CA Access Control for Virtual Environments

제품 안내서

r2.0

타사 고지 사항

CONTAINS IBM(R) 32-bit Runtime Environment for AIX(TM), Java(TM) 2 Technology Edition, Version 1.4 Modules

샘플 스크립트와 샘플 SDK 코드

CA Access Control 제품에 포함된 샘플 스크립트와 샘플 SDK 코드는 정보 제공 목적으로만 "있는 그대로" 제공됩니다. 이 항목은 특정 환경에 맞게 수정이 필요할 수 있으며, 프로덕션 환경에 사용하려면 프로덕션 시스템에 배포하기 전에 반드시 테스트 및 검사를 수행해야 합니다.

CA Technologies 는 이러한 샘플에 대한 지원을 제공하지 않으며 이 스크립트로 인한 어떠한 오류에도 책임을 지지 않습니다.

CA 제품 참조

이 문서는 다음 CA Technologies 제품을 참조합니다 :

- CA Access Control Enterprise Edition
- CA Access Control
- CA User Activity Reporting Module
- CA Identity Manager

설명서 규칙

CA Access Control 설명서는 다음과 같은 규칙을 따릅니다.

형식	의미
고정 폭 글꼴	코드 또는 프로그램 출력
기울임꼴	강조 또는 새 용어
굵게	표시된 대로 동일하게 입력해야 하는 텍스트
슬래시(/)	UNIX 및 Windows 경로를 기술하는 데 사용되는 플랫폼 독립적인 디렉터리 구분 기호

이 설명서는 또한 명령 구문과 사용자 입력(고정 폭 글꼴로 표시됨)을 설명할 때 다음과 같은 특별한 규칙을 사용합니다.

형식	의미
기울임꼴	반드시 입력해야 하는 정보
대괄호([ ]) 사이	선택적 피연산자
중괄호({ }) 사이	필수 피연산자 집합
파이프(|)로 구분된 선택 사항	대체 피연산자(하나 선택)를 구분합니다. 예를 들어, 다음은 사용자 이름 *또는* 그룹 이름 중 *하나*라는 의미입니다. {*username*|*groupname*}

형식	의미
...	앞의 항목 또는 항목 그룹이 반복될 수 있음을 나타냅니다.
밑줄	기본값
줄 마지막에 공백 다음의 백슬래시(\)	때때로 이 안내서에서 명령이 한 줄에 모두 표시되지 않는 경우가 있습니다. 이런 경우에는 줄 끝에 공백과 백슬래시(\)를 표시하여 명령이 다음 줄에서 계속됨을 나타냅니다. **참고:** 실제 명령을 입력할 때는 이러한 백슬래시를 포함하지 말고 줄바꿈 없이 명령을 한 줄에 입력하십시오. 백슬래시 및 줄바꿈은 실제 명령 구문에 포함되지 않습니다.

예제: 명령 표기 규칙

다음 코드는 이 안내서에서 명령 규칙이 사용되는 방식을 보여 줍니다.

ruler *className* [props({all|{*propertyName1*[,*propertyName2*]...})]

설명:

- 표시되는 그대로 입력해야 하는 명령 이름(ruler)은 일반 고정 폭 글꼴로 표시됩니다.
- *className* 옵션은 클래스 이름(예: USER)이 들어갈 자리이므로 기울임꼴로 표시됩니다.
- 대괄호로 묶인 두 번째 부분은 선택적 피연산자를 의미하므로 이 부분 없이 명령을 실행할 수도 있습니다.
- 옵션 매개 변수(props)를 사용할 때 키워드 *all*을 선택하거나 하나 이상의 속성 이름을 쉼표로 구분하여 지정할 수 있습니다.

파일 위치 규칙

CA Access Control 설명서는 다음과 같은 파일 위치 규칙을 따릅니다.

- *ACVEInstallDir* - 기본 CA Access Control for Virtual Environments 설치 디렉터리:
  - /opt/CA/AccessControlServer/VirtualAppliance
- *ACInstallDir* - 기본 CA Access Control 설치 디렉터리입니다.
  - /opt/CA/AccessControl
- *ACSharedDir* - UNIX 에서 CA Access Control 에 의해 사용되는 기본 디렉터리입니다.
  - /opt/CA/SharedComponents
- *ACServerInstallDir* - 기본 CA Access Control 엔터프라이즈 관리 설치 디렉터리입니다.
  - /opt/CA/AccessControlServer
- *JBoss_HOME* - 기본 JBoss 설치 디렉터리입니다.
  - /opt/jboss-4.2.3.GA

CA 에 문의

기술 지원팀에 문의

온라인 기술 지원 및 지사 목록, 기본 서비스 시간, 전화 번호에 대해서는 http://www.ca.com/worldwide에서 기술 지원팀에 문의하십시오.

목차

제 4 장: CA Access Control for Virtual Environments 관리 35

제 1 장: 소개

이 섹션은 다음 항목을 포함하고 있습니다.

안내서 정보

이 안내서는 VMware vCenter 환경에서 CA Access Control for Virtual Environments 를 계획하고, 배포하고, 구성하고, 관리하는 방법에 대한 정보를 제공합니다.

이 안내서는 회사에서 VMware 기반 가상화 환경을 관리하고 보안을 유지하는 작업을 하는 시스템, 보안, VMware 관리자를 대상으로 합니다.

환경에서 CA Access Control for Virtual Environments 의 배포 및 구성을 시작하기 전에 이 안내서를 읽으십시오.

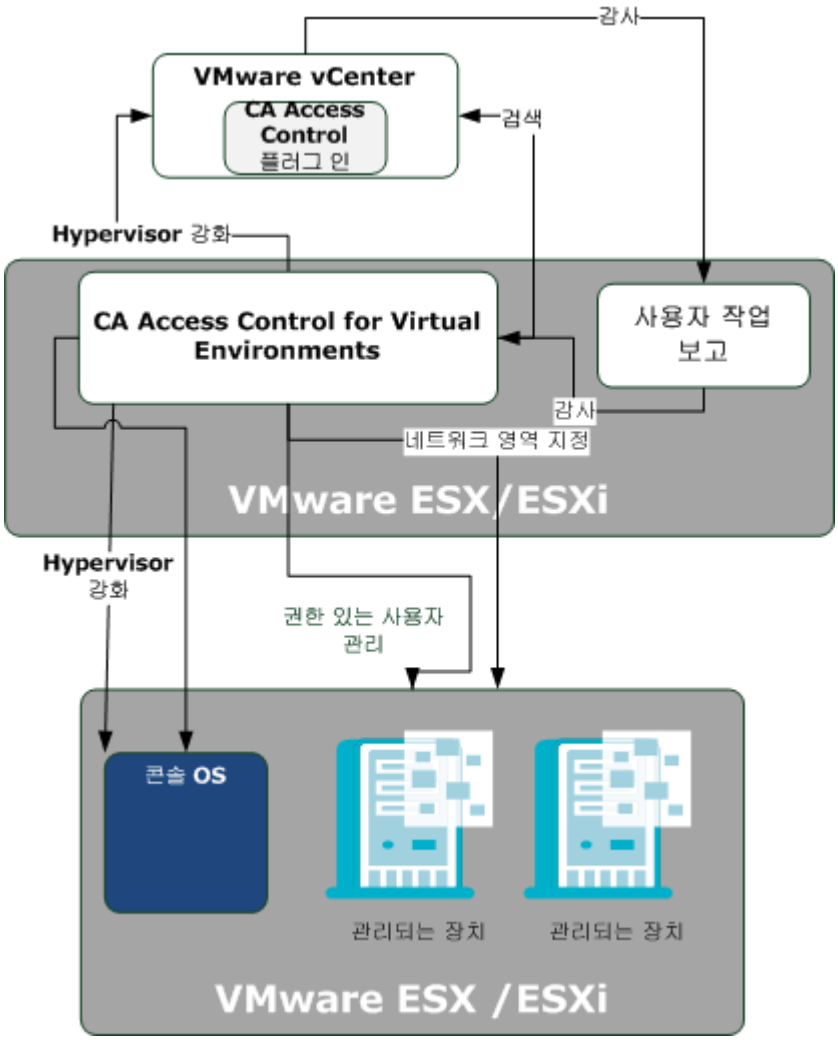
용어를 간단히 하기 위해 이 안내서에서는 제품을 CA Access Control 이라고 칭합니다.

CA Access Control for Virtual Environments 정보

CA Access Control for Virtual Environments(CA VE)는 가상 환경의 규모가 커짐에 따라 확장 가능한 가상 환경에 대한 권한 있는 사용자 액세스의 보안을 유지하기 위한 독립 실행형 솔루션입니다. CA Access Control for Virtual Environments 는 VMware vCenter 와 통합되어 관리되는 장치, 보안 그룹, 네트워크 영역, 정책을 제어할 수 있는 관리 인터페이스를 제공합니다. 태그, 태그 규칙, 정책을 사용하여 CA Access Control for Virtual Environments 는 많은 관리 작업을 자동화함으로써 가상 환경을 관리하는 데 도움을 줍니다.

CA Access Control for Virtual Environments 환경 아키텍처

다음 다이어그램은 CA Access Control for Virtual Environments 환경 아키텍처를 표시합니다.

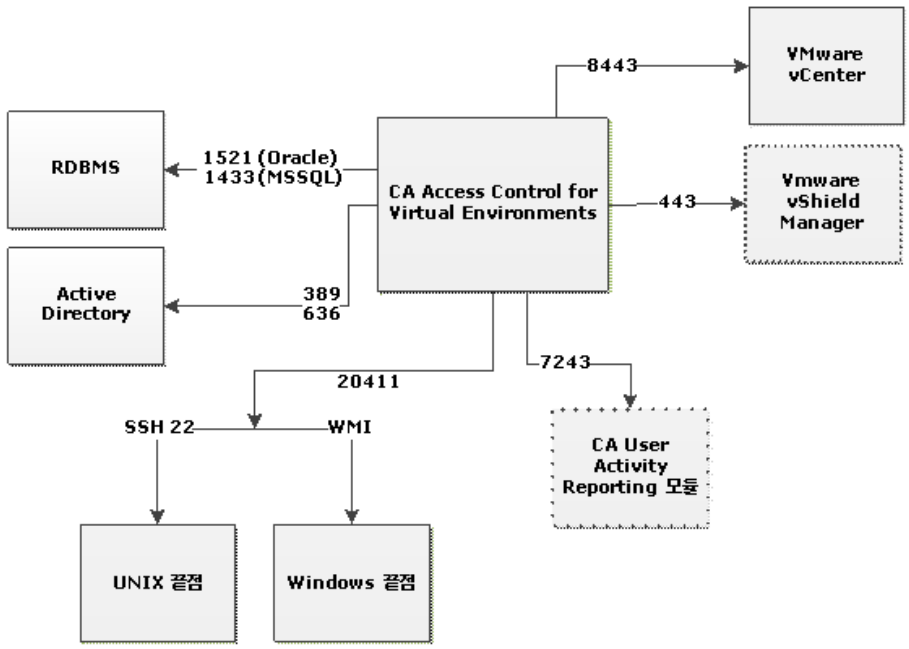


앞의 다이어그램에서 설명한 것처럼 CA Access Control for Virtual Environments 는 다음을 수행합니다.

- 가상 환경의 관리되는 장치에서 권한 있는 사용자 암호 관리
- VMware ESX/ESXi 서버에서 Hypervisor 강화
- 네트워크 영역 지정
- CA User Activity Reporting Module 보고서 생성을 위해 관리되는 장치로부터 감사 이벤트 수집

CA Access Control for Virtual Environments 네트워크 프로토콜 및 포트

다음 다이어그램은 CA Access Control for Virtual Environments 가 사용하는 네트워크 프로토콜 및 포트를 표시합니다.



참고: 점선은 선택적 구성 요소를 나타냅니다.

Access Control 이 보호하는 엔티티

CA Access Control for Virtual Environments 는 다음 엔터티를 보호하고 개선합니다.

- **Hypervisor** - CA Access Control for Virtual Environments 는 여러 강화 수준을 지원합니다. 강화 정책은 VMware vCenter Server 에 대한 사용자 로그인을 제한하고, 원격 감사 수집, 원격 관리, SNMP 트랩 수집을 제어합니다.
- **관리되는 장치** - CA Access Control for Virtual Environments 는 권한 있는 계정 암호를 관리하기 위해 암호 잠금 정책을 배포할 수 있도록 함으로써 관리되는 장치를 보호합니다. 또한 관리되는 장치를 네트워크 영역에 할당하고 감사 수집 정책을 통해 감사 레코드를 수집할 수도 있습니다.

