠금 모드에서는 기본적으로 작업을 vCenter Server를 통해 수행해야 합니다.

정상 잠금 모드 또는 엄격 잠금 모드를 선택하여 다른 수준의 잠금을 제공할 수 있습니다. 예외 사용자 목록을 사용할 수도 있습니다. 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 지정의 내용을 참조하십시오.

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 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 계정은 DCUI에 액세스할 수 있습니다. 또한 `DCUI.Access` 고급 시스템 설정에서 지정된 사용자는 DCUI에 액세스할 수 있습니다.
- ESXi Shell 또는 SSH가 사용 설정되고 호스트가 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. 관리자 권한이 없는 사용자에 대한 ESXi 또는 SSH 세션은 닫힙니다.

엄격 및 정상 잠금 모드 모두에 대해 모든 액세스가 기록됩니다.

표 3-7. 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 사용자, 권한 기반 vCloud Director(vslauser, 사용 가능한 경우)
DCUI(Direct Console User Interface)	호스트에서 관리자 권한이 있는 사용자 및 `DCUI.Access` 고급 옵션의 사용자	`DCUI.Access` 고급 옵션에서 정의된 사용자 호스트에서 관리자 권한이 있는 예외 사용자	DCUI 서비스가 중지됩니다.
ESXi Shell(사용하도록 설정된 경우) 및 SSH(사용하도록 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. 다른 모든 사용자에 대해서는 세션이 닫힙니다. 종료는 정상 및 엄격 잠금 모드에 모두 적용됩니다.

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 동작의 내용을 참조하십시오.

절차

1 vSphere Client 인벤토리에서 호스트를 찾습니다.

2 **구성**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 사용할 수 있도록 설정된 경우 액세스가 가능할 수 있습니다.
엄격	vCenter Server를 통해서만 호스트에 액세스할 수 있습니다. SSH 또는 ESXi Shell이 사용할 수 있도록 설정된 경우 `DCUI.Access` 고급 옵션의 계정 및 관리자 권한이 있는 예외 사용자 계정에 대해 실행 중인 세션은 사용 상태로 유지되고 기타 모든 세션은 닫힙니다.

6 **확인**을 클릭합니다.

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.

다음과 같이 잠금 모드를 사용하지 않도록 설정할 수 있습니다.

그래픽 사용자 인터페이스에서

사용자는 vSphere 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 Client 인벤토리에서 호스트를 찾습니다.

2 **구성**을 클릭합니다.

3 시스템 아래에서 **보안 프로파일**을 선택합니다.

4 [잠금 모드] 패널에서 **편집**을 클릭합니다.

5 **잠금 모드**를 클릭하고 **사용 안 함**을 선택하여 잠금 모드를 사용하지 않도록 설정합니다.

6 **확인**을 클릭합니다.

결과

시스템이 잠금 모드를 종료하고 vCenter Server가 경보를 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 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.

잠금 모드를 사용하도록 설정하면 사용자 권한이 유지됩니다. 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 전환하기 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 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 버전에 따라 다릅니다.

- vSphere 5.0 이하 버전에서는 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 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

심각한 오류가 발생하는 경우 vCenter Server에서 호스트에 액세스할 수 없을 때 `DCUI.Access` 고급 옵션을 사용하여 잠금 모드를 종료할 수 있습니다. vSphere Client에서 호스트에 대한 고급 설정을 편집하여 사용자를 목록에 추가합니다.

참고 DCUI.Access 목록의 사용자는 권한과 관계없이 잠금 모드 설정을 변경할 수 있습니다. 잠금 모드를 변경하는 기능은 호스트 보안에 영향을 줄 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 지정의 내용을 참조하십시오.

절차

1 vSphere Client 인벤토리에서 호스트를 찾습니다.

2 **구성**을 클릭합니다.

3 [시스템] 아래에서 **고급 시스템 설정**을 선택하고 **편집**을 클릭합니다.

4 DCUI로 필터링합니다.

5 **DCUI.Access** 텍스트 상자에 쉼표로 구분된 로컬 ESXi 사용자 이름을 입력합니다.

기본적으로 루트 사용자가 포함됩니다. DCUI.Access 목록에서 루트 사용자를 제거하고 감사 가능성 향상을 위해 명명된 계정을 지정하는 것을 고려해 보십시오.

6 **확인**을 클릭합니다.

잠금 모드 예외 사용자 지정

vSphere Client에서 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 Client 인벤토리에서 호스트를 찾습니다.

2 **구성**을 클릭합니다.

3 시스템 아래에서 **보안 프로파일**을 선택합니다.

4 [잠금 모드] 패널에서 **편집**을 클릭합니다.

5 **예외 사용자**를 클릭하고 **사용자 추가** 아이콘을 클릭하여 예외 사용자를 추가합니다.

VIB를 사용하여 보안 업데이트 수행

ESXCLI를 사용하여 ESXi를 업그레이드하려면 VIB, 이미지 프로파일 및 소프트웨어 디포에 대한 이해가 필요합니다.

ESXi는 실제 소프트웨어가 포함된 일련의 VIB(vSphere 설치 번들)를 설명하는 이미지 프로파일로 구성됩니다. VIB는 Linux 시스템의 RPM 또는 DEB와 거의 유사한 시스템의 구성 요소를 나타내는 서명된 ramdisk입니다. 이미지 프로파일은 VIB의 모음입니다. 소프트웨어 디포는 VIB 및 이미지 프로파일의 모음으로, ESXi 패치 및 디포에는 공통 VIB 집합으로 구성되어 있는 업데이트된 이미지 프로파일이 포함되어 있습니다.

`esxcli software` 명령을 사용하여 독립형 호스트에 ESXi 업데이트를 설치할 수 있습니다. 자세한 내용은 "VMware ESXi 업그레이드" 설명서를 참조하십시오.

참고 일반적으로 vSphere 7.0 이상 환경에서는 ESXi 호스트의 수명 주기 관리에 VMware vSphere® vSphere Lifecycle Manager를 사용합니다.

설치된 모든 VIB와 해당 VIB의 현재 버전 또는 현재 이미지 프로파일을 나열하려면 다음 ESXCLI 명령을 사용하면 됩니다.

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

일반적으로 ESXi를 안전하게 업그레이드하는 개략적인 단계는 다음과 같습니다.

- ESXi 호스트를 유지 보수 모드로 전환
- SSH를 통해 호스트로 전송된 ZIP 파일 또는 URL을 가리키는 `esxcli software profile update` 명령 실행
- ESXi 호스트 다시 시작

VMware는 VIB에 암호화 방식으로 서명하기 때문에 VIB 또는 전체 디포의 보안 전송이 필요하지 않으며 업데이트 프로세스에서 해당 서명이 확인됩니다.

호스트 및 VIB의 수락 수준 관리

VIB의 수락 수준은 해당 VIB의 인증 정도에 따라 달라집니다. 호스트의 수락 수준은 가장 낮은 VIB 수준에 따라 달라집니다. 더 낮은 수준의 VIB를 허용하려는 경우 호스트의 허용 수준을 변경할 수 있습니다. CommunitySupported VIB를 제거하여 호스트 수락 수준을 변경할 수 있습니다.

VIB는 VMware 또는 VMware 파트너의 서명이 포함된 소프트웨어 패키지입니다. 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.

호스트의 수락 수준은 호스트에 추가하려는 VIB의 수락 수준과 같거나 이보다 덜 제한적이어야 합니다. 예를 들어 호스트 수락 수준이 VMwareAccepted인 경우 PartnerSupported 수준으로 VIB를 설치할 수 없습니다. ESXCLI 명령을 사용하여 호스트의 수락 수준을 설정할 수 있습니다. ESXi 호스트의 보안 및 무결성을 보호하려면 운영 시스템에 있는 호스트에 서명되지 않은(CommunitySupported) VIB를 설치하도록 허용하지 마십시오.

ESXi 호스트의 수락 수준은 vSphere Client의 **보안 프로파일**에 표시됩니다.

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. 현재 IOVP(I/O Vendor Program) 프로그램 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 통해 파트너의 지원 조직에 문의하도록 고객에게 안내합니다.

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 통해 파트너의 지원 조직에 문의하도록 고객에게 안내합니다.

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, VMwareAccepted 또는 PartnerSupported로 설정되어 있는지 확인합니다.

```
esxcli software acceptance get
```

2 호스트의 수락 수준이 CommunitySupported인 경우 다음 명령을 실행하여 CommunitySupported 수준에 해당하는 VIB가 있는지 확인합니다.

```
esxcli software vib list
esxcli software vib get -n vibname
```

3 다음 명령을 실행하여 CommunitySupported VIB를 제거합니다.

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

4 다음 방법 중 하나를 사용하여 호스트의 수락 수준을 변경합니다.

옵션	설명
CLI 명령	`esxcli software acceptance set --level level` `level` 매개 변수는 필수이며 설정할 허용 수준을 지정합니다. **VMwareCertified**, **VMwareAccepted**, **PartnerSupported** 또는 **CommunitySupported** 중 하나여야 합니다. 자세한 내용은 "ESXCLI 참조" 의 내용을 참조하십시오.
vSphere Client	a 인벤토리에서 호스트를 선택합니다. b **구성**을 클릭합니다. c 시스템 아래에서 **보안 프로파일**을 선택합니다. d 호스트 이미지 프로파일 수락 수준에 대해 **편집**을 클릭하고 수락 수준을 선택합니다.

결과

새 수락 수준이 적용됩니다.

참고 ESXi는 수락 수준에 의해 관리되는 VIB에 대한 무결성 검사를 수행합니다. `VMkernel.Boot.execInstalledOnly` 설정을 사용하여 ESXi가 호스트에 설치된 유효한 VIB에서 생성된 바이너리만 실행하도록 지시할 수 있습니다. 이 설정은 보안 부팅과 결합되어 ESXi 호스트에서 실행되는 모든 단일 프로세스가 서명, 허용 및 예상되도록 합니다. 기본적으로 `VMkernel.Boot.execInstalledOnly` 설정은 vSphere 7에서의 파트너 호환성을 위해 사용되지 않도록 설정됩니다. 가능한 경우 이 설정을 사용하도록 설정하면 보안이 향상됩니다. ESXi의 고급 옵션 구성에 대한 자세한 내용은 https://kb.vmware.com/kb/1038578에서 VMware 기술 자료 문서를 참조하십시오.

ESXi 호스트에 대한 권한 할당

일반적으로 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 Client를 통해 관리 작업을 수행합니다.

vCenter Server 개체 계층에서 ESXi 호스트 개체를 선택하고 제한된 수의 사용자에게 관리자 역할을 할당할 수 있습니다. 그런 다음 해당 사용자가 ESXi 호스트에서 직접 관리를 수행할 수 있습니다. 역할을 사용하여 권한 할당의 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

로컬 사용자를 추가하고 VMware Host Client의 [관리] 탭에서 사용자 지정 역할을 정의할 수 있습니다. "vSphere 단일 호스트 관리 - VMware Host Client" 설명서를 참조하십시오.

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 역할은 기본 역할입니다. 기본 역할은 재정의할 수 있습니다.

ESXi 호스트에 직접 연결된 VMware Host Client를 사용하여 로컬 사용자 및 그룹을 관리하고 로컬 사용자 지정 역할을 ESXi 호스트에 추가할 수 있습니다. "vSphere 단일 호스트 관리 - VMware Host Client" 설명서를 참조하십시오.

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. ESXi 사용자에게 역할을 할당하는 경우 vCenter Server 사용자에는 동일한 역할이 할당되지 않습니다.

미리 정의된 권한

환경에 vCenter Server 시스템이 포함되지 않는 경우 다음 사용자가 미리 정의됩니다.

루트 사용자

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.

루트 사용자 권한을 할당하면 이 이름이 이미 알려져 있으므로 ESXi 호스트에 더 쉽게 침입할 수 있습니다. 또한 공통 루트 계정을 가지면 사용자에 대한 작업을 일치시키기도 더 어려워집니다.

더 나은 감사가 이루어지도록 하려면 관리자 권한을 가진 개별 계정을 생성하십시오. 루트 계정에 매우 복잡한 암호를 설정하고 vCenter Server에 호스트를 추가하는 등의 경우에 사용하기 위한 루트 계정의 사용을 제한합니다. 루트 계정은 제거하지 마십시오. ESXi 호스트에 대한 사용 권한을 사용자에게 할당하는 데 대한 자세한 내용은 "vSphere 단일 호스트 관리 - VMware Host Client" 설명서를 참조하십시오.

가장 좋은 방법은 ESXi 호스트에서 관리자 역할이 있는 계정이 명명된 계정이 있는 특정 사용자에게 할당되었는지 확인하는 것입니다. ESXi Active Directory 기능을 사용하여 Active Directory 자격 증명을 관리합니다.

중요 루트 사용자의 액세스 권한을 제거할 수 있습니다. 하지만 먼저 루트 수준에서 다른 권한을 생성하여 관리자 역할에 다른 사용자를 할당해야 합니다.

vpxuser 사용자

vCenter Server에서는 호스트의 작업을 관리할 때 vpxuser 권한을 사용합니다.

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. 관리자 권한을 가진 사용자만 호스트에서 직접 이러한 작업을 수행할 수 있습니다.

참고 Active Directory를 사용하여 vpxuser를 관리할 수는 없습니다.

경고 어떠한 방법으로든 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

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.

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 사용의 내용을 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 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 동기화의 내용을 참조하십시오.

2 호스트에 대해 구성한 DNS 서버에서 Active Directory 컨트롤러의 호스트 이름을 확인할 수 있는지 확인합니다.

  a vSphere Client 인벤토리에서 호스트를 찾습니다.

  b **구성**을 클릭합니다.

  c [네트워킹]에서 **TCP/IP 구성**을 클릭합니다.

  d [TCP/IP 스택: 기본값]에서 **DNS**를 클릭하고 호스트의 호스트 이름 및 DNS 서버 정보가 정확한지 확인합니다.

다음에 수행할 작업

호스트를 디렉토리 서비스 도메인에 가입시킵니다. 디렉토리 서비스 도메인에 호스트 추가의 내용을 참조하십시오. Auto Deploy를 사용하여 프로비저닝된 호스트의 경우 vSphere Authentication Proxy를 설정합니다. vSphere Authentication Proxy 사용의 내용을 참조하십시오. 가입된 Active Directory 도메인의 사용자 및 그룹이 vCenter Server 구성 요소에 액세스하기 위한 사용 권한을 구성할 수 있습니다. 사용 권한 관리에 대한 자세한 내용은 인벤토리 개체에 사용 권한 추가 의 내용을 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 사용의 내용을 참조하십시오.

절차

1 vSphere Client 인벤토리에서 호스트를 찾습니다.

2 **구성**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.

다음에 수행할 작업

가입된 Active Directory 도메인의 사용자 및 그룹이 vCenter Server 구성 요소에 액세스하기 위한 사용 권한을 구성할 수 있습니다. 사용 권한 관리에 대한 자세한 내용은 인벤토리 개체에 사용 권한 추가 의 내용을 참조하십시오.

디렉토리 서비스 설정 보기

호스트가 사용자를 인증하는 데 사용하는 디렉토리 서버(있는 경우)의 유형과 디렉토리 서버 설정을 볼 수 있습니다.

절차

1 vSphere Client 인벤토리에서 호스트를 찾습니다.

2 **구성**을 클릭합니다.

3 시스템 아래에서 **인증 서비스**를 선택합니다.

[인증 서비스] 페이지에 디렉토리 서비스 및 도메인 설정이 표시됩니다.

다음에 수행할 작업

가입된 Active Directory 도메인의 사용자 및 그룹이 vCenter Server 구성 요소에 액세스하기 위한 사용 권한을 구성할 수 있습니다. 사용 권한 관리에 대한 자세한 내용은 인벤토리 개체에 사용 권한 추가 의 내용을 참조하십시오.

vSphere Authentication Proxy 사용

명시적으로 Active Directory 도메인에 ESXi 호스트를 추가하는 대신 vSphere Authentication Proxy를 사용하여 Active Directory 도메인에 호스트를 추가할 수 있습니다.

Active Directory 서버의 도메인 이름과 vSphere Authentication Proxy의 IP 주소만 지정하여 호스트를 설정하면 됩니다. vSphere Authentication Proxy가 사용하도록 설정된 경우 이를 통해 Auto Deploy를 사용하여 프로비저닝되는 호스트가 Active Directory 도메인에 자동으로 추가됩니다. 또한 Auto Deploy를 사용하여 프로비저닝되지 않는 호스트에도 vSphere Authentication Proxy를 사용할 수 있습니다.

vSphere Authentication Proxy에서 사용하는 TCP 포트에 대한 자세한 내용은 vCenter Server의 필수 포트의 내용을 참조하십시오.

Auto Deploy

Auto Deploy를 사용하여 호스트를 프로비저닝하는 경우 Authentication Proxy를 가리키는 참조 호스트를 설정할 수 있습니다. 그런 다음 Auto Deploy를 사용하여 프로비저닝된 모든 ESXi 호스트에 참조 호스트의 프로파일을 적용하는 규칙을 설정합니다. vSphere Authentication Proxy는 Auto Deploy가 PXE를 사용하여 프로비저닝하는 모든 호스트의 IP 주소를 해당 액세스 제어 목록에 저장합니다. 호스트가 부팅될 때 호스트에서 vSphere Authentication Proxy에 연결하며 vSphere Authentication Proxy가 해당 액세스 제어 목록에 이미 있는 호스트를 Active Directory 도메인에 가입시킵니다.

VMCA 또는 타사 인증서로 프로비저닝된 인증서를 사용하는 환경에서 vSphere Authentication Proxy를 사용하더라도 Auto Deploy를 사용한 사용자 지정 인증서 사용에 대한 지침을 따르는 한 프로세스가 원활하게 작동합니다.

Auto Deploy와 함께 사용자 지정 인증서 사용의 내용을 참조하십시오.

다른 ESXi 호스트

다른 호스트가 Active Directory 자격 증명을 사용하지 않고 도메인에 가입할 수 있도록 하려는 경우 해당 호스트가 vSphere Authentication Proxy를 사용하도록 설정할 수 있습니다. 즉, 해당 호스트에 Active Directory 자격 증명을 전송할 필요가 없고 호스트 프로파일에 Active Directory 자격 증명이 저장되지 않습니다.

이 경우 호스트의 IP 주소가 vSphere Authentication Proxy 액세스 제어 목록에 추가되고 vSphere Authentication Proxy에서 기본적으로 IP 주소를 기반으로 호스트를 인증합니다. 클라이언트 인증을 사용하도록 설정하여 vSphere Authentication Proxy에서 호스트의 인증서를 확인하게 할 수 있습니다.

참고 IPv6만 지원하는 환경에서는 vSphere Authentication Proxy를 사용할 수 없습니다.

vSphere Authentication Proxy를 사용하도록 설정

각 vCenter Server 시스템에서 vSphere Authentication Proxy 서비스를 사용할 수 있습니다. 기본적으로 이 서비스는 실행되지 않습니다. 환경에서 vSphere Authentication Proxy를 사용하려는 경우 vCenter Server 관리 인터페이스 또는 명령줄을 사용하여 서비스를 시작할 수 있습니다.

vSphere Authentication Proxy 서비스는 vCenter Server와의 통신을 위해 IPv4 주소에 바인딩되지만 IPv6은 지원하지 않습니다. vCenter Server 인스턴스는 IPv4 전용 또는 IPv4/IPv6 혼합 모드 네트워크 환경의 호스트 시스템에 있을 수 있습니다. 하지만 vSphere Authentication Proxy의 주소를 지정하는 경우 IPv4 주소를 지정해야 합니다.

사전 요구 사항

vCenter Server 6.5 이상을 사용하는지 확인합니다. 이전 버전의 vSphere에서는 vSphere Authentication Proxy가 별도로 설치됩니다. 자세한 지침은 이전 버전 제품에 대한 설명서를 참조하십시오.

절차

1 VMware vSphere Authentication Proxy 서비스를 시작합니다.

옵션	설명
vCenter Server 관리 인터페이스	a 웹 브라우저에서 vCenter Server 관리 인터페이스 https://*vcenter-IP-address-or-FQDN*:5480으로 이동합니다. b 루트로 로그인합니다. 기본 루트 암호는 vCenter Server를 배포하는 중에 설정하는 암호입니다. c **서비스**를 클릭하고 **VMware vSphere Authentication Proxy** 서비스를 클릭합니다. d **시작**을 클릭합니다. e (선택 사항) 서비스가 시작된 후에 **시작 유형 설정**을 클릭하고 **자동**을 클릭하여 자동으로 시작되도록 설정합니다.
CLI	`service-control --start vmcam`

2 서비스가 성공적으로 시작되었는지 확인합니다.

결과

이제 vSphere Authentication Proxy 도메인을 설정할 수 있습니다. 그 후에는 vSphere Authentication Proxy가 Auto Deploy를 사용하여 프로비저닝되는 모든 호스트를 처리하며 vSphere Authentication Proxy에 호스트를 명시적으로 추가할 수 있습니다.

vSphere Client를 사용하여 vSphere Authentication Proxy에 도메인 추가

vSphere Client 또는 `camconfig` 명령을 사용하여 vSphere Authentication Proxy에 도메인을 추가할 수 있습니다.

프록시를 사용하도록 설정한 후에만 vSphere Authentication Proxy에 도메인을 추가할 수 있습니다. 도메인을 추가한 후 vSphere Authentication Proxy는 사용자가 Auto Deploy를 통해 프로비저닝한 모든 호스트를 해당 도메인에 추가합니다. 기타 호스트의 경우에도 이러한 호스트에 도메인 권한을 부여하지 않으려면 vSphere Authentication Proxy를 사용할 수 있습니다.

절차

1 vSphere Client를 사용하여 vCenter Server 시스템에 연결합니다.

2 vCenter Server를 선택하고 **구성**을 클릭합니다.

3 **인증 프록시**를 클릭하고 **편집**을 클릭합니다.

4 vSphere Authentication Proxy가 호스트를 추가할 도메인의 이름과 도메인에 호스트를 추가할 수 있는 Active Directory 권한을 가진 사용자의 이름과 암호를 입력합니다.

5 **저장**을 클릭합니다.

camconfig 명령을 사용하여 vSphere Authentication Proxy에 도메인 추가

`camconfig` 명령을 사용하여 vSphere Authentication Proxy에 도메인을 추가할 수 있습니다.

프록시를 사용하도록 설정한 후에만 vSphere Authentication Proxy에 도메인을 추가할 수 있습니다. 도메인을 추가한 후 vSphere Authentication Proxy는 사용자가 Auto Deploy를 통해 프로비저닝한 모든 호스트를 해당 도메인에 추가합니다. 기타 호스트의 경우에도 이러한 호스트에 도메인 권한을 부여하지 않으려면 vSphere Authentication Proxy를 사용할 수 있습니다.

절차

1 관리자 권한을 가진 사용자로 vCenter Server 시스템에 로그인합니다.

2 Bash 셸에 액세스할 수 있도록 설정하는 명령을 실행합니다.

```
shell
```

3 **camconfig** 스크립트가 있는 `/usr/lib/vmware-vmcam/bin/` 디렉토리로 이동합니다.

4 도메인 및 사용자 Active Directory 자격 증명을 Authentication Proxy 구성에 추가하려면 다음 명령을 실행합니다.

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

암호를 묻는 메시지가 나타납니다.

vSphere Authentication Proxy에 사용자 이름과 암호가 캐시됩니다. 필요에 따라 사용자를 제거하고 다시 생성할 수 있습니다. 도메인은 DNS를 통해 연결할 수 있어야 하지만 vCenter Single Sign-On ID 소스일 필요는 없습니다.

vSphere Authentication Proxy는 *사용자*에 의해 지정된 사용자 이름을 사용하여 Active Directory에 ESXi 호스트에 대한 계정을 생성합니다. 사용자는 호스트를 추가하려는 Active Directory 도메인에 계정을 생성할 수 있는 권한이 있어야 합니다. 이 정보를 작성하는 시점에서 계정 생성 권한에 대한 배경 정보는 Microsoft 기술 자료 문서 932455에 나와 있습니다.

5 이후에 vSphere Authentication Proxy에서 도메인 및 사용자 정보를 제거하려면 다음 명령을 실행합니다.

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

vSphere Authentication Proxy를 사용하여 도메인에 호스트 추가

Auto Deploy 서버는 프로비저닝하는 모든 호스트를 vSphere Authentication Proxy에 추가하며, vSphere Authentication Proxy는 그러한 호스트를 도메인에 추가합니다. vSphere Authentication Proxy를 사용하여 도메인에 다른 호스트를 추가하려는 경우 해당 호스트를 vSphere Authentication Proxy에 명시적으로 추가할 수 있습니다. 그 후에 vSphere Authentication Proxy 서버는 해당 호스트를 도메인에 추가합니다. 따라서 사용자 제공 자격 증명을 더 이상 vCenter Server 시스템에 전송할 필요가 없습니다.

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

- ESXi 호스트에서 VMCA 서명된 인증서를 사용하고 있는 경우 호스트가 vCenter Server에 추가되었는지 확인합니다. 그렇지 않은 경우 Authentication Proxy 서비스는 ESXi 호스트를 신뢰할 수 없습니다.
- ESXi 호스트에서 루트 CA 서명 인증서를 사용하는 경우 적절한 루트 CA 서명 인증서가 vCenter Server 시스템에 추가되었는지 확인합니다. ESXi 호스트에 대한 인증서 관리의 내용을 참조하십시오.

절차

1 vSphere Client 인벤토리에서 호스트를 찾습니다.

2 **구성**을 클릭합니다.

3 **시스템** 아래에서 **인증 서비스**를 선택합니다.

4 **도메인 가입**을 클릭합니다.

5 도메인을 입력합니다.

name.tld 형식(예: **mydomain.com**) 또는 **name.tld/container/path** 형식(예: **mydomain.com/organizational_unit1/organizational_unit2**)을 사용합니다.

6 **프록시 서버 사용**을 선택합니다.

7 Authentication Proxy 서버의 IP 주소를 입력합니다. 이는 항상 vCenter Server 시스템의 IP 주소와 동일합니다.

8 **확인**을 클릭합니다.

vSphere Authentication Proxy에 대한 클라이언트 인증을 사용하도록 설정

기본적으로 vSphere Authentication Proxy는 해당 액세스 제어 목록에 IP 주소가 있는 호스트를 모두 추가합니다. 보안 강화를 위해 클라이언트 인증을 사용하도록 설정할 수 있습니다. 클라이언트 인증을 사용하도록 설정된 경우 vSphere Authentication Proxy는 호스트의 인증서도 확인합니다.

사전 요구 사항

- vCenter Server 시스템이 호스트를 신뢰하는지 확인합니다. 기본적으로 vCenter Server에 호스트를 추가하면 vCenter Server의 신뢰할 수 있는 루트 CA에서 서명한 인증서가 호스트에 할당됩니다. vSphere Authentication Proxy는 vCenter Server의 신뢰할 수 있는 루트 CA를 신뢰합니다.
- 환경에서 ESXi 인증서를 교체하려는 경우 vSphere Authentication Proxy를 사용하도록 설정하기 전에 교체를 수행하십시오. ESXi 호스트의 인증서가 호스트 등록 인증서와 일치해야 합니다.

절차

1 관리자 권한을 가진 사용자로 vCenter Server 시스템에 로그인합니다.

2 Bash 셸에 액세스할 수 있도록 설정하는 명령을 실행합니다.

```
shell
```

3 **camconfig** 스크립트가 있는 `/usr/lib/vmware-vmcam/bin/` 디렉토리로 이동합니다.

4 다음 명령을 실행하여 클라이언트 인증을 사용하도록 설정합니다.

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

이후부터 vSphere Authentication Proxy는 추가된 각 호스트의 인증서를 확인합니다.

5 나중에 다시 클라이언트 인증을 사용하지 않도록 설정하려면 다음 명령을 실행합니다.

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

ESXi 호스트에 vSphere Authentication Proxy 인증서 가져오기

기본적으로 ESXi 호스트는 vSphere Authentication Proxy 인증서를 명시적으로 확인해야 합니다. vSphere Auto Deploy를 사용하는 경우 Auto Deploy 서비스에서 프로비저닝하는 호스트에 인증서를 추가합니다. 다른 호스트의 경우 명시적으로 인증서를 추가해야 합니다.

사전 요구 사항

- ESXi 호스트에 액세스할 수 있는 데이터스토어에 vSphere Authentication Proxy 인증서를 업로드합니다. WinSCP와 같은 SFTP 애플리케이션을 사용하여 다음 위치의 vCenter Server 호스트에서 인증서를 다운로드할 수 있습니다.

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

- `UserVars.ActiveDirectoryVerifyCAMCertificate` ESXi 고급 설정이 1(기본값)로 설정되어 있는지 확인합니다.

절차

1 ESXi 호스트를 선택하고 **구성**을 클릭합니다.

2 **시스템** 아래에서 **인증 서비스**를 선택합니다.

3 **인증서 가져오기**를 클릭합니다.

4 `[datastore]/path/certname.crt` 형식으로 인증서 파일 경로를 입력하고 **확인**을 클릭합니다.

vSphere Authentication Proxy용 새 인증서 생성

VMCA에서 프로비저닝되는 새 인증서 또는 VMCA를 하위 인증서로 포함하는 새 인증서를 생성할 수 있습니다.

타사 또는 엔터프라이즈 CA가 서명한 사용자 지정 인증서를 사용하려는 경우 사용자 지정 인증서를 사용하도록 vSphere Authentication Proxy 설정 항목을 참조하십시오.

사전 요구 사항

vSphere Authentication Proxy가 실행되는 시스템에 대한 루트 또는 관리자 권한이 있어야 합니다.

절차

1 `certool.cfg`의 복사본을 생성합니다.

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

2 다음 예와 같이 조직에 대한 몇 가지 정보를 포함하여 복사본을 편집합니다.

```
Country = IE
Name = vmcam
Organization = VMware
OrgUnit = vTSU
State = Cork
Locality = Cork
Hostname = test-cam-1.test1.vmware.com
```

3 `/var/lib/vmware/vmcam/ssl/`에 새 개인 키를 생성합니다.

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

*localhost*에 대해 vCenter Server의 FQDN을 제공합니다.

4 1단계와 2단계에서 생성한 키와 `vmcam.cfg` 파일을 사용하여 `/var/lib/vmware/vmcam/ssl/`에 새 인증서를 생성합니다.

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

*localhost*에 대해 vCenter Server의 FQDN을 제공합니다.

사용자 지정 인증서를 사용하도록 vSphere Authentication Proxy 설정

vSphere Authentication Proxy에서 사용자 지정 인증서를 사용하려면 몇 가지 단계를 수행해야 합니다. 먼저 CSR을 생성하고 CA에 보내 서명을 받습니다. 그런 다음 서명된 인증서와 키 파일을 vSphere Authentication Proxy에서 액세스할 수 있는 위치에 배치합니다.

기본적으로 vSphere Authentication Proxy는 처음 부팅 시 CSR을 생성하고 해당 CSR에 서명하도록 VMCA에 요청합니다. vSphere Authentication Proxy는 해당 인증서를 사용하여 vCenter Server에 등록합니다. 사용자 지정 인증서를 vCenter Server에 추가하면 이러한 인증서를 환경에서 사용할 수 있습니다.

절차

1 vSphere Authentication Proxy용 CSR 생성

a 다음 예와 같이 구성 파일 `/var/lib/vmware/vmcam/ssl/vmcam.cfg`를 생성합니다.

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

b `openssl`을 실행하여 CSR 파일과 키 파일을 생성하고 구성 파일에 전달합니다.

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

2 다음 위치에 저장된 `rui.crt` 인증서와 `rui.key` 파일을 백업합니다.

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

3 vSphere Authentication Proxy 등록 취소

a `camregister` 스크립트가 있는 `/usr/lib/vmware-vmcam/bin` 디렉토리로 이동합니다.

b 다음 명령을 실행합니다.

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

*user*는 vCenter Server에 대한 관리자 사용 권한이 있는 vCenter Single Sign-On 사용자여야 합니다.

4 vSphere Authentication Proxy 서비스를 중지합니다.

도구	단계
vCenter Server 구성 관리 인터페이스	a 웹 브라우저에서 vCenter Server 구성 관리 인터페이스 https://*vcenter-IP-address-or-FQDN*:5480으로 이동합니다. b 루트로 로그인합니다. 기본 루트 암호는 vCenter Server를 배포하는 중에 설정하는 암호입니다. c **서비스**를 클릭하고 **VMware vSphere Authentication Proxy 서비스**를 클릭합니다. d **중지**를 클릭합니다.
CLI	`service-control --stop vmcam`

5 기존 `rui.crt` 인증서와 `rui.key` 파일을 CA에서 받은 파일로 교체합니다.

6 vSphere Authentication Proxy 서비스를 다시 시작합니다.

7 새 인증서와 키를 사용해 vSphere Authentication Proxy를 vCenter Server에 명시적으로 재등록합니다.

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

ESXi에 대한 스마트 카드 인증 구성

사용자 이름 및 암호를 지정하는 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 사용되도록 설정된 경우 DCUI는 사용자 이름 및 암호에 대한 기본 프롬프트 대신 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 의 내용을 참조하십시오.
- vSphere Client를 사용하여 루트 인증서를 추가합니다. ESXi 호스트에 대한 인증서 관리의 내용을 참조하십시오.

절차

1 vSphere Client 인벤토리에서 호스트를 찾습니다.

2 **구성**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.

인증서는 PEM 형식이어야 합니다.

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 Client 인벤토리에서 호스트를 찾습니다.

2 **구성**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 문제 발생 시 사용자 이름과 암호를 사용하여 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. 이 경우 로컬 ESXi 관리자 사용자 자격 증명을 사용하여 ESXi DCUI에 로그인할 수 있습니다. 로그인한 후에는 진단 또는 기타 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 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 지정의 내용을 참조하십시오.

엄격 잠금 모드에서는 DCUI 서비스가 중지됩니다. 따라서 스마트 카드 인증을 사용하여 호스트에 액세스할 수 없습니다.

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 모드와 상관이 없습니다. 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.

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.

- ESXi Shell에 대한 액세스를 사용하도록 설정

  ESXi Shell 및 SSH 인터페이스는 기본적으로 사용하지 않도록 설정됩니다. 문제 해결 또는 지원 작업을 수행하지 않는 한 이러한 인터페이스를 사용하지 않도록 설정해 두어야 합니다. 일상적인 작업의 경우 vSphere Client를 사용합니다. 여기서 작업은 역할 기반 액세스 제어 및 최신 액세스 제어 방법을 따릅니다.

- Direct Console User Interface를 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 Client, ESXCLI 또는 VMware PowerCLI를 사용하여 ESXi 구성 작업을 수행합니다. 문제 해결을 위해서만 ESXi Shell(이전의 Tech Support Mode 또는 TSM)에 로그인합니다.

ESXi Shell에 대한 액세스를 사용하도록 설정

ESXi Shell 및 SSH 인터페이스는 기본적으로 사용하지 않도록 설정됩니다. 문제 해결 또는 지원 작업을 수행하지 않는 한 이러한 인터페이스를 사용하지 않도록 설정해 두어야 합니다. 일상적인 작업의 경우

vSphere Client를 사용합니다. 여기서 작업은 역할 기반 액세스 제어 및 최신 액세스 제어 방법을 따릅니다.

참고 vSphere Client, 원격 명령줄 도구(ESXCLI 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 키의 내용을 참조하십시오.

절차

1 인벤토리에서 호스트를 찾습니다.

2 **구성**을 클릭한 다음 [시스템]에서 **서비스**를 클릭합니다.

3 ESXi, SSH 또는 직접 콘솔 UI 서비스를 관리합니다.

   a [서비스] 창에서 서비스를 선택합니다.

   b **시작 정책 편집**을 클릭하고 시작 정책으로 **수동으로 시작 및 중지**를 선택합니다.

   c 서비스를 사용하도록 설정하려면 **시작**을 클릭합니다.

   수동으로 시작 및 중지를 선택하면 호스트를 재부팅할 때 서비스가 시작되지 않습니다. 호스트를 재부팅할 때 서비스가 시작되도록 하려면 **호스트와 함께 시작 및 중지**를 선택합니다.

다음에 수행할 작업

ESXi Shell에 대한 가용성 및 유휴 시간 초과를 설정합니다. ESXi Shell 가용성에 대한 시간 초과 설정 생성 및 유휴 ESXi Shell 세션에 대한 시간 초과 설정 생성 항목을 참조하십시오.

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 vSphere Client 인벤토리에서 호스트를 찾습니다.

2 **구성**을 클릭합니다.

3 시스템 아래에서 **고급 시스템 설정**을 선택합니다.

4 **편집**을 클릭하고 `UserVars.ESXiShellTimeOut`을 선택합니다.

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 경과될 때 로그인되어 있으면 세션이 지속됩니다. 하지만 사용자가 로그아웃했거나 세션이 종료되면 사용자는 로그인할 수 없습니다.

유휴 ESXi Shell 세션에 대한 시간 초과 설정 생성

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 늘어납니다. 유휴 세션에 대한 시간 초과를 설정하여 이 문제를 방지합니다.

유휴 시간 초과는 사용자가 유휴 대화형 세션에서 로그아웃할 때까지의 최대 대기 시간입니다. DCUI(Direct Console Interface) 또는 vSphere Client에서 로컬 및 원격(SSH) 세션 모두에 대한 시간을 제어할 수 있습니다.

절차

1 vSphere Client 인벤토리에서 호스트를 찾습니다.

2 **구성**을 클릭합니다.

3 시스템 아래에서 **고급 시스템 설정**을 선택합니다.

4 **편집**을 클릭하고 `UserVars.ESXiShellInteractiveTimeOut`을 선택하고 시간 초과 설정을 입력합니다.

   0 값은 유휴 시간을 사용하지 않도록 설정합니다.

5 시간 초과를 적용하려면 ESXi Shell 서비스 및 SSH 서비스를 다시 시작합니다.

결과

세션이 유휴 상태일 때 시간 초과 기간이 경과하면 사용자가 로그아웃됩니다.

Direct Console User Interface를 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.

DCUI(Direct Console User Interface)를 사용하여 ESXi Shell에 대한 로컬 및 원격 액세스가 가능하도록 설정할 수 있습니다. Direct Console User Interface는 호스트에 연결된 물리적 콘솔에서 액세스합니다. 호스트가 재부팅되고 ESXi를 로드한 후에 F2 키를 눌러 DCUI에 로그인합니다. ESXi를 설치할 때 생성한 자격 증명을 입력합니다.

참고 Direct Console User Interface, vSphere Client, ESXCLI 또는 다른 관리자 도구를 사용하여 호스트에 변경한 내용은 매시간 또는 정상 종료 시 영구 스토리지에 커밋됩니다. 변경 내용이 커밋되기 전에 호스트에 장애가 발생하면 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 Shell을 사용하도록 설정합니다.
- 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 유휴 시간 초과를 설정합니다. ESXi Shell에 대한 가용성 시간 초과 또는 유휴 시간 초과 설정의 내용을 참조하십시오.

ESXi Shell에 대한 가용성 시간 초과 또는 유휴 시간 초과 설정

ESXi Shell은 기본적으로 사용하지 않도록 설정되어 있습니다. 셸을 사용하도록 설정할 때 보안을 향상시키기 위해 가용성 시간 초과, 유휴 시간 초과 또는 둘 다를 설정할 수 있습니다.

두 가지 유형의 시간 초과는 서로 다른 상황에 적용됩니다.

유휴 시간 제한

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 이런 상황을 방지할 수 있습니다.

가용성 시간 제한

가용성 시간 초과 설정은 처음 셸을 사용하도록 설정한 후 로그인할 때까지의 최대 대기 시간을 지정합니다. 더 오래,대기하면 서비스가 사용되지 않도록 설정되고 ESXi Shell에 로그인할 수 없습니다.

사전 요구 사항

ESXi Shell을 사용하도록 설정합니다. Direct Console User Interface를 사용하여 ESXi Shell에 액세스할 수 있도록 설정의 내용을 참조하십시오.

절차

1 ESXi Shell에 로그인합니다.

2 문제 해결 모드 옵션 메뉴에서 **ESXi Shell 및 SSH 시간 초과 수정**을 선택하고 Enter 키를 누릅니다.

3 유휴 시간 초과(초) 또는 가용성 시간 초과를 입력합니다.

시간 초과를 적용하려면 SSH 서비스 및 ESXi Shell 서비스를 다시 시작해야 합니다.

4 Enter 키를 누르고 Direct Console User Interface의 기본 메뉴로 돌아갈 때까지 Esc 키를 누릅니다.

5 **확인**을 클릭합니다.

결과

- 유휴 시간 초과가 설정된 경우 지정된 시간 동안 세션이 유휴 상태이면 사용자가 로그아웃됩니다.
- 가용성 시간 초과가 설정된 경우 시간 초과 기간이 경과하기 전에 로그인하지 않으면 로그인이 다시 사용되지 않도록 설정됩니다.

문제 해결을 위해 ESXi Shell에 로그인

vSphere Client, ESXCLI 또는 VMware 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+F1을 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 호스트를 위한 UEFI 보안 부팅

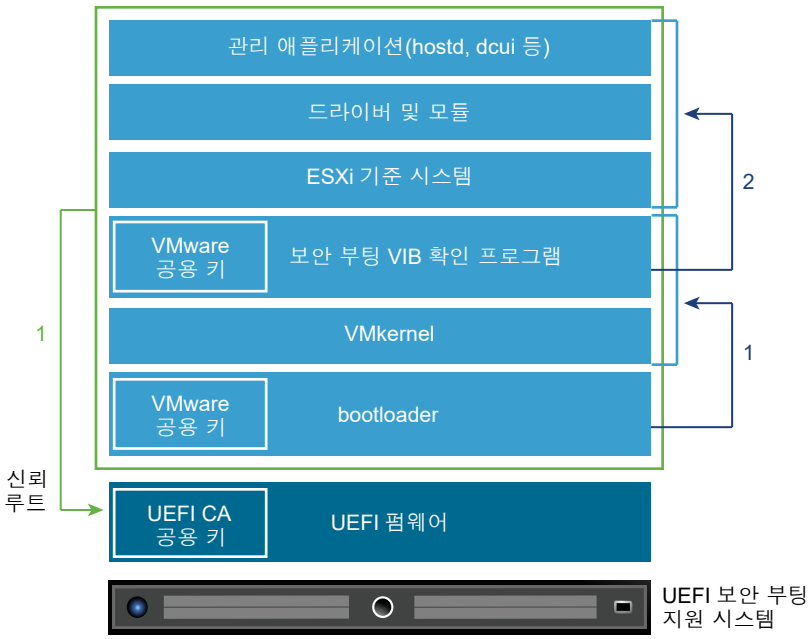
보안 부팅은 UEFI 펌웨어 표준의 일부입니다. 보안 부팅을 사용하도록 설정하는 경우 운영 체제 부팅 로더의 서명이 암호화된 경우가 아니면 시스템에서 모든 UEFI 드라이버 또는 애플리케이션의 로드를 거부합니다. vSphere 6.5부터 ESXi는 보안 부팅을 지원합니다(하드웨어에서 보안 부팅을 사용하도록 설정한 경우).

ESXi가 UEFI 보안 부팅을 사용하는 방법

ESXi 버전 6.5 이상에서는 부팅 스택의 각 수준에서 UEFI 보안 부팅을 지원합니다.

참고 업그레이드된 호스트에서 UEFI 보안 부팅을 사용하기 전에 업그레이드된 ESXi 호스트에서 보안 부팅 유효성 검사 스크립트 실행의 다음 지침에 따라 호환성을 확인하십시오.

그림 3-1. UEFI 보안 부팅



보안 부팅을 사용하도록 설정하는 경우 부팅 순서는 다음과 같이 진행됩니다.

1 vSphere 6.5부터 ESXi 부팅 로더에는 VMware 공용 키가 포함됩니다. 부팅 로더는 이 키를 사용하여 커널의 서명 그리고 보안 부팅 VIB 확인 프로그램이 포함된 시스템의 작은 하위 집합을 확인합니다.

2 VIB 확인 프로그램은 시스템에 설치된 모든 VIB 패키지를 확인합니다.

이때, UEFI 펌웨어의 일부인 인증서의 신뢰 루트와 함께 전체 시스템이 부팅됩니다.

참고 vSphere 7.0 업데이트 2 이상을 설치하거나 업그레이드하고 ESXi 호스트에 TPM이 있는 경우 TPM은 UEFI 보안 부팅의 PCR 값을 기반으로 TPM 정책을 사용하여 중요 정보를 봉인합니다. 이 값은 정책이 true로 충족되는 경우 후속 재부팅 중에 로드됩니다. vSphere 7.0 업데이트 2 이상에서 UEFI 보안 부팅을 사용하거나 사용하지 않도록 설정하려면 보안 ESXi 구성에 대한 보안 부팅 적용 사용 또는 사용 안 함의 내용을 참조하십시오.

UEFI 보안 부팅 문제 해결

보안 부팅이 부팅 순서의 임의 수준에서 실패하는 경우 오류가 발생합니다.

오류 메시지는 하드웨어 벤더 그리고 확인이 실패한 수준에 따라 달라집니다.

- 서명되지 않았거나 임의로 변경된 부팅 로더를 사용하여 부팅을 시도하는 경우 부팅 순서 중에 오류가 발생합니다. 정확한 메시지 내용은 하드웨어 벤더에 따라 다릅니다. 다음과 같은 오류가 표시될 수 있습니다(내용이 다를 수도 있음).

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

- 커널이 임의로 변경된 경우 다음과 같은 오류가 발생할 수 있습니다.

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

- 패키지(VIB 또는 드라이버)가 임의로 변경된 경우 보라색 화면에 다음과 같은 메시지가 표시됩니다.

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

보안 부팅 관련 문제를 해결하려면 다음 단계를 수행합니다.

1 보안 부팅이 사용되지 않도록 설정하고 호스트를 재부팅합니다.

2 보안 부팅 확인 스크립트를 실행합니다(업그레이드된 ESXi 호스트에서 보안 부팅 유효성 검사 스크립트 실행 참조).

3 `/var/log/esxupdate.log` 파일의 정보를 검토합니다.

업그레이드된 ESXi 호스트에서 보안 부팅 유효성 검사 스크립트 실행

UEFI 보안 부팅을 지원하지 않는 이전 버전의 ESXi에서 ESXi 호스트를 업그레이드한 후 보안 부팅을 사용하도록 설정할 수도 있습니다. 보안 부팅을 사용할 수 있는지 여부는 업그레이드를 수행한 방법과 업그레이드를 통해 기존의 모든 VIB를 대체했는지, 아니면 일부 VIB를 그대로 유지했는지에 따라 달라집니다. 업그레이드를 수행한 후 유효성 검사 스크립트를 실행하여 업그레이드된 설치에서 보안 부팅이 지원되는지 여부를 확인할 수 있습니다.

보안 부팅이 성공하려면 설치된 모든 VIB의 서명을 시스템에서 사용할 수 있어야 합니다. 이전 버전의 ESXi에서는 VIB를 설치할 때 서명이 저장되지 않습니다.

- ESXCLI 명령을 사용하여 업그레이드하는 경우 이전 버전의 ESXi에서 새 VIB 설치가 수행되기 때문에 서명이 저장되지 않고 보안 부팅이 불가능합니다.
- ISO를 사용하여 업그레이드하면 새 VIB에 서명이 저장됩니다. ISO를 사용하는 vSphere Lifecycle Manager 업그레이드에서도 마찬가지입니다.
- 이전 VIB가 시스템에 남아 있는 경우 해당 VIB의 서명을 사용할 수 없으며 보안 부팅도 불가능합니다.
  - 시스템에서 타사 드라이버를 사용하고 VMware 업그레이드에 드라이버 VIB의 새 버전이 포함되지 않은 경우 이전 VIB가 업그레이드 후 시스템에 남아 있습니다.
  - 드물지만 경우에 따라 VMware에서 특정 VIB의 진행 중인 개발을 중단하고 이를 대체하거나 폐기시키는 새 VIB를 제공하지 않을 경우 이전 VIB가 업그레이드 후 시스템에 남아 있습니다.

참고 UEFI 보안 부팅에는 최신 부팅 로더도 필요합니다. 이 스크립트는 최신 부팅 로더를 확인하지 않습니다.

사전 요구 사항

- 하드웨어가 UEFI 보안 부팅을 지원하는지 확인합니다.

- 모든 VIB가 최소 PartnerSupported의 허용 수준으로 서명되었는지 확인합니다. CommunitySupported 수준에서 VIB를 포함하는 경우 보안 부팅을 사용할 수 없습니다.

절차

1 ESXi를 업그레이드하고 다음 명령을 실행합니다.

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

2 출력을 확인합니다.

출력에는 `Secure boot can be enabled` 또는 `Secure boot CANNOT be enabled`가 포함됩니다.

신뢰할 수 있는 플랫폼 모듈을 통한 ESXi 호스트 보안

ESXi 호스트는 소프트웨어가 아닌 하드웨어에 기반하는 신뢰 보장을 제공하여 호스트 보안을 개선하는 보안 암호화 프로세서인 TPM(신뢰할 수 있는 플랫폼 모듈) 칩을 사용할 수 있습니다.

TPM은 보안 암호화 프로세서의 업계 표준입니다. 랩톱부터 데스크톱과 서버에 이르는 현재의 컴퓨터 대부분에서 TPM 칩을 찾아볼 수 있습니다. vSphere 6.7 이상은 TPM 버전 2.0을 지원합니다.

TPM 2.0 칩은 ESXi 호스트 ID를 증명합니다. 호스트 증명은 지정된 시점에 호스트 소프트웨어의 상태를 인증하고 증명하는 프로세스입니다. 부팅 시 서명된 소프트웨어만 로드될 수 있도록 하는 UEFI 보안 부팅이 성공적인 증명의 요구 사항입니다. 시스템에서 부팅되는 소프트웨어 모듈의 측정값이 TPM 2.0 칩에 기록되고 안전하게 저장되며 vCenter Server가 이를 원격으로 확인합니다.

원격 증명 프로세스의 단계를 간략하게 설명하면 다음과 같습니다.

1 원격 TPM의 신뢰도를 설정하고 해당 TPM에 AK(증명 키)를 생성합니다.

ESXi 호스트가 vCenter Server에 추가되거나 재부팅되거나 다시 연결되면 vCenter Server가 호스트의 AK를 요청합니다. AK 생성 프로세스에는 TPM 하드웨어 자체를 확인하여 알려진(신뢰할 수 있는) 벤더가 하드웨어를 생산했는지 여부를 확인하는 작업도 포함됩니다.

2 호스트에서 증명 보고서를 검색합니다.

vCenter Server는 호스트에 증명 보고서를 보내도록 요청합니다. 이 보고서에는 TPM이 서명한 PCR(플랫폼 구성 레지스터)의 인용문과 기타 서명된 호스트 이진 메타데이터가 포함됩니다. vCenter Server는 이 정보가 신뢰할 수 있는 구성에 해당하는지 확인하여 이전에 신뢰되지 않은 호스트의 플랫폼을 식별합니다.

3 호스트의 신뢰성을 확인합니다.

vCenter Server는 서명된 인용문의 신뢰성을 확인하고 소프트웨어 버전을 유추하고 언급된 소프트웨어 버전의 신뢰도를 결정합니다. vCenter Server가 서명된 인용문이 유효하지 않다고 결정하면 원격 증명이 실패하고 호스트가 신뢰되지 않습니다.

TPM 2.0 칩을 사용하려면 vCenter Server 환경이 다음 요구 사항을 충족해야 합니다.

- vCenter Server 6.7 이상

- TPM 2.0 칩이 설치되고 UEFI에서 사용되도록 설정된 ESXi 6.7 호스트 이상
- UEFI 보안 부팅 사용

ESXi 호스트의 BIOS에 TPM이 SHA-256 해싱 알고리즘 및 TIS/FIFO(First-In, First-Out) 인터페이스를 사용하고 CRB(Command Response Buffer)를 사용하지 않도록 구성되어 있는지 확인합니다. 이러한 필수 BIOS 옵션 설정에 대한 자세한 내용은 벤더 설명서를 참조하십시오.

다음 위치에서 VMware가 인증한 TPM 2.0 칩을 검토합니다.

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

TPM 2.0 칩이 설치된 ESXi 호스트를 부팅하면 vCenter Server가 호스트의 증명 상태를 모니터링합니다. vSphere Client는 vCenter Server의 **보안** 아래 **요약** 탭에 다음 경보와 함께 하드웨어의 신뢰 상태를 표시합니다.

- 녹색: 정상 상태이며 완전히 신뢰할 수 있음을 나타냅니다.
- 빨간색: 증명에 실패했습니다.

참고 TPM 2.0 칩을 vCenter Server에서 이미 관리하는 ESXi 호스트에 추가하는 경우 먼저 호스트의 연결을 끊었다가 다시 연결해야 합니다. 호스트 연결 해제 및 다시 연결에 대한 정보는 "vCenter Server 및 호스트 관리" 설명서를 참조하십시오.

(ESXi 및 신뢰할 수 있는 플랫폼 모듈 2.0 기능 데모)

ESXi 호스트 증명 상태 보기

TPM(신뢰할 수 있는 플랫폼 모듈) 2.0 호환 칩을 ESXi 호스트에 추가하면 플랫폼의 무결성이 증명됩니다. vSphere Client에서 호스트의 증명 상태를 볼 수 있습니다. Intel TXT(Trusted Execution Technology) 상태도 볼 수 있습니다.

절차

1. vSphere Client를 사용하여 vCenter Server에 연결합니다.
2. 데이터 센터로 이동하고 **모니터** 탭을 클릭합니다.
3. **보안**을 클릭합니다.
4. [무결성] 열에서 호스트의 상태를 검토하고 **메시지** 열에서 함께 제공된 메시지를 읽습니다.
5. 이 호스트가 신뢰할 수 있는 호스트인 경우 자세한 내용은 신뢰할 수 있는 클러스터 증명 상태 보기 항목을 참조하십시오.

다음에 수행할 작업

실패 또는 경고 증명 상태에 대한 내용은 ESXi 호스트 무결성 문제 해결 항목을 참조하십시오. 신뢰할 수 있는 호스트의 경우 신뢰할 수 있는 호스트 증명 문제 해결 항목을 참조하십시오.

ESXi 호스트 무결성 문제 해결

ESXi 호스트에 TPM(신뢰할 수 있는 플랫폼 모듈) 디바이스를 설치할 때 호스트가 무결성을 전달하는 데 실패할 수 있습니다. 이 문제의 잠재적 원인을 해결할 수 있습니다.

절차

1 ESXi 호스트 경보 상태 및 관련 오류 메시지를 확인합니다. ESXi 호스트 증명 상태 보기의 내용을 참조하십시오.

2 오류 메시지가 호스트 보안 부팅이 사용되지 않도록 설정되었습니다인 경우 문제를 해결하기 위해 보안 부팅을 다시 사용하도록 설정해야 합니다.

3 호스트의 증명 상태가 실패한 경우 vCenter Server `vpxd.log` 파일에서 다음 메시지를 확인합니다.

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

이 메시지는 vCenter Server에서 이미 관리하고 있는 ESXi 호스트에 TPM 2.0 칩을 추가하고 있음을 나타냅니다. 먼저 호스트의 연결을 끊었다가 다시 연결해야 합니다. 호스트 연결 해제 및 다시 연결에 대한 정보는 "vCenter Server 및 호스트 관리" 설명서를 참조하십시오.

위치 및 로그 순환을 포함한 vCenter Server 로그 파일에 대한 자세한 내용은 VMware 기술 자료 문서 (https://kb.vmware.com/s/article/1021804)를 참조하십시오.

4 다른 모든 오류 메시지의 경우 고객 지원에 문의하십시오.

ESXi 로그 파일

로그 파일은 공격 문제를 해결하고 침해에 대한 정보를 얻을 수 있는 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 조치를 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 대한 전용 활동 기록이 생성됩니다.
- 중앙 호스트로 원격 로깅하면 중앙 호스트에서 로그 파일을 수집할 수 있습니다. 이 호스트에서 하나의 도구로 모든 호스트를 모니터링하고, 집계 분석을 수행하고, 로그 데이터를 검색할 수 있습니다. 이러한 접근 방법을 사용하면 편리하게 모니터링할 수 있고 여러 호스트에 대한 조정된 공격과 같은 상황에 대한 정보도 파악할 수 있습니다.
- ESXCLI 또는 PowerCLI를 사용하거나 API 클라이언트를 사용하여 ESXi 호스트에서 원격 보안 syslog를 구성합니다.
- syslog 구성을 쿼리하여 syslog 서버와 포트가 올바른지 확인합니다.

syslog 설정에 대한 자세한 내용 및 ESXi 로그 파일에 대한 추가 정보는 "vSphere 모니터링 및 성능" 설명서를 참조하십시오.

ESXi 호스트의 Syslog 구성

vSphere Client나 `esxcli system syslog` 명령을 사용하여 syslog 서비스를 구성할 수 있습니다.

`esxcli system syslog` 명령 및 기타 ESXCLI 명령을 사용하는 방법에 대한 자세한 내용은 "ESXCLI 시작" 항목을 참조하십시오.

절차

1 vSphere Client 인벤토리에서 호스트를 찾습니다.

2 **구성**을 클릭합니다.

3 시스템 아래에서 **고급 시스템 설정**을 클릭합니다.

4 **편집**을 클릭합니다.

5 **syslog**를 필터링합니다.

6 로깅을 전체적으로 설정하려면 변경할 설정을 선택하고 값을 입력합니다.

옵션	설명
Syslog.global.defaultRotate	유지할 아카이브의 최대 수입니다. 이 숫자는 전체적으로 설정할 수 있으며 개별 하위 로거에 대해 설정할 수도 있습니다.
Syslog.global.defaultSize	시스템에서 로그를 회전할 때까지의 기본 로그 크기(KB)입니다. 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 있을 수 있습니다. 로컬 파일 시스템의 `/scratch` 디렉토리만 여러 번 재부팅해도 영구적으로 유지됩니다. 디렉토리는 [*datastorename*] *path_to_file*로 지정해야 하며, 여기서 경로는 데이터스토어 백업 볼륨의 루트에 상대적입니다. 예를 들어 경로 `[storage1] /systemlogs`는 경로 `/vmfs/volumes/storage1/systemlogs`에 매핑됩니다.
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://hostName1:1514`처럼 프로토콜과 포트를 포함할 수 있습니다. UDP(포트 514에서만), TCP 및 SSL이 지원됩니다. 전달된 syslog 메시지를 수신하려면 원격 호스트에 syslog가 설치되고 올바르게 구성되어 있어야 합니다. 원격 호스트 구성에 대한 자세한 내용은 원격 호스트에 설치된 syslog 서비스에 대한 설명서를 참조하십시오. 원격 호스트를 무제한으로 사용하여 syslog 메시지를 수신할 수 있습니다.

7 (선택 사항) 로그의 기본 로그 크기와 로그 순환을 덮어쓰려면 다음을 수행합니다.

a 사용자 지정할 로그의 이름을 클릭합니다.

b 원하는 순환 수와 로그 크기를 입력합니다.

8 **확인**을 클릭합니다.

결과

syslog 옵션에 대한 변경 내용이 즉시 적용됩니다.

ESXi 로그 파일 위치

ESXi에서는 syslog 기능을 사용하여 호스트 작업을 로그 파일에 기록합니다.

표 3-8. ESXi 로그 파일 위치

구성 요소	위치	용도
인증	/var/log/auth.log	로컬 시스템의 인증과 관련된 모든 이벤트가 들어 있습니다.
ESXi 호스트 에이전트 로그	/var/log/hostd.log	ESXi 호스트와 해당 가상 시스템을 관리하고 구성하는 에이전트에 대한 정보가 들어 있습니다.
셸 로그	/var/log/shell.log	ESXi 셸에 입력한 모든 명령의 기록과 셸 이벤트(예: 셸이 사용되도록 설정된 시점)가 들어 있습니다.
시스템 메시지	/var/log/syslog.log	모든 일반 로그 메시지가 들어 있으며 이 메시지를 문제 해결에 이용할 수 있습니다. 기존에는 이 정보가 메시지 로그 파일에 있었습니다.
vCenter Server 에이전트 로그	/var/log/vpxa.log	vCenter Server와 통신하는 에이전트에 대한 정보가 들어 있습니다(vCenter Server로 호스트를 관리하는 경우).
가상 시스템	영향을 받는 가상 시스템의 구성 파일과 같은 디렉토리에 있는 vmware.log 및 vmware*.log 파일. 예: /vmfs/volumes/datastore/virtual machine/vwmare.log	가상 시스템 전원 이벤트, 시스템 오류 정보, 도구 상태 및 작업, 시간 동기화, 가상 하드웨어 변경, vMotion 마이그레이션, 시스템 복제 등이 들어 있습니다.
VMkernel	/var/log/vmkernel.log	가상 시스템 및 ESXi와 관련된 작업을 기록합니다.
VMkernel 요약	/var/log/vmksummary.log	ESXi의 가동 시간 및 가용성 통계를 확인하는 데 사용합니다(쉼표로 구분).
VMkernel 주의	/var/log/vmkwarning.log	가상 시스템과 관련된 작업을 기록합니다.
신속 부팅	/var/log/loadESX.log	신속 부팅을 통한 ESXi 호스트 다시 시작과 관련된 모든 이벤트가 들어 있습니다.
신뢰할 수 있는 인프라 에이전트	/var/run/log/kmxa.log	ESXi 신뢰할 수 있는 호스트에서 클라이언트 서비스와 관련된 활동을 기록합니다.
키 제공자 서비스	/var/run/log/kmxd.log	vSphere 신뢰 기관 키 제공자 서비스와 관련된 활동을 기록합니다.
증명 서비스	/var/run/log/attestd.log	vSphere 신뢰 기관 증명 서비스와 관련된 활동을 기록합니다.

표 3-8. ESXi 로그 파일 위치 (계속)

구성 요소	위치	용도
ESX 토큰 서비스	/var/run/log/esxtokend.log	vSphere 신뢰 기관 ESX 토큰 서비스와 관련된 활동을 기록합니다.
ESX API 전달자	/var/run/log/esxapiadapter.log	vSphere 신뢰 기관 API 전달자와 관련된 활동을 기록합니다.

Fault Tolerance 로깅 트래픽 보안

VMware FT(Fault Tolerance)는 기본 VM에서 수행되는 입력 및 이벤트를 캡처하여 다른 호스트에서 실행 중인 보조 VM으로 이를 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.

Fault Tolerance 암호화 사용

Fault Tolerance 로그 트래픽을 암호화할 수 있습니다.

vSphere Fault Tolerance는 기본 VM과 보조 VM 간에 빈번한 검사를 수행하기 때문에 보조 VM은 마지막에 성공한 체크포인트에서 빠르게 재개할 수 있습니다. 체크포인트에는 이전 체크포인트 이후에 수정된 VM 상태가 포함됩니다. Fault Tolerance 로그 트래픽을 암호화할 수 있습니다.

Fault Tolerance를 설정하면 FT 암호화는 기본적으로 **편의적**으로 설정됩니다. 즉, 기본 호스트와 보조 호스트 모두 암호화가 가능한 경우에만 암호화를 사용하도록 설정됩니다. FT 암호화 모드를 수동으로 변경해야 하는 경우 다음 절차를 수행하십시오.

참고 Fault Tolerance는 vSphere 7.0 업데이트 2 이상에서 vSphere 가상 시스템 암호화를 지원합니다. 게스트 내 및 어레이 기반 암호화는 VM 암호화에 의존하거나 VM 암호화를 방해하지 않습니다. 여러 암호화 계층이 있으면 추가 계산 리소스가 사용되며 이로 인해 가상 시스템 성능에 영향을 미칠 수 있습니다. 이 영향은 하드웨어와 I/O의 양 및 유형에 따라 달라지지만 대부분의 워크로드에서 전반적인 성능에 미치는 영향은 미미합니다. 중복 제거, 압축 및 복제와 같은 백엔드 스토리지 기능의 효율성 및 호환성도 VM 암호화의 영향을 받을 수 있습니다.

사전 요구 사항

FT 암호화에는 SMP-FT가 필요합니다. Legacy FT(Record-Play FT)에 대한 암호화는 지원되지 않습니다.

절차

1 VM을 선택하고 **설정 편집**을 선택합니다.

2 **VM 옵션**에서 **암호화된 FT** 드롭다운 메뉴를 선택합니다.

3 다음 옵션 중 하나를 선택합니다.

옵션	설명
사용 안 함	암호화된 Fault Tolerance 로깅을 설정하지 않습니다.
편의적	양측이 모두 가능한 경우만 암호화를 설정합니다. 암호화된 Fault Tolerance 로깅을 지원하지 않는 ESXi 호스트로 Fault Tolerance VM을 이동할 수 있습니다.
필수	Fault Tolerance 기본 및 보조 호스트(둘 다 암호화된 FT 로깅을 지원함)를 선택합니다.

참고 VM 암호화를 사용하도록 설정되어 있는 동안 FT 암호화 모드는 기본적으로 **필수**로 설정되며 수정할 수 없습니다.

FT 암호화 모드가 **필수**로 설정된 경우:

- FT를 설정하면 FT 보조 배치에 대해 FT 암호화 지원 호스트만 나열됩니다.
- FT 페일오버는 FT 암호화 지원 호스트에서만 발생할 수 있습니다.

4 **확인**을 클릭합니다.

ESXi 감사 레코드 관리

감사 레코드는 RFC 5424를 준수하며, ESXi 호스트의 작업에서 발생한 이벤트에 대해 기록된 시간, 상태, 설명 및 사용자 정보와 같은 항목과 관련된 이벤트에 대한 정보를 포함합니다. 로컬 및 원격 감사 레코드 유지가 모두 가능합니다. 감사 레코드 유지 기능은 기본적으로 비활성화되어 있습니다. 로컬 및 원격 감사 모드는 둘 다 수동으로 활성화해야 합니다.

로컬 ESXi 감사 로그는 최근 감사 메시지의 고정 크기 버퍼로 작동합니다. 메시지가 버퍼를 채우면 새 레코드가 가장 오래된 레코드를 덮어씁니다. 원격 감사 로그는 표준 syslog 형식(RFC 3164)의 동일한 감사 레코드 스트림을 암호화되지 않은 형식 또는 암호화된(RFC 5425) 형식으로 원격 서버에 전달합니다. 감사 메시지는 RFC 5424를 준수하지만 일반 syslog 메시지는 RFC 3164만 준수합니다. 시스템은 생성된 감사 메시지를 로컬 저장소와 원격 저장소에 동시에 전송합니다.

호스트와 원격 저장소 간의 연결이 끊어지면 원격 저장소는 생성된 감사 메시지를 삭제합니다. 다시 연결하면 시스템에서 잠재적인 메시지 손실을 나타내는 감사 메시지가 생성됩니다.

감사 레코드 구성

ESXCLI를 사용하여 로컬 감사 레코드 유지를 구성합니다. 자세한 내용은 https://code.vmware.com/에서 "ESXCLI 참조" 항목을 참조하십시오.

감사 레코드 보기

감사 레코드는 다음과 같이 볼 수 있습니다.

- 로컬: ESXi `/bin/viewAudit` 애플리케이션을 사용합니다.
- 원격: ESXCLI를 사용하여 원격 감사 서버를 구성합니다.

FetchAuditRecords API(DiagnosticsManager 관리 개체에 있음)를 사용하여 감사 레코드를 볼 수도 있습니다.

ESXi 구성 보호

vSphere 7.0 업데이트 2부터 ESXi 구성이 암호화로 보호됩니다. ESXi 호스트가 필요에 따라 TPM으로 보호되는 경우 ESXi 구성 암호화 키가 TPM으로 봉인됩니다.

수많은 ESXi 서비스가 구성 파일에 암호를 저장합니다. 이러한 구성은 ESXi 호스트의 부트 뱅크에서 아카이브된 파일로 지속됩니다. vSphere 7.0 업데이트 2부터 이 아카이브된 파일이 암호화됩니다. 따라서 공격자가 ESXi 호스트의 스토리지에 대한 물리적 액세스 권한이 있는 경우에도 이 파일을 직접 읽거나 변경할 수 없습니다.

공격자가 암호에 액세스하지 못하도록 방지할 뿐 아니라 TPM에 사용될 때 보안 ESXi 구성이 재부팅 시 가상 시스템 암호화 키를 저장할 수 있습니다. 따라서 키 서버를 사용할 수 없거나 키 서버에 연결하지 못할 때 암호화된 워크로드가 계속 작동할 수 있습니다. 키 지속성 개요의 내용을 참조하십시오.

ESXi 구성 보호 개요

수동으로 ESXi 구성 암호화를 사용하도록 설정할 필요가 없습니다. vSphere 7.0 업데이트 2 이상을 설치하거나 이 버전으로 업그레이드하는 경우 아카이브된 ESXi 구성 파일이 암호화됩니다.

vSphere 7.0 업데이트 2 이전에는 아카이브된 ESXi 구성 파일이 암호화되지 않았습니다. vSphere 7.0 업데이트 2 이상에서는 아카이브된 구성 파일이 암호화됩니다. ESXi 호스트가 TPM(신뢰할 수 있는 플랫폼 모듈)으로 구성된 경우 TPM이 호스트에 대한 구성을 "봉인"하는 데 사용되어 강력한 보안을 보장합니다.

vSphere 7.0 업데이트 2 이전 ESXi 구성 파일 개요

ESXi 호스트의 구성은 호스트에서 실행되는 각 서비스에 대한 구성 파일로 구성됩니다. 구성 파일은 일반적으로 `/etc/` 디렉토리에 있지만 다른 네임스페이스에도 상주할 수 있습니다. 구성 파일에는 서비스의 상태에 대한 런타임 정보가 포함되어 있습니다. 예를 들어 ESXi 호스트의 설정을 변경하는 경우 시간이 경과하면 구성 파일의 기본값이 변경될 수 있습니다. cron 작업은 정기적으로 ESXi 구성 파일을 백업하거나, ESXi가 정상적으로 종료되거나 요청 시 부트 뱅크에서 아카이브된 구성 파일을 생성합니다. ESXi가 재부팅되면 아카이브된 구성 파일을 읽고 백업을 생성한 시점의 ESXi의 상태를 재생성합니다. vSphere 7.0 업데이트 2 이전에는 아카이브된 구성 파일이 암호화되지 않았습니다. 따라서 시스템이 오프라인 상태일 때 물리적 ESXi 스토리지에 대한 액세스 권한이 있는 공격자가 이 파일을 읽고 변경할 수 있습니다.

보안 ESXi 구성 개요

ESXi 호스트를 설치하거나 vSphere 7.0 업데이트 2 이상으로 업그레이드한 후 처음 부팅할 때 다음과 같은 문제가 발생합니다.

- ESXi 호스트에 TPM이 있고 펌웨어에서 사용되도록 설정된 경우 TPM에 저장된 암호화 키로 아카이브된 구성 파일이 암호화됩니다. 이 시점부터 호스트의 구성은 TPM에 의해 봉인됩니다.

- ESXi 호스트에 TPM이 없는 경우 ESXi가 KDF(키 파생 함수)를 사용하여 아카이브된 구성 파일에 대한 보안 구성 암호화 키를 생성합니다. KDF에 대한 입력이 `encryption.info` 파일의 디스크에 저장됩니다.

참고 ESXi 호스트에 TPM 디바이스가 사용되도록 설정되어 있는 경우 보호 기능이 강화됩니다.

처음 부팅 후 ESXi 호스트가 재부팅되면 다음과 같은 문제가 발생합니다.

- ESXi 호스트에 TPM이 있는 경우 호스트가 해당 특정 호스트에 대한 TPM에서 암호화 키를 얻어야 합니다. TPM 측정값이 암호화 키를 생성할 때 사용된 봉인 정책을 충족하는 경우 호스트가 TPM에서 암호화 키를 얻습니다.
- ESXi 호스트에 TPM이 없는 경우 ESXi가 `encryption.info` 파일에서 정보를 읽어 보안 구성을 잠금 해제합니다.

보안 ESXi 구성 요구 사항

- ESXi 7.0 업데이트 2 이상
- 구성 암호화를 위한 TPM 2.0 및 봉인 정책 사용 기능

보안 ESXi 구성 복구 키

보안 ESXi 구성에는 복구 키가 포함됩니다. ESXi 보안 구성을 복구해야 하는 경우 명령줄 부팅 옵션으로 입력한 컨텐츠가 있는 복구 키를 사용합니다. 복구 키를 나열하여 복구 키 백업을 생성할 수 있습니다. 보안 요구 사항의 일부로 복구 키를 순환할 수도 있습니다.

복구 키의 백업 수행은 보안 ESXi 구성 관리에서 중요한 부분입니다. vCenter Server는 복구 키를 백업하도록 알리는 경보를 생성합니다.

복구 키 경보

복구 키의 백업 수행은 보안 ESXi 구성 관리에서 중요한 부분입니다. TPM 모드의 ESXi 호스트가 vCenter Server에 연결되었거나 다시 연결될 때마다 vCenter Server가 복구 키를 백업하도록 알리는 경보를 생성합니다. 경보를 재설정할 때 조건이 변경되지 않는 한 경보가 다시 트리거되지 않습니다.

보안 ESXi 구성에 대한 모범 사례

복구 키에 대한 다음 모범 사례를 따릅니다.

- 복구 키를 나열하면 복구 키가 일시적으로 신뢰할 수 없는 환경에 표시되고 메모리에 위치합니다. 키의 추적을 제거합니다.
  - 호스트를 재부팅하면 메모리에서 남은 키가 제거됩니다.
  - 향상된 보호를 위해 호스트에서 암호화 모드를 사용하도록 설정할 수 있습니다. 호스트 암호화 모드를 사용하도록 명시적으로 설정의 내용을 참조하십시오.
- 복구를 수행할 때:
  - 신뢰할 수 없는 환경에서 복구 키의 추적을 제거하려면 호스트를 재부팅합니다.

- 향상된 보안을 위해 키를 한 번 복구한 후 복구 키를 순환하여 새 키를 사용합니다.

TPM 봉인 정책 개요

vSphere 7.0 업데이트 2 이상에서 ESXi 호스트는 TPM을 사용하여 PCR(플랫폼 구성 레지스터) 정책에 따라 호스트의 구성을 봉인합니다. UEFI 보안 부팅 및 기타 설정을 적용하도록 PCR 정책을 구성할 수 있습니다.

TPM은 PCR(플랫폼 구성 레지스터) 측정을 사용하여 중요 데이터에 대한 무단 액세스를 제한하는 정책을 구현할 수 있습니다. TPM이 있는 ESXi 호스트를 vSphere 7.0 업데이트 2 이상으로 업그레이드하거나 설치하는 경우 TPM은 보안 부팅 설정을 통합하는 정책을 사용하여 중요 정보를 봉인합니다. 이 정책은 데이터가 TPM으로 처음 봉인되었을 때 보안 부팅을 사용한 경우 후속 부팅에서 데이터의 봉인을 해제하려고 시도할 때 보안 부팅을 계속 사용하도록 설정해야 할지 확인합니다.

보안 부팅은 UEFI 펌웨어 표준의 일부입니다. UEFI 보안 부팅을 사용하도록 설정하는 경우 운영 체제 부팅 로더에 유효한 디지털 서명이 있는 경우가 아니면 호스트가 모든 UEFI 드라이버 또는 애플리케이션의 로드를 거부합니다.

UEFI 보안 부팅 적용을 사용 또는 사용하지 않도록 선택할 수 있습니다. 보안 ESXi 구성에 대한 보안 부팅 적용 사용 또는 사용 안 함의 내용을 참조하십시오.

참고 vSphere 7.0 업데이트 2 이상으로 업그레이드하거나 설치할 때 TPM을 활성화하지 않으면 나중에 다음 명령을 사용하여 활성화할 수 있습니다.

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

TPM을 활성화한 후에는 설정을 실행 취소할 수 없습니다.

호스트에 대해 TPM을 사용하도록 설정한 경우에도 일부 TPM에서 `esxcli system settings encryption set` 명령이 실패합니다.

- vSphere 7.0 업데이트 2: NTZ(NationZ), IFX(Infineon Technologies)의 TPM 및 NTC(Nuvoton Technologies Corporation)의 특정 새 모델(예: NPCT75x)
- vSphere 7.0 업데이트 3: NTZ(NationZ)의 TPM

vSphere 7.0 업데이트 2 이상의 설치 또는 업그레이드 시 처음 부팅하는 동안 TPM을 사용할 수 없으면 설치 또는 업그레이드가 계속되고 모드의 기본값은 NONE으로 설정됩니다(즉, `--mode=NONE`). 결과 동작은 TPM이 활성화되지 않은 것과 같습니다.

또한 TPM은 봉인 정책에서 execInstalledOnly 부팅 옵션에 대한 설정을 적용할 수도 있습니다. execInstalledOnly 적용은 VMkernel이 VIB의 일부로 제대로 패키지되고 서명된 바이너리만 실행하도록 보장하는 고급 ESXi부팅 옵션입니다. execInstalledOnly 부팅 옵션은 보안 부팅 옵션에 종속됩니다. 봉인 정책에서 execInstalledOnly 부팅 옵션을 적용하려면 먼저 보안 부팅 적용을 사용하도록 설정해야 합니다. 보안 ESXi 구성에 대한 execInstalledOnly 적용 사용 또는 사용 안 함의 내용을 참조하십시오.

보안 ESXi 구성 관리

ESXCLI 명령을 사용하여 보안 ESXi 구성 복구 키를 나열하고, 복구 키를 순환하고, TPM 정책을 변경(예: UEFI 보안 부팅 적용)할 수 있습니다.

보안 ESXi 구성 복구 키의 컨텐츠 나열

ESXCLI를 사용하여 보안 ESXi 구성 복구 키의 컨텐츠를 표시할 수 있습니다.

이 작업은 TPM이 있는 ESXi 호스트에만 적용됩니다. 일반적으로 백업을 생성하기 위해 또는 복구 키 순환의 일환으로 보안 ESXi 구성 복구 키의 컨텐츠를 나열합니다.

사전 요구 사항

- ESXCLI 명령 집합에 대한 액세스 권한. ESXCLI 명령을 원격으로 실행하거나 ESXi 셸에서 실행할 수 있습니다.
- ESXCLI 독립형 버전 또는 PowerCLI를 사용하는 데 필요한 권한: **호스트.구성.설정**

절차

1 ESXi 호스트에서 다음 명령을 실행합니다.

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

2 보안 구성을 복구해야 하는 경우를 대비하여 출력을 안전한 원격 위치에 백업으로 저장합니다.

결과

복구 키 ID 및 키가 표시됩니다.

예제: 보안 ESXi 구성 복구 키 나열

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

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

보안 ESXi 구성 복구 키 순환

ESXCLI를 사용하여 보안 ESXi 구성 복구 키를 순환할 수 있습니다.

이 작업은 TPM이 있는 ESXi 호스트에만 적용됩니다. 보안 모범 사례의 일부로 ESXi 보안 구성 복구 키를 순환할 수 있습니다.

사전 요구 사항

- ESXCLI 명령 집합에 대한 액세스 권한. ESXCLI 명령을 원격으로 실행하거나 ESXi 셸에서 실행할 수 있습니다.
- ESXCLI 독립형 버전 또는 PowerCLI를 사용하는 데 필요한 권한: **호스트.구성.설정**

절차

1 복구 키를 나열합니다.

보안 ESXi 구성 복구 키의 컨텐츠 나열의 내용을 참조하십시오.

2 다음 명령을 실행합니다.

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

이 명령에서 선택적 *keyID*는 VMkernel 키 캐시의 키 ID이고 *uuid*는 복구 ID(`esxcli system settings encryption recovery list` 명령으로 가져옴)입니다. 선택적 키 ID를 제공하지 않으면 ESXi는 이전 복구 키를 임의로 생성된 새 복구 키로 바꿉니다.

결과

이제 복구 키는 제공되는 경우 키 ID로 참조되는 키의 컨텐츠로 설정됩니다. 그렇지 않으면 ESXi가 새 키 ID를 제공합니다.

보안 ESXi 구성 문제 해결 및 복구

보안 ESXi 구성에서 발생할 수 있는 부팅 문제를 해결하고 복구할 수 있습니다.

TPM을 지우거나(즉, TPM의 시드 값 재설정) TPM이 실패하는 경우 ESXi 보안 구성을 복구하는 단계를 수행해야 합니다. 구성을 복구하려면 복구 키가 있어야 합니다. 구성을 복구할 때까지 ESXi 호스트를 부팅할 수 없습니다. 보안 ESXi 구성 복구의 내용을 참조하십시오.

드문 경우지만 ESXi 호스트가 보안 구성을 복원하거나 암호 해독하지 못해 호스트가 부팅되지 않을 수 있습니다. 가능한 상황은 다음과 같습니다.

- 보안 부팅 설정(또는 기타 정책)으로 변경
- 실제 변조
- 복구 키를 사용할 수 없음

이러한 상황을 해결하려면 https://kb.vmware.com/kb/81446에서 VMware 기술 자료 문서를 참조하십시오.

보안 ESXi 구성 복구

TPM이 실패하거나 TPM을 지우는 경우 보안 ESXi 구성을 복구해야 합니다. 구성을 복구할 때까지 ESXi 호스트를 부팅할 수 없습니다.

보안 ESXi 구성 복구는 다음과 같은 상황을 참조합니다.

- TPM을 지웠습니다(즉 TPM의 시드가 재설정됨).
- TPM이 실패했습니다.

다른 보안 ESXi 구성 문제를 해결하려면 https://kb.vmware.com/kb/81446에서 VMware 기술 자료 문서를 참조하십시오.

수동으로 복구를 수행합니다. 설치 또는 업그레이드 스크립트의 일부로 복구를 수행하지 마십시오.

사전 요구 사항

복구 키를 가져옵니다. 이전에 복구 키를 나열하고 저장했을 것입니다. 보안 ESXi 구성 복구 키의 컨텐츠 나열의 내용을 참조하십시오.

절차

1 (선택 사항) TPM이 실패하면 디스크(부트 뱅크가 있는 디스크)를 TPM이 있는 다른 호스트로 이동합니다.

2 ESXi 호스트를 시작합니다.

3 ESXi 설치 관리자 창이 나타나면 Shift+O를 눌러 부팅 옵션을 편집합니다.

4 명령 프롬프트에서 부팅 옵션을 입력하여 구성을 복구합니다.

```
encryptionRecoveryKey=recovery_key
```

보안 ESXi 구성이 복구되고 ESXi 호스트가 부팅됩니다.

5 변경 내용을 유지하려면 다음 명령을 입력합니다.

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

다음에 수행할 작업

복구 키를 입력하면 복구 키가 일시적으로 신뢰할 수 없는 환경에 표시되고 메모리에 위치합니다. 꼭 필요한 것은 아니지만 호스트를 재부팅하여 메모리에 남아 있는 키의 흔적을 제거하는 것이 가장 좋습니다. 또는 키를 순환할 수 있습니다. 보안 ESXi 구성 복구 키 순환의 내용을 참조하십시오.

보안 ESXi 구성에 대한 보안 부팅 적용 사용 또는 사용 안 함

UEFI 보안 부팅 적용을 사용하도록 설정하거나 이전에 사용하도록 설정된 UEFI 보안 부팅 적용을 사용하지 않도록 설정하도록 선택할 수 있습니다. ESXi 호스트에서 TPM의 설정을 변경하려면 ESXCLI를 사용해야 합니다.

이 작업은 TPM이 있는 ESXi 호스트에만 적용됩니다. UEFI 보안 부팅은 펌웨어에서 시작된 소프트웨어를 신뢰할 수 있도록 하는 펌웨어 설정입니다. TPM을 사용하여 부팅할 때마다 UEFI 보안 부팅의 사용 설정을 적용할 수 있습니다.

사전 요구 사항

- ESXCLI 명령 집합에 대한 액세스 권한. ESXCLI 명령을 원격으로 실행하거나 ESXi 셸에서 실행할 수 있습니다.
- ESXCLI 독립형 버전 또는 PowerCLI를 사용하는 데 필요한 권한: **호스트.구성.설정**

절차

1 ESXi 호스트의 현재 설정을 나열합니다.

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

보안 부팅 적용을 사용하도록 설정하면 [보안 부팅 필요]가 true로 표시됩니다. 보안 부팅 적용을 사용하지 않도록 설정하면 [보안 부팅 필요]가 false로 표시됩니다.

