DMZ에 VMware Identity Manager 배포

VMware Identity Manager 2.9.1
VMware Identity Manager 2.8

vmware®

VMware 웹 사이트 (https://docs.vmware.com/kr/) 에서 최신 기술 문서를 확인할 수 있습니다.
또한 VMware 웹 사이트에서 최신 제품 업데이트를 제공합니다.
이 문서에 대한 의견이 있으면 docfeedback@vmware.com으로 사용자 의견을 보내주십시오.

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

목차

DMZ에서 VMware Identity Manager 배포

DMZ에 VMware Identity Manager 배포에서는 내부 네트워크 대신 DMZ에 VMware Identity Manager를 배포하는 방법에 대한 정보를 제공합니다. 내부 네트워크에 VMware Identity Manager를 배포하는 방법에 대한 자세한 내용은 VMware Identity Manager 설치 및 구성을 참조하십시오.

대상

이 정보는 VMware 기술(특히 vCenter™, ESX™ 및 vSphere®), 네트워킹 개념, Active Directory 및 데이터베이스를 잘 아는 숙련된 Windows 및 Linux 시스템 관리자를 위해 작성되었습니다. SUSE Linux 11은 VMware Identity Manager 및 VMware Identity Manager 커넥터 가상 장치를 위한 기본 운영 체제입니다.

이러한 기능을 구현하려는 경우에는 RSA 어댑티브 인증, RSA SecurID 및 RADIUS와 같은 기술을 아는 것도 도움이 됩니다.

VMware 기술 자료 용어집

VMware 기술 자료 사이트에서는 익숙하지 않을 수 있는 새로운 용어를 정리한 용어집을 제공하고 있습니다. VMware 기술 문서에 사용되는 용어의 정의를 보려면 http://www.vmware.com/kr/support/pubs로 이동하십시오.

1 배포 모델

VMware AirWatch® 배포에 통합되는 배포 모델 및 AirWatch를 요구하지 않고 VMware Identity Manager 커넥터를 사용하는 배포 모델의 두 가지 기본 배포 모델 유형을 사용하여 DMZ에 VMware Identity Manager를 배포할 수 있습니다.

모델 중 하나에서 지원되지 않는 기능이 필요한 경우 배포 모델을 결합할 수도 있습니다.

- AirWatch Cloud Connector를 사용한 배포 모델

  기존 AirWatch 배포가 있는 경우 VMware Identity Manager를 이와 빠르게 통합할 수 있습니다. 이 모델에서 엔터프라이즈 디렉토리에서의 사용자 및 그룹 동기화와 사용자 인증은 AirWatch에서 처리됩니다. DMZ에서 VMware Identity Manager를 배포합니다.

  Horizon 7 및 Citrix 게시된 리소스와 같은 리소스에 VMware Identity Manager를 통합하는 것은 이 모델에서 지원되지 않습니다. 웹 애플리케이션 및 기본 모바일 애플리케이션과의 통합만 지원됩니다.

  "AirWatch Cloud Connector를 사용한 온-프레미스 배포 모델," (8 페이지)의 내용을 참조하십시오.

- 아웃바운드 전용 연결 모드에서 VMware Identity Manager Connector를 사용한 배포 모델

  AirWatch 배포를 요구하지 않는 시나리오에서는 DMZ에 VMware Identity Manager 서버 가상 장치를 설치하고 엔터프라이즈 네트워크에 VMware Identity Manager 커넥터 가상 장치를 설치할 수 있습니다. 커넥터는 Active Directory와 같은 온-프레미스 서비스에 서버를 연결합니다. 커넥터는 아웃바운드 전용 연결 모드에서 설치되며 인바운드 방화벽 포트 443을 열 필요가 없습니다. 이 모델에서 엔터프라이즈 디렉토리에서의 사용자 및 그룹 동기화와 사용자 인증은 VMware Identity Manager 커넥터에서 처리됩니다.

  "아웃바운드 전용 연결 모드에서 VMware Identity Manager Connector를 사용한 온-프레미스 배포 모델," (10 페이지)의 내용을 참조하십시오.

  - VMware Identity Manager Connector 배포에 Kerberos 인증 지원 추가

    내부 사용자(인바운드 연결 모드 필요)용 Kerberos 인증을 아웃바운드 전용 연결 모드 커넥터를 기반으로 하는 배포에 추가할 수 있습니다.

    "배포에 Kerberos 인증 지원 추가," (12 페이지)의 내용을 참조하십시오.