권한 있는 계정 암호 관리

CA Access Control for Virtual Environments 는 환경에 있는 관리되는 장치에서 권한 있는 계정 암호를 검색하여 이 암호를 자체 데이터베이스에 저장합니다. CA Access Control for Virtual Environments 는 또한 권한 있는 계정 및 응용 프로그램 ID 암호를 안전하게 저장하고 정의하는 정책에 기반하여 권한 있는 계정 및 암호에 대한 액세스를 제어합니다.

네트워크 트래픽 격리

CA Access Control for Virtual Environments 는 *보안 그룹*에 관리되는 장치를 할당하여 네트워크 트래픽 및 액세스를 제어합니다. 보안 그룹은 그룹 구성원에 대해 보안 제어를 강제하는 관리되는 장치의 논리적 그룹입니다. 보안 그룹의 각 구성원은 네트워크 영역 내 모든 다른 구성원과 통신할 수 있습니다.

CA Access Control for Virtual Environments 는 VMware vShield Manager 와 통합되어 네이티브 방화벽 기능을 사용하여 네트워크 액세스 규칙을 시행합니다.

가상 환경 도구 및 인터페이스 개선

CA Access Control for Virtual Environments 는 네이티브 VMware 가상 관리 도구를 개선합니다. CA Access Control for Virtual Environments 는 VMware vSphere Client 에 플러그 인으로 추가되어 권한 있는 암호 관리 기능을 추가함으로써 네이티브 환경의 편의를 높입니다.

더 나아가, CA Access Control for Virtual Environments 는 VMWare vShield App 와 통합되어 네트워크 액세스 규칙을 시행합니다. VMware vShield Manager 는 액세스 제어 정책을 시행하는 vNIC 수준 방화벽입니다.

자산 태깅

자산 태깅을 사용하면 관리되는 장치 및 보안 그룹에 논리적 태그를 할당할 수 있습니다. 태그를 할당하면 관리되는 장치는 해당 태그가 적용되는 보안 그룹의 구성원이 됩니다.

태그를 수동으로 관리되는 장치에 할당하고 이 장치를 보안 그룹에 추가할 수 있습니다. 태그 규칙을 정의하고 관리되는 장치에 할당한 태그에 따라 보안 그룹에 관리되는 장치를 연결하도록 규칙 조건을 설정할 수 있습니다.

제 2 장: 구현 준비

이 섹션은 다음 항목을 포함하고 있습니다.

구현 크기 계획

CA Access Control for Virtual Environments 를 구현하기 전에 구현의 크기를 결정하고 이 크기에 적절한 리소스를 할당하십시오. 다음 정보는 구현의 크기를 산정하는 데 도움이 됩니다.

다음 표는 CA Access Control for Virtual Environments 의 지원되는 구성에 대해 설명합니다.

구성 요소	제한
호스트당 가상 컴퓨터	320
vCenter Server 당 호스트	3200
vCenter Server 당 등록된 가상 컴퓨터	15000
데이터 센터당 가상 컴퓨터	5000
vCenter Server 당 실행되는 가상 컴퓨터	10000

CA Access Control for Virtual Environments 의 구성 요소

CA Access Control for Virtual Environments 는 다음 소프트웨어 구성 요소를 포함하고 있습니다.

CA Access Control 서버

CA Access Control 서버는 CA Access Control for Virtual Environments 배포의 일부로 설치되며 VMware ESX/ESXi 서버에 배치됩니다. CA Access Control 서버는 다음을 관리합니다.

- 네트워크 트래픽 관리
- 네트워크 영역 관리
- 권한 있는 암호 관리
- Hypervisor 강화

CA Access Control 엔터프라이즈 관리

CA Access Control 엔터프라이즈 관리는 회사를 관리하는 사용하는 사용자 인터페이스입니다. 제품의 최초 설치가 완료된 이후에 사용자 인터페이스에 대해 스스로 친숙해지도록 하는 것이 좋습니다.

엔터프라이즈 관리에서 다음을 수행할 수 있습니다.

- 회사 전체에서 CA Access Control for Virtual Environments 의 구현을 봅니다.
- 호스트 및 호스트 그룹을 구성하고 정책을 보안 그룹 및 PUPM 끝점에 할당합니다.
- 권한 있는 계정 암호를 체크 아웃 및 체크 인합니다.
- 권한 있는 계정, 끝점, 암호 정책, 암호 소비자를 구성합니다.
- 보고서를 표시하고, 스냅숏 정의를 관리하고, 스냅숏 데이터를 캡처합니다.
- 사용자, 그룹, 역할, 작업을 관리합니다.
- 시스템 전반의 연결 설정을 관리합니다.
- 태그 및 태그 규칙을 관리합니다.
- 감사 레코드를 봅니다.

참고: CA Access Control 엔터프라이즈 관리에서 작업을 완료하는 방법에 대한 자세한 내용은 *온라인 도움말*을 참조하십시오.

CA Access Control 플러그 인

CA Access Control 플러그 인은 가상 환경을 관리하는 데 도움을 줍니다. 이 플러그 인은 VMware vCenter Server 에 포함되며 VMware vSphere Client 에서 다음을 수행할 수 있게 해 줍니다.

- PUPM 끝점 및 암호 검색
- 권한 있는 계정 암호 관리
- 관리되는 장치에 태그 할당
- CA User Activity Reporting Module 보고서 표시

중앙 RDBMS

중앙 RDBMS 는 다음 항목을 저장합니다.

- 보고서에서 사용되는 끝점 데이터
- 권한 있는 계정 암호
- 웹 기반 응용 프로그램의 세션 데이터
- 웹 기반 응용 프로그램의 사용자 데이터(사용자 저장소로 Active Directory 를 사용하지 않는 경우)

사용자 저장소

Active Directory 또는 데이터베이스에 정의된 그룹 및 사용자를 사용하도록 CA Access Control for Virtual Environments 를 구성할 수 있습니다. 따라서 모든 사용자에 대해 하나의 데이터 저장소를 사용할 수 있습니다.

제 3 장: CA Access Control for Virtual Environments 구현

이 섹션은 다음 항목을 포함하고 있습니다.

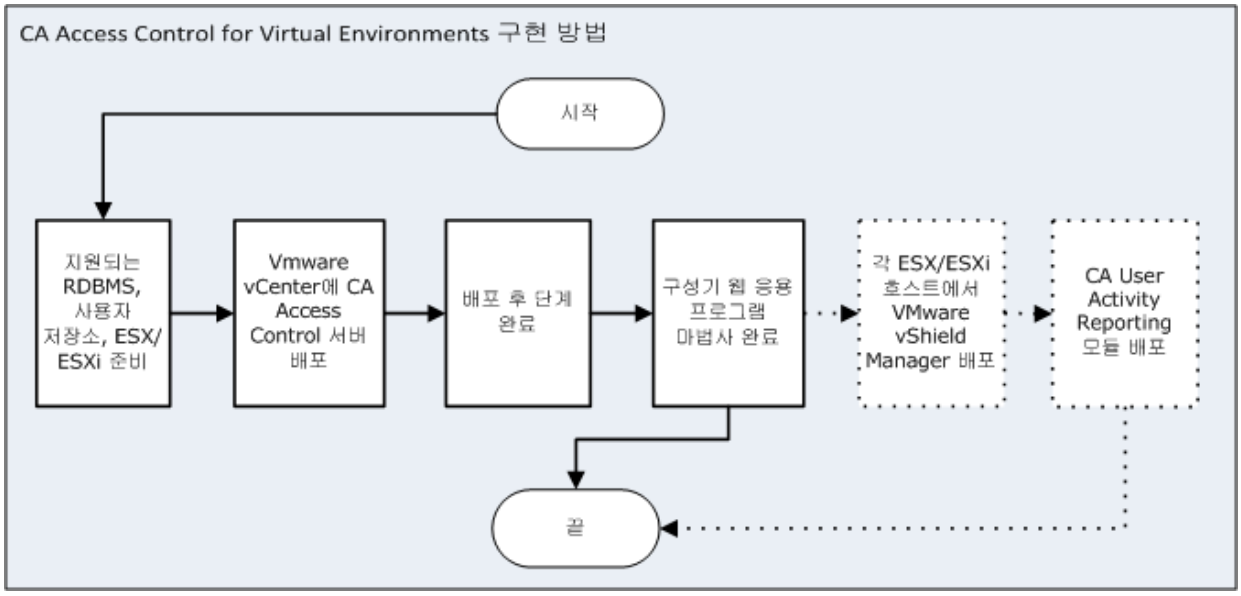
CA Access Control for Virtual Environments 가상 어플라이언스

CA Access Control for Virtual Environments 는 가상 어플라이언스로 배포됩니다. *가상 어플라이언스*는 미리 설치되어 구성된 운영 체제와 응용 프로그램 패키지를 갖춘 가상 컴퓨터입니다.

CA Access Control for Virtual Environments 구현 방법

CA Access Control for Virtual Environments 는 권한 있는 계정을 관리하고, 네트워크 영역 지정을 구성하고, hypervisor 및 감사 수집 정책을 작성하고, 자산에 태그를 할당할 수 있게 합니다.

다음 다이어그램은 CA Access Control for Virtual Environments 를 구성하는 방법을 설명합니다.



다음에 주의하십시오.

- 지원되는 RDBMS 및 사용자 저장소에 대한 자세한 내용은 *릴리스 정보*를 참조하십시오.
- 점선은 선택적 단계를 나타냅니다.

CA Access Control 서버 배포

CA Access Control for Virtual Environments 가상 어플라이언스의 배포는 운영 체제를 설치하고, CA Access Control 서버를 설치하고, ESX/ESXi 서버에 가상 컴퓨터를 만듭니다.

다음 단계를 수행하십시오.

1. VMware vSphere Client 를 열고 "File"(파일), "Deploy OVF Template"(OVF 템플릿 배포)로 이동합니다.

   "Deploy OVF Template"(OVF 템플릿 배포) 마법사가 열립니다.

2. "Deploy from File"(파일에서 배포) 단추를 클릭한 다음 CA Access Control for Virtual Environments OVF 템플릿을 찾습니다.

3. "다음"을 클릭합니다.

   OVF 템플릿 정보 화면이 나타납니다. 다음 작업을 수행하십시오.

   a. 정보를 검토하고 "Next"(다음)를 클릭하여 계속합니다.

      "End User License Agreement"(최종 사용자 사용권 계약) 페이지가 나타납니다.

   b. 라이선스 계약을 읽고 "Accept"(동의함)를 선택한 다음 "Next"(다음)를 클릭합니다.

      "Name and Location"(이름 및 위치) 화면이 나타납니다.

   c. 가상 컴퓨터 이름을 지정하고 가상 어플라이언스를 배포할 폴더를 선택합니다. "다음"을 클릭합니다.

      "Host/Cluster"(호스트/클러스터) 화면이 열립니다.

      참고: 이 화면은 OVF 템플릿의 배포를 시작하기 전에 리소스 풀을 선택하지 않은 경우에만 나타납니다.

   d. 가상 어플라이언스를 호스트할 데이터 센터를 선택합니다. "다음"을 클릭합니다.

      "Resource Pool"(리소스 풀) 화면이 열립니다.

   e. 템플릿을 배포할 리소스 풀을 선택합니다. "다음"을 클릭합니다.

      "Datastore"(데이터 저장소) 화면이 열립니다.

   f. 가상 어플라이언스를 저장할 데이터 저장소를 선택합니다. "다음"을 클릭합니다.

      네트워크 매핑 화면이 열립니다.

g. 사용할 네트워크를 선택합니다. "다음"을 클릭합니다.

참고: OVF 템플릿이 사용하는 네트워크를 환경에서 정의된 네트워크로 매핑할 수 있습니다.

네트워킹 속성 화면이 나타납니다.

h. 다음 필드를 완료하십시오.

Domain Names(도메인 이름)

호스트 이름 조회에 대한 검색 경로를 지정합니다. 여러 검색 경로를 지정할 수 있습니다.

Host Name(호스트 이름)

가상 컴퓨터의 정규화된 이름을 지정합니다.

Time zone(표준 시간대)

CA Access Control 서버가 있는 표준 시간대를 지정합니다.