모드가 [없음]으로 표시되면 호스트의 펌웨어에서 TPM을 사용하도록 설정하고 다음 명령을 실행하여 모드를 설정해야 합니다.

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

2 보안 부팅 적용을 사용하거나 사용하지 않도록 설정합니다.

옵션	설명

사용	a 호스트를 정상적으로 종료합니다.
	예를 들어 vSphere Client에서 ESXi 호스트를 마우스 오른쪽 버튼으로 클릭하고 **전원 > 종료**를 선택합니다.
	b 호스트의 펌웨어에서 보안 부팅을 사용하도록 설정합니다.
	자세한 벤더 하드웨어 설명서를 참조하십시오.
	c 호스트를 다시 시작합니다.
	d 다음 ESXCLI 명령을 실행합니다.
	`esxcli system settings encryption set --require-secure-boot=T`
	e 변경 내용을 확인합니다.
	`esxcli system settings encryption get`
	`Mode: TPM`
	`Require Executables Only From Installed VIBs: false`
	`Require Secure Boot: true`
	[보안 부팅 필요]가 true로 표시되는지 확인합니다.
	f 설정을 저장하려면 다음 명령을 실행합니다.
	`/sbin/auto-backup.sh`

사용 안 함	a 다음 ESXCLI 명령을 실행합니다.
	`esxcli system settings encryption set --require-secure-boot=F`
	b 변경 내용을 확인합니다.
	`esxcli system settings encryption get`
	`Mode: TPM`
	`Require Executables Only From Installed VIBs: false`
	`Require Secure Boot: false`
	[보안 부팅 필요]가 false로 표시되는지 확인합니다.
	c 설정을 저장하려면 다음 명령을 실행합니다.
	`/sbin/auto-backup.sh`
	호스트의 펌웨어에서 보안 부팅을 사용하지 않도록 설정할 수 있지만 이때, 펌웨어 설정과 TPM 적용 간의 종속성은 더 이상 설정되지 않습니다.

결과

선택 항목에 따라 ESXi 호스트가 보안 부팅 적용이 사용되거나 사용되지 않도록 설정된 상태로 실행됩니다.

참고 vSphere 7.0 업데이트 2 이상으로 업그레이드하거나 설치할 때 TPM을 활성화하지 않으면 나중에 다음 명령을 사용하여 활성화할 수 있습니다.

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

TPM을 활성화한 후에는 설정을 실행 취소할 수 없습니다.

호스트에 대해 TPM을 사용하도록 설정한 경우에도 일부 TPM에서 `esxcli system settings encryption set` 명령이 실패합니다.

- vSphere 7.0 업데이트 2: NTZ(NationZ), IFX(Infineon Technologies)의 TPM 및 NTC(Nuvoton Technologies Corporation)의 특정 새 모델(예: NPCT75x)
- vSphere 7.0 업데이트 3: NTZ(NationZ)의 TPM

vSphere 7.0 업데이트 2 이상의 설치 또는 업그레이드 시 처음 부팅하는 동안 TPM을 사용할 수 없으면 설치 또는 업그레이드가 계속되고 모드의 기본값은 NONE으로 설정됩니다(즉, `--mode=NONE`). 결과 동작은 TPM이 활성화되지 않은 것과 같습니다.

보안 ESXi 구성에 대한 execInstalledOnly 적용 사용 또는 사용 안 함

execInstalledOnly 적용을 사용하도록 설정하거나 이전에 사용하도록 설정된 execInstalledOnly 적용을 사용하지 않도록 설정하도록 선택할 수 있습니다. ESXi 호스트에서 TPM의 설정을 변경하려면 ESXCLI를 사용해야 합니다. execInstalledOnly 적용을 사용하도록 설정하려면 먼저 UEFI 보안 부팅 적용을 사용하도록 설정해야 합니다.

이 작업은 TPM이 있는 ESXi 호스트에만 적용됩니다. execInstalledOnly 고급 ESXi 부팅 옵션이 TRUE로 설정되어 있는 경우 VMkernel은 VIB의 일부로 패키지되고 서명된 이진만 실행하도록 보장합니다. TPM을 사용하여 부팅할 때마다 이 부팅 옵션의 사용 설정을 적용할 수 있습니다.

사전 요구 사항

- execInstalledOnly 적용을 사용하도록 설정하려면 먼저 UEFI 보안 부팅 적용을 사용하도록 설정해야 합니다. execInstalledOnly 적용은 UEFI 보안 부팅 적용을 기반으로 구축됩니다. 보안 ESXi 구성에 대한 보안 부팅 적용 사용 또는 사용 안 함의 내용을 참조하십시오.
- ESXCLI 명령 집합에 대한 액세스 권한. ESXCLI 명령을 원격으로 실행하거나 ESXi 셸에서 실행할 수 있습니다.
- ESXCLI 독립형 버전 또는 PowerCLI를 사용하는 데 필요한 권한: **호스트.구성.설정**

절차

1 ESXi 호스트의 현재 설정을 나열합니다.

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

execInstalledOnly 적용을 사용하도록 설정하면 [설치된 VIB에서 실행 파일만 필요]가 true로 표시됩니다. execInstalledOnly 적용을 사용하지 않도록 설정하면 [설치된 VIB에서 실행 파일만 필요]가 false로 표시됩니다. execInstalledOnly 적용을 사용하도록 설정하려면 보안 부팅 적용을 사용하도록 설정해야 하며, 이 경우 [보안 부팅 필요]가 true로 표시됩니다.

모드가 [없음]으로 표시되면 호스트의 펌웨어에서 TPM을 사용하도록 설정하고 다음 명령을 실행하여 모드를 설정해야 합니다.

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

또한 [보안 부팅 필요]가 False로 표시되면 보안 ESXi 구성에 대한 보안 부팅 적용 사용 또는 사용 안 함 항목을 참조하여 적용이 가능하도록 설정합니다.

2 execInstalledOnly 적용을 사용하거나 사용하지 않도록 설정합니다.

옵션	설명

사용	a 보안 부팅 옵션이 적용되는지 확인합니다.
	`esxcli system settings encryption get`
	`Mode: TPM`
	`Require Executables Only From Installed VIBs: false`
	`Require Secure Boot: true`
	[보안 부팅 필요]가 true로 표시되는지 확인합니다. 그렇지 않은 경우 보안 ESXi 구성에 대한 보안 부팅 적용 사용 또는 사용 안 함의 내용을 참조하십시오.
	b execInstalledOnly 부팅 옵션의 런타임 값을 TRUE로 구성하려면 다음 ESXCLI 명령을 실행합니다.
	`esxcli system settings kernel set -s execInstalledOnly -v TRUE`
	c 호스트를 정상적으로 종료합니다.
	예를 들어 vSphere Client에서 ESXi 호스트를 마우스 오른쪽 버튼으로 클릭하고 **전원 > 종료**를 선택합니다.
	d 호스트를 다시 시작합니다.
	e execInstalledOnly 적용을 설정하려면 다음 ESXCLI 명령을 실행합니다.
	`esxcli system settings encryption set --require-exec-installed-only=T`
	f 변경 내용을 확인합니다.
	`esxcli system settings encryption get`
	`Mode: TPM`
	`Require Executables Only From Installed VIBs: true`
	`Require Secure Boot: true`
	[설치된 VIB에서 실행 파일만 필요]가 true로 표시되는지 확인합니다.
	g 설정을 저장하려면 다음 명령을 실행합니다.
	`/sbin/auto-backup.sh`

사용 안 함	a 다음 ESXCLI 명령을 실행합니다.
	`esxcli system settings encryption set --require-exec-installed-only=F`
	b 변경 내용을 확인합니다.
	`esxcli system settings encryption get`
	`Mode: TPM`
	`Require Executables Only From Installed VIBs: false`
	`Require Secure Boot: true`
	[설치된 VIB에서 실행 파일만 필요]가 false로 표시되는지 확인합니다.
	c 설정을 저장하려면 다음 명령을 실행합니다.
	`/sbin/auto-backup.sh`

옵션	설명
	TPM이 더 이상 execInstalledOnly 부팅 옵션을 적용하지 않습니다.

결과

선택 항목에 따라 ESXi 호스트가 execInstalledOnly 적용이 사용되거나 사용되지 않도록 설정된 상태로 실행됩니다.

vCenter Server 시스템 보안

4

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
- vCenter Server의 필수 포트

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

- 관리자 역할은 필요한 관리자에게만 부여합니다. 사용자 지정 역할을 생성하거나 보다 제한된 권한이 있는 관리자에 대해 암호화 관리자 없음 역할을 사용할 수 있습니다. 멤버 자격이 엄격히 제어되지 않는 그룹에는 이 역할을 적용하지 마십시오.
- vCenter Server 시스템에 연결할 때 애플리케이션이 고유한 서비스 계정을 사용해야 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.

액세스 최소화

사용자가 vCenter Server 호스트 시스템에 직접 로그인하도록 허용하지 마십시오. vCenter Server 호스트 시스템에 로그인된 사용자는 설정을 변경하고 프로세스를 수정하여 의도적이든 의도적이지 않든 피해를 끼칠 수 있습니다. 해당 사용자는 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 데이터베이스 사용자에게 최소 권한 부여

데이터베이스 사용자에게는 데이터베이스 액세스와 관련된 일부 권한만 필요합니다.

일부 권한은 설치 및 업그레이드의 경우에만 필요합니다. vCenter Server가 설치되거나 업그레이드된 후 데이터베이스 관리자에서 이러한 권한을 제거할 수 있습니다.

데이터스토어 브라우저 액세스 제한

데이터스토어.데이터스토어 찾아보기 권한은 해당 권한이 실제로 필요한 사용자 또는 그룹에만 할당합니다. 해당 권한이 있는 사용자는 웹 브라우저 또는 vSphere Client를 통해 vSphere 배포와 연결된 데이터스토어에서 파일을 보거나 업로드하거나 다운로드할 수 있습니다.

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 사용자 지정 액세스 역할을 생성해야 합니다. 사용자가 가상 시스템 내에서 명령을 실행하지 못하도록 제한의 내용을 참조하십시오.

vpxuser에 대한 암호 정책 수정 고려

기본적으로 vCenter Server는 30일마다 자동으로 vpxuser 암호를 변경합니다. 이 설정이 회사 정책을 충족하는지 확인하거나 vCenter Server 암호 정책을 구성합니다. vCenter Server 암호 정책 설정의 내용을 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 폴더에 대해 관리자 역할이 있는 사용자 또는 그룹이 다시 시작 동안 검증될 수 없는 경우 역할이 해당 사용자 또는 그룹에서 제거됩니다. 대신 vCenter Server는 관리자 역할을 기본적으로 vCenter Single Sign-On 관리자 administrator@vsphere.local에 부여합니다 그러면 이 계정은 vCenter Server 관리자 역할을 수행합니다.

명명된 관리자 계정을 다시 설정하고 관리자 역할을 해당 계정에 할당하여 익명 vCenter Single Sign-On 관리자 계정(기본적으로 administrator@vsphere.local) 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 Client 인증서 확인

vSphere Client 또는 다른 클라이언트 애플리케이션 사용자가 인증서 확인 경고에 주의를 기울이도록 지시합니다. 인증서가 확인되지 않으면 사용자가 MiTM 공격의 대상이 될 수 있습니다.

vCenter Server 암호 정책 설정

기본적으로 vCenter Server는 30일마다 자동으로 vpxuser 암호를 변경합니다. vSphere Client에서 해당 값을 변경할 수 있습니다.

절차

1. vSphere Client를 사용하여 vCenter Server 시스템에 로그인합니다.
2. 개체 계층에서 vCenter Server 시스템을 선택합니다.
3. **구성**을 클릭합니다.
4. **고급 설정**을 클릭하고 **설정 편집**을 클릭합니다.
5. **필터** 아이콘을 클릭하고 **VimPasswordExpirationInDays**를 입력합니다.
6. 요구 사항에 맞게 `VirtualCenter.VimPasswordExpirationInDays`를 설정합니다.

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 Client가 있습니다.
- DNS, Active Directory 및 PTP 또는 NTP와 같은 인프라 서비스
- vCenter Server 시스템의 기능에 필수적인 구성 요소를 실행하는 기타 시스템

vCenter Server에서 방화벽을 사용합니다. 필요한 구성 요소만 vCenter Server 시스템과 통신할 수 있도록 IP 기반 액세스 제한을 포함합니다.

CLI 및 SDK와 함께 Linux 클라이언트 사용 평가

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.

보안을 강화하려면 ESXi 시스템 및 vCenter Server 호스트의 VMCA 서명된 인증서를 엔터프라이즈 또는 타사 CA에서 서명된 인증서로 교체할 수 있습니다. 그러나 Linux 클라이언트와의 특정 통신이 계속해서 메시지 가로채기(machine-in-the-middle) 공격에 취약할 수 있습니다. 다음 구성 요소는 Linux 운영 체제에서 실행될 때 취약성이 드러납니다.

- ESXCLI 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.
- 배스천 호스트(점프 박스 시스템)를 사용하여 Linux 클라이언트를 "점프" 뒤에 배치합니다.

클라이언트 플러그인 검사

vSphere 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 설치를 사용하십시오.

vCenter 설치에는 vSphere Client에 대한 확장성 프레임워크가 포함됩니다. 이 프레임워크를 사용하여 메뉴 선택이나 도구 모음 아이콘을 통해 클라이언트를 확장할 수 있습니다. 확장을 통해 vCenter 추가 기능 구성 요소 또는 외부 웹 기반 기능에 액세스할 수 있습니다.

확장성 프레임워크를 사용하면 의도하지 않는 기능이 도입될 위험이 있습니다. 예를 들어 관리자가 vSphere Client의 인스턴스에 플러그인을 설치하면 이 플러그인은 해당 관리자의 권한 수준으로 임의의 명령을 실행할 수 있습니다.

vSphere 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 Client에 로그인합니다.
2. 홈 페이지에서 **관리**를 선택한 다음 **솔루션** 아래에서 **클라이언트 플러그인**을 선택합니다.
3. 클라이언트 플러그인 목록을 검토합니다.

vCenter Server 보안 모범 사례

vCenter Server 시스템 보호를 위한 모든 모범 사례를 준수하십시오. 추가 단계는 vCenter Server를 더욱 안전하게 보호하는 데 도움이 됩니다.

PTP 또는 NTP 구성

모든 시스템이 동일한 상대적 시간 소스를 사용하는지 확인합니다. 이 시간 소스는 UTC(협정 세계시)와 같은 합의된 시간 표준과 동기화해야 합니다. 동기화된 시스템은 인증서 검증에 필수적입니다. 또한 PTP 및 NTP는 로그 파일에서 침입자 추적을 용이하게 합니다. 잘못된 시간 설정은 공격을 감지하기 위해 로그 파일을 검사하고 연관시키기 어렵게 할 뿐 아니라 감사의 정확성을 떨어뜨립니다. NTP 서버와 vCenter Server의 시간 동기화의 내용을 참조하십시오.

vCenter Server 네트워크 액세스 제한

vCenter Server와 통신해야 하는 구성 요소에 대한 액세스를 제한합니다. 불필요한 시스템의 액세스 차단은 운영 체제에 대한 공격의 가능성을 줄입니다.

vSphere 및 vSAN을 포함한 VMware 제품의 지원되는 모든 포트 및 프로토콜 목록은 https://ports.vmware.com/에서 VMware Ports and Protocols Tool™을 참조하십시오. VMware 제품별로 포트를 검색하고, 사용자 지정된 포트 목록을 생성하고, 포트 목록을 인쇄하거나 저장할 수 있습니다.

배스천 호스트 구성

자산을 보호하기 위해 승격된 관리 작업을 수행하도록 배스천 호스트(점프 박스라고도 함)를 구성합니다. 배스천 호스트는 최소한의 관리 애플리케이션을 호스팅하는 특수 용도의 컴퓨터입니다. 다른 모든 불필요한 서비스는 제거됩니다. 이 호스트는 일반적으로 관리 네트워크에 상주합니다. 배스천 호스트는 로그인을 주요 인원으로 제한하고, 로그인에 방화벽 규칙을 요구하며, 감사 도구를 통한 모니터링을 추가하여 자산에 대한 보호를 강화합니다.

vCenter 암호 요구 사항 및 잠금 동작

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

이 섹션에서는 vCenter Single Sign-On 암호에 대해 설명합니다. ESXi 로컬 사용자의 암호에 대한 자세한 내용은 ESXi 암호 및 계정 잠금 항목을 참조하십시오.

vCenter Single Sign-On 관리자 암호

vCenter Single Sign-On 관리자, administrator@vsphere.local의 암호는 기본적으로 vCenter Single Sign-On 암호 정책을 통해 지정됩니다. 기본적으로 이 암호는 다음 요구 사항을 충족해야 합니다.

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

이 사용자의 암호는 20자 이내여야 합니다. ASCII가 아닌 문자를 사용할 수 있습니다. 관리자는 기본 암호 정책을 변경할 수 없습니다. "vSphere 인증" 설명서를 참조하십시오.

vCenter Server 암호

vCenter Server에서 암호 요구 사항은 vCenter Single Sign-On 또는 구성된 ID 소스(예: Active Directory, OpenLDAP 등)에 의해 지정됩니다.

vCenter Single Sign-On 잠금 동작

사용자는 미리 설정된 수의 연속 시도 실패 후에 잠깁니다. 기본적으로 사용자는 3분 동안 5번의 연속 시도 실패 후에 잠기며, 잠긴 계정은 5분 후에 자동으로 잠금이 해제됩니다. vCenter Single Sign-On 잠금 정책을 사용하여 이러한 기본값을 변경할 수 있습니다. "vSphere 인증" 설명서를 참조하십시오.

vCenter Single Sign-On 도메인 관리자(기본적으로 administrator@vsphere.local)는 잠금 정책의 영향을 받지 않습니다. 사용자는 암호 정책의 영향을 받습니다.

암호 변경

암호를 아는 경우 사용자가 `dir-cli password change` 명령을 사용하여 암호를 변경할 수 있습니다. 암호를 잊은 경우 vCenter Single Sign-On 관리자가 `dir-cli password reset` 명령을 사용하여 사용자의 암호를 재설정할 수 있습니다.

다른 vSphere 버전의 암호 만료 및 관련 항목에 대한 정보는 VMware 기술 자료를 검색하십시오.

기존 ESXi 호스트 지문 확인

vSphere 6.0 이상에서는 기본적으로 호스트에 VMCA 인증서가 할당됩니다. 인증서 모드를 지문으로 변경하는 경우 기존 호스트에 대해 계속해서 지문 모드를 사용할 수 있습니다. vSphere Client에서 지문을 확인할 수 있습니다.

참고 기본적으로 인증서는 업그레이드 동안 보존됩니다.

절차

1. vSphere Client 인벤토리에서 vCenter Server를 찾습니다.
2. **구성**을 클릭합니다.
3. **설정**에서 **일반**을 클릭합니다.
4. **편집**을 클릭합니다.
5. **SSL 설정**을 클릭합니다.
6. 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.
7. 지문이 일치하면 호스트 옆의 **확인** 확인란을 선택합니다.

   선택되지 않은 호스트는 **확인**을 클릭한 후 연결 해제됩니다.
8. **저장**을 클릭합니다.

vCenter Server의 필수 포트

vCenter Server 시스템은 모든 관리 호스트에 데이터를 보낼 수 있고 모든 vSphere Client에서 데이터를 받을 수 있어야 합니다. 관리 호스트 간에 마이그레이션 및 프로비저닝 작업이 가능하려면 소스 및 대상 호스트가 사전 결정된 TCP 및 UDP 포트를 통해 상호 간에 데이터를 받을 수 있어야 합니다.

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. vSphere에서 지원되는 모든 포트 및 프로토콜 목록은 https://ports.vmware.com에서 VMware Ports and Protocols Tool™을 참조하십시오.

설치 중 포트가 사용 중이거나 거부 목록을 사용하여 차단된 경우 vCenter Server 설치 관리자가 오류 메시지를 표시합니다. 설치를 진행하려면 다른 포트 번호를 사용해야 합니다. 프로세스 간 통신에만 사용되는 내부 포트가 있습니다.

VMware는 지정된 포트를 사용하여 통신합니다. 또한 관리 호스트는 지정된 포트에서 vCenter Server의 데이터를 모니터링합니다. 이들 요소 사이에 기본 제공 방화벽이 있는 경우에는 설치 관리자가 설치 또는 업그레이드 프로세스 중에 포트를 엽니다. 사용자 지정 방화벽의 경우 필요한 포트를 수동으로 열어야 합니다. 두 관리 호스트 사이에 방화벽이 있는 경우 마이그레이션 또는 복제 등의 소스 또는 타겟 작업을 수행하려면 관리 호스트가 데이터를 수신하는 방법을 구성해야 합니다.

다른 포트를 사용하여 vSphere Client 데이터를 수신하도록 vCenter Server 시스템을 구성하려면 "vCenter Server 및 호스트 관리" 설명서를 참조하십시오.

가상 시스템 보안

5

가상 시스템에서 실행되는 게스트 운영 체제에는 물리적 시스템과 동일한 보안 위험이 따릅니다. 가상 시스템을 물리적 시스템처럼 보호하고 이 문서와 "보안 구성 가이드" (이전 명칭: "강화 지침")에 설명되어 있는 모범 사례를 따릅니다.

"보안 구성 가이드" 는 https://core.vmware.com/security에서 제공됩니다.

본 장은 다음 항목을 포함합니다.

- 가상 시스템에 대해 UEFI 보안 부팅 사용 또는 사용 안 함
- 가상 시스템에서 VMX 파일로의 정보 메시지 제한
- 가상 시스템 보안 모범 사례
- Intel Software Guard Extensions를 사용하여 가상 시스템 보호
- AMD Secure Encrypted Virtualization-Encrypted State를 사용하여 가상 시스템 보호

가상 시스템에 대해 UEFI 보안 부팅 사용 또는 사용 안 함

UEFI 보안 부팅은 PC 부팅 시 PC 제조업체에서 신뢰하는 소프트웨어만 사용하도록 보장하는 보안 표준입니다. 특정 가상 시스템 하드웨어 버전 및 운영 체제의 경우 물리적 시스템과 동일한 방법으로 보안 부팅을 사용할 수 있습니다.

UEFI 보안 부팅을 지원하는 운영 체제에서 부팅 로더, 운영 체제 커널, 운영 체제 드라이버를 포함하여 모든 부팅 소프트웨어가 서명됩니다. 가상 시스템의 기본 구성에는 여러 코드 서명 인증서가 포함됩니다.

- Windows 부팅에만 사용되는 Microsoft 인증서
- Microsoft에서 서명한 타사 코드에 사용되는 Microsoft 인증서(예: Linux 부팅 로더)
- 가상 시스템 내에서 ESXi 부팅에만 사용되는 VMware 인증서

가상 시스템의 기본 구성에는 가상 시스템 내의 보안 부팅 구성(보안 부팅 해지 목록 포함)을 수정하려는 요청의 인증에 필요한 단일 인증서가 포함되며, 이는 Microsoft KEK(키 교환 키) 인증서입니다.

대부분의 경우 기존 인증서를 바꿀 필요가 없습니다. 인증서를 교체하려면 VMware 기술 자료 시스템을 참조하십시오.

UEFI 보안 부팅을 사용하는 가상 시스템에는 VMware Tools 버전 10.1 이상이 필요합니다. VMware Tools의 최신 버전을 사용할 수 있게 되면 이러한 가상 시스템을 최신 버전으로 업그레이드할 수 있습니다.

Linux 가상 시스템의 경우 VMware Host-Guest Filesystem이 보안 부팅 모드에서 지원되지 않습니다. 보안 부팅을 사용하도록 설정하기 전에 VMware Tools에서 VMware Host-Guest Filesystem을 제거합니다.

참고 가상 시스템에 대해 보안 부팅을 설정하면 서명된 드라이버만 해당 가상 시스템에 로드할 수 있습니다.