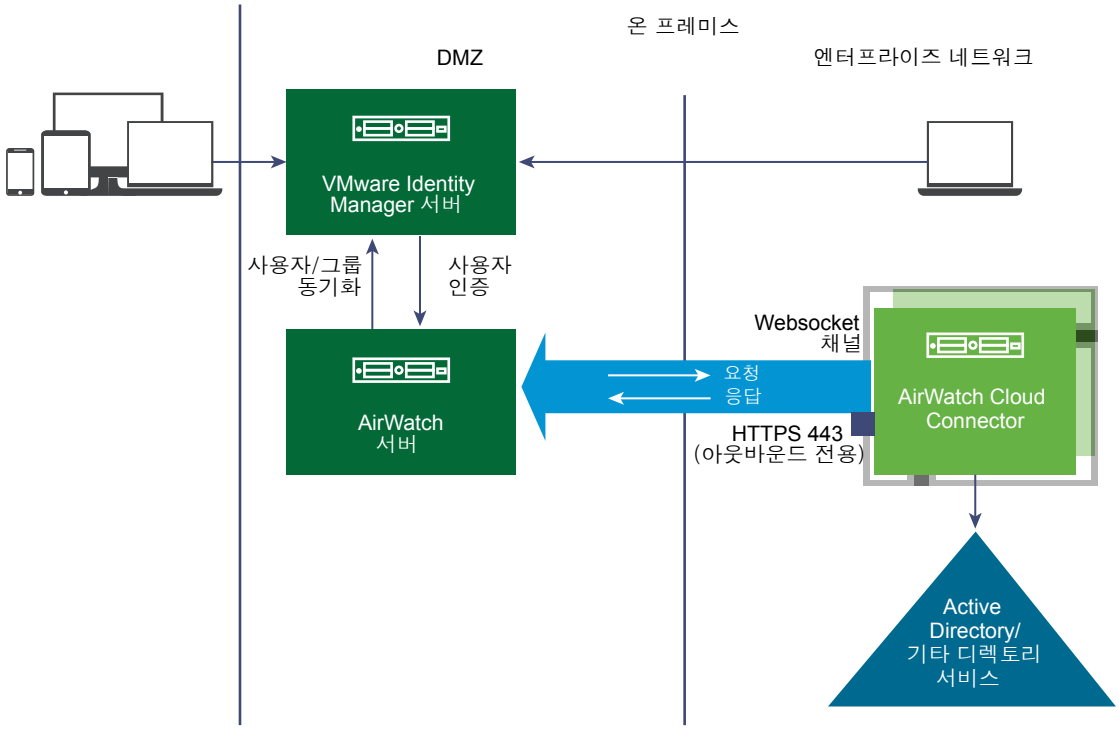
이 장에서는 다음 주제에 대해 설명합니다.

AirWatch Cloud Connector를 사용한 온-프레미스 배포 모델

기존 AirWatch 배포가 있는 경우 VMware Identity Manager를 이와 통합할 수 있습니다. DMZ에 VMware Identity Manager 가상 장치를 배포합니다. 이 모델에서 엔터프라이즈 디렉토리에서의 사용자 및 그룹 동기화와 사용자 인증은 AirWatch에서 처리됩니다.

Horizon 7 또는 Citrix 게시된 리소스와 같은 리소스에 VMware Identity Manager를 통합하는 것은 이 모델에서 지원되지 않습니다. 웹 애플리케이션 및 기본 모바일 애플리케이션과의 통합만 지원됩니다.

그림 1-1. AirWatch Cloud Connector를 사용한 배포



사전 요구 사항

다음 구성 요소가 있어야 합니다.

- AirWatch 서버 배포
- AirWatch Cloud Connector 인스턴스가 온-프레미스에 배포되고 엔터프라이즈 디렉토리와 통합되어야 합니다.

포트 요구 사항

VMware Identity Manager 서버에 다음 포트가 필요합니다.

- 인바운드 443(HTTPS)
- 인바운드 88(TCP/UDP) - iOS만 해당
- 인바운드 5262(TCP/UDP) - Android만 해당

AirWatch 배포 요구 사항에 대해서는 AirWatch 설명서를 참조하십시오.

지원되는 인증 방법

이 배포 모델은 다음 인증 방법을 지원합니다. 이러한 방법은 VMware Identity Manager 기본 제공 ID 제공자를 통해 사용할 수 있습니다.