Default gateway(기본 게이트웨이)

기본 게이트웨이 IP 주소를 지정합니다. DHCP가 사용되는 경우 이 필드를 비워두십시오.

DNS

이 가상 컴퓨터에 대한 DNS 서버를 지정합니다. DHCP가 사용되는 경우 이 필드를 비워두십시오.

Network IP Address(네트워크 IP 주소)

가상 컴퓨터 IP 주소를 지정합니다. DHCP가 사용되는 경우 이 필드를 비워두십시오.

Network Netmask(네트워크 마스크)

선택한 네트워크 카드에 대한 네트워크 마스크 또는 접두사를 지정합니다. DHCP가 사용되는 경우 이 필드를 비워두십시오.

i. "다음"을 클릭합니다.

j. 배포 설정을 검토하고 "Finish"(마침)을 클릭합니다.

VMware vSphere Client 가 템플릿을 배포하고 지정한 위치에 가상 컴퓨터를 추가합니다. 이 과정은 완료할 때까지 몇 분 정도 걸릴 수 있습니다. 템플릿이 성공적으로 배포되었음을 알리는 메시지가 나타납니다.

4. VMware vSphere Client 에서 CA Access Control for Virtual Environments 컴퓨터의 전원을 켭니다.

   CA Access Control for Virtual Environments 설치 과정이 시작됩니다. 이 작업은 완료될 때까지 몇 분 정도 걸릴 수 있습니다.

5. "Console"(콘솔) 탭으로 이동합니다.

6. root 및 superadminuser 사용자 계정의 암호를 정의합니다.

   다음에 주의하십시오.

   - 원격 root 로그인은 기본적으로 차단됩니다. root 계정을 사용하여 CA Access Control for Virtual Environments 컴퓨터 콘솔에만 로그인할 수 있습니다.
   - superadminuser 계정을 사용하여 가상 컴퓨터를 원격으로 관리할 수 있습니다. 예를 들어, SSH 를 사용합니다.
   - 기본적으로 superadminuser 에게는 root 계정과 동일한 암호가 할당됩니다. 기본 암호를 변경하려면 CA Access Control for Virtual Environments 콘솔에서 passwd superadminuser 명령을 실행하십시오.

7. (선택 사항) 자동으로 감지되지 않은 경우 네트워크 설정과 호스트 이름을 정의합니다. 설정을 변경하려면 'N'을 입력하고 설정을 승인하려면 'Y'를 입력하십시오.

8. 'Y'를 입력하여 설치를 완료합니다.

   CA Access Control for Virtual Environments 설치가 완료되었습니다. 이 과정은 완료할 때까지 몇 분 정도 걸릴 수 있습니다.

9. root 사용자 계정 암호를 입력하여 CA Access Control for Virtual Environments 에 로그인합니다.

   CA Access Control for Virtual Environments 가 성공적으로 배포되었습니다. 이제 배포 후 작업을 완료해야 합니다.

배포 후 작업

환경에서 CA Access Control for Virtual Environments 가상 어플라이언스를 배포한 후에는 다음 절차를 완료하여 사용자 저장소와 데이터베이스 연결 정보를 구성하십시오.

중앙 데이터베이스를 준비하는 방법

CA Access Control for Virtual Environments 에는 RDBMS(relational database management system)가 필요하므로, CA Access Control for Virtual Environments 를 구성하기 전에 데이터베이스를 준비해야 합니다.

1. 이미 설치되지 않은 경우 지원되는 RDBMS 를 중앙 데이터베이스로 설치합니다.

   RDBMS 를 설치하기 전에 다음을 참고하십시오.

   - 지원되는 RDBMS 소프트웨어 목록을 보려면 릴리스 정보를 참조하십시오.
   - CA Access Control for Virtual Environments 가상 컴퓨터에 중앙 데이터베이스를 설치할 필요가 없습니다. RDBMS 의 시스템 요구 사항에 대한 자세한 내용은 제품의 설명서를 참조하십시오.

2. CA Access Control 엔터프라이즈 관리를 위해 RDBMS 를 구성합니다.

   로컬에서와 원격 클라이언트에서 데이터베이스에 액세스할 수 있어야 합니다.

   - SQL 서버의 경우 다음을 수행하십시오.
     - 대소문자를 구분하지 *않는* 새 데이터베이스를 만듭니다.
     - 정렬 순서를 SQL_Latin1_General_CP1_CI_AS 로 설정합니다.
     - 새 사용자를 만들고, 새 데이터베이스를 사용자의 기본 데이터베이스로 만들고, 사용자에게 다음 권한을 할당합니다: DBCREATOR, SYSADMIN

- Oracle 의 경우 다음을 수행하십시오.
  - 중앙 데이터베이스를 위한 새 사용자를 만들고 다음 권한을 할당합니다.

    CONNECT (다음과 같은 시스템 권한 부여: ALTER SESSION, CREATE CLUSTER, CREATE DATABASE LINK, CREATE SEQUENCE, CREATE SESSION, CREATE SYNONYM, CREATE TABLE, CREATE VIEW)

    RESOURCE (다음과 같은 시스템 권한 부여: CREATE CLUSTER, CREATE INDEXTYPE, CREATE OPERATOR, CREATE PROCEDURE, CREATE SEQUENCE, CREATE TABLE, CREATE TRIGGER, CREATE TYPE)
  - 다음 쿼리를 사용하여 CA Access Control for Virtual Environments 데이터베이스에 사용자 추가 권한을 부여합니다.

    grant adminiser database trigger to <*DB_USER*>;
  - CA Access Control for Virtual Environments 를 호스트하는 테이블스페이스에 대한 할당량을 무제한으로 설정합니다.

데이터베이스 연결 정보 구성

CA Access Control for Virtual Environments 에는 RDBMS(relational database management system)가 필요하므로,

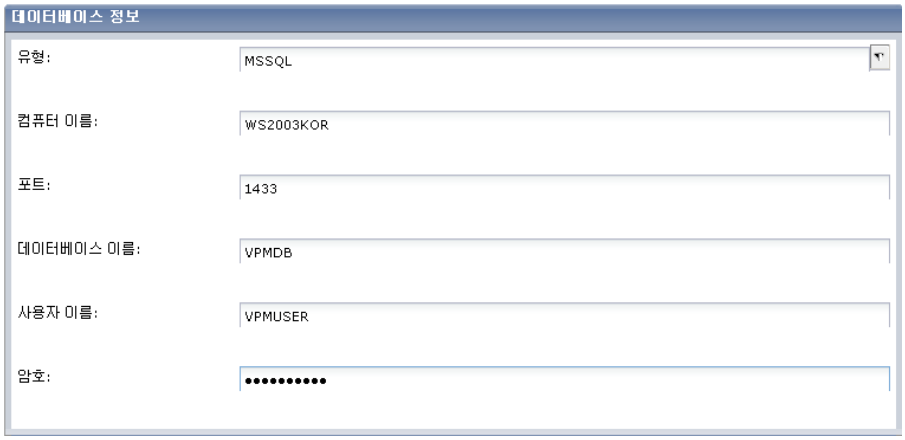
다음 단계를 수행하십시오.

1. 웹 브라우저를 열고 호스트에 대해 다음 URL 을 입력합니다.

   https://*enterprise_host*:18443/iam/ac

   예: https://192.168.1.1:18443/iam/ac

   CA 가상 어플라이언스 구성 마법사가 나타나 데이터베이스 정보 테이블을 표시합니다.



2. 다음 필드를 완료하십시오.

   데이터베이스 유형 - 지원되는 RDBMS 를 지정합니다.

   컴퓨터 이름 - RDBMS 가 설치된 호스트의 이름을 지정합니다.

   포트 번호 - RDBMS 에서 사용하는 포트를 정의합니다.

   - **Oracle** - 1521
   - **SQL** - 1433

   데이터베이스 이름 - 만든 데이터베이스의 이름을 정의합니다.

   사용자 이름 - CA Access Control for Virtual Environments 가 데이터베이스에 연결하기 위해 사용하는 사용자 이름을 정의합니다. 데이터베이스를 준비할 때 만든 사용자 이름을 지정하십시오.

3. "다음"을 클릭합니다.

   서버 이름 구성 화면이 열립니다.

4. 엔터프라이즈 관리 서버의 정규화된 이름을 정의합니다.

5. "다음"을 클릭합니다.

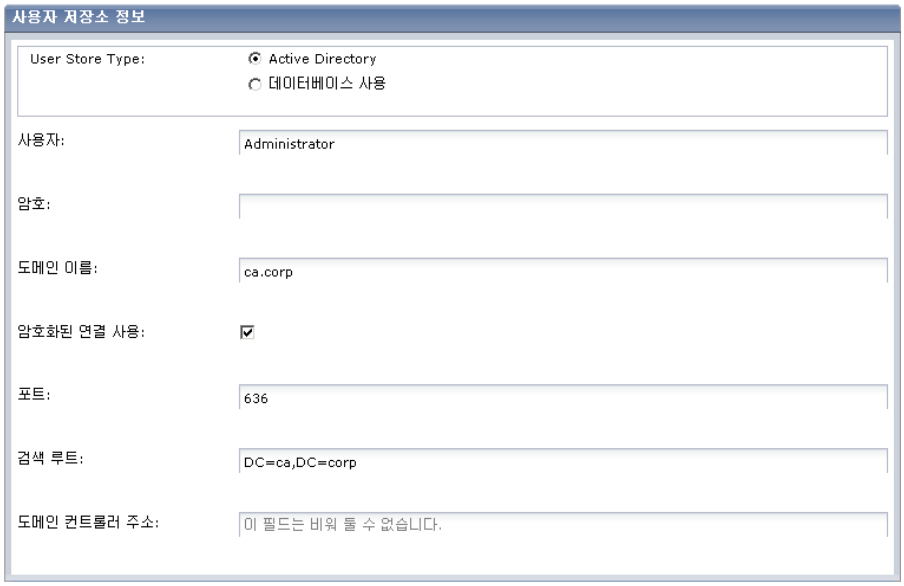
   설치 프로그램은 계속하기 전에 데이터베이스에 대한 연결을 검사합니다. 이제 사용자 저장소 연결 정보를 구성하십시오.

사용자 저장소 연결 정보 구성

CA Access Control for Virtual Environments 는 Active Directory 와 이전에 사용자 저장소로 지정한 데이터베이스를 지원합니다.

다음 단계를 수행하십시오.

1. CA 가상 어플라이언스 구성 화면에서 사용자 저장소 유형을 선택합니다.



다음 중 *하나*를 선택하십시오.

Active Directory - 세부적인 연결 정보를 지정합니다.

데이터베이스 - DBMS 에 사용자 정보를 저장합니다.

2. (Active Directory) 다음 필드를 완료합니다.

사용자

CA Access Control for Virtual Environments를 관리하는 데 사용된 Active Directory 사용자 계정 이름을 정의합니다.

참고: 이 매개 변수에 대한 읽기 전용 권한을 갖는 사용자를 정의할 수 있습니다.

암호

CA Access Control for Virtual Environments를 관리하는 데 사용된 Active Directory 사용자 계정의 암호를 정의합니다.

도메인 이름

Active Directory DNS 도메인 이름을 정의합니다.

암호화된 연결 사용

Active Directory에 암호화된 연결을 사용하도록 지정합니다.

포트

Active Directory에 대한 LDAP 쿼리에 기본적으로 사용되는 포트를 정의합니다. 예: 636

검색 루트

검색 루트를 정의합니다. 예: ou=DomainName, DC=com

참고: 검색 루트는 사용자가 정의된 컨테이너보다 디렉터리에서 1개 노드 이상 높게 설정하십시오. 그렇지 않으면 CA Access Control for Virtual Environments가 시작될 때 탭이 표시되지 않을 수 있습니다.

도메인 컨트롤러 주소

도메인 컨트롤러 IP 주소를 정의합니다.

설치 프로그램이 계속하기 전에 Active Directory 에 대한 연결을 검사합니다.

3. (데이터베이스) 데이터베이스를 준비할 때 만든 사용자의 RDBMS 암호를 정의합니다.
4. "다음"을 클릭합니다.

   시스템 사용자 화면이 열립니다.
5. 다음 필드를 완료하십시오.

   시스템 사용자

   (Active Directory 에만 해당) CA Access Control for Virtual Environments 에서 시스템 관리자 관리 역할이 할당된 Active Directory 사용자의 DN 을 정의합니다.