이 작업은 vSphere Client를 사용하여 가상 시스템에 보안 부팅을 사용하고 사용하지 않도록 설정하는 방법을 설명합니다. 스크립트를 작성하여 가상 시스템 설정을 관리할 수도 있습니다. 예를 들어 다음 PowerCLI 코드를 사용하여 가상 시스템에 대해 펌웨어를 BIOS에서 EFI로 변경하는 것을 자동화할 수 있습니다.

```
$vm = Get-VM TestVM

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

자세한 내용은 "VMware PowerCLI 사용자 가이드" 를 참조하십시오.

사전 요구 사항

모든 사전 요구 사항이 충족된 경우에만 보안 부팅을 사용할 수 있습니다. 사전 요구 사항이 충족되지 않으면 vSphere Client에 확인란이 표시되지 않습니다.

- 가상 시스템 운영 체제 및 펌웨어가 UEFI 부팅을 지원하는지 확인합니다.
  - EFI 펌웨어
  - 가상 하드웨어 버전 13 이상
  - UEFI 보안 부팅을 지원하는 운영 체제.

  참고 일부 게스트 운영 체제에서는 게스트 운영 체제를 수정하지 않고 BIOS 부팅에서 UEFI 부팅으로 변경할 수 없습니다. UEFI 부팅으로 변경하기 전에 게스트 운영 체제 설명서에서 확인하십시오. 이미 UEFI 부팅을 사용하는 가상 시스템을 UEFI 보안 부팅을 지원하는 운영 체제로 업그레이드하는 경우, 해당 가상 시스템에 대해 보안 부팅 기능을 사용할 수 있습니다.
- 가상 시스템을 끕니다. 가상 시스템이 실행 중이면 확인란이 흐리게 표시됩니다.

절차

1. vSphere Client 인벤토리에서 가상 시스템을 찾습니다.
2. 가상 시스템을 마우스 오른쪽 버튼으로 클릭하고 **설정 편집**을 선택합니다.
3. **VM 옵션** 탭을 클릭하고 **부팅 옵션**을 확장합니다.
4. **부팅 옵션**에서 펌웨어가 **EFI**로 설정되었는지 확인합니다.

5 작업을 선택합니다.

- **보안 부팅** 확인란을 선택하여 보안 부팅을 사용 하도록 설정하고
- **보안 부팅** 확인란의 선택을 해제하여 보안 부팅을 사용하지 않도록 설정합니다.

6 **확인**을 클릭합니다.

결과

가상 시스템이 부팅될 때 유효한 서명이 있는 구성 요소만 허용됩니다. 누락되었거나 잘못된 서명이 있는 구성 요소가 발견되면 부팅 프로세스가 오류와 함께 중지됩니다.

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 DoS가 발생할 수 있습니다.

가상 시스템 구성 파일(VMX 파일) 제한은 기본적으로 1MB입니다. 대개 이 용량이면 충분하지만 필요한 경우 이 값을 변경할 수 있습니다. 예를 들어 대량의 사용자 지정 정보를 파일에 저장하는 경우에는 제한을 늘릴 수 있습니다.

참고 필요한 정보의 분량을 신중하게 고려합니다. 정보의 양이 데이터스토어의 용량을 초과하면 DoS가 발생할 수 있습니다.

`tools.setInfo.sizeLimit` 매개 변수가 고급 옵션에 나열되지 않더라도 1MB의 기본 제한이 적용됩니다.

절차

1 vSphere Client 인벤토리에서 가상 시스템을 찾습니다.

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 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 서버에서 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 있습니다. 따라서 콘솔 액세스로 인해 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 실행되는 애플리케이션 또는 서비스를 지원하는 데 필요하지 않은 시스템 구성 요소를 사용하지 않도록 설정하여 공격 가능성을 줄입니다.

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 올바로 구성된 확장된 운영 체제를 포함하는 템플릿을 사용하여 다른 애플리케이션별 템플릿을 생성하거나, 애플리케이션 템플릿을 사용하여 가상 시스템을 배포할 수 있습니다.

절차

- 패치가 적용되고 올바로 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 서버에서 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 있습니다. 따라서 콘솔 액세스로 인해 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 가상 시스템 콘솔에 대한 연결을 제한합니다.

예를 들어 보안 수준이 높은 환경에서 연결을 하나로 제한합니다. 일부 환경에서는 정상 작업을 수행하는 데 몇 개의 동시 연결이 필요한 경우 제한을 늘릴 수 있습니다.

a vSphere Client에서, 가상 시스템의 전원을 끕니다.

b 가상 시스템을 마우스 오른쪽 버튼으로 클릭하고 **설정 편집**을 선택합니다.

c **VM 옵션** 탭을 클릭하고 **VMware 원격 콘솔 옵션**을 확장합니다.

d 최대 세션 수(예: **2**)를 입력합니다.

e **확인**을 클릭합니다.

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.

영향을 완전하게 이해할 때까지 제한을 설정하거나 리소스 풀을 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 실행되는 애플리케이션 또는 서비스를 지원하는 데 필요하지 않은 시스템 구성 요소를 사용하지 않도록 설정하여 공격 가능성을 줄입니다.

가상 시스템에는 일반적으로 물리적 서버만큼 많은 서비스나 기능이 필요하지 않습니다. 시스템을 가상화할 때는 특정 서비스나 기능이 필요한지 여부를 평가하십시오.

참고 가능한 경우 "최소" 또는 "코어" 설치 모드로 게스트 운영 체제를 설치하여 게스트 운영 체제의 크기, 복잡성 및 공격 표면을 줄이십시오.

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.
- 사용되지 않는 표시 기능이나 가상 시스템(호스트 게스트 파일 시스템)에 호스트 파일 공유를 가능하게 하는 VMware 공유 폴더와 같이 사용되지 않는 기능을 사용하지 않도록 설정합니다.
- 화면 보호기를 끄십시오.
- 꼭 필요한 경우 이외에는 Linux, BSD 또는 Solaris 게스트 운영 체제 맨 위에서 X Window 시스템을 실행하지 마십시오.

불필요한 하드웨어 디바이스 제거

사용하도록 설정되거나 연결된 디바이스는 잠재적인 공격 채널이 될 수 있습니다. 가상 시스템에 대한 권한이 있는 사용자 및 프로세스는 네트워크 어댑터, CD-ROM 드라이브와 같은 하드웨어 디바이스에 연결하거나 연결을 끊을 수 있습니다. 공격자는 이 기능을 사용하여 가상 시스템의 보안을 침해할 수 있습니다. 따라서 불필요한 하드웨어 디바이스를 제거하면 공격을 방지하는 데 도움이 됩니다.

가상 시스템에 대한 액세스 권한이 있는 공격자는 연결이 끊어진 하드웨어 디바이스에 연결하여 하드웨어 디바이스에 남아 있는 미디어의 중요 정보에 액세스할 수 있습니다. 또한 공격자는 네트워크 어댑터의 연결을 끊어 가상 시스템을 네트워크에서 격리하여 서비스 거부를 유발할 수도 있습니다.

- 인증되지 않은 디바이스를 가상 시스템에 연결하지 않습니다.
- 불필요하거나 사용하지 않는 하드웨어 디바이스는 제거합니다.
- 불필요한 가상 디바이스는 가상 시스템 내에서 사용되지 않도록 설정합니다.
- 필요한 디바이스만 가상 시스템에 연결합니다. 가상 시스템에서는 직렬 및 병렬 포트가 거의 사용되지 않습니다. 규칙에 따라 CD/DVD 드라이브는 소프트웨어를 설치할 때만 일시적으로 연결됩니다.

절차

1. vSphere Client 인벤토리에서 가상 시스템을 찾습니다.
2. 가상 시스템을 마우스 오른쪽 버튼으로 클릭한 후 **설정 편집**을 클릭합니다.

3 불필요한 하드웨어 디바이스를 사용하지 않도록 설정합니다.

다음 디바이스에 대한 확인이 포함됩니다.

- 직렬 포트
- 병렬 포트
- USB 컨트롤러
- CD-ROM 드라이브

참고 vSphere 7.0 이상에서 플로피 드라이브 디바이스를 관리하려면 PowerCLI 명령을 사용해야 합니다.

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.

사전 요구 사항

가상 시스템의 전원을 끕니다.

절차

1 vSphere Client 인벤토리에서 가상 시스템을 찾습니다.

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 적절한 경우 다음 매개 변수를 추가 또는 편집합니다.

옵션	설명
svga.vgaonly	이 매개 변수를 TRUE로 설정할 경우 고급 그래픽 기능이 작동하지 않습니다. 최신 게스트 운영 체제에서 이 매개 변수를 TRUE로 설정하지 마십시오. 그러면 운영 체제가 올바르게 작동하지 않습니다. `svga.vgaonly`가 TRUE로 설정되면 문자 셀 콘솔 모드만 사용할 수 있습니다. 이 설정을 사용하는 경우 `mks.enable3d`에 영향을 미치지 않습니다. **참고** 이 설정은 가상화된 비디오 카드가 필요하지 않은 가상 시스템에만 적용합니다.
mks.enable3d	3D 기능이 필요하지 않은 가상 시스템에서 이 매개 변수를 FALSE로 설정합니다.

표시되지 않는 기능 사용 안 함

VMware 가상 시스템은 VMware Workstation 및 VMware Fusion과 같은 호스팅되는 가상화 플랫폼 및 vSphere 환경에서 작동할 수 있습니다. 가상 시스템을 vSphere 환경에서 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 Client 인벤토리에서 가상 시스템을 찾습니다.

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

6 **확인**을 클릭합니다.

가상 시스템에 호스트 파일을 공유하는 VMware 공유 폴더를 사용하지 않도록 설정

보안 수준이 높은 환경에서는 특정 구성 요소를 사용하지 않도록 설정하여, 공격자가 HGFS(호스트 게스트 파일 시스템)를 사용하여 게스트 운영 체제 내에서 파일을 전송할 수 있는 위험을 최소화할 수 있습니다.

이 섹션에 설명된 매개 변수를 수정하면 공유 폴더 기능에만 영향을 미치며 게스트 가상 시스템에서 도구의 일부로 실행되는 HGFS 서버에는 영향을 미치지 않습니다. 또한 이러한 매개 변수는 도구의 파일 전송을 사용하는 자동 업그레이드 및 VIX 명령에는 영향을 주지 않습니다.

절차

1 vSphere Client 인벤토리에서 가상 시스템을 찾습니다.

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.

TRUE로 설정하면 VMX 프로세스가 HGFS 서버 기능의 각 도구 서비스, 데몬 또는 업그레이드 프로세스에서 알림을 수신하지 못합니다.

6 (선택 사항) isolation.tools.hgfs.disable 매개 변수가 TRUE로 설정되었는지 확인합니다.

TRUE로 설정하면 호스트 파일을 가상 시스템에 공유하는 VMware 공유 폴더 기능을 사용하지 않도록 설정합니다.

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 Client를 사용하여 해당 작업을 사용하도록 설정해야 합니다.

이러한 옵션에 대한 기본값이 보안 환경을 보장하기 위해 설정됩니다. 하지만 설정이 올바른지 확인하기 위해 감사 도구를 사용하도록 설정하려면 명시적으로 값을 true로 설정해야 합니다.

사전 요구 사항

가상 시스템을 끕니다.

절차

1 vSphere Client 인벤토리에서 가상 시스템을 찾습니다.

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 값이 [이름] 및 [값] 열에 있는지 확인하거나 추가합니다.

이름	값
isolation.tools.copy.disable	true
isolation.tools.paste.disable	true
isolation.tools.setGUIOptions.enable	false

이 옵션은 게스트 운영 체제의 VMware Tools 제어판에서 지정된 설정을 모두 재정의합니다.

6 **확인**을 클릭합니다.

7 (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 창이 포커스를 얻으면 가상 시스템에서 실행되는 프로세스와 권한 없는 사용자가 가상 시스템 콘솔 클립보드에 액세스할 수 있습니다. 콘솔을 사용하기 전에 사용자가 클립보드에 중요한 정보를 복사한 경우에는 사용자의 중요한 데이터가 가상 시스템에 노출될 수 있습니다. 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 역할을 가진 사용자는 가상 시스템의 게스트 운영 체제 내에서 파일 및 애플리케이션과 상호 작용할 수 있습니다. 게스트 기밀성, 가용성 또는 무결성이 침해될 위험을 줄이려면 **게스트 작업** 권한이 없는 게스트가 아닌 액세스 역할을 생성해야 합니다. 해당 역할을 가상 시스템 파일 액세스 권한이 필요하지 않은 관리자에게 할당합니다.

보안을 위해 물리적 데이터 센터와 마찬가지로 가상 데이터 센터에 대한 액세스도 제한적으로 허용하십시오. 관리자 권한이 필요하지만 게스트 운영 체제의 파일 및 애플리케이션과 상호 작용할 권한이 없는 사용자에게 게스트 액세스를 사용하지 않도록 설정하는 사용자 지정 역할을 적용합니다.

예를 들어 구성에는 중요한 정보가 들어 있는 인프라의 가상 시스템이 포함될 수 있습니다.

vMotion을 사용하여 마이그레이션과 같은 작업을 수행하려면 데이터 센터 관리자가 가상 시스템에 액세스하고 일부 원격 게스트 운영 체제 작업을 사용하지 않도록 설정하여 해당 관리자가 중요한 정보에 액세스할 수 없도록 해야 합니다.

사전 요구 사항

역할을 생성하는 vCenter Server 시스템에서 **관리자** 권한이 있는지 확인합니다.

절차

1. 역할을 생성하려는 vCenter Server 시스템에서 **관리자** 권한이 있는 사용자로 vSphere Client에 로그인합니다.
2. **관리**를 선택하고 **역할**을 클릭합니다.
3. 관리자 역할을 클릭하고 **역할 복제 작업** 아이콘을 클릭합니다.
4. 역할 이름과 설명을 입력하고 **확인**을 클릭합니다.

   예를 들어 **`Administrator No Guest Access`**를 입력합니다.
5. 복제된 역할을 선택하고 **역할 편집 작업** 아이콘을 클릭합니다.
6. **가상 시스템** 권한에서 **게스트 작업**을 선택 취소하고 **다음**을 클릭합니다.
7. **마침**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. 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.

게스트 OS의 가상 시스템 사용자 및 게스트 OS에서 실행 중인 프로세스가 가상 시스템 고급 설정을 변경하여 디바이스를 변경하지 못하도록 할 수 있습니다.

사전 요구 사항

가상 시스템을 끕니다.

절차

1 vSphere Client 인벤토리에서 가상 시스템을 찾습니다.

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 값이 [이름] 및 [값] 열에 있는지 확인하거나 추가합니다.

이름	값
isolation.device.connectable.disable	true
isolation.device.edit.disable	true

이러한 설정은 가상 시스템에 연결된 디바이스를 연결하거나 연결을 끊는 vSphere 관리자의 기능에 영향을 미치지 않습니다.

6 **확인**을 클릭하여 구성 매개 변수 대화상자를 닫고 **확인**을 다시 클릭합니다.

게스트 운영 체제 프로세스가 호스트에 구성 메시지를 보내지 않도록 방지

게스트 운영 체제에서 구성 설정을 수정하지 못하도록 이러한 프로세스가 이름-값 쌍을 구성 파일에 쓰지 못하게 할 수 있습니다.

사전 요구 사항

가상 시스템을 끕니다.

절차

1 vSphere Client 인벤토리에서 가상 시스템을 찾습니다.

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 **구성 매개 변수 추가**를 클릭하고 [이름] 및 [값] 열에 다음 값을 입력합니다.

열	값
이름	`isolation.tools.setinfo.disable`
값	`true`

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.

Intel Software Guard Extensions를 사용하여 가상 시스템 보호

vSphere에서는 가상 시스템에 대해 가상 Intel® Software Guard Extensions(vSGX)를 구성할 수 있습니다. vSGX를 사용하면 워크로드에 추가적인 보안을 제공할 수 있습니다.

일부 현대의 Intel CPU는 Intel® SGX(Intel® Software Guard Extensions)라고 하는 보안 확장을 구현합니다. Intel SGX는 공개 또는 수정으로부터 특정 코드와 데이터를 보호하려는 애플리케이션 개발자들을 위한 프로세서별 기술입니다. Intel SGX를 사용하면 사용자 수준 코드에서 Enclave라고 하는 메모리의 개인 영역을 정의할 수 있습니다. Enclave 컨텐츠는 Enclave 외부에서 실행되는 코드가 Enclave 컨텐츠에 액세스할 수 없도록 하는 방식으로 보호됩니다.

가상 시스템은 하드웨어에서 사용할 수 있는 경우 vSGX를 통해 Intel SGX 기술을 사용할 수 있습니다. vSGX를 사용하려면 SGX 지원 CPU에 ESXi 호스트를 설치해야 하며 ESXi 호스트의 BIOS에서 SGX를 사용하도록 설정해야 합니다. vSphere Client를 사용하여 가상 시스템에 대해 SGX를 사용하도록 설정할 수 있습니다.

vSGX 개요

가상 시스템은 하드웨어에서 사용할 수 있는 경우 Intel SGX 기술을 사용할 수 있습니다.

vSGX를 위한 요구 사항

vSGX를 사용하려면 vSphere 환경이 다음과 같은 요구 사항을 충족해야 합니다.

- 가상 시스템 요구 사항:
  - EFI 펌웨어
  - 하드웨어 버전 17 이상
- 구성 요소 요구 사항:
  - vCenter Server 7.0 이상
  - ESXi 7.0 이상
- 게스트 운영 체제 지원:
  - Linux
  - Windows Server 2016(64비트) 이상
  - Windows 10(64비트) 이상

Intel 하드웨어

vSGX에 대해 지원되는 Intel 하드웨어는 https://www.vmware.com/resources/compatibility/search.php에서 vSphere 호환성 가이드를 참조하십시오.

ESXi 호스트에서 SGX를 사용하도록 설정하려면 특정 CPU에서 하이퍼스레딩을 꺼야 할 수 있습니다. 자세한 내용은 VMware KB 문서(https://kb.vmware.com/s/article/71367)를 참조하십시오.

vSGX에서 지원되지 않는 VMware 기능

vSGX가 사용되도록 설정된 경우 다음과 같은 기능은 가상 시스템에서 지원되지 않습니다.

- vMotion/DRS 마이그레이션
- 가상 시스템 일시 중단 및 재개
- 가상 시스템 스냅샷(가상 시스템의 메모리에 대한 스냅샷을 생성하지 않는 경우에는 가상 시스템 스냅샷이 지원됩니다.)
- Fault Tolerance

- 게스트 무결성(GI, VMware AppDefense™ 1.0의 플랫폼 기반)

참고 이러한 VMware 기능은 Intel SGX 아키텍처가 작동하는 방식으로 인해 지원되지 않습니다. VMware 결함으로 인한 결과가 아닙니다.

가상 시스템에서 vSGX 사용

가상 시스템을 생성할 때 동시에 가상 시스템에서 vSGX를 사용하도록 설정할 수 있습니다.

사전 요구 사항

SGX 지원 CPU에 ESXi 호스트를 설치해야 하며 호스트의 BIOS에서 SGX를 사용하도록 설정해야 합니다. 지원되는 Intel CPU에 대해서는 vSGX 개요의 내용을 참조하십시오.

하드웨어 버전 17 이상과 지원되는 다음 게스트 운영 체제 중 하나를 사용하는 가상 시스템을 생성합니다.

- Linux
- Windows 10(64비트) 이상
- Windows Server 2016(64비트) 이상

절차

1 vSphere Client를 사용하여 vCenter Server에 연결합니다.

2 ESXi 호스트 또는 클러스터 같이 가상 시스템의 올바른 상위 개체인 인벤토리의 개체를 선택합니다.

3 개체를 마우스 오른쪽 버튼으로 클릭하고 **새 가상 시스템**을 선택한 다음 프롬프트에 따라 가상 시스템을 생성합니다.

옵션	작업
생성 유형 선택	가상 시스템을 생성합니다.
이름 및 폴더 선택	이름 및 대상 위치를 지정합니다.
계산 리소스 선택	가상 시스템을 생성할 권한이 있는 개체를 지정합니다.
스토리지 선택	VM 스토리지 정책에서 스토리지 정책을 선택합니다. 호환되는 데이터스토어를 선택합니다.
호환성 선택	**ESXi 7.0 이상**이 선택되어 있는지 확인합니다.
게스트 운영 체제 선택	Linux, Windows 10(64비트) 또는 Windows Server 2016(64비트)을 선택합니다.
하드웨어 사용자 지정	[보안 디바이스]에서 SGX에 대해 **사용** 확인란을 선택합니다. **VM 옵션 > 부팅 옵션 > 펌웨어**에서 EFI가 선택되었는지 확인합니다. EPC(Enclave 페이지 캐시) 크기를 입력하고 그에 따라 FLC(Flexible Launch Control) 모드를 선택합니다.
완료 준비	정보를 검토하고 **마침**을 클릭합니다.

기존 가상 시스템에서 vSGX 사용

기존 가상 시스템에서 vSGX를 사용하도록 설정할 수 있습니다.

vSphere 7.0 이상에서 실행되는 가상 시스템에서 vSGX를 사용하도록 설정할 수 있습니다.

사전 요구 사항

- SGX 지원 CPU에 ESXi 호스트를 설치해야 하며 호스트의 BIOS에서 SGX를 사용하도록 설정해야 합니다. 지원되는 Intel CPU에 대해서는 vSGX 개요의 내용을 참조하십시오.
- 사용하는 게스트 운영 체제가 Linux, Windows Server 2016(64 비트) 이상 또는 Windows 10(64비트) 이상이어야 합니다.
- 환경에서 실행하는 ESXi 호스트가 ESXi 7.0 이상이어야 합니다.
- 가상 시스템이 꺼져 있는지 확인합니다.
- 가상 시스템에 EFI 펌웨어를 사용해야 합니다.
- 가상 시스템은 하드웨어 버전 17 이상을 사용해야 합니다.

절차

1. vSphere Client를 사용하여 vCenter Server에 연결합니다.
2. 인벤토리에서 수정할 가상 시스템을 마우스 오른쪽 버튼으로 클릭하고 **설정 편집**을 선택합니다.
3. **설정 편집** 대화상자의 **보안 디바이스**에서 SGX에 대해 **사용** 확인란을 선택합니다.
4. EPC(Enclave 페이지 캐시) 크기를 입력하고 그에 따라 FLC(Flexible Launch Control) 모드를 선택합니다.
5. **VM 옵션 > 부팅 옵션 > 펌웨어**에서 EFI가 선택되었는지 확인합니다.
6. **확인**을 클릭합니다.

가상 시스템에서 vSGX 제거

가상 시스템에서 vSGX를 제거할 수 있습니다.

절차

1. vSphere Client를 사용하여 vCenter Server에 연결합니다.
2. 인벤토리에서 수정할 가상 시스템을 마우스 오른쪽 버튼으로 클릭하고 **설정 편집**을 선택합니다.
3. **설정 편집** 대화상자의 **보안 디바이스**에서 SGX에 대해 **사용** 확인란을 선택 취소합니다.
4. **확인**을 클릭합니다.

   vSGX 항목이 **VM 하드웨어** 창의 가상 시스템 **요약** 탭에 더 이상 나타나지 않는지 확인합니다.

AMD Secure Encrypted Virtualization-Encrypted State를 사용하여 가상 시스템 보호

SEV-ES(Secure Encrypted Virtualization-Encrypted State)는 게스트 운영 체제의 메모리 및 레지스터 상태를 암호화된 상태로 유지하여 하이퍼바이저의 액세스로부터 보호하는 최신 AMD CPU에 사용되도록 설정된 하드웨어 기능입니다.

추가적인 보안 향상으로 가상 시스템에 SEV-ES를 추가할 수 있습니다. SEV-ES는 CPU 레지스터가 하이퍼바이저와 같은 구성 요소로 레지스터의 정보를 누출하지 못하도록 합니다. SEV-ES는 또한 CPU 레지스터 상태에 대한 악의적인 수정 사항을 감지할 수 있습니다.

AMD SEV-ES(Secure Encrypted Virtualization-Encrypted State) 개요

vSphere 7.0 업데이트 1 이상의 경우, 지원되는 AMD CPU 및 게스트 운영 체제에서 SEV-ES(Secure Encrypted Virtualization-Encrypted State)를 사용하도록 설정할 수 있습니다.

현재 SEV-ES는 AMD EPYC 7xx2 CPU(코드명 "Rome") 이상 CPU와 SEV-ES에 대한 특정 지원을 포함하는 Linux 커널 버전만 지원합니다.

SEV-ES 구성 요소 및 아키텍처

SEV-ES 아키텍처는 다음과 같은 구성 요소로 이루어져 있습니다.

- AMD CPU: 특히 암호화 키를 관리하고 암호화를 처리하는 PSP(Platform Security Processor).
- 인식 운영 체제: 게스트 시작 하이퍼바이저 호출을 사용하는 운영 체제입니다.
- VMM(가상 시스템 모니터) 및 가상 시스템 실행 파일(VMX): 가상 시스템의 전원을 켜는 동안 암호화된 가상 시스템 상태를 초기화하고 게스트 운영 체제의 호출을 처리합니다.
- VMkernel 드라이버: 하이퍼바이저와 게스트 운영 체제 간에 암호화되지 않은 데이터를 전달합니다.

ESXi에서 SEV-ES 구현 및 관리

먼저 시스템의 BIOS 구성에서 SEV-ES를 사용하도록 설정해야 합니다. BIOS 구성 액세스에 대 한 자세한 내용은 시스템 설명서를 참조하십시오. 시스템의 BIOS에서 SEV-ES를 사용하도록 설정한 후에 가상 시스템에 SEV-ES를 추가할 수 있습니다.

vSphere Client(vSphere 7.0 업데이트 2부터 시작) 또는 PowerCLI 명령을 사용하여 가상 시스템에서 SEV-ES를 사용하거나 사용하지 않도록 설정합니다. SEV-ES가 있는 새 가상 시스템을 생성하거나 기존 가상 시스템에서 SEV-ES를 사용하도록 설정할 수 있습니다. SEV-ES를 사용하도록 설정된 가상 시스템을 관리할 수 있는 권한은 일반 가상 시스템을 관리하는 권한과 동일합니다.

SEV-ES에서 지원되지 않는 VMware 기능

SEV-ES를 사용하도록 설정하면 다음 기능이 지원되지 않습니다.

- 시스템 관리 모드
- vMotion

- 전원이 켜진 스냅샷(단, 메모리가 없는 스냅샷은 지원됨)
- CPU 또는 메모리 무중단 추가 또는 제거
- 일시 중단/재개
- VMware Fault Tolerance
- 복제 및 즉시 복제
- 게스트 무결성
- UEFI 보안 부팅

vSphere Client를 사용하여 가상 시스템에 AMD SEV-ES(Secure Encrypted Virtualization-Encrypted State) 추가

vSphere 7.0 업데이트 2 이상에서는 vSphere Client를 사용하여 가상 시스템에 SEV-ES를 추가하여 게스트 운영 체제에 향상된 보안을 제공할 수 있습니다.

ESXi 7.0 업데이트 1 이상에서 실행되는 가상 시스템에 SEV-ES를 추가할 수 있습니다.

사전 요구 사항

- 시스템에 AMD EPYC 7xx2(코드명 "Rome") 이상의 CPU가 설치되어 있고 BIOS를 지원해야 합니다.
- BIOS에 SEV-ES를 사용하도록 설정되어 있어야 합니다.
- ESXi 호스트당 SEV-ES 가상 시스템 수는 BIOS에서 제어됩니다. BIOS에서 SEV-ES를 사용하도록 설정할 때 **Minimum SEV non-ES ASID** 설정 값을 SEV-ES 가상 시스템의 수에 1을 더한 값과 동일하게 입력합니다. 예를 들어 동시에 실행하려는 가상 시스템이 12개이면 **13**을 입력합니다.

  참고 vSphere 7.0 업데이트 1은 SEV-ES를 사용하도록 설정된 가상 시스템을 ESXi 호스트당 16개 지원합니다. BIOS에서 더 높은 설정을 사용해도 SEV-ES는 계속 작동하지만 16개라는 제한은 여전히 적용됩니다. vSphere 7.0 업데이트 2는 SEV-ES를 사용하도록 설정된 가상 시스템을 ESXi 호스트당 480개 지원합니다.

- 환경에서 실행하는 ESXi 호스트는 ESXi 7.0 업데이트 1 이상이어야 합니다.
- vCenter Server는 vSphere 7.0 업데이트 2 이상이어야 합니다.
- 게스트 운영 체제가 SEV-ES를 지원해야 합니다.

  현재는 SEV-ES를 지원하는 특정 Linux 커널만 지원됩니다.
- 가상 시스템은 하드웨어 버전 18 이상이어야 합니다.
- 가상 시스템에 **모든 게스트 메모리 예약** 옵션을 사용하도록 설정되어 있어야 합니다.그렇지 않으면 전원이 켜지지 않습니다.

절차

1 vSphere Client를 사용하여 vCenter Server에 연결합니다.

2 ESXi 호스트 또는 클러스터 같이 가상 시스템의 올바른 상위 개체인 인벤토리의 개체를 선택합니다.

3 개체를 마우스 오른쪽 버튼으로 클릭하고 **새 가상 시스템**을 선택한 다음 프롬프트에 따라 가상 시스템을 생성합니다.

옵션	작업
생성 유형 선택	가상 시스템을 생성합니다.
이름 및 폴더 선택	이름 및 대상 위치를 지정합니다.
계산 리소스 선택	가상 시스템을 생성할 권한이 있는 개체를 지정합니다.
스토리지 선택	VM 스토리지 정책에서 스토리지 정책을 선택합니다. 호환되는 데이터스토어를 선택합니다.
호환성 선택	**ESXi 7.0 이상**이 선택되어 있는지 확인합니다.
게스트 운영 체제 선택	Linux를 선택하고 SEV-ES를 지원하는 특정 Linux 버전을 선택합니다.
하드웨어 사용자 지정	**VM 옵션 > 부팅 옵션 > 펌웨어**에서 EFI가 선택되었는지 확인합니다. **VM 옵션 > 암호화**에서 AMD SEV-ES에 대해 **사용** 확인란을 선택합니다.
완료 준비	정보를 검토하고 **마침**을 클릭합니다.

결과

SEV-ES가 있는 가상 시스템이 생성됩니다.

가상 시스템에 AMD SEV-ES(Secure Encrypted Virtualization-Encrypted State) 추가

가상 시스템에 SEV-ES를 추가하여 게스트 운영 체제에 향상된 보안을 제공할 수 있습니다.

ESXi 7.0 업데이트 1 이상에서 실행되는 가상 시스템에 SEV-ES를 추가할 수 있습니다.

사전 요구 사항

- 시스템에 AMD EPYC 7xx2(코드명 "Rome") 이상의 CPU가 설치되어 있고 BIOS를 지원해야 합니다.
- BIOS에 SEV-ES를 사용하도록 설정되어 있어야 합니다.
- ESXi 호스트당 SEV-ES 가상 시스템 수는 BIOS에서 제어됩니다. BIOS에서 SEV-ES를 사용하도록 설정할 때 **Minimum SEV non-ES ASID** 설정 값을 SEV-ES 가상 시스템의 수에 1을 더한 값과 동일하게 입력합니다. 예를 들어 동시에 실행하려는 가상 시스템이 12개이면 **13**을 입력합니다.

  참고 vSphere 7.0 업데이트 1은 SEV-ES를 사용하도록 설정된 가상 시스템을 ESXi 호스트당 16개 지원합니다. BIOS에서 더 높은 설정을 사용해도 SEV-ES는 계속 작동하지만 16개라는 제한은 여전히 적용됩니다. vSphere 7.0 업데이트 2는 SEV-ES를 사용하도록 설정된 가상 시스템을 ESXi 호스트당 480개 지원합니다.

- 환경에서 실행하는 ESXi 호스트는 ESXi 7.0 업데이트 1 이상이어야 합니다.
- 게스트 운영 체제가 SEV-ES를 지원해야 합니다.

현재는 SEV-ES를 지원하는 특정 Linux 커널만 지원됩니다.

- 가상 시스템은 하드웨어 버전 18 이상이어야 합니다.
- 가상 시스템에 **모든 게스트 메모리 예약** 옵션을 사용하도록 설정되어 있어야 합니다.그렇지 않으면 전원이 켜지지 않습니다.
- 환경에 액세스할 수 있는 시스템에 PowerCLI 12.1.0 이상을 설치해야 합니다.

절차

1 PowerCLI 세션에서 `Connect-VIServer` cmdlet을 실행하여 SEV-ES가 있는 가상 시스템을 추가하려는 ESXi 호스트를 관리하는 vCenter Server에 관리자로 연결합니다.

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

2 `New-VM` cmdlet을 사용하고 `-SEVEnabled $true`를 지정하여 가상 시스템을 생성합니다.

예를 들어, 먼저 호스트 정보를 변수에 할당한 다음, 가상 시스템을 생성합니다.

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

가상 하드웨어 버전을 지정해야 하는 경우에는 `New-VM` cmdlet을 `-HardwareVersion vmx-18` 매개 변수와 함께 실행합니다. 예:

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

결과

SEV-ES가 있는 가상 시스템이 생성됩니다.

vSphere Client를 사용하여 기존 가상 시스템에서 AMD SEV-ES(Secure Encrypted Virtualization-Encrypted State)를 사용하도록 설정

vSphere 7.0 업데이트 2 이상에서는 vSphere Client를 사용하여 기존 가상 시스템에 SEV-ES를 추가하여 게스트 운영 체제에 향상된 보안을 제공할 수 있습니다.

ESXi 7.0 업데이트 1 이상에서 실행되는 가상 시스템에 SEV-ES를 추가할 수 있습니다.

사전 요구 사항

- 시스템에 AMD EPYC 7xx2(코드명 "Rome") 이상의 CPU가 설치되어 있고 BIOS를 지원해야 합니다.
- BIOS에 SEV-ES를 사용하도록 설정되어 있어야 합니다.

- ESXi 호스트당 SEV-ES 가상 시스템 수는 BIOS에서 제어됩니다. BIOS에서 SEV-ES를 사용하도록 설정할 때 **Minimum SEV non-ES ASID** 설정 값을 SEV-ES 가상 시스템의 수에 1을 더한 값과 동일하게 입력합니다. 예를 들어 동시에 실행하려는 가상 시스템이 12개이면 **13**을 입력합니다.

  참고 vSphere 7.0 업데이트 1은 SEV-ES를 사용하도록 설정된 가상 시스템을 ESXi 호스트당 16개 지원합니다. BIOS에서 더 높은 설정을 사용해도 SEV-ES는 계속 작동하지만 16개라는 제한은 여전히 적용됩니다. vSphere 7.0 업데이트 2는 SEV-ES를 사용하도록 설정된 가상 시스템을 ESXi 호스트당 480개 지원합니다.

- 환경에서 실행하는 ESXi 호스트는 ESXi 7.0 업데이트 1 이상이어야 합니다.
- vCenter Server는 vSphere 7.0 업데이트 2 이상이어야 합니다.
- 게스트 운영 체제가 SEV-ES를 지원해야 합니다.

  현재는 SEV-ES를 지원하는 특정 Linux 커널만 지원됩니다.
- 가상 시스템은 하드웨어 버전 18 이상이어야 합니다.
- 가상 시스템에 **모든 게스트 메모리 예약** 옵션을 사용하도록 설정되어 있어야 합니다.그렇지 않으면 전원이 켜지지 않습니다.
- 가상 시스템의 전원이 꺼졌는지 확인합니다.

절차

1 vSphere Client를 사용하여 vCenter Server에 연결합니다.

2 인벤토리에서 수정할 가상 시스템을 마우스 오른쪽 버튼으로 클릭하고 **설정 편집**을 선택합니다.

3 **VM 옵션 > 부팅 옵션 > 펌웨어**에서 EFI가 선택되었는지 확인합니다.

4 **설정 편집** 대화 상자의 **VM 옵션 > 암호화**에서 AMD SEV-ES에 대한 **사용** 확인란을 선택합니다.

5 **확인**을 클릭합니다.

결과

가상 시스템에 SEV-ES가 추가됩니다.

기존 가상 시스템에서 AMD SEV-ES(Secure Encrypted Virtualization-Encrypted State) 사용

기존 가상 시스템에 SEV-ES를 추가하여 게스트 운영 체제에 향상된 보안을 제공할 수 있습니다.

ESXi 7.0 업데이트 1 이상에서 실행되는 가상 시스템에 SEV-ES를 추가할 수 있습니다.

사전 요구 사항

- 시스템에 AMD EPYC 7xx2(코드명 "Rome") 이상의 CPU가 설치되어 있고 BIOS를 지원해야 합니다.
- BIOS에 SEV-ES를 사용하도록 설정되어 있어야 합니다.

- ESXi 호스트당 SEV-ES 가상 시스템 수는 BIOS에서 제어됩니다. BIOS에서 SEV-ES를 사용하도록 설정할 때 **Minimum SEV non-ES ASID** 설정 값을 SEV-ES 가상 시스템의 수에 1을 더한 값과 동일하게 입력합니다. 예를 들어 동시에 실행하려는 가상 시스템이 12개이면 **13**을 입력합니다.

  참고 vSphere 7.0 업데이트 1은 SEV-ES를 사용하도록 설정된 가상 시스템을 ESXi 호스트당 16개 지원합니다. BIOS에서 더 높은 설정을 사용해도 SEV-ES는 계속 작동하지만 16개라는 제한은 여전히 적용됩니다. vSphere 7.0 업데이트 2는 SEV-ES를 사용하도록 설정된 가상 시스템을 ESXi 호스트당 480개 지원합니다.

- 환경에서 실행하는 ESXi 호스트는 ESXi 7.0 업데이트 1 이상이어야 합니다.
- 게스트 운영 체제가 SEV-ES를 지원해야 합니다.

  현재는 SEV-ES를 지원하는 특정 Linux 커널만 지원됩니다.
- 가상 시스템은 하드웨어 버전 18 이상이어야 합니다.
- 가상 시스템에 **모든 게스트 메모리 예약** 옵션을 사용하도록 설정되어 있어야 합니다.그렇지 않으면 전원이 켜지지 않습니다.
- 환경에 액세스할 수 있는 시스템에 PowerCLI 12.1.0 이상을 설치해야 합니다.
- 가상 시스템의 전원이 꺼졌는지 확인합니다.

절차

1 PowerCLI 세션에서 `Connect-VIServer` cmdlet을 실행하여 SEV-ES를 추가할 가상 시스템이 있는 ESXi 호스트를 관리하는 vCenter Server에 관리자로 연결합니다.

  예:

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

2 `Set-VM` cmdlet을 사용하고 `-SEVEnabled $true`를 지정하여 가상 시스템에 SEV-ES를 추가합니다.

  예:

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

  가상 하드웨어 버전을 지정해야 하는 경우에는 `Set-VM` cmdlet을 `-HardwareVersion vmx-18` 매개 변수와 함께 실행합니다. 예:

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

결과

가상 시스템에 SEV-ES가 추가됩니다.

vSphere Client를 사용하여 가상 시스템에 AMD SEV-ES(Secure Encrypted Virtualization-Encrypted State)를 사용하지 않도록 설정

vSphere 7.0 업데이트 2 이상에서는 vSphere Client를 사용하여 가상 시스템에서 SEV-ES를 사용하지 않도록 설정할 수 있습니다.

사전 요구 사항

- 가상 시스템의 전원이 꺼졌는지 확인합니다.

절차

1. vSphere Client를 사용하여 vCenter Server에 연결합니다.
2. 인벤토리에서 수정할 가상 시스템을 마우스 오른쪽 버튼으로 클릭하고 **설정 편집**을 선택합니다.
3. **설정 편집** 대화 상자의 **VM 옵션 > 암호화**에서 AMD SEV-ES에 대한 **사용** 확인란의 선택을 취소합니다.
4. **확인**을 클릭합니다.

결과

가상 시스템에서 SEV-ES가 사용되지 않도록 설정됩니다.

가상 시스템에서 AMD SEV-ES(Secure Encrypted Virtualization-Encrypted State) 사용 안 함

가상 시스템에서 SEV-ES를 사용하지 않도록 설정할 수 있습니다.

사전 요구 사항

- 가상 시스템의 전원이 꺼졌는지 확인합니다.
- 환경에 액세스할 수 있는 시스템에 PowerCLI 12.1.0 이상을 설치해야 합니다.

절차

1. PowerCLI 세션에서 `Connect-VIServer` cmdlet을 실행하여 SEV-ES를 제거할 가상 시스템이 있는 ESXi 호스트를 관리하는 vCenter Server에 관리자로 연결합니다.

   예:

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

2. `Set-VM` cmdlet을 사용하고 `-SEVEnabled $false`를 지정하여 가상 시스템에서 SEV-ES를 사용하지 않도록 설정합니다.

   예를 들어, 먼저 호스트 정보를 변수에 할당한 다음, 가상 시스템에 대해 SEV-ES를 사용하지 않도록 설정합니다.

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

결과

가상 시스템에서 SEV-ES가 사용되지 않도록 설정됩니다.

가상 시스템 암호화

6

vSphere 가상 시스템 암호화를 사용하면 민감한 워크로드를 더욱 안전한 방식으로 암호화할 수 있습니다. 암호화 키에 대한 액세스를 ESXi 호스트가 신뢰할 수 있는 상태에 있다는 것을 조건으로 허용할 수 있습니다.

가상 시스템 암호화 작업을 시작하려면 먼저 키 제공자를 설정해야 합니다. 다음 키 제공자 유형을 사용할 수 있습니다.

표 6-1. vSphere 키 제공자

키 제공자	설명	추가 정보
표준 키 제공자	vSphere 6.5이상에서 사용할 수 있는 표준 키 제공자는 vCenter Server를 사용하여 외부 키 서버에서 키를 요청합니다. 키 서버가 키를 생성 및 저장하고 배포를 위해 vCenter Server에 키를 전달합니다.	장 7 표준 키 제공자 구성 및 관리의 내용을 참조하십시오.
신뢰할 수 있는 키 제공자	vSphere 7.0이상에서 사용할 수 있는 신뢰할 수 있는 vSphere 신뢰 기관 키 제공자는 워크로드 클러스터의 증명 상태에 따라 암호화 키에 액세스할 수 있도록 합니다. vSphere 신뢰 기관를 사용하려면 외부 키 서버가 필요합니다.	장 9 vSphere 신뢰 기관의 내용을 참조하십시오.
VMware vSphere® Native Key Provider™	vSphere 7.0 업데이트 2 이상에서 사용할 수 있는 vSphere Native Key Provider는 모든 vSphere 버전에 포함되어 있으며 외부 키 서버가 필요하지 않습니다.	장 8 vSphere Native Key Provider 구성 및 관리의 내용을 참조하십시오.

본 장은 다음 항목을 포함합니다.

- vSphere 키 제공자 비교
- vSphere 가상 시스템 암호화를 통해 환경을 보호하는 방법
- vSphere 가상 시스템 암호화 구성 요소
- 암호화 프로세스 흐름
- 가상 디스크 암호화
- 가상 시스템 암호화 오류

- 암호화 작업의 사전 요구 사항 및 필요한 권한
- vSphere vMotion 암호화
- 암호화 모범 사례, 주의 사항 및 상호 운용성
- 키 지속성 개요

vSphere 키 제공자 비교

vSphere 키 제공자의 기능에 대한 개략적인 개요를 검토하면 암호화 전략을 계획하는 데 도움이 됩니다.

일반적으로 키 제공자 일별 작업 간에 기능 또는 제품 지원의 차이는 거의 없습니다. 키 제공자의 모양과 동작은 유사하지만 다음 표에 나와 있는 것과 같이 키 제공자를 선택할 때 고려해야 할 요구 사항과 규정이 있을 수 있습니다.

표 6-2. 키 제공자 고려 사항

키 제공자	외부 키 서버 필요?	빠른 설정?	vSphere만 사용?
표준 키 제공자	예	아니요	아니요
신뢰할 수 있는 키 제공자	예	아니요	아니요
vSphere Native Key Provider	아니요	예	예

암호화 기능

다음 암호화 기능은 각 키 제공자 유형에서 지원됩니다.

- 동일한 키 제공자를 사용하여 키 재생성 또는 다른 키 제공자에 대해 키 재생성
- 키 순환
- vTPM(신뢰할 수 있는 가상 플랫폼 모듈)
- 디스크 암호화
- vSphere 가상 시스템 암호화
- 다른 키 제공자와 공존
- 다른 키 제공자로 업그레이드

vSphere 기능

다음은 몇 가지 중요 vSphere 기능에 대한 키 제공자 지원에 대해 설명합니다.

- 암호화된 vSphere vMotion: 모든 키 제공자 유형에서 지원됩니다. 대상 호스트에서 동일한 키 제공자를 사용할 수 있어야 합니다. vSphere vMotion 암호화의 내용을 참조하십시오.

- vCenter Server 파일 기반 백업 및 복원: 표준 키 제공자와 vSphere Native Key Provider는 vCenter Server 파일 기반 백업 및 복원을 지원합니다. 대부분의 vSphere 신뢰 기관 구성 정보는 ESXi 호스트에 저장되어 있기 때문에 vCenter Server 파일 기반 백업 메커니즘은 이 정보를 백업하지 않습니다. vSphere 신뢰 기관 배포에 대한 구성 정보가 저장되었는지 확인하려면 vSphere 신뢰 기관 구성 백업의 내용을 참조하십시오.

VMware 제품

다음 표에서는 몇몇 VMware 제품에 대한 키 제공자 지원을 비교합니다.

표 6-3. VMware 제품에 대한 지원 비교

키 제공자	vSAN	Site Recovery Manager	vSphere Replication
표준 키 제공자	예	예	예
신뢰할 수 있는 키 제공자	예	예 동일한 vSphere 신뢰 기관 서비스 구성을 복구 측에서 사용할 수 있는 경우 어레이 기반 복제가 있는 SRM이 지원됩니다.	아니요
vSphere Native Key Provider	예	예	예

필요한 하드웨어

다음 표에서는 몇 가지 최소 키 제공자 하드웨어 요구 사항을 비교합니다.

표 6-4. 필요한 하드웨어 비교

키 제공자	ESXi 호스트의 TPM
표준 키 제공자	필요하지 않음
신뢰할 수 있는 키 제공자	신뢰할 수 있는 호스트(신뢰할 수 있는 클러스터의 호스트)에 필요합니다. **참고** 현재 신뢰 기관 클러스터의 ESXi 호스트에는 TPM이 필요하지 않습니다. 하지만 모범 사례로서 TPM과 함께 새 ESXi 호스트 설치를 고려하십시오.
vSphere Native Key Provider	필요하지 않음 필요한 경우 vSphere Native Key Provider 가용성을 TPM이 있는 호스트로 제한할 수 있습니다.

키 제공자 이름 지정

vSphere는 키 제공자 이름을 사용하여 키 식별자를 조회합니다. 두 키 제공자의 이름이 같으면 vSphere는 두 키 제공자가 동일하고 동일한 키에 액세스할 수 있다고 가정합니다. 유형(표준 키 제공자, 신뢰할 수 있는 키 제공자 및 네이티브 키 제공자)에 관계없이 각 논리적 키 제공자는 모든 vCenter Server 시스템에서 고유한 이름이 있어야 합니다.

일부 인스턴스에서는 다음과 같이 여러 vCenter Server 시스템에 동일한 키 제공자를 구성합니다.

- vCenter Server 시스템 간에 암호화된 가상 시스템 마이그레이션
- vCenter Server를 재해 복구 사이트로 설정

vSphere 가상 시스템 암호화를 통해 환경을 보호하는 방법

사용 중인 키 제공자에 관계없이, vSphere 가상 시스템 암호화를 통해 암호화된 가상 시스템을 생성하고 기존 가상 시스템을 암호화할 수 있습니다. 중요한 정보가 포함되어 있는 모든 가상 시스템 파일이 암호화되므로 가상 시스템이 보호됩니다. 암호화 권한을 가진 관리자만 암호화 및 암호 해독 작업을 수행할 수 있습니다.

vSphere 가상 시스템 암호화에서 지원하는 스토리지

vSphere 가상 시스템 암호화는 VMware vSAN을 비롯하여 지원되는 모든 스토리지 유형(NFS, iSCSI, Fibre Channel, 직접 연결된 스토리지 등)에서 작동합니다. vSAN 클러스터에서의 암호화 사용에 대한 자세한 내용은 "VMware vSAN 관리" 설명서를 참조하십시오.

vSphere 가상 시스템 암호화 및 vSAN은 동일한 암호화 라이브러리를 사용하지만 서로 다른 프로파일을 가지고 있습니다. VM 암호화는 VM당 암호화이고 vSAN은 데이터스토어 수준 암호화입니다.

vSphere 암호화 키 및 키 제공자

vSphere는 KEK(키 암호화 키) 및 DEK(데이터 암호화 키)의 형태로 두 가지 암호화 수준을 사용합니다. 간단히 말해서, ESXi 호스트는 가상 시스템 및 디스크를 암호화하기 위해 DEK를 생성합니다. KEK는 키 서버에서 제공되며 DEK를 암호화(또는 "래핑")합니다. KEK는 AES256 알고리즘을 사용하여 암호화되고 DEK는 XTS-AES-256 알고리즘을 사용하여 암호화됩니다. 키 제공자의 유형에 따라 DEK 및 KEK를 생성하고 관리하는 데 다른 방법이 사용됩니다.

표준 키 제공자는 다음과 같이 작동합니다.

1 ESXi 호스트는 가상 시스템과 디스크를 암호화하기 위해 내부 키를 생성하고 사용합니다. 이러한 키는 DEK로 사용됩니다.

2 vCenter Server는 키 서버(KMS)에 키를 요청합니다. 이러한 키는 KEK로 사용됩니다. vCenter Server는 키 자체가 아니라 각 KEK의 ID만 저장합니다.

3 ESXi는 KEK를 사용하여 내부 키를 암호화하고, 암호화된 내부 키를 디스크에 저장합니다. ESXi는 KEK를 디스크에 저장하지 않습니다. 호스트가 재부팅되면 vCenter Server는 해당하는 ID를 가진 KEK를 키 서버에 요청하여 ESXi가 사용할 수 있도록 합니다. 그러면 ESXi는 필요에 따라 내부 키를 암호 해독합니다.

vSphere 신뢰 기관 신뢰할 수 있는 키 제공자는 다음과 같이 작동합니다.

1 신뢰할 수 있는 클러스터의 vCenter Server는 암호화된 가상 시스템이 생성될 ESXi 호스트에서 신뢰할 수 있는 기본 키 제공자에 액세스할 수 있는지 확인합니다.

2 신뢰할 수 있는 클러스터의 vCenter Server가 신뢰할 수 있는 키 제공자를 가상 시스템 ConfigSpec에 추가합니다.

3 가상 시스템 생성 요청이 ESXi 호스트로 전송됩니다.

4 ESXi 호스트가 아직 증명 토큰을 사용할 수 없는 경우 증명 서비스에서 하나를 요청합니다.

5 키 제공자 서비스가 증명 토큰을 검증하고 ESXi 호스트로 전송할 하나의 KEK를 생성합니다. KEK가 키 제공자에서 구성되는 기본 키로 래핑(암호화)됩니다. KEK 암호와 KEK 일반 텍스트가 모두 신뢰할 수 있는 호스트로 반환됩니다.

6 ESXi 호스트가 가상 시스템 디스크 암호화를 위해 DEK를 생성합니다.

7 KEK는 ESXi 호스트에서 생성한 DEK를 래핑하는 데 사용되며, 키 제공자의 암호는 암호화된 데이터와 함께 저장됩니다.

8 가상 시스템이 암호화되고 스토리지에 기록됩니다.

참고 암호화된 가상 시스템을 삭제하거나 등록 취소하면 ESXi 호스트와 클러스터가 캐시에서 KEK를 제거합니다. ESXi 호스트에서 더 이상 KEK를 사용할 수 없습니다. 이 동작은 표준 키 제공자 및 신뢰할 수 있는 키 제공자에 대해 동일합니다.

vSphere Native Key Provider는 다음과 같이 작동합니다.

1 키 제공자를 생성하면 vCenter Server가 기본 키를 생성한 후 클러스터의 ESXi 호스트에 푸시합니다. (외부 키 서버는 관여하지 않습니다.)

2 ESXi 호스트는 요청 시 DEK를 생성합니다.

3 암호화 작업을 수행하면 데이터가 DEK를 사용하여 암호화됩니다.

   암호화된 DEK는 암호화된 데이터와 함께 저장됩니다.

4 데이터를 암호 해독할 때 기본 키가 DEK를 암호 해독한 다음 데이터를 암호 해독하는 데 사용됩니다.

암호화 대상

vSphere 가상 시스템 암호화는 가상 시스템 파일, 가상 디스크 파일 및 코어 덤프 파일의 암호화를 지원합니다.

가상 시스템 파일

대부분의 가상 시스템 파일, 특히 VMDK 파일에 저장되지 않는 게스트 데이터가 암호화됩니다. 이 파일 집합에는 NVRAM, VSWP 및 VMSN 파일을 비롯하여 다양한 파일이 포함되나 이에 국한되지 않습니다. 키 제공자의 키가 내부 키와 기타 암호가 포함되어 있는 VMX 파일의 암호화된 번들을 잠금 해제합니다. 키 검색은 키 제공자에 따라 다음과 같이 작동합니다.

- 표준 키 제공자: vCenter Server가 키 서버의 키를 관리하고 ESXi 호스트가 키 제공자에 직접 액세스할 수 없습니다. 호스트가 vCenter Server가 키를 푸시할 때까지 기다립니다.
- 신뢰할 수 있는 키 제공자 및 vSphere Native Key Provider: ESXi 호스트가 키 제공자에 직접 액세스하여 vSphere 신뢰 기관 서비스에서 직접 또는 vSphere Native Key Provider에서 요청된 키를 가져옵니다.

vSphere Client를 사용하여 암호화된 가상 시스템을 생성하는 경우 가상 시스템 파일과는 별개로 가상 디스크를 암호화 및 암호 해독할 수 있습니다. 모든 가상 디스크가 기본적으로 암호화됩니다. 기존 가상 시스템을 암호화하는 것과 같은 기타 암호화 작업을 수행할 때는 가상 시스템 파일과는 별개로 가상 디스크를 암호화 및 암호 해독할 수 있습니다.

참고 암호화된 가상 디스크를 암호화되지 않은 가상 시스템과 연결할 수 없습니다.

가상 디스크 파일

암호화된 VMDK(가상 디스크) 파일 내의 데이터는 스토리지 또는 물리적 디스크에 일반 텍스트로 기록되지 않습니다. 또한 네트워크를 통해 일반 텍스트로 전송되는 경우도 절대 없습니다. VMDK 설명자 파일은 대부분 일반 텍스트이지만 암호화된 번들에 KEK의 키 ID와 내부 키(DEK)가 포함됩니다.

vSphere API를 사용하면 새 KEK로 얕은 이중 암호화 작업을 수행하거나 새 내부 키로 깊은 이중 암호화 작업을 수행할 수 있습니다.

코어 덤프

암호화 모드를 사용하도록 설정된 ESXi 호스트의 코어 덤프는 항상 암호화됩니다. vSphere 가상 시스템 암호화 및 코어 덤프의 내용을 참조하십시오. vCenter Server 시스템의 코어 덤프는 암호화되지 않습니다. vCenter Server 시스템에 대한 액세스를 보호합니다.

참고 vSphere 가상 시스템 암호화와 상호 운용될 수 있는 장치 및 기능과 관련된 몇 가지 제한 사항에 대한 자세한 내용은 가상 시스템 암호화 상호 운용성의 내용을 참조하십시오.

암호화되지 않는 대상

가상 시스템과 관련된 일부 파일은 암호화되지 않거나 부분적으로 암호화됩니다.

로그 파일

로그 파일은 중요한 데이터가 포함되지 않기 때문에 암호화되지 않습니다.

가상 시스템 구성 파일

VMX 및 VMSD 파일에 저장되는 대부분의 가상 시스템 구성 정보는 암호화되지 않습니다.

가상 디스크 설명자 파일

대부분의 가상 디스크 설명자 파일은 키 없이 디스크 관리 기능을 지원하기 위해 암호화되지 않습니다.

암호화 작업을 수행할 수 있는 사용자

암호화 작업 권한이 할당된 사용자만 암호화 작업을 수행할 수 있습니다. 이 권한 집합은 세분화되어 있습니다. 기본 관리자 시스템 역할에는 모든 **암호화 작업** 권한이 포함됩니다. [암호화 관리자 없음]이라는 역할은 **암호화 작업** 권한을 제외한 모든 관리자 권한을 지원합니다.

암호 사용자.* 권한 사용 외에도 vSphere Native Key Provider는 **Cryptographer.ReadKeyServersInfo** 권한을 사용할 수 있습니다. 이 권한은 vSphere Native Key Provider에 한정됩니다.

자세한 내용은 암호화 작업 권한의 내용을 참조하십시오.

추가적인 사용자 지정 역할을 생성할 수도 있습니다. 예를 들면 사용자 그룹이 가상 시스템을 암호화할 수 있도록 허용하고 가상 시스템을 암호 해독하지 못하게 방지할 수 있습니다.

암호화 작업을 수행하는 방법

vSphere Client에서는 다양한 암호화 작업을 지원합니다. 기타 작업은 vSphere API를 사용하여 수행할 수 있습니다.

표 6-5. 암호화 작업을 수행하기 위한 인터페이스

인터페이스	작업	정보
vSphere Client	암호화된 가상 시스템 생성 가상 시스템 암호화 및 암호 해독	본 설명서
PowerCLI	암호화된 가상 시스템 생성 가상 시스템 암호화 및 암호 해독 vSphere 신뢰 기관 구성	"VMware PowerCLI Cmdlets 참조"
vSphere Web Services SDK	암호화된 가상 시스템 생성 가상 시스템 암호화 및 암호 해독 가상 시스템의 깊은 이중 암호화 수행(다른 DEK 사용) 가상 시스템의 얕은 이중 암호화 수행(다른 KEK 사용)	"vSphere Web Services SDK 프로그래밍 가이드" "vSphere Web Services API 참조"
crypto-util	암호화된 코어 덤프 암호 해독 파일이 암호화되었는지 여부 확인 ESXi 호스트에서 직접 다른 관리 작업 수행	명령줄 도움말 vSphere 가상 시스템 암호화 및 코어 덤프

가상 시스템 이중 암호화

예를 들어 키가 만료되었거나 손상된 경우 새 키를 사용하여 가상 시스템을 이중 암호화할 수 있습니다. 다음 옵션을 사용할 수 있습니다.

- DEK(디스크 암호화 키) 및 KEK(키 암호화 키)를 모두 바꾸는 깊은 이중 암호화
- KEK만 바꾸는 얕은 이중 암호화

API를 사용하여 가상 시스템의 이중 암호화를 수행해야 합니다. "vSphere Web Services SDK 프로그래밍 가이드" 의 내용을 참조하십시오.

깊은 이중 암호화를 사용하려면 가상 시스템의 전원이 꺼져 있고 스냅샷이 없어야 합니다. 가상 시스템의 전원이 켜져 있고 가상 시스템에 스냅샷이 있다면 얕은 이중 암호화 작업을 수행할 수 있습니다. 스냅샷이 있는 암호화된 가상 시스템의 얕은 이중 암호화는 단일 스냅샷 분기(디스크 체인)에서만 허용됩니다. 여러 개의 스냅샷 분기는 지원되지 않습니다. 또한 가상 시스템 또는 디스크의 연결된 복제에서는 얕은 이중 암호화가 지원되지 않습니다. 새 KEK를 사용하여 체인에 있는 모든 링크를 업데이트하기 전에 얕은 이중 암호화가 실패하는 경우 이전 및 새 KEK가 있다면 암호화된 가상 시스템에 계속 액세스할 수 있습니다. 하지만 스냅샷 작업을 수행하기 전에 얕은 이중 암호화 작업을 다시 실행하는 것이 좋습니다.

vSphere 가상 시스템 암호화 구성 요소

사용하는 키 제공자에 따라 외부 키 서버, vCenter Server 시스템 및 ESXi 호스트가 잠재적으로 암호화 솔루션에 영향을 미칩니다.

다음 구성 요소는 vSphere 가상 시스템 암호화를 구성합니다.

- KMS라고도 하는 외부 키 서버(vSphere Native Key Provider에는 필요하지 않음)
- vCenter Server
- ESXi 호스트

키 서버

키 서버는 키 제공자와 연결된 KMIP(Key Management Interoperability Protocol) 관리 서버입니다. 표준 키 제공자 및 신뢰할 수 있는 키 제공자에는 키 서버가 필요합니다. vSphere Native Key Provider에는 키 서버가 필요하지 않습니다. 다음 표에서는 키 제공자 및 키 서버 상호 작용의 차이점에 대해 설명합니다.

표 6-6. 키 제공자 및 키 서버 상호 작용

키 제공자	키 서버와의 상호 작용
표준 키 제공자	표준 키 제공자는 vCenter Server를 사용하여 키 서버에서 키를 요청합니다. 키 서버가 키를 생성 및 저장하고 ESXi 호스트에 배포하기 위해 vCenter Server에 키를 전달합니다.
신뢰할 수 있는 키 제공자	신뢰할 수 있는 키 제공자는 신뢰할 수 있는 ESXi 호스트가 키를 직접 가져오도록 하는 키 제공자 서비스를 사용합니다. vSphere 신뢰 기관 키 제공자 서비스란?의 내용을 참조하십시오.
vSphere Native Key Provider	vSphere Native Key Provider에는 키 서버가 필요하지 않습니다. vCenter Server에서 기본 키를 생성하고 이를 ESXi 호스트로 푸시합니다. 그러면 ESXi 호스트가 데이터 암호화 키를 생성합니다(vCenter Server에 연결되어 있지 않은 경우에도). vSphere Native Key Provider 개요의 내용을 참조하십시오.

vSphere Client 또는 vSphere API를 사용하여 키 제공자 인스턴스를 vCenter Server 시스템에 추가할 수 있습니다. 여러 키 제공자 인스턴스를 사용하는 경우 모두 동일한 벤더의 인스턴스여야 하며 모든 인스턴스는 키를 복제해야 합니다.

다양한 환경에서 다양한 키 서버 벤더를 사용하는 환경인 경우 각 키 서버에 대해 키 제공자를 추가하고 기본 키 제공자를 지정할 수 있습니다. 첫 번째로 추가한 키 제공자는 기본 키 제공자가 됩니다. 기본값은 나중에 명시적으로 지정할 수 있습니다.

KMIP 클라이언트인 vCenter Server는 선택한 키 서버를 쉽게 사용할 수 있도록 KMIP(Key Management Interoperability Protocol)를 사용합니다.

vCenter Server

다음 표에서는 암호화 프로세스에서 vCenter Server의 역할에 대해 설명합니다.

표 6-7. 키 제공자 및 vCenter Server

키 제공자	vCenter Server의 역할	권한 확인 방법
표준 키 제공자	vCenter Server에만 키 서버에 로그인하기 위한 자격 증명이 있습니다. ESXi 호스트에는 이러한 자격 증명이 없습니다. vCenter Server는 키 서버에서 키를 가져와 ESXi 호스트로 푸시합니다. vCenter Server는 키 서버 키를 저장하지 않지만 키 ID 목록은 보관합니다.	vCenter Server는 암호화 작업을 수행하는 사용자의 권한을 확인합니다.
신뢰할 수 있는 키 제공자	vSphere 신뢰 기관는 vCenter Server가 키 서버에서 키를 요청하지 않도록 하고, 워크로드 클러스터의 증명 상태에 따라 암호화 키에 액세스할 수 있도록 합니다. 신뢰할 수 있는 클러스터 및 신뢰 기관 클러스터에 대해 별도의 vCenter Server 시스템을 사용해야 합니다.	vCenter Server는 암호화 작업을 수행하는 사용자의 권한을 확인합니다. 신뢰할 수 있는 관리자 SSO 그룹의 멤버인 사용자만 관리 작업을 수행할 수 있습니다.
vSphere Native Key Provider	vCenter Server에서 키를 생성합니다.	vCenter Server는 암호화 작업을 수행하는 사용자의 권한을 확인합니다.

vSphere Client를 사용하여 암호화 작업 권한을 할당하거나 사용자 그룹에 **암호화 관리자 아님** 사용자 지정 역할을 할당할 수 있습니다. 암호화 작업의 사전 요구 사항 및 필요한 권한의 내용을 참조하십시오.

vCenter Server는 vSphere Client 이벤트 콘솔에서 보고 내보낼 수 있는 이벤트 목록에 암호화 이벤트를 추가합니다. 각 이벤트에는 사용자, 시간, 키 ID와 암호화 작업이 포함됩니다.

키 서버의 키는 KEK(키 암호화 키)로 사용됩니다.

ESXi 호스트

ESXi 호스트는 암호화 워크플로의 여러 측면을 담당합니다.

표 6-8. ESXi 호스트

키 제공자	ESXi 호스트 측면
표준 키 제공자	■ vCenter Server는 ESXi 호스트에 키가 필요할 때 키를 푸시합니다. 호스트가 암호화 모드를 사용하도록 설정되어 있어야 합니다. 현재 사용자의 역할에 암호화 작업 권한이 포함되어 있어야 합니다. 암호화 작업의 사전 요구 사항 및 필요한 권한 및 암호화 작업 권한 항목을 참조하십시오. ■ 암호화된 가상 시스템의 게스트 데이터가 디스크에 저장될 때 암호화되는지 확인합니다. ■ 암호화된 가상 시스템의 게스트 데이터가 암호화 없이 네트워크를 통해 전송되지 않는지 확인합니다.
신뢰할 수 있는 키 제공자	ESXi 호스트는 신뢰할 수 있는 호스트인지 아니면 신뢰 기관 호스트인지에 따라 vSphere 신뢰 기관 서비스를 실행합니다. 신뢰할 수 있는 ESXi 호스트는 신뢰 기관 호스트에서 게시한 키 제공자로 암호화할 수 있는 워크로드 가상 시스템을 실행합니다. 신뢰할 수 있는 인프라 개요의 내용을 참조하십시오.
vSphere Native Key Provider	ESXi 호스트는 vSphere Native Key Provider에서 키를 직접 가져옵니다.

ESXi 호스트가 생성하는 키는 이 문서에서 내부 키라고 합니다. 이러한 키는 일반적으로 DEK(데이터 암호화 키)로 작동합니다.

암호화 프로세스 흐름

키 제공자를 설정한 후 필요한 권한이 있는 사용자는 암호화된 가상 시스템과 디스크를 생성할 수 있습니다. 또한 이러한 사용자는 기존의 가상 시스템을 암호화하고, 암호화된 가상 시스템의 암호를 해독하며, 가상 시스템에 vTPM(신뢰할 수 있는 가상 플랫폼 모듈)을 추가할 수도 있습니다.

키 제공자 유형에 따라 프로세스 흐름에 키 서버, vCenter Server 및 ESXi 호스트가 포함될 수 있습니다.

표준 키 제공자 암호화 프로세스 흐름

암호화 과정에서 여러 vSphere 구성 요소가 다음과 같이 상호 작용합니다.

1 사용자가 암호화된 가상 시스템 생성과 같은 암호화 작업을 수행하는 경우 vCenter Server는 기본 키 서버에서 새 키를 요청합니다. 이 키가 KEK로 사용됩니다.

2 vCenter Server가 키 ID를 저장하고 ESXi 호스트에 키를 전달합니다. ESXi 호스트가 클러스터의 일부인 경우 vCenter Server가 KEK를 클러스터 내 각 호스트에 전송합니다.

   키 자체는 vCenter Server 시스템에 저장되어 있지 않습니다. 키 ID만 알려져 있습니다.

3 ESXi 호스트는 가상 시스템과 해당 디스크에 대한 내부 키(DEK)를 생성합니다. 내부 키를 메모리에만 유지하고 KEK를 사용하여 내부 키를 암호화합니다.

   암호화되지 않은 내부 키는 디스크에 저장되지 않습니다. 암호화된 데이터만 저장됩니다. KEK는 키 서버에서 전송되므로 호스트는 계속 동일한 KEK를 사용합니다.

4 ESXi 호스트는 암호화된 내부 키를 사용하여 가상 시스템을 암호화합니다.

KEK가 있고 암호화된 키 파일에 액세스할 수 있는 모든 호스트는 암호화된 가상 시스템 또는 디스크에 대한 작업을 수행할 수 있습니다.

신뢰할 수 있는 키 제공자 암호화 프로세스 흐름

vSphere 신뢰 기관 암호화 프로세스 흐름에는 vSphere 신뢰 기관 서비스, 신뢰할 수 있는 키 제공자, vCenter Server 및 ESXi 호스트가 포함됩니다.

신뢰할 수 있는 키 제공자를 사용하여 가상 시스템을 암호화하는 것은 표준 키 제공자를 사용할 때의 가상 시스템 암호화 사용자 환경과 동일합니다. vSphere 신뢰 기관에서의 가상 시스템 암호화는 가상 시스템 암호화 시점을 결정하기 위해 가상 시스템 암호화 스토리지 정책 또는 vTPM 디바이스의 존재 여부에 계속 의존합니다. vSphere Client에서 가상 시스템을 암호화할 때에는 여전히 기본 구성된 키 제공자(vSphere 6.5 및 6.7에서는 KMS 클러스터라고 함)를 사용합니다. 또한 유사한 방식으로 API를 사용하여 키 제공자를 수동으로 지정할 수 있습니다. vSphere 6.5용으로 추가된 기존의 암호화 권한은 vSphere 신뢰 기관과 관련하여 여전히 vSphere 7.0에서도 유효합니다.

신뢰할 수 있는 키 제공자에 대한 암호화 프로세스에는 표준 키 제공자의 경우와 다른 몇 가지 중요한 차이점이 있습니다.

- 신뢰 기관 관리자는 vCenter Server 인스턴스에 대해 키 서버를 설정할 때 정보를 직접 지정하지 않으며 키 서버 신뢰를 설정하지 않습니다. 대신, vSphere 신뢰 기관에서 신뢰할 수 있는 호스트가 사용할 수 있는 신뢰할 수 있는 키 제공자를 게시합니다.
- vCenter Server는 더 이상 키를 ESXi 호스트로 푸시하지 않으며 대신 각각의 신뢰할 수 있는 키 제공자를 단일 최상위 키로 처리할 수 있습니다.
- 신뢰할 수 있는 호스트만 신뢰 기관 호스트의 암호화 작업을 요청할 수 있습니다.

vSphere Native Key Provider 암호화 프로세스 흐름

vSphere Native Key Provider는 7.0 업데이트 2 릴리스부터 vSphere에 포함됩니다. vSphere Native Key Provider를 구성하면 vCenter Server에서 기본 키를 클러스터의 모든 ESXi 호스트로 푸시합니다. 마찬가지로 vSphere Native Key Provider를 업데이트하거나 삭제하면 변경 내용이 클러스터의 호스트로 푸시됩니다. 암호화 프로세스 흐름은 신뢰할 수 있는 키 제공자가 작동하는 방식과 유사합니다. 차이점은 vSphere Native Key Provider의 경우 키를 생성하고 이를 기본 키로 래핑한 다음 다시 전달하여 암호화를 수행한다는 것입니다.

키 서버의 사용자 지정 특성

KMIP(Key Management Interoperability Protocol)는 벤더 특정 목적에 사용할 사용자 지정 특성의 추가를 지원합니다. 사용자 지정 특성을 사용하면 키 서버에 저장된 키를 보다 구체적으로 식별할 수 있습니다. vCenter Server는 가상 시스템 키 및 호스트 키에 대해 다음과 같은 사용자 지정 특성을 추가합니다.

표 6-9. 가상 시스템 암호화 사용자 지정 특성

사용자 지정 특성	값
x-Vendor	VMware, Inc.
x-Product	VMware vSphere
x-Product_Version	vCenter Server 버전
x-Component	가상 시스템
x-Name	가상 시스템 이름(ConfigInfo 또는 ConfigSpec에서 수집)
x-Identifier	가상 시스템의 인스턴스 UUID(ConfigInfo 또는 ConfigSpec에서 수집)

표 6-10. 호스트 암호화 사용자 지정 특성

사용자 지정 특성	값
x-Vendor	VMware, Inc.
x-Product	VMware vSphere
x-Product_Version	vCenter Server 버전
x-Component	ESXi 서버
x-Name	호스트 이름
x-Identifier	호스트의 하드웨어 UUID

vCenter Server는 키 서버에서 키를 생성할 때 x-Vendor, x-Product 및 x-Product_Version 특성을 추가합니다. 키를 사용하여 가상 시스템 또는 호스트를 암호화할 때 vCenter Server는 x-Component, x-Identifier 및 x-Name 특성을 설정합니다. 키 서버 사용자 인터페이스에서 이러한 사용자 지정 특성을 볼 수 있습니다. 키 서버 벤더에 확인하십시오.

호스트 키와 가상 시스템 키에는 각각 6개의 사용자 지정 특성이 있습니다. x-Vendor, x-Product 및 x-Product_Version은 두 키 모두에 대해 동일할 수 있습니다. 이러한 특성은 키가 생성될 때 설정됩니다. 키의 대상이 가상 시스템인지 아니면 호스트인지에 따라 x-Component, x-Identifier 및 x-Name 특성이 추가될 수 있습니다.

키 오류

키 서버에서 ESXi 호스트로 키를 전송하는 동안 오류가 발생하면 vCenter Server는 이벤트 로그에 다음 이벤트에 대한 메시지를 생성합니다.

- 호스트 연결 또는 호스트 지원 문제로 ESXi 호스트에 키를 추가하지 못했습니다.
- 키 서버에 키가 없어서 키 서버에서 키를 가져오지 못했습니다.
- 키 서버 연결로 인해 키 서버에서 키를 가져오지 못했습니다.

암호화된 가상 시스템 암호 해독

나중에 암호화된 가상 시스템의 암호를 해독하려는 경우 스토리지 정책을 변경합니다. 가상 시스템과 모든 디스크에 대한 스토리지 정책을 변경할 수 있습니다. 개별 구성 요소의 암호를 해독하려는 경우 먼저 선택한 디스크의 암호를 해독한 후 VM 홈에 대한 스토리지 정책을 변경하여 가상 시스템의 암호를 해독합니다. 각 구성 요소의 암호 해독에 두 키가 모두 필요합니다. 암호화된 가상 시스템 또는 가상 디스크 암호 해독의 내용을 참조하십시오.

가상 디스크 암호화

vSphere Client에서 암호화된 가상 시스템을 생성하는 경우 암호화에서 제외할 디스크를 결정할 수 있습니다. 이후에 디스크를 추가하고 암호화 정책을 설정할 수 있습니다. 암호화된 디스크를 암호화되지 않은 가상 시스템에 추가할 수 없으며, 가상 시스템이 암호화되지 않은 경우 디스크를 암호화할 수 없습니다.

가상 시스템과 디스크 암호화는 스토리지 정책을 통해 제어됩니다. VM 홈에 대한 스토리지 정책은 가상 시스템 자체를 제어하며 각 가상 디스크에는 연결된 스토리지 정책이 있습니다.

- VM 홈의 스토리지 정책을 암호화 정책으로 설정하면 가상 시스템만 암호화됩니다.
- VM 홈과 모든 디스크의 스토리지 정책을 암호화 정책으로 설정하면 모든 구성 요소가 암호화됩니다.

다음 사용 사례를 고려하십시오.

표 6-11. 가상 디스크 암호화 사용 사례

사용 사례	세부 정보
암호화된 가상 시스템을 생성합니다.	암호화된 가상 시스템을 생성하는 동안 디스크를 추가할 경우 디스크가 기본적으로 암호화됩니다. 하나 이상의 디스크를 암호화하지 않도록 정책을 변경할 수 있습니다. 가상 시스템을 생성한 후 각 디스크에 대한 스토리지 정책을 명시적으로 변경할 수 있습니다. 가상 디스크에 대한 암호화 정책 변경의 내용을 참조하십시오.
가상 시스템을 암호화합니다.	기존 가상 시스템을 암호화하려면 스토리지 정책을 변경합니다. 가상 시스템과 모든 가상 디스크에 대한 스토리지 정책을 변경할 수 있습니다. 가상 시스템만 암호화하려는 경우 VM 홈에 대한 암호화 정책을 지정하고 각 가상 디스크에 대해 다른 스토리지 정책(예: 데이터스토어 기본값)을 선택할 수 있습니다. 암호화된 가상 시스템 생성의 내용을 참조하십시오.
기존의 암호화되지 않은 디스크를 암호화된 가상 시스템에 추가합니다(암호화 스토리지 정책).	오류 메시지와 함께 실패합니다. 기본 스토리지 정책을 사용하여 디스크를 추가해야 하지만 이후에 스토리지 정책을 변경할 수 있습니다. 가상 디스크에 대한 암호화 정책 변경의 내용을 참조하십시오.
암호화가 포함되지 않은 스토리지 정책(예: 데이터스토어 기본값)을 사용하여 암호화된 가상 시스템에 기존 암호화되지 않은 디스크를 추가합니다.	디스크에서 기본 스토리지 정책을 사용합니다. 암호화된 디스크를 원하는 경우 디스크를 추가한 후에 스토리지 정책을 명시적으로 변경할 수 있습니다. 가상 디스크에 대한 암호화 정책 변경의 내용을 참조하십시오.
암호화된 가상 시스템에 암호화된 디스크를 추가합니다. VM 홈 스토리지 정책은 암호화입니다.	디스크를 추가할 때 디스크가 암호화됩니다. vSphere Client는 암호화 상태를 비롯한 크기 및 기타 특성을 표시합니다.

표 6-11. 가상 디스크 암호화 사용 사례 (계속)

사용 사례	세부 정보
암호화되지 않은 가상 시스템에 암호화된 기존 디스크를 추가합니다.	이 사용 사례는 지원되지 않습니다.
암호화된 가상 시스템 등록	암호화된 가상 시스템을 vCenter Server에서 제거해도 디스크에서 삭제하지 않으면, VM의 가상 시스템 구성(vmx) 파일을 등록하여 vCenter Server 인벤토리로 반환할 수 있습니다. 암호화된 VM을 등록하려면 사용자에게 **암호화 작업.VM 등록** 권한이 있어야 합니다. VM이 표준 키 제공자를 사용하여 암호화된 경우, 암호화된 VM을 등록하면 vCenter Server가 필수 키를 ESXi 호스트로 푸시합니다. VM을 등록하는 사용자에게 **암호화 작업.VM 등록** 권한이 없으면, vCenter Server는 등록 시 VM을 잠그고 잠금이 해제될 때까지 VM을 사용할 수 없습니다. VM이 신뢰할 수 있는 키 제공자 또는 vSphere Native Key Provider를 사용하여 암호화된 경우, 암호화된 VM이 등록되면 vCenter Server는 키를 ESXi 호스트로 더 이상 푸시하지 않습니다. 대신 VM이 등록될 때 호스트에서 키를 가져옵니다. VM을 등록하는 사용자에게 **암호화 작업.VM 등록** 권한이 없으면 vCenter Server는 작업을 허용하지 않습니다.

가상 시스템 암호화 오류

vCenter Server가 가상 시스템 암호화에서 심각한 오류를 감지하면 이벤트를 생성합니다. 이러한 이벤트를 보면 암호화 오류를 해결하는 데 도움이 됩니다.

vCenter Server는 다음과 같은 심각한 가상 시스템 암호화 오류에 대해 이벤트를 생성합니다.

- KEK를 생성하지 못했습니다.
- 데이터스토어에 디스크 공간이 부족하여 암호화된 가상 시스템을 생성할 수 없습니다.
- 사용자 권한이 부족하여 암호화 작업을 시작할 수 없습니다.
- 키 제공자에 지정된 키가 없어서 ESXi 호스트 키가 새 키로 갱신됩니다.
- 지정된 키가 있는 키 제공자에서 오류가 발생하여 ESXi 호스트 키가 새 키로 갱신됩니다.

암호화 작업의 사전 요구 사항 및 필요한 권한

암호화 작업은 vCenter Server가 포함된 환경에서만 가능합니다. 또한 ESXi 호스트에서 대부분의 암호화 작업에 대해 암호화 모드를 사용하도록 설정해야 합니다. 작업을 수행하는 사용자에게 적절한 권한이 있어야 합니다. **암호화 작업** 권한 집합을 통해 권한 부여를 세부적으로 제어할 수 있습니다. 가상 시스템 암호화 작업에서 호스트 암호화 모드를 변경해야 할 경우 추가 권한이 필요합니다.

참고 vSphere 신뢰 기관에는 추가적인 사전 요구 사항 및 필요한 권한이 있습니다. vSphere 신뢰 기관에 대한 사전 요구 사항 및 필요한 권한의 내용을 참조하십시오.

암호화 권한 및 역할

기본적으로 vCenter Server 관리자 역할의 사용자는 모든 권한을 갖습니다. **암호화 관리자 없음** 역할은 암호화 작업에 필요한 다음 권한을 갖지 않습니다.

- **암호화 작업** 권한을 추가합니다.
- **글로벌.진단**
- **호스트.인벤토리.클러스터에 호스트 추가**
- **호스트.인벤토리.독립형 호스트 추가**
- **호스트.로컬 작업.사용자 그룹 관리**

암호화 작업 권한이 필요 없는 vCenter Server 관리자에게 **암호화 관리자 없음** 역할을 할당할 수 있습니다.

사용자가 수행할 수 있는 작업을 추가로 제한하기 위해 **암호화 관리자 없음** 역할을 복제하여 일부 **암호화 작업** 권한만 가진 사용자 지정 역할을 생성할 수 있습니다. 예를 들어 사용자가 가상 시스템을 암호화할 수 있지만 암호를 해독할 수 없도록 하는 역할을 생성할 수 있습니다. 역할을 사용하여 권한 할당의 내용을 참조하십시오.

호스트 암호화 모드

호스트 암호화 모드는 ESXi 호스트가 가상 시스템 및 가상 디스크를 암호화하기 위한 암호화 자료를 수락할 준비가 되었는지 여부를 결정합니다. 호스트에서 암호화 작업을 수행하려면 먼저 호스트 암호화 모드를 사용하도록 설정해야 합니다. 호스트 암호화 모드는 종종 필요할 때 자동으로 사용되도록 설정되지만 명시적으로 사용하도록 설정할 수 있습니다. vSphere Client 또는 vSphere API를 사용하여 현재 호스트 암호화 모드를 확인하고 명시적으로 설정할 수 있습니다.

호스트 암호화 모드를 사용하도록 설정하면 vCenter Server가 호스트에 호스트 키를 설치하며, 이는 호스트의 암호화가 "안전"함을 보장합니다. 호스트 키가 올바르게 있으면 vCenter Server가 키 제공자에서 키를 가져와 ESXi 호스트에 푸시하는 등의 다른 암호화 작업을 진행할 수 있습니다.

"안전" 모드에서는 사용자 월드(즉, hostd) 및 암호화된 가상 시스템의 코어 덤프가 암호화됩니다. 암호화되지 않은 가상 시스템의 코어 덤프는 암호화되지 않습니다.

암호화된 코어 덤프 및 VMware 기술 지원에서 암호화된 코어 덤프를 사용하는 방법에 대한 자세한 내용은 VMware 기술 자료 문서(http://kb.vmware.com/kb/2147388)를 참조하십시오.

자세한 내용은 호스트 암호화 모드를 사용하도록 명시적으로 설정의 내용을 참조하십시오.

호스트 암호화 모드를 사용하도록 설정한 경우 사용하지 않도록 설정하기가 쉽지 않습니다. API를 사용하여 호스트 암호화 모드 사용 안 함의 내용을 참조하십시오.

암호화 작업에서 호스트 암호화 모드를 사용하도록 설정하려고 하면 자동 변경이 이루어집니다. 예를 들어 암호화된 가상 시스템을 독립형 호스트에 추가할 때 호스트 암호화 모드가 사용되도록 설정되지 않은 경우, 호스트에 대한 필요한 권한이 있으면 암호화 모드가 자동으로 사용으로 변경됩니다.

클러스터에 호스트 A, B, C의 세 ESXi 호스트가 있고 호스트 A에 암호화된 가상 시스템을 생성할 경우 이루어지는 작업은 몇 가지 요소에 따라 달라집니다.

- 호스트 A, B, C가 이미 암호화를 사용하도록 설정된 경우 가상 시스템을 생성하기 위해 **암호화 작업.새 항목 암호화** 권한만 필요합니다.
- 호스트 A와 B는 암호화를 사용하도록 설정되고 C는 사용하도록 설정되지 않은 경우 다음과 같이 진행됩니다.
  - 각 호스트에 **암호화 작업.새 항목 암호화**와 **암호화 작업.호스트 등록** 권한이 모두 있는 경우, 가상 시스템 생성 중에 호스트 C에서 암호화를 사용하도록 설정됩니다. 암호화 프로세스를 통해 호스트 C에서 호스트 암호화 모드를 사용하도록 설정되고 클러스터의 각 호스트에 키가 푸시됩니다.

    이 경우에도 호스트 C에서 호스트 암호화를 사용하도록 명시적으로 설정할 수 있습니다.
  - 가상 시스템 또는 가상 시스템 폴더에 **암호화 작업.새 항목 암호화** 권한만 있는 경우, 가상 시스템 생성이 성공하고 호스트 A와 호스트 B에서 키를 사용할 수 있게 되며, 호스트 C는 암호화를 사용하지 않도록 유지되고 가상 시스템 키를 갖지 않습니다.
- 암호화가 사용되도록 설정된 호스트가 없고 호스트 A에 **암호화 작업.호스트 등록** 권한이 있는 경우 가상 시스템 생성 중에 해당 호스트에서 호스트 암호화가 사용되도록 설정됩니다. 그렇지 않은 경우 오류가 발생합니다.
- 또한 vSphere API를 사용하여 클러스터의 암호화 모드를 "강제 사용"으로 설정할 수 있습니다. 강제 사용은 클러스터의 모든 호스트가 암호적으로 "안전한" 상태가 되도록 합니다. 즉, vCenter Server에서 호스트에 호스트 키를 설치합니다. "vSphere Web Services SDK 프로그래밍 가이드" 의 내용을 참조하십시오.

디스크 공간 요구 사항

기존 가상 시스템을 암호화하는 경우 해당 가상 시스템이 현재 사용하는 공간보다 두 배 이상 많은 공간이 필요합니다.

vSphere vMotion 암호화

vSphere vMotion은 암호화된 가상 시스템을 마이그레이션할 때 항상 암호화를 사용합니다. 암호화되지 않은 가상 시스템의 경우 암호화된 vSphere vMotion 옵션 중 하나를 선택할 수 있습니다.

암호화된 vSphere vMotion은 vSphere vMotion을 통해 전송되는 데이터의 기밀성, 무결성 및 신뢰성을 보장합니다. vSphere는 vCenter Server 인스턴스 간에 암호화되지 않은 또는 암호화된 가상 시스템의 암호화된 vMotion을 지원합니다.

암호화 대상

암호화된 디스크의 경우 데이터는 모든 경우에 암호화된 상태로 전송됩니다. 암호화되지 않은 디스크의 경우 다음이 적용됩니다.

- 디스크 데이터가 호스트 내에서 전송되는 경우(즉 호스트를 변경하지 않음) 데이터스토어만 변경하면 암호화되지 않은 상태로 전송됩니다.

- 호스트 간에 디스크 데이터가 전송되고 암호화된 vMotion이 사용되는 경우 전송이 암호화됩니다. 암호화된 vMotion을 사용하지 않는 경우 전송은 암호화되지 않습니다.

암호화된 가상 시스템의 경우 vSphere vMotion을 사용한 마이그레이션에서 항상 암호화된 vSphere vMotion을 사용합니다. 암호화된 가상 시스템에 대해 암호화된 vSphere vMotion을 해제할 수 없습니다.

암호화된 vSphere vMotion 상태

암호화되지 않은 가상 시스템의 경우 암호화된 vSphere vMotion을 다음 상태 중 하나로 설정할 수 있습니다. 기본값은 [편의적]입니다.

사용 안 함

암호화된 vSphere vMotion을 사용하지 않습니다.

편의적

소스 및 대상 호스트가 지원하는 경우 암호화된 vSphere vMotion을 사용합니다. ESXi 버전 6.5 이상에서만 암호화된 vSphere vMotion을 사용합니다.

필수

암호화된 vSphere vMotion만 허용합니다. 소스 또는 대상 호스트가 암호화된 vSphere vMotion을 지원하지 않으면 vSphere vMotion을 사용한 마이그레이션이 허용되지 않습니다.

가상 시스템을 암호화하는 경우 가상 시스템이 현재 암호화된 vSphere vMotion 설정 기록을 유지합니다. 이후에 해당 가상 시스템에 대한 암호화를 사용하지 않도록 설정할 경우 설정을 명시적으로 변경할 때까지 암호화된 vMotion 설정이 [필수]로 유지됩니다. **설정 편집**을 사용하여 설정을 변경할 수 있습니다.

암호화되지 않은 가상 시스템에 암호화된 vSphere vMotion을 사용하거나 사용하지 않도록 설정하는 방법에 대한 자세한 내용은 "vCenter Server 및 호스트 관리" 설명서를 참조하십시오.

참고 현재는 vCenter Server 인스턴스 전체에서 암호화된 가상 시스템을 마이그레이션하거나 복제하려면 vSphere API를 사용해야 합니다. "vSphere Web Services SDK 프로그래밍 가이드" 및 "vSphere Web Services API 참조" 를 참조하십시오.

vCenter Server 인스턴스 간에 암호화된 가상 시스템 마이그레이션 또는 복제

vSphere vMotion은 vCenter Server 인스턴스 간에 암호화된 가상 시스템의 마이그레이션 및 복제를 지원합니다.

vCenter Server 인스턴스 간에 암호화된 가상 시스템을 마이그레이션 또는 복제할 때 소스 및 대상 vCenter Server 인스턴스는 가상 시스템을 암호화하는 데 사용된 키 제공자를 공유하도록 구성되어야 합니다. 또한 키 제공자 이름은 소스 및 대상 vCenter Server 인스턴스에서 동일해야 하며 다음과 같은 특징을 가져야 합니다.

- 표준 키 제공자: 동일한 키 서버가 키 제공자에 있어야 합니다.
- 신뢰할 수 있는 키 제공자: 동일한 vSphere 신뢰 기관 서비스를 대상 호스트에 구성해야 합니다.

- vSphere Native Key Provider: 동일한 KDK를 가져야 합니다.

대상 vCenter Server는 대상 ESXi 호스트에서 암호화 모드를 사용하도록 설정하여 호스트가 암호적으로 "안전한" 상태가 되도록 합니다.

vSphere vMotion을 사용하여 vCenter Server 인스턴스 간에 암호화된 가상 시스템을 마이그레이션 또는 복제할 때에는 다음 권한이 필요합니다.

- 마이그레이션: 가상 시스템에 대한 **암호화 작업.마이그레이션**
- 복제: 가상 시스템에 대한 **암호화 작업.복제**

또한 대상 vCenter Server에도 **암호화 작업.EncryptNew** 권한이 있어야 합니다. 대상 ESXi 호스트가 "안전" 모드가 아닌 경우 **암호화 작업.RegisterHost** 권한도 대상 vCenter Server에 있어야 합니다.

동일한 vCenter Server 또는 vCenter Server 인스턴스 간에 가상 시스템(암호화되거나 암호화되지 않은 경우)을 마이그레이션할 때는 특정 작업이 허용되지 않습니다.

- VM 스토리지 정책을 변경할 수 없습니다.
- 키 변경을 수행할 수 없습니다.

참고 가상 시스템을 복제하는 동안 VM 스토리지 정책을 변경할 수 있습니다.

vCenter Server 인스턴스 간에 암호화된 가상 시스템을 마이그레이션 또는 복제하기 위한 최소 요구 사항

vSphere vMotion을 사용하여 vCenter Server 인스턴스 간에 표준 키 제공자로 암호화된 가상 시스템을 마이그레이션하거나 복제하기 위한 최소 버전 요구 사항은 다음과 같습니다.

- 소스 및 대상 vCenter Server 인스턴스는 7.0 이상 버전에 있어야 합니다.
- 소스 및 대상 ESXi 호스트는 6.7 이상 버전에 있어야 합니다.

vSphere vMotion을 사용하여 vCenter Server 인스턴스 간에 신뢰할 수 있는 키 제공자로 암호화된 가상 시스템을 마이그레이션하거나 복제하기 위한 최소 버전 요구 사항은 다음과 같습니다.

- vSphere 신뢰 기관 서비스가 대상 호스트에 대해 구성되어야 하며 대상 호스트가 증명되어야 합니다.
- 마이그레이션 시 암호화를 변경할 수 없습니다. 예를 들어 가상 시스템이 새 스토리지로 마이그레이션되는 동안은 암호화되지 않은 디스크를 암호화할 수 없습니다.
- 표준 암호화된 가상 시스템을 신뢰할 수 있는 호스트로 마이그레이션할 수 있습니다. 키 제공자 이름은 소스 및 대상 vCenter Server 인스턴스에서 동일해야 합니다.
- vSphere 신뢰 기관 암호화된 가상 시스템을 신뢰할 수 있는 호스트가 아닌 호스트로 마이그레이션할 수 없습니다.

신뢰할 수 있는 키 제공자 vMotion 및 크로스 vCenter Server vMotion

신뢰할 수 있는 키 제공자는 ESXi 호스트 전체에서 vMotion을 완전하게 지원합니다.

크로스 vCenter Server vMotion도 지원되지만 다음과 같은 제한 사항이 있습니다.

1 필요한 신뢰할 수 있는 서비스가 대상 호스트에 대해 구성되어야 하며 대상 호스트가 증명되어야 합니다.

2 마이그레이션 시 암호화를 변경할 수 없습니다. 예를 들어 디스크는 가상 시스템이 새 스토리지로 마이그레이션되는 동안 암호화될 수 없습니다.

크로스 vCenter Server vMotion을 수행할 때, vCenter Server는 대상 호스트에서 신뢰할 수 있는 키 제공자를 사용할 수 있는지 그리고 호스트가 해당 키 제공자에 액세스할 수 있는지 확인합니다.

vSphere Native Key Provider vMotion 및 크로스 vCenter Server vMotion

vSphere Native Key Provider는 ESXi 호스트 전체에서 vMotion 및 암호화된 vMotion을 지원합니다. 크로스 vCenter Server vMotion은 vSphere Native Key Provider가 대상 호스트에서 구성된 경우에 지원됩니다.

암호화 모범 사례, 주의 사항 및 상호 운용성

물리적 시스템의 암호화에 적용되는 모든 모범 사례와 주의 사항이 가상 시스템 암호화에도 적용됩니다. 또한 가상 시스템 암호화 아키텍처에는 몇 가지 추가 권장 사항이 있습니다. 가상 시스템 암호화 전략을 계획할 때는 상호 운용성 제한 사항을 고려해야 합니다.

참고 vSphere 신뢰 기관 상호 운용성에 대한 자세한 내용은 vSphere 신뢰 기관 모범 사례, 주의 사항 및 상호 운용성 항목을 참조하십시오.

가상 시스템 암호화 모범 사례

`vm-support` 번들을 생성할 때와 같이 나중에 문제를 방지하려면 가상 시스템 암호화 모범 사례를 따르십시오.

일반 모범 사례

문제를 방지하려면 다음과 같은 일반적인 모범 사례를 따르십시오.

- vCenter Server Appliance 가상 시스템은 암호화하지 마십시오.
- ESXi 호스트에서 오류가 발생하면 가능한 한 빨리 지원 번들을 검색합니다. 암호를 사용하는 지원 번들을 생성하거나 코어 덤프의 암호를 해독하려는 경우 호스트 키를 사용할 수 있어야 합니다. 호스트가 재부팅되면 호스트 키가 변경될 수 있고 사용자는 더 이상 해당 호스트 키를 사용하여 암호를 사용하는 지원 번들을 생성하거나 지원 번들의 코어 덤프 암호를 해독할 수 없습니다.
- 키 제공자 이름을 주의하여 관리합니다. 키 제공자 이름이 이미 사용 중인 키 서버에 대해 변경되면 해당 키 서버의 키로 암호화된 모든 VM은 전원 켜기 또는 등록 중에 잠긴 상태로 전환됩니다. 이 경우 키 서버를 vCenter Server에서 제거하고 처음에 사용한 키 제공자 이름과 함께 키 서버를 추가합니다.
- VMX 파일 및 VMDK 설명자 파일을 편집하지 마십시오. 이러한 파일에는 암호화 번들이 포함되어 있습니다. 변경하면 가상 시스템을 복구할 수 없고 복구 문제를 수정하지 못할 수 있습니다.

- vSphere 가상 시스템 암호화 프로세스는 데이터를 스토리지에 쓰기 전에 호스트의 데이터를 암호화합니다. 이러한 방식으로 가상 시스템을 암호화할 때 중복 제거, 압축, 복제 등과 같은 백엔드 스토리지 기능의 효율성이 영향을 받을 수 있습니다.
- vSphere 가상 시스템 암호화 및 게스트 내 암호화(BitLocker, dm-crypt 등)와 같은 여러 암호화 계층을 사용하는 경우 암호화 프로세스가 CPU 및 메모리 리소스를 추가로 사용하기 때문에 전반적인 가상 시스템 성능이 영향을 받을 수 있습니다.
- vSphere 가상 시스템 암호화로 암호화된 가상 시스템의 복제된 복사본이 복구 사이트의 암호화 키에 액세스할 수 있는지 확인합니다. 표준 키 제공자의 경우 이 사항은 vSphere 외부에서 키 관리 시스템 설계의 일부로 처리됩니다. vSphere Native Key Provider의 경우 네이티브 키 제공자 키의 백업 복사본이 존재하고 손실로부터 보호되는지 확인합니다. 자세한 내용은 vSphere Native Key Provider 백업의 내용을 참조하십시오.
- 암호화에는 많은 CPU가 사용됩니다. AES-NI는 암호화 성능을 크게 개선합니다. BIOS에서 AES-NI를 사용하도록 설정하십시오.

암호화된 코어 덤프의 모범 사례

문제를 진단하기 위해 코어 덤프를 검사할 때 문제를 방지할 수 있도록 다음 모범 사례를 따릅니다.

- 코어 덤프에 대한 정책을 설정합니다. 코어 덤프는 키 등 중요한 정보를 포함할 수 있기 때문에 암호화됩니다. 코어 덤프의 암호를 해독하는 경우 이를 중요한 정보로 간주하십시오. ESXi 코어 덤프에는 ESXi 호스트의 키와 호스트에 있는 가상 시스템의 키가 포함될 수 있습니다. 코어 덤프 암호를 해독한 후에는 호스트 키를 변경하고 암호화된 가상 시스템을 이중 암호화하는 것이 좋습니다. 두 작업 모두 vSphere API를 사용하여 수행할 수 있습니다.

  자세한 내용은 vSphere 가상 시스템 암호화 및 코어 덤프 항목을 참조하십시오.
- `vm-support` 번들을 수집할 때 항상 암호를 사용합니다. vSphere Client에서 지원 번들을 생성할 때 또는 `vm-support` 명령을 사용하여 암호를 지정할 수 있습니다.

  암호는 암호에 기반한 키를 사용하기 위해 내부 키를 사용하는 코어 덤프를 이중 암호화합니다. 나중에 지원 번들에 포함되었을 수도 있는 암호화된 코어 덤프의 암호를 해독하는 데 이 암호를 사용할 수 있습니다. 암호화되지 않은 코어 덤프 및 로그는 암호 옵션 사용의 영향을 받지 않습니다.
- `vm-support` 번들 생성 동안 지정하는 암호는 vSphere 구성 요소에서 지속되지 않습니다. 지원 번들용 암호를 추적하는 것은 사용자의 책임입니다.
- 호스트 키를 변경하기 전에 암호를 사용하는 `vm-support` 번들을 생성합니다. 나중에 이 암호를 사용하여 이전 호스트 키로 암호화되었을 수 있는 코어 덤프에 액세스할 수 있습니다.

키 수명주기 관리 모범 사례

키 서버 가용성을 보장하고 키 서버의 키를 모니터링하는 모범 사례를 구현합니다.

- 키 서버 가용성을 보장하는 정책을 갖추는 것은 사용자의 책임입니다.

키 서버를 사용할 수 없는 경우 vCenter Server가 키 서버에서 키를 요청하도록 요구하는 가상 시스템 작업은 불가능합니다. 즉, 실행 중인 가상 시스템은 계속 실행되며 해당 가상 시스템의 전원을 켜고, 끄고, 재구성할 수 있습니다. 하지만 해당 가상 시스템을 키 정보가 없는 호스트에 재배치할 수 없습니다.

대부분의 키 서버 솔루션에는 고가용성 기능이 포함되어 있습니다. vSphere Client 또는 API를 사용하여 키 제공자 및 연결된 키 서버를 지정할 수 있습니다.

참고 버전 7.0 업데이트 2부터는 키 서버가 일시적으로 오프라인 상태이거나 사용할 수 없는 경우에도 암호화된 가상 시스템과 가상 TPM이 계속 작동할 수 있습니다. ESXi 호스트는 암호화 키를 계속 유지하여 암호화 및 vTPM 작업을 계속할 수 있습니다. 키 지속성 개요의 내용을 참조하십시오.

- 기존 가상 시스템에 대한 키가 활성 상태가 아닌 경우 키를 추적하고 업데이트 적용을 수행하는 것은 사용자의 책임입니다.

  KMIP 표준은 키에 대해 다음 상태를 정의합니다.

  - 활성 전
  - 활성
  - 비활성화됨
  - 손상됨
  - 제거됨
  - 제거됨 손상됨

  vSphere 가상 시스템 암호화는 암호화에 활성 키만 사용합니다. 키가 활성 전인 경우 vSphere 가상 시스템 암호화가 이를 활성화시킵니다. 키 상태가 비활성화됨, 손상됨, 제거됨, 제거됨 손상됨인 경우 해당 키로 가상 시스템 또는 디스크를 암호화할 수 없습니다.

  키가 다른 상태인 경우 해당 키를 사용하는 가상 시스템은 계속 작동합니다. 복제 또는 마이그레이션 작업의 성공 여부는 키가 이미 호스트에 있는지 여부에 따라 다릅니다.

  - 키가 대상 호스트에 있으면 키 서버에서 키가 활성 상태가 아니어도 작업이 성공합니다.
  - 필요한 가상 시스템 및 가상 디스크 키가 대상 호스트에 없으면 vCenter Server는 키 서버에서 키를 가져와야 합니다. 키 상태가 비활성화됨, 손상됨, 제거됨, 제거됨 손상됨인 경우 vCenter Server는 오류를 표시하고 작업은 실패합니다.

  키가 이미 호스트에 있으면 복제 또는 마이그레이션 작업이 성공합니다. vCenter Server가 키 서버에서 키를 끌어와야 할 경우 작업이 실패합니다.

  키가 활성 상태가 아닌 경우 API를 사용하여 작업 키를 재생성합니다. "vSphere Web Services SDK 프로그래밍 가이드" 를 참조하십시오.

- 특정 시간 이후에 키가 회수되고 롤오버되도록 키 순환 정책을 개발합니다.
  - 신뢰할 수 있는 키 제공자: 신뢰할 수 있는 키 제공자의 기본 키를 변경합니다.
  - vSphere Native Key Provider: vSphere Native Key Provider의 `key_id`를 변경합니다.

백업 및 복원 모범 사례

백업 및 복원 작업에 대한 정책을 설정합니다.

- 모든 백업 아키텍처가 지원되지는 않습니다. 가상 시스템 암호화 상호 운용성의 내용을 참조하십시오.
- 복원 작업에 대한 정책을 설정합니다. 백업은 항상 일반 텍스트 형식이므로 복원이 완료된 즉시 가상 시스템을 암호화하도록 계획합니다. 복원 작업의 일부로 가상 시스템이 암호화되도록 지정할 수 있습니다. 가능한 경우 복원 프로세스의 일부로 가상 시스템을 암호화하여 중요한 정보의 노출을 방지합니다. 가상 시스템과 관련된 디스크에 대한 암호화 정책을 변경하려면 디스크에 대한 스토리지 정책을 변경합니다.
- VM 홈 파일이 암호화되어 있기 때문에 복원 시 암호화 키를 사용할 수 있는지 확인합니다.

성능 모범 사례

- 암호화 성능은 CPU 및 스토리지 속도에 따라 다릅니다.
- 기존 가상 시스템을 암호화하면 생성 중인 가상 시스템을 암호화하는 것보다 더 많은 시간이 소요됩니다. 가능하면 가상 시스템 생성 시 암호화하십시오.

스토리지 정책 모범 사례

번들 VM 암호화 샘플 스토리지 정책을 수정하지 마십시오. 대신 해당 정책을 복제하고 그 복제본을 편집합니다.

참고 VM 암호화 정책을 원래 설정으로 되돌리는 자동화된 방법은 없습니다.

스토리지 정책을 사용자 지정하는 자세한 내용은 "vSphere 스토리지" 설명서를 참조하십시오.

암호화 키 제거 모범 사례

클러스터에서 암호화 키를 제거하려면 암호화된 가상 시스템을 삭제, 등록 취소 또는 다른 vCenter Server로 이동한 후 클러스터에서 ESXi 호스트를 재부팅합니다.

가상 시스템 암호화 주의 사항

나중에 문제를 방지하려면 가상 시스템 암호화 주의 사항을 검토하십시오.

가상 시스템 암호화에 사용할 수 없는 디바이스 및 기능을 이해하려면 가상 시스템 암호화 상호 운용성을 참조하십시오.

제한 사항

가상 시스템 암호화 전략을 계획할 때 다음 주의 사항을 고려합니다.

- 암호화된 가상 시스템을 복제하거나 Storage vMotion 작업을 수행할 때 디스크 형식 변경을 시도해 볼 수 있습니다. 이러한 변환이 항상 성공하는 것은 아닙니다. 예를 들어 가상 시스템을 복제하고 느리게 비워지는 씩 형식에서 씬 형식으로 디스크 형식을 변경하려는 경우 가상 시스템 디스크는 느리게 비워지는 씩 형식을 유지합니다.

- 디스크를 가상 시스템에서 분리하면 가상 디스크에 대한 스토리지 정책 정보는 유지되지 않습니다.
  - 가상 디스크가 암호화된 경우 암호화를 포함하는 스토리지 정책 또는 VM 암호화 정책으로 스토리지 정책을 명시적으로 설정해야 합니다.
  - 가상 디스크가 암호화되지 않은 경우 디스크를 가상 시스템에 추가할 때 스토리지 정책을 변경할 수 있습니다.

  자세한 내용은 가상 디스크 암호화 항목을 참조하십시오.
- 가상 시스템을 다른 클러스터로 이동하기 전에 코어 덤프의 암호를 해독합니다.

  vCenter Server는 KMS 키를 저장하지 않고 키 ID를 추적하기만 합니다. 따라서 vCenter Server는 ESXi 호스트 키를 지속적으로 저장하지 않습니다.

  특정 상황에서, 예를 들어 ESXi 호스트를 다른 클러스터로 이동하고 해당 호스트를 재부팅하는 경우 vCenter Server는 호스트에 새 호스트 키를 할당합니다. 새 호스트 키로 기존 코어 덤프의 암호를 해독할 수 없습니다.
- OVF 내보내기는 암호화된 가상 시스템에 대해 지원되지 않습니다.
- VMware Host Client를 사용하여 암호화된 가상 시스템을 등록하는 것은 지원되지 않습니다.

가상 시스템 잠김 상태

가상 시스템 키 또는 하나 이상의 가상 디스크 키가 분실된 경우 가상 시스템은 잠김 상태로 전환됩니다. 잠김 상태에서는 가상 시스템 작업을 수행할 수 없습니다.

- vSphere Client의 가상 시스템과 해당 디스크를 모두 암호화하는 경우 동일한 키가 사용됩니다.
- API를 사용하여 암호화를 수행하면 가상 시스템과 디스크에 대해 다른 암호화 키를 사용할 수 있습니다. 이런 경우 가상 시스템의 전원을 켜려고 하는데 디스크 키 중 하나가 없는 경우 전원 켜기 작업이 실패합니다. 가상 디스크를 제거하면 가상 시스템의 전원을 켤 수 있습니다.

문제 해결 제안 사항은 없는 키 문제 해결의 내용을 참조하십시오.

가상 시스템 암호화 상호 운용성

vSphere 가상 시스템 암호화에는 상호 운용할 수 있는 디바이스 및 기능에 관한 몇 가지 제한 사항이 있습니다.

다음 제한 사항 및 설명은 vSphere 가상 시스템 암호화사용에 관한 것입니다. vSAN 암호화 사용에 대한 유사한 정보는 "VMware vSAN 관리" 설명서를 참조하십시오.

특정 암호화 작업에 대한 제한 사항

암호화된 가상 시스템에서 특정 작업을 수행할 때 몇 가지 제한 사항이 적용됩니다.

- 전원이 켜진 가상 시스템에서는 대부분의 암호화 작업을 수행할 수 없습니다. 가상 시스템의 전원을 꺼야 합니다. 가상 시스템의 전원이 켜져 있는 동안에는 암호화된 가상 시스템을 복제하고 단순 암호 해독을 수행할 수 있습니다.

- 스냅샷이 포함된 가상 시스템에서 깊은 이중 암호화를 수행할 수 없습니다. 스냅샷이 포함된 가상 시스템에서 얕은 이중 암호화를 수행할 수 있습니다.

신뢰할 수 있는 가상 플랫폼 모듈 디바이스 및 vSphere 가상 시스템 암호화

vTPM(가상의 신뢰할 수 있는 플랫폼 모듈)은 물리적 TPM(신뢰할 수 있는 플랫폼 모듈) 2.0 칩의 소프트웨어 기반 표현입니다. 새 가상 시스템 또는 기존 가상 시스템에 vTPM을 추가할 수 있습니다. 가상 시스템에 vTPM을 추가하려면 vSphere 환경에서 키 제공자를 구성해야 합니다. vTPM을 구성할 때 가상 시스템 "홈" 파일(메모리 스왑, NVRAM 파일 등)이 암호화됩니다. 디스크 파일 또는 VMDK 파일은 자동으로 암호화되지 않습니다. 가상 시스템 디스크에 대해 명시적으로 암호화를 추가하도록 선택할 수 있습니다.

경고 가상 시스템을 복제하면 vTPM과 같은 가상 디바이스를 포함하여 전체 가상 시스템이 복제됩니다. vTPM에 저장된 정보(소프트웨어가 시스템의 ID를 확인하는 데 사용할 수 있는 vTPM의 속성을 포함)도 복제됩니다.

vSphere 가상 시스템 암호화 및 일시 중단 상태 및 스냅샷

암호화된 가상 시스템의 일시 중단된 상태에서 재개하거나 암호화된 시스템의 메모리 스냅샷으로 되돌릴 수 있습니다. 메모리 스냅샷이 있고 일시 중단된 상태인 암호화된 가상 시스템을 ESXi 호스트 간에 마이그레이션할 수 있습니다.

vSphere 가상 시스템 암호화 및 IPv6

IPv6 전용 모드 또는 혼합 모드에서 vSphere 가상 시스템 암호화 기능을 사용할 수 있습니다. IPv6 주소를 사용하여 키 서버를 구성할 수 있습니다. IPv6 주소만 사용하여 vCenter Server 및 키 서버를 모두 구성할 수 있습니다.

vSphere 가상 시스템 암호화의 복제에 대한 제한 사항

특정 복제 기능은 vSphere 가상 시스템 암호화에서 작동하지 않습니다.

- 표준 키 제공자의 경우 복제가 조건부로 지원됩니다.
  - 전체 복제가 지원됩니다. 복제는 키를 포함하여 상위 암호화 상태를 상속합니다. 전체 복제를 암호화하고 전체 복제를 다시 암호화하여 새 키를 사용하거나 해당 전체 복제의 암호를 해독할 수 있습니다.

    연결된 복제는 지원되며 복제는 키를 포함하여 상위 암호화 상태를 상속받습니다. 연결된 복제의 암호를 해독하거나 다른 키를 사용하여 연결된 복제를 다시 암호화할 수 없습니다.

    참고 다른 애플리케이션이 연결된 복제를 지원하는지 확인합니다. 예를 들어 VMware Horizon® 7은 전체 복제와 즉시 복제를 모두 지원하지만 연결된 복제는 지원하지 않습니다.
- 신뢰할 수 있는 키 제공자 또는 vSphere Native Key Provider의 경우 복제가 지원되지만 복제 시 암호화 키를 변경할 수 없습니다. 이 동작은 클론을 생성할 때 키를 변경할 수 있는 표준 암호화와 대비됩니다. 다음 작업은 가상 시스템의 복제 중 vSphere 신뢰 기관 또는 vSphere Native Key Provider에서 지원되지 않습니다.
  - 암호화되지 않은 가상 시스템에서 암호화된 가상 시스템으로 복제

  - 암호화된 가상 시스템에서 복제 및 암호화 키 변경
  - 암호화된 가상 시스템에서 암호화되지 않은 가상 시스템으로 복제
- [즉시 복제]는 모든 키 제공자 유형에서 지원되지만 복제 시 암호화 키를 변경할 수는 없습니다.

vSphere 가상 시스템 암호화로 지원되지 않는 디스크 구성

특정 유형의 가상 시스템 디스크 구성은 vSphere 가상 시스템 암호화로 지원되지 않습니다.

- RDM(원시 디바이스 매핑). 하지만 vVols(vSphere Virtual Volumes)는 지원됩니다.
- 다중 작성기 또는 공유 디스크(MSCS, WSFC 또는 Oracle RAC). 암호화된 가상 시스템 "홈" 파일은 다중 작성기 디스크에 대해 지원됩니다. 다중 작성기 디스크에는 암호화된 가상 디스크가 지원되지 않습니다. 암호화된 가상 디스크가 있는 가상 시스템의 **설정 편집** 페이지에서 다중 작성기를 선택하려고 하면 **확인** 버튼이 비활성화되어 있습니다.

vSphere 가상 시스템 암호화의 기타 제한 사항

vSphere 가상 시스템 암호화와 함께 작동하지 않는 기타 기능은 다음과 같습니다.

- vSphere ESXi Dump Collector
- 컨텐츠 라이브러리
  - 컨텐츠 라이브러리는 OVF 템플릿 유형과 VM 템플릿 유형의 두 가지 템플릿 유형을 지원합니다. 암호화된 가상 시스템은 OVF 템플릿 유형으로 내보낼 수 없습니다. OVF Tool은 암호화된 가상 시스템을 지원하지 않습니다. VM 템플릿 유형을 사용하여 암호화된 VM 템플릿을 생성할 수 있습니다. "vSphere 가상 시스템 관리" 설명서를 참조하십시오.
- 암호화된 가상 디스크를 백업하기 위한 소프트웨어는 VADP(VMware vSphere Storage API - Data Protection)를 사용하여 SSL을 사용하도록 설정한 상태에서 무중단 추가 모드 또는 NBD 모드로 디스크를 백업해야 합니다. 단, 가상 디스크 백업에 VADP를 사용하는 백업 솔루션이 모두 지원되는 것은 아닙니다. 자세한 내용은 백업 벤더에 문의하십시오.
  - VADP SAN 전송 모드 솔루션은 암호화된 가상 디스크 백업용으로 지원되지 않습니다.
  - VADP 무중단 추가 솔루션은 암호화된 가상 디스크에 대해 지원됩니다. 백업 소프트웨어는 무중단 추가 백업 워크플로의 일부로 사용되는 프록시 VM의 암호화를 지원해야 합니다. 벤더에게 **Cryptographic Operations.Encrypt Virtual Machine** 권한이 있어야 합니다.
  - 암호화된 가상 디스크 백업에는 NBD-SSL 전송 모드를 사용하는 백업 솔루션이 지원됩니다. 벤더 애플리케이션에 **Cryptographic Operations.Direct Access** 권한이 있어야 합니다.
- 암호화된 가상 시스템에서 직렬 포트 또는 병렬 포트로 출력을 전송할 수 없습니다. 구성이 성공한 것으로 보이는 경우에도 출력은 파일로 전송됩니다.
- vSphere 가상 시스템 암호화는 VMware Cloud on AWS에서 지원되지 않습니다. "VMware Cloud on AWS 데이터 센터 관리" 설명서를 참조하십시오.

키 지속성 개요

vSphere 7.0 업데이트 2 이상에서는 키 서버가 일시적으로 오프라인 상태이거나 사용할 수 없는 경우에도 암호화된 가상 시스템과 가상 TPM이 선택적으로 계속 작동할 수 있습니다. ESXi 호스트는 암호화 키를 계속 유지하여 암호화 및 vTPM 작업을 계속할 수 있습니다.

vSphere 7.0 업데이트 2 이전의 경우 암호화된 가상 시스템 및 vTPM을 사용하려면 키 서버가 항상 작동되어야 합니다. vSphere 7.0 업데이트 2 이상에서는 키 서버에 대한 액세스가 중단된 경우에도 암호화된 디바이스를 작동할 수 있습니다.

vSphere 7.0 업데이트 3부터는 키 제공자에 대한 액세스가 중단된 경우에도 암호화된 vSAN 클러스터가 작동할 수 있습니다.

참고 vSphere Native Key Provider를 사용하는 경우 키 지속성이 필요하지 않습니다. vSphere Native Key Provider는 키 서버에 액세스할 필요 없이 바로 실행되도록 설계되었습니다. "키 지속성 및 vSphere Native Key Provider" 섹션을 참조하십시오.

ESXi 호스트의 키 지속성

표준 키 제공자를 사용하는 경우 ESXi 호스트는 vCenter Server에 의존하여 암호화 키를 관리합니다. 신뢰할 수 있는 키 제공자를 사용하는 경우 ESXi 호스트는 신뢰 기관 호스트에 직접 의존하며 vCenter Server는 관련되지 않습니다.

ESXi 호스트는 키 제공자 유형에 관계없이 처음에 키를 가져와서 해당 키 캐시에 유지합니다. ESXi 호스트가 재부팅되면 해당 키 캐시가 손실됩니다. 그러면 ESXi 호스트가 키 서버(표준 키 제공자) 또는 신뢰 기관 호스트(신뢰할 수 있는 키 제공자)에서 키를 다시 요청합니다. ESXi 호스트에서 키를 가져오려고 할 때 그리고 키 서버가 오프라인 상태이거나 키 서버에 연결할 수 없는 경우 vTPM 및 워크로드 암호화는 작동하지 않습니다. 일반적으로 키 서버가 사이트에 배포되지 않는 Edge 형식 배포인 경우 키 서버에 대한 연결이 끊기면 암호화된 워크로드에 대한 불필요한 다운타임이 발생할 수 있습니다.

vSphere 7.0 업데이트 2 이상에서는 키 서버가 오프라인 상태이거나 키 서버에 연결할 수 없는 경우에도 암호화된 워크로드가 계속 작동할 수 있습니다. 호스트에 ESXi TPM이 있는 경우 재부팅 시 암호화 키가 TPM에 유지됩니다. 따라서 ESXi 호스트가 재부팅되어도 호스트에서 암호화 키를 요청할 필요가 없습니다. 또한 키가 TPM에 유지되므로 키 서버를 사용할 수 없는 경우에도 암호화 및 암호 해독 작업을 계속할 수 있습니다. 기본적으로 키 서버 또는 신뢰 기관 호스트를 사용할 수 없을 때에는 "키 서버 없이" 암호화된 워크로드를 계속 실행할 수 있습니다. 또한 마찬가지로 vTPM은 키 서버에 연결할 수 없는 경우에도 계속 작동할 수 있습니다.

키 지속성 및 vSphere Native Key Provider

vSphere Native Key Provider를 사용하는 경우 vSphere에서 암호화 키를 생성하며 키 서버가 필요하지 않습니다. ESXi 호스트는 다른 키를 파생시키는 데 사용되는 KDK(Key Derivation Key)를 가져옵니다. KDK를 수신하고 다른 키를 생성한 후 ESXi 호스트는 암호화 작업을 수행하기 위해 vCenter Server에 액세스할 필요가 없습니다. 기본적으로 vSphere Native Key Provider는 항상 "키 서버 없이" 실행됩니다.

KDK는 재부팅 후에도 기본적으로 ESXi 호스트에서 유지되며 호스트 재부팅 후 vCenter Server를 사용할 수 없는 경우에도 마찬가지입니다.

vSphere Native Key Provider를 사용하여 키 지속성을 활성화할 수 있지만 일반적으로 필요하지는 않습니다. ESXi 호스트는 vSphere Native Key Provider에 대한 전체 액세스 권한이 있으므로 키의 추가 지속성은 중복됩니다. vSphere Native Key Provider를 사용하여 키 지속성을 활성화하는 한 가지 사용 사례는 표준 키 제공자(외부 KMIP 서버)도 구성된 경우입니다.

키 지속성을 설정하는 방법

키 지속성을 사용하거나 사용하지 않도록 설정하려면 ESXi 호스트에서 키 지속성 사용 및 사용 안 함의 내용을 참조하십시오.

표준 키 제공자 구성 및 관리

7

vSphere 환경에서 표준 키 제공자를 사용하려면 몇 가지 준비가 필요합니다. 환경을 설정한 후 암호화된 가상 시스템과 가상 디스크를 생성하고 기존 가상 시스템과 디스크를 암호화할 수 있습니다.

표준 키 제공자에 대해 환경을 설정한 후 vSphere Client를 사용하여 암호화된 가상 시스템과 가상 디스크를 생성하고 기존 가상 시스템과 디스크를 암호화할 수 있습니다. 장 10 vSphere 환경에서 암호화 사용의 내용을 참조하십시오.

API 및 crypto-util CLI를 사용하여 추가 작업을 수행할 수 있습니다. API 설명서는 "vSphere Web Services SDK 프로그래밍 가이드" 의 내용을, 해당 도구에 대한 세부 정보는 `crypto-util` 명령줄 도움말을 참조하십시오.

본 장은 다음 항목을 포함합니다.

- 표준 키 제공자 개요
- 표준 키 제공자 설정
- 서로 다른 사용자를 위해 별도의 키 제공자 설정

표준 키 제공자 개요

표준 키 제공자를 사용하여 가상 시스템 암호화 작업을 수행할 수 있습니다.

표준 키 제공자란?

vSphere에서 표준 키 제공자는 키 서버에서 암호화 키를 직접 가져오고 vCenter Server는 데이터 센터의 필수 ESXi 호스트에 키를 배포합니다.

서로 다른 사용자를 위해 별도의 표준 키 제공자를 추가하고 기본 표준 키 제공자를 설정할 수 있습니다.

vSphere 표준 키 제공자 요구 사항

- vSphere 6.5 이상
- 외부 키 서버(KMS)

키 관리 서버는 KMIP(Key Management Interoperability Protocol) 1.1 표준을 지원해야 합니다. 자세한 내용은 "vSphere 호환성 매트릭스" 항목을 참조하십시오.

플랫폼 및 컴퓨팅 아래에 있는 VMware 호환성 가이드에서 VMware 인증 KMS 벤더에 대한 정보를 찾을 수 있습니다. 호환성 가이드를 선택하면 KMS(키 관리 서버)의 호환성 설명서를 열 수 있습니다. 이 설명서는 자주 업데이트됩니다.

표준 키 제공자 권한

표준 키 제공자는 **Cryptographer.*** 권한을 사용합니다. 암호화 작업 권한의 내용을 참조하십시오.

표준 키 제공자 설정

가상 시스템 암호화 작업을 시작하려면 먼저 표준 키 제공자를 설정해야 합니다.

표준 키 제공자 설정에는 키 제공자를 추가하고 키 서버와 신뢰를 설정하는 것이 포함됩니다. 키 제공자를 추가할 때 해당 키 제공자를 기본값으로 설정하라는 메시지가 표시됩니다. 명시적으로 기본 키 제공자를 변경할 수 있습니다. vCenter Server가 기본 키 제공자에서 키를 프로비저닝합니다.

참고 vSphere 6.5 및 6.7에서 키 관리 서버 클러스터라고 했던 것을 이제 키 제공자라고 합니다.

(가상 시스템 암호화 표준 키 제공자 설정)

vSphere Client를 사용하여 표준 키 제공자 추가

vSphere Client 또는 공용 API를 사용하여 vCenter Server 시스템에 표준 키 제공자를 추가할 수 있습니다.

vSphere Client를 사용하면 표준 키 제공자를 vCenter Server 시스템에 추가하고 키 서버와 vCenter Server 간에 신뢰를 설정할 수 있습니다.

- 동일한 벤더의 여러 키 서버를 추가할 수 있습니다.
- 환경에서 여러 벤더의 솔루션을 지원하는 경우 여러 키 제공자를 추가할 수 있습니다.
- 환경에 여러 키 제공자가 포함되어 있을 때 기본 키 제공자를 삭제하는 경우 다른 기본값을 명시적으로 설정해야 합니다.
- IPv6 주소를 사용하여 키 서버를 구성할 수 있습니다.
  - IPv6 주소만 사용하여 vCenter Server 시스템과 키 서버를 모두 구성할 수 있습니다.

사전 요구 사항

- 키 서버(KMS)가 "KMS(키 관리 서버)용 VMware 호환성 가이드" 에 있고 KMIP 1.1을 준수하며 대칭 키 Foundry 및 서버가 될 수 있는지 확인합니다.
- 필요한 권한이 있는지 확인합니다. **암호화 작업.키 서버 관리**.

- 키 서버가 고가용성인지 확인합니다. 정전 또는 재해 복구 이벤트 동안과 같이 키 서버에 대한 연결이 끊어지면 암호화된 가상 시스템에 액세스할 수 없게 됩니다.

  참고 vSphere 7.0 업데이트 2부터는 키 서버가 일시적으로 오프라인 상태이거나 사용할 수 없는 경우에도 암호화된 가상 시스템과 가상 TPM이 계속 작동할 수 있습니다. 키 지속성 개요의 내용을 참조하십시오.

- 키 서버에 대한 인프라의 종속성을 신중하게 고려합니다. 일부 KMS 솔루션은 가상 장치로 제공되므로 종속성 루프 또는 잘못된 KMS 장치 배치와 관련한 기타 가용성 문제를 생성할 수 있습니다.

절차

1 vSphere Client를 사용하여 vCenter Server 시스템에 로그인합니다.

2 인벤토리 목록을 찾아서 vCenter Server 인스턴스를 선택합니다.

3 **구성**을 클릭하고 **보안**에서 **키 제공자**를 클릭합니다.

4 **표준 키 제공자 추가**를 클릭하고 키 제공자 정보를 입력합니다.

옵션	값
이름	키 제공자의 이름입니다. 유형(표준 키 제공자, 신뢰할 수 있는 키 제공자 및 네이티브 키 제공자)에 관계없이 각 논리적 키 제공자는 모든 vCenter Server 시스템에서 고유한 이름이 있어야 합니다. 자세한 내용은 키 제공자 이름 지정의 내용을 참조하십시오.
KMS	키 서버(KMS)의 별칭입니다.
주소	키 서버의 IP 주소 또는 FQDN입니다.
포트	vCenter Server에서 키 서버에 연결할 포트입니다.
프록시 서버	키 서버에 연결하기 위한 선택적 프록시 서버 주소입니다.
프록시 포트	키 서버에 연결하기 위한 선택적 프록시 포트입니다.
사용자 이름	일부 키 서버 벤더에서는 사용자가 사용자 이름과 암호를 지정하여 서로 다른 사용자 또는 그룹이 사용하는 암호화 키를 분리할 수 있도록 합니다. 키 서버에서 이 기능을 지원하고 이 기능을 사용하려는 경우에만 사용자 이름을 지정합니다.
암호	일부 키 서버 벤더에서는 사용자가 사용자 이름과 암호를 지정하여 서로 다른 사용자 또는 그룹이 사용하는 암호화 키를 분리할 수 있도록 합니다. 키 서버에서 이 기능을 지원하고 이 기능을 사용하려는 경우에만 암호를 지정합니다.

   KMS 추가를 클릭하여 키 서버를 더 추가할 수 있습니다.

5 **키 제공자 추가**를 클릭합니다.

6 **신뢰**를 클릭합니다.

   vCenter Server는 키 제공자를 추가하고 상태를 연결됨으로 표시합니다.

다음에 수행할 작업

인증서를 교환하여 표준 키 제공자 신뢰할 수 있는 연결 설정의 내용을 참조하십시오.

인증서를 교환하여 표준 키 제공자 신뢰할 수 있는 연결 설정

표준 키 제공자를 vCenter Server 시스템에 추가한 후 신뢰할 수 있는 연결을 설정할 수 있습니다. 정확한 프로세스는 키 제공자가 수락하는 인증서와 회사 정책에 따라 달라집니다.

사전 요구 사항

표준 키 제공자를 추가합니다.

절차

1 vCenter Server로 이동합니다.

2 **구성**을 클릭하고 **보안**에서 **키 제공자**를 선택합니다.

3 키 제공자를 선택합니다.

키 제공자에 대한 KMS가 표시됩니다.

4 KMS를 선택합니다.

5 **신뢰 설정** 드롭다운 메뉴에서 **KMS가 vCenter를 신뢰하도록 만들기**를 선택합니다.

6 서버에 적합한 옵션을 선택하고 단계를 수행합니다.

옵션	자세한 내용은
vCenter Server 루트 CA 인증서	루트 CA 인증서 옵션을 사용하여 표준 키 제공자 신뢰할 수 있는 연결 설정.
vCenter Server 인증서	인증서 옵션을 사용하여 표준 키 제공자 신뢰할 수 있는 연결 설정.
인증서 및 개인 키 업로드	인증서 및 개인 키 업로드 옵션을 사용하여 표준 키 제공자 신뢰할 수 있는 연결 설정.
새 인증서 서명 요청	새 인증서 서명 요청 옵션을 사용하여 표준 키 제공자 신뢰할 수 있는 연결 설정.

루트 CA 인증서 옵션을 사용하여 표준 키 제공자 신뢰할 수 있는 연결 설정

일부 KMS(키 관리 서버) 벤더의 경우 루트 CA 인증서를 KMS에 업로드해야 합니다. 그러면 루트 CA가 서명한 모든 인증서를 이 KMS에서 신뢰하게 됩니다.

vSphere 가상 시스템 암호화에 사용되는 루트 CA 인증서는 자체 서명된 인증서로, vCenter Server 시스템의 VECS(VMware Endpoint Certificate Store) 내 별도의 저장소에 저장됩니다.

참고 기존 인증서를 교체하려는 경우에만 루트 CA 인증서를 생성합니다. 루트 CA 인증서를 생성하면 해당 루트 CA에서 서명한 다른 인증서가 무효화됩니다. 이 워크플로의 일부로 새 루트 CA 인증서를 생성할 수 있습니다.

절차

1 vCenter Server로 이동합니다.

2 **구성**을 클릭하고 **보안**에서 **키 제공자**를 선택합니다.

3 신뢰 연결을 설정할 키 제공자를 선택합니다.

키 제공자에 대한 KMS가 표시됩니다.

4 **신뢰 설정** 드롭다운 메뉴에서 **KMS가 vCenter를 신뢰하도록 만들기**를 선택합니다.

5 **vCenter 루트 CA 인증서**를 선택하고 **다음**을 클릭합니다.

[루트 CA 인증서 다운로드] 대화상자가 vCenter Server에서 암호화에 사용하는 루트 인증서로 채워집니다. 이 인증서는 VECS에 저장됩니다.

6 인증서를 클립보드에 복사하거나 인증서를 파일로 다운로드합니다.

7 KMS 벤더의 지침을 따라 인증서를 해당 시스템에 업로드합니다.

참고 일부 KMS 벤더는 업로드한 루트 인증서를 사용하기 위해 해당 KMS 벤더에서 KMS를 재시작해야 합니다.

다음에 수행할 작업

인증서 교체를 완료합니다. 표준 키 제공자에 대한 신뢰 설정 완료의 내용을 참조하십시오.

인증서 옵션을 사용하여 표준 키 제공자 신뢰할 수 있는 연결 설정

일부 KMS(키 관리 서버) 벤더의 경우 vCenter Server 인증서를 KMS에 업로드해야 합니다. 업로드 후에 KMS는 이 인증서를 사용하여 시스템에서 들어오는 트래픽을 수락합니다.

vCenter Server에서는 인증서를 생성하여 KMS와의 연결을 보호합니다. 인증서는 vCenter Server 시스템의 VECS(VMware Endpoint Certificate Store) 내 별도 키 저장소에 저장됩니다.

절차

1 vCenter Server로 이동합니다.

2 **구성**을 클릭하고 **보안**에서 **키 제공자**를 선택합니다.

3 신뢰 연결을 설정할 키 제공자를 선택합니다.

키 제공자에 대한 KMS가 표시됩니다.

4 **신뢰 설정** 드롭다운 메뉴에서 **KMS가 vCenter를 신뢰하도록 만들기**를 선택합니다.

5 **vCenter 인증서** 를 선택하고 **다음**을 클릭합니다.

[인증서 다운로드] 대화상자가 vCenter Server에서 암호화에 사용하는 루트 인증서로 채워집니다. 이 인증서는 VECS에 저장됩니다.

참고 기존 인증서를 교체하려는 경우가 아니라면 새 인증서를 생성하지 마십시오.

6 인증서를 클립보드에 복사하거나 파일로 다운로드합니다.

7 KMS 벤더의 지침을 따라 인증서를 KMS에 업로드합니다.

다음에 수행할 작업

신뢰 관계를 완료합니다. 표준 키 제공자에 대한 신뢰 설정 완료의 내용을 참조하십시오.

인증서 및 개인 키 업로드 옵션을 사용하여 표준 키 제공자 신뢰할 수 있는 연결 설정

일부 KMS(키 관리 서버) 벤더의 경우 사용자가 KMS 서버 인증서 및 개인 키를 vCenter Server 시스템에 업로드해야 합니다.

일부 KMS 벤더는 연결용 인증서와 개인 키를 생성하여 제공합니다. 파일을 업로드한 후에 KMS는 vCenter Server 인스턴스를 신뢰합니다.

사전 요구 사항

- KMS 벤더에서 인증서와 개인 키를 요청합니다. 파일은 PEM 형식의 X509 파일입니다.

절차

1. vCenter Server로 이동합니다.
2. **구성**을 클릭하고 **보안**에서 **키 제공자**를 선택합니다.
3. 신뢰 연결을 설정할 키 제공자를 선택합니다.

   키 제공자에 대한 KMS가 표시됩니다.
4. **신뢰 설정** 드롭다운 메뉴에서 **KMS가 vCenter를 신뢰하도록 만들기**를 선택합니다.
5. **KMS 인증서 및 개인 키**를 선택하고 **다음**을 클릭합니다.
6. KMS 벤더에서 수신한 인증서를 상단 텍스트 상자에 붙여 넣거나 **파일 업로드**를 클릭하여 인증서 파일을 업로드합니다.
7. 키 파일을 하단 텍스트 상자에 붙여 넣거나 **파일 업로드**를 클릭하여 키 파일을 업로드합니다.
8. **신뢰 설정**을 클릭합니다.

다음에 수행할 작업

신뢰 관계를 완료합니다. 표준 키 제공자에 대한 신뢰 설정 완료의 내용을 참조하십시오.

새 인증서 서명 요청 옵션을 사용하여 표준 키 제공자 신뢰할 수 있는 연결 설정

일부 KMS(키 관리 서버) 벤더의 경우 vCenter Server에서 CSR(인증서 서명 요청)을 생성하고 해당 CSR을 KMS에 보내야 합니다. KMS에서는 CSR에 서명하여 서명된 인증서를 반환합니다. 서명된 인증서를 vCenter Server에 업로드할 수 있습니다.

새 인증서 서명 요청 옵션을 사용하는 프로세스는 2단계로 이루어집니다. 먼저 CSR을 생성하고 KMS 벤더에 보냅니다. 그런 다음 KMS 벤더에서 받은 서명된 인증서를 vCenter Server에 업로드합니다.

절차

1. vCenter Server로 이동합니다.
2. **구성**을 클릭하고 **보안**에서 **키 제공자**를 선택합니다.

3 신뢰 연결을 설정할 키 제공자를 선택합니다.

키 제공자에 대한 KMS가 표시됩니다.

4 **신뢰 설정** 드롭다운 메뉴에서 **KMS가 vCenter를 신뢰하도록 만들기**를 선택합니다.

5 **새 CSR(인증서 서명 요청)**을 선택하고 **다음**을 클릭합니다.

6 대화상자에서 텍스트 상자의 전체 인증서를 클립보드에 복사하거나 파일로 다운로드합니다.

명시적으로 CSR을 생성하려는 경우에만 대화상자에서 **새 CSR 생성** 버튼을 사용합니다. 이 옵션을 사용하면 이전 CSR 기반의 서명된 인증서가 모두 무효해집니다.

7 KMS 벤더의 지침을 따라 CSR을 제출합니다.

8 KMS 벤더에서 서명된 인증서를 수신하는 경우 **키 제공자**를 다시 클릭하고 키 제공자를 선택하고 **신뢰 설정** 드롭다운 메뉴에서 **서명된 CSR 인증서 업로드**를 선택합니다.

9 서명된 인증서를 하단 텍스트 상자에 붙여 넣거나 **파일 업로드**를 클릭하여 파일을 업로드한 후 **업로드**를 클릭합니다.

다음에 수행할 작업

신뢰 관계를 완료합니다. 표준 키 제공자에 대한 신뢰 설정 완료의 내용을 참조하십시오.

기본 키 제공자 설정

첫 번째 키 제공자를 기본값으로 설정하지 않거나 환경에서 여러 키 제공자를 사용하여 기본 키 제공자를 제거하는 경우 기본 키 제공자를 설정해야 합니다.

사전 요구 사항

키 제공자 탭의 [연결 상태]에 [연결됨] 및 녹색 확인 표시가 있는지 확인하는 것이 모범 사례입니다.

절차

1 vCenter Server로 이동합니다.

2 **구성**을 클릭하고 **보안**에서 **키 제공자**를 선택합니다.

3 키 제공자를 선택합니다.

4 **기본값으로 설정**을 클릭합니다.

[확인] 대화상자가 나타납니다.

5 **기본값으로 설정**을 클릭합니다.

키 제공자는 현재 기본값으로 표시됩니다.

표준 키 제공자에 대한 신뢰 설정 완료

KMS를 신뢰하도록 **표준 키 제공자 추가** 대화상자가 표시된 경우가 아니면 인증서 교환이 완료된 이후에 신뢰를 명시적으로 설정해야 합니다.

KMS를 신뢰하거나, KMS 인증서를 업로드하는 방법으로 신뢰 설정을 완료, 즉 vCenter Server가 KMS를 신뢰하도록 설정할 수 있습니다. 다음 두 가지 옵션 중에서 선택할 수 있습니다.

- **KMS 인증서 업로드** 옵션을 사용하여 인증서를 명시적으로 신뢰합니다.
- **vCenter가 KMS를 신뢰하도록 만들기** 옵션을 사용하여 KMS 리프 인증서 또는 KMS CA 인증서를 vCenter Server에 업로드합니다.

참고 루트 CA 인증서 또는 중간 CA 인증서를 업로드하면 vCenter Server는 해당 CA에서 서명한 모든 인증서를 신뢰합니다. 보안을 강화하려면 KMS 벤더가 제어하는 리프 인증서나 중간 CA 인증서를 업로드해야 합니다.

절차

1 vCenter Server로 이동합니다.

2 **구성**을 클릭하고 **보안**에서 **키 제공자**를 선택합니다.

3 신뢰 연결을 설정할 키 제공자를 선택합니다.

키 제공자에 대한 KMS가 표시됩니다.

4 KMS를 선택합니다.

5 **신뢰 설정** 드롭다운 메뉴에서 다음 옵션 중 하나를 선택합니다.

옵션	작업
vCenter가 KMS를 신뢰하도록 만들기	표시되는 대화상자에서 **신뢰**를 클릭합니다.
KMS 인증서 업로드	a 표시되는 대화상자에서 인증서에 붙여 넣거나 **파일 업로드**를 클릭하고 인증서 파일을 찾습니다. b **업로드**를 클릭합니다.

서로 다른 사용자를 위해 별도의 키 제공자 설정

동일한 KMS 인스턴스의 서로 다른 사용자를 위해 서로 다른 키 제공자를 가진 환경을 설정할 수 있습니다. 여러 키 제공자를 가지면 유용합니다. 예를 들어 회사의 각 부서에 서로 다른 암호화 키 집합에 대한 액세스를 부여하려는 경우가 이에 해당합니다.

동일한 KMS에 대해 여러 키 제공자를 사용하여 키를 분리할 수 있습니다. 별도의 키 집합을 가지는 것은 서로 다른 BU 또는 서로 다른 고객과 같은 사용 사례에 필수적입니다.

참고 모든 KMS 벤더가 여러 사용자를 지원하는 것은 아닙니다.

사전 요구 사항

KMS와의 연결을 설정합니다.

절차

1 KMS에서 해당하는 사용자 이름과 암호를 가진 2명의 사용자를 생성합니다(예: C1 및 C2).

2 vCenter Server에 로그인하고 첫 번째 키 제공자를 생성합니다.

3 사용자 이름과 암호를 입력하라는 메시지가 표시되면 첫 번째 사용자에 고유한 정보를 제공합니다.

4 두 번째 키 제공자를 생성하고 동일한 KMS를 추가하되 두 번째 사용자 이름과 암호를 사용합니다(C2).

결과

2개의 키 제공자가 KMS에 각각 독립적으로 연결되어 있으며, 서로 다른 키 집합을 사용합니다.

vSphere Native Key Provider 구성 및 관리

8

vSphere 환경에서 VMware vSphere® Native Key Provider™를 사용하려면 몇 가지 준비가 필요합니다. vSphere Native Key Provider를 구성한 후 가상 시스템에서 vTPM(신뢰할 수 있는 가상 플랫폼 모듈)을 사용할 수 있습니다.

vSphere Native Key Provider에 대한 환경을 설정한 후 vSphere Client 및 API를 사용하여 vTPM을 생성할 수 있습니다. VMware vSphere® Enterprise Plus Edition™을 구입한 경우에는 가상 시스템과 가상 디스크를 암호화하고 기존 가상 시스템과 디스크를 암호화할 수도 있습니다.

 (vSphere Native Key Provider 구성)

본 장은 다음 항목을 포함합니다.

- vSphere Native Key Provider 개요
- vSphere Native Key Provider 프로세스 흐름
- vSphere Native Key Provider 구성
- vSphere Native Key Provider 백업
- 고급 연결 모드 구성에서 vSphere Native Key Provider 가져오기
- vSphere Native Key Provider 복구
- vSphere Native Key Provider 업데이트
- vSphere Native Key Provider 삭제

vSphere Native Key Provider 개요

vSphere 7.0 업데이트 2 이상에서는 기본 제공 vSphere Native Key Provider를 사용하여 vTPM(가상 TPM)과 같은 암호화 기술을 사용하도록 설정할 수 있습니다.

vSphere Native Key Provider는 모든 vSphere 버전에 포함되어 있으며 외부 키 서버(업계에서는 KMS(키 관리 서버)라고도 함)가 필요하지 않습니다. vSphere 가상 시스템 암호화에 vSphere Native Key Provider를 사용할 수도 있지만 VMware vSphere® Enterprise Plus Edition™을 구매해야 합니다.

vSphere Native Key Provider란?

표준 키 제공자 또는 신뢰할 수 있는 키 제공자를 사용하여 외부 키 서버를 구성해야 합니다. 표준 키 제공자 설정의 경우, vCenter Server가 외부 키 서버에서 키를 가져와서 ESXi 호스트에 키를 배포합니다. 신뢰할 수 있는 키 제공자(vSphere 신뢰 기관) 설정의 경우, 신뢰할 수 있는 ESXi 호스트가 키를 직접 가져옵니다.

vSphere Native Key Provider를 사용하면 외부 키 서버가 더 이상 필요하지 않습니다. vCenter Server가 KDK(Key Derivation Key)라는 기본 키를 생성하여 클러스터의 모든 ESXi 호스트에 푸시합니다. 그러면 ESXi 호스트가 데이터 암호화 키를 생성하여(vCenter Server에 연결되어 있지 않은 경우에도) vTPM과 같은 보안 기능을 사용하도록 설정합니다. vTPM 기능은 모든 vSphere 버전에 포함되어 있습니다. vSphere 가상 시스템 암호화에 vSphere Native Key Provider를 사용하려면 vSphere Enterprise Plus Edition을 구매해야 합니다. vSphere Native Key Provider는 기존 키 서버 인프라와 공존할 수 있습니다.

vSphere Native Key Provider:

- 외부 키 서버가 필요하지 않거나 원하는 경우 vTPM, vSphere 가상 시스템 암호화 및 vSAN 미사용 데이터 암호화를 사용할 수 있습니다.
- VMware 인프라 제품에서만 작동합니다.
- 외부 상호 운용성, KMIP 지원, 하드웨어 보안 모듈 또는 기존의 타사 외부 키 서버가 상호 운용성 또는 규정 준수를 위해 제공할 수 있는 기타 기능을 제공하지 않습니다. 조직에서 비 VMware 제품 및 구성 요소에 대해 이 기능이 필요한 경우에는 기존의 타사 키 서버를 설치하십시오.
- 외부 키 서버를 사용할 수 없거나 사용하지 않으려는 조직의 요구를 해결하는 데 유용합니다.
- 플래시 및 SSD와 같이 삭제하기 어려운 미디어에서 암호화 기술을 조기에 사용할 수 있도록 설정하여 데이터 삭제 및 시스템 재사용 방식을 개선합니다.
- 키 제공자 간의 전환 경로를 제공합니다. vSphere Native Key Provider는 VMware 표준 키 제공자 및 vSphere Trust Authority 신뢰할 수 있는 키 제공자와 호환됩니다.
- 고급 연결 모드 구성 또는 vCenter Server 고가용성 구성을 사용하여 여러 vCenter Server 시스템에서 작동합니다.
- 모든 버전의 vSphere에서 vTPM을 사용하도록 설정하고 vSphere 가상 시스템 암호화가 포함된 vSphere Enterprise Plus Edition을 구매하여 가상 시스템을 암호화하는 데 사용할 수 있습니다. vSphere 가상 시스템 암호화는 VMware 표준 키 제공자 및 신뢰할 수 있는 키 제공자와 마찬가지로 vSphere Native Key Provider와 함께 작동합니다.
- 적절한 vSAN 라이센스를 사용하여 vSAN 미사용 데이터 암호화를 사용하도록 설정하는 데 사용할 수 있습니다.
- TPM(신뢰할 수 있는 플랫폼 모듈) 2.0을 사용하여 ESXi 호스트에 설치된 경우 보안을 강화할 수 있습니다. TPM 2.0이 설치된 호스트에서만 사용할 수 있도록 vSphere Native Key Provider를 구성할 수도 있습니다.

참고 ESXi 호스트는 vSphere Native Key Provider를 사용하기 위해 TPM 2.0이 필요하지 않습니다. 다만, TPM 2.0은 향상된 보안을 제공합니다.

모든 보안 솔루션과 마찬가지로 시스템 설계, 구현 고려 사항 및 네이티브 키 제공자 사용의 장단점을 고려합니다. 예를 들어 ESXi 키 지속성은 항상 사용 가능한 키 서버에 대한 종속성을 방지합니다. 그러나 키 지속성은 네이티브 키 제공자 암호화 정보를 클러스터링된 호스트에 저장하기 때문에 악의적인 행위자가 ESXi 호스트 자체를 도용할 경우 여전히 위험합니다. 환경이 다르기 때문에 조직의 규정 및 보안 요구 사항, 운영 요구 사항 및 위험에 대한 허용 범위에 따라 보안 제어를 평가하고 구현합니다.

vSphere Native Key Provider에 대한 자세한 개요는 https://core.vmware.com/native-key-provider 항목을 참조하십시오.

vSphere Native Key Provider 요구 사항

vSphere Native Key Provider를 사용하려면 다음을 수행해야 합니다.

- vCenter Server 시스템과 ESXi 호스트 둘 다 vSphere 7.0 업데이트 2 이상을 실행하고 있는지 확인합니다.
- 클러스터에서 ESXi 호스트를 구성합니다. 필수는 아니지만 TPM을 포함하여 가능한 한 동일한 ESXi 호스트를 사용하는 것이 가장 좋습니다. 클러스터 호스트가 동일하면 클러스터 관리 및 기능 사용 설정이 훨씬 더 쉬워집니다.
- vCenter Server 파일 기반 백업을 구성하고 백업에 KDK(Key Derivation Key)가 포함되어 있는 백업을 안전하게 복원하고 저장합니다. "vCenter Server 설치 및 설정" 에서 vCenter Server 백업 및 복원에 대한 항목을 참조하십시오.

vSphere Native Key Provider를 사용하여 vSphere 가상 시스템 암호화 또는 vSAN 암호화를 수행하려면 적절한 라이센스가 포함된 해당 제품의 버전을 구입해야 합니다.

vSphere Native Key Provider 및 고급 연결 모드

고급 연결 모드 구성으로 구성된 vCenter Server 시스템 간에 공유할 수 있는 단일 vSphere Native Key Provider를 구성할 수 있습니다. 이 시나리오의 개략적인 단계는 다음과 같습니다.

1 vCenter Server 시스템 중 하나에 vSphere Native Key Provider 생성

2 생성된 vCenter Server에서 네이티브 키 제공자 백업

3 네이티브 키 제공자 내보내기

4 고급 연결 모드 구성에서 네이티브 키 제공자를 다른 vCenter Server 시스템으로 가져오기

고급 연결 모드 구성에서 vSphere Native Key Provider 가져오기의 내용을 참조하십시오.

vSphere Native Key Provider 권한

표준 및 신뢰할 수 있는 키 제공자와 마찬가지로 vSphere Native Key Provider는**Cryptographer.*** 권한을 사용합니다. 또한 vSphere Native Key Provider는 vSphere Native Key Provider에만 해당하는 **Cryptographer.ReadKeyServersInfo** 권한을 사용하여 vSphere Native Key Provider를 나열합니다. 암호화 작업 권한의 내용을 참조하십시오.

vSphere Native Key Provider 경보

vSphere Native Key Provider를 백업해야 합니다. vSphere Native Key Provider를 백업하지 않으면 vCenter Server에서 경보를 생성합니다. 경보가 생성된 vSphere Native Key Provider를 백업하면 vCenter Server에서 경보를 재설정합니다. 기본적으로 vCenter Server는 하루에 한 번 백업된 vSphere Native Key Provider를 검사합니다. `vpxd.KMS.backupCheckInterval` 옵션을 수정하여 검사 간격을 변경할 수 있습니다.

주기적인 vSphere Native Key Provider 업데이트 적용 검사

vCenter Server에서는 vCenter Server 및 ESXi 호스트의 vSphere Native Key Provider 구성이 일치하는지 주기적으로 검사합니다. 예를 들어 클러스터에 호스트를 추가할 때 호스트 상태가 변경되면 클러스터의 키 제공자 구성과 호스트의 구성 간에 편차가 발생합니다. 구성(keyID)이 호스트의 구성과 다르면 vCenter Server가 호스트의 구성을 자동으로 업데이트합니다. 수동 작업은 필요하지 않습니다.

기본적으로 vCenter Server는 5분마다 구성을 검사합니다. `vpxd.KMS.remediationInterval` 옵션을 사용하여 간격을 수정할 수 있습니다.

재해 복구 사이트에서 vSphere Native Key Provider 사용

백업 재해 복구 사이트에서 vSphere Native Key Provider를 사용할 수 있습니다. 기본 사이트에서 백업 DR 사이트의 vCenter Server로 vSphere Native Key Provider 백업을 가져오면 해당 클러스터가 암호화된 가상 시스템을 암호 해독하고 실행할 수 있습니다.

항상 DR 솔루션을 테스트하십시오. 복구를 시도하지 않고 솔루션이 작동한다고 가정하지 마십시오. vSphere Native Key Provider 백업의 복사본을 DR 사이트에서도 사용할 수 있는지 확인하십시오.

vSphere Native Key Provider 프로세스 흐름

vSphere Native Key Provider를 구성하고 관리하는 방법을 알려면 필수적으로 vSphere Native Key Provider 프로세스 흐름을 이해해야 합니다.

기본 제공 vSphere Native Key Provider를 통해 암호화 기반의 vTPM(가상 TPM)을 사용할 수 있습니다. vSphere Native Key Provider는 모든 vSphere 버전에 포함되어 있으며 외부 키 서버(KMS)가 필요하지 않습니다. vSphere 가상 시스템 암호화에 vSphere Native Key Provider를 사용하려면 vSphere Enterprise+ 버전을 구매해야 합니다.

vSphere Native Key Provider 구성

vSphere Native Key Provider 구성에는 다음과 같은 기본적인 작업이 포함됩니다.

1 적절한 관리 권한이 있는 사용자가 vSphere Client를 사용하여 vCenter Server에서 vSphere Native Key Provider를 생성합니다.

2 그러면 vCenter Server에서 ESXi 호스트의 모든 클러스터에 대해 vSphere Native Key Provider를 구성합니다.

이 단계에서 vCenter Server는 기본 키를 클러스터의 모든 ESXi 호스트로 푸시합니다. 마찬가지로 vSphere Native Key Provider를 업데이트하거나 삭제하면 변경 내용이 클러스터의 호스트로 푸시됩니다.

3 적절한 암호화 권한이 있는 사용자가 vTPM 및 암호화된 가상 시스템을 생성합니다(vSphere Enterprise+ 버전을 구매한 경우).

장 11 신뢰할 수 있는 가상 플랫폼 모듈로 가상 시스템 보호 및 장 10 vSphere 환경에서 암호화 사용의 내용을 참조하십시오.

vSphere Native Key Provider 암호화 프로세스 흐름

서로 다른 구성 요소가 vSphere Native Key Provider를 사용하여 암호화 작업을 수행하기 위해 상호 작용하는 방법을 이해하려면 암호화 프로세스 흐름의 내용을 참조하십시오.

vSphere Native Key Provider 구성

암호화 작업을 시작하려면 먼저 vCenter Server에서 vSphere Native Key Provider를 구성해야 합니다.

vSphere 7.0 업데이트 2 이상에는 vSphere Native Key Provider라는 키 제공자가 포함되어 있습니다. vSphere Native Key Provider는 외부 키 서버(KMS) 없이도 암호화 관련 기능을 사용하도록 설정할 수 있습니다. 처음에 vCenter Server는 vSphere Native Key Provider로 구성되지 않습니다. vSphere Native Key Provider를 수동으로 구성해야 합니다.

ESXi 호스트는 vSphere Native Key Provider를 사용하기 위해 TPM 2.0이 필요하지 않습니다. 다만, TPM 2.0은 향상된 보안을 제공합니다.

참고 vSphere Native Key Provider를 구성할 때 키 제공자는 키 제공자가 구성되는 vCenter Server의 모든 클러스터에서 사용할 수 있습니다. 그 결과 vCenter Server에 연결된 모든 호스트는 사용자가 구성하는 모든 vSphere Native Key Provider에 액세스할 수 있습니다.

사전 요구 사항

필요한 권한: **암호화 작업.키 서버 관리**

절차

1 vSphere Client를 사용하여 vCenter Server 시스템에 로그인합니다.

2 인벤토리 목록을 찾아서 vCenter Server 인스턴스를 선택합니다.

3 **구성**을 클릭하고 **보안**에서 **키 제공자**를 클릭합니다.

4 **추가**를 클릭한 다음 **Native Key Provider 추가**를 클릭합니다.

5 vSphere Native Key Provider의 이름을 입력합니다.

유형(표준 키 제공자, 신뢰할 수 있는 키 제공자 및 네이티브 키 제공자)에 관계없이 각 논리적 키 제공자는 모든 vCenter Server 시스템에서 고유한 이름이 있어야 합니다.

자세한 내용은 키 제공자 이름 지정의 내용을 참조하십시오.

6 이 vSphere Native Key Provider를 TPM 2.0이 있는 호스트에서만 사용하려면 **TPM으로 보호되는 ESXi 호스트에만 키 제공자 사용** 확인란을 선택합니다.

사용되도록 설정되는 경우 vSphere Native Key Provider는 TPM 2.0이 있는 호스트에서만 사용할 수 있습니다.

7 **키 제공자 추가**를 클릭합니다.

참고 데이터 센터의 모든 클러스터된 ESXi 호스트에서 키 제공자를 가져오고 vCenter Server에서 해당 캐시를 업데이트하는 데에는 5분 정도 걸립니다. 정보가 전파되는 방식으로 인해 일부 호스트에서 키 작업에 키 제공자를 사용하려면 몇 분 정도 기다려야 할 수 있습니다.

결과

vSphere Native Key Provider가 추가되고 **키 제공자** 창에 나타납니다. 이때 vSphere Native Key Provider는 백업되지 않습니다. vSphere Native Key Provider를 사용할 수 있으려면 먼저 백업해야 합니다.

다음에 수행할 작업

vSphere Native Key Provider 백업의 내용을 참조하십시오.

vSphere Native Key Provider 백업

키 제공자 구성을 복원해야 하는 경우 재해 복구 시나리오의 일부로 vSphere Native Key Provider를 백업해야 합니다. vSphere Client, PowerCLI 또는 API를 사용하여 vSphere Native Key Provider를 백업할 수 있습니다.

vSphere Native Key Provider는 vCenter Server 파일 기반 백업의 일부로 백업됩니다. 하지만 vSphere Native Key Provider를 사용할 수 있으려면 먼저 한 번 이상 백업해야 합니다. vSphere Native Key Provider는 생성할 때 백업되지 않습니다.

백업은 구성을 복원해야 하는 경우 필요합니다. vSphere Native Key Provider를 복원하려면 vSphere Client를 사용하여 vSphere Native Key Provider 복원 항목을 참조하십시오.

백업 파일을 안전한 곳에 보관합니다. 백업을 생성할 때 백업을 암호로 보호할 수 있습니다. 백업 파일은 PKCS#12 형식입니다.

vSphere Native Key Provider가 백업되지 않으면 vCenter Server에서 경보를 생성합니다. 경보는 확인할 수 있지만 vSphere Native Key Provider를 백업할 때까지 24시간마다 다시 나타납니다.

사전 요구 사항

필요한 권한: **암호화 작업.키 서버 관리**

참고 [고급 연결 모드] 구성에서는 키 제공자가 속한 vCenter Server에 대한 백업을 수행해야 합니다.

절차

1 vSphere Client를 사용하여 vCenter Server 시스템에 로그인합니다.

2 인벤토리 목록을 찾아서 vCenter Server 인스턴스를 선택합니다.

3 **구성**을 클릭하고 **보안**에서 **키 제공자**를 클릭합니다.

4 백업할 vSphere Native Key Provider를 선택합니다.

백업하지 않은 키 제공자에 대해 [백업되지 않음]이라는 상태가 나타납니다.

5 **백업**을 클릭합니다.

6 백업을 암호로 보호하려면 **암호로 Native Key Provider 데이터 보호** 상자를 선택합니다.

a 암호를 입력하고 안전한 곳에 저장합니다.

b **암호를 안전한 곳에 저장했습니다.** 상자를 선택하여 암호를 안전한 장소에 저장했음을 나타냅니다.

7 **키 제공자 백업**을 클릭합니다.

백업 파일은 PKCS#12 형식입니다.

8 백업 파일을 안전한 곳에 저장합니다.

결과

vSphere Native Key Provider의 상태가 [백업되지 않음]에서 [주의], [활성]으로 변경됩니다. [주의]는 vCenter Server에서 여전히 정보를 데이터 센터의 모든 ESXi 호스트로 푸시하고 있음을 나타냅니다. [활성]은 정보가 모든 호스트에 푸시되었음을 의미합니다.

다음에 수행할 작업

vTPM을 ESXi 호스트에 추가하려면 장 11 신뢰할 수 있는 가상 플랫폼 모듈로 가상 시스템 보호의 내용을 참조하십시오. 가상 시스템을 암호화하려면 장 10 vSphere 환경에서 암호화 사용의 내용을 참조하십시오.

고급 연결 모드 구성에서 vSphere Native Key Provider 가져오기

고급 연결 모드 구성에서 하나의 vCenter Server에 Native Key Provider를 생성한 후 vSphere Client를 사용하여 구성의 다른 vCenter Server에 가져올 수 있습니다.

고급 연결 모드 구성으로 구성된 vCenter Server 시스템 간에 공유할 수 있는 단일 vSphere Native Key Provider를 구성할 수 있습니다. 고급 연결 모드 구성의 한 vCenter Server 시스템에 vSphere Native Key Provider를 생성한 다음 **복원** 기능을 사용하여 암호화된 키 파일을 다른 ELM 연결 vCenter Server 시스템으로 가져옵니다.

사전 요구 사항

- 필요한 권한: **암호화 작업.키 서버 관리**
- 고급 연결 모드 구성의 vCenter Server 시스템 중 하나에서 vSphere Native Key Provider를 생성합니다. vSphere Native Key Provider 구성의 내용을 참조하십시오.

- vSphere Native Key Provider를 백업하고 암호화된 백업 키 파일을 다운로드합니다. vSphere Native Key Provider 백업의 내용을 참조하십시오. 가져올 때 액세스할 수 있는 안전한 위치에 암호화된 백업 키 파일을 배치합니다.

절차

1. vSphere Client를 사용하여 vSphere Native Key Provider를 가져오려는 고급 연결 모드 구성의 vCenter Server에 로그인합니다.
2. 인벤토리 목록을 찾아서 vCenter Server 인스턴스를 선택합니다.
3. **구성**을 클릭하고 **보안**에서 **키 제공자**를 클릭합니다.
4. **복원**을 클릭합니다.
5. vSphere Native Key Provider 암호화된 백업 키 파일을 저장한 파일 위치로 이동합니다.

   파일은 PKCS#12 형식으로 저장되어 있습니다.
6. 파일을 선택합니다.
7. (선택 사항) 파일이 암호로 보호되어 있는 경우 암호를 입력합니다.
8. **다음**을 클릭합니다.
9. (선택 사항) 이 키 제공자를 TPM으로 보호된 ESXi 호스트에만 사용하기로 결정한 경우 확인란을 선택합니다.
10. **마침**을 클릭합니다.

결과

vSphere Native Key Provider를 vCenter Server로 가져와집니다. 암호화 작업에 vSphere Native Key Provider를 사용하려면 먼저 **키 제공자** 창에서 이를 선택하고 **기본값으로 설정**을 클릭합니다.

다음에 수행할 작업

vSphere Native Key Provider를 추가하려는 고급 연결 모드 구성의 다른 vCenter Server 시스템에 대해 이 단계를 반복합니다.

vSphere Native Key Provider 복구

vSphere Client를 통해 또는 vCenter Server Appliance 백업에서 vSphere Native Key Provider를 복구할 수 있습니다.

필요한 경우 다음과 같은 방법으로 vSphere Native Key Provider를 복구할 수 있습니다.

1. vCenter Server Appliance를 재구축해야 하는 경우 vSphere Client를 사용하여 키 제공자를 복원합니다. vSphere Client를 사용하여 vSphere Native Key Provider 복원의 내용을 참조하십시오.

2 vCenter Server Appliance를 재구축해야 하는 경우 vCenter Server Appliance 백업에서 키 제공자를 복원해야 합니다. vCenter Server Appliance 백업을 수행하면 Native Key Provider가 저장됩니다. 백업에서 vCenter Server Appliance를 복원하는 것에 대한 자세한 내용은 https://blogs.vmware.com/vsphere/2018/05/vcenter-server-appliance-6-7-file-based-backup-and-restore-walkthroughs.html에서 참조하십시오.

vSphere Client를 사용하여 vSphere Native Key Provider 복원

vSphere Client를 사용하여 vSphere Native Key Provider를 복원할 수 있습니다.

Native Key Provider가 실수로 삭제되었거나 재해 복구를 수행해야 하는 경우 Native Key Provider를 복원할 수 있습니다.

vSphere Native Key Provider를 복원할 때 키 제공자를 다시 백업할 필요가 없습니다. 초기 백업이면 충분합니다. 백업 파일을 안전한 위치에 계속 유지합니다.

사전 요구 사항

- 필요한 권한: **암호화 작업.키 서버 관리**
- 키 제공자 백업 파일.
- 키 제공자 파일의 암호(키 제공자를 백업할 때 암호를 입력한 경우).

절차

1 vSphere Client를 사용하여 vCenter Server 시스템에 로그인합니다.

2 인벤토리 목록을 찾아서 vCenter Server 인스턴스를 선택합니다.

3 **구성**을 클릭하고 **보안**에서 **키 제공자**를 클릭합니다.

4 vSphere Native Key Provider를 선택하고 **복원**을 클릭합니다.

5 파일 위치로 이동하고 백업 암호화된 키 파일을 선택합니다.

   파일은 PKCS#12 형식으로 저장되어 있습니다.

6 (선택 사항) 파일이 암호로 보호되어 있는 경우 암호를 입력합니다.

7 **다음**을 클릭합니다.

8 (선택 사항) 이 키 제공자를 TPM으로 보호된 ESXi 호스트에만 사용하기로 결정한 경우 확인란을 선택합니다.

9 **마침**을 클릭합니다.

결과

vSphere Native Key Provider가 복원됩니다.

vSphere Native Key Provider 업데이트

정기적인 키 순환 계획의 일부로 PowerCLI를 사용하여 vSphere Native Key Provider를 업데이트할 수 있습니다.

키 순환에 대한 정책이 있는 경우 vSphere Native Key Provider를 업데이트하고 해당 키 제공자를 사용하여 암호화한 가상 시스템의 키를 재생성할 수 있습니다. vSphere Native Key Provider를 업데이트하려면 PowerCLI를 사용해야 합니다. 키 제공자를 업데이트하지 않고 암호화된 가상 시스템의 키를 재생성할 수도 있습니다. 이 경우 가상 시스템 키만 변경됩니다. 가상 시스템의 키를 재생성하려면 vSphere Client를 사용하여 암호화된 가상 시스템 키 재생성 항목을 참조하십시오.

사전 요구 사항

- 필요한 권한: **암호화 작업.키 서버 관리**
- PowerCLI 12.3.0

절차

1 PowerCLI 세션에서 `Connect-VIServer` cmdlet을 실행하여 업데이트할 vSphere Native Key Provider를 구성한 vCenter Server에 관리자로 연결합니다.

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

2 vSphere Native Key Provider 이름을 가져오려면 `Type` cmdlet을 선택적 `Get-KeyProvider` 매개변수와 함께 실행합니다.