- 암호(AirWatch Connector)
- 모바일 SSO(iOS용)
- 모바일 SSO(Android용)
- 디바이스 규정 준수(AirWatch 사용)
- 인증서(클라우드 배포)
- VMware Verify

지원되는 디렉토리 통합

엔터프라이즈 디렉토리를 AirWatch에 통합합니다. 지원되는 디렉토리 유형에 대해서는 AirWatch 설명서를 참조하십시오.

지원되는 리소스

이 배포 모델에서는 다음 유형의 리소스를 VMware Identity Manager에 통합할 수 있습니다.

- 웹 애플리케이션
- 기본 모바일 애플리케이션

이 배포 모델에서는 다음 리소스를 VMware Identity Manager에 통합할 수 없습니다.

- Horizon 7, Horizon 6 또는 View 데스크톱 및 애플리케이션 풀
- Citrix 게시된 리소스
- ThinApp 패키징된 애플리케이션
- Horizon Air – 클라우드 호스팅된 애플리케이션 및 데스크톱

추가 정보

- 2장, “DMZ에 VMware Identity Manager 배포,”(13 페이지)
- VMware Identity Manager 관리 가이드의 AirWatch와 VMware Identity Manager 통합
- AirWatch 설명서

아웃바운드 전용 연결 모드에서 VMware Identity Manager Connector를 사용한 온-프레미스 배포 모델

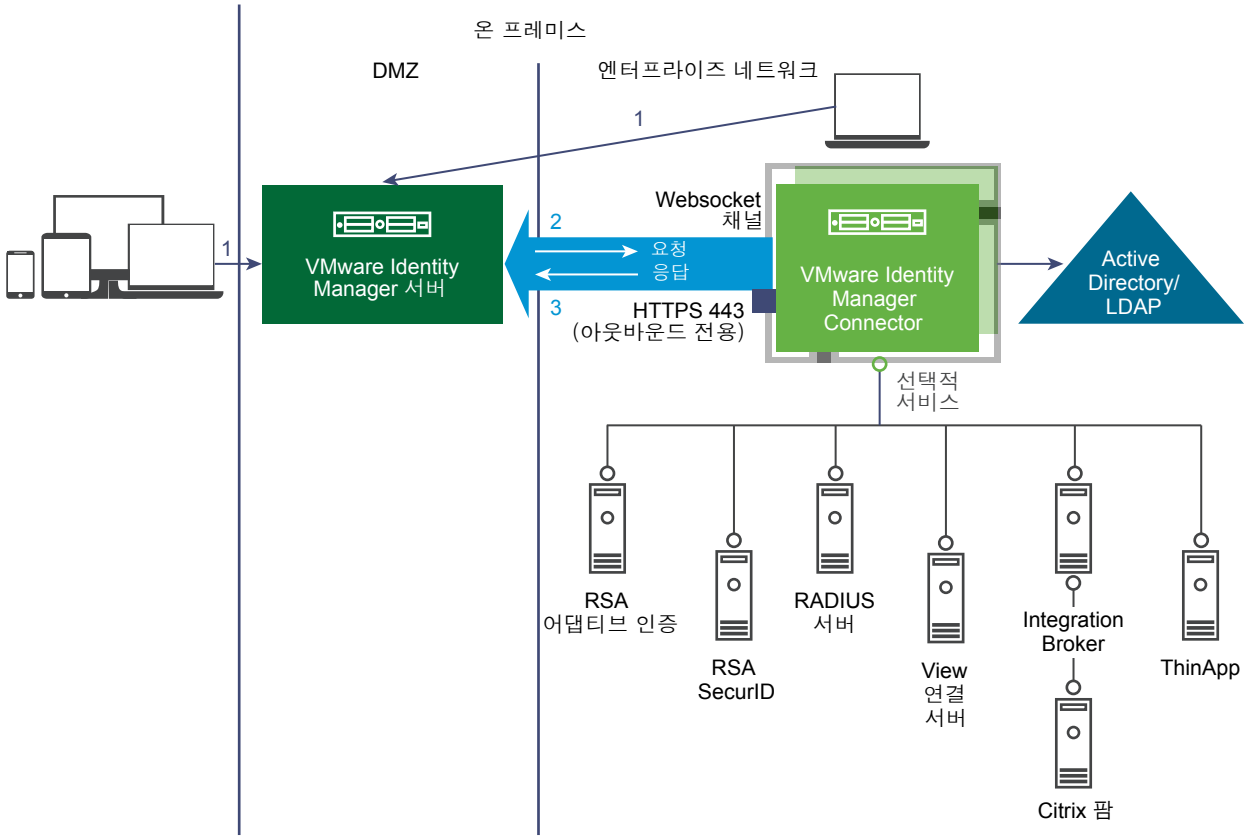
이 모델에서는 DMZ에 VMware Identity Manager 가상 장치를 설치합니다. 엔터프라이즈 네트워크에도 아웃바운드 전용 연결 모드로 독립 실행형 VMware Identity Manager 커넥터 가상 장치를 설치합니다. 이 모델에는 AirWatch 구성 요소가 포함되지 않습니다.