   참고: 기본적으로 시스템 관리자 관리 역할이 있는 사용자는 CA Access Control for Virtual Environments 에서 모든 작업을 수행하고, 만들고, 관리할 수 있습니다. 시스템 관리자 관리 역할에 대한 자세한 내용은 *엔터프라이즈 관리 안내서*를 참조하십시오.

   암호

   (데이터베이스만 해당) CA Access Control for Virtual Environments 관리자인 *superadmin* 의 암호를 정의합니다. 설치가 완료되었을 때 CA Access Control for Virtual Environments 에 로그인할 수 있도록 암호를 메모해 두십시오.

   참고: 이 단계에서 데이터베이스에 superadmin 사용자를 만듭니다. superadmin 사용자는 CA Access Control 엔터프라이즈 관리에서 시스템 관리자 관리 역할이 할당됩니다. CA Access Control for Virtual Environments 에 처음 로그인할 때 superadmin 으로 로그인합니다. 시스템 관리자 관리 역할에 대한 자세한 내용은 *엔터프라이즈 관리 안내서*를 참조하십시오.
6. "다음"을 클릭합니다.

   데이터베이스와 사용자 저장소 연결 정보를 정의했습니다. VMware vCenter 에 대한 연결을 구성합니다.

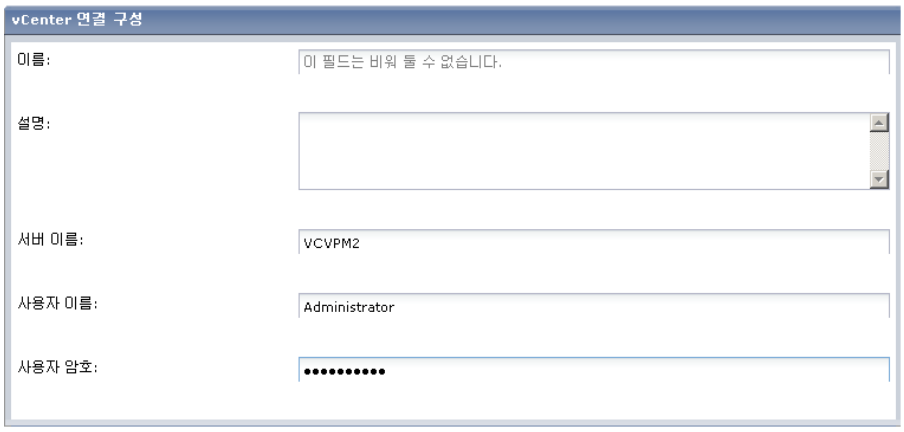
VMware vCenter Server 에 대한 연결 구성

VMware vCenter 에 대한 연결을 구성하여 CA Access Control 보안 기능을 VMware vCenter Server 의 관리되는 장치와 통합하십시오.

다음 단계를 수행하십시오.

1. CA 가상 어플라이언스 구성 마법사에서 "vCenter 연결 구성"으로 이동합니다.

   다음 화면이 나타납니다.



   대화 상자의 필드를 완성합니다.

   이름

   VMware vCenter 연결에 사용할 이름을 정의합니다.

   설명

   (선택 사항) 이 VMware vCenter 연결에 대한 설명을 정의합니다.

   서버 이름

   관리할 VMware vCenter Server 의 DNS 이름을 정의합니다.

   예: vcenter.company.com

   사용자 이름

   VMware vCenter Server 관리 권한이 있는 사용자 계정의 이름을 정의합니다.

   암호

   VMware vCenter Server 관리 권한이 있는 사용자 계정의 암호를 정의합니다.

2. "다음"을 클릭합니다.

   CA Access Control for Virtual Environments 가 설정을 검사하고 공유 암호 화면으로 계속 진행합니다.

3. 다음 필드를 완료합니다.

   통신 암호

   CA Access Control 엔터프라이즈 관리 서버의 구성 요소 간 통신에 사용되는 암호를 정의합니다. "다음"을 클릭합니다.

   서버 이름 구성 화면이 열립니다.

4. 엔터프라이즈 관리 서버의 정규화된 이름을 정의합니다. "다음"을 클릭합니다.

   요약 화면이 열립니다.

5. 정보를 검토하고 "마침"을 클릭하여 마법사를 완료합니다.

   CA Access Control for Virtual Environments 가 데이터베이스와 사용자 저장소를 사용하기 위해 구성합니다.

   CA Access Control for Virtual Environments 는 사용자가 지정한 정보를 사용하여 VMware vCenter Server 에 연결을 시도합니다. 정보가 정확하면 연결이 설정되고 VMware vSphere Client 를 사용하여 CA Access Control for Virtual Environments 의 엔터프라이즈 배포를 관리할 수 있게 됩니다. 정보가 정확하지 않으면 CA Access Control for Virtual Environments 가 VMware vCenter 에 연결하지 못하고 오류 메시지가 표시됩니다. 연결하지 못한 이유가 메시지가 설명됩니다.

SSL 통신을 사용하도록 CA Access Control for Virtual Environments 를 구성하는 방법

기본적으로 CA Access Control for Virtual Environments 는 자체 서명된 인증서를 사용하는 SSL 지원을 통해 설치됩니다. 다른 인증서를 사용하여 SSL 지원을 구성하려면 Active Directory 를 사용하여 작업할 때 SSL 을 사용하도록 CA Access Control for Virtual Environments 를 구성하십시오.

다음 단계를 수행하십시오.

1. DER, CRT, CERT 형식으로 사용자 디렉터리 인증서를 획득합니다.
2. 인증서를 키 저장소에 추가합니다.

추가 정보:

사용자 디렉터리 인증서를 키 저장소에 추가 (페이지 32)

사용자 디렉터리 인증서를 키 저장소에 추가

SSL 통신을 사용하도록 CA Access Control for Virtual Environments 를 구성하기 전에 사용자 디렉터리 인증서를 키 저장소에 추가하십시오.

참고: Active Directory 또는 CA Directory 에서 SSL 을 구성하는 방법에 대한 자세한 내용은 Active Directory 및 CA Directory 설명서를 참조하십시오.

예: Active Directory 인증서를 키 저장소에 추가

중요! 이 예는 Active Directory 와의 보안 통신을 위해 SSL 을 사용하도록 CA Access Control for Virtual Environments 를 구성하는 방법을 보여줍니다. 이 절차를 시작하기 전에 DER, CER, CERT 암호화된 바이너리 형식의 Active Directory 인증서를 획득해야 합니다.

1. CA Access Control 서버에서 JBoss 가 실행 중인 경우 중지합니다. 다음 작업을 수행하십시오.
   - JBoss 작업 창에서 프로세스를 인터럽트(Ctrl+C)합니다.
2. 다음 디렉터리로 이동합니다. 여기서 *JBOSS_HOME* 은 JBoss 가 설치된 디렉터리를 나타냅니다.

   JBOSS_HOME/server/default/deploy/IdentityMinder.ear/custom/ppm/truststore
3. 다음 명령을 입력합니다.

   keytool -import -keystore ssl.keystore -*alias ad* -file <*activedirecoty.cert*>

   암호 프롬프트가 나타납니다.

   -import

   유틸리티가 인증서를 읽어 키 저장소에 저장하도록 지정합니다.

   -alias

   키 저장소에 항목을 추가하기 위해 사용할 별칭을 지정합니다.

   -file

   Active Directory 인증서 파일의 전체 경로 이름을 지정합니다.

4. 암호 *secret* 를 입력합니다.
5. JBoss bin 디렉터리로 이동합니다. 기본적으로 이 디렉터리는 다음 위치에 있습니다.

   JbossInstallDir/bin

6. run.bat 파일을 열고 트러스트된 사용자 저장소 데이터로 java_ops 매개 변수를 설정합니다. 예:

   set JAVA_OPTS=%JAVA_OPTS% -Xms128m -Xmx512m
   -Djavax.net.ssl.trustStore=C:\jboss-4.2.3.GA\server\default\deploy\IdentityMinder.ear\custom\ppm\truststore\ssl.keystor
   e

7. 파일을 저장하고 JBoss 를 시작합니다.

   키 저장소에 사용자 저장소 인증서를 추가했습니다.

제 4 장: CA Access Control for Virtual Environments 관리

이 섹션은 다음 항목을 포함하고 있습니다.

CA Access Control for Virtual Environments 열기

CA Access Control 서버를 설치 및 시작한 후에 CA Access Control for Virtual Environments 에 대한 URL 을 사용하여 원격 컴퓨터에서 웹 기반 인터페이스를 시작할 수 있습니다.

Follow these steps:

1. 웹 브라우저를 열고 호스트에 대해 다음 URL 을 입력합니다.

   https://*enterprise_host:18443*/iam/ac

2. CA Access Control 서버를 설치할 때 지정한 자격 증명을 사용하여 로그인합니다.

   CA Access Control for Virtual Environments 홈 페이지가 나타납니다.

예: CA Access Control for Virtual Environments 열기

네트워크에 있는 임의의 컴퓨터에서 CA Access Control for Virtual Environments 를 열려면 웹 브라우저에 다음 URL 을 입력하십시오.

https://appserver123:18443/iam/ac

이 URL 은 CA Access Control for Virtual Environments 가 appserver123 이라는 이름의 호스트에 설치되었으며 기본 CA Access Control for Virtual Environments SSL 포트 18443 을 사용함을 나타냅니다.

월드 뷰

CA Access Control for Virtual Environments 의 월드 뷰를 사용하면 관리하는 CA Access Control for Virtual Environments 의 엔터프라이즈 구현을 볼 수 있습니다.

월드 뷰를 사용하여 다음을 수행할 수 있습니다.

- CA Access Control for Virtual Environments 에 의해 관리되는 장치 및 보안 그룹의 식별
- VMware vCenter 계층 탐색
- 관리되는 장치 및 보안 그룹에 대한 정보 보기. 이 정보에는 어떤 정책이 배포되었고, 그룹 및 관리되는 장치의 총 수, 각 장치의 규정 준수 상태 등이 포함됩니다.
- 관리되는 장치 또는 보안 그룹 관리
- 정책, 구성원, 태그, 태그 규칙을 할당 또는 제거할 보안 그룹 관리

엔터프라이즈 구현 관리

CA Access Control 엔터프라이즈 관리를 사용하여 CA Access Control for Virtual Environments 의 엔터프라이즈 구현을 보고 관리할 수 있습니다. 엔터프라이즈 "월드 뷰"는 PUPM 끝점 및 관리되는 장치, 그 논리 보안 그룹, 배포된 정책, 정책 태그의 스냅숏입니다.

엔터프라이즈 배포 스냅숏은 VMware vCenter Server 에 구성한 관리되는 장치 및 그룹 계층에 기반합니다. VMware vCenter 의 계층에 대한 모든 변경 사항은 월드 뷰에도 표시됩니다.

다음 단계를 수행하십시오.

1. "월드 뷰" 탭, "보안 그룹", "보안 그룹 관리"로 이동합니다.

   "보안 그룹 관리" 페이지가 나타나 CA Access Control 서버에 의해 정의된 VMware vCenter Server 의 보안 그룹과 논리 그룹을 표시합니다.

   참고: CA Access Control for Virtual Environments 관리되는 장치에 대해서만 계층을 구성, 수정, 변경할 수 있습니다.

2. (선택 사항) CA Access Control 서버에서 추가 관리되는 장치, 보안 그룹, 태그, 태그 규칙을 정의할 수 있습니다. "작업" 메뉴에서 다음을 선택합니다.

   - 보안 그룹 만들기 (페이지 38)
   - 태그 만들기 (페이지 49)
   - 태그 규칙 만들기 (페이지 50)
   - 정책 상태 보기

3. "보안 그룹" 섹션에서 보안 그룹을 선택합니다.

   CA Access Control 엔터프라이즈 관리는 보안 그룹 정보, 할당된 정책, 그룹 구성원, 각 구성원의 규정 준수 상태를 표시합니다.

4. "정책 추가"를 선택하여 보안 그룹 정책을 관리합니다.

   다음은 사용 가능한 정책입니다.

   - 네트워크 영역 (페이지 45) - 네트워크 분리 정책 구성
   - 감사 수집 (페이지 57) - CA User Activity Reporting Module 감사 수집 정책 구성
   - Hypervisor 강화 (페이지 54) - hypervisor 강화 정책 구성
   - 암호 잠금 (페이지 42) - 권한 있는 계정 암호 잠금 정책 구성

5. (선택 사항) "구성"을 선택하여 기존 정책을 수정하거나 "제거"를 선택하여 정책을 제거합니다.