```
Get-KeyProvider -Type NativeKeyProvider
```

3 키 제공자를 업데이트하려면 키 제공자 이름 및 GUID를 지정하여 `Set-KeyProvider` cmdlet을 실행합니다.

`New-Guid` cmdlet을 실행하여 사용할 GUID를 생성할 수 있습니다.

```
Set-KeyProvider -KeyProvider KeyProvider_name -KeyId Guid
```

구성 백업에 대한 주의가 나타납니다.

4 키 제공자를 백업하려면 `Export-KeyProvider` cmdlet을 실행합니다.

```
Export-KeyProvider -KeyProvider KeyProvider_name -FilePath path_file_name
```

vSphere Client를 사용하여 키 제공자를 백업할 수도 있습니다. vSphere Native Key Provider 백업의 내용을 참조하십시오.

결과

키 제공자가 업데이트되면 해당 상태가 [백업되지 않음]으로 변경됩니다. 키 제공자를 백업하면 해당 상태가 [활성]으로 변경됩니다.

vSphere Native Key Provider 삭제

vCenter Server에서 vSphere Native Key Provider를 삭제할 수 있습니다.

vSphere Native Key Provider를 삭제한 후 vTPM이 있거나 암호화된 가상 시스템은 계속 실행됩니다. ESXi 호스트를 재부팅하면 암호화된 가상 시스템은 잠긴 상태로 전환됩니다. 이러한 가상 시스템을 등록 취소한 후 등록을 다시 시도하면 해당 시스템이 잠긴 상태로 전환됩니다. 가상 시스템을 잠금 해제하는 유일한 방법은 이전 vSphere Native Key Provider를 복원하는 것입니다.

사전 요구 사항

필요한 권한: **암호화 작업.키 서버 관리**

vSphere Native Key Provider를 삭제하기 전에 해당 키 제공자를 사용하여 암호화된 모든 암호화된 가상 시스템과 데이터스토어를 다른 키 제공자로 키를 재생성합니다. vSphere Client를 사용하여 암호화된 가상 시스템 키 재생성의 내용을 참조하십시오.

또한 키 제공자를 삭제한 후 암호화된 가상 시스템의 키를 재생성해야 하는 경우 vSphere Native Key Provider의 백업을 유지합니다.

절차

1. vSphere Client를 사용하여 vCenter Server 시스템에 로그인합니다.
2. 인벤토리 목록을 찾아서 vCenter Server 인스턴스를 선택합니다.
3. **구성**을 클릭하고 **보안**에서 **키 제공자**를 클릭합니다.
4. 삭제할 키 제공자를 선택합니다.
5. **삭제**를 클릭합니다.
6. 주의 메시지를 읽고 슬라이더를 오른쪽 끝까지 밉니다.
7. **삭제**를 클릭합니다.

결과

vCenter Server에서 vSphere Native Key Provider가 제거됩니다.

vSphere 신뢰 기관

9

vSphere 7.0 이상에서는 VMware® vSphere Trust Authority™를 활용할 수 있습니다. vSphere 신뢰 기관은 워크로드 보안을 향상시키는 기본 기술입니다. vSphere 신뢰 기관은 ESXi 호스트의 하드웨어 신뢰 루트를 워크로드 자체에 연결하여 조직의 신뢰 수준을 높입니다.

본 장은 다음 항목을 포함합니다.

- vSphere 신뢰 기관 개념 및 기능
- vSphere 신뢰 기관 구성
- vSphere 환경에서 vSphere 신뢰 기관 관리

vSphere 신뢰 기관 개념 및 기능

vSphere 신뢰 기관은 신뢰할 수 있는 컴퓨팅 기반의 신뢰성을 조직의 전체 컴퓨팅 인프라로 확장하여 악의적인 공격으로부터 SDDC를 보호합니다. vSphere 신뢰 기관은 원격 증명 및 고급 암호화 기능에 대한 제어된 액세스를 사용합니다.

vSphere 신뢰 기관은 높은 보안 요구 사항을 충족하는 일련의 서비스입니다. vSphere 신뢰 기관을 사용하여 보안 인프라를 설정하고 유지할 수 있습니다. 민감한 워크로드가 정품 소프트웨어를 부팅한 것으로 입증된 ESXi 호스트에서만 실행되도록 할 수 있습니다.

vSphere 신뢰 기관에서 환경을 보호하는 방식

ESXi 호스트를 증명하도록 vSphere 신뢰 기관 서비스를 구성하면 호스트에서 신뢰할 수 있는 암호화 작업을 수행할 수 있게 됩니다.

vSphere 신뢰 기관은 ESXi 호스트에 대한 원격 증명을 사용하여 부팅 소프트웨어의 신뢰성을 입증합니다. 증명은 ESXi 호스트가 정품 VMware 소프트웨어 또는 VMware에서 서명한 파트너 소프트웨어를 실행 중인지 확인합니다. 증명에서는 ESXi 호스트에 설치된 TPM(신뢰할 수 있는 플랫폼 모듈) 2.0 칩에 루팅되어 있는 측정값을 사용합니다. vSphere 신뢰 기관에서, ESXi는 증명이 된 후에만 암호화 키에 액세스할 수 있고 암호화 작업을 수행할 수 있습니다.

vSphere 신뢰 기관 용어집

vSphere 신뢰 기관에는 이해하고 있어야 하는 몇 가지 중요한 용어와 정의가 포함되어 있습니다.

표 9-1. vSphere 신뢰 기관 용어집

용어	정의
VMware vSphere® 신뢰 기관™	신뢰할 수 있는 인프라를 사용하도록 설정하는 서비스 집합을 지정합니다. 이는 ESXi 호스트가 신뢰할 수 있는 소프트웨어를 실행 중인지 확인하고 신뢰할 수 있는 ESXi 호스트에만 암호화 키가 릴리스되도록 합니다.
vSphere 신뢰 기관 구성 요소	vSphere 신뢰 기관 구성 요소는 다음과 같습니다. ■ 증명 서비스 ■ 키 제공자 서비스
증명 서비스	원격 ESXi 호스트의 상태를 증명합니다. TPM 2.0을 사용하여 하드웨어 신뢰 루트를 설정하고 관리자가 승인한 ESXi 버전 목록에 대해 소프트웨어 측정값을 확인합니다.
키 제공자 서비스	하나 이상의 키 서버를 캡슐화하고 가상 시스템을 암호화할 때 지정할 수 있는 신뢰할 수 있는 키 제공자를 노출합니다. 현재 키 서버는 KMIP 프로토콜로 제한됩니다.
신뢰할 수 있는 인프라	신뢰할 수 있는 인프라는 다음으로 구성됩니다. ■ 신뢰 기관 vCenter Server ■ 워크로드 vCenter Server ■ 최소 하나의 vSphere 신뢰 기관 클러스터(신뢰 기관 vCenter Server의 일부로 구성) ■ 최소 하나의 신뢰할 수 있는 클러스터(워크로드 vCenter Server의 일부로 구성) ■ 신뢰할 수 있는 클러스터에서 실행 중인 암호화된 워크로드 가상 시스템 ■ 최소 하나의 KMIP 준수 키 관리 서버 **참고** 신뢰 기관 클러스터 및 신뢰할 수 있는 클러스터에 대해 별도의 vCenter Server 시스템을 사용해야 합니다.
신뢰 기관 클러스터	vSphere 신뢰 기관 구성 요소(증명 서비스 및 키 제공자 서비스)를 실행하는 ESXi 호스트의 vCenter Server 클러스터로 구성됩니다.
신뢰 기관 호스트	vSphere 신뢰 기관 구성 요소(증명 서비스 및 키 제공자 서비스)를 실행하는 ESXi 호스트입니다.
신뢰할 수 있는 클러스터	신뢰 기관 클러스터에 의해 원격으로 증명되는 신뢰할 수 있는 ESXi 호스트의 vCenter Server 클러스터로 구성됩니다. 꼭 필요한 것은 아니지만 구성된 키 제공자 서비스는 신뢰할 수 있는 클러스터에서 제공하는 값을 크게 증가시킵니다.
신뢰할 수 있는 호스트	신뢰 기관 클러스터 증명 서비스에 의해 해당 소프트웨어가 검증된 ESXi 호스트입니다. 이 호스트는 신뢰 기관 클러스터 키 제공자 서비스에서 게시한 키 제공자를 사용하여 암호화할 수 있는 워크로드 가상 시스템을 실행합니다.
가상 시스템에 대한 vSphere 암호화	vSphere 가상 시스템 암호화를 사용하면 암호화된 가상 시스템을 생성하고 기존 가상 시스템을 암호화할 수 있습니다. ■ vSphere 6.5부터 vCenter Server는 외부 키 서버로부터 키를 요청합니다. 키 서버가 키를 생성 및 저장하고 배포를 위해 vCenter Server에 키를 전달합니다. ■ vSphere 7.0부터 vSphere Trust Authority와 키 서버 간에 신뢰할 수 있는 연결을 설정할 수 있습니다. 이 설정을 사용하는 경우 vCenter Server 및 워크로드 ESXi 호스트가 키 서버 자격 증명을 직접 요구하지 않아도 되며 심층 방어 보안의 추가 계층을 사용할 수 있습니다.
신뢰할 수 있는 키 제공자	단일 암호화 키를 키 서버에 캡슐화하는 키 제공자입니다. 암호화 키에 액세스하려면 ESXi 소프트웨어가 신뢰할 수 있는 호스트에서 확인되었음을 증명 서비스가 승인해야 합니다.
표준 키 제공자	키 서버에서 암호화 키를 직접 가져와서 데이터 센터의 필수 호스트에 키를 배포하는 키 제공자입니다. vSphere에서 이전 명칭은 KMS 클러스터였습니다.

표 9-1. vSphere 신뢰 기관 용어집 (계속)

용어	정의
키 서버	키 제공자와 연결된 KMIP KMS(키 관리 서버)입니다.
워크로드 vCenter Server	하나 이상의 신뢰할 수 있는 클러스터를 관리하고 구성하는 데 사용되는 vCenter Server입니다.

vSphere 신뢰 기관 기본 사항

vSphere 신뢰 기관을 통해 다음을 할 수 있습니다.

- ESXi 호스트에 하드웨어 신뢰 루트 및 원격 증명 기능을 제공합니다.
- 증명된 ESXi 호스트에만 키를 릴리스하여 암호화 키 관리를 제한합니다.
- 신뢰 관리를 위한 더 나은 보안 관리 환경을 생성합니다.
- 다중 키 서버의 관리를 중앙 집중화합니다.
- 향상된 암호화 키 관리 수준으로 가상 시스템에서 암호화 작업을 계속 수행합니다.

vSphere 6.5 및 6.7에서, 가상 시스템 암호화는 vCenter Server를 통해 키 서버에서 암호화 키를 가져와 이를 필요에 따라 ESXi 호스트로 푸시합니다. vCenter Server는 VECS(VMware Endpoint 인증서 저장소)에 저장되는 클라이언트 및 서버 인증서를 사용하여 키 서버를 인증합니다. 키 서버로부터 전송되는 암호화 키는 vCenter Server 메모리를 통해 필수 ESXi 호스트로 전달됩니다(유선을 통해 TLS에서 제공되는 데이터 암호화 포함). 또한 vSphere는 vCenter Server에서 권한 확인을 통해 사용자 권한을 검증하고 키 서버 액세스 제한을 적용합니다. 이 아키텍처가 안전하기는 하지만 vCenter Server 손상, 악성 vCenter Server 관리자 또는 암호 유출 또는 도난으로 이어질 수 있는 관리 오류나 구성 오류의 가능성을 해결하지는 못합니다.

vSphere 7.0에서 vSphere 신뢰 기관은 이러한 문제점을 해결합니다. 안전하고 관리 가능한 ESXi 호스트 집합으로 구성된 신뢰할 수 있는 컴퓨팅 기반을 생성할 수 있습니다. vSphere 신뢰 기관은 신뢰하려는 ESXi 호스트에 대한 원격 증명 서비스를 구현합니다. 또한 vSphere 신뢰 기관은 TPM 2.0 증명 지원(6.7 릴리스부터 vSphere에 추가됨)을 개선하여 암호화 키에 대한 액세스 제한을 구현하고 가상 시스템 워크로드 암호 보호를 강화합니다. 이 외에도 vSphere 신뢰 기관은 권한 있는 신뢰 기관 관리자만 vSphere 신뢰 기관 서비스 및 신뢰 기관 호스트를 구성할 수 있도록 허용합니다. 신뢰 기관 관리자는 vSphere 관리자와 동일한 사용자이거나 별도의 사용자일 수 있습니다.

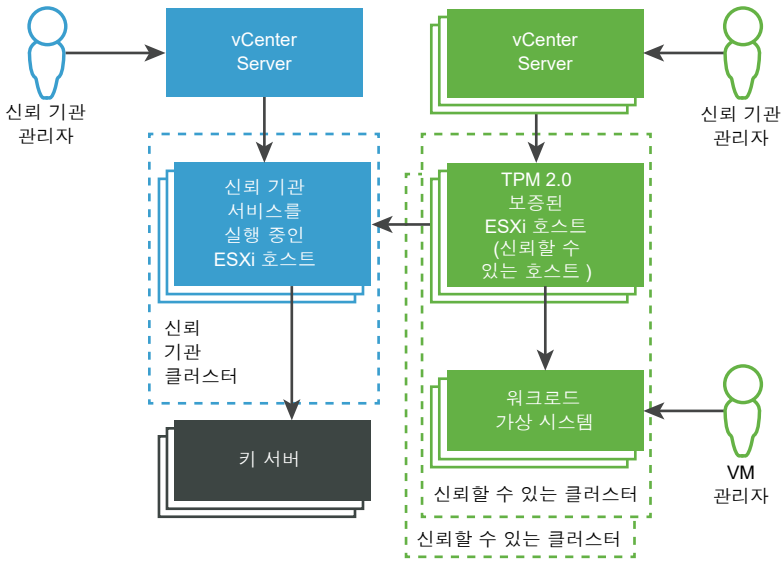
마지막으로 vSphere 신뢰 기관을 사용하면 다음을 통해 더 안전한 보안 환경에서 워크로드를 실행할 수 있습니다.

- 변조 감지
- 무단 변경 불허
- 멀웨어 및 수정 방지
- 민감한 워크로드가 확인되고 안전한 하드웨어 및 소프트웨어 스택에서만 실행되도록 제한

vSphere 신뢰 기관 아키텍처

다음 그림은 vSphere 신뢰 기관 아키텍처의 간단한 보기를 보여 줍니다.

그림 9-1. vSphere 신뢰 기관 아키텍처



이 그림에서:

1 vCenter Server 시스템

별도의 vCenter Server 시스템이 신뢰 기관 클러스터 및 신뢰할 수 있는 클러스터를 관리합니다.

2 신뢰 기관 클러스터

vSphere 신뢰 기관 구성 요소를 실행하는 ESXi 호스트로 구성됩니다.

3 키 서버

암호화 작업이 수행될 때 키 제공자 서비스에서 사용하는 암호화 키를 저장합니다. 키 서버는 vSphere 신뢰 기관 외부에 있습니다.

4 신뢰할 수 있는 클러스터

TPM을 통해 원격으로 증명되고, 암호화된 워크로드를 실행하는 ESXi 신뢰할 수 있는 호스트로 구성됩니다.

5 신뢰 기관 관리자

vCenter Server 신뢰할 수 있는 관리자 그룹의 멤버이며, 신뢰할 수 있는 인프라를 구성하는 관리자입니다.

vSphere 신뢰 기관을 사용하면 유연한 방식으로 신뢰 기관 관리자를 지정할 수 있습니다. 그림의 신뢰 기관 관리자는 개별 사용자일 수 있습니다. 또한 신뢰 기관 관리자가 vCenter Server 시스템 전반에 연결된 자격 증명을 사용하는 동일 사용자일 수도 있습니다. 이 경우 동일한 사용자이며 동일한 신뢰할 수 있는 관리자 그룹입니다.

6 VM 관리자

신뢰할 수 있는 호스트에서 암호화된 워크로드 가상 시스템을 관리할 수 있는 권한이 부여된 관리자입니다.

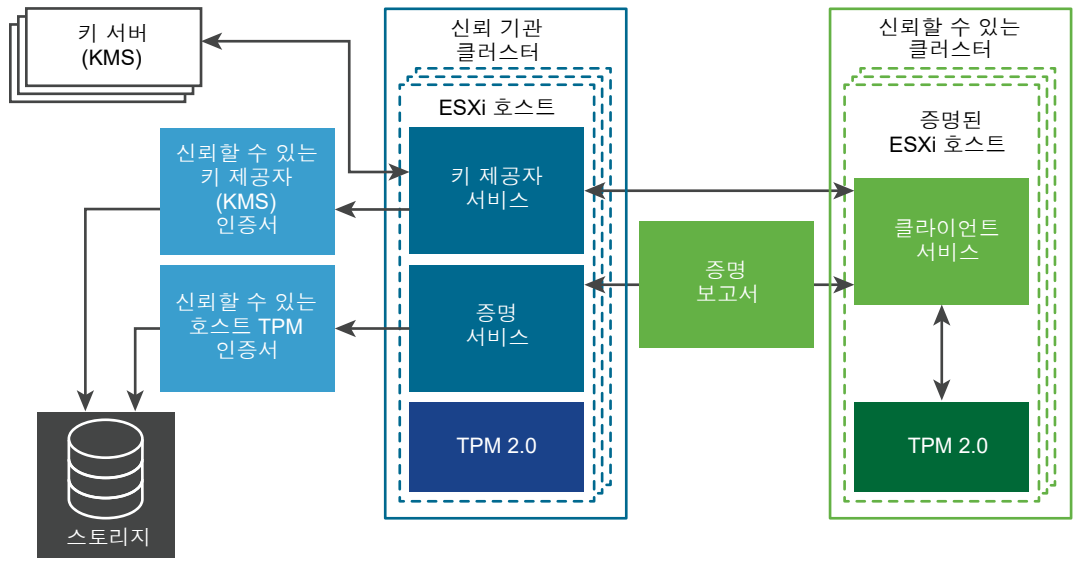
신뢰할 수 있는 인프라 개요

vSphere 신뢰 기관 서비스, 하나 이상의 외부 KMIP 준수 키 서버, vCenter Server 시스템 및 ESXi 호스트는 신뢰할 수 있는 인프라에 포함됩니다.

신뢰할 수 있는 인프라란?

신뢰할 수 있는 인프라는 하나 이상의 vSphere 신뢰 기관 클러스터, 하나 이상의 신뢰할 수 있는 클러스터 및 하나 이상의 외부 KMIP 준수 키 서버로 구성됩니다. 각 클러스터에는 다음 그림에 나와 있는 것처럼 특정 vSphere 신뢰 기관 서비스를 실행하는 ESXi 호스트가 포함됩니다.

그림 9-2. vSphere 신뢰 기관 서비스



신뢰 기관 클러스터 구성은 다음 두 서비스를 지원합니다.

- 증명 서비스
- 키 제공자 서비스

vSphere 신뢰 기관을 구성하는 경우 신뢰할 수 있는 클러스터의 ESXi 호스트가 증명 서비스와 통신합니다. 키 제공자 서비스는 신뢰할 수 있는 호스트와 하나 이상의 신뢰할 수 있는 키 제공자를 중재합니다.

참고 현재 신뢰 기관 클러스터의 ESXi 호스트에는 TPM이 필요하지 않습니다. 하지만 모범 사례로서 TPM과 함께 새 ESXi 호스트 설치를 고려하십시오.

vSphere 신뢰 기관 증명 서비스 정보

증명 서비스는 신뢰할 수 있는 클러스터의 원격 ESXi 호스트의 이진 및 구성 상태를 설명하는 어설션이 포함된 서명된 문서를 생성합니다. 증명 서비스는 TPM(신뢰할 수 있는 플랫폼 모듈) 2.0 칩을 사용하여 ESXi 호스트의 상태를 소프트웨어 측정 및 보고를 위한 기반으로 증명합니다. 원격 ESXi 호스트에 대한 TPM은 소프트웨어 스택을 측정하고 구성 데이터를 증명 서비스로 보냅니다. 증명 서비스는 소프트웨어 측정 서명이 이전에 구성된 신뢰할 수 있는 TPM EK(승인 키)의 영향을 받았을 수 있음을 확인합니다. 또한 증명 서비스는 소프트웨어 측정이 이전에 블레싱된 ESXi 이미지의 집합 중 하나와 일치함을 보장합니다. 증명 서비스는 ESXi 호스트에 발급하는 JWT(JSON 웹 토큰)를 서명하여 ESXi 호스트의 ID, 유효성 및 구성에 대한 증명을 제공합니다.

vSphere 신뢰 기관 키 제공자 서비스란?

키 제공자 서비스를 사용하면 vCenter Server 및 ESXi 호스트가 직접 키 서버 자격 증명을 요구할 필요가 없습니다. vSphere 신뢰 기관에서는 ESXi 호스트가 암호화 키에 액세스하기 위해 키 제공자 서비스로 인증해야 합니다.

키 제공자 서비스를 키 서버에 연결하려면 신뢰 기관 관리자가 신뢰 설정을 구성해야 합니다. 대부분의 KMIP 준수 서버의 경우 신뢰 설정 구성에 클라이언트 및 서버 인증서 구성이 포함됩니다.

키가 ESXi 신뢰할 수 있는 호스트로만 릴리스되도록 하기 위해 키 제공자 서비스는 키 서버에 대한 게이트키퍼 역할을 수행합니다. 키 제공자 서비스는 신뢰할 수 있는 키 제공자의 개념을 사용하여 나머지 데이터 센터 소프트웨어 스택에서 키 서버 세부 사항을 숨깁니다. 각각의 신뢰할 수 있는 키 제공자는 구성된 하나의 기본 암호화 키를 가지며 하나 이상의 키 서버를 참조합니다. 키 제공자 서비스에는 구성된 신뢰할 수 있는 키 제공자가 여러 개 있을 수 있습니다. 예를 들어 조직의 각 부서에 대해 별도의 신뢰할 수 있는 키 제공자를 갖고자 할 수 있습니다. 각각의 신뢰할 수 있는 키 제공자는 서로 다른 기본 키를 사용하지만 동일한 백업 키 서버를 참조할 수 있습니다.

신뢰할 수 있는 키 제공자를 생성한 후에는 키 제공자 서비스가 ESXi 신뢰할 수 있는 호스트의 요청을 수락하여 신뢰할 수 있는 키 제공자에 대한 암호화 작업을 실행할 수 있습니다.

ESXi 신뢰할 수 있는 호스트가 신뢰할 수 있는 키 제공자에 대한 작업을 요청하는 경우 키 제공자 서비스는 암호화 키를 얻으려고 하는 ESXi 호스트가 증명되도록 합니다. 모든 검사를 통과한 후에는 ESXi 신뢰할 수 있는 호스트가 키 제공자 서비스에서 암호화 키를 수신합니다.

vSphere 신뢰 기관에서 사용되는 포트

vSphere 신뢰 기관 서비스는 ESXi 호스트의 역방향 프록시 뒤에서 연결을 수신합니다. 모든 통신은 포트 443에서 HTTPS를 통해 발생합니다.

vSphere 신뢰 기관 신뢰할 수 있는 호스트란?

ESXi 신뢰할 수 있는 호스트는 신뢰할 수 있는 키 제공자를 사용하여 암호화 작업을 수행하도록 구성됩니다. ESXi 신뢰할 수 있는 호스트는 키 제공자 서비스 및 증명 서비스와 통신하여 주요 작업을 수행합니다. 인증 및 권한 부여의 경우 ESXi 신뢰할 수 있는 호스트는 증명 서비스에서 얻은 토큰을 사용합니다. 유효한 토큰을 가져오려면 ESXi 신뢰할 수 있는 호스트가 증명 서비스를 성공적으로 증명해야 합니다. 토큰에는 ESXi 신뢰할 수 있는 호스트가 신뢰할 수 있는 키 제공자에 액세스할 수 있는 권한을 가졌는지 여부를 결정하는 데 사용되는 특정 할당이 포함되어 있습니다.

vSphere 신뢰 기관 및 키 서버

vSphere 신뢰 기관에는 하나 이상의 키 서버 사용이 필요합니다. 이전 vSphere 릴리스에서는 키 서버를 키 관리 서버 또는 KMS라고 했습니다. 현재 vSphere 가상 시스템 암호화 솔루션은 KMIP 1.1 준수 키 서버를 지원합니다.

vSphere 신뢰 기관에서 구성 및 상태 정보를 저장하는 방법

vCenter Server는 대개 vSphere 신뢰 기관 구성 및 상태 정보에 대한 패스스루 서비스입니다. 대부분의 vSphere 신뢰 기관 구성 및 상태 정보는 ConfigStore 데이터베이스의 ESXi 호스트에 저장됩니다. 일부 상태 정보는 vCenter Server 데이터베이스에도 저장되어 있습니다.

참고 대부분의 vSphere 신뢰 기관 구성 정보는 ESXi 호스트에 저장되어 있기 때문에 vCenter Server 파일 기반 백업 메커니즘이 이 정보를 백업하지 않습니다. vSphere 신뢰 기관 배포에 대한 구성 정보가 저장되었는지 확인하려면 vSphere 신뢰 기관 구성 백업의 내용을 참조하십시오.

vSphere 신뢰 기관가 vCenter Server와 통합하는 방법

별도의 vCenter Server 인스턴스를 구성하여 신뢰 기관 클러스터 및 신뢰할 수 있는 클러스터를 관리합니다. vSphere 신뢰 기관 구성의 내용을 참조하십시오.

신뢰할 수 있는 클러스터에서 vCenter Server는 신뢰 기관 API 호출을 관리하고 ESXi 호스트를 통해 전달합니다. vCenter Server는 신뢰할 수 있는 클러스터의 모든 ESXi 호스트에서 API 호출을 복제합니다.

처음에 vSphere 신뢰 기관을 구성한 후 신뢰 기관 클러스터 또는 신뢰할 수 있는 클러스터를 대상으로 ESXi 호스트를 추가하거나 제거할 수 있습니다. vSphere 신뢰 기관 호스트 추가 및 제거의 내용을 참조하십시오.

vSphere 신뢰 기관 프로세스 흐름

신뢰할 수 있는 인프라를 구성하고 관리하는 방법을 알려면 vSphere 신뢰 기관 프로세스 흐름을 이해하는 것이 필수적입니다.

vSphere 신뢰 기관를 구성하는 방법

vSphere 신뢰 기관는 기본적으로 활성화되어 있지 않습니다. 환경에서 수동으로 vSphere 신뢰 기관을 구성해야 합니다. vSphere 신뢰 기관 구성의 내용을 참조하십시오.

vSphere 신뢰 기관를 구성할 때 증명 서비스에서 허용하는 ESXi 소프트웨어의 버전과 신뢰할 수 있는 TPM(신뢰할 수 있는 플랫폼 모듈)을 지정해야 합니다.

TPM 및 증명

이 가이드에서는 TPM 및 증명을 설명할 때 다음 정의를 사용합니다.

표 9-2. TPM 및 증명 용어집

용어	정의
EK(승인 키)	TPM은 EK(승인 키)라고 하는 하드웨어에 내장된 RSA 공용/개인 키 쌍으로 제작됩니다. EK는 특정 TPM에 고유합니다.
EK 공용 키	EK 키 쌍의 공용 부분입니다.
EK 개인 키	EK 키 쌍의 개인 부분입니다.
EK 인증서	서명으로 래핑된 EK 공용 키입니다. EK 인증서는 해당 인증 기관 개인 키를 사용하여 EK 공용 키에 서명하는 TPM 제조업체에서 생성합니다. 모든 TPM에 EK 인증서가 포함되어 있는 것은 아닙니다. 이 경우 EK 공용 키는 서명되어 있지 않습니다.
TPM 증명	원격 호스트에서 실행되고 있는 소프트웨어를 확인하는 증명 서비스의 기능입니다. TPM 증명은 원격 호스트가 시작하는 동안 TPM에서 수행한 암호화 측정을 통해 이루어지고 요청 시 증명 서비스로 릴레이됩니다. 증명 서비스는 EK 공용 키 또는 EK 인증서를 통해 TPM에서 신뢰를 설정합니다.

신뢰할 수 있는 호스트에서 TPM 신뢰 구성

ESXi 신뢰할 수 있는 호스트에는 TPM이 포함되어야 합니다. TPM은 EK(승인 키)라고 하는 하드웨어에 내장된 공용/개인 키 쌍으로 제작됩니다. TPM 2.0은 여러 키/인증서 쌍을 허용하지만 가장 일반적인 것은 RSA-2048 키 쌍입니다. CA에서 TPM EK 공용 키에 서명하면 EK 인증서가 됩니다. TPM 제조업체는 보통 하나 이상의 EK를 미리 생성하고, 인증 기관을 통해 공용 키에 서명한 후, 서명된 인증서를 TPM의 비휘발성 메모리에 포함시킵니다.

다음과 같이 TPM을 신뢰하도록 증명 서비스를 구성할 수 있습니다.

- 제조업체가 TPM에 서명하는 데 사용한 모든 CA 인증서(EK 공용 키)를 신뢰합니다. 증명 서비스에 대한 기본 설정은 CA 인증서를 신뢰하는 것입니다. 이 접근 방법의 경우 동일한 CA 인증서가 많은 ESXi 호스트를 처리하므로 관리 오버헤드가 줄어듭니다.
- ESXi 호스트의 TPM CA 인증서와 EK 공용 키를 신뢰합니다. 후자는 EK 인증서 또는 EK 공용 키일 수 있습니다. 이 접근 방법은 더 강화된 보안을 제공하지만 신뢰할 수 있는 호스트 각각에 대해 정보를 구성해야 합니다.
- 일부 TPM에는 EK 인증서가 포함되어 있지 않습니다. 이 경우에는 EK 공용 키를 신뢰합니다.

모든 TPM CA 인증서를 신뢰하기로 결정하는 것이 운영상 편리합니다. 새 인증서는 새 하드웨어 클래스를 데이터 센터에 추가할 때에만 구성합니다. 개별 EK 인증서를 신뢰하여 액세스를 특정 ESXi 호스트로 제한할 수 있습니다.

TPM CA 인증서를 신뢰하지 않는 것으로 결정할 수도 있습니다. 드문 상황이기는 하지만 CA가 EK에 서명하지 않은 경우 이 구성을 사용할 수 있습니다. 현재 이 기능은 완전히 구현되지 않았습니다.

참고 일부 TPM에는 EK 인증서가 포함되어 있지 않습니다. 개별 ESXi 호스트를 신뢰하려는 경우 TPM에는 EK 인증서가 포함되어야 합니다.

TPM 증명

증명 프로세스를 시작하기 위해 신뢰할 수 있는 클러스터의 ESXi 신뢰할 수 있는 호스트는 미리 구성된 EK 공용 키 및 EK 인증서를 신뢰 기관 클러스터의 증명 서비스로 보냅니다. 증명 서비스에서 요청을 받으면 해당 구성에서 EK를 조회합니다. 이것은 구성에 따라 EK 공용 키 또는 EK 인증서이거나 둘 다일 수 있습니다. 어떤 경우도 유효하지 않으면 증명 서비스가 증명 요청을 거부합니다.

EK는 서명에 직접 사용되지 않으므로 증명 키(AK 또는 AIK)가 협상됩니다. 협상 프로토콜은 새로 생성된 AK가 이전에 확인된 EK에 바인딩되도록 하여 중간자 상황이나 가장 주체를 방지합니다. AK가 협상된 후에는 매번 새로 생성하는 대신 향후 증명 요청에 재사용됩니다.

ESXi 신뢰할 수 있는 호스트는 TPM에서 견적과 PCR 값을 읽습니다. 견적은 AK에서 서명합니다. ESXi 신뢰할 수 있는 호스트는 TCG 이벤트 로그도 읽습니다. 여기에는 현재 PCR 상태를 초래한 모든 이벤트가 포함됩니다. 이 TPM 정보는 검증을 위해 증명 서비스로 전송됩니다. 증명 서비스는 이벤트 로그를 사용하여 PCR 값을 확인합니다.

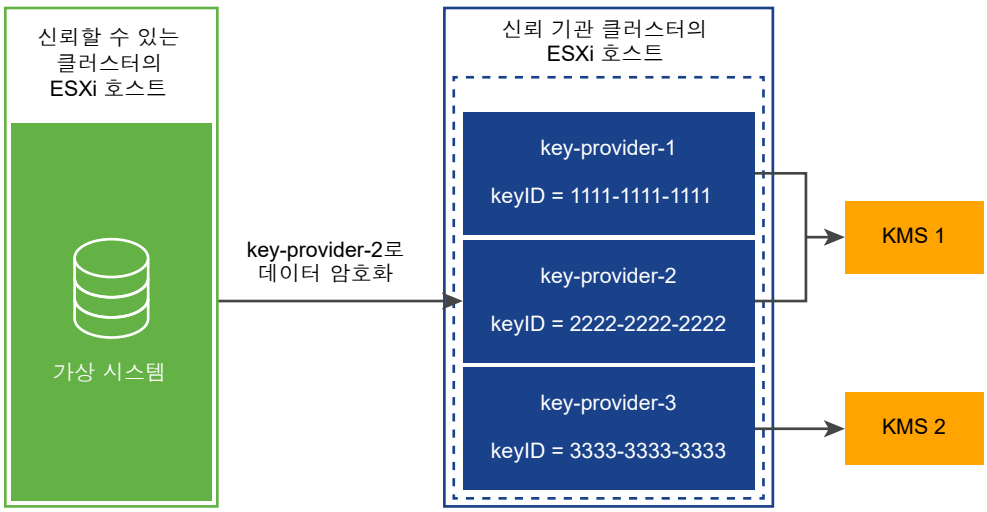
키 제공자가 키 서버와 작동하는 방식

키 제공자 서비스는 신뢰할 수 있는 키 제공자의 개념을 사용하여 나머지 데이터 센터 소프트웨어에서 키 서버의 특정 정보를 숨깁니다. 각각의 신뢰할 수 있는 키 제공자는 구성된 하나의 기본 암호화 키를 가지며 하나 이상의 키 서버를 참조합니다. 기본 암호화 키는 키 서버에 있습니다. vSphere 신뢰 기관 구성의 일부로, 기본 키를 별도의 작업으로 프로비저닝하고 활성화해야 합니다. 키 제공자 서비스에는 구성된 신뢰할 수 있는 키 제공자가 여러 개 있을 수 있습니다. 각각의 신뢰할 수 있는 키 제공자는 서로 다른 기본 키를 사용하지만 동일한 백업 키 서버를 참조할 수 있습니다.

새로운 신뢰할 수 있는 키 제공자가 추가되는 경우 신뢰 기관 관리자는 키 서버와 해당 키 서버에 있는 기존의 키 식별자를 지정해야 합니다.

다음 그림은 키 제공자 서비스와 키 서버 간의 관계를 보여 줍니다.

그림 9-3. 키 제공자 및 키 서버



신뢰할 수 있는 클러스터에 대해 신뢰할 수 있는 키 제공자를 구성한 후에는 키 제공자 서비스에서 해당 신뢰할 수 있는 키 제공자에 대한 암호화 작업 실행 요청을 수락할 수 있습니다. 예를 들어 이 그림에는 3개의 신뢰할 수 있는 키 제공자가 구성되어 있습니다. 두 개는 KMS-1용이고, 나머지 하나는 KMS-2용입니다. 신뢰할 수 있는 호스트가 key-provider-2에 대해 암호화 작업을 요청합니다. 신뢰할 수 있는 호스트는 암호화 키의 생성 및 반환을 요청하고 이 암호화 키를 사용하여 암호화 작업을 수행합니다.

키 제공자 서비스는 key-provider-2에서 참조하는 기본 키를 사용하여 지정된 일반 텍스트 데이터를 암호화하고 해당하는 암호를 반환합니다. 이후, 신뢰할 수 있는 호스트는 동일한 암호를 암호 해독 작업에 제공하고 원래 일반 텍스트를 다시 가져올 수 있습니다.

vSphere 신뢰 기관 인증 및 권한 부여

vSphere 신뢰 기관 관리 작업에는 신뢰할 수 있는 관리자 그룹의 멤버인 사용자가 필요합니다. 신뢰 기관 관리자 권한만으로는 ESXi 호스트와 관련된 모든 관리 작업을 수행할 수 없습니다. 자세한 내용은 vSphere 신뢰 기관에 대한 사전 요구 사항 및 필요한 권한의 내용을 참조하십시오.

신뢰할 수 있는 클러스터에 신뢰할 수 있는 호스트 추가

ESXi 호스트를 처음에 신뢰할 수 있는 클러스터에 추가하는 단계는 vSphere 신뢰 기관 구성에 설명되어 있습니다.

나중에 ESXi 호스트를 신뢰할 수 있는 클러스터에 추가하려는 경우에는 워크플로가 달라집니다. vSphere 신뢰 기관 호스트 추가 및 제거의 내용을 참조하십시오.

ESXi 호스트를 처음에 신뢰할 수 있는 클러스터에 추가할 때에는 다음 정보를 수집해야 합니다.

- 클러스터의 각 하드웨어 유형에 대한 TPM 인증서
- 클러스터의 각 ESXi 버전에 대한 ESXi 이미지
- vCenter Server 주체 정보

ESXi 호스트를 나중에 신뢰할 수 있는 클러스터에 추가하는 경우에는 일부 추가 정보를 수집해야 할 수 있습니다. 즉, 새 ESXi 호스트의 하드웨어 버전이나 ESXi 버전이 원래 호스트와 다른 경우에는 새 ESXi 호스트 정보를 수집한 후 신뢰 기관 클러스터로 가져와야 합니다. vCenter Server 시스템별로 한 번만 vCenter Server 주체 정보를 수집해야 합니다.

vSphere 신뢰 기관 토폴로지

vSphere 신뢰 기관을 사용하려면 신뢰 기관 클러스터 및 신뢰할 수 있는 클러스터에 대해 별도의 vCenter Server 시스템이 필요합니다.

신뢰 기관 클러스터는 독립되고 분리된 vCenter Server에서 구성 및 관리됩니다. 신뢰 기관 클러스터의 vCenter Server는 동시에 신뢰할 수 있는 클러스터의 vCenter Server가 될 수 없습니다. 신뢰할 수 있는 클러스터에는 고유한 별도의 vCenter Server가 있어야 합니다. 하나의 vCenter Server가 여러 개의 신뢰할 수 있는 클러스터를 관리할 수 있습니다. 신뢰할 수 있는 클러스터의 여러 vCenter Server 시스템은 고급 연결 모드에 참여할 수 있습니다. 신뢰 기관 클러스터의 vCenter Server는 다른 신뢰 기관 클러스터 vCenter Server 시스템 또는 신뢰할 수 있는 클러스터 vCenter Server 시스템과 함께 고급 연결 모드에 참여할 수 없습니다.

신뢰 기관 관리자는 신뢰 기관 클러스터와 여기에 연결된 vCenter Server를 다른 vCenter Server 인스턴스에 독립적으로 관리합니다. 이러한 접근 방식이 최상의 보안 격리를 제공하기 때문입니다.

신뢰 기관 관리자는 신뢰할 수 있는 클러스터 관리자가 해당 클러스터를 구성하는 데 사용하는 호스트 이름과 SSL 인증서를 문서화하거나 게시합니다. 또한 신뢰 기관 관리자는 조직과 해당 부서 또는 개별 관리자에 대해서도 신뢰할 수 있는 키 제공자를 프로비저닝합니다.

vSphere 신뢰 기관 서비스를 워크로드 vCenter Server에서 관리하는 신뢰할 수 있는 클러스터에 직접 배포할 수 없습니다. 워크로드 관리자가 ESXi 호스트에 대한 높은 액세스 권한을 가지고 있기 때문입니다. 이러한 유형의 배포는 vSphere 신뢰 기관의 보안 목표를 충족하는 데 필요한 역할을 분리하지 못합니다.

vSphere 신뢰 기관에 대한 사전 요구 사항 및 필요한 권한

vSphere 신뢰 기관을 구성할 때에는 하드웨어 및 소프트웨어 요구 사항을 고려해야 합니다. 암호화를 사용하려면 암호화 권한 및 역할을 설정해야 합니다. vSphere 신뢰 기관 작업을 수행하는 사용자에게 적절한 권한이 있어야 합니다.

vSphere 신뢰 기관에 대한 요구 사항

vSphere 신뢰 기관을 사용하려면 vSphere 환경이 다음과 같은 요구 사항을 충족해야 합니다.

- ESXi 신뢰할 수 있는 호스트 하드웨어 요구 사항:
  - TPM 2.0
  - 보안 부팅 사용
  - EFI 펌웨어
- 구성 요소 요구 사항:
  - vCenter Server 7.0 이상
  - vSphere 신뢰 기관 클러스터 및 ESXi 호스트에 대한 전용 vCenter Server 시스템
  - 신뢰할 수 있는 클러스터 및 ESXi 신뢰할 수 있는 호스트에 대한 별도의 vCenter Server 시스템
  - 키 서버(이전 vSphere 릴리스에서는 KMS(키 관리 서버)라고 함)
- 가상 시스템 요구 사항:
  - EFI 펌웨어
  - 보안 부팅 사용

참고 vSphere 신뢰 기관 구성을 시작하려면 신뢰 기관 클러스터 및 신뢰할 수 있는 클러스터에 대한 vCenter Server 시스템을 설정한 후 ESXi 호스트를 각 클러스터에 추가했는지 확인합니다.

암호화 권한

vSphere 신뢰 기관에 추가된 새로운 암호화 권한은 없습니다. 암호화 권한 및 역할에 설명된 것과 동일한 암호화 권한이 vSphere 신뢰 기관에 적용됩니다.

호스트 암호화 모드

ESXi 신뢰할 수 있는 호스트에서 호스트 암호화 모드를 사용하도록 설정하기 위해 vSphere 신뢰 기관에 추가된 새로운 요구 사항은 없습니다. 호스트 암호화 모드에 대한 자세한 내용은 암호화 작업의 사전 요구 사항 및 필요한 권한 항목을 참조하십시오.

vSphere 신뢰 기관 역할 및 신뢰할 수 있는 관리자 그룹

vSphere 신뢰 기관 작업에는 신뢰할 수 있는 관리자 그룹의 멤버인 사용자가 필요합니다. 이 사용자를 신뢰 기관 관리자라고 합니다. vSphere 관리자는 자기 자신을 신뢰할 수 있는 관리자 그룹에 추가하거나 다른 사용자를 이 그룹에 추가하여 신뢰할 수 있는 인프라 관리자 역할을 얻어야 합니다. 신뢰할 수 있는 인프라 관리자 역할은 vCenter Server 인증을 위해 필요합니다. 신뢰할 수 있는 관리자 그룹은 신뢰할 수 있는 인프라의 일부인 ESXi 호스트에서의 인증을 위해 필요합니다. ESXi 호스트에서 **암호화 작업.호스트 등록** 권한을 가진 사용자는 신뢰할 수 있는 클러스터를 관리할 수 있습니다. vCenter Server 사용 권한은 신뢰 기관 호스트에 전파되지 않고 신뢰할 수 있는 호스트에만 전파됩니다. 신뢰할 수 있는 관리자 그룹의 멤버에게만 신뢰 기관 호스트에 대한 권한이 부여됩니다. 그룹 멤버 자격은 ESXi 호스트 자체에서 확인됩니다.

참고 vSphere 관리자와 관리자 그룹의 멤버에게는 신뢰할 수 있는 인프라 관리자 역할이 할당되지만 이 역할 자체만으로는 사용자가 vSphere 신뢰 기관 작업을 수행하도록 허용되지 않습니다. 신뢰할 수 있는 관리자 그룹의 멤버 자격도 필요합니다.

vSphere 신뢰 기관이 사용되도록 설정되면 신뢰 기관 관리자가 신뢰할 수 있는 호스트에 신뢰할 수 있는 키 제공자를 할당할 수 있습니다. 그러면 신뢰할 수 있는 호스트가 신뢰할 수 있는 키 제공자를 사용하여 암호화 작업을 수행할 수 있습니다.

vSphere 신뢰 기관은 신뢰할 수 있는 인프라 관리자 역할 외에도 vSphere 신뢰 기관 API를 호출하는 권한을 제외한 vCenter Server의 모든 권한이 포함된 신뢰할 수 있는 인프라 관리자 없음 역할을 제공합니다.

vSphere 신뢰 기관 그룹, 역할 및 사용자는 다음과 같이 작동합니다.

- 처음 부팅 시 vSphere는 신뢰할 수 있는 관리자 그룹에 글로벌 사용 권한을 가진 신뢰할 수 있는 인프라 관리자 역할을 부여합니다.
- 신뢰할 수 있는 인프라 관리자 역할은 vSphere 신뢰 기관 API(`TrustedAdmin.*`)를 호출하는 데 필요한 권한과 인벤토리 개체를 보기 위한 시스템 권한 **System.Read**, **System.View** 및 **System.Anonymous**를 가진 시스템 역할입니다.
- 신뢰할 수 있는 인프라 관리자 없음 역할은 vSphere 신뢰 기관 API를 호출하는 권한을 제외한 모든 vCenter Server 권한이 포함된 시스템 역할입니다. vCenter Server에 새 권한을 추가하면 해당 권한이 신뢰할 수 있는 인프라 관리자 없음 역할에도 추가됩니다. (신뢰할 수 있는 인프라 관리자 없음 역할은 암호화 관리자 없음 역할과 유사합니다.)
- 암호화 관리자 없음 역할에는 vSphere 신뢰 기관 권한(`TrustedAdmin.*` API)이 포함되어 있지 않으므로 이 역할을 가진 사용자는 신뢰할 수 있는 인프라를 설정하거나 암호화 작업을 수행할 수 없습니다.

이러한 사용자, 그룹 및 역할에 대한 사용 사례가 다음 표에 표시되어 있습니다.

표 9-3. vSphere 신뢰 기관 사용자, 그룹 및 역할

사용자, 그룹 또는 역할	vSphere 신뢰 기관 vCenter Server API 호출(vSphere 신뢰 기관 ESXi API에 대한 호출 포함) 가능	vSphere 신뢰 기관 vCenter Server API 호출(vSphere 신뢰 기관 ESXi API에 대한 호출 불포함) 가능	vSphere 신뢰 기관와 관련되지 않은 클러스터에서 호스트 작업 수행 가능	설명
Administrators@*system.domain* 그룹 및 TrustedAdmins@*system.domain* 그룹의 사용자	예	예	예	해당 없음
TrustedAdmins@*system.domain* 그룹의 사용자만	예	예	아니요	이러한 사용자는 정기적인 클러스터 관리 작업을 수행할 수 없음
Administrators@*system.domain* 그룹의 사용자만	예	아니요	예	해당 없음
신뢰할 수 있는 인프라 관리자 역할이 있지만 TrustedAdmins@*system.domain* 그룹에 없는 사용자	예	아니요	아니요	ESXi 호스트는 사용 권한 부여를 위해 사용자의 그룹 멤버 자격을 검사합니다.
신뢰할 수 있는 인프라 관리자 없음 역할만 있는 사용자	아니요	아니요	예	이러한 사용자는 vSphere 신뢰 기관 작업을 수행할 수 없는 관리자와 유사합니다.

vSphere 신뢰 기관 모범 사례, 주의 사항 및 상호 운용성

vSphere 신뢰 기관 아키텍처에는 몇 가지 추가적인 권장 사항이 있습니다. vSphere 신뢰 기관 전략을 계획할 때에는 상호 운용성 제한 사항을 고려해야 합니다.

신뢰할 수 있는 인프라 상호 운용성

ESXi 버전의 경우, 증명 서비스는 이전 버전 및 이후 버전 호환이 가능합니다. 예를 들어 vSphere 신뢰 기관 클러스터에서 ESXi 7.0을 실행하는 ESXi 호스트의 클러스터를 보유한 상태에서 신뢰할 수 있는 클러스터의 ESXi 호스트를 최신의 ESXi 버전으로 업그레이드 또는 패치할 수 있습니다. 마찬가지로, 신뢰할 수 있는 클러스터에서 현재 버전의 ESXi 호스트를 유지하는 동안 신뢰 기관 클러스터의 ESXi 호스트를 업그레이드하거나 패치할 수 있습니다.

하나의 클러스터 기능을 신뢰 기관 클러스터와 신뢰할 수 있는 클러스터 둘 다로 사용할 수 없습니다. 이 구성은 지원되지 않습니다.

신뢰할 수 있는 클러스터 구성 제한

워크로드 vCenter Server당 신뢰할 수 있는 클러스터는 하나만 구성할 수 있습니다. 신뢰할 수 있는 클러스터 하나가 여러 개의 신뢰 기관 클러스터를 참조하도록 구성할 수 없습니다.

지원되는 기능

vSphere 신뢰 기관은 다음을 지원합니다.

- vCenter HA(vCenter High Availability)
- VMware vSphere High Availability
- DRS
- DPM
- SRM, 참고:
  - 복구 측에서 동일한 vSphere 신뢰 기관 서비스 구성을 사용할 수 있는 경우 어레이 기반 복제가 포함된 SRM이 지원됩니다.
  - SPPG
- VADP
  - 지원은 표준 암호화와 동일합니다. Hot Add 및 NFC 모드는 지원되지만 SAN 모드는 지원되지 않습니다. 백업이 암호 해독됩니다. VADP 파트너는 원래 가상 시스템과 동일한 암호화 키를 사용하여 백업 가상 시스템을 복구할 수 있습니다.
- vSAN
  - 가상 시스템 암호화는 vSAN에서 완전하게 지원됩니다.
- OVF
  - 암호화된 가상 시스템을 OVF로 내보낼 수 없습니다. 하지만 OVF에서 가져오는 동안 가상 시스템을 암호화할 수는 있습니다.
- vVol

지원되지 않는 기능

현재 vSphere 신뢰 기관은 다음을 지원하지 않습니다.

- vSAN 암호화
- FCD(First Class Disk) 암호화
- vSphere Replication
- vSphere 호스트 프로파일

vSphere 신뢰 기관 수명 주기

vSphere 신뢰 기관 서비스는 기본 ESXi 이미지의 일부로 패키지가 구성되고 설치됩니다.

서비스 시작 및 중지

vSphere Client에서는 ESXi 호스트에서 실행되는 vSphere 신뢰 기관 서비스를 시작, 중지 및 다시 시작할 수 있습니다. 구성 변경 후 또는 기능적 또는 성능 문제가 의심되는 경우 서비스를 다시 시작할 수 있습니다. ESXi 신뢰할 수 있는 호스트에서 서비스를 다시 시작하려면 호스트 자체에 로그인하여 서비스를 다시 시작해야 합니다. vSphere 신뢰 기관 서비스 시작, 중지 및 다시 시작의 내용을 참조하십시오.

업그레이드 및 패치 적용

ESXi 신뢰할 수 있는 호스트를 업그레이드하거나 패치를 적용할 때마다 새 ESXi 버전 정보로 vSphere 신뢰 기관 클러스터를 업데이트해야 합니다. 그렇게 하는 한 가지 방법은 테스트 ESXi 호스트를 업그레이드하거나 패치를 적용하고 ESXi 기본 이미지 정보를 내보내고 이미지 파일을 신뢰 기관 클러스터로 가져온 다음 ESXi 신뢰할 수 있는 호스트를 업그레이드하거나 패치를 적용하는 것입니다.

업그레이드 모범 사례

vSphere 신뢰 기관 인프라를 업그레이드하기 위한 모범 사례는 먼저 신뢰 기관 vCenter Server 및 신뢰 기관 호스트를 업그레이드하는 것입니다. 이러한 방식으로 최신 vSphere 신뢰 기관 기능에서 가장 많은 이점을 얻을 수 있습니다. 그러나 특정 비즈니스 이유에 맞게 vCenter Server 및 ESXi 호스트의 별도의 독립형 업그레이드를 수행할 수 있습니다.

일반적으로 다음 순서에 따라 vSphere 신뢰 기관 인프라를 업그레이드합니다.

1 신뢰 기관 클러스터 vCenter Server를 업그레이드합니다.

2 신뢰 기관 호스트를 업그레이드합니다.

3 신뢰할 수 있는 클러스터 vCenter Server를 업그레이드합니다.

4 신뢰할 수 있는 호스트를 업그레이드합니다.

원활한 프로세스를 보장하려면 신뢰 기관 호스트와 신뢰할 수 있는 호스트를 하나씩 점진적으로 업그레이드합니다.

업그레이드 문제 해결

신뢰 기관 호스트의 업그레이드가 실패하는 경우 다음 단계를 수행합니다.

1 신뢰할 수 있는 클러스터에서 신뢰 기관 호스트를 제거합니다.

2 이전 버전의 ESXi로 되돌립니다.

3 https://kb.vmware.com/s/article/77234의 VMware 기술 자료 문서에 설명된 대로 신뢰 기관 호스트를 클러스터에 다시 추가합니다.

4 신뢰 기관 호스트의 구성이 신뢰 기관 클러스터의 다른 신뢰 기관 호스트와 일치하는지 확인합니다. 신뢰할 수 있는 클러스터 상태 확인의 내용을 참조하십시오.

신뢰할 수 있는 호스트에서 새 버전의 ESXi로 업그레이드하는 경우 새 ESXi 기본 이미지 정보를 사용하여 신뢰 기관 클러스터를 업데이트할 때까지 증명이 실패합니다. 이 동작은 예상된 동작입니다. 더 이상 가상 시스템을 암호화하거나 문제를 해결할 때까지 업그레이드 전에 암호화된 기존 가상 시스템을 사용할 수 없습니다. 증명 오류 메시지는 vSphere Client **최근 작업** 창 및 `attestd.log`, `kmxa.log` 및 `vpxd.log` 파일에 표시됩니다.

문제를 수정하려면 다음 단계를 수행합니다.

1 `Export-VMHostImageDb` cmdlet을 실행하여 ESXi 기본 이미지를 다시 내보냅니다. 신뢰할 수 있는 ESXi 호스트 및 vCenter Server에 대한 정보 수집의 5단계를 참조하십시오.

2 `New-TrustAuthorityVMHostBaseImage` cmdlet을 실행하여 새 기본 이미지를 신뢰 기관 클러스터의 vCenter Server로 다시 가져옵니다. 신뢰 기관 클러스터로 신뢰할 수 있는 호스트 정보 가져오기의 8단계를 참조하십시오.

3 이전 버전의 ESXi를 더 이상 증명할 필요가 없는 경우(모든 신뢰할 수 있는 호스트가 업그레이드됨) `Remove-TrustAuthorityVMHostBaseImage` cmdlet을 실행하여 해당 버전을 제거합니다. 예:

```
$vTA = Get-TrustAuthorityCluster 'vTA Cluster'
$baseImages = Get-TrustAuthorityVMHostBaseImage -TrustAuthorityCluster $vTA
Remove-TrustAuthorityVMHostBaseImage -VMHostBaseImage $baseImages
```

vSphere 신뢰 기관 구성 백업

대부분의 vSphere 신뢰 기관 구성 정보는 ESXi 호스트에 저장되어 있기 때문에 vCenter Server 백업이 이 vSphere 신뢰 기관 정보를 백업하지 않습니다. vSphere 신뢰 기관 구성 백업의 내용을 참조하십시오.

vSphere 신뢰 기관 구성

vSphere 신뢰 기관은 기본적으로 사용되도록 설정되어 있지 않습니다. vSphere 신뢰 기관 사용을 시작하려면 먼저 해당 환경을 구성해야 합니다.

vSphere 신뢰 기관 클러스터라고 하는 전용 vCenter Server 클러스터에서 vSphere 신뢰 기관 서비스를 사용하도록 설정합니다. 신뢰 기관 클러스터는 중앙 집중식 보안 관리 플랫폼으로 작동합니다. 그런 다음 워크로드 vCenter Server 클러스터를 신뢰할 수 있는 클러스터로 사용하도록 설정합니다. 신뢰할 수 있는 클러스터에는 ESXi 신뢰할 수 있는 호스트가 포함됩니다.

신뢰 기관 클러스터는 신뢰할 수 있는 클러스터의 ESXi 호스트를 원격으로 증명합니다. 신뢰 기관 클러스터는 신뢰할 수 있는 키 제공자를 사용하여 가상 시스템 및 가상 디스크를 암호화할 수 있도록, 신뢰할 수 있는 클러스터의 증명된 ESXi 호스트에만 암호화 키를 릴리스합니다.

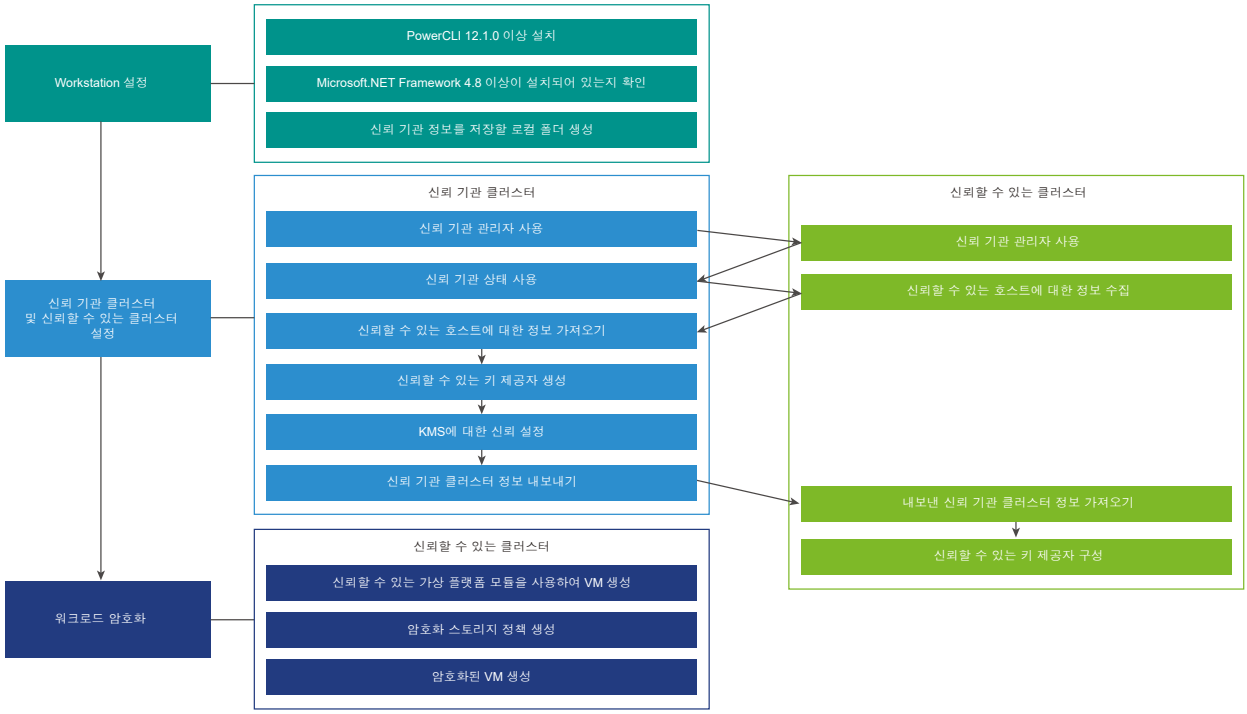
vSphere 신뢰 기관 구성을 시작하기 전에 vSphere 신뢰 기관에 대한 사전 요구 사항 및 필요한 권한에서 vCenter Server 시스템 및 ESXi 호스트의 필수 설정에 대한 자세한 내용을 참조하십시오.

vSphere 신뢰 기관의 다양한 측면은 다음과 같은 방법으로 관리할 수 있습니다.

- PowerCLI cmdlet 또는 vSphere API를 사용하여 vSphere 신뢰 기관 서비스 및 신뢰할 수 있는 연결을 구성합니다. "VMware PowerCLI Cmdlet 참조" 및 "vSphere Automation SDK 프로그래밍 가이드" 를 참조하십시오.

- PowerCLI cmdlet를 사용하거나 vSphere Client에서 신뢰할 수 있는 키 제공자의 구성을 관리합니다.
- 이전 vSphere 릴리스와 마찬가지로 vSphere Client 및 API를 사용하여 암호화 워크플로를 수행합니다.

그림 9-4. vSphere Trust Authority 워크플로



vSphere 신뢰 기관를 구성하고 관리하려면 VMware PowerCLI를 사용하지만 일부 기능은 vSphere Client에서 사용할 수 있습니다.

vSphere 신뢰 기관를 구성할 때는 신뢰 기관 클러스터와 신뢰할 수 있는 클러스터 모두에서 설정 작업을 완료해야 합니다. 이러한 작업 중 일부는 순서대로 수행해야 합니다. 이 가이드에 설명된 작업 순서를 사용하십시오.

참고 초기 vSphere 신뢰 기관 설정을 완료한 후 신뢰할 수 있는 클러스터에 ESXi 호스트를 더 추가할 때는 신뢰할 수 있는 호스트 정보를 다시 내보내고 가져와야 할 수도 있습니다. 즉, 새 ESXi 호스트가 원래 호스트와 다르면 새 ESXi 호스트 정보를 수집하여 신뢰 기관 클러스터로 가져와야 합니다. vSphere 신뢰 기관 호스트 추가 및 제거의 내용을 참조하십시오.

절차

1 Workstation 설정

vSphere 신뢰 기관 배포를 구성하려면 먼저 필요한 소프트웨어 및 설정으로 Workstation을 준비해야 합니다.

2 신뢰 기관 관리자 사용

vSphere 신뢰 기관를 사용하도록 설정하려면 vSphere 신뢰할 수 있는 관리자 그룹에 사용자를 추가해야 합니다. 이 사용자는 신뢰 기관 관리자가 됩니다. 대부분의 vSphere 신뢰 기관 구성 작업에는 신뢰 기관 관리자를 사용합니다.

3 신뢰 기관 상태 사용

vCenter Server 클러스터를 vSphere 신뢰 기관 클러스터로 만들면(신뢰 기관 상태 사용이라고도 함) 클러스터의 ESXi 호스트에서 필수 신뢰 기관 서비스가 시작됩니다.

4 신뢰할 수 있는 ESXi 호스트 및 vCenter Server에 대한 정보 수집

신뢰를 설정하려면 vSphere 신뢰 기관 클러스터에 신뢰할 수 있는 클러스터의 ESXi 호스트 및 vCenter Server에 대한 정보가 필요합니다. 신뢰 기관 클러스터로 가져오기 위해 이 정보를 파일로 내보냅니다. 이러한 파일은 기밀로 유지해야 하며 안전하게 전송해야 합니다.

5 신뢰 기관 클러스터로 신뢰할 수 있는 호스트 정보 가져오기

신뢰 기관 클러스터에서 증명 가능한 호스트를 파악할 수 있도록 내보낸 ESXi 호스트 및 vCenter Server 정보를 vSphere 신뢰 기관 클러스터로 가져옵니다.

6 신뢰 기관 클러스터에서 키 제공자 생성

키 제공자 서비스가 키 제공자에 연결하려면, 신뢰할 수 있는 키 제공자를 생성한 다음 vSphere 신뢰 기관 클러스터와 키 서버(KMS) 간에 신뢰 설정을 구성해야 합니다. 대부분의 KMIP 준수 키 서버의 경우, 이 구성에는 클라이언트 및 서버 인증서 설정이 포함됩니다.

7 신뢰 기관 클러스터 정보 내보내기

신뢰할 수 있는 클러스터가 vSphere 신뢰 기관 클러스터에 연결되려면 신뢰 기관 클러스터의 서비스 정보를 파일 형태로 내보낸 다음, 이 파일을 신뢰할 수 있는 클러스터로 가져와야 합니다. 이러한 파일은 기밀로 유지해야 하며 안전하게 전송해야 합니다.

8 신뢰할 수 있는 호스트로 신뢰 기관 클러스터 정보 가져오기

vSphere 신뢰 기관 클러스터 정보를 신뢰할 수 있는 클러스터로 가져오면 신뢰할 수 있는 호스트에서 신뢰 기관 클러스터를 사용하여 증명 프로세스를 시작합니다.

9 vSphere Client를 사용하여 신뢰할 수 있는 호스트를 위한 신뢰할 수 있는 키 제공자 구성

vSphere Client를 사용하여 신뢰할 수 있는 키 제공자를 구성할 수 있습니다.

10 명령줄을 사용하여 신뢰할 수 있는 호스트를 위한 신뢰할 수 있는 키 제공자 구성

명령줄을 사용하여 신뢰할 수 있는 키 제공자를 구성할 수 있습니다. vCenter Server 서버에 대해 또는 vCenter 개체 계층의 클러스터 또는 폴더 수준에서 신뢰할 수 있는 기본 키 제공자를 구성할 수 있습니다.

Workstation 설정

vSphere 신뢰 기관 배포를 구성하려면 먼저 필요한 소프트웨어 및 설정으로 Workstation을 준비해야 합니다.

vSphere 신뢰 기관 환경에 액세스할 수 있는 Workstation에서 다음 단계를 수행합니다.

절차

1 PowerCLI 12.1.0 이상을 설치합니다. "PowerCLI 사용자 가이드" 를 참조하십시오.

2 Microsoft .NET Framework 4.8 이상이 설치되어 있는지 확인합니다.

3 파일로 내보내는 신뢰 기관 정보를 저장할 로컬 폴더를 생성합니다.

다음에 수행할 작업

신뢰 기관 관리자 사용으로 계속 진행합니다.

신뢰 기관 관리자 사용

vSphere 신뢰 기관를 사용하도록 설정하려면 vSphere 신뢰할 수 있는 관리자 그룹에 사용자를 추가해야 합니다. 이 사용자는 신뢰 기관 관리자가 됩니다. 대부분의 vSphere 신뢰 기관 구성 작업에는 신뢰 기관 관리자를 사용합니다.

vCenter Server 관리자가 아닌 사용자를 신뢰 기관 관리자로 지정하십시오. 독립된 사용자를 지정하면 환경의 보안이 강화됩니다. 신뢰 기관 클러스터 및 신뢰할 수 있는 클러스터 모두에 대해 신뢰 기관 관리자를 사용하도록 설정해야 합니다.

사전 요구 사항

신뢰 기관 관리자가 될 사용자를 만들거나 기존 사용자를 식별합니다.

절차

1 vSphere Client를 사용하여 신뢰 기관 클러스터의 vCenter Server에 연결합니다.

2 관리자로 로그인합니다.

3 **홈** 메뉴에서 **관리**를 선택합니다.

4 **Single Sign-On**에서 **사용자 및 그룹**을 클릭합니다.

5 **그룹**을 클릭하고 **신뢰할 수 있는 관리자** 그룹을 클릭합니다.

   신뢰할 수 있는 관리자 그룹이 처음에 나타나지 않으면 **필터** 아이콘을 사용하여 필터링하거나 창의 맨 아래에 있는 오른쪽 화살표를 클릭하여 그룹을 살펴봅니다.

6 **그룹 멤버** 영역에서 **멤버 추가**를 클릭합니다.

   로컬 ID 소스가 선택되어 있는지 확인하고(vsphere.local이 기본값이지만 설치 중에 다른 도메인을 선택했을 수 있음) 그룹에 신뢰 기관 관리자로 추가할 멤버(사용자)를 검색합니다.

7 멤버를 선택합니다.

8 **저장**을 클릭합니다.

9 신뢰할 수 있는 클러스터의 vCenter Server에 대해 1-8단계를 반복합니다.

다음에 수행할 작업

신뢰 기관 상태 사용으로 계속 진행합니다.

신뢰 기관 상태 사용

vCenter Server 클러스터를 vSphere 신뢰 기관 클러스터로 만들면(신뢰 기관 상태 사용이라고도 함) 클러스터의 ESXi 호스트에서 필수 신뢰 기관 서비스가 시작됩니다.

사전 요구 사항

- 신뢰 기관 관리자 사용.

절차

1 PowerCLI 세션에서 `Connect-VIServer` cmdlet을 실행하여 신뢰 기관 클러스터의 vCenter Server에 신뢰 기관 관리자 사용자로 연결합니다.