엔터프라이즈 디렉토리에서의 사용자 및 그룹 동기화와 사용자 인증은 독립 실행형 VMware Identity Manager 커넥터에서 처리됩니다. 커넥터는 Horizon 7 데스크톱 및 애플리케이션과 같은 리소스를 VMware Identity Manager 서비스에 동기화할 수도 있습니다.

참고 일부 인증 방법은 커넥터를 사용하지 않으며 서비스를 통해 직접 관리됩니다.

중요 VMware Identity Manager 장치와 통합된 커넥터 대신 독립 실행형 커넥터를 사용하여 사용자 및 그룹을 동기화하고 사용자 인증을 처리합니다.

그림 1-2. 아웃바운드 모드에서 VMware Identity Manager Connector 사용



포트 요구 사항

VMware Identity Manager 서버에 다음 포트가 필요합니다.

- 인바운드 443(HTTPS)
- 인바운드 88(TCP/UDP) - iOS만 해당
- 인바운드 5262(TCP/UDP) - Android만 해당

VMware Identity Manager 커넥터는 아웃바운드 전용 연결 모드에서 설치되므로 인바운드 포트 443을 열 필요가 없습니다. 커넥터는 Websocket 기반 통신 채널을 통해 VMware Identity Manager 서비스와 통신합니다.

사용되는 전체 포트 목록은 2장, "DMZ에 VMware Identity Manager 배포," (13 페이지) 및 3장, "엔터프라이즈 네트워크에 VMware Identity Manager Connector 배포," (15 페이지)를 참조하십시오.

지원되는 인증 방법

이 배포 모델은 모든 인증 방법을 지원합니다. 이러한 인증 방법 중 일부는 커넥터가 필요하지 않으며 기본 제공 ID 제공자를 통해 서비스에서 직접 관리됩니다.

- 암호 – 커넥터 사용
- RSA 어댑티브 인증 – 커넥터 사용
- RSA SecurID – 커넥터 사용
- RADIUS – 커넥터 사용
- 인증서(클라우드 배포) – 기본 제공 ID 제공자를 통해
- VMware Verify – 기본 제공 ID 제공자를 통해
- 모바일 SSO(iOS) – 기본 제공 ID 제공자를 통해
- 모바일 SSO(Android) – 기본 제공 ID 제공자를 통해
- 타사 ID 제공자를 통한 인바운드 SAML

참고 Kerberos 사용에 대한 자세한 내용은 "배포에 Kerberos 인증 지원 추가," (12 페이지)의 내용을 참조하십시오.

참고 이 배포 모델은 커넥터를 통한 인증서 인증을 지원하지 않습니다. 인증서(클라우드 배포) 인증 방법을 사용할 수 있습니다.

지원되는 디렉토리 통합

이 배포 모델에서는 다음 유형의 엔터프라이즈 디렉토리를 VMware Identity Manager 서비스에 통합할 수 있습니다.

- LDAP를 통한 Active Directory
- Active Directory, Windows 통합 인증
- LDAP 디렉토리

  LDAP 디렉토리를 통합하려는 경우 VMware Identity Manager 설치 및 구성의 "LDAP 디렉토리와 통합"에서 제한 사항을 참조하십시오.

또는 다음 방법을 사용하여 VMware Identity Manager 서비스에서 사용자를 생성할 수 있습니다.

- VMware Identity Manager 서비스에서 직접 로컬 사용자를 생성합니다.
- Just-in-Time 프로비저닝을 사용하여 타사 ID 제공자가 보낸 SAML 어설션을 통해 로그인 시 VMware Identity Manager 서비스에서 동적으로 사용자를 생성합니다.

지원되는 리소스

이 배포 모델에서는 다음 유형의 리소스를 VMware Identity Manager 서비스에 통합할 수 있습니다.