보안 그룹 만들기

환경에 있는 보안 그룹을 관리하여 구성원을 추가 또는 제거하거나 태그를 할당 또는 제거합니다.

다음 단계를 수행하십시오.

1. "월드 뷰" 탭, "보안 그룹", "보안 그룹 관리"로 이동합니다.

   "보안 그룹 관리" 페이지가 나타나 VMware vCenter Server 에 있는 보안 그룹 및 CA Access Control 서버 정보를 표시합니다.

2. 만들기 또는 수정을 선택하여 보안 그룹 구성에 액세스합니다.

   "일반" 탭이 열립니다.

3. 다음 필드를 완료하십시오.

   이름

   보안 그룹의 이름을 표시합니다.

   설명

   보안 그룹의 설명을 지정합니다.

   소유자

   보안 그룹의 소유자 이름을 지정합니다.

   조직 단위

   보안 그룹의 부서 단위를 지정합니다.

4. "관리되는 장치 선택" 탭을 선택합니다.

   호스트 선택 탭이 열립니다.

5. "추가"를 클릭하여 관리되는 장치를 그룹에 추가합니다.
6. "보안 그룹 구성원" 탭을 선택합니다.

   그룹 구성원 탭이 열리고 그룹의 구성원인 보안 그룹을 표시합니다.

7. "추가"를 클릭하여 보안 그룹을 그룹의 구성원으로 추가합니다.

8. "태그" 탭을 선택합니다.

   태그 탭이 열리고 할당된 태그를 표시합니다.

9. "추가"를 클릭하여 태그를 컴퓨터 그룹에 할당합니다.

10. "태그별 구성원 자격" 탭을 선택합니다.

    태그별 구성원 자격 탭이 열립니다.

11. AND 를 클릭하여 구성원 자격 기준에 태그를 추가합니다. ADD 를 클릭하여 조건 목록에 태그를 추가하십시오.

    목록에 구성원 자격 기준이 추가됩니다.

    참고: 하나의 구성원 자격 기준에 최대 3 개까지 태그를 추가할 수 있습니다.

12. "제출"을 클릭합니다.

    CA Access Control 엔터프라이즈 관리가 변경 내용을 보안 그룹에 커밋합니다.

태그 구성원 자격 기준 정보

관리되는 장치 관리를 자동화하고 간편하게 하기 위해 태그 구성원 자격 기준을 사용할 수 있습니다. 태그 구성원 기준을 사용하면 정의하는 규칙 조건을 따르는 구성원을 포함하는 보안 그룹을 정의할 수 있습니다. CA Access Control for Virtual Environments 는 조건 규칙이 보안 그룹에 적용되는 각 관리되는 장치를 자동으로 추가합니다.

태그 구성원 자격 기준은 다음 구문을 사용합니다.

[tag1] AND | OR [tag2] AND | OR [tag3]

예: 태그 구성원 기준 만들기

이 예에서는 "개발", "회계", "마케팅" 태그 중 하나가 할당된 관리되는 장치에 할당할 태그 구성원 자격 기준을 구성합니다.

개발 OR 회계 OR 마케팅

이 예에서는 "회계" 및 "마케팅" 태그만 할당된 관리되는 장치에 자동으로 할당할 태그 구성원 자격 기준을 구성합니다.

회계 AND 마케팅

관리되는 장치 상태 보기

상태 보기에서 관리되는 장치와 관련된 오류 및 경고 메시지를 검토할 수 있습니다. 경고에는 보안 그룹에 할당하는 배포된 정책에 대한 정보가 표시됩니다.

다음 단계를 수행하십시오.

1. "월드 뷰", "보기", "상태"를 선택합니다.

   상태 창이 열리고 가장 최신 경고를 표시합니다.
2. 모든 메시지를 보거나 오류 및 경고 메시지만 보도록 선택합니다.
3. "새로 고침"을 클릭하여 경고 목록을 갱신합니다.

권한 있는 계정 암호 관리

권한 있는 계정 암호 잠금 정책은 통합된 정책을 구성하고 보안 그룹에 있는 모든 권한 있는 계정에 할당할 수 있게 해 줍니다.

CA Access Control for Virtual Environments 가 끝점과 계정을 만드는 방법

CA Access Control for Virtual Environments 는 자동으로 PUPM 끝점을 만들고, 권한 있는 계정을 검색하고, 암호 정책을 계정 암호에 할당합니다.

다음 프로세스는 CA Access Control for Virtual Environments 가 PUPM 끝점 및 계정을 구성하는 방법을 설명합니다.

1. 가상화 관리자가 PUPM 끝점을 보안 그룹에 추가합니다.
2. 관리자가 보안 그룹의 각 끝점 유형에 대해 CA Access Control 엔터프라이즈 관리에 관리 권한이 있는 연결 끊긴 권한 있는 계정을 만듭니다.

   CA Access Control for Virtual Environments 는 연결 끊긴 계정을 사용하여 각 끝점에 연결하고 권한 있는 계정 암호를 검색합니다.
3. CA Access Control 엔터프라이즈 관리에서 관리자는 암호 잠금 정책을 구성하고 보안 그룹에 이 정책을 할당합니다.
4. CA Access Control for Virtual Environments 는 끝점을 검색하고 끝점 연결 설정을 자동으로 구성하고 이 끝점에서 권한 있는 계정을 구성하려고 시도합니다.
5. 성공하면 CA Access Control for Virtual Environments 는 해당 끝점 유형에서 권한 있는 계정을 사용하기 위해 끝점 권한 있는 계정 역할을 만듭니다.

   예를 들어, Windows Agentless 끝점에서 권한 있는 계정을 처음 발견했을 때 CA Access Control for Virtual Environments 는 자동으로 Windows Agentless Connection 끝점 권한 있는 액세스 역할을 만듭니다.
6. CA Access Control for Virtual Environments 는 자동으로 권한 있는 계정 암호 정책을 보안 그룹의 각 구성원의 권한 있는 계정에 할당합니다.

계정 암호 잠금 정책 구성

CA Access Control for Virtual Environments 가 관리하는 각 보안 그룹에 대해 계정 암호 잠금 정책을 구성합니다. CA Access Control for Virtual Environments 는 그룹에 추가하는 각 관리되는 장치에서 권한 있는 암호 잠금 정책을 시행합니다.

중요! 이 절차를 완료하기 전에 CA Access Control for Virtual Environments 가 만들어 관리하도록 할 각 끝점 유형에 대해 관리 권한이 있는 권한 있는 계정을 만드십시오.

다음 단계를 수행하십시오.

1. "월드 뷰", "보안 그룹", "보안 그룹 관리"로 이동합니다.

   "보안 그룹 관리" 페이지가 나타나 VMware vCenter 에 있는 보안 그룹 및 CA Access Control 서버 정보를 표시합니다.

2. 보안 그룹을 선택합니다.

   CA Access Control 엔터프라이즈 관리는 보안 그룹 정보와 구성원을 표시합니다.

3. "작업" 메뉴에서 "계정 암호 정책 추가"를 선택합니다.

   관리 암호 잠금: *호스트 이름* 창이 열립니다.

4. 드롭다운 메뉴에서 운영 체제 프로필을 선택합니다. 옵션:

   - Windows 컴퓨터 프로필
   - Linux 컴퓨터 프로필
   - Solaris 컴퓨터 프로필

   각 운영 체제 프로필에 대해 특정 암호 잠금 정책을 구성할 수 있습니다.

5. 다음 필드를 완료하십시오.

설명

암호 잠금 정책에 대한 설명을 지정합니다.

운영 체제 프로필

이전에 선택한 운영 체제 프로필을 표시합니다.

연결 계정

CA Access Control for Virtual Environments 가 각 관리되는 장치를 연결하는 데 사용하는 관리자 사용자 계정을 정의합니다. "계정 만들기"를 선택하여 관리자 계정을 만듭니다.

연결 계정 잠금

연결 계정이 연결된 계정임을 지정합니다.

관리되는 계정

CA Access Control for Virtual Environments 가 각 관리되는 장치에 만드는 권한 있는 계정을 정의합니다.

암호 정책

권한 있는 계정 또는 서비스 계정에 적용할 암호 정책을 지정합니다. "암호 정책 만들기"를 선택하여 암호 정책을 만듭니다.

체크 아웃 만료

체크 아웃 계정이 만료되는 기간(분)을 정의합니다.

배타적 계정

한 번에 하나의 사용자만 계정에 액세스할 수 있는지 여부를 지정합니다. *배타적 계정*은 한 번에 하나의 사용자만 권한 있는 계정을 사용하도록 제한합니다.

체크 아웃 시 암호 변경

CA Access Control 엔터프라이즈 관리가 권한 있는 계정을 체크 아웃할 때마다 이 계정 암호를 변경할지 여부를 지정합니다.

체크 인 시 암호 변경

사용자 또는 프로그램이 권한 있는 계정을 체크 인할 때마다 또는 체크 아웃 기간이 만료될 때 CA Access Control 엔터프라이즈 관리가 이 계정 암호를 변경할지 여부를 지정합니다.

참고: 배타적 계정이 아닌 경우 CA Access Control 엔터프라이즈 관리는 *모든* 사용자가 계정을 체크 인한 경우에만 새 권한 있는 계정 암호를 생성합니다.

참고: 이 옵션은 서비스 계정에 적용되지 않습니다.

로그인 응용 프로그램

로그인 응용 프로그램을 이 끝점에 할당하도록 지정합니다.

참고: 끝점에 할당하기 전에 로그인 응용 프로그램을 만드십시오. 동일한 끝점에 여러 개의 로그인 응용 프로그램을 할당할 수 있습니다.

6. "제출"을 클릭합니다.

   CA Access Control 엔터프라이즈 관리가 권한 있는 계정 암호 잠금 정책을 그룹에 제출합니다.

네트워크 분리

네트워크 분리는 호스트 또는 태그의 물리적 위치와 같은 일반 조건을 기준으로 보안 또는 가상화 관리자가 네트워크 영역에 있는 관리되는 장치의 그룹을 정의하는 데 사용하는 프로세스입니다.

네트워크 영역의 구성원은 해당 영역 내에서만 다른 구성원과 통신할 수 있으며 네트워크의 다른 네트워크 영역 또는 호스트에 액세스할 수 없습니다. 네트워크 서비스를 보안 그룹에 할당하여 구성원이 네트워크에 액세스할 수 있게 할 수 있습니다.

CA Access Control 엔터프라이즈 관리에서 네트워크 영역 정책 구성

정의하는 네트워크 분리 규칙은 네트워크 영역을 지정하고 보안 그룹에 적용됩니다. 적용되면 구성원은 이 영역 내에서만 통신할 수 있습니다. 보안 그룹을 정의하고 구성원을 그룹에 할당하거나 자동으로 생성된 보안 그룹을 사용할 수 있습니다.

참고: 네트워크 영역 정책을 구성하기 전에 사용할 네트워크 서비스를 정의하십시오.

다음 단계를 수행하십시오.

1. "월드 뷰", "보안 그룹", "보안 그룹 관리"로 이동합니다.

   "보안 그룹 관리" 페이지가 나타나 VMware vCenter 에 있는 보안 그룹 및 CA Access Control 서버 정보를 표시합니다.

2. 보안 그룹을 선택합니다.

   CA Access Control 엔터프라이즈 관리는 보안 그룹 정보와 구성원을 표시합니다.

3. "작업" 메뉴에서 "네트워크 영역 정책 추가"를 선택합니다.

   네트워크 규칙 관리 창이 열립니다.

4. 다음을 완성하십시오.

   설명

   네트워크 영역 정책의 설명을 지정합니다.

   서비스

   네트워크 영역 정책에 할당할 네트워크 서비스를 정의합니다. "추가"를 클릭하여 할당할 네트워크 서비스를 검색합니다.

   방향

   네트워크 서비스가 사용하도록 허가된 네트워크 트래픽 방향을 정의합니다.

   옵션: 인바운드, 아웃바운드, 양방향

5. "제출"을 클릭합니다.

   CA Access Control 엔터프라이즈 관리가 네트워크 분리 규칙을 제출합니다. 작업이 성공적으로 완료되었음을 알리는 확인 메시지가 표시됩니다.