```
Connect-VIServer -server TrustAuthorityCluster_VC_ip_address -User trust_admin_user
-Password 'password'
```

2 클러스터의 현재 상태를 확인하려면 `Get-TrustAuthorityCluster` cmdlet을 실행합니다.

예를 들어 이 명령은 `vTA Cluster`라는 클러스터가 사용 안 함 상태인 것을 보여줍니다.

```
Get-TrustAuthorityCluster

Name                 State                Id
----                 -----                --
vTA Cluster          Disabled             TrustAuthorityCluster-domain-c8
```

출력은 발견된 각 클러스터의 [상태] 열에 [사용] 또는 [사용 안 함]을 표시합니다. [사용 안 함]은 신뢰 기관 서비스가 실행되고 있지 않음을 의미합니다.

3 신뢰 기관 클러스터를 사용하도록 설정하려면 `Set-TrustAuthorityCluster` cmdlet을 실행합니다.

예를 들어 이 명령은 `vTA Cluster`라는 클러스터를 사용하도록 설정합니다.

```
Set-TrustAuthorityCluster -TrustAuthorityCluster 'vTA Cluster' -State Enabled
```

시스템에서 확인 메시지로 응답합니다.

```
Confirmation
Setting TrustAuthorityCluster 'vTA Cluster' with new State 'Enabled'. Do you want to
proceed?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"):
```

4 확인 메시지가 표시되면 Enter 키를 누릅니다. (기본값은 **Y**입니다.)

출력은 클러스터의 상태를 보여 줍니다. 예를 들어 다음은 `vTA Cluster`라는 클러스터가 사용되도록 설정된 것을 보여줍니다.

```
Name                 State                Id
----                 -----                --
vTA Cluster          Enabled              TrustAuthorityCluster-domain-c8
```

결과

두 개의 서비스, 즉 증명 서비스와 키 제공자 서비스가 신뢰 기관 클러스터의 ESXi 호스트에서 시작됩니다.

예제: 신뢰 기관 클러스터에서 신뢰됨 상태 사용

이 예는 PowerCLI를 사용하여 신뢰 기관 클러스터에서 서비스를 사용하도록 설정하는 방법을 보여 줍니다. 다음 표에는 사용되는 예제 구성 요소 및 값이 나와 있습니다.

표 9-4. vSphere 신뢰 기관 설정 예

구성 요소	값
신뢰 기관 클러스터의 vCenter Server	192.168.210.22
신뢰 기관 클러스터 이름	vTA 클러스터
신뢰 기관 관리자	trustedadmin@vsphere.local

```
PS C:\Users\Administrator.CORP> Disconnect-VIServer -server * -Confirm:$false
PS C:\Users\Administrator.CORP> Connect-VIServer -server 192.168.210.22 -User
trustedadmin@vsphere.local -Password 'VMware1!'

Name                           Port  User
----                           ----  ----
192.168.210.22                 443   VSPHERE.LOCAL\trustedadmin

PS C:\Users\Administrator.CORP> Get-TrustAuthorityCluster

Name                 State                Id
----                 -----                --
vTA Cluster          Disabled             TrustAuthorityCluster-domain-c8

PS C:\Users\Administrator.CORP> Set-TrustAuthorityCluster -TrustAuthorityCluster 'vTA
Cluster' -State Enabled

Confirmation
Setting TrustAuthorityCluster 'vTA Cluster' with new State 'Enabled'. Do you want to proceed?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"): y

Name                 State                Id
----                 -----                --
vTA Cluster          Enabled              TrustAuthorityCluster-domain-c8
```

다음에 수행할 작업

신뢰할 수 있는 ESXi 호스트 및 vCenter Server에 대한 정보 수집으로 계속 진행합니다.

신뢰할 수 있는 ESXi 호스트 및 vCenter Server에 대한 정보 수집

신뢰를 설정하려면 vSphere 신뢰 기관 클러스터에 신뢰할 수 있는 클러스터의 ESXi 호스트 및 vCenter Server에 대한 정보가 필요합니다. 신뢰 기관 클러스터로 가져오기 위해 이 정보를 파일로 내보냅니다. 이러한 파일은 기밀로 유지해야 하며 안전하게 전송해야 합니다.

vSphere 신뢰 기관 PowerCLI cmdlet를 사용하여 신뢰할 수 있는 클러스터의 ESXi 호스트에서 다음과 같은 정보를 파일로 내보내서 신뢰 기관 클러스터가 신뢰할 수 있는 소프트웨어와 하드웨어를 알 수 있게 합니다.

- ESXi 버전
- TPM 제조업체(CA 인증서)
- (선택 사항) 개별 TPM(EK 인증서)

참고 이러한 내보낸 파일은 vSphere 신뢰 기관 구성을 복원해야 하는 경우를 대비해 안전한 위치에 보관하십시오.

유형 및 벤더가 동일하고 동일한 기간 및 위치에서 제조된 호스트가 있는 경우 TPM 하나의 CA 인증서만 가져와서 모든 TPM을 신뢰할 수 있습니다. 개별 TPM을 신뢰하려면 TPM의 EK 인증서를 가져옵니다.

신뢰할 수 있는 클러스터의 vCenter Server에서 주체 정보도 가져와야 합니다. 주체 정보에는 vpxd 솔루션 사용자와 해당 인증서 체인이 포함되어 있습니다. 주체 정보를 사용하면 신뢰할 수 있는 클러스터의 vCenter Server에서 신뢰 기관 클러스터에 구성된 가용한 신뢰할 수 있는 키 제공자를 검색할 수 있습니다.

vSphere 신뢰 기관를 처음 구성하려면 ESXi 버전 및 TPM 정보를 수집해야 합니다. 또한, 업그레이드 또는 패치 적용을 비롯하여, ESXi의 새 버전을 배포한 후에는 매번 ESXi 버전을 수집해야 합니다.

vCenter Server 시스템별로 한 번만 vCenter Server 주체 정보를 수집합니다.

사전 요구 사항

- 신뢰할 수 있는 클러스터에 있는 ESXi 버전 및 TPM 하드웨어 유형을 확인하고 모든 TPM 하드웨어 유형 또는 특정 유형만 신뢰할지 아니면 개별 호스트를 신뢰할지 결정합니다.
- PowerCLI cmdlet을 실행하는 시스템에서 파일로 내보내는 정보를 저장할 로컬 폴더를 생성합니다.
- 신뢰 기관 관리자 사용.
- 신뢰 기관 상태 사용.

절차

1 PowerCLI 세션에서 다음 명령을 실행하여 현재 연결을 끊고 신뢰할 수 있는 클러스터의 ESXi 호스트 중 하나에 루트 사용자로 연결합니다.

```
Disconnect-VIServer -server * -Confirm:$false
Connect-VIServer -server host_ip_address -User root -Password 'password'
```

2 `Get-VMHost` cmdlet을 실행하여 ESXi 호스트를 확인합니다.

```
Get-VMHost
```

호스트 정보가 표시됩니다.

3 `Get-VMHost`를 변수에 할당합니다.

예:

```
$vmhost = Get-VMHost
```

4 `Export-Tpm2CACertificate` cmdlet을 실행하여 지정된 TPM 제조업체의 CA 인증서를 내보냅니다.

a `Get-Tpm2EndorsementKey -VMHost $vmhost`를 변수에 할당합니다.

예를 들어 다음 명령은 `Get-Tpm2EndorsementKey -VMHost $vmhost`를 변수 `$tpm2`에 할당합니다.

```
$tpm2 = Get-Tpm2EndorsementKey -VMHost $vmhost
```

b `Export-Tpm2CACertificate` cmdlet을 실행합니다.

예를 들어 다음 명령은 TPM 인증서를 `cacert.zip` 파일로 내보냅니다. 이 명령을 실행하기 전에 대상 디렉토리가 있는지 확인합니다.

```
Export-Tpm2CACertificate -Tpm2EndorsementKey $tpm2 -FilePath C:\vta\cacert.zip
```

파일이 생성됩니다.

c 신뢰할 클러스터의 각 TPM 하드웨어 유형에 대해 반복합니다. 이전에 내보낸 파일을 덮어쓰지 않도록 각 TMP 하드웨어 유형마다 다른 파일 이름을 사용하십시오.

5 `Export-VMHostImageDb` cmdlet을 실행하여 소프트웨어의 ESXi 호스트 설명(ESXi 이미지)을 내보냅니다.

예를 들어 다음 명령은 정보를 `image.tgz` 파일로 내보냅니다. 이 명령을 실행하기 전에 대상 디렉토리가 있는지 확인합니다.

```
Export-VMHostImageDb -VMHost $vmhost -FilePath C:\vta\image.tgz
```

참고 `Export-VMHostImageDb` cmdlet은 신뢰할 수 있는 클러스터의 vCenter Server에 로그인하려는 경우에도 작동합니다.

파일이 생성됩니다.

신뢰할 클러스터의 각 ESXi 버전에 대해 반복합니다. 이전에 내보낸 파일을 덮어쓰지 않도록 각 버전마다 다른 파일 이름을 사용하십시오.

6 신뢰할 수 있는 클러스터의 vCenter Server 주체 정보를 내보냅니다.

a ESXi 호스트와의 연결을 끊습니다.

```
Disconnect-VIServer -server * -Confirm:$false
```

b 신뢰 기관 관리자를 사용하여 신뢰할 수 있는 클러스터의 vCenter Server에 연결합니다. (또는 **관리자** 권한이 있는 사용자를 사용할 수 있습니다.)

```
Connect-VIServer -server TrustedCluster_VC_ip_address -User trust_admin_user -Password
'password'
```

c 신뢰할 수 있는 클러스터의 vCenter Server 주체 정보를 내보내려면 `Export-TrustedPrincipal` cmdlet을 실행합니다.

예를 들어 다음 명령은 정보를 `principal.json` 파일로 내보냅니다. 이 명령을 실행하기 전에 대상 디렉토리가 있는지 확인합니다.

```
Export-TrustedPrincipal -FilePath C:\vta\principal.json
```

파일이 생성됩니다.

7 (선택 사항) 개별 호스트를 신뢰하려는 경우에는 TPM EK 공용 키 인증서를 내보내야 합니다.

TPM 승인 키 인증서 내보내기 및 가져오기의 내용을 참조하십시오.

결과

다음 파일이 생성됩니다.

- TPM CA 인증서 파일(.zip 파일 확장명)
- ESXi 이미지 파일(.tgz 파일 확장명)
- vCenter Server 주체 파일(.json 파일 확장명)

예제: 신뢰할 수 있는 ESXi 호스트 및 vCenter Server에 대한 정보 수집

이 예는 PowerCLI를 사용하여 ESXi 호스트 정보와 vCenter Server 주체를 내보내는 방법을 보여줍니다. 다음 표에는 사용되는 예제 구성 요소 및 값이 나와 있습니다.

표 9-5. vSphere 신뢰 기관 설정 예

구성 요소	값
신뢰할 수 있는 클러스터의 ESXi 호스트	192.168.110.51
신뢰할 수 있는 클러스터의 vCenter Server	192.168.110.22
변수 `$vmhost`	`Get-VMHost`
변수 `$tpm2`	`Get-Tpm2EndorsementKey -VMHost $vmhost`

표 9-5. vSphere 신뢰 기관 설정 예 (계속)

구성 요소	값
신뢰 기관 관리자	trustedadmin@vsphere.local
출력 파일을 포함할 로컬 디렉토리	C:\vta

```
PS C:\Users\Administrator.CORP> Connect-VIServer -server 192.168.110.51 -User root -Password
'VMware1!'

Name                           Port  User
----                           ----  ----
192.168.110.51                  443  root

PS C:\Users\Administrator.CORP> Get-VMHost

Name               ConnectionState PowerState NumCpu CpuUsageMhz CpuTotalMhz MemoryUsageGB
MemoryTotalGB Version
----               --------------- ---------- ------ ----------- ----------- -------------
------------- -------
192.168.110.51     Connected       PoweredOn       4         200        9576
1.614         7.999   7.0.0

PS C:\Users\Administrator.CORP> $vmhost = Get-VMHost
PS C:\Users\Administrator.CORP> $tpm2 = Get-Tpm2EndorsementKey -VMHost $vmhost
PS C:\> Export-Tpm2CACertificate -Tpm2EndorsementKey $tpm2 -FilePath C:\vta\cacert.zip

Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        10/8/2019   6:55 PM           1004 cacert.zip

PS C:\Users\Administrator.CORP> Export-VMHostImageDb -VMHost $vmhost -FilePath
C:\vta\image.tgz

Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         10/8/2019  11:02 PM           2391 image.tgz

PS C:\Users\Administrator.CORP> Disconnect-VIServer -server * -Confirm:$false
PS C:\Users\Administrator.CORP> Connect-VIServer -server 192.168.110.22 -User
trustedadmin@vsphere.local -Password 'VMware1!'

Name                           Port  User
----                           ----  ----
192.168.110.22                  443  VSPHERE.LOCAL\trustedadmin

PS C:\Users\Administrator.CORP> Export-TrustedPrincipal -FilePath C:\vta\principal.json

Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         10/8/2019  11:14 PM           1873 principal.json
```

다음에 수행할 작업

신뢰 기관 클러스터로 신뢰할 수 있는 호스트 정보 가져오기으로 계속 진행합니다.

TPM 승인 키 인증서 내보내기 및 가져오기

ESXi 호스트에서 TPM EK(승인 키) 인증서를 내보내고 vSphere 신뢰 기관 클러스터로 가져올 수 있습니다. 신뢰할 수 있는 클러스터에서 개별 ESXi 호스트를 신뢰하려는 경우 이렇게 합니다.

TPM EK 인증서를 신뢰 기관 클러스터로 가져오려면, EK 인증서를 수락하도록 신뢰 기관 클러스터의 기본 증명 유형을 변경해야 합니다. 기본 증명 유형은 TPM CA(인증 기관) 인증서를 수락합니다. 일부 TPM에는 EK 인증서가 포함되어 있지 않습니다. 개별 ESXi 호스트를 신뢰하려는 경우 TPM에는 EK 인증서가 포함되어야 합니다.

참고 내보낸 EK 인증서 파일은 vSphere 신뢰 기관 구성을 복원해야 하는 경우를 대비해 안전한 위치에 보관하십시오.

사전 요구 사항

- 신뢰 기관 관리자 사용.
- 신뢰 기관 상태 사용.

절차

1 신뢰 기관 클러스터의 vCenter Server에 신뢰 기관 관리자로 연결되어 있는지 확인합니다.

예를 들어 `$global:defaultviservers`를 입력하여 연결된 모든 서버를 표시할 수 있습니다.

2 (선택 사항) 필요한 경우 다음 명령을 실행하여 신뢰 기관 클러스터의 vCenter Server에 연결되어 있는지 확인할 수 있습니다.

```
Disconnect-VIServer -server * -Confirm:$false
Connect-VIServer -server TrustAuthorityCluster_VC_ip_address -User trust_admin_user
-Password 'password'
```

3 신뢰 기관 클러스터의 증명 유형을 변경하려면:

a `Get-TrustAuthorityCluster` cmdlet을 실행하여 vCenter Server로 관리되는 클러스터를 표시합니다.

```
Get-TrustAuthorityCluster
```

클러스터가 표시됩니다.

b 변수에 `Get-TrustAuthorityCluster` 정보를 할당합니다.

예를 들어 다음 명령은 `vTA Cluster`라는 클러스터를 변수 `$vTA`에 할당합니다.

```
$vTA = Get-TrustAuthorityCluster 'vTA Cluster'
```

c 변수에 Get-TrustAuthorityTpm2AttestationSettings 정보를 할당합니다.

예를 들어 다음 명령은 변수 $tpm2Settings에 정보를 할당합니다.

```
$tpm2Settings = Get-TrustAuthorityTpm2AttestationSettings -TrustAuthorityCluster $vTA
```

d RequireEndorsementKey 또는 RequireCertificateValidation 또는 둘 모두를 지정하여 Set-TrustAuthorityTpm2AttestationSettings cmdlet을 실행합니다.

예를 들어, 이 명령은 RequireEndorsementKey를 지정합니다.

```
Set-TrustAuthorityTpm2AttestationSettings -Tpm2AttestationSettings $tpm2Settings
-RequireEndorsementKey
```

시스템이 다음과 유사한 확인 메시지로 응답합니다.

```
Confirmation
Configure the Tpm2AttestationSettings 'TrustAuthorityTpm2AttestationSettings-domain-
c8' with the following parameters:
 RequireCertificateValidation: False
 RequireEndorsementKey: True
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"):
```

e 확인 메시지가 표시되면 Enter 키를 누릅니다. (기본값은 **Y**입니다.)

지정된 설정에 대한 상태가 True로 출력에 표시됩니다. 예를 들어 이 상태는 Require Endorsement Key에 대해서는 True를 Require Certificate Validation에 대해서는 False를 표시합니다.

```
Name                                    RequireEndorsementKey
RequireCertificateValidation   Health
----                                    ---------------------
----------------------------   ------
TrustAuthorityTpm2AttestationSettings... True
False                          Ok
```

4 TPM EK 인증서를 내보내려면 다음을 수행합니다.

a 신뢰 기관 클러스터의 vCenter Server와 연결을 끊습니다.

```
Disconnect-VIServer -server * -Confirm:$false
```

b Connect-VIServer cmdlet를 실행하여 신뢰할 수 있는 클러스터의 ESXi 호스트 중 하나에 루트 사용자로 연결합니다.

```
Connect-VIServer -server host_ip_address -User root -Password 'password'
```

c Get-VMHost cmdlet을 실행하여 ESXi 호스트를 확인합니다.

```
Get-VMHost
```

호스트 정보가 표시됩니다.

d Get-VMHost를 변수에 할당합니다.

예:

```
$vmhost = Get-VMHost
```

e Export-Tpm2EndorsementKey cmdlet을 실행하여 ESXi 호스트의 EK 인증서를 내보냅니다.

예를 들어 다음 명령은 EK 인증서를 tpm2ek.json 파일로 내보냅니다.

```
Export-Tpm2EndorsementKey -VMHost $vmhost -FilePath C:\vta\tpm2ek.json
```

파일이 생성됩니다.

5 TPM EK를 가져오려면 다음을 수행합니다.

a 신뢰할 수 있는 클러스터의 ESXi 호스트와 연결을 끊습니다.

```
Disconnect-VIServer -server * -Confirm:$false
```

b 신뢰 기관 관리자 사용자를 사용하여 신뢰할 수 있는 클러스터의 vCenter Server에 연결합니다.

```
Connect-VIServer -server TrustAuthorityCluster_VC_ip_address -User trust_admin_user
-Password 'password'
```

c Get-TrustAuthorityCluster cmdlet을 실행합니다.

```
Get-TrustAuthorityCluster
```

신뢰 기관 클러스터의 클러스터가 표시됩니다.

d Get-TrustAuthorityCluster '*cluster*' 정보를 변수에 할당합니다.

예를 들어 다음 명령은 클러스터 vTA Cluster에 대한 정보를 변수 $vTA에 할당합니다.

```
$vTA = Get-TrustAuthorityCluster  'vTA Cluster'
```

e New-TrustAuthorityTpm2EndorsementKey cmdlet을 실행합니다.

예를 들어 다음 명령은 이전에 4단계에서 내보낸 tpm2ek.json 파일을 사용합니다.

```
New-TrustAuthorityTpm2EndorsementKey -TrustAuthorityCluster $vTA -FilePath
C:\vta\tpm2ek.json
```

가져온 승인 키 정보가 표시됩니다.

결과

신뢰 기관 클러스터의 증명 유형이 EK 인증서를 수락하도록 변경되었습니다. EK 인증서는 신뢰할 수 있는 클러스터에서 내보내고 신뢰 기관 클러스터로 가져옵니다.

예제: TPM EK 인증서 내보내기 및 가져오기

이 예시에서는 PowerCLI를 사용하여, 신뢰 기관 클러스터의 기본 증명 유형을 EK 인증서를 수락하도록 변경하고, 신뢰할 수 있는 클러스터의 ESXi 호스트에서 TPM EK 인증서를 내보낸 다음, 신뢰 기관 클러스터로 가져오는 방법을 보여줍니다. 다음 표에는 사용되는 예제 구성 요소 및 값이 나와 있습니다.

표 9-6. vSphere 신뢰 기관 설정 예

구성 요소	값
신뢰 기관 클러스터의 vCenter Server	192.168.210.22
변수 `$vTA`	`Get-TrustAuthorityCluster 'vTA Cluster'`
변수 `$tpm2Settings`	`Get-TrustAuthorityTpm2AttestationSettings -TrustAuthorityCluster $vTA`
변수 `$vmhost`	`Get-VMHost`
신뢰할 수 있는 클러스터의 ESXi 호스트	192.168.110.51
신뢰 기관 관리자	trustedadmin@vsphere.local
출력 파일을 포함할 로컬 디렉토리	`C:\vta`

```
PS C:\Users\Administrator> Connect-VIServer -server 192.168.210.22 -User
trustedadmin@vsphere.local -Password 'VMware1!'

Name                           Port  User
----                           ----  ----
192.168.210.22                 443   VSPHERE.LOCAL\TrustedAdmin

PS C:\Users\Administrator> Get-TrustAuthorityCluster

Name                 State                Id
----                 -----                --
vTA Cluster          Enabled              TrustAuthorityCluster-domain-c8

PS C:\Users\Administrator> $vTA = Get-TrustAuthorityCluster 'vTA Cluster'

PS C:\Users\Administrator> $tpm2Settings = Get-TrustAuthorityTpm2AttestationSettings
-TrustAuthorityCluster $vTA

PS C:\Users\Administrator> Set-TrustAuthorityTpm2AttestationSettings -Tpm2AttestationSettings
$tpm2Settings -RequireEndorsementKey

Confirmation
Configure the Tpm2AttestationSettings 'TrustAuthorityTpm2AttestationSettings-domain-c8' with
the following parameters:
 RequireCertificateValidation: False
 RequireEndorsementKey: True
```

```
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"): y

Name                                    RequireEndorsementKey
RequireCertificateValidation   Health
----                                    ---------------------
----------------------------   ------
TrustAuthorityTpm2AttestationSettings... True
False                          Ok

PS C:\Users\Administrator> Disconnect-VIServer -server * -Confirm:$false
PS C:\Users\Administrator> Connect-VIServer -server 192.168.110.51 -User root -Password
'VMware1!'

Name                           Port  User
----                           ----  ----
192.168.110.51                 443   root

PS C:\Users\Administrator> Get-VMHost

Name                 ConnectionState PowerState NumCpu CpuUsageMhz CpuTotalMhz
MemoryUsageGB   MemoryTotalGB Version
----                 --------------- ---------- ------ ----------- -----------
-------------   ------------- -------
192.168.110.51       Connected       PoweredOn       4          55        9576
1.230           7.999   7.0.0

PS C:\Users\Administrator> $vmhost = Get-VMHost
PS C:\Users\Administrator> Export-Tpm2EndorsementKey -VMHost $vmhost -FilePath
C:\vta\tpm2ek.json

Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----        12/3/2019  10:16 PM           2391 tpm2ek.json

PS C:\Users\Administrator> Disconnect-VIServer -server * -Confirm:$false
PS C:\Users\Administrator> Connect-VIServer -server 192.168.210.22 -User
trustedadmin@vsphere.local -Password 'VMware1!'

Name                           Port  User
----                           ----  ----
192.168.210.22                 443   VSPHERE.LOCAL\TrustedAdmin

PS C:\Users\Administrator> Get-TrustAuthorityCluster

Name                 State               Id
----                 -----               --
vTA Cluster          Enabled             TrustAuthorityCluster-domain-c8

PS C:\Users\Administrator> $vTA = Get-TrustAuthorityCluster  'vTA Cluster'
PS C:\Users\Administrator> New-TrustAuthorityTpm2EndorsementKey -TrustAuthorityCluster $vTA
-FilePath C:\vta\tpm2ek.json

TrustAuthorityClusterId                 Name                                    Health
```

```
-----------------------                    ----                                   ------
TrustAuthorityCluster-domain-c8            1a520e42-4db8-1cbb-6dd7-f493fd921ccb   Ok
```

다음에 수행할 작업

신뢰 기관 클러스터로 신뢰할 수 있는 호스트 정보 가져오기으로 계속 진행합니다.

신뢰 기관 클러스터로 신뢰할 수 있는 호스트 정보 가져오기

신뢰 기관 클러스터에서 증명 가능한 호스트를 파악할 수 있도록 내보낸 ESXi 호스트 및 vCenter Server 정보를 vSphere 신뢰 기관 클러스터로 가져옵니다.

이러한 작업을 순서대로 수행하려는 경우 신뢰 기관 클러스터의 vCenter Server에 대한 연결 상태를 유지해야 합니다.

사전 요구 사항

- 신뢰 기관 관리자 사용.
- 신뢰 기관 상태 사용.
- 신뢰할 수 있는 ESXi 호스트 및 vCenter Server에 대한 정보 수집.

절차

1 신뢰 기관 클러스터의 vCenter Server에 신뢰 기관 관리자로 연결되어 있는지 확인합니다.

예를 들어 `$global:defaultviservers`를 입력하여 연결된 모든 서버를 표시할 수 있습니다.

2 (선택 사항) 필요한 경우 다음 명령을 실행하여 신뢰 기관 클러스터의 vCenter Server에 연결되어 있는지 확인할 수 있습니다.

```
Disconnect-VIServer -server * -Confirm:$false
Connect-VIServer -server TrustAuthorityCluster_VC_ip_address -User trust_admin_user
-Password 'password'
```

3 이 vCenter Server에서 관리하는 클러스터를 표시하려면 `Get-TrustAuthorityCluster` cmdlet을 실행합니다.

```
Get-TrustAuthorityCluster
```

클러스터가 표시됩니다.

4 `Get-TrustAuthorityCluster` '*cluster*' 정보를 변수에 할당합니다.

예를 들어 다음 명령은 클러스터 `vTA Cluster`에 대한 정보를 변수 `$vTA`에 할당합니다.

```
$vTA = Get-TrustAuthorityCluster 'vTA Cluster'
```

5 신뢰할 수 있는 클러스터의 vCenter Server 주체 정보를 신뢰 기관 클러스터로 가져오려면 `New-TrustAuthorityPrincipal` cmdlet을 실행합니다.

예를 들어 다음 명령은 신뢰할 수 있는 ESXi 호스트 및 vCenter Server에 대한 정보 수집에서 이전에 내보낸 `principal.json` 파일을 가져옵니다.

```
New-TrustAuthorityPrincipal -TrustAuthorityCluster $vTA -FilePath C:\vta\principal.json
```

TrustAuthorityPrincipal 정보가 표시됩니다.

6 가져오기를 확인하려면 `Get-TrustAuthorityPrincipal` cmdlet을 실행합니다.

예:

```
Get-TrustAuthorityPrincipal -TrustAuthorityCluster $vTA
```

가져온 TrustAuthorityPrincipal 정보가 표시됩니다.

7 TPM(신뢰할 수 있는 플랫폼 모듈) CA 인증서 정보를 가져오려면 `New-TrustAuthorityTpm2CACertificate` cmdlet을 실행합니다.

예를 들어 다음 명령은 신뢰할 수 있는 ESXi 호스트 및 vCenter Server에 대한 정보 수집에서 이전에 내보낸 `cacert.zip` 파일에서 TPM CA 인증서 정보를 가져옵니다.

```
New-TrustAuthorityTpm2CACertificate -TrustAuthorityCluster $vTA -FilePath C:\vta\cacert.zip
```

가져온 인증서 정보가 표시됩니다.

8 ESXi 호스트 기본 이미지 정보를 가져오려면 `New-TrustAuthorityVMHostBaseImage` cmdlet을 실행합니다.

예를 들어 다음 명령은 신뢰할 수 있는 ESXi 호스트 및 vCenter Server에 대한 정보 수집에서 이전에 내보낸 `image.tgz` 파일에서 이미지 정보를 가져옵니다.

```
New-TrustAuthorityVMHostBaseImage -TrustAuthorityCluster $vTA -FilePath C:\vta\image.tgz
```

가져온 이미지 정보가 표시됩니다.

결과

신뢰 기관 클러스터는 원격으로 증명할 수 있는 ESXi 호스트를 알고 있기 때문에 어떤 호스트를 신뢰할 수 있는지 알 수 있습니다.

예제: 신뢰 기관 클러스터로 신뢰할 수 있는 호스트 정보 가져오기

이 예에서는 PowerCLI을 사용하여 신뢰할 수 있는 클러스터 및 신뢰할 수 있는 호스트 정보 파일의 vCenter Server 주체 정보를 신뢰 기관 클러스터로 가져오는 방법을 보여줍니다. 여기서는 사용자가 신뢰 기관 클러스터의 vCenter Server에 신뢰 기관 관리자로 연결되어 있다고 가정합니다. 다음 표에는 사용되는 예제 구성 요소 및 값이 나와 있습니다.

표 9-7. vSphere 신뢰 기관 설정 예

구성 요소	값
변수 `$vTA`	`Get-TrustAuthorityCluster 'vTA Cluster1'`
신뢰 기관 클러스터의 vCenter Server	192.168.210.22
신뢰 기관 클러스터 이름	vTA Cluster1(사용) vTA Cluster2(사용 안 함)
주체 정보 파일	`C:\vta\principal.json`
TPM 인증서 파일	`C:\vta\cacert.cer`
ESXi 호스트 기본 이미지 파일	`C:\vta\image.tgz`
신뢰 기관 관리자	trustedadmin@vsphere.local

```
PS C:\Users\Administrator> Disconnect-VIServer -server * -Confirm:$false
PS C:\Users\Administrator> Connect-VIServer -server 192.168.210.22 -User
trustedadmin@vsphere.local -Password 'VMware1!'

Name                           Port  User
----                           ----  ----
192.168.210.22                  443  VSPHERE.LOCAL\trustedadmin

PS C:\Users\Administrator> Get-TrustAuthorityCluster

Name                 State               Id
----                 -----               --
vTA Cluster1         Enabled             TrustAuthorityCluster-domain-c8
vTA Cluster2         Disabled            TrustAuthorityCluster-domain-c26

PS C:\Users\Administrator> $vTA = Get-TrustAuthorityCluster 'vTA Cluster1'

PS C:\Users\Administrator.CORP> New-TrustAuthorityPrincipal -TrustAuthorityCluster $vTA
-FilePath C:\vta\principal.json

Name                                          Domain          Type
TrustAuthorityClusterId
----                                          ------          ----
------------------------
vpxd-de207929-0601-43ef-9616-47d0cee0302f     vsphere.local   STS_USER
TrustAuthorityCluster-domain-c8

PS C:\Users\Administrator.CORP> Get-TrustAuthorityPrincipal -TrustAuthorityCluster $vTA

Name                                          Domain          Type
TrustAuthorityClusterId
----                                          ------          ----
------------------------
vpxd-de207929-0601-43ef-9616-47d0cee0302f     vsphere.local   STS_USER
TrustAuthorityCluster-domain-c8

PS C:\Users\Administrator.CORP> New-TrustAuthorityTpm2CACertificate -TrustAuthorityCluster
```

```
$vTA -FilePath C:\vta\cacert.cer

TrustAuthorityClusterId                  Name                                      Health
-----------------------                  ----                                      ------
TrustAuthorityCluster-domain-c8          52BDB7B4B2F55C925C047257DED4588A7767D961 Ok

PS C:\Users\Administrator.CORP> New-TrustAuthorityVMHostBaseImage -TrustAuthorityCluster $vTA
-FilePath C:\vta\image.tgz

TrustAuthorityClusterId                  VMHostVersion                             Health
-----------------------                  -------------                             ------
TrustAuthorityCluster-domain-c8          ESXi 7.0.0-0.0.14828939                   Ok
```

다음에 수행할 작업

신뢰 기관 클러스터에서 키 제공자 생성으로 계속 진행합니다.

신뢰 기관 클러스터에서 키 제공자 생성

키 제공자 서비스가 키 제공자에 연결하려면, 신뢰할 수 있는 키 제공자를 생성한 다음 vSphere 신뢰 기관 클러스터와 키 서버(KMS) 간에 신뢰 설정을 구성해야 합니다. 대부분의 KMIP 준수 키 서버의 경우, 이 구성에는 클라이언트 및 서버 인증서 설정이 포함됩니다.

vSphere 6.7에서는 KMS 클러스터라고 했지만 vSphere 7.0에서는 키 제공자라고 부릅니다. 키 제공자에 대한 자세한 내용은 vSphere 신뢰 기관 키 제공자 서비스란? 항목을 참조하십시오.

운영 환경에서는 여러 개의 키 제공자를 생성할 수 있습니다. 여러 개의 키 제공자를 생성하면 회사 조직, 서로 다른 사업 단위 또는 고객 등을 기반으로 배포를 관리하는 방식을 결정할 수 있습니다.

이러한 작업을 순서대로 수행하려는 경우 vSphere 신뢰 기관 클러스터의 vCenter Server에 대한 연결 상태를 유지해야 합니다.

사전 요구 사항

- 신뢰 기관 관리자 사용.
- 신뢰 기관 상태 사용.
- 신뢰할 수 있는 ESXi 호스트 및 vCenter Server에 대한 정보 수집.
- 신뢰 기관 클러스터로 신뢰할 수 있는 호스트 정보 가져오기.
- 키 서버에서 키를 생성하고 활성화하여 신뢰할 수 있는 키 제공자의 기본 키가 되도록 합니다. 이 키는 신뢰할 수 있는 키 제공자가 사용하는 다른 키와 암호를 래핑합니다. 키 생성에 대한 자세한 내용은 키 서버 벤더 설명서를 참조하십시오.

절차

1 신뢰 기관 클러스터의 vCenter Server에 연결되어 있는지 확인합니다. 예를 들어 `$global:defaultviservers`를 입력하여 연결된 모든 서버를 표시할 수 있습니다.

2 (선택 사항) 필요한 경우 다음 명령을 실행하여 신뢰 기관 클러스터의 vCenter Server에 연결되어 있는지 확인할 수 있습니다.

```
Disconnect-VIServer -server * -Confirm:$false
Connect-VIServer -server TrustAuthorityCluster_VC_ip_address -User trust_admin_user
-Password 'password'
```

3 신뢰할 수 있는 키 제공자를 생성하려면 `New-TrustAuthorityKeyProvider` cmdlet을 실행합니다.

예를 들어 이 명령은 PrimaryKeyID에 `1`을 사용하고 `clkp`라는 이름을 사용합니다. 이러한 작업을 순서대로 수행하는 경우, 이전에 `Get-TrustAuthorityCluster` 정보를 변수에 할당했습니다(예: `$vTA = Get-TrustAuthorityCluster 'vTA Cluster'`).

```
New-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA -PrimaryKeyId 1 -Name clkp
-KmipServerAddress ip_address
```

PrimaryKeyID는 일반적으로 키 서버에서 UUID 형식으로 제공되는 키 ID입니다. PrimaryKeyID에 키 이름을 사용하지 마십시오. PrimaryKeyID 값은 벤더에 따라 다릅니다. 키 서버 설명서를 참조하십시오. `New-TrustAuthorityKeyProvider` cmdlet은 `KmipServerPort`, `ProxyAddress` 및 `ProxyPort`와 같은 다른 옵션을 사용할 수 있습니다. 자세한 내용은 `New-TrustAuthorityKeyProvider` 도움말 시스템을 참조하십시오.

유형(표준 키 제공자, 신뢰할 수 있는 키 제공자 및 네이티브 키 제공자)에 관계없이 각 논리적 키 제공자는 모든 vCenter Server 시스템에서 고유한 이름이 있어야 합니다.

자세한 내용은 키 제공자 이름 지정의 내용을 참조하십시오.

참고 키 제공자에 키 서버를 여러 개 추가하려면 `Add-TrustAuthorityKeyProviderServer` cmdlet을 사용합니다.

키 제공자 정보가 표시됩니다.

4 신뢰할 수 있는 키 제공자를 키 서버가 신뢰하도록 신뢰할 수 있는 연결을 설정합니다. 정확한 프로세스는 키 서버가 수락하는 인증서와 회사 정책에 따라 달라집니다. 서버에 적합한 옵션을 선택하고 단계를 완료합니다.

옵션	자세한 내용은
클라이언트 인증서 업로드	클라이언트 인증서를 업로드하여 신뢰할 수 있는 키 제공자가 신뢰할 수 있는 연결 설정.
KMS 인증서 및 개인 키 업로드	인증서 및 개인 키를 업로드하여 신뢰할 수 있는 키 제공자가 신뢰할 수 있는 연결 설정.
새 인증서 서명 요청	인증서 서명 요청을 생성하여 신뢰할 수 있는 키 제공자가 신뢰할 수 있는 연결 설정.

5 신뢰할 수 있는 키 제공자가 키 서버를 신뢰하도록 키 서버 인증서를 업로드하여 신뢰 설정을 완료합니다.

a 변수에 `Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA` 정보를 할당합니다.

예:

```
$kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
```

이 변수는 지정된 신뢰 기관 클러스터에서 신뢰할 수 있는 키 제공자를 가져옵니다(이 경우 `$vTA`).

참고 신뢰할 수 있는 키 제공자가 둘 이상이면, 다음과 유사한 명령을 사용하여 원하는 항목을 선택합니다.

```
Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
<The trusted key providers listing is displayed.>
$kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA | Select-Object -Last 1
```

`Select-Object -Last 1`를 사용하면 목록의 마지막에 있는 신뢰할 수 있는 키 제공자가 선택됩니다.

b 키 서버 서버 인증서를 받으려면 `Get-TrustAuthorityKeyProviderServerCertificate` 명령을 실행합니다.

예:

```
Get-TrustAuthorityKeyProviderServerCertificate -KeyProviderServer
$kp.KeyProviderServers
```

서버 인증서 정보가 표시됩니다. 처음에는 인증서가 신뢰되지 않으므로 [신뢰됨] 상태는 False입니다. 키 서버가 둘 이상 구성된 경우 인증서 목록이 반환 됩니다. 다음 지침을 사용하여 각 인증서를 확인하고 추가합니다.

c 인증서를 신뢰하기 전에 `Get-TrustAuthorityKeyProviderServerCertificate -KeyProviderServer $kp.KeyProviderServers` 정보를 변수(예: `cert`)에 할당하고 `$cert.Certificate.ToString()` 명령을 실행하여 출력을 확인합니다.

예:

```
$cert = Get-TrustAuthorityKeyProviderServerCertificate -KeyProviderServer
$kp.KeyProviderServers
$cert.Certificate.ToString()
```

주체, 발급자 및 기타 정보를 포함한 인증서 정보가 표시됩니다.

d KMIP 서버 인증서를 신뢰할 수 있는 키 제공자에 추가하려면 `Add-TrustAuthorityKeyProviderServerCertificate`를 실행합니다.

예:

```
Add-TrustAuthorityKeyProviderServerCertificate -ServerCertificate $cert
```

인증서 정보가 표시되고 [신뢰됨] 상태가 이제 True로 나타납니다.

6 키 제공자의 상태를 확인합니다.

a 키 제공자 상태를 새로 고치려면 `$kp` 변수를 다시 할당합니다.

예:

```
$kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
```

참고 신뢰할 수 있는 키 제공자가 둘 이상이면, 다음과 유사한 명령을 사용하여 원하는 항목을 선택합니다.

```
Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
<The trusted key providers listing is displayed.>
$kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA | Select-Object -Last 1
```

`Select-Object -Last 1`를 사용하면 목록의 마지막에 있는 신뢰할 수 있는 키 제공자가 선택됩니다.

b `$kp.Status` 명령을 실행하여 키 제공자 상태를 가져옵니다.

예:

```
$kp.Status
```

참고 상태를 새로 고치는 데 몇 분 정도 걸릴 수 있습니다. 상태를 보려면 `$kp` 변수를 다시 할당하고 `$kp.Status` 명령을 다시 실행합니다.

상태가 정상이면 키 제공자가 올바르게 실행되고 있음을 나타냅니다.

결과

신뢰할 수 있는 키 제공자가 생성되었고 키 서버와 신뢰가 설정되었습니다.

예제: 신뢰 기관 클러스터에서 키 제공자 생성

이 예는 PowerCLI를 사용하여 신뢰 기관 클러스터에서 신뢰할 수 있는 키 제공자를 생성하는 방법을 보여 줍니다. 여기서는 사용자가 신뢰 기관 클러스터의 vCenter Server에 신뢰 기관 관리자로 연결되어 있다고 가정합니다. 또한 CSR을 벤더에 제출한 후 키 서버 벤더가 서명한 인증서를 사용합니다.

다음 표에는 사용되는 예제 구성 요소 및 값이 나와 있습니다.

표 9-8. vSphere 신뢰 기관 설정 예

구성 요소	값
변수 `$vTA`	`Get-TrustAuthorityCluster 'vTA Cluster'`
변수 `$kp`	`Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA`
변수 `$cert`	`Get-TrustAuthorityKeyProviderServerCertificate -KeyProviderServer $kp.KeyProviderServers`
신뢰 기관 클러스터의 vCenter Server	192.168.210.22
KMIP 준수 키 서버	192.168.110.91
KMIP 준수 키 서버 사용자	vcqekmip
신뢰 기관 클러스터 이름	vTA 클러스터
신뢰 기관 관리자	trustedadmin@vsphere.local

```
PS C:\Users\Administrator.CORP> Disconnect-VIServer -server * -Confirm:$false
PS C:\Users\Administrator.CORP> Connect-VIServer -server 192.168.210.22 -User
trustedadmin@vsphere.local -Password 'VMware1!'

PS C:\Users\Administrator.CORP> New-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
-PrimaryKeyId 8 -Name clkp -KmipServerAddress 192.168.110.91
Name                 PrimaryKeyId         Type       TrustAuthorityClusterId
----                 ------------         ----       -----------------------
clkp                 8                    KMIP       TrustAuthorityCluster-domain-c8

PS C:\Users\Administrator.CORP> New-TrustAuthorityKeyProviderClientCertificate -KeyProvider
$kp
<Export the client certificate when you need to use it.>
PS C:\Users\Administrator.CORP> Export-TrustAuthorityKeyProviderClientCertificate
-KeyProvider $kp -FilePath clientcert.pem

PS C:\Users\Administrator.CORP> $kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster
$vTA
PS C:\Users\Administrator.CORP> Get-TrustAuthorityKeyProviderServerCertificate
-KeyProviderServer $kp.KeyProviderServers

Certificate                                Trusted    KeyProviderServerId       KeyProviderId
```

```
-----------                              -------    -------------------       -------------
[Subject]...                             False      domain-c8-clkp:192.16.... domain-c8-clkp

PS C:\WINDOWS\system32> $cert.Certificate.ToString()
[Subject]
  E=<domain>, CN=<IP address>, OU=VMware Engineering, O=VMware, L=Palo Alto, S=California,
C=US

[Issuer]
  O=<host>.eng.vmware.com, C=US, DC=local, DC=vsphere, CN=CA

[Serial Number]
  00CEF192BBF9D80C9F

[Not Before]
  8/10/2015 4:16:12 PM

[Not After]
  8/9/2020 4:16:12 PM

[Thumbprint]
  C44068C124C057A3D07F51DCF18720E963604B70

PS C:\Users\Administrator.CORP> $cert = Get-TrustAuthorityKeyProviderServerCertificate
-KeyProviderServer $kp.KeyProviderServers
PS C:\Users\Administrator.CORP> Add-TrustAuthorityKeyProviderServerCertificate
-ServerCertificate $cert

Certificate                              Trusted    KeyProviderServerId       KeyProviderId
-----------                              -------    -------------------       -------------
[Subject]...                             True                                 domain-c8-clkp

PS C:\Users\Administrator.CORP> $kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster
$vTA
PS C:\Users\Administrator.CORP> $kp.Status

KeyProviderId Health HealthDetails ServerStatus
------------- ------ ------------- ------------
domain-c8-kp4     Ok {}            {192.168.210.22}
```

다음에 수행할 작업

신뢰 기관 클러스터 정보 내보내기으로 계속 진행합니다.

클라이언트 인증서를 업로드하여 신뢰할 수 있는 키 제공자가 신뢰할 수 있는 연결 설정

일부 키 서버(KMS) 벤더의 경우 신뢰할 수 있는 키 제공자의 클라이언트 인증서를 키 서버에 업로드해야 합니다. 업로드하면, 키 서버는 신뢰할 수 있는 키 제공자로부터 오는 트래픽을 수락합니다.

사전 요구 사항

- 신뢰 기관 관리자 사용.
- 신뢰 기관 상태 사용.

- 신뢰할 수 있는 ESXi 호스트 및 vCenter Server에 대한 정보 수집.
- 신뢰 기관 클러스터로 신뢰할 수 있는 호스트 정보 가져오기.
- 신뢰 기관 클러스터에서 키 제공자 생성.

절차

1 신뢰 기관 클러스터의 vCenter Server에 연결되어 있는지 확인합니다. 예를 들어 `$global:defaultviservers`를 입력하여 연결된 모든 서버를 표시할 수 있습니다.

2 (선택 사항) 필요한 경우 다음 명령을 실행하여 신뢰 기관 클러스터의 vCenter Server에 연결되어 있는지 확인할 수 있습니다.

```
Disconnect-VIServer -server * -Confirm:$false
Connect-VIServer -server TrustAuthorityCluster_VC_ip_address -User trust_admin_user
-Password 'password'
```

3 변수에 `Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA` 정보를 할당합니다.

예:

```
$kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
```

이러한 작업을 순서대로 수행하는 경우, 이전에 `Get-TrustAuthorityCluster` 정보를 변수에 할당했습니다(예: `$vTA = Get-TrustAuthorityCluster 'vTA Cluster'`).

이 변수는 지정된 신뢰 기관 클러스터에서 신뢰할 수 있는 키 제공자를 가져옵니다(이 경우 `$vTA`).

참고 신뢰할 수 있는 키 제공자가 둘 이상이면, 다음과 유사한 명령을 사용하여 원하는 항목을 선택합니다.

```
Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
<The trusted key providers listing is displayed.>
$kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA | Select-Object -Last 1
```

`Select-Object -Last 1`를 사용하면 목록의 마지막에 있는 신뢰할 수 있는 키 제공자가 선택됩니다.

4 신뢰할 수 있는 키 제공자 클라이언트 인증서를 생성하려면 `New-TrustAuthorityKeyProviderClientCertificate` cmdlet을 실행합니다.

예:

```
New-TrustAuthorityKeyProviderClientCertificate -KeyProvider $kp
```

지문이 표시됩니다.

5 키 제공자 클라이언트 인증서를 내보내려면 `Export-TrustAuthorityKeyProviderClientCertificate` cmdlet을 실행합니다.

예:

```
Export-TrustAuthorityKeyProviderClientCertificate -KeyProvider $kp -FilePath clientcert.pem
```

인증서가 파일로 내보내집니다.

6 인증서 파일을 키 서버에 업로드합니다.

자세한 내용은 사용하는 키 서버의 설명서를 참조하십시오.

결과

신뢰할 수 있는 키 제공자가 키 서버와 신뢰를 설정했습니다.

인증서 및 개인 키를 업로드하여 신뢰할 수 있는 키 제공자가 신뢰할 수 있는 연결 설정

일부 키 서버(KMS) 벤더의 경우, 키 서버가 제공한 클라이언트 인증서 및 개인 키를 사용하여 신뢰할 수 있는 키 제공자를 구성해야 합니다. 신뢰할 수 있는 키 제공자를 구성하면 키 서버가 신뢰할 수 있는 키 제공자의 트래픽을 수락합니다.

사전 요구 사항

- 신뢰 기관 관리자 사용.
- 신뢰 기관 상태 사용.
- 신뢰할 수 있는 ESXi 호스트 및 vCenter Server에 대한 정보 수집.
- 신뢰 기관 클러스터로 신뢰할 수 있는 호스트 정보 가져오기.
- 신뢰 기관 클러스터에서 키 제공자 생성.
- 키 서버 벤더에 PEM 형식의 인증서와 개인 키를 요청합니다. 인증서가 PEM이 아닌 형식으로 반환되면 PEM으로 변환합니다. 개인 키가 암호로 보호되는 경우 암호가 제거된 PEM 파일을 생성합니다. 두 작업 모두에 `openssl` 명령을 사용할 수 있습니다. 예:
  - 인증서를 CRT에서 PEM 형식으로 변환하려면 다음을 수행합니다.

    ```
    openssl x509 -in clientcert.crt -out clientcert.pem -outform PEM
    ```

  - 인증서를 DER에서 PEM 형식으로 변환하려면 다음을 수행합니다.

    ```
    openssl x509 -inform DER -in clientcert.der -out clientcert.pem
    ```

  - 개인 키에서 암호를 제거하려면:

    ```
    openssl rsa -in key.pem -out keynopassword.pem
    Enter pass phrase for key.pem:
    writing RSA key
    ```

절차

1 신뢰 기관 클러스터의 vCenter Server에 연결되어 있는지 확인합니다. 예를 들어 `$global:defaultviservers`를 입력하여 연결된 모든 서버를 표시할 수 있습니다.

2 (선택 사항) 필요한 경우 다음 명령을 실행하여 신뢰 기관 클러스터의 vCenter Server에 연결되어 있는지 확인할 수 있습니다.

```
Disconnect-VIServer -server * -Confirm:$false
Connect-VIServer -server TrustAuthorityCluster_VC_ip_address -User trust_admin_user
-Password 'password'
```

3 변수에 `Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA` 정보를 할당합니다.

예:

```
$kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
```

이러한 작업을 순서대로 수행하는 경우, 이전에 `Get-TrustAuthorityCluster` 정보를 변수에 할당했습니다(예: `$vTA = Get-TrustAuthorityCluster 'vTA Cluster'`).

`$kp` 변수는 지정된 신뢰 기관 클러스터에서 신뢰할 수 있는 키 제공자를 가져옵니다(이 경우 `$vTA`).

참고 신뢰할 수 있는 키 제공자가 둘 이상이면, 다음과 유사한 명령을 사용하여 원하는 항목을 선택합니다.

```
Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
<The trusted key providers listing is displayed.>
$kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA | Select-Object -Last 1
```

`Select-Object -Last 1`를 사용하면 목록의 마지막에 있는 신뢰할 수 있는 키 제공자가 선택됩니다.

4 `Set-TrustAuthorityKeyProviderClientCertificate` 명령을 사용하여 인증서 및 개인 키를 업로드합니다.

예:

```
Set-TrustAuthorityKeyProviderClientCertificate -KeyProvider $kp -CertificateFilePath
<path/to/certfile.pem> -PrivateKeyFilePath <path/to/privatekey.pem>
```

결과

신뢰할 수 있는 키 제공자가 키 서버와 신뢰를 설정했습니다.

인증서 서명 요청을 생성하여 신뢰할 수 있는 키 제공자가 신뢰할 수 있는 연결 설정

일부 키 서버(KMS) 벤더의 경우, CSR(인증서 서명 요청)을 생성한 후 이 CSR을 키 서버 벤더에 보내야 합니다. 키 서버 벤더는 CSR에 서명하고 서명된 인증서를 반환합니다. 서명된 인증서를 신뢰할 수 있는 키 제공자의 클라이언트 인증서로 구성하면, 키 서버는 신뢰할 수 있는 키 제공자로부터 들어오는 트래픽을 수락합니다.

이 작업은 2단계 프로세스입니다. 먼저 CSR을 생성하여 키 서버 벤더에 보냅니다. 그런 다음 키 서버 벤더로부터 받은 서명된 인증서를 업로드합니다.

사전 요구 사항

- 신뢰 기관 관리자 사용.
- 신뢰 기관 상태 사용.
- 신뢰할 수 있는 ESXi 호스트 및 vCenter Server에 대한 정보 수집.
- 신뢰 기관 클러스터로 신뢰할 수 있는 호스트 정보 가져오기.
- 신뢰 기관 클러스터에서 키 제공자 생성.

절차

1 신뢰 기관 클러스터의 vCenter Server에 연결되어 있는지 확인합니다. 예를 들어 `$global:defaultviservers`를 입력하여 연결된 모든 서버를 표시할 수 있습니다.

2 (선택 사항) 필요한 경우 다음 명령을 실행하여 신뢰 기관 클러스터의 vCenter Server에 연결되어 있는지 확인할 수 있습니다.

```
Disconnect-VIServer -server * -Confirm:$false
Connect-VIServer -server TrustAuthorityCluster_VC_ip_address -User trust_admin_user
-Password 'password'
```

3 변수에 `Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA` 정보를 할당합니다.

예:

```
$kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
```

이러한 작업을 순서대로 수행하는 경우, 이전에 `Get-TrustAuthorityCluster` 정보를 변수에 할당했습니다(예: `$vTA = Get-TrustAuthorityCluster 'vTA Cluster'`).

이 변수는 지정된 신뢰 기관 클러스터에서 신뢰할 수 있는 키 제공자를 가져옵니다(이 경우 `$vTA`).

참고 신뢰할 수 있는 키 제공자가 둘 이상이면, 다음과 유사한 명령을 사용하여 원하는 항목을 선택합니다.

```
Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
<The trusted key providers listing is displayed.>
$kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA | Select-Object -Last 1
```

`Select-Object -Last 1`를 사용하면 목록의 마지막에 있는 신뢰할 수 있는 키 제공자가 선택됩니다.

4 CSR을 생성하려면 `New-TrustAuthorityKeyProviderClientCertificateCSR` cmdlet을 사용합니다.

예:

```
New-TrustAuthorityKeyProviderClientCertificateCSR -KeyProvider $kp
```

CSR이 표시됩니다. `Get-TrustAuthorityKeyProviderClientCertificateCSR -KeyProvider $kp` cmdlet을 사용하여 CSR을 가져올 수도 있습니다.

5 서명된 인증서를 가져오려면 CSR을 키 서버 벤더에 제출합니다.

인증서는 PEM 형식이어야 합니다. 인증서가 PEM이 아닌 형식으로 반환되면 `openssl` 명령을 사용하여 PEM으로 변환합니다. 예:

- 인증서를 CRT에서 PEM 형식으로 변환하려면 다음을 수행합니다.

  ```
  openssl x509 -in clientcert.crt -out clientcert.pem -outform PEM
  ```

- 인증서를 DER에서 PEM 형식으로 변환하려면 다음을 수행합니다.

  ```
  openssl x509 -inform DER -in clientcert.der -out clientcert.pem
  ```

6 키 서버 벤더로부터 서명된 인증서를 받으면 `Set-TrustAuthorityKeyProviderClientCertificate` cmdlet을 사용하여 인증서를 키 서버에 업로드합니다.

예:

```
Set-TrustAuthorityKeyProviderClientCertificate -KeyProvider $kp -CertificateFilePath
<path/tp/certfile.pem>
```

결과

신뢰할 수 있는 키 제공자가 키 서버와 신뢰를 설정했습니다.

신뢰 기관 클러스터 정보 내보내기

신뢰할 수 있는 클러스터가 vSphere 신뢰 기관 클러스터에 연결되려면 신뢰 기관 클러스터의 서비스 정보를 파일 형태로 내보낸 다음, 이 파일을 신뢰할 수 있는 클러스터로 가져와야 합니다. 이러한 파일은 기밀로 유지해야 하며 안전하게 전송해야 합니다.

이러한 작업을 순서대로 수행하려는 경우 신뢰 기관 클러스터의 vCenter Server에 대한 연결 상태를 유지해야 합니다.

참고 내보낸 서비스 정보 파일은 vSphere 신뢰 기관 구성을 복원해야 하는 경우를 대비해 안전한 위치에 보관하십시오.

사전 요구 사항

- 신뢰 기관 관리자 사용.
- 신뢰 기관 상태 사용.
- 신뢰할 수 있는 ESXi 호스트 및 vCenter Server에 대한 정보 수집.
- 신뢰 기관 클러스터로 신뢰할 수 있는 호스트 정보 가져오기.
- 신뢰 기관 클러스터에서 키 제공자 생성.

절차

1 신뢰 기관 클러스터의 vCenter Server에 연결되어 있는지 확인합니다. 예를 들어 `$global:defaultviservers`를 입력하여 연결된 모든 서버를 표시할 수 있습니다.

2 (선택 사항) 필요한 경우 다음 명령을 실행하여 신뢰 기관 클러스터의 vCenter Server에 연결되어 있는지 확인할 수 있습니다.

```
Disconnect-VIServer -server * -Confirm:$false
Connect-VIServer -server TrustAuthorityCluster_VC_ip_address -User trust_admin_user
-Password 'password'
```

3 신뢰 기관 클러스터의 증명 서비스 및 키 제공자 서비스 정보를 내보내려면 `Export-TrustAuthorityServicesInfo` cmdlet을 실행합니다.

예를 들어 다음 명령은 서비스 정보를 `clsettings.json` 파일로 내보냅니다. 이러한 작업을 순서대로 수행하는 중이면, 이전에 `Get-TrustAuthorityCluster` 정보를 변수에 할당했습니다(예: `$vTA = Get-TrustAuthorityCluster 'vTA Cluster'`).

```
Export-TrustAuthorityServicesInfo -TrustAuthorityCluster $vTA -FilePath
C:\vta\clsettings.json
```

파일이 생성됩니다.

결과

신뢰 기관 클러스터 정보가 들어 있는 파일이 생성됩니다.

예제: 신뢰 기관 클러스터 정보 내보내기

이 예는 PowerCLI를 사용하여 신뢰 기관 클러스터 서비스 정보를 내보내는 방법을 보여 줍니다. 다음 표에는 사용되는 예제 구성 요소 및 값이 나와 있습니다.

표 9-9. vSphere 신뢰 기관 설정 예

구성 요소	값
변수 `$vTA`	`Get-TrustAuthorityCluster 'vTA Cluster'`
신뢰 기관 클러스터의 vCenter Server	192.168.210.22
신뢰 기관 관리자	trustedadmin@vsphere.local

```
PS C:\Users\Administrator.CORP> Disconnect-VIServer -server * -Confirm:$false
PS C:\Users\Administrator.CORP> Connect-VIServer -server 192.168.210.22 -User
trustedadmin@vsphere.local -Password 'VMware1!'

PS C:\Users\Administrator.CORP> Export-TrustAuthorityServicesInfo -TrustAuthorityCluster $vTA
-FilePath C:\vta\clsettings.json

Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        10/16/2019   9:59 PM           8177 clsettings.json
```

다음에 수행할 작업

신뢰할 수 있는 호스트로 신뢰 기관 클러스터 정보 가져오기으로 계속 진행합니다.

신뢰할 수 있는 호스트로 신뢰 기관 클러스터 정보 가져오기

vSphere 신뢰 기관 클러스터 정보를 신뢰할 수 있는 클러스터로 가져오면 신뢰할 수 있는 호스트에서 신뢰 기관 클러스터를 사용하여 증명 프로세스를 시작합니다.

사전 요구 사항

- 신뢰 기관 관리자 사용.
- 신뢰 기관 상태 사용.
- 신뢰할 수 있는 ESXi 호스트 및 vCenter Server에 대한 정보 수집.
- 신뢰 기관 클러스터로 신뢰할 수 있는 호스트 정보 가져오기.
- 신뢰 기관 클러스터에서 키 제공자 생성.
- 신뢰 기관 클러스터 정보 내보내기.

절차

1 신뢰할 수 있는 클러스터의 vCenter Server에 신뢰 기관 관리자로 연결되어 있는지 확인합니다.

예를 들어 `$global:defaultviservers`를 입력하여 연결된 모든 서버를 표시할 수 있습니다.

2 (선택 사항) 필요한 경우 다음 명령을 실행하여 신뢰할 수 있는 클러스터의 vCenter Server에 연결되어 있는지 확인할 수 있습니다.

```
Disconnect-VIServer -server * -Confirm:$false
Connect-VIServer -server TrustedCluster_VC_ip_address -User trust_admin_user -Password
'password'
```

참고 또는 다른 PowerCLI 세션을 시작하여 신뢰할 수 있는 클러스터의 vCenter Server에 연결할 수도 있습니다.

3 신뢰할 수 있는 클러스터가 사용되지 않도록 설정된 상태인지 확인합니다.

```
Get-TrustedCluster
```

상태가 [사용 안 함]으로 표시되어 있습니다.

4 변수에 `Get-TrustedCluster` 정보를 할당합니다.

예를 들어 다음 명령은 클러스터 `Trusted Cluster`에 대한 정보를 변수 `$TC`에 할당합니다.

```
$TC = Get-TrustedCluster -Name 'Trusted Cluster'
```

5 변수를 에코하여 변수의 값을 확인합니다.

예:

```
$TC
```

`Get-TrustedCluster` 정보가 표시됩니다.

6 신뢰 기관 클러스터 정보를 vCenter Server로 가져오려면 `Import-TrustAuthorityServicesInfo` cmdlet을 실행합니다.

예를 들어 다음 명령은 신뢰 기관 클러스터 정보 내보내기에서 이전에 내보낸 `clsettings.json` 파일에서 서비스 정보를 가져옵니다.

```
Import-TrustAuthorityServicesInfo -FilePath C:\vta\clsettings.json
```

시스템에서 확인 메시지로 응답합니다.

```
Confirmation
Importing the TrustAuthorityServicesInfo into Server 'ip_address'. Do you want to proceed?

[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"):
```

7 확인 메시지가 표시되면 Enter 키를 누릅니다. (기본값은 **Y**입니다.)

신뢰 기관 클러스터의 호스트에 대한 서비스 정보가 표시됩니다.

8 신뢰할 수 있는 클러스터를 사용하도록 설정하려면 `Set-TrustedCluster` cmdlet을 실행합니다.

예:

```
Set-TrustedCluster -TrustedCluster $TC -State Enabled
```

시스템에서 확인 메시지로 응답합니다.

```
Confirmation
Setting TrustedCluster 'cluster' with new TrustedState 'Enabled'. Do you want to proceed?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"):
```

신뢰할 수 있는 클러스터가 정상 상태가 아니면 확인 메시지 앞에 다음과 같은 주의 메시지가 표시됩니다.

```
WARNING: The TrustedCluster 'cluster' is not healthy in its TrustedClusterAppliedStatus.
This cmdlet will automatically remediate the TrustedCluster.
```

9 확인 메시지가 표시되면 Enter 키를 누릅니다. (기본값은 **Y**입니다.)

신뢰할 수 있는 클러스터가 사용되도록 설정되었습니다.

참고 증명 서비스 및 키 제공자 서비스를 개별적으로 사용하도록 설정하여 신뢰할 수 있는 클러스터를 사용하도록 설정할 수도 있습니다. `Add-TrustedClusterAttestationServiceInfo` 및 `Add-TrustedClusterKeyProviderServiceInfo` 명령을 사용합니다. 예를 들어 다음 명령은 두 개의 키 제공자 서비스와 두 개의 증명 서비스가 있는 클러스터 `Trusted Cluster`에 대해 서비스를 한 번에 하나씩 사용하도록 설정합니다.

```
Add-TrustedClusterAttestationServiceInfo -TrustedCluster 'Trusted Cluster'
-AttestationServiceInfo (Get-AttestationServiceInfo | Select-Object -index 0,1)
Add-TrustedClusterKeyProviderServiceInfo  -TrustedCluster 'Trusted Cluster'
-KeyProviderServiceInfo (Get-KeyProviderServiceInfo | Select-Object -index 0,1)
```

---

10 신뢰할 수 있는 클러스터에서 증명 서비스 및 키 제공자 서비스가 구성되었는지 확인합니다.

a 변수에 Get-TrustedCluster 정보를 할당합니다.

예를 들어 다음 명령은 클러스터 Trusted Cluster에 대한 정보를 변수 $TC에 할당합니다.

```
$TC = Get-TrustedCluster -Name 'Trusted Cluster'
```

b 증명 서비스가 구성되었는지 확인합니다.

```
$tc.AttestationServiceInfo
```

증명 서비스 정보가 표시됩니다.

c 키 제공자 서비스가 구성되었는지 확인합니다.

```
$tc.KeyProviderServiceInfo
```

키 제공자 서비스 정보가 표시됩니다.

결과

신뢰할 수 있는 클러스터의 ESXi 신뢰할 수 있는 호스트가 신뢰 기관 클러스터를 사용하여 증명 프로세스를 시작합니다.

예제: 신뢰할 수 있는 호스트로 신뢰 기관 클러스터 정보 가져오기

이 예는 신뢰 기관 클러스터 서비스 정보를 신뢰할 수 있는 클러스터로 가져오는 방법을 보여 줍니다. 다음 표에는 사용되는 예제 구성 요소 및 값이 나와 있습니다.

표 9-10. vSphere 신뢰 기관 설정 예

구성 요소	값
신뢰할 수 있는 클러스터의 vCenter Server	192.168.110.22
신뢰 기관 관리자	trustedadmin@vsphere.local
신뢰할 수 있는 클러스터 이름	신뢰할 수 있는 클러스터
신뢰 기관 클러스터의 ESXi 호스트	192.168.210.51 및 192.168.210.52
변수 $TC	Get-TrustedCluster -Name 'Trusted Cluster'

```
PS C:\Users\Administrator.CORP> Disconnect-VIServer -server * -Confirm:$false
PS C:\Users\Administrator.CORP> Connect-VIServer -server 192.168.110.22 -User
trustedadmin@vsphere.local -Password 'VMware1!'

Name                           Port  User
----                           ----  ----
192.168.110.22                 443   VSPHERE.LOCAL\trustedadmin

PS C:\Users\Administrator.CORP> Get-TrustedCluster
```

```
Name                   State              Id
----                   -----              --
Trusted Cluster        Disabled           TrustedCluster-domain-c8

PS C:\Users\Administrator.CORP> $TC = Get-TrustedCluster -Name 'Trusted Cluster'
PS C:\Users\Administrator.CORP> $TC

Name                   State              Id
----                   -----              --
Trusted Cluster        Disabled           TrustedCluster-domain-c8

PS C:\Users\Administrator.CORP> Import-TrustAuthorityServicesInfo -FilePath
C:\vta\clsettings.json

Confirmation
Importing the TrustAuthorityServicesInfo into Server '192.168.110.22'. Do you want to proceed?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"): y

ServiceAddress                 ServicePort          ServiceGroup
--------------                 -----------          ------------
192.168.210.51                 443                  host-13:86f7ab6c-ad6f-4606-...
192.168.210.52                 443                  host-16:86f7ab6c-ad6f-4606-...
192.168.210.51                 443                  host-13:86f7ab6c-ad6f-4606-...
192.168.210.52                 443                  host-16:86f7ab6c-ad6f-4606-...

PS C:\Users\Administrator.CORP> Set-TrustedCluster -TrustedCluster $TC -State Enabled

Confirmation
Setting TrustedCluster 'Trusted Cluster' with new TrustedState 'Enabled'. Do you want to
proceed?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"):

Name                   State              Id
----                   -----              --
Trusted Cluster        Enabled            TrustedCluster-domain-c8

PS C:\Users\Administrator.CORP> $TC = Get-TrustedCluster -Name 'Trusted Cluster'
PS C:\Users\Administrator.CORP> $tc.AttestationServiceInfo

ServiceAddress                 ServicePort          ServiceGroup
--------------                 -----------          ------------
192.168.210.51                 443                  host-13:dc825986-73d2-463c-...
192.168.210.52                 443                  host-16:dc825986-73d2-463c-...

PS C:\Users\Administrator.CORP> $tc.KeyProviderServiceInfo

ServiceAddress                 ServicePort          ServiceGroup
--------------                 -----------          ------------
192.168.210.51                 443                  host-13:dc825986-73d2-463c-...
192.168.210.52                 443                  host-16:dc825986-73d2-463c-...
```

다음에 수행할 작업

vSphere Client를 사용하여 신뢰할 수 있는 호스트를 위한 신뢰할 수 있는 키 제공자 구성 또는 명령줄을 사용하여 신뢰할 수 있는 호스트를 위한 신뢰할 수 있는 키 제공자 구성 항목으로 계속 진행합니다.

vSphere Client를 사용하여 신뢰할 수 있는 호스트를 위한 신뢰할 수 있는 키 제공자 구성

vSphere Client를 사용하여 신뢰할 수 있는 키 제공자를 구성할 수 있습니다.

사전 요구 사항

- 신뢰 기관 관리자 사용.
- 신뢰 기관 상태 사용.
- 신뢰할 수 있는 ESXi 호스트 및 vCenter Server에 대한 정보 수집.
- 신뢰 기관 클러스터로 신뢰할 수 있는 호스트 정보 가져오기.
- 신뢰 기관 클러스터에서 키 제공자 생성.
- 신뢰 기관 클러스터 정보 내보내기.
- 신뢰할 수 있는 호스트로 신뢰 기관 클러스터 정보 가져오기.

절차

1 vSphere Client를 사용하여 신뢰할 수 있는 클러스터의 vCenter Server에 연결합니다.

2 vCenter Server 관리자 또는 **암호화 작업.키 서버 관리** 권한이 있는 관리자로 로그인합니다.

3 vCenter Server를 선택한 다음 **구성**을 선택합니다.

4 **보안**에서 **키 제공자**를 선택합니다.

5 **신뢰할 수 있는 키 제공자 추가**를 선택합니다.

사용 가능한 신뢰할 수 있는 키 제공자가 [연결됨] 상태로 표시됩니다.

6 신뢰할 수 있는 키 제공자를 선택하고 **키 제공자 추가**를 클릭합니다.

신뢰할 수 있는 키 제공자가 [신뢰됨] 및 [연결됨]으로 표시됩니다. 처음으로 추가한 신뢰할 수 있는 키 제공자인 경우에는 기본값으로 표시됩니다.

참고 모든 호스트가 키 제공자를 가져오고 vCenter Server에서 해당 캐시를 업데이트하려면 시간이 걸립니다. 정보가 전파되는 방식으로 인해 일부 호스트에서 키 작업에 키 제공자를 사용하려면 몇 분 정도 기다려야 할 수 있습니다.

결과

ESXi 신뢰할 수 있는 호스트가 이제 암호화된 가상 시스템 생성과 같은 암호화 작업을 수행할 수 있습니다.

다음에 수행할 작업

신뢰할 수 있는 키 제공자를 사용하여 가상 시스템을 암호화하는 것은 vSphere 6.5에 처음 제공되었던 가상 시스템 암호화 사용자 환경과 동일합니다. 장 10 vSphere 환경에서 암호화 사용의 내용을 참조하십시오.

명령줄을 사용하여 신뢰할 수 있는 호스트를 위한 신뢰할 수 있는 키 제공자 구성

명령줄을 사용하여 신뢰할 수 있는 키 제공자를 구성할 수 있습니다. vCenter Server 서버에 대해 또는 vCenter 개체 계층의 클러스터 또는 폴더 수준에서 신뢰할 수 있는 기본 키 제공자를 구성할 수 있습니다.

사전 요구 사항

- 신뢰 기관 관리자 사용.
- 신뢰 기관 상태 사용.
- 신뢰할 수 있는 ESXi 호스트 및 vCenter Server에 대한 정보 수집.
- 신뢰 기관 클러스터로 신뢰할 수 있는 호스트 정보 가져오기.
- 신뢰 기관 클러스터에서 키 제공자 생성.
- 신뢰 기관 클러스터 정보 내보내기.
- 신뢰할 수 있는 호스트로 신뢰 기관 클러스터 정보 가져오기.

신뢰할 수 있는 클러스터에는 **암호화 작업.KMS 관리** 권한이 포함된 역할이 있어야 합니다.

절차

1 신뢰할 수 있는 클러스터의 vCenter Server에 관리자로 연결되어 있는지 확인합니다.

예를 들어 `$global:defaultviservers`를 입력하여 연결된 모든 서버를 표시할 수 있습니다.

2 (선택 사항) 필요한 경우 다음 명령을 실행하여 신뢰할 수 있는 클러스터의 vCenter Server에 연결되어 있는지 확인할 수 있습니다.

```
Disconnect-VIServer -server * -Confirm:$false
Connect-VIServer -server TrustedCluster_VC_ip_address -User admin_user -Password 'password'
```

3 신뢰할 수 있는 키 제공자를 가져옵니다.

```
Get-KeyProvider
```

`-Name` *keyprovider* 옵션을 사용하여 신뢰할 수 있는 단일 키 제공자를 지정할 수 있습니다.

4 `Get-KeyProvider` 신뢰할 수 있는 키 제공자 정보를 변수에 할당합니다.

예를 들어 다음 명령은 변수 `$workload_kp`에 정보를 할당합니다.

```
$workload_kp = Get-KeyProvider
```

신뢰할 수 있는 키 제공자가 여러 개 있는 경우 Select-Object를 사용하여 하나를 선택할 수 있습니다.

```
$workload_kp = Get-KeyProvider | Select-Object -Index 0
```

5 신뢰할 수 있는 키 제공자를 등록합니다.

```
Register-KeyProvider -KeyProvider $workload_kp
```

신뢰할 수 있는 키 제공자를 추가로 등록하려면 4단계 및 5단계를 반복합니다.

참고 모든 호스트가 키 제공자를 가져오고 vCenter Server에서 해당 캐시를 업데이트하려면 시간이 걸립니다. 정보가 전파되는 방식으로 인해 일부 호스트에서 키 작업에 키 제공자를 사용하려면 몇 분 정도 기다려야 할 수 있습니다.

6 기본으로 사용할 신뢰할 수 있는 키 제공자를 설정합니다.

a vCenter Server 수준에서 기본 키 제공자를 설정하려면 다음 명령을 실행합니다.

```
Set-KeyProvider -KeyProvider $workload_kp -DefaultForSystem
```

b 클러스터 수준에서 키 제공자를 설정하려면 다음 명령을 실행합니다.

예를 들어 이 명령은 클러스터 Trusted Cluster에 대한 키 제공자를 설정합니다.

```
Add-EntityDefaultKeyProvider -KeyProvider $workload_kp -Entity 'Trusted Cluster'
```

c 폴더 수준에서 키 제공자를 설정하려면 다음 명령을 실행합니다.

예를 들어 이 명령은 workLoad 데이터 센터에서 생성된 TC Folder 폴더에 대한 키 제공자를 설정합니다.

```
Add-EntityDefaultKeyProvider -KeyProvider $workload_kp -Entity 'TC Folder'
```

다음에 수행할 작업

신뢰할 수 있는 키 제공자를 사용하여 가상 시스템을 암호화하는 것은 vSphere 6.5에 처음 제공되었던 가상 시스템 암호화 사용자 환경과 동일합니다. 장 10 vSphere 환경에서 암호화 사용의 내용을 참조하십시오.

vSphere 환경에서 vSphere 신뢰 기관 관리

vSphere 신뢰 기관을 구성한 후 서비스 중지 및 시작, 클러스터에 호스트 추가 및 신뢰 기관 클러스터의 상태 보기와 같은 추가 작업을 수행할 수 있습니다.

vSphere Client, API 및 PowerCLI cmdlet을 사용하여 작업을 수행할 수 있습니다. "vSphere Web Services SDK 프로그래밍 가이드" , "VMware PowerCLI" 설명서 및 "VMware PowerCLI Cmdlet 참조" 설명서를 참조하십시오.

vSphere 신뢰 기관 서비스 시작, 중지 및 다시 시작

vSphere Client를 사용하여 vSphere 신뢰 기관 서비스를 시작, 중지 및 다시 시작할 수 있습니다.

vSphere 신뢰 기관을 구성하는 이 서비스는 증명 서비스(attestd) 및 키 제공자 서비스(kmxd)입니다.

절차

1 vSphere Client를 사용하여 vSphere 신뢰 기관 클러스터의 vCenter Server에 연결합니다.

2 관리자로 로그인합니다.

3 신뢰 기관 클러스터의 ESXi 호스트를 찾습니다.

4 **구성**을 선택한 다음 **시스템**에서 **서비스**를 선택합니다.

5 attestd 서비스 및 kmxd 서비스를 찾습니다.

6 필요한 경우 **다시 시작**, **시작** 또는 **중지** 작업을 선택합니다.

신뢰 기관 호스트 보기

vSphere Client를 사용하여 신뢰할 수 있는 클러스터에 대해 구성된 vSphere 신뢰 기관 호스트를 볼 수 있습니다.

절차

1 vSphere Client를 사용하여 신뢰할 수 있는 클러스터의 vCenter Server에 연결합니다.

2 관리자로 로그인합니다.

3 vCenter Server 인스턴스를 선택합니다.

4 **구성** 탭을 클릭하고 **보안**에서 **신뢰 기관**을 선택합니다.

신뢰할 수 있는 클러스터에 대해 구성된 신뢰 기관 클러스터의 ESXi 호스트가 표시됩니다.

vSphere 신뢰 기관 클러스터 상태 보기

vSphere Client를 사용하여 vSphere 신뢰 기관 클러스터의 상태를 볼 수 있습니다. 이 상태는 사용 또는 사용되지 않도록 설정되어 있습니다.

신뢰 기관 클러스터 상태가 사용되도록 설정된 경우 신뢰할 수 있는 클러스터의 신뢰할 수 있는 호스트가 증명 서비스 및 키 제공자 서비스와 통신할 수 있습니다.

절차

1 vSphere Client를 사용하여 신뢰 기관 클러스터의 vCenter Server에 연결합니다.

2 관리자로 로그인합니다.

3 개체 계층에서 신뢰 기관 클러스터를 선택합니다.

4 **구성** 탭을 클릭하고 **신뢰 기관**에서 **신뢰 기관 클러스터**를 선택합니다.

상태가 사용 또는 사용 안 함으로 표시됩니다.

신뢰할 수 있는 호스트 서비스 다시 시작

신뢰할 수 있는 호스트에서 실행되는 서비스를 다시 시작할 수 있습니다.

kmxa 서비스는 ESXi 신뢰할 수 있는 호스트에서 실행됩니다.

사전 요구 사항

ESXi Shell에 대한 액세스를 사용하도록 설정해야 합니다. ESXi Shell에 대한 액세스를 사용하도록 설정의 내용을 참조하십시오.

절차

1 SSH 또는 다른 원격 콘솔 연결을 사용하여 ESXi 신뢰할 수 있는 호스트에서 세션을 시작합니다.

2 root로 로그인합니다.

3 다음 명령을 실행합니다.