- 웹 애플리케이션
- Horizon 7, Horizon 6 또는 View 데스크톱 및 애플리케이션 풀

- Citrix 게시된 리소스
- ThinApp 패키징된 애플리케이션
- Horizon Air – 클라우드 호스팅된 애플리케이션 및 데스크톱(기술 미리보기)

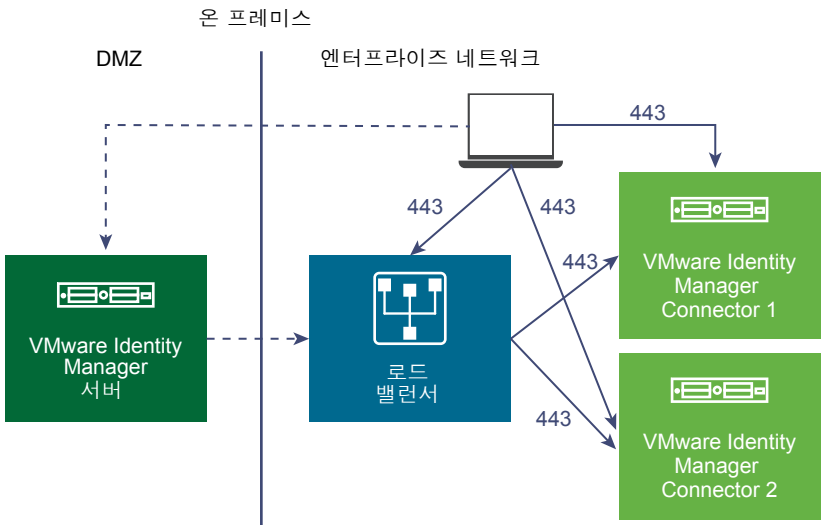
추가 정보

- 2장, "DMZ에 VMware Identity Manager 배포," (13 페이지) 및 3장, "엔터프라이즈 네트워크에 VMware Identity Manager Connector 배포," (15 페이지)
- 디렉토리
  - VMware Identity Manager 설치 및 구성의 "엔터프라이즈 디렉토리와 통합"
  - VMware Identity Manager 설치 및 구성의 "로컬 디렉토리 사용"
  - VMware Identity Manager 관리의 "Just-in Time 사용자 프로비저닝"
- VMware Identity Manager 관리의 "VMware Identity Manager에서 사용자 인증 구성"
- VMware Identity Manager에서 리소스 설정

배포에 Kerberos 인증 지원 추가

인바운드 연결 모드가 필요한 내부 사용자용 Kerberos 인증을 VMware Identity Manager 아웃바운드 전용 연결 모드 커넥터를 기반으로 하는 배포에 추가할 수 있습니다. 내부 네트워크에서 오는 사용자를 위해 Kerberos 인증을 사용하고 외부에서 들어오는 사용자를 위해 다른 인증 방법을 사용하도록 동일한 커넥터를 구성할 수 있습니다. 이 작업은 네트워크 범위를 기준으로 인증 정책을 정의하여 수행할 수 있습니다.

그림 1-3. Kerberos 인증 추가



Kerberos 인증의 고가용성을 구성하는 프로세스는 서로 다릅니다.

자세한 정보는 "VMware Identity Manager Connector 배포에 Kerberos 인증 지원 추가," (25 페이지)의 내용을 참조하십시오.

DMZ에 VMware Identity Manager 배포

2

VMware Identity Manager 가상 장치를 엔터프라이즈 네트워크에 배포하지 않으려는 경우 DMZ에 배포할 수 있습니다. DMZ에 VMware Identity Manager 장치를 배포할 때 엔터프라이즈 네트워크에도 아웃바운드 전용 연결 모드로 독립 실행형 VMware Identity Manager 커넥터를 배포합니다.

시스템 및 네트워크 구성 요구 사항

DMZ에 VMware Identity Manager를 배포하기 위한 시스템 및 네트워크 구성 요구 사항은 여기에 나열된 차이점을 제외하고, VMware Identity Manager 설치 및 구성의 시스템 및 네트워크 구성 요구 사항 및 VMware Identity Manager 배포 준비에 설명된 대로 엔터프라이즈 네트워크에 VMware Identity Manager를 배포하기 위한 요구 사항과 비슷합니다.

- 엔터프라이즈 네트워크의 장치에 대해 인바운드 방화벽 포트를 열 필요가 없습니다.

  VMware Identity Manager 가상 장치가 DMZ에 배포되어 있습니다. VMware Identity Manager 커넥터는 아웃바운드 전용 연결 모드로 엔터프라이즈 네트워크에 배포되어 있고, Websocket 기반 통신 채널을 통해 서비스와 통신합니다.