   네트워크 영역 정책을 보안 그룹에 성공적으로 적용했습니다.

네트워크 서비스 구성

네트워크 영역의 구성원이 네트워크 영역 밖에 위치한 서비스와 리소스에 액세스하도록 보안 그룹에 대한 네트워크 서비스를 구성합니다.

다음 단계를 수행하십시오.

1. CA Access Control 엔터프라이즈 관리에서 다음을 수행합니다.
   a. "시스템"을 클릭합니다.
   b. "네트워크 서비스"를 클릭합니다.
   c. "네트워크 서비스 구성"을 선택합니다.

   네트워크 서비스 구성:네트워크 검색 구성 화면이 열립니다.
2. (선택 사항) 다음과 같이 사본을 만들기 위해 기존 네트워크 서비스를 선택합니다.
   a. 네트워크 서비스 유형의 개체를 만들도록 선택합니다.
   b. 검색 특성을 선택하고 필터 값을 입력한 다음 "검색"을 클릭합니다.

      필터 조건에 일치하는 네트워크 서비스의 목록이 표시됩니다.
   c. 새 네트워크 서비스에 대한 기준으로 사용할 개체를 선택합니다.

3. "확인"을 클릭합니다.

   "네트워크 서비스 만들기" 작업 페이지가 나타납니다. 기존 개체에서 네트워크 서비스를 만든 경우 기존 개체의 값이 대화 상자 필드에 미리 입력됩니다.

4. 다음 필드를 완성합니다. 다음 필드는 자동으로 채워지지 않습니다.

   네트워크 주소

   네트워크 서비스를 제공하는 호스트 이름 또는 IP 주소를 정의합니다.

   서비스

   네트워크 서비스 속성을 정의합니다.

   - 프로토콜 - UDP, TCP
   - 포트 번호
   - 서비스

5. "추가"를 클릭합니다.

   CA Access Control 엔터프라이즈 관리가 네트워크 서비스를 추가합니다.

   참고: 각 보안 그룹에 대해 하나 이상의 네트워크 서비스를 정의할 수 있습니다.

6. "제출"을 클릭합니다.

   CA Access Control 엔터프라이즈 관리가 작업을 제출하고 네트워크 서비스를 보안 그룹에 할당합니다.

자산 태깅

자산 태깅은 시스템, 보안 또는 가상 환경 관리자가 태그를 관리되는 장치 및 보안 그룹에 연계하는 프로세스입니다. 태그를 할당함으로써 관리자는 개별 자산을 그룹으로 관리하여 정책 배포를 자동화하고 관리 범위를 정의할 수 있습니다.

관리를 자동화하기 위해 각 관리되는 장치는 보안 그룹에 추가하는 태그를 상속 받습니다. 태깅 규칙은 IP 주소 범위와 같은 자산 특성을 기초로 정의할 수 있습니다. CA Access Control for Virtual Environments 가 그룹 내 모든 구성원에게 자동으로 배포하는 태깅 정책을 정의할 수도 있습니다.

관리자 보안 그룹에 태그를 사용하는 방법

태그 및 태그 규칙을 사용하면 편리하게 보안 그룹을 관리할 수 있습니다. 정의하는 태그 및 태그 규칙에 따라 CA Access Control 엔터프라이즈 관리는 자동으로 관리되는 장치를 보안 그룹에 추가하고 관리되는 장치에 정책을 적용할 수 있습니다.

다음 단계를 수행하십시오.

1. CA Access Control 엔터프라이즈 관리에 태그를 만듭니다.
2. 다음 중 *하나*를 수행합니다.
   - 관리되는 장치에 태그를 수동으로 할당

     관리되는 장치가 보안 그룹에 추가됩니다. 보안 그룹에 할당된 정책이 관리되는 장치에 적용됩니다.
   - 태그 규칙 만들기
3. 태그 규칙을 정의하고, 만든 규칙에 태그를 연결하고, 규칙 조건을 정의합니다.
4. CA Access Control 엔터프라이즈 관리는 다음을 수행합니다.
   a. 태그가 연결된 보안 그룹에 규칙을 적용합니다.
   b. 태그 규칙을 구성하는 각 관리되는 장치에 태그를 할당합니다.
   c. 태그 규칙을 따르는 관리되는 장치를 보안 그룹에 추가합니다
   d. 보안 그룹에 대해 구성한 정책을 관리되는 장치에 적용합니다.

   이제 보안 그룹의 관리되는 장치를 관리할 수 있습니다.

   참고: 태그 규칙을 삭제하면 CA Access Control 엔터프라이즈 관리는 보안 그룹의 관리되는 장치를 제거합니다.

CA Access Control 엔터프라이즈 관리에서 태그 구성

CA Access Control 엔터프라이즈 관리는 폴더, 데이터 센터, 리소스 풀 등의 관리되는 장치를 호스트 그룹에 매핑합니다. 보안 그룹에 태그를 할당하면 가상화된 환경에서 간편하게 자산을 관리할 수 있습니다. 할당하는 태그를 기초로 관리 범위 지정을 간편하게 수행할 수 있습니다.

다음 단계를 수행하십시오.

1. "월드 뷰", "태그", "태그 만들기"로 이동합니다.

   태그 만들기: 태그 검색 창이 열립니다.

2. (선택 사항) 다음과 같이 태그를 만들 때 복사하여 사용할 기존 태그를 선택합니다.

   a. "태그" 유형의 새 개체에 대한 복사본을 만들도록 선택합니다.

   b. 검색 특성을 선택하고 필터 값을 입력한 다음 "검색"을 클릭합니다.

      필터 조건에 일치하는 태그의 목록이 표시됩니다.

   c. 새 태그에 대한 기준으로 사용할 개체를 선택합니다.

3. "확인"을 클릭합니다.

   "태그 만들기" 창이 나타납니다.

4. 태그의 이름을 입력합니다.

5. "제출"을 클릭합니다.

   CA Access Control 엔터프라이즈 관리가 태그를 생성합니다. 이제 태그를 관리되는 장치에 할당하거나 태그 규칙을 만들 수 있습니다.

CA Access Control 엔터프라이즈 관리에 태그 규칙 만들기

정의하는 속성을 기준으로 관리되는 장치를 보안 그룹에 할당할 태그 규칙을 만듭니다. CA Access Control for Virtual Environments 가 태그 규칙과 일치하는 IP 주소의 관리되는 장치를 발견하면 이 장치가 태깅되고 보안 그룹과 연계됩니다.

다음 단계를 수행하십시오.

1. "월드 뷰", "태그", "태그 규칙 만들기"로 이동합니다.

   태그 규칙 만들기: 태그 규칙 검색 창이 열립니다.

2. (선택 사항) 다음과 같이 태그 규칙을 만들 때 복사하여 사용할 기존 태그를 선택합니다.

   a. "태그 규칙" 유형의 새 개체에 대한 복사본을 만들도록 선택합니다.

   b. 검색 특성을 선택하고 필터 값을 입력한 다음 "검색"을 클릭합니다.

      필터 조건에 일치하는 태그 규칙의 목록이 표시됩니다.

   c. 새 태그에 대한 기준으로 사용할 개체를 선택합니다.

3. "확인"을 클릭합니다.

   "태그 규칙 만들기" 창이 나타납니다.

4. 다음 필드를 완료하십시오.

   이름

   태그 규칙의 이름을 지정합니다.

   설명

   태그 규칙의 설명을 지정합니다.

   적용된 태그

   태깅된 규칙과 연계할 태그를 선택합니다.

   일치하는 개체 유형

   태그 규칙이 적용되는 개체 유형을 표시합니다.

   기준

   다음과 같이 태그 규칙 조건을 지정합니다.

   Name|*IP Address*|*Host*[equal|not equal] *managed_device*

   이름

   관리되는 장치 DNS 이름을 지정합니다.

   IP

   관리되는 장치 IP 주소를 지정합니다.

   OS 정보

   VMware vCenter에 정의된 대로 관리되는 장치 운영 체제를 지정합니다.

   VM 네트워크

   관리되는 장치가 사용하는 가상 네트워크의 이름을 지정합니다.

   주석

   VMware vCenter에 정의된 대로 주석 키와 값을 지정합니다.

   예: "Owner=John"

   참고: 여러 관리되는 장치에 태그를 적용하려면 와일드카드(*)를 사용하십시오.

5. "제출"을 클릭합니다.

CA Access Control 엔터프라이즈 관리는 태그 규칙을 만들어 관리되는 장치에 적용합니다.

VMware vSphere Client 에서 관리되는 장치에 태그 할당

VMware vSphere Client 에서 CA Access Control for Virtual Environments 가 관리하는 각 관리되는 장치에 태그를 할당할 수 있습니다.

다음 단계를 수행하십시오.

1. 왼쪽 창에서 관리되는 장치를 선택한 다음 CA Security 탭을 선택합니다.

   CA Security 탭이 열리고 요약 탭의 내용이 표시됩니다.
2. "태크 추가" 단추를 클릭합니다.
3. 풀다운 메뉴에서 태그를 선택한 다음 "확인"을 클릭합니다.

   태그가 관리되는 장치에 할당됩니다.

Hypervisor 강화

VMware hypervisor, vSphere Client 콘솔, 관리되는 장치는 악의적인 공격과 사용자에 의한 의도되지 않은 손상에 취약합니다. hypervisor 와 vSphere Client 콘솔을 강화하면 VMware 환경의 보안을 유지하고 보안 취약점을 줄이는 데 도움이 됩니다.

CA Access Control for Virtual Environments 는 시스템, 보안, VMware 관리자가 정책을 구성하는 데 도움을 줍니다. 정책은 CA Access Control 엔터프라이즈 관리에서 hypervisor 와 VMware vSphere Client 콘솔을 강화하고 정책을 호스트 그룹에 배포합니다.

참고: VMware hypervisor 와 vSphere Client 콘솔 강화에 대한 자세한 내용은 VMware 웹 사이트에서 *VMware vSphere Hardening Guide*(VMware vSphere 강화 안내서)를 참조하십시오.

Hypervisor 강화 정책

적용할 강화 수준을 결정하기 전에 다음과 같은 지원되는 hypervisor 강화 정책을 검토하십시오.

- **원격 액세스** - (ESXi 전용) ESXi 서버에 대한 모든 원격 액세스를 비활성화하기 위해 잠금 모드를 사용함으로써 원격 액세스를 제한합니다. 활성화되면 잠금 모드는 관리자들이 중앙 위치에서만 작업을 수행하도록 강제하여 감사되지 않는 작업 수행의 위험을 줄입니다.
- **원격 Syslog** - 중앙 위치에 이벤트를 로깅하면 관리 기능을 개선하고 중앙 위치에서 모든 장치를 모니터링할 수 있습니다. 더욱이, 이벤트를 중앙 위치에 저장하면 로그 손상을 방지하는 데 도움이 됩니다.
- **영구 로깅** - 데이터베이스가 서버 로그를 더 오래 유지하도록 영구 로깅을 구성합니다. 영구 로깅은 더 쉽게 이벤트를 모니터링하고 서버 문제를 진단할 수 있게 해 줍니다.
- **NTP 시간 동기화** - 잘못된 시간 설정은 공격을 파악하고 추적하는 것을 어렵게 합니다. NTP 시간 동기화를 구성하면 모든 시스템이 동일한 시간을 사용하므로 공격을 추적 및 식별하는 데 도움을 줍니다.
- **SNMP 구성** - (ESXi 전용) SNMP 에이전트가 올바로 구성되지 않으면 공격자는 악의적 호스트로 트랩을 리디렉션하거나 악의적 용도로 정보를 사용할 수 있습니다.
- **DCUI** - (ESXi 전용) DCUI(Direct Console User Interface)는 관리자가 호스트 구성 및 관리 작업을 수행할 수 있게 해 주는 ESXi 관리 콘솔입니다. 로컬 관리 권한이 있는 사용자는 DCUI 에서 직접 작업을 수행할 수 있으며 이러한 작업은 VMware vCenter Server 에서 감사되지 않습니다. 사용자가 ESXi 서버에서 직접 관리 작업을 수행하지 못하도록 하려면 DCUI 를 비활성화하십시오.
- **기술 지원 모드**(ESXi 전용) - 기술 지원 모드는 서버 콘솔 또는 SSH 콘솔에서 사용 가능한 대화형 명령줄입니다. 활성화되면 ESXi 서버에서 직접 문제 해결 및 지원 관련 작업을 수행할 수 있습니다. 서버에 대한 무단 액세스를 방지하려면 기술 지원 모드를 비활성화하십시오.
- **VMSafe Network API** - VMSafe Network API 는 가상화된 환경에 대한 보안 아키텍처를 제공합니다. VMSafe Network API 를 사용하지 않는 경우 VMSafe Network API 를 비활성화하십시오.