```
/etc/init.d/kmxa restart
```

vSphere 신뢰 기관 호스트 추가 및 제거

VMware 제공 스크립트를 사용하여 vSphere 신뢰 기관 클러스터에 ESXi 호스트를 추가하고 제거합니다.

vSphere 7.0에서는VMware 제공 스크립트를 사용하여 기존 vSphere 신뢰 기관 클러스터 또는 신뢰할 수 있는 클러스터에 ESXi 호스트를 추가하고 제거합니다. vSphere 7.0 업데이트 1부터는 업데이트 적용 기능을 사용하여 ESXi 호스트를 기존의 신뢰할 수 있는 클러스터에 추가합니다. vSphere Client를 사용하여 신뢰할 수 있는 클러스터에 호스트 추가 및 CLI를 사용하여 신뢰할 수 있는 클러스터에 호스트 추가의 내용을 참조하십시오. vSphere 7.0 업데이트 1에서 기존 신뢰 기관 클러스터에 ESXi 호스트를 추가하려면 여전히 스크립트를 사용해야 합니다. https://kb.vmware.com/s/article/77234 및 https://kb.vmware.com/s/article/77146에서 VMware 기술 자료 문서를 참조하십시오.

vSphere Client를 사용하여 신뢰할 수 있는 클러스터에 호스트 추가

vSphere Client를 사용하여 기존의 신뢰할 수 있는 클러스터에 ESXi 호스트를 추가할 수 있습니다.

신뢰할 수 있는 클러스터를 처음 구성한 후 ESXi 호스트를 더 추가해야 할 수도 있습니다. 단, 신뢰할 수 있는 클러스터에 호스트를 추가하는 경우에는 업데이트 적용의 추가 단계를 수행해야 합니다. 신뢰할 수 있는 클러스터에 업데이트를 적용하는 경우 원하는 구성 상태가 적용된 구성과 일치하는지 확인합니다.

vSphere 7.0에서 릴리스된 vSphere 신뢰 기관의 첫 번째 버전에서는 스크립트를 실행하여 신뢰할 수 있는 기존 클러스터에 호스트를 추가합니다. vSphere 7.0 업데이트 1부터는 업데이트 적용 기능을 사용하여 신뢰할 수 있는 클러스터에 호스트를 추가합니다. vSphere 7.0 업데이트 1에서도 기존 신뢰 기관 클러스터에 호스트를 추가하려면 스크립트를 사용해야 합니다. vSphere 신뢰 기관 호스트 추가 및 제거의 내용을 참조하십시오.

사전 요구 사항

신뢰할 수 있는 클러스터에 대한 vCenter Server는 vSphere 7.0 업데이트 1 이상을 실행하고 있어야 합니다.

신뢰할 수 있는 클러스터에 대해 처음 구성한 것과 다른 ESXi 버전 또는 다른 TPM 하드웨어 유형의 ESXi 호스트를 추가하는 경우에는 추가 단계가 필요합니다. 이러한 정보를 vSphere 신뢰 기관 클러스터로 내보내고 가져와야 합니다. 신뢰할 수 있는 ESXi 호스트 및 vCenter Server에 대한 정보 수집 및 신뢰 기관 클러스터로 신뢰할 수 있는 호스트 정보 가져오기의 내용을 참조하십시오.

필요한 권한: 일반 작업에 필요한 권한에서 호스트 추가 작업을 참조하십시오.

절차

1 vSphere Client를 사용하여 신뢰할 수 있는 클러스터의 vCenter Server에 연결합니다.

2 신뢰 기관 관리자로 로그인합니다.

3 신뢰할 수 있는 클러스터로 이동합니다.

4 **구성** 탭에서 **구성 > Quickstart**를 선택합니다.

5 **호스트 추가** 카드에서 **추가**를 클릭합니다.

6 표시되는 메시지를 따릅니다.

7 **신뢰 기관** 탭에서 **업데이트 적용**을 클릭합니다.

8 신뢰할 수 있는 클러스터가 정상인지 확인하려면 **상태 점검**을 클릭합니다.

CLI를 사용하여 신뢰할 수 있는 클러스터에 호스트 추가

명령줄을 사용하여 기존의 신뢰할 수 있는 클러스터에 ESXi 호스트를 추가할 수 있습니다.

신뢰할 수 있는 클러스터를 처음 구성한 후 ESXi 호스트를 더 추가해야 할 수도 있습니다. 단, 신뢰할 수 있는 클러스터에 호스트를 추가하는 경우에는 업데이트 적용의 추가 단계를 수행해야 합니다. 신뢰할 수 있는 클러스터에 업데이트를 적용하는 경우 원하는 구성 상태가 적용된 구성과 일치하는지 확인합니다.

vSphere 7.0에서 릴리스된 vSphere 신뢰 기관의 첫 번째 버전에서는 스크립트를 실행하여 신뢰할 수 있는 기존 클러스터에 호스트를 추가합니다. vSphere 7.0 업데이트 1부터는 업데이트 적용 기능을 사용하여 신뢰할 수 있는 호스트를 추가합니다. vSphere 7.0 업데이트 1에서도 기존 신뢰 기관 클러스터에 호스트를 추가하려면 스크립트를 사용해야 합니다. vSphere 신뢰 기관 호스트 추가 및 제거의 내용을 참조하십시오.

사전 요구 사항

- 신뢰할 수 있는 클러스터에 대한 vCenter Server는 vSphere 7.0 업데이트 1 이상을 실행하고 있어야 합니다.
- PowerCLI 12.1.0 이상이 필요합니다.
- 필요한 권한: 일반 작업에 필요한 권한에서 호스트 추가 작업을 참조하십시오.

절차

1 일반적으로 수행하는 단계를 사용하여 신뢰할 수 있는 클러스터에 ESXi 호스트를 추가합니다.

2 PowerCLI 세션에서 `Connect-VIServer` cmdlet을 실행하여 신뢰 기관 관리자로 신뢰할 수 있는 클러스터의 vCenter Server에 연결합니다.

```
Connect-VIServer -server TrustedCluster_VC_ip_address -User trust_admin_user -Password
'password'
```

3 신뢰할 수 있는 클러스터의 상태를 확인하려면 `Get-TrustedClusterAppliedStatus` PowerCLI cmdlet을 실행합니다.

```
Get-TrustedClusterAppliedStatus -TrustedCluster 'TrustedCluster'
```

4 신뢰할 수 있는 클러스터가 정상이 아닌 경우 `Set-TrustedCluster` cmdlet을 `-Remediate` 매개 변수와 함께 실행합니다.

```
Set-TrustedCluster -TrustedCluster 'TrustedCluster' -Remediate
```

5 신뢰할 수 있는 클러스터가 정상인지 확인하려면 `Get-TrustedClusterAppliedStatus` cmdlet을 다시 실행합니다.

```
Get-TrustedClusterAppliedStatus -TrustedCluster 'TrustedCluster'
```

신뢰할 수 있는 클러스터에서 신뢰할 수 있는 호스트 서비스 해제

신뢰할 수 있는 클러스터에서 신뢰할 수 있는 호스트를 제거하거나 서비스 해제할 수 있습니다. 시나리오에 따라 신뢰할 수 있는 클러스터에서 신뢰할 수 있는 호스트 하나 또는 모두를 서비스 해제할 수 있습니다.

신뢰할 수 있는 호스트를 서비스 해제하면 업데이트 적용 기능은 신뢰할 수 있는 호스트의 원하는 상태를 이 호스트가 이동하여 들어간 신뢰할 수 없는 클러스터의 상태로 설정합니다. 서비스 해제된 신뢰할 수 있는 호스트는 일반 호스트가 됩니다. 신뢰할 수 있는 클러스터(신뢰할 수 있는 호스트가 이동하여 나간)는 원하는 상태 구성을 계속 유지하고 신뢰할 수 있는 클러스터로 계속 작동합니다.

신뢰할 수 있는 클러스터에서 신뢰할 수 있는 호스트를 모두 제거하면 신뢰할 수 있는 클러스터를 서비스 해제합니다. 신뢰할 수 있는 호스트와 신뢰할 수 있는 클러스터에서 원하는 상태 구성과 적용된 구성을 모두 제거한 다음, 신뢰할 수 있는 호스트를 신뢰할 수 없는 클러스터로 모두 이동합니다.

사용자 환경에서 서비스 해제된 신뢰할 수 있는 호스트를 재사용할 수 있습니다. 예를 들어,신뢰할 수 없는 인프라 용량의 호스트를 재사용하거나 vSphere 신뢰 기관 호스트로 재사용할 수 있습니다. 서비스 해제된 호스트를 동일한 vCenter Server 또는 다른 vCenter Server에서 사용할 수 있습니다.

신뢰할 수 있는 클러스터 구성 및 상태에 대한 자세한 내용은 신뢰할 수 있는 클러스터 상태 및 업데이트 적용 개요 항목을 참조하십시오.

사전 요구 사항

- 신뢰할 수 있는 클러스터에 대한 vCenter Server는 vSphere 7.0 업데이트 1 이상을 실행하고 있어야 합니다.
- PowerCLI를 사용하는 경우 버전 12.1.0 이상이 필요합니다.

절차

1 vSphere Client를 사용하여 신뢰할 수 있는 클러스터의 vCenter Server에 연결합니다.

2 신뢰 기관 관리자로 로그인합니다.

3 신뢰할 수 있는 클러스터로 이동합니다.

4 신뢰할 수 있는 클러스터에서 신뢰할 수 있는 호스트를 서비스 해제하는 방법을 결정합니다.

작업	단계
신뢰할 수 있는 클러스터 및 나머지 신뢰할 수 있는 호스트의 원하는 구성 상태를 유지	a 호스트를 유지 보수 모드로 전환하고, 비어 있는 새 클러스터(즉,클러스터에 호스트가 포함되어 있지 않음)로 이동합니다. b 호스트에서 유지 보수 모드를 종료합니다. c 비어 있는 새 클러스터(신뢰할 수 있는 클러스터가 아님)의 경우 **신뢰 기관** 탭에서 **업데이트 적용**을 클릭합니다. 업데이트 적용은 이동된 호스트에서 신뢰할 수 있는 구성을 제거합니다. 신뢰할 수 있는 클러스터는 원하는 상태 구성을 유지합니다.

모든 신뢰할 수 있는 호스트의 원하는 구성 상태 및 적용된 구성 상태를 제거	a PowerCLI 세션에서 `Connect-VIServer` cmdlet을 실행하여 신뢰 기관 관리자로 신뢰할 수 있는 클러스터의 vCenter Server에 연결합니다.
	`Connect-VIServer -server TrustedCluster_VC_ip_address -User trust_admin_user -Password 'password'`
	b `Set-TrustedCluster` cmdlet을 실행합니다.예를 들면 다음과 같습니다.
	`Set-TrustedCluster -TrustedCluster 'TrustedCluster' -State Disabled`
	신뢰할 수 있는 인프라 구성이 모든 신뢰할 수 있는 호스트에서 제거되고 신뢰할 수 있는 클러스터에서 원하는 상태 구성이 제거됩니다.
	c 모든 호스트를 유지 보수 모드로 전환하고 다른 클러스터로 이동합니다.
	d 호스트에서 유지 보수 모드를 종료합니다.

5 신뢰할 수 있는 클러스터가 정상인지 확인하려면, 신뢰할 수 있는 클러스터의 **신뢰 기관** 탭에서 **상태 점검**을 클릭합니다.

다음에 수행할 작업

서비스 해제된 ESXi 호스트에서 특정 버전의 ESXi 또는 TPM하드웨어를 더 이상 증명할 계획이 없으면, 최적의 보안을 위해 신뢰 기관 클러스터의 구성을 업데이트합니다. VMware 기술 자료 문서(https://kb.vmware.com/s/article/77146)를 참조하십시오.

vSphere 신뢰 기관 구성 백업

vSphere 신뢰 기관을 신뢰 기관 백업으로 구성할 때 내보낸 파일을 사용합니다. 이러한 파일을 사용하여 신뢰 기관 배포를 복원할 수 있습니다. 이러한 구성 파일을 기밀로 유지하고 안전하게 전송합니다.

대부분의 vSphere 신뢰 기관 구성 및 상태 정보는 ConfigStore 데이터베이스의 ESXi 호스트에 저장됩니다. vCenter Server 인스턴스를 백업하는 데 사용하는 vCenter Server 관리 인터페이스는 vSphere 신뢰 기관에 대한 구성 정보를 백업하지 않습니다. vSphere 신뢰 기관 환경을 설정할 때 내보낸 구성 파일을 저장하고 안전하게 보관하면 vSphere 신뢰 기관 구성을 복원하는 데 필요한 정보가 있는 것입니다. 이 정보를 생성해야 하는 경우 신뢰할 수 있는 ESXi 호스트 및 vCenter Server에 대한 정보 수집의 내용을 참조하십시오.

키 제공자의 기본 키 변경

키 제공자의 기본 키를 변경할 수 있습니다(예: 사용되는 기본 키를 순환하려는 경우).

키 수명주기에 대한 지침은 가상 시스템 암호화 모범 사례에서 참조하십시오.

사전 요구 사항

신뢰할 수 있는 키 제공자의 새 기본 키로 사용할 키를 키 서버(KMS)에 생성하고 활성화합니다. 이 키는 신뢰할 수 있는 키 제공자가 사용하는 다른 키와 암호를 래핑합니다. 키 생성에 대한 자세한 내용은 KMS 벤더 설명서를 참조하십시오.

절차

1 `Set-TrustAuthorityKeyProvider` 명령을 실행합니다.

예:

```
Set-TrustAuthorityKeyProvider -MasterKeyId Key-ID
```

2 키 제공자의 상태를 확인합니다.

a 변수에 Get-TrustAuthorityCluster 정보를 할당합니다.

예:

```
$vTA = Get-TrustAuthorityCluster 'vTA Cluster'
```

b 변수에 Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA 정보를 할당합니다.

예:

```
$kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
```

c $kp.Status를 실행하여 키 제공자의 상태를 확인합니다.

예:

```
$kp.Status

KeyProviderId Health HealthDetails ServerStatus
------------- ------ ------------- ------------
domain-c8-kp4     Ok {}            {IP_address}
```

상태가 정상이면 키 제공자가 올바르게 실행되고 있음을 나타냅니다.

결과

새 기본 키는 새로운 암호화 작업에 사용됩니다. 이전 기본 키로 암호화된 데이터는 여전히 이전 키를 사용하여 암호 해독됩니다.

신뢰할 수 있는 호스트 증명 보고 개요

vSphere 신뢰 기관에서 vCenter Server는 신뢰할 수 있는 호스트의 증명 상태를 확인하고 보고합니다. vSphere Client를 사용하여 신뢰할 수 있는 호스트의 증명 상태를 볼 수 있습니다.

vSphere 신뢰 기관은 신뢰할 수 있는 호스트에 대한 원격 증명을 사용하여 부팅 소프트웨어의 신뢰성을 입증합니다. 증명은 신뢰할 수 있는 호스트가 정품 VMware 소프트웨어 또는 VMware에서 서명한 파트너 소프트웨어를 실행 중인지 확인합니다. 신뢰할 수 있는 클러스터의 vCenter Server는 신뢰할 수 있는 호스트와 통신하여 내부 증명 보고서를 가져옵니다. 증명 보고서는 신뢰할 수 있는 호스트가 신뢰 기관 클러스터에서 실행 중인 증명 서비스로 증명되었는지 여부를 지정합니다. 신뢰할 수 있는 호스트가 증명되지 않은 경우에는 증명 보고서가 오류 메시지도 지정합니다. vSphere Client는 신뢰할 수 있는 호스트에 대해 다음과 같은 증명 상태를 표시합니다.

통과

신뢰할 수 있는 호스트가 vSphere 신뢰 기관 증명 서비스를 사용하여 증명되고 내부 증명 보고서를 vCenter Server에 사용할 수 있습니다.

실패

신뢰할 수 있는 호스트가 vSphere 신뢰 기관 증명 서비스를 사용하여 증명될 수 없습니다. vCenter Server 내부 증명 보고서에는 신뢰할 수 있는 호스트가 증명을 시도하는 증명 서비스에서 보고한 오류가 포함되어 있습니다.

vSphere Client는 호스트가 vSphere 신뢰 기관 또는 vCenter Server로 증명되었는지 여부도 표시합니다.

신뢰할 수 있는 호스트가 증명되지 않은 경우 신뢰할 수 있는 호스트에서 실행 중인 암호화된 가상 시스템을 포함한 가상 시스템에 계속 액세스할 수 있습니다. 증명되지 않은 신뢰할 수 있는 호스트에서 가상 시스템의 전원을 켤 수 없습니다. 그러나 암호화되지 않은 가상 시스템을 여전히 추가할 수 있습니다. 신뢰할 수 있는 호스트가 증명되지 않은 경우 증명 문제를 해결하는 단계를 수행합니다. 증명 개념에 대한 자세한 내용은 vSphere 신뢰 기관 프로세스 흐름 항목을 참조하십시오.

여러 신뢰 기관 호스트를 구성한 경우 각 호스트에서 여러 개의 증명 보고서를 사용할 수 있습니다. 상태 보고 시 vSphere Client는 첫 번째 "증명된" 보고서에서 발견한 상태를 표시합니다. "증명된" 보고서가 없는 경우 vSphere Client는 첫 번째 "증명되지 않은" 보고서에서 발견한 오류를 표시합니다.

여러 신뢰 기관 호스트를 구성한 경우에도 vSphere Client는 하나의 증명 보고서에서만 상태를 표시하고 오류 메시지를 잠재적으로 표시합니다.

신뢰할 수 있는 클러스터 증명 상태 보기

vSphere Client를 사용하여 신뢰할 수 있는 호스트의 증명 상태를 볼 수 있습니다.

사전 요구 사항

- 신뢰할 수 있는 호스트와 vSphere 신뢰 기관 호스트가 ESXi 7.0 업데이트 1 이상을 실행 중이어야 합니다.
- 해당 클러스터에 대한 vCenter Server 호스트가 vSphere 7.0 업데이트 1 이상을 실행 중이어야 합니다.

절차

1. vSphere Client를 사용하여 신뢰할 수 있는 클러스터의 vCenter Server에 연결합니다.
2. 관리자로 로그인합니다.

   신뢰 기관 관리자 또는 vSphere 관리자로 로그인할 수 있습니다.
3. 데이터 센터로 이동하고 **모니터** 탭을 클릭합니다.
4. **보안**을 클릭합니다.
5. [무결성] 열에서 신뢰할 수 있는 호스트의 상태를 검토하고 [메시지] 열에서 함께 제공된 메시지를 읽습니다.

다음에 수행할 작업

오류가 있는 경우 신뢰할 수 있는 호스트 증명 문제 해결 항목을 참조하십시오.

신뢰할 수 있는 호스트 증명 문제 해결

vSphere 신뢰 기관 증명 보고는 신뢰할 수 있는 호스트 증명 오류 문제 해결을 위한 시작 지점을 제공합니다.

절차

1 신뢰할 수 있는 클러스터 증명 상태 보기.

2 다음 표를 사용하여 문제 및 오류를 해결합니다.

Error	원인 및 해결 방법
증명서비스가 구성되지 않았습니다.	증명 서비스가 구성되지 않았습니다. 업데이트 적용 작업을 사용하여 증명 서비스를 사용하도록 신뢰할 수 있는 호스트를 구성합니다. 신뢰할 수 있는 클러스터에 업데이트 적용의 내용을 참조하십시오.
사용 가능한 TPM2 디바이스가 없습니다.	TPM(신뢰할 수 있는 플랫폼 모듈)을 사용하도록 신뢰할 수 있는 호스트를 설치 및 구성합니다. 벤더 설명서를 참조하십시오.
TPM2 승인 공용 키 또는 인증서를 검색할 수 없습니다.	TPM이 지원되고 유효한 승인 키가 있는지 확인합니다. VMware 지원팀에 문의해야 할 수 있습니다.
증명 보고서를 사용할 수 없습니다.	신뢰할 수 있는 호스트가 증명을 마치지 않았을 수 있습니다. 몇 분 정도 기다린 후 증명 상태를 다시 확인합니다.
증명 서비스 버전이 요청과 호환되지 않습니다.	증명 서비스를 실행하는 신뢰 기관 호스트를 vSphere 7.0 업데이트 1 이상으로 업데이트합니다.
보안 부팅을 사용하도록 설정하지 않아 증명에 실패했습니다.	신뢰할 수 있는 호스트가 보안 부팅을 사용하도록 구성되었는지 확인합니다. ESXi 호스트를 위한 UEFI 보안 부팅의 내용을 참조하십시오.
증명을 통해 원격 소프트웨어 버전을 식별하지 못했습니다.	신뢰할 수 있는 호스트의 기본 이미지 정보를 증명 서비스로 가져옵니다. 신뢰 기관 클러스터로 신뢰할 수 있는 호스트 정보 가져오기의 내용을 참조하십시오.
TPM 인증서 필요 사항으로 인해 증명에 실패했습니다.	TPM이 지원되는지 확인합니다. 또는 다음 PowerCLI cmdlet을 실행하여 `requireCertificateValidation`을 `false`로 설정하도록 com.vmware.esx.attestation.tpm2.settings를 수정합니다. `Set-TrustAuthorityTpm2AttestationSettings -TrustAuthorityCluster TrustedCluster -RequireCertificateValidation:$false -RequireEndorsementKey:$true`
알 수 없는 TPM으로 인해 증명에 실패했습니다.	TPM 승인 키를 증명 서비스로 가져옵니다. 신뢰 기관 클러스터로 신뢰할 수 있는 호스트 정보 가져오기의 내용을 참조하십시오.
오류: vapi.send.failed.	kmxa 서비스가 신뢰할 수 있는 호스트에서 실행되고 있지 않거나 kmxa 서비스를 증명 서비스에 연결할 수 없습니다. kmxa 서비스가 시작되었는지 확인합니다. 또한 증명 서비스가 실행 중인지 확인합니다. 신뢰할 수 있는 호스트 서비스 다시 시작의 내용을 참조하십시오.

신뢰할 수 있는 클러스터 상태 확인 및 업데이트 적용

신뢰할 수 있는 클러스터의 상태를 확인하고 검증할 수 있습니다. 신뢰할 수 있는 클러스터의 상태에 문제가 발생하면 신뢰할 수 있는 클러스터의 구성에 업데이트를 적용할 수 있습니다.

신뢰할 수 있는 클러스터 상태 및 업데이트 적용 개요

신뢰할 수 있는 클러스터의 구성이 정상이 아닌 경우 구성 불일치를 해결해야 합니다. 이렇게 하려면 신뢰할 수 있는 클러스터에 업데이트를 적용합니다. 신뢰할 수 있는 클러스터에 업데이트를 적용할 때 신뢰할 수 있는 클러스터의 모든 신뢰할 수 있는 호스트에 동일한 신뢰할 수 있는 구성이 있는지 확인합니다.

신뢰할 수 있는 클러스터는 신뢰 기관 클러스터에 의해 원격으로 증명되는 신뢰할 수 있는 ESXi 호스트의 vCenter Server 클러스터로 구성됩니다. vSphere 신뢰 기관을 처음으로 구성하는 경우 신뢰 기관 클러스터에서 신뢰할 수 있는 클러스터로 신뢰 기관 서비스 정보를 가져와야 합니다. 신뢰할 수 있는 클러스터는 신뢰 기관 클러스터에서 실행되는 증명 서비스 및 키 제공자 서비스 연결을 위한 구성 요소의 구성을 사용합니다. 신뢰할 수 있는 클러스터 구성에 대한 자세한 내용은 신뢰할 수 있는 호스트로 신뢰 기관 클러스터 정보 가져오기 항목을 참조하십시오. 신뢰할 수 있는 클러스터를 구성한 후에는 해당 상태를 확인하고 업데이트를 적용할 수 있습니다.

신뢰할 수 있는 클러스터 상태 개요

신뢰할 수 있는 클러스터의 상태를 확인하는 작업은 다음에 따라 달라집니다.

원하는 상태 구성

원하는 상태 구성은 신뢰할 수 있는 클러스터로 가져오는 신뢰 기관 서비스 정보를 기반으로 합니다. 원하는 상태 구성은 신뢰할 수 있는 클러스터의 "믿을 수 있는 소스"입니다. 신뢰할 수 있는 클러스터를 설정할 때 처음에 생성된 것으로 원하는 상태 구성을 고려합니다.

적용된 구성

적용된 구성은 신뢰할 수 있는 클러스터를 구성한 특정 증명 서비스 및 키 제공자 서비스 등록입니다. 적용된 구성은 신뢰할 수 있는 클러스터가 현재 실행 중인 것입니다. 적용된 구성을 "런타임" 구성으로 간주할 수 있습니다. 원하는 상태 구성은 적용된 구성과 일치해야 합니다. 단, 적용된 구성이 원하는 상태 구성과 일치하지 않으면 신뢰할 수 있는 클러스터가 "정상이 아님"으로 간주됩니다. 정상이 아닌 신뢰할 수 있는 클러스터는 성능이 저하되거나 전혀 작동하지 않을 수 있습니다.

이 상태 점검은 신뢰할 수 있는 클러스터 또는 vSphere 신뢰 기관 인프라의 전반적인 상태에 대한 표시기가 아닙니다. 상태 점검은 신뢰할 수 있는 클러스터의 원하는 상태 구성을 적용된 구성과 비교만 합니다.

신뢰할 수 있는 클러스터 업데이트 적용 개요

업데이트 적용은 vSphere 신뢰 기관이 신뢰할 수 있는 클러스터의 일관되지 않은 구성을 해결하는 프로세스입니다. 신뢰할 수 있는 클러스터의 구성이 시간이 경과하거나 다른 작업 오류로 인해 일관되지 않을 수 있습니다.

다음과 같은 방식으로 업데이트 적용을 사용합니다.

- 신뢰할 수 있는 클러스터 상태를 확인합니다.
- 신뢰할 수 있는 클러스터가 비정상이면 업데이트를 적용합니다.

vSphere Client 또는 CLI를 사용하여 신뢰할 수 있는 클러스터 상태를 확인할 수 있습니다. 신뢰할 수 있는 클러스터 상태 확인의 내용을 참조하십시오. vSphere Client 또는 CLI를 사용하여 신뢰할 수 있는 클러스터에 업데이트를 적용할 수도 있습니다. 신뢰할 수 있는 클러스터에 업데이트 적용의 내용을 참조하십시오.

참고 업데이트 적용은 기존의 신뢰할 수 있는 클러스터에 호스트를 추가할 때 사용하는 적절한 프로세스이기도 합니다. vSphere Client를 사용하여 신뢰할 수 있는 클러스터에 호스트 추가 및 CLI를 사용하여 신뢰할 수 있는 클러스터에 호스트 추가의 내용을 참조하십시오.

신뢰할 수 있는 클러스터 상태 확인

vSphere Client 또는 명령줄을 사용하여 신뢰할 수 있는 클러스터의 상태를 확인할 수 있습니다.

자세한 내용은 신뢰할 수 있는 클러스터 상태 및 업데이트 적용 개요의 내용을 참조하십시오.

사전 요구 사항

- 신뢰할 수 있는 클러스터에 대한 vCenter Server는 vSphere 7.0 업데이트 1 이상을 실행하고 있어야 합니다.
- PowerCLI를 사용하는 경우 버전 12.1.0 이상이 필요합니다.

절차

1 신뢰할 수 있는 클러스터 상태를 확인합니다.

도구	단계
vSphere Client	a vSphere Client를 사용하여 신뢰할 수 있는 클러스터의 vCenter Server에 연결합니다. b 신뢰 기관 관리자로 로그인합니다. c 신뢰할 수 있는 클러스터로 이동하고 **구성**을 선택한 다음, **신뢰 기관**을 선택합니다. d **상태 점검**을 클릭합니다.

CLI	a PowerCLI 세션에서 `Connect-VIServer` cmdlet을 실행하여 신뢰 기관 관리자로 신뢰할 수 있는 클러스터의 vCenter Server에 연결합니다.
	`Connect-VIServer -server TrustedCluster_VC_ip_address -User trust_admin_user -Password 'password'`
	b `Get-TrustedClusterAppliedStatus` cmdlet을 실행합니다.예를 들면 다음과 같습니다.
	`Get-TrustedClusterAppliedStatus -TrustedCluster 'TrustedCluster'`

2 오류가 있는 경우 신뢰할 수 있는 클러스터에 업데이트 적용 항목을 참조하십시오.

신뢰할 수 있는 클러스터에 업데이트 적용

vSphere Client 또는 명령줄을 사용하여 신뢰할 수 있는 클러스터의 구성에 업데이트를 적용할 수 있습니다.

사전 요구 사항

신뢰할 수 있는 클러스터에 대한 vCenter Server는 vSphere 7.0 업데이트 1 이상을 실행하고 있어야 합니다.

절차

1 신뢰할 수 있는 클러스터의 vCenter Server에 연결합니다.

도구	단계
vSphere Client	a vSphere Client를 사용하여 신뢰할 수 있는 클러스터의 vCenter Server에 연결합니다. b 신뢰 기관 관리자로 로그인합니다.
CLI	PowerCLI 세션에서 `Connect-VIServer` cmdlet을 실행하여 신뢰 기관 관리자로 신뢰할 수 있는 클러스터의 vCenter Server에 연결합니다. `Connect-VIServer -server TrustedCluster_VC_ip_address -User trust_admin_user -Password 'password'`

2 신뢰할 수 있는 클러스터에 업데이트를 적용한 후 신뢰할 수 있는 클러스터 상태를 다시 확인합니다.

도구	단계
vSphere Client	a 신뢰할 수 있는 클러스터로 이동합니다. b **구성**을 선택한 다음 **신뢰 기관**을 선택합니다. c **업데이트 적용**을 클릭합니다. d **상태 점검**을 클릭합니다.

CLI	a 다음과 같이 `-Remediate` 매개 변수를 사용하여 `Set-TrustedCluster` cmdlet을 실행합니다.
	`Set-TrustedCluster -TrustedCluster 'TrustedCluster' -Remediate`
	b `Get-TrustedClusterAppliedStatus` cmdlet을 실행합니다.예를 들면 다음과 같습니다.
	`Get-TrustedClusterAppliedStatus -TrustedCluster 'TrustedCluster'`

vSphere 환경에서 암호화 사용 10

표준 키 제공자, 신뢰할 수 있는 키 제공자, vSphere Native Key Provider 중에 무엇을 사용하든 vSphere 환경에서 암호화를 사용하려면 몇 가지 준비가 필요합니다.

환경을 설정한 후 vSphere Client를 사용하여 암호화된 가상 시스템과 가상 디스크를 생성하고 기존 가상 시스템과 디스크를 암호화할 수 있습니다.

API 및 `crypto-util` CLI를 사용하여 추가 작업을 수행할 수 있습니다. API 설명서는 "vSphere Web Services SDK 프로그래밍 가이드" 의 내용을, 해당 도구에 대한 세부 정보는 `crypto-util` 명령줄 도움말을 참조하십시오.

암호화 스토리지 정책 생성

암호화된 가상 시스템을 생성하려면 먼저 암호화 스토리지 정책을 생성해야 합니다. 스토리지 정책은 한 번 생성하여 가상 시스템 또는 가상 디스크를 암호화할 때마다 할당합니다.

다른 I/O 필터와 함께 가상 시스템 암호화를 사용하거나 vSphere Client에서 **VM 스토리지 정책 생성** 마법사를 사용하려는 경우에는 "vSphere 스토리지" 설명서에서 세부 정보를 참조하십시오.

사전 요구 사항

- 키 제공자에 대한 연결을 설정합니다.

  키 제공자에 연결되지 않은 상태에서 VM 암호화 스토리지 정책을 생성할 수 있지만 키 제공자와 신뢰할 수 있는 연결을 설정해야만 암호화 작업을 수행할 수 있습니다.

- 필요한 권한: **암호화 작업.암호화 정책 관리**.

절차

1. vSphere Client를 사용하여 vCenter Server에 로그인합니다.
2. **홈**을 선택하고 **정책 및 프로파일**을 클릭한 후 **VM 스토리지 정책**을 클릭합니다.
3. **생성**을 클릭합니다.
4. vCenter Server를 선택하고 정책 이름을 입력한 다음 필요한 경우 설명을 입력한 후 **다음**을 클릭합니다.
5. **정책 구조** 페이지에서 **호스트 기반 역할 사용**을 선택하고 **다음**을 클릭합니다.

6 **호스트 기반 서비스** 페이지에서 **스토리지 정책 구성 요소 사용**을 선택하고 드롭다운 메뉴에서 **기본 암호화 속성**을 선택한 후 **다음**을 클릭합니다.

7 **스토리지 호환성** 페이지에서 **호환**을 선택한 상태로 두고 데이터스토어를 선택한 후 **다음**을 클릭합니다.

8 정보를 검토하고 **마침**을 클릭합니다.

결과

VM 암호화 스토리지 정책이 목록에 추가되고 가상 시스템을 암호화할 때 사용할 수 있습니다.

호스트 암호화 모드를 사용하도록 명시적으로 설정

암호화된 가상 시스템을 생성하는 것과 같은 암호화 작업을 ESXi 호스트에서 수행하려면 호스트 암호화 모드를 사용하도록 설정해야 합니다. 대부분의 경우 호스트 암호화 모드는 암호화 작업을 수행할 때 자동으로 사용하도록 설정됩니다.

경우에 따라 암호화 모드를 명시적으로 사용하도록 설정하는 것이 필요합니다. 암호화 작업의 사전 요구 사항 및 필요한 권한의 내용을 참조하십시오.

사전 요구 사항

필요한 권한: **암호화 작업.호스트 등록**

절차

1 vSphere Client를 사용하여 vCenter Server에 로그인합니다.

2 ESXi 호스트를 찾아서 **구성**을 클릭합니다.

3 시스템 아래에서 **보안 프로파일**을 클릭합니다.

4 [호스트 암호화 모드] 패널에서 **편집**을 클릭합니다.

5 **사용**을 선택하고 **확인**을 클릭합니다.

API를 사용하여 호스트 암호화 모드 사용 안 함

호스트 암호화 모드는 암호화 작업을 수행할 때 사용자가 암호화 모드를 사용할 권한이 충분하다면 자동으로 사용되도록 설정됩니다. 호스트 암호화 모드가 사용하도록 설정된 후에는 중요한 정보가 지원 담당자에게 노출되지 않도록 모든 코어 덤프가 암호화됩니다. ESXi 호스트에서 가상 시스템 암호화를 더 이상 사용하지 않는 경우에는 암호화 모드를 사용하지 않도록 설정할 수 있습니다.

ESXi 호스트에 대해 암호화 모드가 사용되도록 설정한 후 사용되지 않도록 설정해야 할 수도 있습니다. 예를 들어 ESXi 지원 번들을 생성하기 위해 암호화 모드가 사용되지 않도록 설정해야 할 수 있습니다(`vm-support` 명령 사용). 호스트에 키 자료가 있는 경우 [호스트 암호화 모드 사용 안 함] 토글(**호스트 > 구성 > 보안 프로파일 > 호스트 암호화 모드 편집**)을 사용하면 작동하지 않습니다.

API를 사용하여 `CryptoManagerHostDisable` API 메서드를 호출하여 호스트 암호화 모드가 사용되지 않도록 설정할 수 있습니다.

ESXi 호스트에 대해 정의된 암호화 모드 또는 상태는 다음과 같습니다.

- pendingIncapable: 호스트에 암호화가 사용되지 않도록 설정되어 있습니다. 즉, 호스트가 vSphere 가상 시스템 암호화 작업을 수행할 수 없습니다.
- incapable: 호스트가 중요한 자료를 수신하기에 안전하지 않습니다.
- prepared: 호스트가 중요한 자료를 수신할 준비가 되었지만 호스트 키가 아직 설정되어 있지 않습니다.
- safe: 호스트가 암호화 보안 상태이고(사용하도록 설정됨) 호스트 키가 설정되어 있습니다. 즉, vSphere 가상 시스템 암호화 작업이 가능합니다.

호스트에서 `CryptoManagerHostDisable`을 호출하면 호스트의 암호화 상태가 다음과 같이 변경됩니다.

- 원래 호스트 암호화 상태가 incapable 또는 prepared이면 호스트 암호화 상태가 incapable로 변경됩니다.
- 원래 호스트 암호화 상태가 safe이면 호스트 암호화 상태가 pendingIncapable로 변경됩니다.
- 호스트 암호화 상태가 pendingIncapable이면 호스트 암호화 상태는 여전히 pendingIncapable입니다.

이 작업은 vCenter Server MOB(Managed Object Browser)를 사용하여 호스트 암호화 모드가 사용되지 않도록 설정하는 방법을 보여줍니다. API 사용에 대한 자세한 내용은 https://developer.vmware.com/apis/968/vsphere에서 "vSphere Web Services API" 설명서를 참조하십시오.

절차

1. vCenter Server에 관리자로 로그인합니다.
2. 호스트 암호화 모드가 사용되지 않도록 설정할 ESXi 호스트에서 모든 암호화된 가상 시스템을 등록 취소합니다.
3. vCenter Server에서 MOB에 액세스합니다.

   ```
   https://vcenter_server/mob
   ```

4. 호스트에서 `CryptoManagerHostDisable` 메서드를 호출합니다.
   a. 컨텐츠 이름에서 **content**를 클릭합니다.
   b. rootFolder에서 **group-D1(Datacenters)**을 클릭합니다.
   c. childEntity에서 적절한 데이터 센터를 클릭합니다.
   d. hostFolder에서 적절한 호스트를 클릭합니다.
   e. childEntity에서 적절한 클러스터를 클릭합니다.
   f. host에서 적절한 호스트를 클릭합니다.

g configManager에서 **configManager**를 클릭합니다.

h cryptoManager에서 **CryptoManagerHost-***number*를 클릭합니다.

i **CryptoManagerHostDisable**을 클릭합니다.

호스트 암호화 상태는 원래 암호화 상태에 따라 pendingIncapable 또는 incapable로 변경됩니다.

5 암호화 모드가 사용되지 않도록 설정할 다른 호스트에 대해 4단계를 반복합니다.

6 호스트를 재부팅합니다.

결과

호스트 암호화 모드가 사용되지 않도록 설정되면 호스트 암호화 모드가 다시 사용되도록 설정하지 않는 한 암호화 작업(예: 암호화된 가상 시스템 추가)을 수행할 수 없습니다.

참고 암호화 모드가 사용되지 않도록 설정한 ESXi 호스트를 재부팅한 후(호스트 암호화 상태가 원래 pendingIncapable이면) 호스트 암호화 상태는 여전히 pendingIncapable입니다. 호스트 암호화 모드가 다시 사용되도록 설정하려면 vCenter Server MOB에 다시 액세스하고 `ConfigureCryptoKey` API 메서드를 호출합니다. 호스트 암호화 모드가 다시 사용되도록 설정할 때 호스트 암호화 상태가 pendingIncapable이면 원래 호스트 키 ID를 사용합니다.

암호화된 가상 시스템 생성

KMS를 설정한 후에는 암호화된 가상 시스템을 생성할 수 있습니다.

이 작업에서는 vSphere Client를 사용하여 암호화된 가상 시스템을 생성하는 방법에 대해 설명합니다. vSphere Client는 가상 시스템 암호화 스토리지 정책을 기준으로 필터링하여 암호화된 가상 시스템의 생성을 용이하게 합니다.

참고 기존 가상 시스템을 암호화하는 것보다는 암호화된 가상 시스템을 생성하는 것이 더 빠르고 스토리지 리소스도 적게 사용합니다. 가능하면 가상 시스템을 생성하는 동안 암호화합니다.

사전 요구 사항

- KMS와의 신뢰 연결을 설정하고 기본 KMS를 선택합니다.
- 암호화 스토리지 정책을 생성하거나 번들로 제공되는 VM 암호화 정책 샘플을 사용합니다.
- 가상 시스템의 전원이 꺼졌는지 확인합니다.
- 필수 권한이 있는지 확인합니다.
  - **암호화 작업.새 항목 암호화**
  - 호스트 암호화 모드가 사용이 아니면 **암호화 작업.호스트 등록**도 필요합니다.

절차

1 vSphere Client를 사용하여 vCenter Server에 연결합니다.

2 ESXi 호스트 또는 클러스터 같이 가상 시스템의 올바른 상위 개체인 인벤토리의 개체를 선택합니다.

3 개체를 마우스 오른쪽 버튼으로 클릭하고 **새 가상 시스템**을 선택합니다.

4 지시에 따라 암호화된 가상 시스템을 생성합니다.

옵션	작업
생성 유형 선택	새 가상 시스템을 생성합니다.
이름 및 폴더 선택	가상 시스템의 고유한 이름과 대상 위치를 지정합니다.
계산 리소스 선택	암호화된 가상 시스템을 생성할 수 있는 권한이 있는 개체를 지정합니다. 암호화 작업의 사전 요구 사항 및 필요한 권한의 내용을 참조하십시오.
스토리지 선택	**이 가상 시스템 암호화** 확인란을 선택합니다. 암호화가 포함된 가상 시스템 스토리지 정책이 나타납니다. 가상 시스템 스토리지 정책(번들로 제공되는 샘플은 VM 암호화 정책)을 선택하고 호환되는 데이터스토어를 선택합니다.
호환성 선택	호환성을 선택합니다. 암호화된 가상 시스템은 호환성이 ESXi 6.5 이상인 호스트로만 마이그레이션할 수 있습니다.
게스트 운영 체제 선택	이후에 가상 시스템에 설치할 게스트 운영 체제를 선택합니다.
하드웨어 사용자 지정	예를 들면 디스크 크기 또는 CPU를 변경하여 하드웨어를 사용자 지정합니다. (선택 사항) **VM 옵션** 탭을 선택하고 **암호화**를 확장합니다. 암호화에서 제외할 디스크를 선택합니다. 디스크의 선택을 취소하면 VM 홈과 선택된 다른 디스크만 암호화됩니다. 추가하는 모든 새 하드 디스크가 암호화됩니다. 이후에 개별 하드 디스크에 대해 스토리지 정책을 변경할 수 있습니다.
완료 준비	정보를 검토하고 **마침**을 클릭합니다.

암호화된 가상 시스템 복제

암호화된 가상 시스템을 복제하는 경우 복제본이 동일한 키를 사용하여 암호화됩니다. 복제본의 키를 변경하려면 API를 사용하여 복제본의 이중 암호화를 수행합니다. "vSphere Web Services SDK 프로그래밍 가이드" 의 내용을 참조하십시오.

복제 중에 다음 작업을 수행할 수 있습니다.

- 암호화되지 않은 가상 시스템 또는 템플릿 가상 시스템에서 암호화된 가상 시스템을 생성합니다.
- 암호화된 가상 시스템 또는 템플릿 가상 시스템에서 암호 해독된 가상 시스템을 생성합니다.
- 소스 가상 시스템의 키와 다른 키를 사용하여 대상 가상 시스템을 이중 암호화합니다.

즉시 복제에서 소스 가상 시스템과 동일한 키를 공유한다는 주의 사항과 함께 암호화된 가상 시스템에서 즉시 복제 가상 시스템을 생성할 수 있습니다. 소스 또는 즉시 복제 가상 시스템 중 하나에서 키를 이중 암호화할 수 없습니다. "vSphere Web Services SDK 프로그래밍 가이드" 의 내용을 참조하십시오.

사전 요구 사항

- KMS와의 신뢰 연결을 설정하고 기본 KMS를 선택합니다.
- 암호화 스토리지 정책을 생성하거나 번들로 제공되는 VM 암호화 정책 샘플을 사용합니다.

- 필요한 권한:
  - **암호화 작업.복제**
  - **암호화 작업.암호화**
  - **암호화 작업.암호 해독**
  - **암호화 작업.이중 암호화**
  - 호스트 암호화 모드가 [사용]이 아니면 **암호화 작업.호스트 등록** 권한도 있어야 합니다.

절차

1 vSphere Client 인벤토리에서 가상 시스템을 찾습니다.

2 암호화된 시스템의 복제본을 생성하려면 가상 시스템을 마우스 오른쪽 버튼으로 클릭하고 **복제 > 가상 시스템으로 복제**를 선택한 후 표시되는 메시지를 따릅니다.

옵션	작업
이름 및 폴더 선택	복제본의 이름과 대상 위치를 지정합니다.
계산 리소스 선택	암호화된 가상 시스템을 생성할 수 있는 권한이 있는 개체를 지정합니다. 암호화 작업의 사전 요구 사항 및 필요한 권한의 내용을 참조하십시오.
스토리지 선택	**가상 디스크 형식 선택** 메뉴에서 항목을 선택하고 데이터스토어를 선택합니다. 복제 작업의 일부로 스토리지 정책을 변경할 수 있습니다. 예를 들어 암호화 정책 사용에서 비 암호화 정책으로 변경하면 디스크의 암호가 해독됩니다.
복제 옵션 선택	"vSphere 가상 시스템 관리" 설명서에 나와 있는 것처럼 복제 옵션을 선택합니다.
완료 준비	정보를 검토하고 **마침**을 클릭합니다.

3 (선택 사항) 복제된 가상 시스템의 키를 변경합니다.

복제된 가상 시스템은 기본적으로 상위 가상 시스템과 동일한 키를 사용하여 생성됩니다. 여러 가상 시스템이 동일한 키를 사용하는 일이 없도록 복제된 가상 시스템 키를 변경하는 것이 좋습니다.

a 얕은 또는 깊은 이중 암호화를 결정합니다.

다른 DEK 및 KEK를 사용하려면 복제된 가상 시스템의 깊은 이중 암호화를 수행합니다. 다른 KEK를 사용하려면 복제된 가상 시스템의 얕은 이중 암호화를 수행합니다. 깊은 이중 암호화를 수행하려면 가상 시스템의 전원을 꺼야 합니다. 가상 시스템의 전원이 켜져 있고 가상 시스템에 스냅샷이 있다면 얕은 이중 암호화 작업을 수행할 수 있습니다. 스냅샷이 있는 암호화된 가상 시스템의 얕은 이중 암호화는 단일 스냅샷 분기(디스크 체인)에서만 허용됩니다. 여러 개의 스냅샷 분기는 지원되지 않습니다. 새 KEK를 사용하여 체인에 있는 모든 링크를 업데이트하기 전에 얕은 이중 암호화가 실패하는 경우 이전 및 새 KEK가 있다면 암호화된 가상 시스템에 계속 액세스할 수 있습니다.

b API를 사용하여 복제본의 이중 암호화를 수행합니다. "vSphere Web Services SDK 프로그래밍 가이드" 의 내용을 참조하십시오.

기존 가상 시스템 또는 가상 디스크 암호화

스토리지 정책을 변경하여 기존 가상 시스템 또는 가상 디스크를 암호화할 수 있습니다. 암호화된 가상 시스템의 경우에만 가상 디스크를 암호화할 수 있습니다.

이 작업에서는 vSphere Client를 사용하여 기존 가상 시스템 또는 가상 디스크를 암호화하는 방법을 설명합니다.

 (vSphere Client에서 가상 시스템 암호화)

사전 요구 사항

- KMS와의 신뢰 연결을 설정하고 기본 KMS를 선택합니다.
- 암호화 스토리지 정책을 생성하거나 번들로 제공되는 VM 암호화 정책 샘플을 사용합니다.
- 가상 시스템의 전원이 꺼졌는지 확인합니다.
- 필수 권한이 있는지 확인합니다.
  - **암호화 작업.새 항목 암호화**
  - 호스트 암호화 모드가 사용이 아니면 **암호화 작업.호스트 등록**도 필요합니다.

절차

1 vSphere Client를 사용하여 vCenter Server에 연결합니다.

2 변경할 가상 시스템을 마우스 오른쪽 버튼으로 클릭하고 **VM 정책 > VM 스토리지 정책 편집**을 선택합니다.

가상 시스템 파일(VM 홈으로 표시)에 대한 스토리지 정책과 가상 디스크에 대한 스토리지 정책을 설정할 수 있습니다.

3 스토리지 정책을 선택합니다.

- VM 및 해당 하드 디스크를 암호화하려면 암호화 스토리지 정책을 선택하고 **확인**을 클릭합니다.
- 가상 디스크는 암호화하지 않고 VM만 암호화하려면 **디스크별 구성**을 설정한 후 VM 홈에 대해 암호화 스토리지 정책을 선택하고 가상 디스크에는 다른 스토리지 정책을 선택한 후 **확인**을 클릭합니다.

암호화되지 않은 VM의 가상 디스크는 암호화할 수 없습니다.

4 원할 경우 vSphere Client에서 **설정 편집** 메뉴를 사용하여 가상 시스템을 암호화하거나 가상 시스템과 디스크 모두를 암호화할 수 있습니다.

a 가상 시스템을 마우스 오른쪽 버튼으로 클릭하고 **설정 편집**을 선택합니다.

b **VM 옵션** 탭을 선택하고 **암호화**를 엽니다. 암호화 정책을 선택합니다. 모든 디스크의 선택을 취소하는 경우 VM 홈만 암호화됩니다.

c **확인**을 클릭합니다.

암호화된 가상 시스템 또는 가상 디스크 암호 해독

스토리지 정책을 변경하여 가상 시스템, 해당 디스크 또는 둘 모두의 암호를 해독할 수 있습니다.

이 작업에서는 vSphere Client를 사용하여 가상 시스템을 암호화하고 암호 해독하는 방법을 설명합니다.

모든 암호화된 가상 시스템에 암호화된 vMotion이 필요합니다. 가상 시스템 암호 해독 과정에서 암호화된 vMotion 설정이 유지됩니다. 이 설정을 변경하여 암호화된 vMotion이 더 이상 사용되지 않도록 하려면 설정을 명시적으로 변경합니다.

이 작업은 스토리지 정책을 사용하여 암호 해독을 수행하는 방법을 설명합니다. 또한 가상 디스크에 대해 **설정 편집** 메뉴를 사용하여 암호 해독을 수행할 수 있습니다.

사전 요구 사항

- 가상 시스템을 암호화해야 합니다.
- 가상 시스템의 전원을 끄거나 가상 시스템을 유지 보수 모드로 설정해야 합니다.
- 필요한 권한: **암호화 작업.암호 해독**

절차

1 vSphere Client를 사용하여 vCenter Server에 연결합니다.

2 변경할 가상 시스템을 마우스 오른쪽 버튼으로 클릭하고 **VM 정책 > VM 스토리지 정책 편집**을 선택합니다.

가상 시스템 파일(VM 홈으로 표시)에 대한 스토리지 정책과 가상 디스크에 대한 스토리지 정책을 설정할 수 있습니다.

3 스토리지 정책을 선택합니다.

- VM 및 해당 하드 디스크 암호를 해독하려면 **디스크별 구성**을 해제한 후 드롭다운 메뉴에서 스토리지 정책을 선택하고 **확인**을 클릭합니다.
- 가상 시스템 암호는 해독하지 않고 가상 디스크 암호만 해독하려면 **디스크별 구성**을 사용하도록 설정한 후 VM 홈에 대해 암호화 스토리지 정책을 선택하고 가상 디스크에는 다른 스토리지 정책을 선택한 후 **확인**을 클릭합니다.

가상 시스템의 암호를 해독하고 디스크를 암호화된 상태로 둘 수 없습니다.

4 원할 경우 vSphere Client를 사용하여 **설정 편집** 메뉴에서 가상 시스템 및 디스크 암호를 해독할 수 있습니다.

a 가상 시스템을 마우스 오른쪽 버튼으로 클릭하고 **설정 편집**을 선택합니다.

b **VM 옵션** 탭을 선택하고 **암호화**를 확장합니다.

c VM 및 해당 하드 디스크 암호를 해독하려면, **VM 암호화** 드롭다운 메뉴에서 **없음**을 선택합니다.

d 가상 시스템 암호는 해독하지 않고 가상 디스크 암호만 해독하려면 해당 디스크의 선택을 취소합니다.

e **확인**을 클릭합니다.

5 (선택 사항) [암호화된 vMotion] 설정을 변경할 수 있습니다.

a 가상 시스템을 마우스 오른쪽 버튼으로 클릭한 후 **설정 편집**을 클릭합니다.

b **VM 옵션**을 클릭하고 **암호화**를 엽니다.

c **암호화된 vMotion** 값을 설정합니다.

가상 디스크에 대한 암호화 정책 변경

vSphere Client에서 암호화된 가상 시스템을 생성하는 경우 가상 시스템 생성 과정에서 추가되는 가상 디스크 중 암호화할 디스크를 선택할 수 있습니다. **VM 스토리지 정책 편집** 옵션을 사용하여 암호화된 가상 디스크의 암호를 해독할 수 있습니다.

참고 암호화된 가상 시스템에 암호화되지 않은 가상 디스크가 있을 수 있습니다. 그러나 암호화되지 않은 가상 시스템에는 암호화된 가상 디스크가 있을 수 없습니다.

가상 디스크 암호화의 내용을 참조하십시오.

이 작업은 스토리지 정책을 사용하여 암호화 정책을 변경하는 방법을 설명합니다. 또한 **설정 편집** 메뉴를 사용하여 이러한 변경을 수행할 수도 있습니다.

사전 요구 사항

- **암호화 작업.암호화 정책 관리** 권한이 있어야 합니다.
- 가상 시스템의 전원이 꺼졌는지 확인합니다.

절차

1 vSphere Client를 사용하여 vCenter Server에 연결합니다.

2 가상 시스템을 마우스 오른쪽 버튼으로 클릭하고 **VM 정책 > VM 스토리지 정책 편집**을 선택합니다.

3 스토리지 정책을 변경합니다.

- VM 및 해당 하드 디스크에 대한 스토리지 정책을 변경하려면 암호화 스토리지 정책을 선택하고 **확인**을 클릭합니다.
- 가상 디스크는 암호화하지 않고 VM만 암호화하려면 **디스크별 구성**을 설정한 후 VM 홈에 대해 암호화 스토리지 정책을 선택하고 가상 디스크에는 다른 스토리지 정책을 선택한 후 **확인**을 클릭합니다.

암호화되지 않은 VM의 가상 디스크는 암호화할 수 없습니다.

4 원할 경우 **설정 편집** 메뉴에서 스토리지 정책을 변경할 수 있습니다.

a 가상 시스템을 마우스 오른쪽 버튼으로 클릭하고 **설정 편집**을 선택합니다.

b **가상 하드웨어** 탭을 선택하고 하드 디스크를 확장한 후 드롭다운 메뉴에서 암호화 정책을 선택합니다.

c **확인**을 클릭합니다.

없는 키 문제 해결

ESXi 호스트가 암호화된 가상 시스템 또는 암호화된 가상 디스크에 대해 vCenter Server에서 키(KEK)를 가져올 수 없으면 암호화된 VM이 잠깁니다. KMS 에서 키를 사용할 수 있도록 설정하면 잠겨 있는 암호화된 가상 시스템의 잠금을 해제할 수 있습니다.

표준 키 제공자를 사용하는 특정 상황에서 ESXi 호스트는 vCenter Server에서 암호화된 가상 디스크 또는 암호화된 가상 시스템의 KEK(키 암호화 키)를 가져올 수 없습니다. 이 경우 가상 시스템을 여전히 등록 취소하거나 다시 로드할 수 있습니다. 하지만 가상 시스템 전원 켜기와 같은 기타 가상 시스템 작업은 수행할 수 없습니다. 필요한 단계를 수행하여 KMS에서 필요한 키를 사용할 수 있도록 설정한 후에는 vSphere Client를 사용하여 잠겨 있는 암호화된 가상 시스템의 잠금을 해제할 수 있습니다.

가상 시스템 키를 사용할 수 없는 경우 vCenter Server 경보가 알려주고 가상 시스템의 상태가 유효하지 않은 것으로 표시됩니다. 가상 시스템의 전원을 켤 수 없습니다. 가상 시스템 키를 사용할 수 있지만 암호화된 디스크의 키를 사용할 수 없는 경우에는 가상 시스템 상태가 잘못된 것으로 표시되지 않습니다. 하지만 가상 시스템의 전원을 켤 수 없고 다음 오류가 발생합니다.

```
The disk [/path/to/the/disk.vmdk] is encrypted and a required key was not found.
```

참고 다음 절차에서는 가상 시스템이 잠길 수 있는 상황과 각 경우에 표시되는 경보와 이벤트 로그 및 권장 조치를 설명합니다.

절차

1 vCenter Server 시스템과 KMS 간 연결에 문제가 있는 경우 vCenter Server는 가상 시스템 경보를 생성합니다. 또한 이벤트 로그에 오류 메시지가 표시됩니다.

KMS에 대한 연결을 복원합니다. KMS와 키를 사용할 수 있게 되면 잠겨 있는 가상 시스템을 잠금 해제합니다. 잠긴 가상 시스템의 잠금 해제의 내용을 참조하십시오. 또한 연결을 복원한 후 호스트를 재부팅하고 가상 시스템을 다시 등록하여 잠금을 해제할 수도 있습니다.

KMS에 대한 연결이 손실된다고 해서 가상 시스템이 자동으로 잠기는 것은 아닙니다. 가상 시스템은 다음 조건이 충족되는 경우에만 잠김 상태로 전환됩니다.

- 키를 ESXi 호스트에서 사용할 수 없습니다.
- vCenter Server가 KMS에서 키를 검색할 수 없습니다.

재부팅할 때마다 ESXi 호스트가 vCenter Server에 연결할 수 있어야 합니다. vCenter Server는 KMS에서 해당 ID를 사용하여 키를 요청하고 ESXi가 사용할 수 있도록 합니다.

참고 vSphere 7.0 업데이트 2 이상에서는 ESXi 재부팅 시 암호화 키를 유지할 수 있습니다. 키 지속성 개요의 내용을 참조하십시오.

키 제공자에 대한 연결을 복원한 후에도 가상 시스템이 계속 잠겨 있는 경우 잠긴 가상 시스템의 잠금 해제의 내용을 참조하십시오.

2 연결이 복원되면 가상 시스템을 등록합니다. 오류가 발생하거나 작업이 성공했지만 가상 시스템이 잠긴 상태인 경우 vCenter Server 시스템에 대한 **암호화 작업.VM 등록** 권한이 있는지 확인합니다.

   키를 사용할 수 있는 경우 이 권한은 암호화된 가상 시스템의 전원을 켜는 데 필요하지 않습니다. 이 권한은 키를 검색해야 하는 경우 가상 시스템을 등록하는 데 필요합니다.

3 KMS에서 키를 더 이상 사용할 수 없으면 vCenter Server는 가상 시스템 경보를 생성합니다. 또한 이벤트 로그에 오류 메시지가 표시됩니다.

   KMS 관리자에게 요청하여 키를 복원하십시오. 인벤토리에서 제거되고 오랫동안 등록되지 않은 가상 시스템의 전원을 켜는 경우 키가 비활성 상태일 수 있습니다. 또한 ESXi 호스트를 재부팅했을 때 KMS를 사용할 수 없는 경우에도 발생합니다.

   a MOB(Managed Object Browser) 또는 vSphere API를 사용하여 키 ID를 검색합니다.

      `VirtualMachine.config.keyId.keyId`에서 `keyId`를 검색합니다.

   b KMS 관리자에게 해당 키 ID와 연결된 키를 다시 활성화하도록 요청합니다.

   c 키를 복원한 후 잠긴 가상 시스템의 잠금 해제 항목을 참조하십시오.

   KMS에서 키를 복원할 수 있는 경우 vCenter Server에서 다음 번에 필요할 때 이 키를 검색하여 ESXi 호스트에 푸시합니다.

4 KMS에 액세스할 수 있고 ESXi 호스트의 전원이 켜져 있지만 vCenter Server 시스템을 사용할 수 없는 경우 다음 단계에 따라 가상 시스템의 잠금을 해제합니다.

   a vCenter Server 시스템을 복원하거나 다른 vCenter Server 시스템을 설정한 후 KMS와 신뢰를 설정합니다.

      동일한 키 제공자 이름을 사용해야 하지만 KMS IP 주소는 다를 수 있습니다.

   b 잠긴 가상 시스템을 모두 재등록합니다.

      새 vCenter Server 인스턴스가 KMS에서 키를 검색하고 가상 시스템의 잠금이 해제됩니다.

5 ESXi 호스트에서만 키가 누락된 경우 vCenter Server에서 가상 시스템 경보가 생성되고 이벤트 로그에 다음 메시지가 나타납니다.

   호스트에 키가 누락되어 가상 시스템이 잠겼습니다.

   vCenter Server 시스템은 키 제공자에서 누락된 키를 검색할 수 있습니다. 키의 수동 복구는 필요 없습니다. 잠긴 가상 시스템의 잠금 해제의 내용을 참조하십시오.

잠긴 가상 시스템의 잠금 해제

암호화된 가상 시스템이 잠금 상태가 되면 이를 알리는 vCenter Server 경보 메시지가 표시됩니다. 필요한 단계를 수행하여 필요한 키를 KMS에서 사용할 수 있도록 설정한 후에 vSphere Client(HTML5 기반 클라이언트)를 사용하여 잠겨 있는 암호화된 가상 시스템을 잠금 해제할 수 있습니다.

사전 요구 사항

- **암호화 작업 .RegisterVM**에서 필요한 권한이 있는지 확인합니다.

- 호스트 암호화를 사용하도록 설정하는 것과 같은 선택적 작업에는 다른 권한이 필요할 수 있습니다.
- 잠긴 가상 시스템을 잠금 해제하기 전에 잠금 문제의 원인을 파악하고 수동으로 문제를 해결해 봅니다. 없는 키 문제 해결의 내용을 참조하십시오.

절차

1 vSphere Client를 사용하여 vCenter Server에 연결합니다.

2 가상 시스템의 **요약** 탭으로 이동합니다.

가상 시스템이 잠겨 있는 경우 가상 시스템 잠김 경보가 표시됩니다.

3 경보를 확인하거나 경보를 녹색으로 재설정하되 지금 가상 시스템을 잠금 해제하지는 마십시오.

확인 또는 **녹색으로 재설정**을 클릭하면 경보가 사라지지만 가상 시스템은 잠금을 해제할 때까지 계속 잠긴 상태로 유지됩니다.

4 가상 시스템의 **모니터** 탭으로 이동하여 **이벤트**를 클릭하고 가상 시스템이 잠긴 이유에 대한 자세한 정보를 확인합니다.

5 가상 시스템을 잠금 해제하기 전에 제안된 문제 해결 조치를 수행합니다.

6 가상 시스템의 **요약** 탭으로 이동한 다음 가상 시스템 콘솔 아래에 있는 **VM 잠금 해제**를 클릭합니다.

암호화 키 데이터가 호스트에 전송되었다는 주의 메시지가 나타납니다.

7 **예**를 클릭합니다.

ESXi 호스트 암호화 모드 문제 해결

특정 상황에서 ESXi 호스트의 암호화 모드가 사용되지 않도록 설정될 수 있습니다.

ESXi 호스트에 암호화된 가상 시스템이 포함된 경우 호스트 암호화 모드가 사용되도록 설정되어야 합니다. 호스트에서 호스트 키가 누락되거나 키 제공자를 사용할 수 없는 것으로 감지될 경우 암호화 모드가 사용되도록 설정되지 않을 수 있습니다. 호스트 암호화 모드를 사용하도록 설정할 수 없는 경우 vCenter Server에서 경보가 생성됩니다.

절차

1 vCenter Server 시스템과 키 제공자 간의 연결에 문제가 있는 경우 경보가 생성되고 이벤트 로그에 오류 메시지가 나타납니다.

해당 암호화 키가 포함된 키 제공자에 대한 연결을 복원해야 합니다.

2 키가 누락된 경우 경보가 생성되고 이벤트 로그에 오류 메시지가 나타납니다.

키 제공자에 키가 있는지 확인해야 합니다. 백업에서 복원하는 방법에 대한 자세한 내용은 키 관리 벤더의 설명서를 참조하십시오.

다음에 수행할 작업

키 제공자에 대한 연결을 복원하거나 수동으로 키 제공자에 키를 복구한 후에도 호스트의 암호화 모드가 계속 사용되지 않도록 설정되어 있는 경우 호스트 암호화 모드를 다시 사용하도록 설정합니다. ESXi 호스트 암호화 모드를 다시 사용하도록 설정의 내용을 참조하십시오.

ESXi 호스트 암호화 모드를 다시 사용하도록 설정

vSphere 6.7부터는 ESXi 호스트의 암호화 모드가 사용되지 않도록 설정되면 이를 알리는 vCenter Server 경보가 표시됩니다. 호스트 암호화 모드가 사용되지 않도록 설정되었다면 다시 사용하도록 설정할 수 있습니다.

사전 요구 사항

- **암호화 작업.호스트 등록**에서 필요한 권한이 있는지 확인합니다.
- 암호화 모드를 다시 사용하도록 설정하기 전에 문제의 원인을 파악하고 수동으로 문제를 해결해 봅니다.

절차

1. vSphere Client를 사용하여 vCenter Server에 연결합니다.
2. ESXi 호스트의 **요약** 탭으로 이동합니다.

   암호화 모드가 사용되지 않도록 설정되면 호스트에 암호화 모드를 사용하도록 설정해야 한다는 경보가 표시됩니다.
3. 경보를 확인하거나 경보를 녹색으로 재설정하되 지금 호스트 암호화 모드를 다시 설정하지는 마십시오.

   확인 또는 **녹색으로 재설정**을 클릭하면 경보가 사라지지만 호스트의 암호화 모드는 다시 사용하도록 설정될 때까지 사용되지 않습니다.
4. ESXi 호스트의 **모니터** 탭으로 이동하여 **이벤트**를 클릭하고 암호화 모드가 사용되지 않도록 설정된 이유에 대한 자세한 정보를 확인합니다.

   암호화 모드를 다시 사용하도록 설정하기 전에 제안된 문제 해결 조치를 수행합니다.
5. **요약** 탭에서 **호스트 암호화 모드 사용**을 클릭하여 호스트 암호화를 다시 사용하도록 설정합니다.

   암호화 키 데이터가 호스트에 전송되었다는 주의 메시지가 나타납니다.
6. **예**를 클릭합니다.

키 관리 서버 인증서 만료 임계값 설정

vCenter Server는 기본적으로 KMS(키 관리 서버) 인증서가 만료되기 30일 전에 알려줍니다. 이 기본값은 변경할 수 있습니다.

KMS 인증서에는 만료 날짜가 있습니다. 만료 날짜의 임계값에 도달하면 경보가 표시됩니다.

vCenter Server 및 키 제공자는 서버와 클라이언트라는 두 가지 유형의 인증서를 교환합니다. vCenter Server 시스템의 VECS(VMware Endpoint Certificate Store)는 키 제공자당 클라이언트 인증서 하나와 서버 인증서를 저장합니다. 인증서 유형이 두 가지이기 때문에 인증서 유형마다 두 가지 경보(클라이언트용 하나, 서버용 하나)가 있습니다.

절차

1 vSphere Client를 사용하여 vCenter Server 시스템에 로그인합니다.

2 개체 계층에서 vCenter Server 시스템을 선택합니다.

3 **구성**을 클릭합니다.

4 **설정**에서 **고급 설정**을 클릭하고 **설정 편집**을 클릭합니다.

5 **필터** 아이콘을 클릭하고 `vpxd.kmscert.threshold`를 입력하거나 구성 매개 변수 자체로 스크롤합니다.

6 일 단위로 값을 입력하고 **저장**을 클릭합니다.

vSphere 가상 시스템 암호화 및 코어 덤프

환경에서 vSphere 가상 시스템 암호화를 사용하는 경우 ESXi 호스트에 오류가 발생하면 고객 데이터를 보호하도록 결과 코어 덤프가 암호화됩니다. vm-support 패키지에 포함되는 코어 덤프도 암호화됩니다.

참고 코어 덤프에는 중요한 정보가 포함될 수 있습니다. 코어 덤프를 처리할 때는 조직의 데이터 보호 및 개인 정보 보호 정책을 따르십시오.

ESXi 호스트의 코어 덤프

ESXi 호스트, 사용자 월드 또는 가상 시스템이 실패할 경우 코어 덤프가 생성되고 호스트가 재부팅됩니다. ESXi 호스트에 암호화 모드가 사용되도록 설정된 경우 ESXi 키 캐시에 있는 키를 사용하여 코어 덤프가 암호화됩니다. 이 키는 KMS에서 가져옵니다. 배경 정보는 vSphere 가상 시스템 암호화를 통해 환경을 보호하는 방법 항목을 참조하십시오.

ESXi 호스트가 암호적으로 "안전한" 상태이면 코어 덤프가 생성되고 이벤트가 생성됩니다. 이 이벤트는 월드 이름, 발생 시간, 코어 덤프를 암호화하는 데 사용된 키의 keyID, 코어 덤프 파일 이름과 같은 정보와 함께 코어 덤프가 발생했음을 나타냅니다. vCenter Server의 **작업 및 이벤트**에서 이벤트 뷰어를 통해 이벤트를 볼 수 있습니다.

다음 표에는 vSphere 릴리스별로 각 코어 덤프 유형에 사용되는 암호화 키가 정리되어 있습니다.

표 10-1. 코어 덤프 암호화 키

코어 덤프 유형	암호화 키(ESXi 6.5)	암호화 키(ESXi 6.7 이상)
ESXi 커널	호스트 키	호스트 키
사용자 월드(hostd)	호스트 키	호스트 키
암호화된 VM(가상 시스템)	호스트 키	가상 시스템 키

ESXi 호스트 재부팅 후 수행할 수 있는 작업은 몇 가지 요인에 따라 달라집니다.

- 대부분의 경우 vCenter Server는 KMS에서 호스트에 대한 키를 검색하고, 재부팅 후 ESXi 호스트에 키를 푸시합니다. 작업이 성공하면 vm-support 패키지를 생성하고 코어 덤프의 암호를 해독하거나 다시 암호화할 수 있습니다. 암호화된 코어 덤프 암호 해독 또는 다시 암호화의 내용을 참조하십시오.
- vCenter Server에서 ESXi 호스트에 연결할 수 없는 경우 KMS에서 키를 검색할 수 있습니다. 없는 키 문제 해결의 내용을 참조하십시오.
- 호스트에서 사용자 지정 키를 사용했고 해당 키가 vCenter Server에서 호스트에 푸시한 키와 다를 경우 코어 덤프를 조작할 수 없습니다. 사용자 지정 키를 사용하지 않도록 합니다.

코어 덤프 및 vm-support 패키지

심각한 오류로 인해 VMware 기술 지원에 문의할 경우 지원 담당자는 대개 vm-support 패키지를 생성하도록 요청합니다. 이 패키지에는 로그 파일과 코어 덤프를 비롯한 기타 정보가 포함되어 있습니다. 지원 담당자가 로그 파일과 기타 정보를 확인하고도 문제를 해결할 수 없는 경우 코어 덤프의 암호를 해독하고 관련 정보를 제공하도록 요청할 수 있습니다. 키와 같은 중요한 정보를 보호하려면 조직의 보안 및 개인 정보 보호 정책을 따르십시오. 암호화를 사용하는 ESXi 호스트에 대해 vm-support 패키지 수집의 내용을 참조하십시오.

vCenter Server 시스템의 코어 덤프

vCenter Server 시스템의 코어 덤프는 암호화되어 있지 않습니다. vCenter Server에는 이미 잠재적으로 중요한 정보가 포함되어 있습니다. 최소한 vCenter Server가 보호되는지 확인합니다. 장 4 vCenter Server 시스템 보안의 내용을 참조하십시오. vCenter Server 시스템에 대한 코어 덤프를 해제하는 것을 고려할 수도 있습니다. 로그 파일의 기타 정보를 통해 문제를 확인할 수도 있습니다.

암호화를 사용하는 ESXi 호스트에 대해 vm-support 패키지 수집

ESXi 호스트에 대해 호스트 암호화 모드를 사용하도록 설정되어 있으면 `vm-support` 패키지의 모든 코어 덤프가 암호화됩니다. vSphere Client에서 패키지를 수집할 수 있으며, 나중에 코어 덤프를 암호 해독하려는 경우에는 암호를 지정할 수 있습니다.

`vm-support` 패키지에는 로그 파일, 코어 덤프 파일 등이 포함되어 있습니다.

사전 요구 사항

ESXi 호스트에 대해 호스트 암호화 모드가 사용하도록 설정되었음을 지원 담당자에게 알립니다. 코어 덤프를 암호 해독하고 관련 정보를 추출하도록 지원 담당자가 요청할 수 있습니다.

참고 코어 덤프에는 중요한 정보가 포함될 수 있습니다. 조직의 보안 및 개인 정보 보호 정책을 따라 호스트 키와 같은 중요한 정보를 보호하십시오.

절차

1 vSphere Client를 사용하여 vCenter Server 시스템에 로그인합니다.

2 **호스트 및 클러스터**를 클릭하고 ESXi 호스트를 마우스 오른쪽 버튼으로 클릭합니다.

3 **시스템 로그 내보내기**를 선택합니다.

4 대화상자에서 **암호화된 코어 덤프에 대한 암호**를 선택하고 암호를 지정하고 확인합니다.

5 다른 옵션의 경우 기본값을 그대로 사용하거나 VMware 기술 지원에서 요청한 대로 변경한 후 **로그 내보내기**를 클릭합니다.

6 파일의 위치를 지정합니다.

7 지원 담당자가 `vm-support` 패키지의 코어 덤프를 암호 해독하라고 요청한 경우, 임의의 ESXi 호스트에 로그인하여 다음 단계를 수행합니다.

   a ESXi에 로그인하여 `vm-support` 패키지가 있는 디렉토리에 연결합니다.

   파일 이름은 esx.date_and_time.tgz와 같은 패턴입니다.

   b 패키지, 압축 해제된 패키지 및 다시 압축된 패키지를 저장하거나 패키지를 이동할 수 있을 정도로 디렉토리의 공간이 충분한지 확인합니다.

   c 패키지를 로컬 디렉토리에 추출합니다.

   ```
   vm-support -x *.tgz .
   ```

   추출 후 생성되는 파일 계층에는 ESXi 호스트의 코어 덤프 파일이 `/var/core`에 포함될 수 있으며, 가상 시스템의 코어 덤프 파일이 여러 개 포함될 수 있습니다.

   d 암호화된 각 코어 덤프 파일을 개별적으로 암호 해독합니다.

   ```
   crypto-util envelope extract --offset 4096 --keyfile vm-support-incident-key-file
   --password encryptedZdump decryptedZdump
   ```

   *vm-support-incident-key-file*은 디렉토리의 최상위 수준에 있는 인시던트 키 파일입니다.

   *encryptedZdump*는 암호화된 코어 덤프 파일의 이름입니다.

   *decryptedZdump*는 명령에서 생성되는 파일의 이름입니다. 이름을 *encryptedZdump* 이름과 비슷하게 지정합니다.

   e `vm-support` 패키지를 생성할 때 지정한 암호를 제공합니다.

   f 암호화된 코어 덤프를 제거하거나, 패키지를 다시 압축합니다.

   ```
   vm-support --reconstruct
   ```

8 기밀 정보가 포함된 모든 파일을 제거합니다.

암호화된 코어 덤프 암호 해독 또는 다시 암호화

`crypto-util` CLI를 사용하면 ESXi 호스트에서 암호화된 코어 덤프를 암호 해독하고 다시 암호화할 수 있습니다.

vm-support 패키지에 있는 코어 덤프를 직접 암호 해독하고 검사할 수 있습니다. 코어 덤프에는 중요한 정보가 포함될 수 있습니다. 조직의 보안 및 개인 정보 보호 정책을 따라 키와 같은 중요한 정보를 보호하십시오.

코어 덤프를 다시 암호화하는 기능 및 `crypto-util`의 다른 기능에 대한 자세한 내용은 명령줄 도움말을 참조하십시오.

참고 `crypto-util`은 고급 사용자를 위한 기능입니다.

사전 요구 사항

코어 덤프를 생성한 ESXi 호스트에서 코어 덤프를 암호화하는 데 사용된 키를 사용할 수 있어야 합니다.

절차

1 코어 덤프가 생성된 ESXi 호스트에 직접 로그인합니다.

ESXi 호스트가 잠금 모드에 있거나 SSH 액세스가 사용되지 않도록 설정되어 있는 경우에는 먼저 액세스가 가능하도록 설정해야 합니다.

2 코어 덤프가 암호화되었는지 여부를 확인합니다.

옵션	설명
코어 덤프 모니터링	`crypto-util envelope describe vmmcores.ve`
zdump 파일	`crypto-util envelope describe --offset 4096 zdumpFile`

3 코어 덤프 유형에 따라 코어 덤프를 암호 해독합니다.

옵션	설명
코어 덤프 모니터링	`crypto-util envelope extract vmmcores.ve vmmcores`
zdump 파일	`crypto-util envelope extract --offset 4096 zdumpEncrypted zdumpUnencrypted`

ESXi 호스트에서 키 지속성 사용 및 사용 안 함

ESXi 호스트에서 키 지속성을 사용하도록 설정해야 합니다 키 지속성은 기본적으로 사용되도록 설정되어 있지 않습니다.

키 지속성에 대한 개념 정보는 키 지속성 개요의 내용을 참조하십시오.

사전 요구 사항

키 지속성 사용 요구 사항:

- ESXi 7.0 업데이트 2 이상

- ESXi TPM 2.0과 함께 설치된 호스트
- ESXCLI 명령 집합에 대한 액세스 권한. ESXCLI 명령을 원격으로 실행하거나 ESXi Shell에서 실행할 수 있습니다.

참고 vSphere Native Key Provider를 사용하는 경우 키 지속성이 필요하지 않습니다. vSphere Native Key Provider는 키 서버에 액세스할 필요 없이 바로 실행되도록 설계되었습니다.

추가적인 보안을 위해 TPM은 ESXi 호스트 부팅 중에 변조를 방지하기 위해 봉인 정책을 사용할 수도 있습니다. TPM 봉인 정책 개요의 내용을 참조하십시오.

절차

1 SSH 또는 다른 원격 콘솔 연결을 사용하여 ESXi 호스트에서 세션을 시작합니다.

2 root로 로그인합니다.

3 키 지속성을 사용하거나 사용하지 않도록 설정합니다.

a 키 지속성을 사용하도록 설정하려면 다음을 수행합니다.

```
esxcli system security keypersistence enable
```

b 키 지속성을 사용하지 않도록 설정하려면 다음을 수행합니다.

```
esxcli system security keypersistence disable --remove-all-stored-keys
```

vSphere Client를 사용하여 암호화된 가상 시스템 키 재생성

vSphere Client를 사용하여 암호화된 가상 시스템의 얕은 수준 키 재생성(shallow rekey)을 수행할 수 있습니다. 비즈니스 또는 규정 준수를 위해 암호화된 가상 시스템의 키 재생성을 수행할 수 있습니다.

얕은 수준의 키 재생성(shallow rekey) 또는 키 재생성(얕은 이중 암호화라고도 함)을 사용하면 암호화된 가상 시스템에서 새롭고 다른 KEK(키 암호화 키)를 사용할 수 있습니다. 가상 시스템의 전원이 켜져 있는 동안 키 재생성 작업을 수행할 수 있습니다. 가상 시스템에 스냅샷이 있는 경우 키 재생성을 수행할 수도 있습니다. 스냅샷이 있는 암호화된 가상 시스템의 키 재생성은 단일 스냅샷 분기(디스크 체인)에서만 허용됩니다. 여러 개의 스냅샷 분기는 지원되지 않습니다. 새 KEK를 사용하여 체인에 있는 모든 링크를 업데이트하기 전에 키 재생성이 실패하는 경우 이전 및 새 KEK가 있다면 암호화된 가상 시스템에 계속 액세스할 수 있습니다.

사전 요구 사항

필요한 권한: **암호화 작업.키 서버 관리**

절차

1 vSphere Client를 사용하여 vCenter Server 시스템에 로그인합니다.

2 인벤토리 목록을 찾아서 암호화된 가상 시스템을 선택합니다.

3 암호화된 가상 시스템을 마우스 오른쪽 버튼으로 클릭하고 **VM 정책**을 선택합니다.

4 **다시 암호화**를 선택합니다.

5 **예**를 클릭합니다.

암호화된 가상 시스템의 키가 새 KEK로 재생성됩니다.

참고 키 재생성이 실패하면 이벤트 하위 시스템이 다음 이벤트를 게시합니다.