- VMware Identity Manager에 대한 외부 액세스를 허용하기 위해 역방향 프록시 또는 로드 밸런서를 배포할 필요가 없습니다.
- 로드 밸런서는 VMware Identity Manager 가상 장치에 대해 고가용성 및 이중화를 구성하는 경우에만 필요합니다.
- 다음 포트가 사용됩니다. 배포에는 일부만 필요할 수 있습니다.

포트	소스	대상	설명
443	로드 밸런서	VMware Identity Manager 가상 장치	HTTPS
443	VMware Identity Manager 가상 장치	VMware Identity Manager 가상 장치	HTTPS
443	브라우저	VMware Identity Manager 가상 장치	HTTPS
88	브라우저	VMware Identity Manager 가상 장치	TCP/UDP iOS만 해당
5262	브라우저	VMware Identity Manager 가상 장치	TCP/UDP Android만 해당
443	VMware Identity Manager 가상 장치	vapp-updates.vmware.com	VMware 업그레이드 서버에 대한 액세스
8443	브라우저	VMware Identity Manager 가상 장치	관리자 포트 HTTPS

포트	소스	대상	설명
25	VMware Identity Manager 가상 장치	SMTP 서버	아웃바운드 메일을 릴레이할 TCP 포트
53	VMware Identity Manager 가상 장치	DNS 서버	TCP/UDP 모든 가상 장치는 포트 53에서 DNS 서버에 액세스할 수 있어야 하며 포트 22에서 수신 SSH 트래픽을 허용해야 합니다.
TCP: 9300-9400 UDP: 54328	VMware Identity Manager 가상 장치	VMware Identity Manager 가상 장치	감사 요구
5432	VMware Identity Manager 가상 장치	데이터베이스	PostgreSQL 기본 포트는 5432입니다. Oracle 기본 포트는 1521입니다.
443	VMware Identity Manager 가상 장치	AirWatch REST API	HTTPS 디바이스 규정 준수 검사 및 ACC 암호 인증 방법(사용되는 경우)

VMware Identity Manager 장치 배포

VMware Identity Manager 가상 장치 배포 및 구성에 대한 자세한 내용은 VMware Identity Manager 설치 및 구성에서 VMware Identity Manager 배포 및 장치 시스템 구성 설정 관리를 참조하십시오.

페일오버 및 이중화 구성

VMware Identity Manager 가상 장치에 대한 페일오버 및 이중화를 구성하는 방법에 대한 자세한 내용은 VMware Identity Manager 설치 및 구성의 다음 섹션을 참조하십시오.

- 단일 데이터 센터에서 페일오버 및 이중화 구성
- 페일오버 및 이중화를 위해 보조 데이터 센터에 VMware Identity Manager 배포

참고 "로드 밸런서 또는 역방향 프록시를 사용하여 VMware Identity Manager에 대한 외부 액세스 사용" 섹션은 VMware Identity Manager를 DMZ에 배포하는 시나리오에는 적용되지 않습니다.

엔터프라이즈 네트워크에 VMware Identity Manager Connector 배포

3

DMZ에 VMware Identity Manager 가상 장치를 배포할 때 엔터프라이즈 네트워크에도 아웃바운드 전용 연결 모드로 독립 실행형 VMware Identity Manager 커넥터 장치를 배포해야 합니다.

커넥터는 VMware Identity Manager 서비스를 Active Directory 및 Horizon 7과 같은 엔터프라이즈 네트워크 내의 다른 구성 요소에 연결합니다.

커넥터는 통신 채널을 통해 아웃바운드 전용 연결 모드로 서비스와 통신합니다.

참고 AirWatch 배포가 있고 AirWatch Cloud Connector를 사용하는 경우 VMware Identity Manager 커넥터에서 지원되는 사용 사례가 필요한 경우가 아니면 VMware Identity Manager 커넥터가 필요하지 않습니다. "AirWatch Cloud Connector를 사용한 온-프레미스 배포 모델," (8 페이지)의 내용을 참조하십시오.

시스템 및 네트워크 구성 요구 사항

"시스템 및 네트워크 구성 요구 사항," (16 페이지)의 내용을 참조하십시오.

VMware Identity Manager Connector 배포 및 구성

아웃바운드 전용 연결 모드로 VMware Identity Manager 커넥터를 배포 및 구성하는 방법에 대한 자세한 내용은 다음 항목을 참조하십시오.