CA Access Control 엔터프라이즈 관리에서 Hypervisor 강화 정책 구성

hypervisor 강화 정책은 hypervisor 에 대한 사용자 액세스를 제한하고, 원격 시스템 로깅을 구성하고, 시간을 동기화하고, SNMP 에이전트 설정을 구성하는 데 도움을 줍니다.

참고: 가상 컴퓨터 액세스 권한을 관리하려면 시스템 관리자 역할이 할당되어야 합니다.

중요! 이 절차를 완성하기 전에 VMware vCenter Server 에 대한 연결을 구성하십시오. 또한 강화 정책을 적용할 각 hypervisor 에 대한 PUPM 끝점을 만드십시오.

다음 단계를 수행하십시오.

1. "월드 뷰", "보안 그룹", "보안 그룹 관리"로 이동합니다.

   "보안 그룹 관리" 페이지가 나타나 VMware vCenter Server 에 있는 보안 그룹 및 CA Access Control 서버 정보를 표시합니다.

2. 보안 그룹을 선택합니다.

   CA Access Control 엔터프라이즈 관리는 보안 그룹 정보와 구성원을 표시합니다.

   중요! 선택하는 보안 그룹에 그룹의 구성원으로서 하나 이상의 ESX 서버가 있는지 확인하십시오.

3. "작업" 메뉴에서 "Hypervisor 강화 정책 추가"를 선택합니다.

   "보안 그룹 Hypervisor 강화 관리" *호스트 그룹 이름* 페이지가 열립니다.

4. 다음 필드를 완료하십시오.

   설명

   강화 정책의 설명을 지정합니다.

   잠금

   hypervisor 에 대한 원격 액세스를 차단하도록 지정합니다.

   다이렉트 콘솔 UI

   로컬 관리 제어를 비활성화하도록 지정합니다.

기술 지원 모드

기술 지원 모드가 비활성화되도록 지정합니다.

기술 지원 모드 시간 만료

기술 지원 모드를 비활성화할 기간(초)을 지정합니다.

로컬 데이터 저장소 경로

(ESXi 전용) syslog 가 메시지를 로깅하는 데이터 저장소의 전체 경로 이름을 지정합니다.

예: [저장소 1]/var/log/messages

원격 Syslog 호스트

원격 syslog 호스트 이름을 정의합니다.

원격 포트

원격 syslog 호스트 포트 번호를 정의합니다.

NTP 서버

NTP(Network Time Protocol) 서버 이름을 지정합니다.

사용

SNMP 구성이 활성화되도록 지정합니다.

SNMP 포트

SNMP 수신 포트 번호를 정의합니다.

읽기 전용 커뮤니티

읽기 전용 액세스 권한이 있는 커뮤니티의 이름을 지정합니다.

예: snmp-server community public RO

트랩 대상

SNMP 트랩 대상 호스트 이름, 포트, 커뮤니티를 정의합니다.

형식: *target_hostname@port/community*

예: SNMP_host@55222/comm

VMSafe Network API

VMSafe Network API 의 사용을 비활성화하도록 지정합니다.

Hypervisor 관리자

hypervisor 관리자 계정의 이름을 정의합니다. CA Access Control for Virtual Environments 는 이 계정을 사용하여 hypervisor 에 연결합니다.

5. "제출"을 클릭합니다.

   CA Access Control 엔터프라이즈 관리가 그룹에 강화 정책을 배포합니다.

감사 수집

CA User Activity Reporting Module 을 사용하면 IT 활동을 수집, 정규화, 집계 및 보고하고 가능한 준수 위반이 발생할 경우 조치를 수행하라는 알림을 생성합니다.

CA User Activity Reporting Module 감사 수집 정책은 그룹에 할당하는 감사 수집 프로필에 따라 각 가상 컴퓨터 그룹에 대한 정책을 할당할 수 있게 해 줍니다.

참고: CA Access Control for Virtual Environments 및 CA User Activity Reporting Module 통합에 대한 자세한 내용은 *엔터프라이즈 관리 안내서*를 참조하십시오.

CA Access Control 엔터프라이즈 관리에서 감사 수집 정책 구성

CA Access Control for Virtual Environments 가 관리하는 각 보안 그룹에 대한 감사 수집 정책을 구성합니다. CA Access Control for Virtual Environments 는 그룹에 추가하는 각 가상 컴퓨터에서 감사 수집 정책을 시행합니다.

다음 단계를 수행하십시오.

1. "월드 뷰", "보안 그룹", "보안 그룹 관리"로 이동합니다.

   "보안 그룹 관리" 페이지가 나타나 VMware vCenter 에 있는 컴퓨터 그룹 및 CA Access Control 서버 정보를 표시합니다.

2. "보안 그룹" 섹션에서 그룹을 선택합니다.

   CA Access Control 엔터프라이즈 관리가 그룹 정보와 구성원을 표시합니다.

3. "작업" 메뉴에서 "감사 수집 정책 추가"를 선택합니다.

   보안 그룹 감사 수집 관리: *보안 그룹 이름* 창이 열립니다.

4. 다음 필드를 완료하십시오.

   설명

   감사 수집 정책에 대한 설명을 지정합니다.

   사용

   관리되는 장치에서 이벤트 수집을 활성화하도록 선택합니다.

   운영 체제 프로필

   감사 수집 정책을 적용할 운영 체제 프로필을 선택합니다.

   감사 수집 프로필

   CA User Activity Reporting Module 에 정의한 감사 수집 프로필을 지정합니다.

   프로파일 설명

   감사 수집 프로필에서 설명을 지정합니다.

   인증 계정

   CA User Activity Reporting Module 에 연결하는 데 사용된 사용자 계정을 정의합니다.

   참고: 이 필드는 선택한 감사 수집 프로필에 따라 활성화 또는 비활성화됩니다.

5. "제출"을 선택합니다.

CA Access Control 엔터프라이즈 관리는 감사 수집 프로필을 만들고 보안 그룹에 정책을 할당합니다. CA User Activity Reporting Module 은 이제 관리되는 장치로부터 감사 이벤트를 직접 수집할 수 있습니다.

VMware vSphere Client 에서 CA User Activity Reporting Module 보고서 보기

CA User Activity Reporting Module 이 관리되는 장치에서 감사 레코드를 수집하도록 구성된 경우 VMware vSphere Client 에서 CA User Activity Reporting Module 을 볼 수 있습니다.

다음 단계를 수행하십시오.

1. 왼쪽 창에서 관리되는 장치를 선택한 다음 CA Security 탭을 선택합니다.

   CA Security 탭이 열리고 요약 탭의 내용이 표시됩니다.
2. "사용자 작업 보고 모듈" 탭을 선택합니다.
3. 풀다운 메뉴에서 보고서를 선택합니다.

   보고서가 표시됩니다.

권한 있는 계정 암호 검색

권한 있는 계정 암호 검색은 CA Access Control for Virtual Environments 가 권한 있는 계정과 응용 프로그램 ID 암호를 검색하고, 저장하고, 관리하는 데 사용하는 프로세스입니다. 검색되면 CA Access Control for Virtual Environments 를 사용하여 정의하는 정책을 기준으로 권한 있는 계정 및 암호에 대한 액세스를 제어할 수 있습니다.

VMware vSphere Client 에서 수동으로 권한 있는 계정 암호 검색

권한 있는 계정 암호에 대한 액세스를 제어하려면 먼저 관리되는 장치에서 권한 있는 계정을 식별한 다음 CA Access Control for Virtual Environments 에 권한 있는 계정 암호를 저장하십시오.

다음 단계를 수행하십시오.

1. 왼쪽 창에서 관리되는 장치를 선택한 다음 CA Security 탭을 선택합니다.

   CA Security 탭이 열리고 요약 탭의 내용이 표시됩니다.

2. PUPM 이 비활성화되어 있는 경우 "서비스" 필드에서 "구성"을 선택하여 계정 검색 마법사를 시작합니다.

   계정 검색 및 저장 마법사가 시작됩니다.

3. 대화 상자에서 다음 필드를 채웁니다.

   이름

   구성하는 관리되는 장치의 이름을 식별합니다.

   설명

   끝점에 대한 설명을 지정합니다.

   끝점 유형

   끝점 유형을 정의합니다.

   참고: 끝점 유형을 선택하면 추가 대화 상자가 열립니다. 이 대화 상자를 사용하여 해당 유형의 끝점에서 권한 있는 계정을 관리하는 데 필요한 자격 증명을 제공하십시오. 선택하는 끝점 유형은 제공해야 하는 연결 정보에 영향을 줍니다.

4. "유효성 검사"를 선택합니다.

   CA Access Control for Virtual Environments 가 끝점 연결 설정의 유효성 검사를 시도합니다.

5. "다음"을 클릭합니다.

6. 검색 특성을 선택하고 필터 값을 입력한 다음 "검색"을 클릭합니다.

   필터 조건에 일치하는 권한 있는 계정의 목록이 표시됩니다.

7. 관리할 권한 있는 계정을 선택하고 "다음"을 클릭합니다.

   잠금 속성 화면이 열립니다.

8. 대화 상자의 필드를 입력합니다. 다음 필드는 자동으로 채워지지 않습니다.

연결 해제된 시스템

계정이 연결 해제된 시스템에 있는지 여부를 지정합니다.

이 옵션을 선택하면 PUPM 이 해당 계정을 관리하지 않습니다. 대신, 연결 해제된 시스템의 권한 있는 계정을 위한 암호 저장소의 역할만 수행합니다. 암호를 변경할 때마다 관리되는 끝점에서도 계정 암호를 수동으로 변경해야 합니다.

암호 정책

권한 있는 계정 또는 서비스 계정에 적용할 암호 정책을 지정합니다.

체크 아웃 만료

체크 아웃 계정이 만료되는 기간(분)을 정의합니다.

배타적 계정

한 번에 하나의 사용자만 계정에 액세스할 수 있는지 여부를 지정합니다. *배타적 계정*은 한 번에 하나의 사용자만 권한 있는 계정을 사용하도록 제한합니다.

체크 아웃 시 암호 변경

권한 있는 계정이 체크 아웃될 때마다 PUPM 이 권한 있는 계정의 암호를 변경할지 여부를 지정합니다.

체크 인 시 암호 변경

사용자 또는 프로그램이 권한 있는 계정을 체크 인할 때마다 또는 체크 아웃 기간이 만료될 때 PUPM 이 권한 있는 계정의 암호를 변경할지 여부를 지정합니다.

참고: 배타적 계정이 아닌 경우 PUPM 은 *모든*사용자가 이 계정을 체크 인한 경우에만 새 권한 있는 계정 암호를 생성합니다.

9. "다음"을 클릭합니다.

   "요약" 화면이 열립니다.

10. 세부 정보를 검토한 다음 "마침"을 클릭합니다.

    CA Access Control for Virtual Environments 는 이 작업을 제출하고 오류가 없는 경우 선택된 권한 있는 계정을 만듭니다.

추가 정보:

Windows Agentless Connection 정보 (페이지 61)
SSH 장치 연결 정보 (페이지 62)
VMware ESX/ESXi 연결 정보 (페이지 64)

Windows Agentless Connection 정보

Windows Agentless 끝점 유형을 사용하면 권한 있는 Windows 계정을 관리할 수 있습니다.

참고: 로컬 컴퓨터에서 도메인 사용자를 구성하는 경우 CA Access Control for Virtual Environments 는 도메인 사용자의 암호를 변경할 수 없습니다. 이 제한 사항은 Windows 의 특성에 기인합니다.

이 유형의 끝점을 만들 때 다음 정보를 제공하십시오.

사용자 이름

끝점의 관리 사용자 이름을 정의합니다. CA Access Control 엔터프라이즈 관리는 이 계정을 사용하여 끝점에서 관리 작업(끝점에 연결하고, 계정을 검색하고, 암호를 변경하는 등의 작업)을 수행합니다.

암호

끝점의 관리 사용자 암호를 정의합니다.

호스트

끝점의 호스트 이름을 정의합니다.