```
com.vmware.vc.vm.crypto.RekeyFail
```

신뢰할 수 있는 가상 플랫폼 모듈로 가상 시스템 보호

11

vTPM(신뢰할 수 있는 가상 플랫폼 모듈) 기능을 사용하면 가상 시스템에 TPM 2.0 가상 암호화 프로세서를 추가할 수 있습니다.

vTPM은 물리적 TPM(신뢰할 수 있는 플랫폼 모듈) 2.0 칩의 소프트웨어 기반 표현입니다. vTPM은 기타 가상 디바이스로 작동합니다. 가상 CPU, 메모리, 디스크 컨트롤러 또는 네트워크 컨트롤러를 추가하는 것과 동일한 방식으로 vTPM을 가상 시스템에 추가할 수 있습니다. vTPM에는 하드웨어 TPM(신뢰할 수 있는 플랫폼 모듈) 칩이 필요하지 않습니다.

본 장은 다음 항목을 포함합니다.

- 신뢰할 수 있는 가상 플랫폼 모듈 개요
- 신뢰할 수 있는 가상 플랫폼 모듈을 사용하여 가상 시스템 생성
- 기존 가상 시스템에 신뢰할 수 있는 가상 플랫폼 모듈을 사용하도록 설정
- 가상 시스템에서 신뢰할 수 있는 가상 플랫폼 모듈 제거
- 신뢰할 수 있는 가상 플랫폼 모듈이 사용되도록 설정된 가상 시스템 식별
- 신뢰할 수 있는 가상 플랫폼 모듈 디바이스 인증서 보기
- 신뢰할 수 있는 가상 플랫폼 모듈 디바이스 인증서 내보내기 및 교체

신뢰할 수 있는 가상 플랫폼 모듈 개요

vTPM(가상의 신뢰할 수 있는 플랫폼 모듈)은 물리적 TPM(신뢰할 수 있는 플랫폼 모듈) 2.0 칩의 소프트웨어 기반 표현입니다. vTPM은 기타 가상 디바이스로 작동합니다.

vTPM이란?

vTPM은 임의 번호 생성, 증명, 키 생성 등과 같은 하드웨어 기반의 보안 관련 기능을 제공합니다. 가상 시스템에 vTPM이 추가되면 게스트 운영 체제가 개인 키를 생성하고 저장할 수 있습니다. 이러한 키는 게스트 운영 체제에 노출되지 않습니다. 따라서 가상 시스템의 공격 표면이 감소합니다. 일반적으로 게스트 운영 체제가 손상되면 암호가 손상되지만 vTPM을 사용하도록 설정하면 이 위험이 크게 줄어듭니다. 이러한 키는 게스트 운영 체제에서 암호화 또는 서명 용도로만 사용할 수 있습니다. vTPM이 연결되어 있으면 클라이언트가 가상 시스템의 ID를 원격으로 검증하고 실행 중인 소프트웨어를 확인할 수 있습니다.

새 가상 시스템 또는 기존 가상 시스템에 vTPM을 추가할 수 있습니다. vTPM은 가상 시스템 암호화를 사용하여 중요한 TPM 데이터를 보호합니다. vTPM을 구성할 때 가상 시스템 파일은 암호화되지만 디스크는 암호화되지 않습니다. 가상 시스템 및 해당 디스크에 대해 명시적으로 암호화를 추가하도록 선택할 수 있습니다.

vTPM을 사용하는 가상 시스템을 백업할 때 백업에는 `*.nvram` 파일을 포함한 모든 가상 시스템 데이터가 포함되어야 합니다. 백업에 `*.nvram` 파일이 포함되지 않은 경우 vTPM을 사용하는 가상 시스템을 복원할 수 없습니다. 또한 vTPM이 사용되도록 설정된 가상 시스템의 VM 홈 파일이 암호화되어 있기 때문에 복원 시 암호화 키를 사용할 수 있는지 확인합니다.

vTPM을 사용하기 위해 ESXi 호스트에 물리적 TPM(신뢰할 수 있는 플랫폼 모듈) 2.0 칩이 있을 필요가 없습니다. 하지만 호스트 증명을 수행하려는 경우 TPM 2.0 물리적 칩과 같은 외부 엔티티가 필요합니다. 신뢰할 수 있는 플랫폼 모듈을 통한 ESXi 호스트 보안의 내용을 참조하십시오.

참고 기본적으로 vTPM이 사용되도록 설정된 가상 시스템에 연결된 스토리지 정책이 없습니다. 가상 시스템 파일(VM 홈)만 암호화됩니다. 원할 경우 가상 시스템 및 해당 디스크에 대해 명시적으로 암호화를 추가하도록 선택할 수 있지만 가상 시스템 파일은 이미 암호화되어 있습니다.

vTPM에 대한 vSphere 요구 사항

vTPM을 사용하려면 vSphere 환경이 다음과 같은 요구 사항을 충족해야 합니다.

- 가상 시스템 요구 사항:
  - EFI 펌웨어
  - 하드웨어 버전 14 이상
- 구성 요소 요구 사항:
  - Windows 가상 시스템의 경우 vCenter Server 6.7 이상, Linux 가상 시스템의 경우 vCenter Server 7.0 업데이트 2 이상.
  - 가상 시스템 암호화(가상 시스템 홈 파일 암호화)
  - vCenter Server에 대해 구성된 키 제공자. vSphere 키 제공자 비교의 내용을 참조하십시오.
- 게스트 운영 체제 지원:
  - Linux
  - Windows Server 2008 이상
  - Windows 7 이상

하드웨어 TPM과 가상 TPM의 차이점

하드웨어 TPM(신뢰할 수 있는 플랫폼 모듈)은 자격 증명 또는 키의 안전한 저장을 위해 사용합니다. vTPM은 TPM과 동일한 기능을 수행하지만 소프트웨어 내에서 암호화 보조 프로세서 기능을 수행합니다. vTPM은 가상 시스템 암호화를 사용하여 암호화된 `.nvram` 파일을 보안 스토리지로 사용합니다.

하드웨어 TPM에는 EK(승인 키)라고 하는 미리 로드된 키가 포함됩니다. EK에는 개인 키와 공용 키가 있습니다. EK는 TPM에 고유한 ID를 제공합니다. vTPM의 경우 이 키는 VMCA(VMware Certificate Authority) 또는 타사 CA(인증 기관)에서 제공됩니다. vTPM에 키가 사용되는 경우 일반적으로 키가 변경되지 않습니다. 키를 변경할 경우 vTPM에 저장된 중요 정보가 무효화되기 때문입니다. vTPM은 타사 CA에 다시 연결되지 않습니다.

신뢰할 수 있는 가상 플랫폼 모듈을 사용하여 가상 시스템 생성

가상 시스템을 생성할 때 vTPM(신뢰할 수 있는 가상 플랫폼 모듈)을 추가하여 게스트 운영 체제에 향상된 보안을 제공할 수 있습니다. vTPM을 추가하려면 먼저 키 제공자를 생성해야 합니다.

VMware 가상 TPM은 TPM 2.0과 호환되며 호스팅하는 게스트 운영 체제 및 가상 시스템에서 사용되는 TPM 지원 가상 칩을 생성합니다.

사전 요구 사항

- vSphere 환경이 키 제공자를 사용하여 구성되었는지 확인합니다. 자세한 내용은 다음을 참조하십시오.
  - vSphere 신뢰 기관 구성
  - 장 7 표준 키 제공자 구성 및 관리
  - 장 8 vSphere Native Key Provider 구성 및 관리
- 사용하는 게스트 운영 체제는 Windows Server 2008 이상, Windows 7이상 또는 Linux일 수 있습니다.
- 환경에서 실행 중인 ESXi 호스트는 ESXi 6.7 이상(Windows 게스트 운영 체제) 또는 7.0 업데이트 2(Linux 게스트 운영 체제)여야 합니다.
- 가상 시스템에 EFI 펌웨어를 사용해야 합니다.
- 필수 권한이 있는지 확인합니다.
  - **암호화 작업.복제**
  - **암호화 작업.암호화**
  - **암호화 작업.새 항목 암호화**
  - **암호화 작업.마이그레이션**
  - **암호화 작업.VM 등록**

절차

1 vSphere Client를 사용하여 vCenter Server에 연결합니다.

2 ESXi 호스트 또는 클러스터 같이 가상 시스템의 올바른 상위 개체인 인벤토리의 개체를 선택합니다.

3 개체를 마우스 오른쪽 버튼으로 클릭하고 **새 가상 시스템**을 선택한 다음 프롬프트에 따라 가상 시스템을 생성합니다.

옵션	작업
생성 유형 선택	새 가상 시스템을 생성합니다.
이름 및 폴더 선택	이름 및 대상 위치를 지정합니다.
계산 리소스 선택	가상 시스템을 생성할 권한이 있는 개체를 지정합니다. 암호화 작업의 사전 요구 사항 및 필요한 권한의 내용을 참조하십시오.
스토리지 선택	호환되는 데이터스토어를 선택합니다.
호환성 선택	Windows 게스트 운영 체제의 경우 **ESXi 6.7 이상**을 선택하고 Linux 게스트 운영 체제의 경우 **ESXi 7.0 U2** 이상을 선택해야 합니다.
게스트 운영 체제 선택	게스트 운영 체제로 사용할 Windows 또는 Linux를 선택합니다.
하드웨어 사용자 지정	**새 디바이스 추가**를 클릭하고 **신뢰할 수 있는 플랫폼 모듈**을 선택합니다. 예를 들면 디스크 크기 또는 CPU를 변경하여 하드웨어를 추가로 사용자 지정할 수 있습니다.
완료 준비	정보를 검토하고 **마침**을 클릭합니다.

결과

vTPM 지원 가상 시스템이 지정된 대로 인벤토리에 나타납니다.

기존 가상 시스템에 신뢰할 수 있는 가상 플랫폼 모듈을 사용하도록 설정

기존 가상 시스템에 vTPM(신뢰할 수 있는 가상 플랫폼 모듈)을 추가하여 게스트 운영 체제에 향상된 보안을 제공할 수 있습니다. vTPM을 추가하려면 먼저 키 제공자를 생성해야 합니다.

VMware 가상 TPM은 TPM 2.0과 호환되며 호스팅하는 게스트 운영 체제 및 가상 시스템에서 사용되는 TPM 지원 가상 칩을 생성합니다.

사전 요구 사항

- vSphere 환경이 키 제공자에 대해 구성되었는지 확인합니다. 자세한 내용은 다음을 참조하십시오.
  - vSphere 신뢰 기관 구성
  - 장 7 표준 키 제공자 구성 및 관리
  - 장 8 vSphere Native Key Provider 구성 및 관리
- 사용하는 게스트 운영 체제는 Windows Server 2008 이상, Windows 7이상 또는 Linux일 수 있습니다.
- 가상 시스템이 꺼져 있는지 확인합니다.
- 환경에서 실행 중인 ESXi 호스트는 ESXi 6.7 이상(Windows 게스트 운영 체제) 또는 7.0 업데이트 2(Linux 게스트 운영 체제)여야 합니다.

- 가상 시스템에 EFI 펌웨어를 사용해야 합니다.
- 필수 권한이 있는지 확인합니다.
  - **암호화 작업.복제**
  - **암호화 작업.암호화**
  - **암호화 작업.새 항목 암호화**
  - **암호화 작업.마이그레이션**
  - **암호화 작업.VM 등록**

절차

1 vSphere Client를 사용하여 vCenter Server에 연결합니다.

2 인벤토리에서 수정할 가상 시스템을 마우스 오른쪽 버튼으로 클릭하고 **설정 편집**을 선택합니다.

3 **설정 편집** 대화 상자에서 **새 디바이스 추가**를 클릭하고 **신뢰할 수 있는 플랫폼 모듈**을 선택합니다.

4 **확인**을 클릭합니다.

이제 가상 시스템 **요약** 탭의 **VM 하드웨어** 창에 신뢰할 수 있는 가상 플랫폼 모듈이 포함됩니다.

가상 시스템에서 신뢰할 수 있는 가상 플랫폼 모듈 제거

가상 시스템에서 vTPM(신뢰할 수 있는 가상 플랫폼 모듈) 보안을 제거할 수 있습니다.

vTPM 디바이스를 제거하면 가상 시스템의 암호화된 정보를 모두 복구할 수 없게 됩니다. 가상 시스템에서 vTPM을 제거하기 전에 BitLocker와 같은 vTPM 디바이스를 사용하는 게스트 운영 체제에서 모든 애플리케이션을 사용하지 않도록 설정합니다. 이렇게 하지 않으면 가상 시스템이 부팅되지 않을 수 있습니다. 또한 스냅샷이 포함된 가상 시스템에서 vTPM을 제거할 수 없습니다.

사전 요구 사항

- 가상 시스템의 전원이 꺼졌는지 확인합니다.
- 필수 **암호화 작업.암호 해독** 권한이 있는지 확인합니다.

절차

1 vSphere Client를 사용하여 vCenter Server에 연결합니다.

2 인벤토리에서 수정할 가상 시스템을 마우스 오른쪽 버튼으로 클릭하고 **설정 편집**을 선택합니다.

3 **설정 편집** 대화상자의 **가상 하드웨어** 탭에서 신뢰할 수 있는 플랫폼 모듈 항목을 찾습니다.

4 포인터를 디바이스 위로 이동하여 **제거** 아이콘을 클릭합니다.

안전하게 제거할 수 있는 가상 하드웨어에만 이 아이콘이 표시됩니다.

5 디바이스 제거를 확인하려면 **삭제**를 클릭합니다.

vTPM 디바이스가 제거로 표시됩니다.

6 **확인**을 클릭합니다.

신뢰할 수 있는 가상 플랫폼 모듈 항목이 **VM 하드웨어** 창의 가상 시스템 **요약** 탭에 더 이상 나타나지 않는지 확인합니다.

신뢰할 수 있는 가상 플랫폼 모듈이 사용되도록 설정된 가상 시스템 식별

어떤 가상 시스템이 vTPM(신뢰할 수 있는 가상 플랫폼 모듈)을 사용하도록 설정되어 있는지 식별할 수 있습니다.

인벤토리 내 모든 가상 시스템의 목록을 생성하여 가상 시스템 이름, 운영 체제 및 vTPM 상태를 표시할 수 있습니다. 이 목록을 규정 준수 감사에 사용하도록 CSV 파일로 내보낼 수도 있습니다.

절차

1 vSphere Client를 사용하여 vCenter Server에 연결합니다.

2 vCenter Server 인스턴스, 호스트 또는 클러스터를 선택합니다.

3 **VM** 탭을 클릭하고 **가상 시스템**을 클릭합니다.

4 TPM이 사용되도록 설정된 모든 가상 시스템을 보려면 왼쪽 아래 모서리에 있는 세 개의 막대형 **열 선택기**를 클릭하고 **TPM**을 선택합니다.

TPM이 사용되도록 설정된 가상 시스템의 경우 TPM 열에 "있음"이 표시됩니다. TPM이 없는 가상 시스템은 "없음"으로 나열됩니다.

5 인벤토리 목록 보기의 내용을 CSV 파일로 내보낼 수 있습니다.

a 목록 보기 오른쪽 아래에 있는 **내보내기**를 클릭합니다.

목록 내용 내보내기 대화 상자가 열리고 CSV 파일에 포함할 수 있는 옵션이 나열됩니다.

b CSV 파일에 모든 행을 나열할지 또는 현재 선택한 행을 나열할지를 선택합니다.

c 사용 가능한 옵션에서 CSV 파일에 나열할 열을 선택합니다.

d **내보내기**를 클릭합니다.

CSV 파일이 생성되어 다운로드 가능합니다.

신뢰할 수 있는 가상 플랫폼 모듈 디바이스 인증서 보기

vTPM(신뢰할 수 있는 가상 플랫폼 모듈) 디바이스는 검토가 가능한 기본 인증서로 미리 구성되어 있습니다.

사전 요구 사항

vTPM 지원 가상 시스템이 환경에 있어야 합니다.

절차

1 vSphere Client를 사용하여 vCenter Server에 연결합니다.

2 ESXi 호스트 또는 클러스터 같이 가상 시스템의 올바른 상위 개체인 인벤토리의 개체를 선택합니다.

3 **VM**을 클릭하고 **가상 시스템**을 클릭합니다.

4 인증서 정보를 보려는 vTPM이 사용되도록 설정된 가상 시스템을 선택합니다.

필요한 경우 왼쪽 하단 모서리에 있는 세 개의 막대형 **열 선택기**를 클릭하고 **TPM**을 선택하여 TPM이 "있음" 상태인 가상 시스템을 표시합니다.

5 **구성** 탭을 클릭합니다.

6 **TPM**에서 **인증서**를 선택합니다.

7 인증서를 선택하고 해당 정보를 봅니다.

8 (선택 사항) 인증서 정보를 내보내려면 **내보내기**를 클릭합니다.

인증서가 디스크에 저장됩니다.

다음에 수행할 작업

기본 인증서를 타사 CA(인증 기관)에서 발급한 인증서로 교체할 수 있습니다. 신뢰할 수 있는 가상 플랫폼 모듈 디바이스 인증서 내보내기 및 교체의 내용을 참조하십시오.

신뢰할 수 있는 가상 플랫폼 모듈 디바이스 인증서 내보내기 및 교체

vTPM(신뢰할 수 있는 가상 플랫폼 모듈) 디바이스와 함께 제공되는 기본 인증서를 교체할 수 있습니다.

사전 요구 사항

vTPM 지원 가상 시스템이 환경에 있어야 합니다.

절차

1 vSphere Client를 사용하여 vCenter Server에 연결합니다.

2 ESXi 호스트 또는 클러스터 같이 가상 시스템의 올바른 상위 개체인 인벤토리의 개체를 선택합니다.

3 인벤토리에서 인증서 정보를 교체할 vTPM 지원 가상 시스템을 선택합니다.

4 **구성** 탭을 클릭합니다.

5 **TPM**에서 **서명 요청**을 선택합니다.

6 인증서를 선택합니다.

7 인증서 정보를 내보내려면 **내보내기**를 클릭합니다.

인증서가 디스크에 저장됩니다.

8 내보낸 CSR(인증서 서명 요청)에 대해 타사 CA(인증 기관)에서 발급한 인증서를 가져옵니다.

IT 환경에 있을 수 있는 모든 CA를 사용할 수 있습니다.

9 새 인증서가 있는 경우 기존 인증서를 교체합니다.

a 인벤토리에서 교체할 인증서가 있는 가상 시스템을 마우스 오른쪽 버튼으로 클릭하고 **설정 편집**을 선택합니다.

b **설정 편집** 대화상자에서 **보안 디바이스**를 확장한 다음 **신뢰할 수 있는 플랫폼 모듈**을 확장합니다.

인증서가 나타납니다.

c 교체하려는 인증서에 대해 **교체**를 클릭합니다.

파일 업로드 대화상자가 나타납니다.

d 로컬 시스템에서 새 인증서를 찾아서 업로드합니다.

새 인증서가 vTPM 디바이스와 함께 제공된 기본 인증서를 교체합니다.

e **신뢰할 수 있는 가상 플랫폼 모듈** 목록 아래에 있는 가상 시스템 **요약** 탭에서 인증서 이름이 업데이트됩니다.

가상화 기반 보안을 사용한 Windows 게스트 운영 체제 보호

12

vSphere 6.7부터는 지원되는 Windows 게스트 운영 체제에서 Microsoft VBS(가상화 기반 보안)를 사용하도록 설정할 수 있습니다.

Windows 10 및 Windows Server 2016 운영 체제의 기능인 Microsoft VBS는 하드웨어 및 소프트웨어 가상화를 사용하여 분리되고 하이퍼바이저로 제한된 전용 하위 시스템을 생성함으로써 시스템 보안을 향상시킵니다.

VBS를 사용하면 다음과 같은 Windows 보안 기능을 통해 시스템을 강화하고 주요 시스템 및 사용자 암호가 손상되지 않도록 분리할 수 있습니다.

- 자격 증명 격리: 주요 시스템 및 사용자 암호를 분리하고 강화하여 손상으로부터 보호합니다.
- 장치 보호: 함께 작동하며 Windows 시스템에서 실행되는 멀웨어를 방지하고 제거하도록 설계된 일련의 기능을 제공합니다.
- 구성 가능한 코드 무결성: 앞으로 부트 로더에서 신뢰할 수 있는 코드만 실행되도록 보장합니다.

자세한 내용은 Microsoft 설명서에 나온 가상화 기반 보안 관련 항목을 참조하십시오.

vCenter Server를 통해 가상 시스템에 VBS를 사용하도록 설정한 후에 Windows 게스트 운영 체제 내에서 VBS를 사용하도록 설정합니다.

본 장은 다음 항목을 포함합니다.

- 가상화 기반 보안 모범 사례
- 가상 시스템에서 가상화 기반 보안을 사용하도록 설정
- 기존 가상 시스템에서 가상화 기반 보안을 사용하도록 설정
- 게스트 운영 체제에서 가상화 기반 보안을 사용하도록 설정
- 가상화 기반 보안을 사용하지 않도록 설정
- VBS를 사용하는 가상 시스템 식별

가상화 기반 보안 모범 사례

Windows 게스트 운영 체제 환경의 보안과 관리 효율성을 극대화하려면 VBS(가상화 기반 보안) 관련 모범 사례를 따릅니다.

이러한 모범 사례를 따르면 문제를 방지할 수 있습니다.

VBS 하드웨어

VBS에 다음 하드웨어를 사용합니다.

- Intel
  - Haswell CPU 이상. 최상의 성능을 얻으려면 Skylake-EP CPU 이상을 사용합니다.
  - Ivy Bridge CPU를 사용할 수 있습니다.
  - Sandy Bridge CPU를 사용하면 성능이 약간 저하될 수 있습니다.
- AMD
  - Zen 2 시리즈 CPU(Rome) 이상.
  - 오래된 CPU를 사용하면 성능이 약간 저하될 수 있습니다.

MCEPSC(페이지 크기 변경 시 시스템 확인 오류) Intel CPU 취약성 완화는 VBS가 사용 중일 때 게스트 운영 체제 성능에 부정적인 영향을 미칠 수 있습니다. 자세한 내용은 VMware KB 문서(https://kb.vmware.com/kb/76050)를 참조하십시오.

Windows 게스트 운영 체제 호환성

Intel에서 VBS는 Windows 10, Windows Server 2016 이상 가상 시스템에 대해 지원됩니다. 단, Windows Server 2016 버전 1607 및 1703의 경우에는 패치를 적용해야 합니다. ESXi 호스트 하드웨어 호환성은 Microsoft 설명서를 확인하십시오. VBS에 Intel CPU를 사용하려면 vSphere 6.7 이상 및 하드웨어 버전 14가 필요합니다.

AMD에서 VBS는 Windows 10, 버전 1809 및 Windows 2019 이상의 가상 시스템에서 지원됩니다. VBS에 AMD CPU를 사용하려면 vSphere 7.0 업데이트 2 이상 및 하드웨어 버전 19이 필요합니다.

처음에는 Windows 10에서 VBS에 Hyper-V를 사용하도록 설정해야 했습니다. Windows 10에서 Hyper-V를 사용하도록 설정할 필요가 없습니다. Windows Server 2016 이상에도 마찬가지입니다. 자세한 내용은 현재 Microsoft 설명서 및 "VMware vSphere 릴리스 정보" 를 참조하십시오.

VBS에서 지원되지 않는 VMware 기능

VBS가 사용되도록 설정된 경우 가상 시스템에서 다음과 같은 기능이 지원되지 않습니다.

- Fault Tolerance
- PCI 패스스루
- CPU 또는 메모리 무중단 추가

VBS 설치 및 업그레이드 관련 주의 사항

VBS를 구성하기 전에 다음과 같은 설치 및 업그레이드 주의 사항을 확인하십시오.

- 버전 14 이전의 가상 하드웨어에서 Windows 10 및 Windows Server 2016 이상에 사용하도록 구성된 새 가상 시스템은 기본적으로 레거시 BIOS를 사용하여 생성됩니다. 가상 시스템의 펌웨어 유형을 레거시 BIOS에서 UEFI로 변경한 후에는 게스트 운영 체제를 다시 설치해야 합니다.

- 이전 vSphere 릴리스에서 vSphere 6.7 이상으로 가상 시스템을 마이그레이션하며 가상 시스템에서 VBS를 사용하도록 설정하려는 경우 UEFI를 사용하면 운영 체제를 다시 설치하지 않아도 됩니다.

가상 시스템에서 가상화 기반 보안을 사용하도록 설정

가상 시스템을 생성할 때 지원되는 Windows 게스트 운영 체제에서 Microsoft VBS(가상화 기반 보안)를 동시에 사용하도록 설정할 수 있습니다.

VBS를 사용하도록 설정하려면 먼저 가상 시스템에서 VBS를 사용하도록 설정한 후에 Windows 게스트 운영 체제에서 VBS를 사용하도록 설정해야 합니다.

사전 요구 사항

사용 가능한 CPU는 가상화 기반 보안 모범 사례를 참조하십시오.

VBS에 Intel CPU를 사용하려면 vSphere 6.7 이상이 필요합니다. 하드웨어 버전 14 이상과 지원되는 다음 게스트 운영 체제 중 하나를 사용하는 가상 시스템을 생성합니다.

- Windows 10(64비트) 이상 릴리스
- Windows Server 2016(64비트) 이상 릴리스

VBS에 AMD CPU를 사용하려면 vSphere 7.0 업데이트 2 이상이 필요합니다. 하드웨어 버전 19 이상과 지원되는 다음 게스트 운영 체제 중 하나를 사용하는 가상 시스템을 생성합니다.

- Windows 10(64비트), 버전 1809 이상 릴리스
- Windows Server 2019(64비트) 이상 릴리스

VBS를 사용하도록 설정하기 전에 Windows 10, 버전 1809 및 Windows Server 2019에 대한 최신 패치를 설치해야 합니다.

절차

1 vSphere Client를 사용하여 vCenter Server에 연결합니다.

2 ESXi 호스트 또는 클러스터 같이 가상 시스템의 올바른 상위 개체인 인벤토리의 개체를 선택합니다.

3 개체를 마우스 오른쪽 버튼으로 클릭하고 **새 가상 시스템**을 선택한 다음 프롬프트에 따라 가상 시스템을 생성합니다.

옵션	작업
생성 유형 선택	가상 시스템을 생성합니다.
이름 및 폴더 선택	이름 및 대상 위치를 지정합니다.
계산 리소스 선택	가상 시스템을 생성할 권한이 있는 개체를 지정합니다.
스토리지 선택	VM 스토리지 정책에서 스토리지 정책을 선택합니다. 호환되는 데이터스토어를 선택합니다.
호환성 선택	Intel CPU: **ESXi 6.7 이상**이 선택되어 있는지 확인합니다. AMD CPU: **ESXi 7.0 U2 이상**이 선택되어 있는지 확인합니다.

옵션	작업
게스트 운영 체제 선택	운영 체제 릴리스에 가장 적합한 Windows 게스트 운영 체제 옵션을 선택합니다. **Windows 가상화 기반 보안 사용** 확인란을 선택합니다.
하드웨어 사용자 지정	예를 들면 디스크 크기 또는 CPU를 변경하여 하드웨어를 사용자 지정합니다.
완료 준비	정보를 검토하고 **마침**을 클릭합니다.

결과

가상 시스템이 생성된 후 해당 **요약** 탭의 게스트 운영 체제 설명에 "VBS true"가 표시되는지 확인합니다.

다음에 수행할 작업

게스트 운영 체제에서 가상화 기반 보안을 사용하도록 설정의 내용을 참조하십시오.

기존 가상 시스템에서 가상화 기반 보안을 사용하도록 설정

지원되는 Windows 게스트 운영 체제에서 기존 가상 시스템에 대한 Microsoft VBS(가상화 기반 보안)를 사용하도록 설정할 수 있습니다.

VBS를 사용하도록 설정하려면 먼저 가상 시스템에서 VBS를 사용하도록 설정한 후에 게스트 운영 체제에서 VBS를 사용하도록 설정해야 합니다.

참고 버전 14 이전의 하드웨어 버전에서 Windows 10, Windows Server 2016 및 Windows Server 2019을 사용하도록 구성된 새 가상 시스템은 기본적으로 레거시 BIOS를 사용하여 생성됩니다. 가상 시스템의 펌웨어 유형을 기존 BIOS에서 UEFI로 변경하는 경우 게스트 운영 체제를 다시 설치해야 합니다.

사전 요구 사항

사용 가능한 CPU는 가상화 기반 보안 모범 사례를 참조하십시오.

VBS에 Intel CPU를 사용하려면 vSphere 6.7 이상이 필요합니다. 하드웨어 버전 14 이상 및 지원되는 다음 게스트 운영 체제 중 하나를 사용하여 가상 시스템이 생성되어 있어야 합니다.

- Windows 10(64비트) 이상 릴리스
- Windows Server 2016(64비트) 이상 릴리스

VBS에 AMD CPU를 사용하려면 vSphere 7.0 업데이트 2 이상이 필요합니다. 하드웨어 버전 19 이상 및 지원되는 다음 게스트 운영 체제 중 하나를 사용하여 가상 시스템이 생성되어 있어야 합니다.

- Windows 10(64비트), 버전 1809 이상 릴리스
- Windows Server 2019(64비트) 이상 릴리스

VBS를 사용하도록 설정하기 전에 Windows 10, 버전 1809 및 Windows Server 2019에 대한 최신 패치를 설치해야 합니다.

절차

1 vSphere Client에서 가상 시스템을 찾습니다.

2 가상 시스템을 마우스 오른쪽 버튼으로 클릭하고 **설정 편집**을 선택합니다.

3 **VM 옵션** 탭을 클릭합니다.

4 가상화 기반 보안에 대해 **사용** 확인란을 선택합니다.

5 **확인**을 클릭합니다.

결과

가상 시스템의 **요약** 탭에서 게스트 운영 체제 설명에 "VBS true"가 표시되는지 확인합니다.

다음에 수행할 작업

게스트 운영 체제에서 가상화 기반 보안을 사용하도록 설정의 내용을 참조하십시오.

게스트 운영 체제에서 가상화 기반 보안을 사용하도록 설정

지원되는 Windows 게스트 운영 체제에서 Microsoft VBS(가상화 기반 보안)를 사용하도록 설정할 수 있습니다.

Windows 게스트 운영 체제 내에서 VBS를 사용하도록 설정할 수 있습니다. Windows는 GPO(그룹 정책 개체)를 통해 VBS를 구성하고 적용합니다. GPO는 보안 부팅, 장치 보호, 자격 증명 격리와 같은 VBS에서 제공하는 다양한 서비스를 설정하고 해제하는 기능을 제공합니다. 또한 특정 Windows 버전에서는 Hyper-V 플랫폼을 사용하도록 설정하는 추가 단계를 수행해야 합니다.

장치 보호를 배포하여 가상화 기반 보안을 사용하도록 설정하는 방법에 대한 자세한 내용은 Microsoft 설명서를 참조하십시오.

사전 요구 사항

- 가상 시스템에서 가상화 기반 보안이 사용되도록 설정되었는지 확인합니다.

절차

1 Microsoft Windows에서 그룹 정책을 편집하여 VBS를 설정하고 다른 VBS 관련 보안 옵션을 선택합니다.

2 (선택 사항) Redstone 4 이전 Microsoft Windows 버전의 경우 Windows 기능 제어판에서 Hyper-V 플랫폼을 사용하도록 설정합니다.

3 게스트 운영 체제를 재부팅합니다.

가상화 기반 보안을 사용하지 않도록 설정

가상 시스템에 VBS(가상화 기반 보안)를 더 이상 사용하지 않는 경우 VBS를 사용하지 않도록 설정할 수 있습니다. 가상 시스템에 VBS를 사용하지 않도록 설정할 경우 Windows VBS 옵션은 변경되지 않고 유지되지만 성능 문제가 발생할 수 있습니다. 가상 시스템에 VBS를 사용하지 않도록 설정하기 전에 Windows 내에서 VBS 옵션을 사용하지 않도록 설정합니다.

사전 요구 사항

가상 시스템의 전원이 꺼졌는지 확인합니다.

절차

1 vSphere Client에서 VBS가 사용되도록 설정된 가상 시스템을 찾습니다.

VBS가 사용되도록 설정된 가상 시스템을 찾는 방법은 VBS를 사용하는 가상 시스템 식별을 참조하십시오.

2 가상 시스템을 마우스 오른쪽 버튼으로 클릭하고 **설정 편집**을 선택합니다.

3 **VM 옵션**을 클릭합니다.

4 가상화 기반 보안에 대한 **사용** 확인란의 선택을 취소합니다.

게스트 운영 체제에서 VBS를 사용하지 않도록 설정하라는 메시지가 표시됩니다.

5 **확인**을 클릭합니다.

6 가상 시스템의 **요약** 탭에서 게스트 운영 체제 설명에 "VBS true"가 더 이상 표시되지 않는지 확인합니다.

VBS를 사용하는 가상 시스템 식별

보고 및 규정 준수 목적으로 VBS를 사용하도록 설정된 가상 시스템을 식별할 수 있습니다.

절차

1 vSphere Client를 사용하여 vCenter Server에 연결합니다.

2 인벤토리에서 vCenter Server 인스턴스, 데이터 센터 또는 호스트를 선택합니다.

3 **VM** 탭을 클릭하고 **가상 시스템**을 클릭합니다.

4 **VBS** 열을 표시하려면 왼쪽 하단 모서리에 있는 세 개의 막대형 **열 선택기**를 클릭하고 **VBS** 확인란을 선택합니다.

5 **VBS** 열에서 "있음"을 검색합니다.

vSphere 네트워킹 보호

13

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
- 표준 스위치 보호 및 VLAN
- vSphere Distributed Switch 및 분산 포트 그룹 보안
- VLAN으로 가상 시스템 보호
- 단일 ESXi 호스트 내에 여러 네트워크 생성
- 인터넷 프로토콜 보안
- 적절한 SNMP 구성 확인
- 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 VM에서 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 네트워크를 설정하는 경우, 가상 네트워크의 맨 앞에 있는 가상 시스템에 호스트 기반 방화벽을 설치합니다. 이 방화벽이 물리적 네트워크 어댑터와 가상 네트워크의 나머지 VM 사이에서 보호 완충 지대 역할을 하게 됩니다.

호스트 기반 방화벽은 성능을 저하시킬 수 있으므로 가상 네트워크 내의 다른 곳에 위치한 VM에 호스트 기반 방화벽을 설치하기 전에 먼저 보안 요구 사항과 성능 목표 간의 균형을 고려해야 합니다.

방화벽으로 네트워크 보호의 내용을 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 영역에서 다른 영역으로 데이터가 누출될 위험이 최소화됩니다. 세그먼트화는 ARP(주소 분석 프로토콜) 스푸핑을 비롯한 다양한 위협을 방지합니다. ARP 스푸핑에서는 공격자가 ARP 테이블을 조작하여 MAC 및 IP 주소를 다시 매핑함으로써 호스트에서 들어오고 나가는 네트워크 트래픽에 액세스할 수 있습니다. 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 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 있습니다. VLAN으로 가상 시스템 보호의 내용을 참조하십시오.

무단 액세스 방지

가상 시스템을 보호하기 위한 요구 사항은 물리적 시스템을 보호하기 위한 요구 사항과 동일한 경우가 많습니다.

- 가상 시스템 네트워크가 물리적 네트워크에 연결되어 있는 경우 물리적 시스템으로 구성된 네트워크와 동일한 침입 위험에 노출될 수 있습니다.
- VM을 물리적 네트워크에 연결하지 않더라도 VM이 다른 VM에 의해 공격을 받을 수 있습니다.

VM은 서로 분리되어 있습니다. VM은 다른 VM에 있는 메모리를 읽거나 쓸 수 없고 데이터에 액세스할 수 없으며 애플리케이션을 사용할 수 없습니다. 하지만 네트워크 내에서는 모든 VM이나 VM 그룹이 다른 VM을 통한 무단 액세스의 대상이 될 수 있으므로 무단 액세스로부터 VM을 보호해야 합니다.

VM 보호에 대한 자세한 내용은 다음 사이트에서 제목이 "Secure Virtual Network Configuration for Virtual Machine (VM) Protection"(VM(가상 시스템) 보호를 위한 안전한 가상 네트워크 구성)인 NIST 문서를 참조하십시오.

https://csrc.nist.gov/publications/detail/sp/800-125b/final

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.

vSphere 및 vSAN을 포함한 VMware 제품의 지원되는 모든 포트 및 프로토콜 목록은 https://ports.vmware.com/에서 VMware Ports and Protocols Tool™을 참조하십시오. VMware 제품별로 포트를 검색하고, 사용자 지정된 포트 목록을 생성하고, 포트 목록을 인쇄하거나 저장할 수 있습니다.

vCenter Server 구성을 위한 방화벽

vCenter Server를 통해 ESXi 호스트에 액세스하는 경우에는 일반적으로 방화벽을 사용하여 vCenter Server를 보호합니다.

방화벽은 진입점에 있어야 합니다. 방화벽은 클라이언트와 vCenter Server 사이에 있을 수 있으며 vCenter Server와 클라이언트는 모두 방화벽 뒤에 있을 수 있습니다.

vSphere 및 vSAN을 포함한 VMware 제품의 지원되는 모든 포트 및 프로토콜 목록은 https://ports.vmware.com/에서 VMware Ports and Protocols Tool™을 참조하십시오. VMware 제품별로 포트를 검색하고, 사용자 지정된 포트 목록을 생성하고, 포트 목록을 인쇄하거나 저장할 수 있습니다.

vCenter Server와 함께 구성된 네트워크는 vSphere Client, 기타 UI 클라이언트 또는 vSphere API를 사용하는 클라이언트를 통해 통신을 수신할 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.

네트워크 사용량 및 클라이언트에 필요한 보안 수준에 따라 네트워크의 다른 액세스 지점에 방화벽을 포함할 수도 있습니다. 네트워크 구성에 대한 보안 위험을 기반으로 방화벽의 위치를 선택합니다. 일반적으로 다음과 같은 방화벽 위치가 사용됩니다.

- vSphere Client 또는 타사 네트워크 관리 클라이언트와 vCenter Server 사이
- 사용자가 웹 브라우저를 통해 가상 시스템에 액세스하는 경우, 웹 브라우저와 ESXi 호스트 사이
- 사용자가 vSphere Client를 통해 가상 시스템에 액세스하는 경우, vSphere Client와 ESXi 호스트 사이. 이 연결은 vSphere 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 간에 방화벽을 추가하고 가상 시스템을 마이그레이션하려는 경우 대상 호스트에서 소스 호스트를 분리하는 방화벽의 포트를 엽니다.
- ESXi 호스트와 NFS 또는 iSCSI 스토리지 등의 네트워크 스토리지 사이. 이러한 포트는 VMware와 관련이 없습니다. 네트워크의 규격에 따라 이러한 포트를 구성하십시오.

방화벽을 통해 vCenter Server에 연결

방화벽에서 TCP 포트 443을 열어 vCenter Server가 데이터를 수신할 수 있도록 합니다.

vCenter Server는 기본적으로 TCP 포트 443을 사용하여 클라이언트의 데이터를 수신합니다. vCenter Server와 클라이언트 사이에 방화벽이 있는 경우 vCenter Server가 클라이언트로부터 데이터를 수신할 수 있는 연결을 구성해야 합니다. 방화벽 구성은 사이트에서 사용하는 방화벽에 따라 다르므로 자세한 내용은 로컬 방화벽 시스템 관리자에게 문의하십시오.

방화벽을 통해 ESXi 호스트 연결

ESXi 호스트와 vCenter Server 사이에 방화벽이 있는 경우 관리 호스트가 데이터를 수신할 수 있는지 확인합니다.

데이터를 수신하기 위한 연결을 구성하려면 vSphere High Availability, vMotion 및 vSphere Fault Tolerance와 같은 서비스에서 들어오는 트래픽을 위한 포트를 엽니다. 구성 파일, vSphere Client 액세스 및 방화벽 명령에 대한 자세한 내용은 ESXi 방화벽 구성 항목을 참조하십시오. 포트 목록은 https://ports.vmware.com에서 VMware Ports and Protocols Tool™을 참조하십시오.

vCenter Server가 없는 구성을 위한 방화벽

환경에 vCenter Server가 포함되지 않은 경우 클라이언트가 ESXi 네트워크에 직접 연결할 수 있습니다.

여러 가지 방법으로 독립형 ESXi 호스트에 연결할 수 있습니다.

- VMware Host Client
- ESXCLI 인터페이스
- vSphere Web Services SDK 또는 vSphere Automation SDK
- 타사 클라이언트

독립형 호스트에 대한 방화벽 요구 사항은 vCenter Server가 있을 때 요구 사항과 유사합니다.

- 방화벽을 사용하여 ESXi 계층 또는 구성에 따라 클라이언트 및 ESXi 계층을 보호합니다. 이 방화벽은 네트워크에 대한 기본적인 보호 기능을 제공합니다.
- 이 구성 유형에서 라이센싱은 각 호스트에 설치하는 ESXi 패키지의 일부입니다. 라이센싱이 ESXi에 있으므로 방화벽이 있는 별도의 License Server가 필요하지 않습니다.

ESXCLI 또는 VMware Host Client를 사용하여 방화벽 포트를 구성할 수 있습니다. "vSphere 단일 호스트 관리 - VMware Host Client" 의 내용을 참조하십시오.

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 Client를 사용하여 vCenter Server를 통해 연결하는지 아니면 VMware Host Client에서 ESXi 호스트에 직접 연결하는지에 따라 다릅니다.

포트, 용도 및 분류(수신, 송신 또는 양방향)에 대한 자세한 내용은 https://ports.vmware.com에서 VMware Ports and Protocols Tool™을 참조하십시오.

vSphere Client를 통해 브라우저 기반의 가상 시스템 콘솔에 연결

vSphere Client를 사용하여 연결하는 경우에는 ESXi 호스트를 관리하는 vCenter Server 시스템에 항상 연결한 후 여기에서 가상 시스템 콘솔에 액세스합니다.

vSphere Client를 사용하여 브라우저 기반 가상 시스템 콘솔에 연결하는 경우에는 다음과 같은 액세스가 가능해야 합니다.

- 방화벽이 포트 443에서 vSphere Client의 vCenter Server 액세스를 허용해야 합니다.
- 방화벽이 포트 902에서 vCenter Server의 ESXi 호스트 액세스를 허용해야 합니다.

vSphere Client를 통해 VMware Remote Console에 연결

vSphere Client를 사용하고 VMRC(VMware Remote Console)에 연결하는 경우에는 다음과 같은 액세스가 가능해야 합니다.

- 방화벽이 포트 443에서 vSphere Client의 vCenter Server 액세스를 허용해야 합니다.

- 방화벽은 VMRC가 포트 443에서 vCenter Server에 액세스하고, VMRC 버전 11.0 미만은 포트 902에서 VMRC 버전 11.0 이상은 포트 443에서 ESXi 호스트에 액세스할 수 있도록 허용해야 합니다. VMRC 버전 11.0 및 ESXi 포트 요구 사항에 대한 자세한 내용은 https://kb.vmware.com/s/article/76672에서 VMware 기술 자료 문서를 참조하십시오.

VMware Host Client를 통해 직접 ESXi 호스트에 연결

ESXi 호스트에 직접 연결하면 VMware Host Client 가상 시스템 콘솔을 사용할 수 있습니다.

참고 vCenter Server 시스템에 의해 관리되는 호스트에 직접 연결할 때는 VMware Host Client를 사용하지 마십시오. VMware Host Client에서 해당 호스트를 변경하는 경우 환경이 불안정해질 수 있습니다.

방화벽은 포트 443과 902에서 ESXi 호스트에 대한 액세스를 허용해야 합니다.

VMware Host 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 스패닝 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 스패닝 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 스패닝 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 포트로 올바르게 구성되어 있는지 확인합니다.

보안 정책으로 표준 스위치 포트 보호

표준 스위치의 VMkernel 포트 그룹 또는 가상 시스템 포트 그룹은 구성 가능한 보안 정책을 갖습니다. 보안 정책은 VM의 가장 및 가로채기 공격에 대한 보호 적용 강도를 결정합니다.

가상 시스템 네트워크 어댑터는 물리적 네트워크 어댑터와 마찬가지로 다른 VM을 가장할 수 있습니다. 가장으로 인해 보안 위험이 발생할 수 있습니다.

- VM은 다른 시스템에서 온 것으로 보이는 프레임을 보내 해당 시스템으로 보내려 하는 네트워크 프레임을 받을 수 있습니다.
- 다른 시스템을 대상으로 하는 프레임을 받도록 가상 시스템 네트워크 어댑터를 구성할 수 있습니다.

VMkernel 포트 그룹 또는 가상 시스템 포트 그룹을 표준 스위치에 추가하면 ESXi는 해당 그룹의 포트에 대한 보안 정책을 구성합니다. 이 보안 정책을 사용하여 호스트에 있는 VM의 게스트 운영 체제가 네트워크의 다른 시스템으로 가장하지 못하게 방지할 수 있습니다. 가장을 시도하는 게스트 운영 체제는 가장이 금지된 것을 감지하지 못합니다.

보안 정책은 VM의 가장 및 가로채기 공격에 대한 보호 적용 강도를 결정합니다. 보안 프로파일의 설정을 올바르게 사용하는 방법은 "vSphere 네트워킹" 문서의 "보안 정책" 섹션을 참조하십시오. 이 섹션에서는 다음을 설명합니다.

- VM 네트워크 어댑터가 전송을 제어하는 방법
- 이 수준에서 공격이 이루어지는 방식

vSphere 표준 스위치 보안

VM 네트워크 어댑터의 일부 MAC 주소 모드를 제한하여 표준 스위치 트래픽을 계층 2 공격으로부터 보호할 수 있습니다.

각 VM 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.

VM 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. 따라서 운영 체제가 수신 네트워크에 의해 인증된 네트워크 어댑터를 가장하여 네트워크의 디바이스에 악의적인 공격을 꾀할 수 있습니다.

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.

- MAC 주소 변경(MAC 주소 변경 사항 참조)
- 비규칙 모드(비규칙(Promiscuous) 모드 작업 참조)
- 위조 전송(위조 전송 참조)

vSphere 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 옵션을 사용하면 가상 시스템이 VMX에 구성된 것과 다른 Mac 주소로 프레임을 수신할 수 있습니다.

MAC 주소 변경 옵션이 **수락**으로 설정되면 ESXi는 가상 시스템의 유효 MAC 주소를 초기 MAC 주소가 아닌 다른 주소로 변경하려는 요청을 수락합니다.

MAC 주소 변경 옵션이 **거부**로 설정되면 ESXi는 가상 시스템의 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.

참고 vSphere 7.0부터 **위조 전송** 및 **MAC 주소 변경**에 대한 기본값이 수락 대신 거부로 변경되었습니다. 확인하려면 스토리지 벤더에 문의하십시오.

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.

참고 vSphere 7.0부터 **위조 전송** 및 **MAC 주소 변경**에 대한 기본값이 수락 대신 거부로 변경되었습니다.

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.

무차별 모드로 가상 시스템 어댑터를 구성하는 방법에 대한 자세한 내용은 "vSphere 네트워킹" 설명서에서 vSphere Standard 스위치 또는 표준 포트 그룹에 대한 보안 정책 구성에 대한 항목을 참조하십시오.

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.

표준 스위치 보호 및 VLAN

VMware 표준 스위치는 VLAN 보안의 특정 위협에 대한 보호 조치를 제공합니다. 표준 스위치는 그 설계 방식 때문에 대부분 VLAN 호핑이 관련된 다양한 공격으로부터 VLAN을 보호합니다.

이 보호를 적용하더라도 가상 시스템 구성은 여전히 다른 유형의 공격에 취약할 수 있습니다. 예를 들어 표준 스위치는 이러한 공격으로부터 물리적 네트워크는 보호하지 않고 가상 네트워크만 보호합니다.

표준 스위치 및 VLAN은 다음 유형의 공격으로부터 보호할 수 있습니다.

MAC 플러딩

다른 소스로부터 들어오는 것으로 태그가 지정된 MAC 주소를 포함하는 패킷들로 스위치에 과부하를 야기합니다. 대부분의 스위치는 내용 주소 지정 가능 메모리 테이블을 사용하여 각 패킷의 소스 주소를 파악하고 저장합니다. 이 테이블이 가득 차면 스위치는 수신되는 모든 패킷이 모든 포트에서 브로드캐

스팅되는 완전 개방 상태에 들어가므로 공격자가 스위치의 모든 트래픽을 볼 수 있게 됩니다. 이 상태가 되면 VLAN에서 패킷 유출이 발생할 수 있습니다.

VMware 표준 스위치는 MAC 주소 테이블을 저장하기는 하지만 관찰 가능한 트래픽에서 MAC 주소를 가져오지 않기 때문에 이러한 유형의 공격에 취약하지 않습니다.

802.1q 및 ISL 태그 지정 공격

트렁크로 작동하고 트래픽을 다른 VLAN으로 브로드캐스팅하도록 스위치를 속여 스위치가 프레임을 한 VLAN에서 다른 VLAN으로 리디렉션하도록 합니다.

VMware 표준 스위치는 이러한 유형의 공격에 필요한 동적 트렁킹을 수행하지 않으므로 취약하지 않습니다.

이중 캡슐화 공격

공격자가 내부 태그의 VLAN 식별자가 외부 태그의 VLAN 식별자와 다른 이중 캡슐화 패킷을 만들 때 발생하는 공격입니다. 네이티브 VLAN은 다르게 동작하도록 구성하지 않는 한 이전 버전과의 호환성을 위해 전송된 패킷에서 외부 태그를 제거합니다. 네이티브 VLAN 스위치가 외부 태그를 제거하면 내부 태그만 남게 되고 이 내부 태그는 제거된 외부 태그에 식별되었던 것과 다른 VLAN으로 패킷을 라우팅합니다.

VMware 표준 스위치는 가상 시스템이 특정 VLAN에 대해 구성된 포트로 전송을 시도하는 모든 이중 캡슐화 프레임을 버립니다. 따라서 이 유형의 공격에 취약하지 않습니다.

멀티캐스트 무차별 암호 대입 공격(brute force attack)

대량의 멀티캐스트 프레임을 알려진 VLAN으로 거의 동시에 전송하여 스위치 오버로드를 유발하고 결과적으로 프레임 일부가 실수로 다른 VLAN에 브로드캐스팅되도록 합니다.

VMware 표준 스위치는 프레임이 올바른 브로드캐스트 도메인(VLAN)을 벗어나는 것을 허용하지 않기 때문에 이러한 유형의 공격에 취약하지 않습니다.

스패닝 트리(spanning tree) 공격

LAN의 부분 간 브리지를 제어하는 데 사용되는 STP(Spanning-Tree Protocol)를 대상으로 합니다. 공격자는 네트워크 토폴로지 변경을 시도하는 BPDU(Bridge Protocol Data Unit) 패킷을 전송하여 스스로를 루트 브리지로 설정합니다. 루트 브리지가 되면 공격자는 전송되는 프레임의 내용을 엿볼 수 있습니다.

VMware 표준 스위치는 STP를 지원하지 않으므로 이 유형의 공격에 취약하지 않습니다.

임의 프레임 공격

소스 및 대상 주소가 동일하게 유지되지만 필드의 길이, 유형 또는 내용이 임의로 변경되는 대량의 패킷을 전송합니다. 이 공격의 목표는 패킷이 실수로 다른 VLAN으로 다시 라우팅되게 하려는 것입니다.

VMware 표준 스위치는 이러한 공격에 대해 취약하지 않습니다.

시간이 지남에 따라 보안 위협이 새로 개발되므로 이 공격 목록이 전부일 것이라고 여기지 마십시오. 웹에서 VMware 보안 리소스를 정기적으로 확인하여 보안, 최신 보안 경고 및 VMware 보안 대책을 알아두십시오.

vSphere Distributed Switch 및 분산 포트 그룹 보안

관리자는 여러 가지 옵션을 통해 vSphere 환경에서 vSphere Distributed Switch를 보호할 수 있습니다.

표준 스위치와 동일한 규칙이 vSphere Distributed Switch의 VLAN에 적용됩니다. 자세한 내용은 표준 스위치 보호 및 VLAN의 내용을 참조하십시오.

절차

1 정적 바인딩을 사용하는 분산 포트 그룹의 경우 자동 확장 기능을 사용하지 않도록 설정합니다.

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 올바르게 추적되지 않는 경우 잘못된 ID 재사용이 의도치 않은 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 텍스트 상자가 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 가상 시스템의 전용 가상 스위치에서 내부 네트워킹용으로만 사용됨을 나타냅니다. 트래픽은 물리적 네트워크 어댑터를 거치지 않습니다.

6 현재 사용하지 않는 경우 vSphere Distributed Switch의 네트워크 상태 점검은 사용하지 않도록 설정합니다.

네트워크 상태 점검은 기본적으로 사용하지 않도록 설정되어 있습니다. 사용하도록 설정되면 상태 점검 패킷에 공격자가 잠재적으로 사용할 수 있는 호스트, 스위치 및 포트에 대한 정보가 포함됩니다. 문제 해결을 위해서만 네트워크 상태 점검을 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.

- MAC 주소 변경(MAC 주소 변경 사항 참조)

- 비규칙 모드(비규칙(Promiscuous) 모드 작업 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.

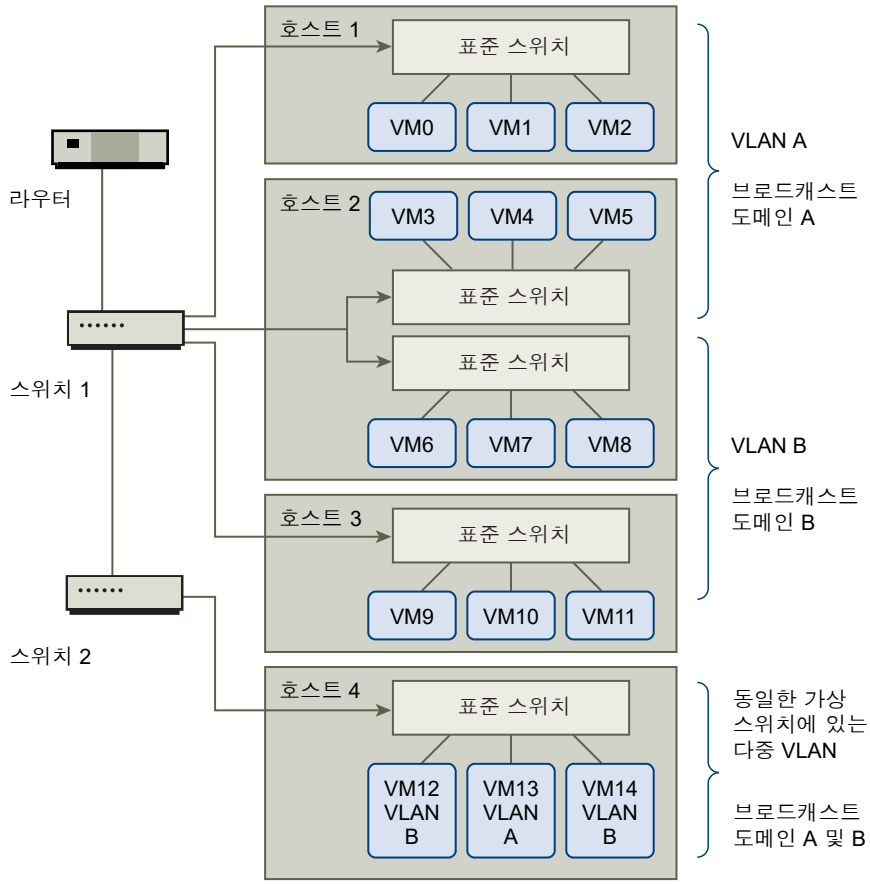
VLAN으로 가상 시스템 보호

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 13-1. 샘플 VLAN 레이아웃



이 구성에서는 회계 부서의 모든 직원은 VLAN A의 가상 시스템을 사용하고 영업 부서의 직원은 VLAN B의 가상 시스템을 사용합니다.

라우터는 회계 데이터가 포함된 패킷을 스위치로 전달합니다. 이러한 패킷에는 VLAN A로만 배포하도록 제한하는 태그가 붙습니다. 따라서 회계 데이터는 브로드캐스트 도메인 A로 제한되고 라우터 구성을 따로 변경하지 않는 한 브로드캐스트 도메인 B로 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 제공받는 가상 시스템들이 서로 다른 VLAN에 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 VLAN을 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 4094 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.

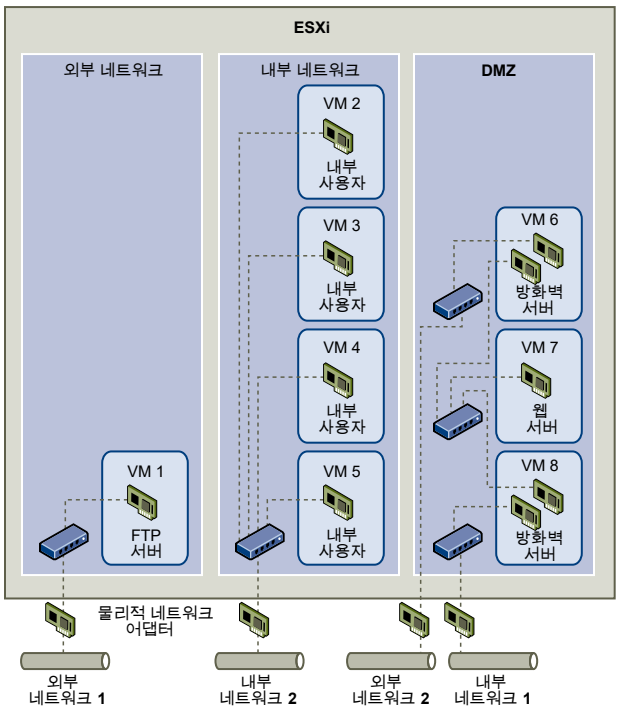
VLAN 네트워킹 모드는 표준 스위치의 경우 스위치 또는 포트 그룹 수준에서 구성할 수 있고, Distributed Switch의 경우 분산 포트 그룹 또는 포트 수준에서 구성할 수 있습니다.

3 각 가상 스위치의 모든 VLAN이 완전히 문서화되었는지 확인하고 각 가상 스위치에 필수 VLAN만 모두 있는지 확인합니다.

단일 ESXi 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 13-2. 단일 ESXi 호스트에 외부 네트워크, 내부 네트워크 및 DMZ 구성



이 그림에서 시스템 관리자는 호스트를 FTP 서버, 내부 가상 시스템 및 DMZ라는 세 가지 개별 가상 시스템 영역으로 구성했습니다. 각 영역은 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 FTP의 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 외부를 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 DMZ로 구성됩니다.

이 가상 시스템 그룹은 외부 네트워크 2 및 내부 네트워크 1과 연결되어 있습니다. 회사는 외부 네트워크 2를 사용하여 마케팅 및 재무 부서가 회사 웹 사이트 및 웹 사이트에서 외부 웹 사용자를 위해 호스팅하는 기타 웹 기능을 호스팅하는 데 사용하는 웹 서버를 지원합니다. 내부 네트워크 1은 마케팅 부서가 회사 웹 사이트에 자체 컨텐츠를 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 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 LAN에 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 Client에서 네트워크 스위치 레이아웃을 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 고유한 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` 명령을 사용하여 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` 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= *source address*	필수. 소스 주소를 지정합니다.
--sa-destination= *destination address*	필수. 대상 주소를 지정합니다.
--sa-mode= *mode*	필수. transport 또는 tunnel으로 모드를 지정합니다.
--sa-spi= *security parameter index*	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= *encryption algorithm*	필수. 다음 매개 변수 중 하나를 사용하여 암호화 알고리즘을 지정합니다. ■ 3des-cbc ■ aes128-cbc ■ null(암호화를 제공하지 않음)
--encryption-key= *encryption key*	암호화 알고리즘을 지정하는 경우 필수. 암호화 키를 지정합니다. ASCII 텍스트 또는 0x 접두사로 시작하는 16진수를 키로 입력할 수 있습니다.
--integrity-algorithm= *authentication algorithm*	필수. 인증 알고리즘을 hmac-sha1 또는 hmac-sha2-256으로 지정합니다.
--integrity-key= *authentication key*	필수. 인증 키를 지정합니다. ASCII 텍스트 또는 0x 접두사로 시작하는 16진수를 키로 입력할 수 있습니다.
--sa-name=*name*	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 0x697076367265616479 6c6f676f336465736362636f757432
--integrity-algorithm hmac-sha1
--integrity-key 0x69707636726561647 96c6f67736861316f757432
--sa-name sa1
```

IPsec 보안 연결 제거

ESXCLI 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 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 명령을 사용하여 보안 정책을 추가할 수 있습니다.

사전 요구 사항

보안 정책을 생성하기 전에 IPsec 보안 연결 추가에 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= *source address*	필수. 소스 IP 주소와 접두사 길이를 지정합니다.
--sp-destination= *destination address*	필수. 대상 주소 및 접두사 길이를 지정합니다.
--source-port= *port*	필수. 소스 포트를 지정합니다. 소스 포트는 0에서 65535 사이의 숫자여야 합니다.
--destination-port= *port*	필수. 대상 포트를 지정합니다. 소스 포트는 0에서 65535 사이의 숫자여야 합니다.

옵션	설명
--upper-layer-protocol= *protocol*	다음 매개 변수 중 하나를 사용하여 상위 계층 프로토콜을 지정합니다. ■ tcp ■ udp ■ icmp6 ■ any
--flow-direction= *direction*	in 또는 out을 사용하여 트래픽을 모니터링할 방향을 지정합니다.
--action= *action*	지정한 매개 변수를 사용하는 트래픽을 발견했을 때 수행할 작업을 지정합니다. 다음 매개 변수 중 하나를 사용할 수 있습니다. ■ none: 어떤 작업도 수행하지 않습니다. ■ discard: 데이터 수신 및 송신을 허용하지 않습니다. ■ ipsec: 보안 연결에 제공되는 인증 및 암호화 정보를 사용하여 데이터가 신뢰할 수 있는 소스에서 제공되었는지 확인합니다.
--sp-mode= *mode*	tunnel 또는 transport으로 모드를 지정합니다.
--sa-name=*security association name*	필수. 보안 정책에 사용할 보안 연결의 이름을 제공합니다.
--sp-name=*name*	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=sa1
--sp-name=sp1
```

IPsec 보안 정책 제거

ESXCLI 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.

ESXi에는 알림(트랩 및 알림)을 보내고 `GET`, `GETBULK`, `GETNEXT` 요청을 수신할 수 있는 SNMP 에이전트가 포함되어 있습니다. SNMP는 기본적으로 사용되도록 설정되어 있지 않습니다. SNMP는 각 ESXi 호스트에서 구성되어야 합니다. ESXCLI, PowerCLI 또는 vSphere Web Services SDK를 사용하여 구성할 수 있습니다.

SNMP v3을 포함한 SNMP 구성에 대한 자세한 내용은 "vSphere 모니터링 및 성능" 설명서를 참조하십시오. SNMP v3은 키 인증 및 암호화를 포함하여 SNMP v1 또는 SNMP v2c보다 강력한 보안을 제공합니다. `esxcli system snmp` 명령 옵션에 대한 자세한 내용은 "ESXCLI 참조" 의 내용을 참조하십시오.

절차

1 SNMP가 사용되는지 여부를 확인하려면 다음 명령을 실행합니다.

```
esxcli system snmp get
```

2 SNMP를 사용하도록 설정하려면 다음 명령을 실행합니다.

```
esxcli system snmp set --enable true
```

3 SNMP를 사용하지 않도록 설정하려면 다음 명령을 실행합니다.

```
esxcli system snmp set --enable false
```

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.

- STP(스패닝 트리 프로토콜)는 네트워크 토폴로지에서 루프가 형성되는 것을 감지하고 방지합니다. VMware 가상 스위치는 다른 방식으로 루프를 방지하지만 STP를 직접 지원하지는 않습니다. 네트워크 토폴로지가 변경되면 네트워크가 토폴로지를 재학습하는 동안 약간의 시간(30~50초)이 필요합니다. 이 시간 동안은 어떤 트래픽도 전달할 수 없습니다. 이러한 문제를 방지하기 위해 네트워크 벤더는 스위치 포트를 사용하도록 설정하여 트래픽을 계속 전달하는 기능을 생성했습니다. 자세한 내용은 https://kb.vmware.com/kb/1003804에서 VMware 기술 자료 문서를 참조하십시오. 적절한 네트워크 및 네트워킹 하드웨어 구성에 대해서는 네트워크 벤더 설명서를 참조하십시오.
- Distributed Virtual Switch에 대한 Netflow 트래픽이 인증된 수집기 IP 주소로만 전송되는지 확인하십시오. Netflow 내보내기는 암호화되지 않고 가상 네트워크에 대한 정보를 포함할 수 있으며, 이런 정보로 인해 중요한 정보가 전송되는 동안 공격자가 보고 캡처할 수 있는 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 관리자 액세스 권한이 있어야 하지만 가상 시스템에 대한 액세스 권한은 없어야 합니다. 액세스를 제한하면 실수든 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 주로 네이티브 VLAN으로 구성되며, 이런 네이티브 VLAN은 기본적으로 VLAN 1인 경우가 많습니다. 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 지정됩니다. 결과적으로 태그가 해제되는 대신 1로 지정되었으므로 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 거부가 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 재정의를 제한합니다. 포트 수준 구성 재정의는 기본적으로 사용하지 않도록 설정됩니다. 재정의를 사용하도록 설정한 경우 가상 시스템에 대해 포트 그룹 수준 설정과 다른 보안 설정을 사용할 수 있습니다. 특정 가상 시스템에는 고유한 구성이 필요하지만 반드시 모니터링해야 합니다. 재정의를 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 적절히 구성해야 합니다. 물리적 스위치가 제대로 구성되지 않으면 VLAN 802.1q 헤더가 포함된 프레임이 도착을 예상하지 않은 스위치로 전달됩니다.

네트워크 분리 방식 채택

네트워크 분리 방식을 사용하면 vSphere 환경의 네트워크 보안이 강화됩니다.

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 VM의 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.

공통 표준 스위치의 전용 VLAN에 vSphere 관리 포트 그룹을 배치합니다. vSphere 관리 포트 그룹의 VLAN이 운영 VM에 의해 사용되지 않는 경우 표준 스위치를 운영(VM) 트래픽과 공유할 수 있습니다.

기타 관리 관련 엔티티가 발견된 네트워크를 제외하고, 네트워크 세그먼트가 라우팅되지 않았는지 확인합니다. 네트워크 세그먼트 라우팅은 vSphere Replication에 적절할 수 있습니다. 특히, 이 네트워크에 운영 VM 트래픽을 라우팅할 수 없어야 합니다.

다음 접근 방식 중 하나를 사용하여 관리 기능에 대한 액세스를 엄격하게 제어합니다.

- 특히 중요한 환경에서 관리 네트워크에 액세스하려면 제어된 게이트웨이 또는 기타 제어된 방법을 구성합니다. 예를 들어 관리자가 VPN을 통해 관리 네트워크에 연결하도록 요구하고 신뢰할 수 있는 관리자에게만 관리 네트워크에 대한 액세스를 허용합니다.
- 관리 클라이언트를 실행하는 베스천 호스트를 구성합니다.

스토리지 트래픽 분리

IP 기반 스토리지 트래픽이 분리되었는지 확인합니다. IP 기반 스토리지에는 iSCSI 및 NFS가 포함됩니다. VM은 IP 기반 스토리지 구성을 통해 가상 스위치 및 VLAN을 공유할 수 있습니다. 이러한 구성 유형은 IP 기반 스토리지 트래픽을 허용되지 않은 VM 사용자에게 노출할 수 있습니다.

IP 기반 스토리지는 대개 암호화되어 있지 않습니다. 이 네트워크에 대한 액세스 권한이 있는 사용자면 누구든지 IP 기반 스토리지 트래픽을 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 VM의 메모리 컨텐츠를 얻을 수 있습니다. 또한 잠재적 공격자는 마이그레이션 동안 컨텐츠가 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 그룹에 일반적인 표준 스위치의 전용 VLAN을 사용합니다. vMotion 포트 그룹의 VLAN이 운영 VM에 의해 사용되지 않는 경우 동일한 표준 스위치를 운영(VM) 트래픽에서 사용할 수 있습니다.

vSAN 트래픽 분리

vSAN 네트워크를 구성할 때 vSAN 트래픽을 고유한 계층 2 네트워크 세그먼트에서 분리합니다. 전용 스위치 또는 포트를 사용하거나 VLAN을 사용하여 이러한 분리를 수행할 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 API가 사용하도록 설정된 경우 공격자가 가상 시스템을 필터에 연결하려고 시도할 수 있으며, 연결되는 경우 공격자가 호스트에 있는 다른 가상 시스템의 네트워크에 액세스할 수 있습니다.

이 API를 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 API를 사용하도록 설정된 경우 `Net.DVFilterBindIpAddress` 매개 변수의 값이 이 API를 사용하는 제품과 일치하는지 확인해야 합니다.

절차

1. vSphere Client 인벤토리에서 호스트를 찾습니다.
2. **구성**을 클릭합니다.
3. 시스템 아래에서 **고급 시스템 설정**을 클릭합니다.
4. 아래로 스크롤하여 `Net.DVFilterBindIpAddress`를 찾은 다음 매개 변수의 값이 비어 있는지 확인합니다.

   매개 변수의 순서는 엄격히 사전순으로 정렬되어 있지 않습니다. 필터 텍스트 상자에 **`DVFilter`**를 입력하여 모든 관련 매개 변수를 표시합니다.
5. 설정을 확인합니다.
   - DvFilter 설정을 사용하지 않는 경우 값이 비어 있는지 확인합니다.
   - DvFilter 설정을 사용하는 경우 매개 변수 값이 정확한지 확인합니다. 값이 DvFilter를 사용하는 제품에서 사용 중인 값과 일치해야 합니다.

여러 vSphere 구성 요소와 관련된 모범 사례

14

환경에서 PTP 또는 NTP 설정과 같은 일부 보안 모범 사례는 둘 이상의 vSphere 구성 요소에 영향을 줍니다. 환경을 구성할 때 다음 권장 사항을 고려하십시오.

관련 정보는 장 3 ESXi 호스트 보안 및 장 5 가상 시스템 보안의 내용을 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 Client에 대한 시간 제한 설정

vSphere 네트워크에서 클럭 동기화

vSphere 네트워크에 있는 모든 구성 요소의 클럭이 동기화되었는지 확인합니다. vSphere 네트워크에 있는 물리적 시스템의 클럭이 동기화되지 않으면 시간에 민감한 SSL 인증서 및 SAML 토큰이 네트워크 시스템 간 통신에서 유효하지 않은 것으로 인식될 수 있습니다.

클럭이 동기화되지 않으면 인증 문제가 발생하여 설치가 실패하거나 vCenter Server `vmware-vpxd` 서비스를 시작하지 못할 수 있습니다.

vSphere에서 시간 불일치가 발생하면 환경 시간이 정확하지 않은 경우와 시간이 동기화되지 않은 경우에 따라 여러 서비스에서 첫 번째 부팅이 실패할 수 있습니다. 문제는 대상 vCenter Server에 대한 대상 ESXi 호스트가 NTP 또는 PTP와 동기화되지 않은 경우 가장 많이 발생합니다. 이와 유사하게 완전 자동화된 DRS로 인해 다른 시간으로 설정된 ESXi 호스트로 대상 vCenter Server가 마이그레이션되는 경우에도 문제가 발생할 수 있습니다.

시간 동기화 문제를 방지하려면 vCenter Server를 설치, 마이그레이션 또는 업그레이드하기 전에 다음이 올바른지 확인하십시오.

- 대상 vCenter Server를 배포할 대상 ESXi 호스트가 NTP 또는 PTP와 동기화되었습니다.
- 소스 vCenter Server를 실행하는 ESXi 호스트가 NTP 또는 PTP와 동기화되었습니다.
- vSphere 6.5 또는 6.7에서 vSphere 7.0으로 업그레이드 또는 마이그레이션 시 vCenter Server Appliance가 외부 Platform Services Controller에 연결되었다면 외부 Platform Services Controller를 실행하는 ESXi 호스트가 NTP 또는 PTP와 동기화되었는지 확인합니다.

- vSphere 6.5 또는 6.7에서 vSphere 7.0으로 업그레이드 또는 마이그레이션하는 경우 소스 vCenter Server 또는 vCenter Server Appliance 및 외부 Platform Services Controller의 시간이 정확해야 합니다.
- 외부 Platform Services Controller가 있는 vCenter Server 6.5 또는 6.7 인스턴스를 vSphere 7.0으로 업그레이드하면 업그레이드 프로세스를 통해 내장형 Platform Services Controller가 있는 vCenter Server 인스턴스로 변환됩니다.

vCenter Server가 실행되는 모든 Windows 호스트 시스템이 NTP(Network Time Server) 서버와 동기화되었는지 확인하십시오. VMware 기술 자료 문서(https://kb.vmware.com/s/article/1318)를 참조하십시오.

ESXi 클럭을 NTP 서버 또는 PTP와 동기화하려면 VMware Host Client를 사용할 수 있습니다. ESXi 호스트의 시간 구성 편집에 대한 자세한 내용은 "vSphere 단일 호스트 관리 - VMware Host Client" 를 참조하십시오.

vCenter Server에 대한 시간 동기화 설정을 변경하는 방법을 알아보려면 "vCenter Server 구성" 에서 "시스템 표준 시간대 및 시간 동기화 설정 구성"을 참조하십시오.

vSphere Client를 사용하여 호스트에 대한 시간 구성을 편집하는 방법에 대한 자세한 내용은 "vCenter Server 및 호스트 관리" 에서 "호스트에 대한 시간 구성 편집"을 참조하십시오.

- 네트워크 시간 서버와 ESXi 클럭 동기화

  vCenter Server를 설치하기 전에 vSphere 네트워크의 모든 시스템에서 해당 클럭을 동기화해야 합니다.
- vCenter Server에서 시간 동기화 설정 구성

  배포 후에 vCenter Server에서 시간 동기화 설정을 변경할 수 있습니다.

네트워크 시간 서버와 ESXi 클럭 동기화

vCenter Server를 설치하기 전에 vSphere 네트워크의 모든 시스템에서 해당 클럭을 동기화해야 합니다.

이 작업은 VMware Host Client에서 NTP를 설정하는 방법을 설명합니다.

절차

1. VMware Host Client를 시작하고 ESXi 호스트에 연결합니다.
2. **관리**를 클릭합니다.
3. **시스템**에서 **시간 및 날짜**를 클릭하고 **설정 편집**을 클릭합니다.
4. **네트워크 시간 프로토콜 사용(NTP 클라이언트 사용)**을 선택합니다.
5. [NTP 서버] 텍스트 상자에서 동기화할 하나 이상의 NTP 서버의 IP 주소나 FQDN(정규화된 도메인 이름)을 입력합니다.
6. **NTP 서비스 시작 정책** 드롭다운 메뉴에서 **호스트와 함께 시작 및 중지**를 선택합니다.

7 **저장**을 클릭합니다.

호스트가 NTP 서버와 동기화됩니다.

vCenter Server에서 시간 동기화 설정 구성

배포 후에 vCenter Server에서 시간 동기화 설정을 변경할 수 있습니다.

vCenter Server를 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 Server를 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 Server에서 한 가지 형태의 정기 시간 동기화만 사용할 수 있습니다. 기본적으로 제공되는 시간 동기화 소프트웨어와 vCenter Server VMware Tools 정기 시간 동기화 중에서 하나를 사용하기로 결정하면 다른 하나는 해제됩니다.

VMware Tools 시간 동기화 사용

VMware Tools 시간 동기화를 사용하도록 vCenter Server를 설정할 수 있습니다.

절차

1 장치 셸에 액세스하고 관리자 또는 수퍼 관리자 역할을 가진 사용자로 로그인합니다.

수퍼 관리자 역할의 기본 사용자는 루트입니다.

2 명령을 실행하여 VMware Tools 시간 동기화를 사용하도록 설정합니다.

```
timesync.set --mode host
```

3 (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 구성에서 NTP 서버 추가 또는 바꾸기

NTP 기반 시간 동기화를 사용하도록 vCenter Server를 설정하려면 NTP 서버를 vCenter Server 구성에 추가해야 합니다.

절차

1 장치 셸에 액세스하고 관리자 또는 수퍼 관리자 역할을 가진 사용자로 로그인합니다.

수퍼 관리자 역할의 기본 사용자는 루트입니다.

2 다음 `ntp.set` 명령을 사용하여 NTP 서버를 vCenter Server 구성에 추가합니다.

```
ntp.set --servers IP-addresses-or-host-names
```

명령에서 *IP-addresses-or-host-names*는 NTP 서버의 IP 주소 또는 호스트 이름을 쉼표로 구분한 목록입니다.

이 명령은 현재 NTP 서버(있는 경우)를 제거하고 새 NTP 서버를 구성에 추가합니다. 시간 동기화가 NTP 서버를 기반으로 하는 경우에는 새 NTP 서버를 다시 불러오기 위해 NTP 데몬이 다시 시작됩니다. 그렇지 않으면 이 명령은 NTP 구성의 현재 NTP 서버를 지정한 새 NTP 서버로 바꿉니다.

3 (선택 사항) 새로운 NTP 구성 설정이 적용되었는지 확인하려면 다음 명령을 실행합니다.

```
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.

4 (선택 사항) NTP 서버에 연결할 수 있는지 확인하려면 다음 명령을 실행합니다.

```
ntp.test --servers IP-addresses-or-host-names
```

이 명령은 NTP 서버의 상태를 반환합니다.

다음에 수행할 작업

NTP 동기화가 사용되지 않는 경우 vCenter Server에서 NTP 서버를 기반으로 하도록 시간 동기화 설정을 구성할 수 있습니다. NTP 서버와 vCenter Server의 시간 동기화의 내용을 참조하십시오.

NTP 서버와 vCenter Server의 시간 동기화

vCenter Server에서 NTP 서버를 기반으로 하도록 시간 동기화 설정을 구성할 수 있습니다.

사전 요구 사항

vCenter Server 구성에서 하나 이상의 NTP(네트워크 시간 프로토콜) 서버를 설정합니다. vCenter Server 구성에서 NTP 서버 추가 또는 바꾸기의 내용을 참조하십시오.

절차

1 장치 셸에 액세스하고 관리자 또는 수퍼 관리자 역할을 가진 사용자로 로그인합니다.

수퍼 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 vSAN 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 액세스하고, SCSI 디바이스에 직접 연결하는 대신 네트워크 포트를 통한 TCP/IP를 사용하여 데이터를 교환할 수 있도록 지원합니다. iSCSI 트랜잭션은 원시 SCSI 데이터 블록을 iSCSI 레코드에 캡슐화하고 요청한 디바이스 또는 사용자에게 데이터를 전송합니다.

iSCSI SAN은 동적으로 공유할 수 있는 스토리지 리소스에 대한 액세스를 호스트에 제공하여 기존 이더넷 인프라를 효율적으로 사용할 수 있도록 지원합니다. iSCSI SAN은 공통 스토리지 풀을 사용하여 많은 사용자에게 스토리지를 제공하는 환경을 위한 경제적인 스토리지 솔루션입니다. 네트워크로 연결된 다른 시스템과 마찬가지로 iSCSI SAN은 보안 침해의 대상이 될 수 있습니다.

참고 iSCSI SAN을 보호하기 위한 요구 사항 및 절차는 호스트에 연결된 하드웨어 iSCSI 어댑터와 호스트를 통해 직접 구성한 iSCSI에 대한 요구 사항 및 절차와 유사합니다.

iSCSI 장치 보안

iSCSI 디바이스를 보호하기 위해 ESXi 호스트(또는 이니시에이터)가 대상 LUN의 데이터에 액세스하려고 할 때마다 대상(iSCSI 디바이스)으로 하여금 호스트를 인증하도록 요구할 수 있습니다.

인증을 통해 이니시에이터에 대상에 액세스할 수 있는 권한이 있는지 확인할 수 있습니다. 이러한 권한은 iSCSI 디바이스에 대한 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 암호를 서로 다르게 설정합니다. 가능한 경우 ESXi 호스트와 다른 인증 암호를 각 클라이언트에 대해 설정합니다. 각기 고유한 암호를 설정하면 단일 호스트가 손상되어도 공격자가 다른 임의 호스트를 생성하여 스토리지 디바이스에 인증할 수 없습니다. 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 위험은 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 정체가 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 사용

NFS 버전 4.1에서 ESXi는 Kerberos 인증 메커니즘을 지원합니다.

RPCSEC_GSS Kerberos 메커니즘은 인증 서비스입니다. 이를 통해 NFS 공유를 마운팅하기 전에 ESXi에 설치된 NFS 4.1 클라이언트가 NFS 서버에 대한 해당 ID를 입증할 수 있습니다. Kerberos 보안은 안전하지 않은 네트워크 연결에서 작업하기 위해 암호화를 사용합니다.

NFS 4.1에 대한 Kerberos의 ESXi 구현은 각기 다른 보안 수준을 제공하는 2개의 보안 모델인 krb5와 krb5i를 제공합니다.

- 인증을 위한 Kerberos(krb5)는 ID 확인만 지원합니다.
- 인증 및 데이터 무결성을 위한 Kerberos(krb5i)는 ID 확인 외에도 데이터 무결성 서비스를 제공합니다. 이러한 서비스를 사용하면 잠재적 수정에 대한 데이터 패킷을 확인하여 NFS 트래픽 변조를 방지할 수 있습니다.

Kerberos는 인증되지 않은 사용자가 NFS 트래픽에 대한 액세스를 권한을 획득하는 것을 방지하는 암호화 알고리즘을 지원합니다. ESXi에 대한 NFS 4.1 클라이언트는 AES256-CTS-HMAC-SHA1-96 또는 AES128-CTS-HMAC-SHA1-96 알고리즘을 사용하여 NAS 서버에 대한 공유에 액세스하려고 시도합니다. NFS 4.1 데이터스토어를 사용하기 전에 AES256-CTS-HMAC-SHA1-96 또는 AES128-CTS-HMAC-SHA1-96이 NAS 서버에서 사용되도록 설정되었는지 확인합니다.

다음 표에서는 ESXi가 지원하는 Kerberos 보안 수준을 비교합니다.

표 14-1. Kerberos 보안 유형

		ESXi 6.0	ESXi 6.5 이상
인증 전용 Kerberos(krb5)	RPC 머리글에 대한 무결성 체크섬	DES에 대해 예	AES에 대해 예
	RPC 데이터에 대한 무결성 체크섬	아니요	아니요

표 14-1. Kerberos 보안 유형 (계속)

		ESXi 6.0	ESXi 6.5 이상
인증 및 데이터 무결성을 위한 Kerberos(krb5i)	RPC 머리글에 대한 무결성 체크섬	krb5i 없음	AES에 대해 예
	RPC 데이터에 대한 무결성 체크섬		AES에 대해 예

Kerberos 인증을 사용할 때 다음 고려 사항이 적용됩니다.

- ESXi는 Active Directory 도메인과 함께 Kerberos를 사용합니다.
- vSphere 관리자는 Active Directory 자격 증명을 지정하여 NFS 사용자에 대해 NFS 4.1 Kerberos 데이터스토어에 대한 액세스를 제공합니다. 해당 호스트에 마운트된 모든 Kerberos 데이터스토어에 액세스하기 위해 단일 자격 증명 집합이 사용됩니다.
- 여러 ESXi 호스트가 NFS 4.1 데이터스토어를 공유하는 경우, 공유 데이터스토어에 액세스하는 모든 호스트에 대해 동일한 Active Directory 자격 증명을 사용해야 합니다. 할당 프로세스를 자동화하려면 호스트 프로파일의 사용자를 설정하고 해당 프로파일을 모든 ESXi 호스트에 적용합니다.
- 여러 호스트가 공유하는 동일한 NFS 4.1 데이터스토어에 대해 2개의 보안 메커니즘인 AUTH_SYS와 Kerberos를 사용할 수 없습니다.

단계별 지침은 "vSphere 스토리지" 설명서를 참조하십시오.

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.

기본적으로 호스트 성능 데이터를 가상 시스템에 전송하는 기능은 사용하지 않도록 설정되어 있습니다. 이 기본 설정을 통해 가상 시스템은 물리적 호스트에 대한 세부 정보를 가져올 수 없습니다. 가상 시스템에서 보안 침해가 발생한 경우 이 설정에 따라 공격자가 호스트 데이터를 사용할 수 없게 됩니다.

참고 다음 절차는 기본 프로세스를 보여줍니다. 모든 호스트에서 동시에 이 작업을 수행하려면 ESXCLI 또는 VMware PowerCLI 명령을 사용하는 것이 좋습니다.

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 Client에 대한 시간 제한 설정

침입자가 유휴 세션을 사용하지 못하도록 하려면 ESXi Shell 및 vSphere Client에 대한 시간 제한을 설정해야 합니다.

ESXi Shell 시간 제한

ESXi Shell의 경우 vSphere 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.

유휴 시간 제한

유휴 시간 초과는 사용자가 유휴 대화형 세션에서 로그아웃할 때까지의 최대 대기 시간입니다. 유휴 시간 초과에 대한 변경 내용은 사용자가 다음에 ESXi Shell에 로그인할 때 적용됩니다. 변경 내용은 기존 세션에 영향을 미치지 않습니다.

vSphere Client 시간 제한

vSphere Client 세션은 기본적으로 120분 후에 종료됩니다. 기본값을 변경하려면:

1 vSphere Client에서 vCenter Server 인스턴스로 이동합니다.

2 **구성** 탭을 선택하고 **설정**에서 **일반**을 선택합니다.

3 **편집**을 클릭합니다.

4 **시간 초과 설정**을 선택합니다.

5 선택 사항을 입력하고 **저장**을 클릭합니다.

TLS 구성 유틸리티를 사용하여 TLS 프로토콜 구성 관리

15

vSphere는 기본적으로 TLS만 사용합니다. TLS 1.0과 TLS 1.1은 기본적으로 사용되지 않도록 설정됩니다. 새로 설치하든 업그레이드하든 마이그레이션하든 관계없이 vSphere에서는 TLS 1.0과 TLS 1.1이 사용되지 않도록 설정됩니다. TLS 구성 유틸리티를 사용하여 vSphere 시스템에서 일시적으로 이전 버전의 프로토콜을 사용하도록 설정할 수 있습니다. 모든 연결에 TLS 1.2가 사용된 후에 보안이 더 낮은 이전 버전을 사용하지 않도록 설정할 수 있습니다.

재구성을 수행하기 전에 환경을 고려하십시오. 환경 요구 사항 및 소프트웨어 버전에 따라 상호 운용성을 유지하기 위해 TLS 1.2 이외에 TLS 1.0과 TLS 1.1을 다시 사용하도록 설정해야 할 수 있습니다. VMware 제품의 경우 VMware 기술 자료 문서 https://kb.vmware.com/s/article/2145796에서 TLS 1.2를 지원하는 VMware 제품 목록을 참조하십시오. 타사 통합의 경우 해당 벤더의 설명서를 참조하십시오. TLS 구성 유틸리티는 vSphere 7.0을 비롯하여 6.7, 6.5 및 6.0을 포함한 이전 릴리스에서 작동합니다.

본 장은 다음 항목을 포함합니다.

- TLS 버전을 사용하지 않도록 설정 가능한 포트
- vSphere에서 TLS 버전을 사용하거나 사용하지 않도록 설정
- 선택적 수동 백업 수행
- vCenter Server 시스템에서 TLS 버전을 사용하거나 사용하지 않도록 설정
- ESXi 호스트에서 TLS 버전을 사용하거나 사용하지 않도록 설정
- vCenter Server에서 사용하도록 설정된 TLS 프로토콜 검색
- TLS 구성 변경 내용 되돌리기

TLS 버전을 사용하지 않도록 설정 가능한 포트

vSphere 환경에서 TLS 구성 유틸리티를 실행하는 경우 vCenter Server 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.

vSphere 7.0부터 vCenter Server는 두 개의 역방향 프록시 서비스를 실행합니다.

- VMware 역방향 프록시 서비스, `rhttpproxy`
- 엔보이

엔보이는 오픈 소스 Edge 및 서비스 프록시입니다. 엔보이는 포트 443을 소유하며, 들어오는 모든 vCenter Server 요청은 엔보이를 통해 라우팅됩니다. vSphere 7.0에서 `rhttpproxy`는 엔보이를 위한 구성 관리 서버 역할을 합니다. 그 결과 TLS 구성이 `rhttpproxy`에 적용되고 여기에서 구성을 엔보이에 전송합니다.

vCenter Server 및 ESXi는 TLS 프로토콜에 사용하거나 사용하지 않도록 설정할 수 있는 포트를 사용합니다. TLS 구성 유틸리티 `scan` 옵션은 각 서비스에 대해 사용되도록 설정된 TLS 버전을 표시합니다. vCenter Server에서 사용하도록 설정된 TLS 프로토콜 검색의 내용을 참조하십시오.

vSphere 및 vSAN을 포함한 VMware 제품의 지원되는 모든 포트 및 프로토콜 목록은 https://ports.vmware.com/에서 VMware Ports and Protocols Tool™을 참조하십시오. VMware 제품별로 포트를 검색하고, 사용자 지정된 포트 목록을 생성하고, 포트 목록을 인쇄하거나 저장할 수 있습니다.