- "VMware Identity Manager 커넥터 배포," (16 페이지)
- "VMware Identity Manager 커넥터에 대해 고가용성 구성," (23 페이지)
- "VMware Identity Manager Connector 배포에 Kerberos 인증 지원 추가," (25 페이지)

페일오버 및 이중화

페일오버 및 이중화를 위해 커넥터를 구성하는 방법에 대한 자세한 내용은 다음 항목을 참조하십시오.

- "VMware Identity Manager 커넥터에 대해 고가용성 구성," (23 페이지)
- "VMware Identity Manager Connector 배포에 Kerberos 인증 지원 추가," (25 페이지)

이 장에서는 다음 주제에 대해 설명합니다.

- "VMware Identity Manager 커넥터 배포," (16 페이지)
- "VMware Identity Manager 커넥터에 대해 고가용성 구성," (23 페이지)
- "VMware Identity Manager Connector 배포에 Kerberos 인증 지원 추가," (25 페이지)

VMware Identity Manager 커넥터 배포

VMware Identity Manager 커넥터를 배포하려면 vCenter Server에 커넥터 가상 장치를 설치하고 전원을 켠 후 VMware Identity Manager 관리 콘솔에서 생성한 활성화 코드를 사용하여 활성화합니다. 또한 암호 설정과 같은 장치 설정을 구성합니다.

connector를 설치 및 구성한 후에 VMware Identity Manager 관리 콘솔로 이동하여 엔터프라이즈 디렉토리에 대한 연결을 설정하고, 커넥터에서 인증 어댑터를 사용하도록 설정하고, 커넥터에 대해 아웃바운드 모드를 사용하도록 설정합니다.

시스템 및 네트워크 구성 요구 사항

통합하려는 리소스를 포함하여 하드웨어, 리소스 및 네트워크 요구 사항에 관한 결정을 내릴 때 배포 전체에 대해 고려합니다.

지원되는 vSphere 및 ESX 버전

vCenter Server에 가상 장치를 설치합니다. 다음과 같은 vSphere 및 ESX 서버가 지원됩니다.

- 5.0 U2 이상
- 5.1 이상
- 5.5 이상
- 6.0 이상

OVA 파일을 배포하고 배포된 가상 장치에 원격으로 액세스하려면 VMware vSphere® Client™ 또는 VMware vSphere® Web Client가 필요합니다. vSphere Client는 my.vmware.com의 vSphere 제품 다운로드 페이지에서 사용할 수 있습니다.

VMware Identity Manager Connector 가상 장치 요구 사항

서버 및 각 서버에 할당된 리소스 개수 요구 사항을 충족해야 합니다.

사용자 수	최대 1000명	1,000~10,000명	10,000~25,000명	25,000~50,000명	50,000~100,000명
커넥터 서버 수	서버 1대	로드 밸런싱 서버 2대	로드 밸런싱 서버 2대	로드 밸런싱 서버 2대	로드 밸런싱 서버 2대
CPU(서버당)	2 CPU	4 CPU	4 CPU	4 CPU	4 CPU
RAM(서버당)	6GB	6GB	8GB	16GB	16GB
디스크 공간(서버당)	60GB	60GB	60GB	60GB	60GB

네트워크 구성 요구 사항

구성 요소	최소 요구 사항
DNS 레코드 및 정적 IP 주소	커넥터에 대한 요구 사항은 VMware Identity Manager 가상 장치에 대한 요구 사항과 같습니다. VMware Identity Manager 설치 및 구성에서 DNS 레코드 및 IP 주소 만들기를 참조하십시오.
방화벽 포트	커넥터 인스턴스에서 VMware Identity Manager URL로 아웃바운드 방화벽 포트 443이 열려 있는지 확인합니다.

포트 요구 사항

아래에서는 connector 서버 구성에 사용되는 포트에 대해 설명합니다. 배포에는 일부만 포함할 수 있습니다.

포트	소스	대상	설명
443	커넥터 가상 장치	VMware Identity Manager 서비스	HTTPS
443	커넥터 가상 장치	vapp-updates.vmware.com	업그레이드 서버에 대한 액세스
8443	브라우저	커넥터 가상 장치	관리자 포트 HTTPS
389, 636, 3268, 3269	커넥터 가상 장치	Active Directory	기본값은 다음과 같습니다. 이러한 포트는 구성할 수 있습니다.
445	Connector-va	VMware ThinApp 저장소	ThinApp 저장소에 대한 액세스
5500	커넥터 가상 장치	RSA SecurID 시스템	기본값은 다음과 같습니다. 이 포트는 구성할 수 있습니다.
53	커넥터 가상 장치	DNS 서버	TCP/UDP 모든 가상 장치는 포트 53에서 DNS 서버에 액세스할 수 있어야 하며 포트 22에서 수신 SSH 트래픽을 허용해야 합니다.
88, 464, 135	커넥터 가상 장치	도메인 컨트롤러	TCP/UDP
389, 443	커넥터 가상 장치	View 연결 서버	Horizon/View 통합을 위해 View 연결 서버 인스턴스에 액세스