예: myhost-ac-1

호스트 도메인

이 호스트가 구성원으로 포함된 도메인 이름을 지정합니다.

참고: 호스트 도메인 이름은 접두사만 사용하여 지정하십시오. 예를 들어, 전체 도메인 이름이 company.com 인 경우 접두사인 company 만 입력합니다.

Active Directory

사용자 계정이 Active Directory 계정인지 여부를 지정합니다.

사용자 도메인

사용자가 구성원으로 포함된 도메인 이름을 지정합니다.

참고: 사용자 도메인 이름은 접두사만 사용하여 지정하십시오. 예를 들어, 전체 도메인 이름이 company.com 인 경우 접두사인 company 만 입력합니다.

중요! PUPM 자동 로그인을 사용하여 끝점에 로그인하려는 경우 호스트 도메인 이름을 지정해야 합니다. 끝점이 워크그룹의 구성원인 경우 워크그룹 이름이 아닌 호스트 이름을 지정하십시오.

참고: Windows Agentless 끝점을 구성하는 데 필요한 추가 단계에 대한 자세한 내용은 *엔터프라이즈 관리 안내서*를 참조하십시오.

SSH 장치 연결 정보

SSH 장치 유형을 사용하면 권한 있는 UNIX 계정을 관리할 수 있습니다.

중요! PUPM SSH 끝점을 구성하기 전에 끝점 설정을 구성하기 전에 끝점에서 터널링된 일반 텍스트 암호를 비활성화하십시오.

이 유형의 장치를 만들 때는 CA Access Control 엔터프라이즈 관리가 장치에 연결할 수 있도록 다음 정보를 제공하십시오.

사용자 이름

끝점의 관리 사용자 이름을 정의합니다. CA Access Control 엔터프라이즈 관리는 이 계정을 사용하여 끝점에서 관리 작업(끝점에 연결하고, 계정을 검색하고, 암호를 변경하는 등의 작업)을 수행합니다. 작업 관리자 계정을 지정하는 경우 PUPM 은 이 계정을 사용하여 끝점에서 관리 작업을 수행합니다.

암호

끝점의 관리 사용자 암호를 정의합니다.

호스트

끝점의 호스트 이름을 정의합니다.

작업 관리자 사용자 로그인

(선택 사항) 끝점의 작업 관리자 사용자의 이름을 정의합니다. PUPM 은 이 계정을 사용하여 끝점에서 관리 작업(예: 권한 있는 계정의 암호 검색 및 변경)을 수행합니다. 작업 관리자 사용자를 지정하지 않으면 PUPM 은 사용자 로그인 계정을 사용하여 끝점에서 관리 작업을 수행합니다.

Check Point Firewall 을 사용하는 SSH 끝점에 대해 작업 관리자 사용자를 지정하는 경우 전문가 사용자를 지정하십시오. 하지만 PUPM 을 사용하여 끝점에서 전문가 계정의 암호를 변경할 수 없습니다. 즉, 전문가 계정은 PUPM 에서 연결이 해제된 계정입니다.

작업 관리자 암호

(선택 사항) 작업 관리자 사용자의 암호를 정의합니다.

구성 파일

SSH 장치 XML 구성 파일의 이름을 지정합니다. 필요에 따라 XML 파일을 사용자 지정할 수 있습니다.

참고: 이 필드에 대한 값을 지정하지 않으면 CA Access Control 엔터프라이즈 관리는 ssh_connector_conf.xml 파일을 사용합니다.

참고: SSH 장치 끝점을 구성하는 데 필요한 추가 단계에 대한 자세한 내용은 *엔터프라이즈 관리 안내서*를 참조하십시오.

VMware ESX/ESXi 연결 정보

VMware ESX/ESXi 끝점 유형을 사용하면 권한 있는 VMware ESX/ESXi 계정을 관리할 수 있습니다.

이 유형의 끝점을 만들 때는 CA Access Control for Virtual Environments 가 끝점에 연결할 수 있도록 다음 정보를 제공하십시오.

사용자 이름

끝점의 관리 사용자 이름을 정의합니다. CA Access Control 엔터프라이즈 관리는 이 계정을 사용하여 끝점에서 관리 작업(끝점에 연결하고, 계정을 검색하고, 암호를 변경하는 등의 작업)을 수행합니다.

참고: "고급" 옵션을 지정하면 PUPM 은 관리 작업을 수행하기 위해 "사용자 로그인" 계정을 사용하지 않습니다. 대신, PUPM 은 지정된 권한 있는 계정을 사용하여 끝점에서 관리 작업을 수행합니다.

암호

끝점의 관리 사용자 암호를 정의합니다.

호스트

끝점의 호스트 이름을 정의합니다.

고급

권한 있는 관리 계정을 사용하여 끝점에서 관리 작업(끝점에 연결하고, 계정을 검색하고, 암호를 변경하는 등의 작업)을 수행할지 여부를 지정합니다. 예를 들어, 여러 끝점에서 관리 작업을 수행할 수 있는 권한 있는 도메인 계정을 지정할 수 있습니다.

이 옵션을 지정하면 PUPM 은 관리 작업을 수행하기 위해 "사용자 로그인" 계정을 사용하지 않습니다.

VMware vSphere Client 에서 권한 있는 계정 암호 체크 아웃

계정이 속한 관리되는 장치에 로그인하기 위해 권한 있는 계정 암호를 체크 아웃합니다. 권한 있는 계정을 체크 아웃할 때 암호를 표시하고, 암호를 클립보드에 복사하고, 관리되는 장치에 로그인할 수 있습니다.

다음 단계를 수행하십시오.

1. VMware vSphere Client 창의 왼쪽 창에서 관리되는 장치를 선택한 다음 CA Security 탭을 선택합니다.

   CA Security 탭이 열리고 요약 탭의 내용이 표시됩니다.

2. "권한 있는 계정 관리" 탭으로 이동합니다.

   "권한 있는 계정 관리" 탭이 열리고 체크 아웃할 수 있는 계정이 표시됩니다.

3. 체크 아웃할 계정과 관리되는 장치를 선택한 다음 "작업" 메뉴에서 다음 옵션 중 *하나*를 선택합니다.

   - 암호를 체크 아웃하려면 "체크 아웃"을 선택합니다.
   - 관리되는 장치에 로그인하려면 "자동 로그인"을 선택합니다.
   - 암호를 표시하려면 "암호 표시"를 선택합니다.

   VMware vSphere Client 가 이 작업을 처리하고 선택한 옵션에 따라 진행합니다.

   관리되는 장치에 로그인하도록 선택한 경우 관리되는 장치에서 창이 열리고 사용자가 로그인됩니다.

   참고: 관리되는 장치에 처음 로그인하는 경우 관리되는 장치에 연결할 수 있기 전에 작업에 대한 승인을 요청받습니다.

   중요! Microsoft Windows 2008 Server 의 경우 Microsoft Internet Explorer 브라우저 보안 설정에서 "자동 ActiveX 컨트롤 확인"을 활성화하십시오. 비활성화된 경우 브라우저가 원격 데스크톱 응용 프로그램을 실행하기 위해 필요한 ActiveX 파일을 차단합니다.

VMware vSphere Client 에서 권한 있는 계정 암호 체크 인

관리되는 장치에서 로그아웃한 다음에 권한 있는 계정 암호를 체크 인합니다. 권한 있는 계정 암호를 체크인한 후에 CA Access Control for Virtual Environments 는 구성 옵션의 설정에 따라 암호를 변경할 수 있습니다.

다음 단계를 수행하십시오.

1. VMware vSphere Client 창의 왼쪽 창에서 관리되는 장치를 선택한 다음 CA Security 탭을 선택합니다.

   CA Security 탭이 열리고 요약 탭의 내용이 표시됩니다.

2. "권한 있는 계정 관리" 탭으로 이동합니다.

   "권한 있는 계정 관리" 탭이 열리고 체크 인할 수 있는 계정이 표시됩니다.

3. 체크 인할 계정 암호를 선택하고 메뉴에서 "체크 인"을 선택합니다.

   CA Access Control for Virtual Environments 가 계정을 체크인합니다.

Break Glass 프로세스가 작동하는 방법

사용자에게 관리 권한이 없는 계정에 즉시 액세스해야 하는 경우 Break Glass 체크 아웃을 수행합니다.

Break Glass 계정은 사용자 역할에 따라 사용자에게 할당되지 않은 권한 있는 계정입니다. 하지만 사용자는 계정 암호를 획득할 수 있습니다.

Break Glass 체크 아웃 프로세스 중에 Break Glass 체크 아웃 프로세스가 발생했음을 알리는 알림 메시지가 역할 관리자에게 전달됩니다. 하지만 이 관리자는 프로세스를 승인 또는 중지할 수 없습니다.

체크 아웃된 Break Glass 계정이 "홈" 탭의 "Break Glass" 옵션에 있는 "내 체크 아웃한 권한 있는 계정" 탭에 추가됩니다.

참고: Break Glass 권한 있는 액세스 역할이 있는 사용자만 Break Glass 프로세스를 수행할 수 있습니다.

CA Access Control 엔터프라이즈 관리에서 Break Glass

액세스 권한이 없는 끝점에 *즉시* 액세스해야 하는 경우 Break Glass 작업을 사용하십시오.

참고: 끝점에 대한 즉각적인 액세스가 필요 없으면 권한 있는 계정에 대한 액세스를 요청할 수 있습니다. 그런 다음 관리자가 이 요청을 승인할 때까지 기다립니다.

다음 단계를 수행하십시오.

1. CA Access Control 엔터프라이즈 관리에서 "홈", "내 계정", "내 권한 있는 계정"을 클릭합니다.

   "내 계정" 페이지가 열려 체크 아웃할 수 있는 계정을 표시합니다.

2. "계정 선택" 필드에서 "고급"을 선택합니다.

   고급 검색 옵션이 나타납니다.

3. Break Glass 계정을 포함하도록 선택하고 "검색"을 선택합니다.

   필터 조건에 일치하는 권한 있는 계정의 목록이 표시됩니다.

4. "작업" 메뉴에서 체크 아웃할 권한 있는 계정을 선택합니다.

5. 체크 아웃 사유를 입력하고 "체크 아웃"을 클릭합니다.

   CA Access Control 엔터프라이즈 관리는 작업을 제출하고 성공하는 경우 확인 메시지에 계정 암호를 표시합니다.

참고: 암호를 체크 아웃한 이후에 "작업" 메뉴에 다음 옵션이 또한 표시됩니다: 체크 인, 로그인 응용 프로그램, 암호 표시

VMware vSphere Client 에서 Break Glass

액세스 권한이 없는 끝점에 *즉시* 액세스해야 하는 경우 Break Glass 작업을 사용하십시오.

다음 단계를 수행하십시오.

1. "호스트 정보" 화면에서 "권한 있는 계정 관리"를 선택합니다.

   "권한 있는 계정 관리" 탭이 열리고 Break Glass 가 가능한 권한 있는 계정을 표시합니다.

2. 체크 아웃할 권한 있는 계정을 선택하고 "Break Glass"를 선택합니다.
3. 체크 아웃 사유를 입력하고 "체크 아웃"을 클릭합니다.

   CA Access Control for Virtual Environments 는 작업을 제출하고 성공하는 경우 확인 메시지에 계정 암호를 표시합니다.

참고: 암호를 체크 아웃한 이후에 "작업" 메뉴에 다음 옵션이 또한 표시됩니다: 체크 인, 로그인 응용 프로그램, 암호 표시

CA Access Control 엔터프라이즈 관리에서 Break Glass 권한 있는 계정 암호 체크 인

관리되는 끝점에서 로그아웃한 다음에 Break Glass 권한 있는 계정 암호를 체크 인합니다.

다음 단계를 수행하십시오.

1. "홈", "내 계정", "내 권한 있는 계정"을 클릭합니다.

   "내 계정" 페이지가 열려 체크 인할 수 있는 계정을 표시합니다.

2. "계정 선택" 필드에서 "고급"을 선택합니다.

   고급 검색 옵션이 나타납니다.

3. Break Glass 계정을 포함하도록 선택하고 "검색"을 선택합니다.

   필터 조건에 일치하는 권한 있는 계정의 목록이 표시됩니다.

4. 체크 인할 계정을 선택하고 "작업" 메뉴에서 "체크 인"을 클릭합니다.

   CA Access Control 엔터프라이즈 관리는 이 작업을 제출하여 계정을 체크 인합니다.