참고 사항 및 주의 사항

- vSphere 6.7 릴리스는 Windows용 vCenter Server의 최종 릴리스입니다. Windows용 vCenter Server에서 Update Manager 포트에 대한 TLS를 다시 구성하는 방법에 대한 자세한 내용은 6.7 제품 버전의 "vSphere 보안" 설명서를 참조하십시오.
- TLS 1.2를 사용하여 vCenter Server와 외부 Microsoft SQL Server 간의 연결을 암호화할 수 있습니다. 외부 Oracle 데이터베이스에는 TLS 1.2 단독 연결을 사용할 수 없습니다. VMware 기술 자료 문서(https://kb.vmware.com/kb/2149745)를 참조하십시오.
- vSphere 6.7 이전 릴리스의 경우, Windows Server 2008에서 실행되는 vCenter Server 또는 Platform Services Controller 인스턴스에서 TLS 1.0이 사용되지 않도록 설정하지 마십시오. Windows 2008은 TLS 1.0만 지원합니다. Microsoft TechNet 문서 "서버 역할 및 기술 가이드" 의 "TLS/SSL 설정" 을 참조하십시오.
- TLS 프로토콜을 변경하는 경우 변경 내용을 적용하기 위해 ESXi 호스트를 다시 시작해야 합니다. 호스트 프로파일을 사용하여 클러스터 구성을 통해 변경 내용을 적용하는 경우에도 호스트를 다시 시작 해야 합니다. 즉시 호스트를 다시 시작하거나 더 편리한 시간에 다시 시작하도록 선택할 수 있습니다.

vSphere에서 TLS 버전을 사용하거나 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.

vSphere Lifecycle Manager는 항상 vCenter Server 시스템에 포함되어 있으며 스크립트를 통해 해당 포트가 업데이트됩니다.

1 vCenter Server에서 TLS 구성 유틸리티를 실행합니다.

2 vCenter Server로 관리되는 각 ESXi 호스트에서 TLS 구성 유틸리티를 실행합니다. 각 호스트 또는 클러스터의 모든 호스트에 대해 이 작업을 수행할 수 있습니다.

사전 요구 사항

사용자 환경에서TLS를 사용하는 방법에는 두 가지가 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

선택적 수동 백업 수행

TLS 구성 유틸리티는 스크립트를 통해 vCenter Server가 수정될 때마다 백업을 수행합니다. 특정 디렉토리에 백업을 수행해야 할 경우 수동 백업을 수행할 수 있습니다.

ESXi 구성의 백업은 지원되지 않습니다.

vCenter Server의 경우 기본 디렉토리는 /tmp/*yearmonthday*T*time*입니다.

절차

1 디렉토리를 /usr/lib/vmware-TlsReconfigurator/VcTlsReconfigurator로 변경합니다.

2 특정 디렉토리에 백업하려면 다음 명령을 실행합니다.

```
directory_path/VcTlsReconfigurator> ./reconfigureVc backup -d backup_directory_path
```

3 백업이 성공적으로 완료되었는지 확인합니다.

백업에 성공하면 다음 예와 유사하게 표시됩니다. reconfigureVc backup 명령이 실행되는 방식 때문에 이 명령을 실행할 때마다 표시되는 서비스 순서가 다를 수 있습니다.

```
vCenter Transport Layer Security reconfigurator, version=7.0.0, build=15518531
For more information refer to the following article: https://kb.vmware.com/kb/2147469
Log file: "/var/log/vmware/vSphere-TlsReconfigurator/VcTlsReconfigurator.log".
================= Backing up vCenter Server TLS configuration ==================
Using backup directory: /tmp/20200206T183550
Backing up: vmware-rbd-watchdog
Backing up: vmware-vpxd
Backing up: vmcam
Backing up: vmware-stsd
Backing up: vmdird
Backing up: vmware-sps
Backing up: vmware-rhttpproxy
Backing up: vami-lighttp
Backing up: vmware-updatemgr
Backing up: rsyslog
```

4 (선택 사항) 이후에 복원을 수행해야 할 경우 다음 명령을 실행할 수 있습니다.

```
reconfigureVc restore -d optional_custom_backup_directory_path
```

vCenter Server 시스템에서 TLS 버전을 사용하거나 사용하지 않도록 설정

TLS 구성 유틸리티를 사용하여 vCenter Server 시스템에서 TLS 버전을 사용하지 않도록 설정할 수 있습니다. 프로세스의 일부로 TLS 1.0을 사용하지 않도록 설정하고 TLS 1.1 및 TLS 1.2를 사용하도록 설정하거나, TLS 1.0 및 TLS 1.1을 사용하지 않도록 설정하고 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 Administrator@vsphere.local 또는 스크립트를 실행할 수 있는 vCenter Single Sign-On 관리자 그룹에 속한 다른 멤버의 사용자 이름과 암호를 사용하여 vCenter Server 시스템에 로그인합니다.

2 스크립트가 있는 디렉토리로 이동합니다.

```
cd /usr/lib/vmware-TlsReconfigurator/VcTlsReconfigurator
```

3 사용할 TLS 버전에 따라 명령을 실행합니다.

- TLS 1.0을 사용하지 않도록 설정하고 TLS 1.1과 TLS 1.2를 모두 사용하도록 설정하려면 다음 명령을 실행합니다.

```
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.

```
directory_path/VcTlsReconfigurator> ./reconfigureVc update -p TLSv1.2
```

4 다른 vCenter Server 시스템이 환경에 포함되어 있는 경우 각 vCenter Server 시스템에서 이 프로세스를 반복합니다.

5 각 ESXi 호스트에 대해 구성을 반복합니다.

ESXi 호스트에서 TLS 버전을 사용하거나 사용하지 않도록 설정

TLS 구성 유틸리티를 사용하여 ESXi 호스트에서 TLS 버전을 사용하지 않도록 설정할 수 있습니다. 프로세스의 일부로 TLS 1.0을 사용하지 않도록 설정하고 TLS 1.1 및 TLS 1.2를 사용하도록 설정하거나, TLS 1.0 및 TLS 1.1을 사용하지 않도록 설정하고 TLS 1.2만 사용하도록 설정할 수 있습니다.

ESXi 호스트의 경우 vSphere 환경의 나머지 구성 요소와 다른 유틸리티를 사용합니다. 이 유틸리티는 해당 릴리스 전용이며 이전 릴리스에는 사용할 수 없습니다.

스크립트를 작성하여 여러 호스트를 구성할 수 있습니다.

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.

vCenter Server Appliance에서 Bash 셸을 사용하도록 설정해야 합니다.

절차

1. SSH를 사용하여 스크립트를 실행할 수 있는 vCenter Single Sign-On 사용자의 사용자 이름과 암호로 vCenter Server Appliance에 연결합니다.
2. Bash 셸을 사용하도록 설정하려면 명령줄에 **shell**을 입력합니다.
3. 스크립트가 있는 디렉토리로 이동합니다.

   ```
   cd /usr/lib/vmware-TlsReconfigurator/EsxTlsReconfigurator
   ```

4. 클러스터에 속한 ESXi 호스트에서 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.

     ```
     ./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.

     ```
     ./reconfigureEsx vCenterCluster -c Cluster_Name -u Administrative_User -p TLSv1.2
     ```

5. 클러스터에 속하지 않은 개별 호스트의 경우 다음 명령 중 하나를 실행합니다.
   - 개별 호스트에 대해 TLS 1.0을 사용하지 않도록 설정하고 TLS 1.1과 TLS 1.2를 모두 사용하도록 설정하려면 다음 명령을 실행합니다.

     ```
     ./reconfigureEsx vCenterHost -h ESXi_Host_Name -u Administrative_User -p TLSv1.1
     TLSv1.2
     ```

- 개별 호스트에 대해 TLS 1.0과 TLS 1.1을 사용하지 않도록 설정하고 TLS 1.2만 사용하도록 설정하려면 다음 명령을 실행합니다.

  ```
  ./reconfigureEsx vCenterHost -h ESXi_Host_Name -u Administrative_User -p TLSv1.2
  ```

  참고 독립형 ESXi 호스트를 재구성하려면 vCenter Server 시스템에 로그인하고 `reconfigureEsx` 명령을 `ESXiHost -h` *HOST* `-u` *ESXi_ USER* 옵션과 함께 실행합니다. *HOST* 옵션에서 단일 ESXi 호스트의 IP 주소 또는 FQDN이나 호스트 IP 주소 또는 FQDN 목록을 지정할 수 있습니다. 예를 들어 vCenter Server에 로그인하고 다음 명령을 실행하면 두 개의 ESXi 호스트에서 TLS 1.1과 TLS 1.2가 모두 사용되도록 설정됩니다.

  ```
  ./reconfigureEsx ESXiHost -h 198.51.100.2 198.51.100.3 -u root -p TLSv1.1 TLSv1.2
  ```

  또는 독립형 ESXi 호스트를 재구성하려면 호스트에 로그인하고 `UserVars.ESXiVPsDisabledProtocols` 고급 설정을 수정하면 됩니다. 자세한 내용은 "vSphere 단일 호스트 관리 - VMware Host Client" 설명서에서 "고급 TLS/SSL 키 옵션 구성" 항목을 참조하십시오.

6 ESXi 호스트를 재부팅하여 TLS 프로토콜 변경을 완료합니다.

vCenter Server에서 사용하도록 설정된 TLS 프로토콜 검색

vCenter Server에서 TLS 버전을 사용하거나 사용하지 않도록 설정한 후 TLS 구성 유틸리티를 사용하여 변경 사항을 확인할 수 있습니다.

TLS 구성 유틸리티 `scan` 옵션은 각 서비스에 대해 사용되도록 설정된 TLS 버전을 표시합니다.

절차

1 vCenter Server 시스템에 로그인합니다.

   a SSH를 사용하여 장치에 연결하고 스크립트를 실행할 수 있는 권한이 있는 사용자로 로그인합니다.

   b bash 셸이 현재 사용되지 않는 경우 다음 명령을 실행합니다.

   ```
   shell.set --enabled true
   shell
   ```

2 `VcTlsReconfigurator` 디렉토리로 이동합니다.

   ```
   cd /usr/lib/vmware-TlsReconfigurator/VcTlsReconfigurator
   ```

3 TLS가 사용되도록 설정된 서비스와 사용되는 포트를 표시하려면 다음 명령을 실행합니다.

   ```
   reconfigureVc scan
   ```

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.

사전 요구 사항

변경 내용을 되돌리기 전에 vCenter Server 관리 인터페이스를 사용하여 vCenter Server의 백업을 수행합니다.

절차

1. 변경 내용을 스크립트를 실행할 수 있는 권한을 가진 사용자로 되돌릴 수 있는 vCenter Server에 연결합니다.
2. Bash 셸이 현재 사용되지 않는 경우 다음 명령을 실행합니다.

   ```
   shell.set --enabled true
   shell
   ```

3. `VcTlsReconfigurator` 디렉토리로 이동합니다.

   ```
   cd /usr/lib/vmware-TlsReconfigurator/VcTlsReconfigurator
   ```

4. 이전 백업을 검토합니다.

   ```
   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
   ```

5. 복원을 수행하려면 다음 명령을 실행합니다.

   ```
   reconfigureVc restore -d Directory_path_from_previous_step
   ```

   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
   ```

6. 다른 vCenter Server 인스턴스에서 이 절차를 반복합니다.

정의된 권한

16

다음 표에는 기본 권한이 나와 있으며, 이러한 권한이 역할에 대해 선택되면 사용자와 쌍을 이루어 개체에 할당될 수 있습니다.

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.

- 경보 권한
- Auto Deploy 및 이미지 프로파일 권한
- 인증서 권한
- 인증 기관 권한
- 인증서 관리 권한
- Cns 권한
- 컨텐츠 라이브러리 권한
- 암호화 작업 권한
- dvPort 그룹 권한
- Distributed Switch 권한
- 데이터 센터 권한
- 데이터스토어 권한
- 데이터스토어 클러스터 권한
- ESX Agent Manager 권한
- 확장 권한
- 외부 통계 제공자 권한
- 폴더 권한

- 글로벌 권한
- 상태 업데이트 제공자 권한
- 호스트 CIM 권한
- 호스트 구성 권한
- 호스트 인벤토리
- 호스트 로컬 작업 권한
- 호스트 vSphere 복제 권한
- 호스트 프로파일 권한
- vSphere with Tanzu 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
- VcTrusts/VcIdentity 권한
- 신뢰할 수 있는 인프라 관리자 권한
- vApp 권한
- VcIdentityProviders 권한
- VMware vSphere Lifecycle Manager 구성 권한
- VMware vSphere Lifecycle Manager ESXi 상태 관점 권한
- VMware vSphere Lifecycle Manager 일반 권한
- VMware vSphere Lifecycle Manager 하드웨어 호환성 권한
- VMware vSphere Lifecycle Manager 이미지 권한
- VMware vSphere Lifecycle Manager 이미지 업데이트 적용 권한
- VMware vSphere Lifecycle Manager 설정 권한

- VMware vSphere Lifecycle Manager 기준선 관리 권한
- VMware vSphere Lifecycle Manager 패치 및 업그레이드 관리 권한
- VMware vSphere Lifecycle Manager 파일 업로드 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
- vServices 권한
- vSphere 태그 지정 권한
- vSphere Client 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 16-1. 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.엔티티에서 경보 사용 또는 사용 안 함	특정 대상 유형에서 특정 경보를 사용하거나 사용하지 않도록 설정할 수 있습니다.	경보가 트리거될 수 있는 개체
경보.경보 수정	경보의 속성을 변경할 수 있습니다.	경보가 정의된 개체

표 16-1. 경보 권한 (계속)

권한 이름	설명	필수
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. "vCenter Server 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 16-2. 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 수있습니다.	vCenter Server
Auto Deploy.이미지 프로파일.편집	이미지 프로파일을 편집할 수있습니다.	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 "vSphere 인증" 설명서의 인증서 관리 작업에 필요한 권한을 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 16-3. 호스트 인증서 권한

권한 이름	설명	필수
인증서.인증서 관리	ESXi 호스트에 대한 인증서 관리를 허용합니다.	vCenter Server

인증 기관 권한

CA(인증 기관) 권한은 VMCA(VMware Certificate Authority) 인증서의 측면을 제어합니다.

표 16-4. 인증 기관 권한

권한 이름	설명	필수
CA(인증 기관).생성/삭제(관리자 권한).	vCenter Server 인증서 관리를 위한 전체 관리 수준 액세스를 허용합니다.	vCenter Server
CA(인증 기관).생성/삭제(관리자 권한 아래).	vSphere Client의 [인증서 관리] 페이지에서 VMCA 루트 인증서를 볼 수 있습니다.	vCenter Server

인증서 관리 권한

인증서 관리 권한은 vCenter Server 인증서를 관리할 수 있는 사용자를 제어합니다.

표 16-5. 인증서 관리 권한

권한 이름	설명	필수
인증서 관리.생성/삭제(관리자 권한).	vCenter Server 인증서 관련 작업을 위한 다양한 내부 API 및 기능에 대한 전체 관리 수준 액세스를 허용합니다.	vCenter Server
인증서 관리.생성/삭제(관리자 권한 아래).	다양한 내부 API 및 기능에 대한 관리 액세스를 줄일 수 있습니다. 이 권한은 사용자가 관리자 이외의 사용자 권한을 승격할 수 없도록 인증서 관련 작업을 제한합니다. 허용되는 작업은 다음과 같습니다. ■ 인증서 서명 요청 생성 ■ 신뢰할 수 있는 루트 체인 생성 및 검색 ■ **인증서 관리.생성/삭제(관리자 권한 아래).** 권한이 있는 사용자가 생성한 신뢰할 수 있는 루트 체인 삭제 ■ 시스템 SSL 인증서 검색 ■ vCenter Server에서 발급된 토큰의 유효성을 검사하기 위해 서명 인증서 체인 검색	vCenter Server

Cns 권한

Cns(클라우드 네이티브 저장소) 권한은 클라우드 네이티브 스토리지 UI에 액세스할 수 있는 사용자를 제어합니다.

표 16-6. Cns 권한

권한 이름	설명	필수
CNS.검색 가능	스토리지 관리자가 클라우드 네이티브 스토리지 UI를 볼 수 있습니다.	루트 vCenter Server

컨텐츠 라이브러리 권한

컨텐츠 라이브러리를 통해 가상 시스템 템플릿 및 vApp를 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.

참고 컨텐츠 라이브러리에 대한 사용 권한 상속은 단일 vCenter Server 인스턴스의 컨텍스트에서 작동합니다. 그러나 컨텐츠 라이브러리는 인벤토리 관점에서 vCenter Server 시스템의 직속 하위 항목이 아닙니다. 컨텐츠 라이브러리에 대한 직속 상위 항목은 글로벌 루트입니다. 즉, vCenter Server 수준에서 사용 권한을 설정하고 하위 개체로 전파하면 해당 사용 권한이 데이터 센터, 폴더, 클러스터, 호스트, 가상 시스템 및 기타 항목에 적용되지만, vCenter Server 인스턴스에 표시되고 작동하는 컨텐츠 라이브러리에는 적용되지 않습니다. 컨텐츠 라이브러리에 대한 사용 권한을 할당하려면 관리자가 사용 권한을 사용자에게 글로벌 사용 권한으로 부여해야 합니다. 글로벌 사용 권한은 글로벌 루트 개체의 솔루션 전체에 대한 권한 할당을 지원합니다.

표 16-7. 컨텐츠 라이브러리 권한

권한 이름	설명	필수
컨텐츠 라이브러리.라이브러리 항목 추가	라이브러리의 항목을 추가할 수 있습니다.	라이브러리
컨텐츠 라이브러리.신뢰 저장소에 루트 인증서 추가	신뢰할 수 있는 루트 인증서 저장소에 루트 인증서를 추가할 수 있습니다.	vCenter Server
컨텐츠 라이브러리.템플릿 체크인	템플릿을 체크인할 수 있습니다.	라이브러리
컨텐츠 라이브러리.템플릿 체크아웃	템플릿을 체크아웃할 수 있습니다.	라이브러리
컨텐츠 라이브러리.게시된 라이브러리에 대한 구독 생성	라이브러리 구독을 생성할 수 있습니다.	라이브러리
컨텐츠 라이브러리.로컬 라이브러리 생성	지정된 vCenter Server 시스템에 로컬 라이브러리를 생성할 수 있습니다.	vCenter Server
컨텐츠 라이브러리.Harbor 레지스트리 생성 또는 삭제	VMware Tanzu Harbor 레지스트리 서비스를 생성하거나 삭제할 수 있습니다.	생성을 위해 vCenter Server에. 삭제를 위해 레지스트리에.
컨텐츠 라이브러리.구독 라이브러리 생성	구독 라이브러리를 생성할 수 있습니다.	vCenter Server

표 16-7. 컨텐츠 라이브러리 권한 (계속)

권한 이름	설명	필수
컨텐츠 라이브러리.Harbor 레지스트리 프로젝트 생성, 삭제 또는 제거	VMware Tanzu Harbor 레지스트리 프로젝트를 생성, 삭제 또는 제거할 수 있습니다.	레지스트리
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.신뢰 저장소에서 루트 인증서 삭제	신뢰할 수 있는 루트 인증서 저장소에서 루트 인증서를 삭제할 수 있습니다.	vCenter Server
컨텐츠 라이브러리.구독 라이브러리 삭제	구독 라이브러리를 삭제할 수 있습니다.	라이브러리
컨텐츠 라이브러리.게시된 라이브러리에 대한 구독 삭제	라이브러리 구독을 삭제할 수 있습니다.	라이브러리
컨텐츠 라이브러리.파일 다운로드	컨텐츠 라이브러리에서 파일을 다운로드할 수 있습니다.	라이브러리
컨텐츠 라이브러리.라이브러리 항목 제거	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.
컨텐츠 라이브러리.구독 라이브러리 제거	구독 라이브러리를 제거할 수 있습니다. 구독 라이브러리의 컨텐츠는 캐시되거나 캐시되지 않을 수 있습니다. 컨텐츠가 캐시된 경우 이 권한이 있으면 라이브러리를 제거하여 릴리스할 수 있습니다.	라이브러리
컨텐츠 라이브러리.스토리지 가져오기	소스 파일 URL이 `ds://` 또는 `file://`로 시작하는 경우 사용자가 라이브러리 항목을 가져올 수 있습니다. 이 권한은 컨텐츠 라이브러리 관리자에 대해 기본적으로 사용되지 않도록 설정되어 있습니다. 스토리지 URL에서 가져오기는 컨텐츠 가져오기를 의미하기 때문에 필요한 경우 및 현재 가져오기를 수행하는 사용자에 대해 보안이 우려되지 않는 경우에만 이 권한을 사용하도록 설정합니다.	라이브러리
컨텐츠 라이브러리.지정된 계산 리소스에서 Harbor 레지스트리 리소스 관리	VMware Tanzu Harbor 레지스트리 리소스를 관리할 수 있습니다.	계산 클러스터
컨텐츠 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
컨텐츠 라이브러리.해당 구독자에게 라이브러리 항목 게시	라이브러리 항목을 구독자에게 게시할 수 있습니다.	라이브러리. 모든 라이브러리 항목에 전파하기 위한 이 사용 권한을 설정합니다.

표 16-7. 컨텐츠 라이브러리 권한 (계속)

권한 이름	설명	필수
컨텐츠 라이브러리.해당 구독자에게 라이브러리 게시	라이브러리를 구독자에 게시할 수 있습니다.	라이브러리
컨텐츠 라이브러리.스토리지 읽기	컨텐츠 라이브러리 스토리지를 읽을 수 있습니다.	라이브러리
컨텐츠 라이브러리.라이브러리 항목 동기화	라이브러리 항목을 동기화할 수 있습니다.	라이브러리. 모든 라이브러리 항목에 전파하기 위한 이 사용 권한을 설정합니다.
컨텐츠 라이브러리.구독 라이브러리 동기화	구독 라이브러리를 동기화할 수 있습니다.	라이브러리
컨텐츠 라이브러리.유형 검사	솔루션 사용자 또는 API는 컨텐츠 라이브러리 서비스의 유형 지원 플러그인을 검사할 수 있습니다.	라이브러리
컨텐츠 라이브러리.구성 설정 업데이트	구성 설정을 업데이트할 수 있습니다. 이 권한과 연결된 vSphere Client 사용자 인터페이스 요소는 없습니다.	라이브러리
컨텐츠 라이브러리.파일 업데이트	컨텐츠를 컨텐츠 라이브러리로 업로드할 수 있습니다. 또한 라이브러리 항목에서 파일을 제거할 수 있습니다.	라이브러리
컨텐츠 라이브러리.라이브러리 업데이트	컨텐츠 라이브러리를 업데이트할 수 있습니다.	라이브러리
컨텐츠 라이브러리.라이브러리 항목 업데이트	라이브러리 항목을 업데이트할 수 있습니다.	라이브러리. 모든 라이브러리 항목에 전파하기 위한 이 사용 권한을 설정합니다.
컨텐츠 라이브러리.로컬 라이브러리 업데이트	로컬 라이브러리를 업데이트할 수 있습니다.	라이브러리
컨텐츠 라이브러리.구독 라이브러리 업데이트	구독 라이브러리 속성을 업데이트할 수 있습니다.	라이브러리
컨텐츠 라이브러리.게시된 라이브러리에 대한 구독 업데이트	구독 매개 변수를 업데이트할 수 있습니다. 사용자는 구독 라이브러리의 vCenter Server 인스턴스 규격 및 해당 가상 시스템 템플릿 항목의 배치와 같은 매개 변수를 업데이트할 수 있습니다.	라이브러리
컨텐츠 라이브러리.구성 설정 보기	구성 설정을 볼 수 있습니다. 이 권한과 연결된 vSphere Client 사용자 인터페이스 요소는 없습니다.	라이브러리

암호화 작업 권한

암호화 작업 권한은 누가 어떤 유형의 개체에서 어떤 유형의 암호화 작업을 수행할 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 16-8. 암호화 작업 권한

권한 이름	설명	필수
암호화 작업.직접 액세스	사용자가 암호화된 리소스에 액세스할 수 있습니다. 사용자는 가상 시스템을 내보내고, 가상 시스템에 대한 NFC 액세스 권한을 갖고, 암호화된 가상 시스템에 대한 콘솔 세션을 열 수 있습니다.	가상 시스템, 호스트 또는 데이터스토어
암호화 작업.디스크 추가	사용자가 암호화된 가상 시스템에 디스크를 추가할 수 있습니다.	가상 시스템
암호화 작업.복제	사용자가 암호화된 가상 시스템을 복제할 수 있습니다.	가상 시스템
암호화 작업.암호 해독	사용자가 가상 시스템 또는 디스크의 암호를 해독할 수 있습니다.	가상 시스템
암호화 작업.암호화	사용자가 가상 시스템 또는 가상 시스템 디스크를 암호화할 수 있습니다.	가상 시스템
암호화 작업.새 항목 암호화	사용자가 가상 시스템 생성 중 가상 시스템을 암호화하거나 디스크 생성 중 디스크를 암호화할 수 있습니다.	가상 시스템 폴더
암호화 작업.암호화 정책 관리	사용자가 암호화 IO 필터로 가상 시스템 스토리지 정책을 관리할 수 있습니다. 기본적으로 암호화 스토리지 정책을 사용하는 가상 시스템은 다른 스토리지 정책을 사용하지 않습니다.	vCenter Server 루트 폴더
암호화 작업.KMS 관리	사용자가 vCenter Server 시스템에 대한 키 관리 서버를 관리할 수 있습니다. 관리 작업에는 KMS 인스턴스 추가 및 제거, KMS와의 신뢰 관계 설정이 포함됩니다.	vCenter Server 시스템
암호화 작업.키 관리	사용자가 키 관리 작업을 수행할 수 있습니다. 이러한 작업은 vSphere Client에서 지원되지 않지만 `crypto-util` 또는 API를 사용하여 수행될 수 있습니다.	vCenter Server 루트 폴더
암호화 작업.마이그레이션	사용자가 암호화된 가상 시스템을 다른 ESXi 호스트로 마이그레이션할 수 있습니다. vMotion 및 Storage vMotion을 사용하거나 사용하지 않는 마이그레이션을 지원합니다. 다른 vCenter Server 인스턴스로의 마이그레이션을 지원합니다.	가상 시스템
암호화 작업.이중 암호화	사용자가 다른 키로 가상 시스템 또는 디스크를 이중 암호화할 수 있습니다. 이 권한은 깊은 이중 암호화 작업과 얕은 이중 암호화 작업 모두에 필요합니다.	가상 시스템

표 16-8. 암호화 작업 권한 (계속)

권한 이름	설명	필수
암호화 작업.VM 등록	사용자가 ESXi 호스트로 암호화된 가상 시스템을 등록할 수 있습니다.	가상 시스템 폴더
암호화 작업.호스트 등록	사용자가 호스트에서 암호화를 사용하도록 설정할 수 있습니다. 사용자가 호스트에서 명시적으로 암호화를 사용하도록 설정하거나 가상 시스템 생성 프로세스에서 이를 사용하도록 설정할 수 있습니다.	독립형 호스트를 위한 호스트 폴더, 클러스터의 호스트를 위한 클러스터
암호화 작업.KMS 정보 읽기	사용자가 vCenter Server 및 호스트에서 vSphere Native Key Provider를 나열할 수 있습니다. 또한 사용자가 vSphere Native Key Provider 정보를 얻을 수 있습니다.	vCenter Server 또는 호스트

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 16-9. 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

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 16-10. 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

데이터 센터 권한

데이터 센터 권한은 vSphere 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 16-11. 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 변경	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 16-12. 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

표 16-12. 데이터스토어 권한 (계속)

권한 이름	설명	필수
데이터스토어.파일 제거	데이터스토어에서 파일을 삭제할 수 있습니다. 이 권한은 사용되지 않습니다. **하위 수준 파일 작업** 권한을 할당하십시오.	데이터스토어
데이터스토어.데이터스토어 이름 변경	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 16-13. 데이터스토어 클러스터 권한

권한 이름	설명	필수
데이터스토어 클러스터.데이터스토어 클러스터 구성	Storage DRS의 데이터스토어 클러스터에 대한 설정을 생성하고 구성할 수 있습니다.	데이터스토어 클러스터

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 16-14. 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 16-15. 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

외부 통계 제공자 권한

외부 통계 제공자 권한은 사전 예방적 DRS(Distributed Resource Scheduler) 통계를 vCenter Server에 알리는 기능을 제어합니다.

이 권한은 VMware 내부용 API에만 적용됩니다.

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 16-16. 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 변경	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 16-17. 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.라이센스	설치된 라이센스를 보고 라이센스를 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	ESXCLI에서 `resxtop` 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

상태 업데이트 제공자 권한

상태 업데이트 제공자 권한은 하드웨어 벤더가 vCenter Server에 Proactive HA 이벤트를 알리는 기능을 제어합니다.

이 권한은 VMware 내부용 API에만 적용됩니다.

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 16-18. 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 16-19. 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

표 16-19. 호스트 구성 권한 (계속)

권한 이름	설명	필수
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
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 16-20. 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

표 16-20. 호스트 인벤토리 권한 (계속)

권한 이름	설명	필수
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
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 변경	클러스터의 이름을 바꿀 수 있습니다.	클러스터

호스트 로컬 작업 권한

호스트 로컬 작업 권한은 VMware Host 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 16-21. 호스트 로컬 작업 권한

권한 이름	설명	필수
호스트.로컬 작업.vCenter에 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.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 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 16-22. 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 16-23. 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

vSphere with Tanzu 권한

네임스페이스 권한은 VMware vSphere® with VMware Tanzu™ 네임스페이스를 생성하고 관리할 수 있는 사람을 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 16-24. 네임스페이스 권한

권한 이름	설명	필수
네임스페이스.디스크 서비스 해제 작업 허용	데이터스토어의 서비스 해제 작업이 가능합니다.	데이터스토어
네임스페이스.백업 워크로드 구성 요소 파일	etcd 클러스터의 컨텐츠를 백업할 수 있습니다(VMware Cloud on AWS에만 사용됨).	클러스터
네임스페이스.클러스터 전체 구성 수정	클러스터 전체 구성을 수정하고 클러스터 네임스페이스를 사용하거나 사용하지 않도록 설정할 수 있습니다.	클러스터
네임스페이스.클러스터 전체 네임스페이스 셀프 서비스 구성 수정	네임스페이스 셀프 서비스 구성을 수정할 수 있습니다.	클러스터 (활성화 및 비활성화용) 템플릿 (구성 수정용) vCenter Server (템플릿 생성용)
네임스페이스.네임스페이스 구성 수정	리소스 할당 및 사용자 사용 권한과 같은 네임스페이스 구성 옵션을 수정할 수 있습니다.	클러스터
네임스페이스.클러스터 기능 전환	클러스터 기능의 상태를 조작할 수 있습니다(VMware Cloud on AWS 경우에만 내부적으로 사용됨).	클러스터
네임스페이스.최신 버전으로 클러스터 업그레이드	클러스터 업그레이드를 시작할 수 있습니다.	클러스터

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 16-25. 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
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 16-26. 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 16-27. 사용 권한에 대한 권한

권한 이름	설명	필수
사용 권한.사용 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 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 프로필과 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 16-28. 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 16-29. 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
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 변경	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 16-30. 스케줄링된 작업 권한

권한 이름	설명	필수
예약된 작업.작업 생성	작업을 스케줄링할 수 있습니다. 스케줄링 시간에 스케줄링된 작업을 수행할 수 있는 권한 외에 추가적으로 필요한 권한입니다.	모든 개체
예약된 작업.작업 수정	스케줄링된 작업 속성을 재구성할 수 있습니다.	모든 개체
예약된 작업.작업 제거	대기열에서 스케줄링된 작업을 제거할 수 있습니다.	모든 개체
예약된 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 16-31. 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
세션.세션의 유효성 검사	세션 유효성을 확인할 수 있습니다.	루트 vCenter Server
세션.세션 보기 및 중지	세션을 볼 수 있고, 로그온한 사용자 한 명 이상을 강제로 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 16-32. 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 16-33. 작업 권한

권한 이름	설명	필수
작업.작업 생성	확장을 통해 사용자 정의 작업을 만들 수 있습니다. 이 권한과 연결된 vSphere Client 사용자 인터페이스 요소는 없습니다.	루트 vCenter Server
작업.작업 업데이트	확장을 통해 사용자 정의 작업을 업데이트할 수 있습니다. 이 권한과 연결된 vSphere Client 사용자 인터페이스 요소는 없습니다.	루트 vCenter Server

전송 서비스 권한

전송 서비스 권한은 VMware 내부입니다. 이러한 권한을 사용하지 마십시오.

VcTrusts/VcIdentity 권한

VcTrusts/VcIdentity 권한은 vCenter Server 시스템 간의 신뢰와 관련된 다양한 내부 API 및 기능에 대한 액세스를 제어합니다.

표 16-34. VcTrusts/VcIdentity 권한

권한 이름	설명	필수
VcTrusts/VcIdentity.생성/업데이트/삭제(관리자 권한)	vCenter Server 시스템 간의 신뢰와 관련된 다양한 내부 API 및 기능에 대한 전체 관리 수준 액세스를 허용합니다.	해당 없음
VcTrusts/VcIdentity.생성/업데이트/삭제(관리자 권한 아래)	vCenter Server 시스템 간의 신뢰와 관련된 다양한 내부 API 및 기능에 대한 관리 액세스를 줄일 수 있습니다. 이 권한은 사용자가 관리자 이외의 사용자 권한을 승격하지 못하도록 VcTrusts/VcIdentity 생성/업데이트/삭제를 제한합니다.	해당 없음

신뢰할 수 있는 인프라 관리자 권한

신뢰할 수 있는 인프라 관리자 권한은 vSphere 신뢰 기관 배포를 구성하고 관리합니다.

이러한 권한은 vSphere 신뢰 기관 배포에 대한 구성 및 관리 작업을 수행할 수 있는 사용자를 결정합니다. 신뢰 기관 역할 및 신뢰할 수 있는 관리자 그룹에 대한 자세한 내용은 vSphere 신뢰 기관에 대한 사전 요구 사항 및 필요한 권한 항목을 참조하십시오.

표 16-35. 신뢰할 수 있는 인프라 관리자 권한

권한 이름	설명	필수
신뢰할 수 있는 인프라 관리자.키 서버 신뢰 구성	키 제공자 서비스의 키 제공자를 관리할 수 있습니다.	루트 vCenter Server
신뢰할 수 있는 인프라 관리자.신뢰 기관 호스트 TPM 인증서 구성	증명 서비스 설정을 생성하고 수정할 수 있습니다.	루트 vCenter Server
신뢰할 수 있는 인프라 관리자.신뢰 기관 호스트 메타데이터 구성	증명 서비스에서 증명할 기본 이미지를 편집할 수 있습니다.	루트 vCenter Server
신뢰할 수 있는 인프라 관리자.증명 SSO 구성	신뢰 기관 호스트에서 신뢰할 수 있는 호스트를 편집할 수 있습니다.	루트 vCenter Server
신뢰할 수 있는 인프라 관리자.토큰 변환 정책 구성	토큰 변환 정책을 구성할 수 있습니다.	루트 vCenter Server
신뢰할 수 있는 인프라 관리자.신뢰할 수 있는 인프라 호스트 나열	신뢰할 수 있는 호스트와 신뢰 기관 호스트에 대한 정보를 읽을 수 있습니다.	루트 vCenter Server
신뢰할 수 있는 인프라 관리자.STS에 대한 정보 나열	신뢰 기관 클러스터로 가져올 수 있도록 신뢰할 수 있는 호스트 세부 정보를 내보낼 수 있습니다.	루트 vCenter Server
신뢰할 수 있는 인프라 관리자.신뢰할 수 있는 인프라 호스트 관리	신뢰할 수 있는 호스트 및 신뢰 기관 호스트에 대한 정보를 편집할 수 있습니다.	루트 vCenter Server
신뢰할 수 있는 인프라 관리자.키 서버 신뢰 읽기	키 제공자 서비스의 키 제공자를 읽을 수 있습니다.	루트 vCenter Server

표 16-35. 신뢰할 수 있는 인프라 관리자 권한 (계속)

권한 이름	설명	필수
신뢰할 수 있는 인프라 관리자. 증명 SSO 읽기	신뢰 기관 호스트에서 신뢰할 수 있는 호스트를 읽을 수 있습니다.	루트 vCenter Server
신뢰할 수 있는 인프라 관리자.TPM 신뢰 기관 호스트 인증서 검색	증명 서비스의 설정을 읽을 수 있습니다.	루트 vCenter Server
신뢰할 수 있는 인프라 관리자. 신뢰 기관 호스트 메타데이터 검색	증명 서비스에서 증명할 수 있는 기본 이미지를 읽을 수 있습니다.	루트 vCenter Server

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 16-36. 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
vApp.전원 켜기	vApp에서 전원 켜기 작업을 수행할 수 있습니다.	vApp
vApp.이름 변경	vApp 이름을 변경할 수 있습니다.	vApp
vApp.일시 중단	vApp을 일시 중단할 수 있습니다.	vApp

표 16-36. vApp 권한 (계속)

권한 이름	설명	필수
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 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

VcIdentityProviders 권한

VcIdentityProviders 권한은 VcIdentityProviders API에 대한 액세스를 제어합니다.

표 16-37. VcIdentityProviders 권한

권한 이름	설명	필수
VcIdentityProviders.생성	VcIdentityProviders API(vCenter Server ID제공자)에 대한 생성 전용 액세스 권한을 허용합니다.	해당 없음
VcIdentityProviders.관리	VcIdentityProviders API(vCenter Server ID제공자)에 대한 관리 수준의 쓰기 액세스 권한(생성, 읽기, 업데이트, 삭제)을 허용합니다.	해당 없음
VcIdentityProviders.읽기	VcIdentityProviders API(vCenter Server ID제공자)에 대한 읽기 액세스 권한을 허용합니다.	해당 없음

VMware vSphere Lifecycle Manager 구성 권한

VMware vSphere Lifecycle Manager 구성 권한은 vSphere Lifecycle Manager 서비스를 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.

참고 관리자 또는 신뢰할 수 있는 사용자에게만 URL을 허용하는 VMware vSphere Lifecycle Manager API를 호출할 수 있는 권한을 사용자에게 할당합니다.

표 16-38. VMware vSphere Lifecycle Manager 구성 권한

권한 이름	설명	필수
VMware vSphere Lifecycle Manager.구성. 서비스 구성	vSphere Lifecycle Manager 서비스 및 스케줄링된 패치 다운로드 작업을 구성할 수 있습니다.	루트 vCenter Server

VMware vSphere Lifecycle Manager ESXi 상태 관점 권한

VMware vSphere Lifecycle Manager ESXi 상태 관점 권한은 ESXi 호스트 및 클러스터의 상태를 확인하는 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 16-39. VMware vSphere Lifecycle Manager ESXi 상태 관점 권한

권한 이름	설명	필수
VMware vSphere Lifecycle Manager.ESXi 상태 관점.읽기	ESXi 호스트 및 클러스터의 상태를 쿼리할 수 있습니다.	호스트 클러스터
VMware vSphere Lifecycle Manager.ESXi 상태 관점.쓰기	해당 없음	해당 없음

VMware vSphere Lifecycle Manager 일반 권한

VMware vSphere Lifecycle Manager 일반 권한은 Lifecycle Manager 리소스를 읽고 쓰는 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 16-40. VMware vSphere Lifecycle Manager 일반 권한

권한 이름	설명	필수
VMware vSphere Lifecycle Manager.Lifecycle Manager: 일반 권한.읽기	vSphere Lifecycle Manager 리소스를 읽을 수 있습니다. 이 권한은 작업 정보를 가져오는 데 필요합니다.	루트 vCenter Server
VMware vSphere Lifecycle Manager.Lifecycle Manager: 일반 권한.쓰기	vSphere Lifecycle Manager 리소스를 쓸 수 있습니다. 이 권한은 vSphere Lifecycle Manager 작업을 취소하는 데 필요합니다.	루트 vCenter Server

VMware vSphere Lifecycle Manager 하드웨어 호환성 권한

VMware vSphere Lifecycle Manager 하드웨어 호환성 권한은 잠재적인 하드웨어 호환성 문제를 검색하고 해결하는 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 16-41. VMware vSphere Lifecycle Manager 하드웨어 호환성 권한

권한 이름	설명	필수
VMware vSphere Lifecycle Manager.Lifecycle Manager: 하드웨어 호환성 권한.하드웨어 호환성에 액세스	하드웨어 호환성 데이터에 액세스하고 잠재적인 하드웨어 호환성 문제를 해결할 수 있습니다.	호스트

VMware vSphere Lifecycle Manager 이미지 권한

VMware vSphere Lifecycle Manager 이미지 권한은 이미지를 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.

참고 관리자 또는 신뢰할 수 있는 사용자에게만 URL을 허용하는 VMware vSphere Lifecycle Manager API를 호출할 수 있는 권한을 사용자에게 할당합니다.

표 16-42. VMware vSphere Lifecycle Manager 이미지 권한

권한 이름	설명	필수
VMware vSphere Lifecycle Manager.Lifecycle Manager: 이미지 권한.읽기	vSphere Lifecycle Manager 이미지를 읽을 수 있습니다. 이 권한이 필요한 작업: ■ 클러스터의 모든 초안 나열 ■ 초안에 대한 추가 정보 가져오기 ■ 초안에서 검색 수행 ■ 초안 검증 ■ 초안의 컨텐츠 검색 ■ 유효 구성 요소 목록 계산 ■ 현재 원하는 상태 문서의 컨텐츠 가져오기 ■ 클러스터에서 검색 시작 ■ 규정 준수 결과 가져오기 ■ 권장 사항 가져오기 ■ 현재 원하는 상태를 디포, JSON 파일 또는 ISO로 내보내기	루트 vCenter Server
VMware vSphere Lifecycle Manager.Lifecycle Manager: 이미지 권한.쓰기	vSphere Lifecycle Manager 이미지를 관리할 수 있습니다. 이 권한이 필요한 작업: ■ 초안 생성, 삭제 또는 커밋 ■ 원하는 상태 가져오기 ■ 권장 사항 생성 ■ 초안의 다른 부분 설정 또는 삭제	루트 vCenter Server

VMware vSphere Lifecycle Manager 이미지 업데이트 적용 권한

VMware vSphere Lifecycle Manager 이미지 권한은 이미지에 업데이트를 적용하는 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 16-43. VMware vSphere Lifecycle Manager 이미지 업데이트 적용 권한

권한 이름	설명	필수
VMware vSphere Lifecycle Manager.Lifecycle Manager: 이미지 업데이트 적용 권한.읽기	업데이트 적용 사전 검사를 수행할 수 있습니다.	클러스터
VMware vSphere Lifecycle Manager.Lifecycle Manager: 이미지 업데이트 적용 권한.쓰기	업데이트 적용을 수행할 수 있습니다.	클러스터

VMware vSphere Lifecycle Manager 설정 권한

VMware vSphere Lifecycle Manager 설정 권한은 디포 및 업데이트 적용 정책을 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.

참고 관리자 또는 신뢰할 수 있는 사용자에게만 URL을 허용하는 VMware vSphere Lifecycle Manager API를 호출할 수 있는 권한을 사용자에게 할당합니다.

표 16-44. VMware vSphere Lifecycle Manager 설정 권한

권한 이름	설명	필수
VMware vSphere Lifecycle Manager.Lifecycle Manager: 설정 권한.읽기	vSphere Lifecycle Manager 디포 및 업데이트 적용 정책을 읽을 수 있습니다.	루트 vCenter Server
VMware vSphere Lifecycle Manager.Lifecycle Manager: 설정 권한.쓰기	vSphere Lifecycle Manager 디포 및 업데이트 적용 정책을 작성할 수 있습니다.	루트 vCenter Server

VMware vSphere Lifecycle Manager 기준선 관리 권한

VMware vSphere Lifecycle Manager 기준선 관리 권한은 기준선 및 기준선 그룹을 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 16-45. VMware vSphere Lifecycle Manager 기준선 관리 권한

권한 이름	설명	필수
VMware vSphere Lifecycle Manager.기준선 관리.기준선 연결	vSphere 인벤토리의 개체에 기준선 및 기준선 그룹을 연결할 수 있습니다.	루트 vCenter Server
VMware vSphere Lifecycle Manager.기준선 관리.기준선 관리	기준선 및 기준선 그룹을 생성, 편집 또는 삭제할 수 있습니다.	루트 vCenter Server

VMware vSphere Lifecycle Manager 패치 및 업그레이드 관리 권한

VMware vSphere Lifecycle Manager 패치 및 업그레이드 관리 권한은 해당 패치, 확장 또는 업그레이드를 보고, 검색하고, 업데이트를 적용하는 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 16-46. VMware vSphere Lifecycle Manager 패치 및 업그레이드 관리 권한

권한 이름	설명	필수
VMware vSphere Lifecycle Manager.패치 및 업그레이드 관리.업데이트를 적용하여 패치/확장/업그레이드 적용	기준선을 사용하는 경우, 가상 시스템 및 호스트에 패치, 확장 또는 업그레이드를 적용하기 위해 업데이트를 적용할 수 있습니다. 이 권한을 사용하여 규정 준수 상태를 볼 수도 있습니다.	루트 vCenter Server
VMware vSphere Lifecycle Manager.패치 및 업그레이드 관리.적용 가능한 패치, 확장 및 업그레이드 검색	기준선을 사용하는 경우, 해당하는 패치, 확장 또는 업그레이드를 찾기 위해 가상 시스템 및 호스트를 검색할 수 있습니다.	루트 vCenter Server
VMware vSphere Lifecycle Manager.패치 및 업그레이드 관리.패치 및 확장 스테이징	기준선을 사용하는 경우, ESXi 호스트에 패치 또는 확장을 스테이징할 수 있습니다. 이 권한을 사용하여 ESXi 호스트의 규정 준수 상태를 볼 수도 있습니다.	루트 vCenter Server
VMware vSphere Lifecycle Manager.패치 및 업그레이드 관리.준수 상태 보기	vSphere 인벤토리에 있는 개체의 기준선 규정 준수 정보를 볼 수 있습니다.	루트 vCenter Server

VMware vSphere Lifecycle Manager 파일 업로드 권한

VMware vSphere Lifecycle Manager 파일 업로드 권한은 vSphere Lifecycle Manager 디포로 업데이트를 가져오는 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.

참고 관리자 또는 신뢰할 수 있는 사용자에게만 URL을 허용하는 VMware vSphere Lifecycle Manager API를 호출할 수 있는 권한을 사용자에게 할당합니다.

표 16-47. VMware vSphere Lifecycle Manager 파일 업로드 권한

권한 이름	설명	필수
VMware vSphere Lifecycle Manager.파일 업로드.파일 업로드	업그레이드 ISO 및 오프라인 패치 번들을 업로드할 수 있습니다.	루트 vCenter Server

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 16-48. 가상 시스템 구성 권한

권한 이름	설명	필수
가상 시스템.구성.디스크 리스 획득	가상 시스템에 대한 디스크 리스 작업을 허용합니다.	가상 시스템
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 구성	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.메모리 변경	가상 시스템에 할당된 메모리 크기를 변경할 수 있습니다.	가상 시스템
가상 시스템.구성.설정 변경	일반적인 가상 시스템 설정을 변경할 수 있습니다.	가상 시스템
가상 시스템.구성.스왑 파일 배치 변경	가상 시스템의 스왑 파일 배치 정책을 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.호스트 USB 디바이스 구성	호스트 기반 USB 디바이스를 가상 시스템에 연결할 수 있습니다.	가상 시스템

표 16-48. 가상 시스템 구성 권한 (계속)

권한 이름	설명	필수
가상 시스템.구성.원시 디바이스 구성	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.managedBy 구성	확장 또는 솔루션을 통해 가상 시스템을 해당 확장 또는 솔루션에 의해 관리되는 것으로 표시할 수 있습니다.	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.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.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 변경	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.디스크 변경 내용 추적 토글	가상 시스템 디스크에 대한 변경 내용 추적을 사용하거나 사용하지 않도록 설정할 수 있습니다.	가상 시스템

표 16-48. 가상 시스템 구성 권한 (계속)

권한 이름	설명	필수
가상 시스템.구성.분기 상위 전환	vmfork 상위를 사용하거나 사용하지 않도록 설정할 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 애플리케이션과 상호 작용하는 기능을 제어합니다.

이러한 작업에 대한 자세한 내용은 "vSphere Web Services 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 16-49. 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 Client 사용자 인터페이스 요소는 없습니다.	가상 시스템

표 16-49. 가상 시스템 게스트 작업 (계속)

권한 이름	설명	적용되는 개체
가상 시스템.게스트 작업.게스트 작업 프로그램 실행	가상 시스템에서의 애플리케이션 실행을 수반하는 가상 시스템 게스트 작업을 허용합니다. 이 권한과 연결된 vSphere 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 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 16-50. 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
가상 시스템.상호 작용.스크린샷 생성	가상 시스템 스크린샷을 생성할 수 있습니다.	가상 시스템

표 16-50. 가상 시스템 상호 작용 (계속)

권한 이름	설명	필수
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.끌어서 놓기	가상 시스템과 원격 클라이언트 간에 파일을 끌어서 놓을 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
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 켜진 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
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 16-50. 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
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 CD 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 16-51. 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 재배치할 수 있습니다. 권한은 소스와 대상에 모두 있어야 합니다.	가상 시스템
가상 시스템.인벤토리.등록	기존 가상 시스템을 vCenter Server 또는 호스트 인벤토리에 추가할 수 있습니다.	클러스터, 호스트, 가상 시스템 폴더

표 16-51. 가상 시스템 인벤토리 권한 (계속)

권한 이름	설명	필수
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 16-52. 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.파일 액세스 허용	.vmx, .disk, .log 및 .nvram을 포함하여 가상 시스템과 연결된 파일에 대해 작업할 수 있습니다.	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.게스트 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 16-52. 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.

표 16-53. 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 16-54. 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 변경	새 이름, 새 설명 또는 둘 모두를 사용하여 스냅샷의 이름을 변경할 수 있습니다.	가상 시스템
가상 시스템.스냅샷 관리.스냅샷으로 되돌리기	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 16-55. 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

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 16-56. vServices

권한 이름	설명	필수
vService.종속성 생성	가상 시스템이나 vApp에 대한 vService 종속성을 만들 수 있습니다.	vApp 및 가상 시스템
vService.종속성 삭제	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

vSphere 태그 지정 권한

vSphere 태그 지정 권한은 태그 생성/삭제, 범주에 태그 지정, vCenter Server 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 16-57. vSphere 태그 지정 권한

권한 이름	설명	필수
vSphere 태그 지정.vSphere 태그 할당 또는 할당 취소	vCenter Server 인벤토리의 개체에 대해 태그를 할당하거나 할당 취소할 수 있습니다.	모든 개체
vSphere 태그 지정.개체에 vSphere 태그 할당 또는 할당 취소	개체에 태그를 할당하거나 태그 할당을 취소할 수 있도록 허용합니다. 이 권한을 사용하여 사용자가 태그를 할당하거나 태그 할당을 취소할 수 있는 개체를 제한합니다.	모든 개체
vSphere 태그 지정.vSphere 태그 생성	태그를 생성할 수 있습니다.	모든 개체
vSphere 태그 지정.vSphere 태그 범주 생성	태그 범주를 생성할 수 있습니다.	모든 개체
vSphere 태그 지정.vSphere 태그 삭제	태그를 삭제할 수 있습니다.	모든 개체
vSphere 태그 지정.vSphere 태그 범주 삭제	태그 범주를 삭제할 수 있습니다.	모든 개체
vSphere 태그 지정.vSphere 태그 편집	태그를 편집할 수 있습니다.	모든 개체
vSphere 태그 지정.vSphere 태그 범주 편집	태그 범주를 편집할 수 있습니다.	모든 개체
vSphere 태그 지정.범주의 UsedBy 필드 수정	태그 범주에 대한 사용자 필드를 변경할 수 있습니다.	모든 개체
vSphere 태그 지정.태그의 UsedBy 필드 수정	태그에 대한 사용자 필드를 변경할 수 있습니다.	모든 개체

vSphere Client 권한

vSphere Client 권한은 vCenter Server에 대한 오프라인 액세스를 제어합니다.

이러한 권한은 VMware Cloud에만 적용됩니다.

vSphere 강화 및 규정 준수 이해

17

조직은 데이터 도용, 사이버 공격 또는 무단 액세스의 위험을 줄여서 데이터 보안을 유지하고자 합니다. 또한 조직은 NIST(National Institute of Standards and Technology) 및 DISA STIG(Defense Information Systems Agency Security Technical Implementation Guides)와 같은 정부 표준에서 민간 표준에 이르는 하나 이상의 규정을 준수해야 합니다. vSphere 환경에서 이러한 표준을 준수하도록 하려면 사람, 프로세스 및 기술을 포함하는 보다 광범위한 고려 사항을 이해해야 합니다.

주의가 필요한 보안 및 규정 준수 주제를 개괄적으로 파악하면 규정 준수 전략을 계획하는 데 도움이 됩니다. VMware 웹 사이트에서 다른 규정 준수 관련 리소스를 활용할 수도 있습니다.

본 장은 다음 항목을 포함합니다.

- vSphere 환경의 보안 및 규정 준수
- vSphere 보안 구성 가이드 이해
- National Institute of Standards and Technology 정보
- DISA STIG 정보
- VMware 보안 개발 수명 주기 정보
- 감사 로깅
- 보안 및 규정 준수 이해 다음 단계
- vCenter Server 및 FIPS

vSphere 환경의 보안 및 규정 준수

보안과 규정 준수라는 용어는 종종 같은 의미로 사용됩니다. 하지만 이들 용어는 고유하며 개념이 다릅니다.

흔히 정보 보안이라고 생각하는 보안은 일반적으로 기밀성, 무결성 및 가용성을 제공하기 위해 구현하는 기술적, 물리적 및 관리 측면의 제어 집합으로 정의됩니다. 예를 들어 호스트의 보안은 해당 호스트에 로그인할 수 있는 계정과 액세스 수단(SSH, 직접 콘솔 등)을 잠그는 방법으로 유지할 수 있습니다. 이와 대조적으로 규정 준수는 특정 유형의 기술, 벤더 또는 구성에 대해 제한된 지침을 제공하는 여러 규정 프레임워크에 제시된 최소한의 제어를 충족하는 데 필요한 요구 사항 집합입니다. 예를 들어 PCI(지불 카드 산업)에는 조직이 고객 계정 데이터를 사전 예방적으로 보호할 수 있도록 하는 보안 지침이 도입되었습니다.

보안은 데이터 도난, 사이버 공격 또는 무단 액세스의 위험을 줄이는 반면 규정 준수는 정의된 타임라인 내에서 보안 제어가 이루어지고 있다는 증명입니다. 보안은 기본적으로 설계 결정에 요약되며 기술 구성 내에 강조 표시됩니다. 규정 준수는 보안 제어와 특정 요구 사항의 상관 관계를 매핑하는 데 중점을 둡니다. 규정 준수 매핑은 여러 필수 보안 제어를 나열하기 위한 중앙 집중식 보기를 제공합니다. 이러한 보안 제어는 각 제어와 매핑되는 규정 준수 정보(도메인에 지정된 NIST, PCI, FedRAMP, HIPAA 등)를 포함하여 구체화됩니다.

효과적인 사이버 보안 및 규정 준수 프로그램은 세 가지 요소인 사용자, 프로세스 및 기술을 기반으로 구축됩니다. 흔히 기술만으로 모든 사이버 보안 요구를 해결할 수 있다고 오해합니다. 정보 보안 프로그램의 개발 및 실행에 있어서 기술이 크고 중요한 역할을 하는 것은 사실입니다. 하지만 프로세스와 절차, 인식과 교육이 결여된 기술은 조직을 보안 문제에 취약하게 만듭니다.

보안 및 규정 준수 전략을 정의할 때 다음 사항에 유의하십시오.

- 사용자에게는 일반적인 인식과 교육이 필요한 반면 IT 직원에게는 구체적인 교육이 필요합니다.
- 프로세스는 조직의 활동, 역할 및 문서를 사용하여 위험을 완화하는 방법을 정의합니다. 프로세스는 사용자가 올바르게 따라야만 효과적입니다.
- 기술을 사용하면 조직에서 사이버 보안 위험을 방지하거나 그 영향을 줄일 수 있습니다. 어떤 기술을 사용할지는 조직의 위험 허용 수준에 따라 달라집니다.

VMware는 감사 가이드와 제품 적용 가능성 가이드가 모두 포함된 규정 준수 키트를 제공하여 규정 준수 및 규정 요건과 구현 가이드 간의 간극을 좁히는 데 도움을 줍니다. 자세한 내용은 https://core.vmware.com/compliance의 내용을 참조하십시오.

규정 준수 용어 정리

규정 준수에는 이해하고 있어야 하는 몇 가지 중요한 용어와 정의가 포함되어 있습니다.

표 17-1. 규정 준수 용어

용어	정의
CJIS	Criminal Justice Information Services. 규정 준수의 맥락에서 CJIS는 지방, 주 및 연방 형사 사법 및 법 집행 기관이 지문 및 전과 기록 같이 민감한 정보를 보호하기 위해 보안 예방 조치를 수행하는 방법에 대한 보안 정책을 생성합니다.
DISA STIG	Defense Information Systems Agency Security Technical Implementation Guide. DISA(Defense Information Systems Agency)는 미국 국방부(DoD) IT 인프라의 보안 태세를 유지하는 기관입니다. DISA는 Security Technical Implementation Guide, 즉 "STIG"를 개발하고 사용하여 이러한 업무를 수행합니다.
FedRAMP	Federal Risk and Authorization Management Program. FedRAMP는 클라우드 제품 및 서비스에 대한 보안 평가, 권한 부여 및 지속적인 모니터링에 대한 표준화된 접근 방식을 제공하는 정부 차원의 프로그램입니다.

표 17-1. 규정 준수 용어 (계속)

용어	정의
HIPAA	Health Insurance Portability and Accountability Act. 1996년 의회에서 통과된 HIPAA는 다음을 수행합니다. ■ 수백만 명의 미국인 근로자와 그 가족이 직장을 옮기거나 잃은 경우에 건강보험 혜택을 조정하고 계속 받을 수 있도록 합니다. ■ 의료 부정 행위 및 남용을 줄입니다. ■ 의료 정보에 대한 업계 전반의 표준을 전자 청구 및 기타 프로세스에 의무화합니다. ■ 보호 대상 건강 정보의 보호 및 기밀 처리를 요구합니다. "vSphere 보안" 설명서에는 마지막 항목이 가장 중요합니다.
NCCoE	National Cybersecurity Center of Excellence. NCCoE는 미국 기업이 직면하는 사이버 보안 문제에 대한 해결 방법을 찾고 공개적으로 공유하는 미국 정부 조직입니다. NCCoE는 사이버 보안 기술 회사, 기타 연방 기관 및 학계 인사들로 팀을 구성하여 각 문제를 해결합니다.
NIST	National Institute of Standards and Technology. 1901년에 설립된 NIST는 미국 상무부 내의 비규제 연방 기관입니다. NIST의 의무는 경제적 안전을 강화하고 삶의 질을 높이는 방향으로 계측학, 표준 및 기술을 발전시킴으로써 미국의 혁신과 산업 경쟁력을 옹호하는 것입니다.
PAG	Product Applicability Guide. 특정 회사의 솔루션을 참고하여 규정 준수 요구 사항을 해결하려는 조직을 위한 일반적인 지침을 제공하는 설명서입니다.
PCI DSS	Payment Card Industry Data Security Standard(지불 카드 산업 데이터 보안 표준). 신용 카드 정보를 수락, 처리, 저장 또는 전송하는 모든 회사가 안전한 환경을 유지할 수 있도록 설계된 보안 표준 집합입니다.
VVD/VCF 규정 준수 솔루션	VMware Validated Design/VMware Cloud Foundation. VMware Validated Design은 소프트웨어 정의 데이터 센터를 구축하고 운영할 수 있도록 포괄적이고 광범위하게 테스트된 Blueprint를 제공합니다. VVD/VCF 규정 준수 솔루션은 고객이 여러 정부 및 산업 규정에 대한 규정 준수 요구 사항을 충족할 수 있도록 도와줍니다.

vSphere 보안 구성 가이드 이해

VMware에서는 안전한 방식으로 VMware 제품을 배포 및 운영하는 데 필요한 지침을 제공하는 보안 강화 가이드를 생성합니다. vSphere의 경우 이러한 가이드를 "vSphere 보안 구성 가이드" (이전 명칭: "강화 가이드")라고 합니다.

"vSphere 보안 구성 가이드" 에는 vSphere에 대한 보안 모범 사례가 포함되어 있습니다. "vSphere 보안 구성 가이드" 는 규정 지침 또는 프레임워크에 직접 매핑되지 않으므로 규정 준수 가이드가 아닙니다. 또한 "vSphere 보안 구성 가이드" 는 보안 검사 목록으로 사용할 수 없습니다. 보안에는 항상 장점과 단점이 공존합니다. 보안 제어를 구현하면 사용 편의성, 성능 또는 기타 운영 작업에 부정적인 영향을 줄 수 있습니다. 보안 결정을 변경할 때에는 해당 조언을 VMware에서 제공했는지 여부와 관계없이 워크로드, 사용 패턴, 조직 구조 등을 신중하게 고려해야 합니다. 조직에 규정 준수 요구가 있는 경우에는 vSphere 환경의 보안 및 규정 준수의 내용을 참조하거나 https://core.vmware.com/compliance를 방문하십시오. 이 사이트는 vSphere 관리자 및 규정 감사자가 NIST 800-53v4, NIST 800-171, PCI DSS, HIPAA, CJIS, ISO 27001 등의 규정 프레임워크에 대한 가상 인프라를 보호하고 증명하는 데 도움이 되는 규정 준수 키트 및 제품 감사 가이드를 제공합니다.

다음 항목에 대한 보안 설정은 "vSphere 보안 구성 가이드" 에서 다루지 않습니다.

- 게스트 운영 체제 및 애플리케이션과 같은 가상 시스템 내에서 실행되는 소프트웨어
- 가상 시스템 네트워크를 통해 이동하는 트래픽
- 추가 기능 제품에 대한 보안

"vSphere 보안 구성 가이드" 는 "규정 준수" 도구로 사용할 가이드가 아닙니다. "vSphere 보안 구성 가이드" 를 통해 규정 준수를 위한 첫 단계를 수행할 수는 있지만 이 가이드만으로는 배포가 규정을 준수하는지 확인할 수 없습니다. 규정 준수에 대한 자세한 내용은 vSphere 환경의 보안 및 규정 준수의 내용을 참조하십시오.

vSphere 보안 구성 가이드 읽기

"vSphere 보안 구성 가이드" 는 vSphere 보안 구성을 수정하는 데 도움이 되는 보안 관련 지침이 포함된 스프레드시트입니다. 이러한 지침은 영향을 받는 구성 요소에 따라 다음과 같은 열의 일부 또는 전체와 함께 탭으로 그룹화됩니다.

표 17-2. vSphere 보안 구성 가이드 스프레드시트 열

열 머리글	설명
지침 ID	보안 구성 또는 강화 권장 사항을 표시하는 두 부분으로 구성된 고유 ID입니다. 첫 번째 부분은 다음과 같이 정의된 구성 요소를 나타냅니다. ■ ESXi: ESXi 호스트 ■ VM: 가상 시스템 ■ vNetwork: 가상 스위치
설명	특정 권장 사항에 대한 간단한 설명입니다.
토론	특정 권장 사항 뒤에 있는 취약점에 대한 설명입니다.
구성 매개 변수	적용 가능한 구성 매개 변수 또는 파일 이름(있는 경우)을 제공합니다.

표 17-2. vSphere 보안 구성 가이드 스프레드시트 열 (계속)

열 머리글	설명
원하는 값	권장 사항에 대해 원하는 상태 또는 값입니다. 가능한 값은 다음과 같습니다. ■ 해당 없음 ■ 특정 사이트 ■ False ■ True ■ 사용 ■ 사용 안 함 ■ 없음 또는 False
기본값	vSphere에서 설정된 기본값입니다.
원하는 값이 기본값입니까?	보안 설정이 기본 제품 구성인지 나타냅니다.
필요한 작업	특정 권장 사항에 대해 수행할 작업의 유형입니다. 작업에는 다음이 포함됩니다. ■ 업데이트 ■ 감사 전용 ■ 수정 ■ 추가 ■ 제거
vSphere Client에서의 설정 위치	vSphere Client를 사용하여 값을 확인하는 단계입니다.
기본값 변경 시 기능에 부정적인 영향이 있습니까?	보안 권장 사항을 사용함으로써 발생할 수도 있는 부정적 영향(이 있는 경우)에 대한 설명입니다.
PowerCLI 명령 평가	PowerCLI를 사용하여 값을 확인하는 단계입니다.
PowerCLI 명령 업데이트 적용 예	PowerCLI를 사용하여 값을 설정(업데이트 적용)하는 단계입니다.
vCLI 명령 업데이트 적용	vCLI 명령을 사용하여 값을 설정(업데이트 적용)하는 단계입니다.
PowerCLI 명령 평가	PowerCLI 명령을 사용하여 값을 확인하는 단계입니다.
PowerCLI 명령 업데이트 적용	PowerCLI 명령을 사용하여 값을 설정(업데이트 적용)하는 단계입니다.
호스트 프로파일을 사용하여 설정 가능	호스트 프로파일을 사용하여 설정을 수행할 수 있는지 여부(ESXi 지침에만 적용됨)입니다.
강화	TRUE이면 지침에 준수해야 하는 구현이 하나뿐입니다. FALSE이면 둘 이상의 구성 설정을 통해 지침 구현을 충족할 수 있습니다. 실제 설정은 종종 사이트별로 다릅니다.
사이트별 설정	TRUE이면, 지침을 준수하는 설정이 해당 vSphere 배포와 관련된 규칙 또는 표준에 따라 다릅니다.
감사 설정	TRUE이면 사이트별 규칙을 충족하기 위해 나열된 설정 값을 수정해야 할 수 있습니다.

참고 이러한 열은 필요에 따라 시간이 지나면서 변경될 수 있습니다. 예를 들어 최근에 추가된 항목에는 DISA STIG ID, 강화 및 사이트별 설정 열이 있습니다. "vSphere 보안 구성 가이드" 업데이트에 대한 공지는 https://blogs.vmware.com의 내용을 참조하십시오.

"vSphere 보안 구성 가이드" 의 지침을 환경에 맹목적으로 적용하지 마십시오. 더 정확히 말하면, 시간을 두고 각 설정을 평가하여 적용할지 여부에 대한 현명한 결정을 내리십시오. 최소한 평가 열에 있는 지침을 사용하여 배포에 대한 보안을 확인할 수 있습니다.

"vSphere 보안 구성 가이드" 는 배포 시 규정 준수를 구현하기 시작하는 데 도움이 되는 자료입니다. DISA(Defense Information Systems Agency) 및 기타 규정 준수 지침과 함께 "vSphere 보안 구성 가이드" 를 사용하면 vSphere 보안 제어를 각 지침에 따른 규정 준수 플레이버에 매핑할 수 있습니다.

National Institute of Standards and Technology 정보

NIST(National Institute of Standards and Technology)는 기술, 지표, 표준 및 지침을 개발하는 비규제 정부 기관입니다. NIST 표준 및 지침을 준수하는 것은 오늘날 많은 업계의 최우선 과제가 되었습니다.

1901년에 설립된 NIST는 현재 미국 상무부의 일부입니다. NIST는 미국에서 가장 오래된 자연 과학 연구 기관 중 하나입니다. 현재 NIST 측정은 나노스케일 장치부터 내진 고층 건물과 글로벌 통신 네트워크에 이르기까지 가장 작은 기술부터 인간이 만든 가장 크고 복잡한 창작물까지 지원합니다.

FISMA(Federal Information Security Management Act)는 2002년에 통과된 미국 연방법으로, 연방 기관에서 정보 보안 및 보호 프로그램을 개발, 문서화 및 구현하도록 의무화합니다. NIST는 주요 보안 표준 및 지침(예: FIPS 199, FIPS 200 및 SP 800 시리즈)을 작성하여 FISMA 구현에 중요한 역할을 합니다.

정부 및 개인 조직은 NIST 800-53을 사용하여 정보 시스템을 보호합니다. 다양한 위협으로부터 조직의 운영(임무, 기능, 이미지 및 평판 포함), 조직의 자산 및 개인을 보호하기 위해서는 사이버 보안 및 개인 정보 보호 제어가 반드시 필요합니다. 이러한 위협에는 악의적인 사이버 공격, 자연 재해, 구조적 장애 및 사용자 오류가 포함됩니다. VMware는 NIST 800-53 제어 카탈로그를 기준으로 VMware 제품 및 솔루션을 평가하기 위해 타사 감사 파트너와 협력합니다. 자세한 내용을 보려면 NIST 웹 페이지(https://www.nist.gov/cyberframework)를 참조하십시오.

DISA STIG 정보

DISA(Defense Information Systems Agency)는 STIG(Security Technical Implementation Guide)를 개발하고 게시합니다. DISA STIG는 시스템 강화 및 위협 감소를 위한 기술 지도를 제공합니다.

DISA(Defense Information Systems Agency)는 DODIN, 즉 DOD Information Network의 보안 태세 유지를 담당하는 미국 국방부(DOD) 지원 기관입니다. DISA가 이러한 업무를 수행하는 방법 중 하나는 STIG, 즉 Security Technical Implementation Guide를 개발 및 전파하고 STIG 구현을 의무화하는 것입니다. 간단히 말해 STIG는 시스템 강화를 위한 표준 기반의 이동 가능한 가이드입니다. STIG는 미국 DoD IT 시스템의 필수 요소이며, 따라서 비DoD 기업이 자체 보안 태세 평가에 사용할 수 있는 검증되고 안전한 기준을 제공합니다.

VMware와 같은 벤더는 DISA 프로토콜 및 피드백에 따라 DISA에 제안된 보안 강화 지침을 평가용으로 제출합니다. 이 프로세스가 완료되면 공식 STIG가 DISA 조직의 웹 사이트(https://public.cyber.mil/stigs/)에 게시됩니다. VMware는 vSphere 대한 보안 기준선 및 강화 지침을 "vSphere 보안 구성 가이드" 의 일부로 제공합니다. https://core.vmware.com/security의 내용을 참조하십시오.

VMware 보안 개발 수명 주기 정보

VMware SDL(보안 개발 수명 주기) 프로그램은 VMware 소프트웨어 제품의 개발 단계 중에 보안 위험을 식별하고 완화합니다. VMware는 VSRC(VMware Security Response Center)도 운영하여 VMware 제품의 소프트웨어 보안 문제를 분석하고 해결합니다.

SDL은 vSECR, 즉 VMware Security Engineering, Communication, and Response 그룹과 VMware 제품 개발 그룹이 보안 문제를 식별하고 완화하기 위해 사용하는 소프트웨어 개발 방법입니다. VMware 보안 개발 수명 주기에 대한 자세한 내용을 보려면 https://www.vmware.com/security/sdl.html 웹 페이지를 참조하십시오.

VSRC는 고객 및 보안 연구 커뮤니티와 협력하여 보안 문제를 해결하고 고객에게 적절한 보안 정보를 적시에 제공하는 목표를 달성합니다. VMware Security Response Center에 대한 자세한 내용을 보려면 https://www.vmware.com/security/vsrc.html 웹 페이지를 참조하십시오.

감사 로깅

네트워크 트래픽, 규정 준수 경고, 방화벽 작업, 운영 체제 변경 내용 및 프로비저닝 작업에 대한 감사 로깅은 IT 환경의 보안을 유지하기 위한 모범 사례로 간주됩니다. 로깅은 다양한 규정 및 표준의 구체적인 요구 사항이기도 합니다.

인프라에 대한 변경 사항을 인지하기 위해 우선적으로 취해야 할 단계 중 하나는 환경을 감시하는 것입니다. 기본적으로 vSphere에는 변경 내용을 보고 추적할 수 있게 도와 주는 도구가 포함되어 있습니다. 예를 들어 vSphere 계층의 개체에 대해 vSphere Client의 [작업 및 이벤트] 탭을 사용하면 어떤 변경 사항이 발생했는지 볼 수 있습니다. PowerCLI를 사용하여 이벤트와 작업을 검색할 수도 있습니다. 또한 vRealize Log Insight는 중요 시스템 이벤트의 수집 및 보존을 지원하기 위해 감사 로깅을 제공합니다. 이 외에 vCenter 감사 기능을 제공하는 여러 타사 도구도 사용할 수 있습니다.

로그 파일은 호스트, 가상 시스템에 액세스하는 사용자 또는 대상을 확인하는 데 도움이 되는 감사 추적을 제공할 수 있습니다. 자세한 내용은 ESXi 로그 파일 위치의 내용을 참조하십시오.

Single Sign-On 감사 이벤트

SSO(Single Sign-On) 감사 이벤트는 SSO 서비스에 액세스하기 위한 사용자 또는 시스템 작업의 기록입니다.

vCenter Server 6.7 업데이트 2 이상에서는 다음 작업에 대한 이벤트를 추가하여 VMware vCenter Single Sign-On 감사가 향상됩니다.

- 사용자 관리
- 로그인
- 그룹 생성
- ID 소스
- 정책 업데이트

지원되는 ID 소스는 vsphere.local, IWA(통합 Windows 인증) 및 LDAP를 통한 Active Directory입니다.

사용자가 Single Sign-On을 통해 vCenter Server에 로그인하거나, SSO에 영향을 주는 변경 작업을 수행하면 다음과 같은 감사 이벤트가 SSO 감사 로그 파일에 기록됩니다.

- **Login and Logout Attempts:** 성공하거나 실패한 모든 로그인/로그아웃 작업에 대한 이벤트입니다.
- **Privilege Change:** 사용자 역할 또는 사용 권한의 변경에 대한 이벤트입니다.
- **Account Change:** 사용자 계정 정보(예: 사용자 이름, 암호 또는 기타 계정 정보)의 변경에 대한 이벤트입니다.
- **Security Change:** 보안 구성, 매개 변수 또는 정책의 변경에 대한 이벤트입니다.
- **Account Enabled or Disabled:** 계정을 사용하도록 설정하거나 사용하지 않도록 설정했을 때의 이벤트입니다.
- **Identity Source:** ID 소스의 추가, 삭제 또는 편집에 대한 이벤트입니다.

vSphere Client에서 이벤트 데이터는 **모니터** 탭에 표시됩니다. "vSphere 모니터링 및 성능" 설명서를 참조하십시오.

SSO 감사 이벤트 데이터에는 다음과 같은 세부 정보가 포함됩니다.

- 이벤트가 발생했을 때의 타임 스탬프
- 작업을 수행한 사용자
- 이벤트에 대한 설명
- 이벤트의 심각도
- vCenter Server에 연결하는 데 사용된 클라이언트의 IP 주소(가능한 경우)

SSO 감사 이벤트 로그 개요

vSphere Single-Sign On 프로세스는 `/var/log/audit/sso-events/` 디렉토리에 있는 `audit_events.log` 파일에 감사 이벤트를 기록합니다.

경고 `audit_events.log` 파일을 수동으로 편집하면 감사 로깅이 실패할 수 있으므로 절대 이 파일을 수동으로 편집하지 마십시오.

`audit_events.log` 파일을 사용할 때는 다음 사항에 유의하십시오.

- 로그 파일은 크기가 50MB에 도달하면 아카이브됩니다.
- 최대 10개의 아카이브 파일이 보관됩니다. 이 제한에 도달하면 새 아카이브가 생성될 때 가장 오래된 파일이 삭제됩니다.
- 아카이브 파일은 `audit_events-<인덱스>.log.gz` 형식으로 이름이 지정됩니다. 여기서 인덱스는 1부터 10까지의 숫자입니다. 생성되는 첫 번째 아카이브의 인덱스가 1이고, 아카이브가 생성될 때마다 인덱스가 증가합니다.

- 가장 오래된 이벤트는 아카이브 인덱스 1에 있습니다. 인덱스가 가장 높은 파일이 가장 최근 아카이브입니다.

보안 및 규정 준수 이해 다음 단계

보안 평가 수행은 인프라에 있을 수 있는 취약점을 파악하는 첫 번째 단계입니다. 보안 평가는 보안 감사의 일환이며, 보안 규정 준수를 비롯한 사례와 시스템을 모두 살펴봅니다.

일반적으로 보안 평가는 조직의 물리적 인프라(방화벽, 네트워크, 하드웨어 등)를 검색하여 취약점 및 결함을 식별하는 것을 말합니다. 보안 평가는 보안 감사와 동일하지 않습니다. 보안 감사에는 물리적 인프라에 대한 검토뿐만 아니라 보안 규정 준수를 비롯한 정책 및 표준 운영 절차와 같은 다른 영역도 포함됩니다. 감사를 거친 후에는 시스템 내에서 문제를 해결하는 단계를 결정할 수 있습니다.

보안 감사를 수행하려고 준비할 때 다음과 같이 일반적인 질문을 할 수 있습니다.

1 귀사는 준수 규정을 준수해야 합니까? 그렇다면 어떤 규정을 준수해야 합니까?

2 귀사의 감사 간격은 어떻게 됩니까?

3 귀사의 내부 자체 평가 간격이 어떻게 됩니까?

4 이전 감사 결과에 대한 액세스 권한이 있고 이전 감사 결과를 살펴본 적이 있습니까?

5 귀사의 감사 준비를 돕기 위해 타사 감사 회사를 이용합니까? 그렇다면 해당 회사의 가상화에 대한 설비 수준이 어떻게 됩니까?

6 귀사는 시스템 및 애플리케이션에 대한 취약점 검색을 실행합니까? 언제 얼마나 자주 수행합니까?

7 귀사의 내부적인 사이버 보안 정책은 무엇입니까?

8 감사 로깅이 필요에 맞게 구성되어 있습니까? 감사 로깅의 내용을 참조하십시오.

어디서부터 시작해야 하는지에 대한 구체적인 지침이나 방향이 없다면, 다음을 수행하여 vSphere 환경에 대한 보안을 신속하게 시작할 수 있습니다.

- 최신 소프트웨어 및 펌웨어 패치를 통해 환경을 최신 상태로 유지
- 모든 계정에 대해 우수한 암호 관리 및 예방 조치 유지
- 벤더가 승인한 보안 권장 사항 검토
- VMware 보안 구성 가이드 참조(vSphere 보안 구성 가이드 이해 참조)
- NIST, ISO 등과 같은 정책 프레임워크에서 언제든지 사용이 가능한 검증된 지침을 사용
- PCI, DISA 및 FedRAMP와 같은 규정 준수 프레임워크의 지침 따르기

vCenter Server 및 FIPS

vSphere 7.0 업데이트 2 이상은 vCenter Server Appliance에서 FIPS 검증 암호화를 사용하도록 설정할 수 있습니다.

FIPS 140-2는 암호화 모듈에 대한 보안 요구 사항을 규정하는 미국 및 캐나다 정부 표준입니다. vSphere에서는 FIPS 검증 암호화 모듈을 사용하여 FIPS 140-2 표준에서 지정하는 모듈과 일치시킵니다. vSphere FIPS 지원의 목표는 다양한 규제 환경에서 규정 준수 및 보안 활동을 용이하게 하는 것입니다.

In vSphere 6.7 이상에서 ESXi 및 vCenter Server는 FIPS 검증 암호화를 사용하여 관리 인터페이스 및 VMCA(VMware Certificate Authority)를 보호합니다.

vSphere 7.0 업데이트 2 이상은 vCenter Server Appliance에 FIPS 검증 암호화를 추가합니다. 기본적으로 이 FIPS 검증 옵션은 사용되지 않도록 설정되어 있습니다.

참고 vSphere에서는 FIPS보다 호환성이 우선되므로 일부 구성 요소에는 알아두어야 할 고려 사항이 있습니다. FIPS 사용 시 고려 사항의 내용을 참조하십시오.

FIPS 모듈

암호화 모듈은 보안 기능을 구현하는 하드웨어, 소프트웨어 또는 펌웨어의 집합입니다. ESXi는 여러 FIPS 140-2 검증 암호화 모듈을 사용합니다.

다음 표는 ESXi에서 사용 중인 FIPS 140-2 검증 암호화 모듈 집합을 보여줍니다.

표 17-3. FIPS 모듈

암호화 모듈	보안 정책 버전	알고리즘(CAVP)	암호화 모듈 검증 프로그램
Vmkernel 암호화 모듈	1.0	AES, SHS, DRBG, HMAC(C 1172)	인증서 #3073
Vmkernel 암호화 모듈 로더	해당 없음	HMAC, SHS(C 1171)	인증서 #3073
VMkernel DRBG 암호화 모듈	해당 없음	AES, DRBG(C 499)	해당 없음
VMware OpenSSL FIPS 개체 모듈	2.0.20-vmw	DRBG, AES, SHS, HMAC, DSA, RSA, ECDSA, KAS-FFC, KAS-ECC(C 470)	인증서 #3550 및 #3857

vCenter Server Appliance에서 FIPS 사용 또는 사용 안 함

HTTP 요청을 사용하여 vCenter Server Appliance에서 FIPS 검증 암호화를 사용하거나 사용하지 않도록 설정할 수 있습니다.

다양한 방법을 사용하여 HTTP 요청을 실행할 수 있습니다. 이 작업은 vSphere Client의 개발자 센터를 사용하여 vCenter Server Appliance에서 FIPS를 사용 및 사용하지 않도록 설정하는 방법을 보여 줍니다. vCenter Server Appliance에서 작동하도록 API를 사용하는 방법에 대한 자세한 내용은 "VMware vCenter Server 관리 프로그래밍 가이드" 를 참조하십시오.

절차

1 vSphere Client를 사용하여 vCenter Server 시스템에 로그인합니다.

2 메뉴에서 **개발자 센터**를 선택합니다.

3 **API 탐색기**를 클릭합니다.

4 **API 선택** 드롭다운 메뉴에서 **장치**를 선택합니다.

5 범주를 아래로 스크롤하여 **system/security/global_fips**를 확장합니다.

6 **GET**을 확장하고 **평가판 사용** 아래에서 **실행**을 클릭합니다.

응답 아래에서 현재 설정을 볼 수 있습니다.

7 설정을 변경합니다.

a FIPS를 사용하도록 설정하려면 **PUT**을 확장하고 `request_body`에 다음을 입력하고 **실행**을 클릭합니다.

```
{
"enabled":true
}
```

b FIPS를 사용하지 않도록 설정하려면 **PUT**을 확장하고 `request_body`에 다음을 입력하고 **실행**을 클릭합니다.

```
{
"enabled":false
}
```

결과

FIPS를 사용하거나 사용하지 않도록 설정한 후 vCenter Server Appliance가 재부팅됩니다.

FIPS 사용 시 고려 사항

vCenter Server Appliance에서 FIPS를 사용하도록 설정하는 경우 일부 구성 요소는 현재 기능적 제약 조건이 있습니다.

vCenter Server에서 FIPS를 사용하도록 설정한 경우 차이는 없지만 몇 가지 고려해야 할 사항이 있습니다.

표 17-4. FIPS 고려 사항

제품 또는 구성 요소	고려 사항	해결 방법
vSphere Single Sign-On	FIPS를 사용하도록 설정하는 경우 vCenter Server는 페더레이션된 인증을 위한 암호화 모듈만 지원합니다. 그 결과 RSA SecureID와 일부 CAC 카드는 더 이상 작동하지 않습니다.	페더레이션된 인증만 사용합니다. 자세한 내용은 "vSphere 인증" 설명서를 참조하십시오.
비 VMware 및 파트너 vSphere Client UI 플러그인	이러한 플러그인은 FIPS를 사용하도록 설정한 경우 작동하지 않을 수 있습니다.	규정 준수 암호화 라이브러리를 사용하려면 플러그인을 업그레이드합니다. https://code.vmware.com/docs/13385/preparing-local-plug-ins-for-fips-compliance에서 "FIPS 규정 준수를 위한 로컬 플러그인 준비"를 참조하십시오.
vCenter Server 파일 기반 백업 및 복원 메커니즘	SMB를 사용한 파일 기반 백업 및 복원은 FIPS 규격이 아닙니다.	백업 및 복원에는 다른 프로토콜(FTP, FTPS, HTTP, HTTPS, SFTP 또는 NFS)을 사용하십시오.