디렉토리 요구 사항

VMware Identity Manager를 엔터프라이즈 디렉토리와 통합하고 엔터프라이즈 디렉토리에서 서비스로 사용자 및 그룹을 동기화할 수 있습니다. 다음 유형의 디렉토리를 통합할 수 있습니다.

- 단일 Active Directory 도메인, 단일 Active Directory 포리스트의 다중 도메인 또는 여러 Active Directory 포리스트의 다중 도메인으로 구성된 Active Directory 환경.

  VMware Identity Manager에서는 Windows 2003 이상의 도메인 기능 수준 및 포리스트 기능 수준을 사용하여 Windows 2008, 2008 R2, 2012 및 2012 R2에서 Active Directory를 지원합니다.

- LDAP 디렉토리

디렉토리는 connector 가상 장치에서 액세스할 수 있어야 합니다.

참고 VMware Identity Manager 서비스에서 로컬 디렉토리를 생성할 수도 있습니다.

배포 체크리스트

커넥터에 대한 요구 사항은 VMware Identity Manager 가상 장치에 대한 요구 사항과 비슷합니다. VMware Identity Manager 설치 및 구성에서 배포 체크리스트를 참조하십시오.

커넥터에 대한 활성화 코드 생성

VMware Identity Manager 커넥터를 설치하기 전에 VMware Identity Manager 관리 콘솔에 로그인하고 커넥터에 대한 활성화 코드를 생성합니다. 이 활성화 코드는 서비스와 커넥터 간의 통신을 설정하는 데 사용됩니다.

프로시저

1 관리 콘솔에 로그인합니다.

2 **ID 및 액세스 관리** 탭을 클릭합니다.

3 **설정**을 클릭합니다.

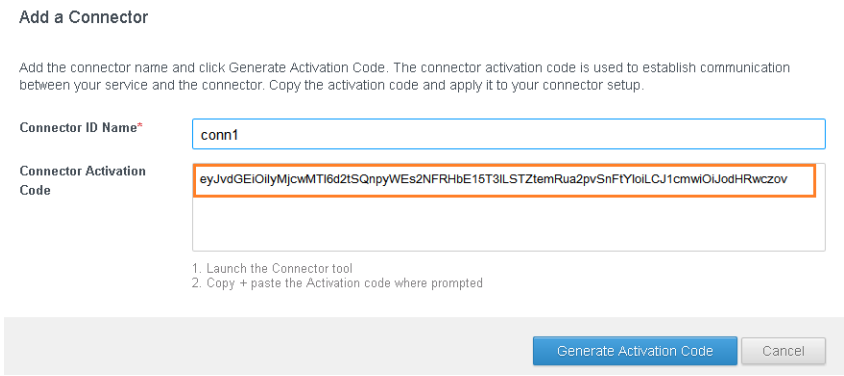
4 [커넥터] 페이지에서 **커넥터 추가**를 클릭합니다.

5 connector의 이름을 입력합니다.

6 **활성화 코드 생성**을 클릭합니다.

활성화 코드가 페이지에 표시됩니다.

7 활성화 코드를 복사하여 저장합니다.



나중에 커넥터를 배포할 때 활성화 코드가 필요합니다.

이제 커넥터 가상 장치를 설치할 수 있습니다.

커넥터 가상 장치 설치 및 구성

커넥터를 배포하려면 vSphere Client 또는 vSphere Web Client를 사용하여 vCenter Server에 커넥터 가상 장치를 설치하고 전원을 켠 후 VMware Identity Manager 관리 콘솔에서 생성한 활성화 코드를 사용하여 활성화합니다.

필수 조건

- my.vmware.com의 VMware Identity Manager 제품 페이지에서 커넥터 OVA 파일을 다운로드합니다.
- vSphere Client 또는 vSphere Web Client가 있는지 확인합니다.
- vSphere Web Client를 사용하는 경우 Firefox 또는 Chrome 브라우저를 사용합니다. OVA 파일을 배포할 때는 Internet Explorer를 사용하면 안 됩니다.
- 장치에 사용할 DNS 레코드 및 호스트 이름을 확인합니다.

프로시저

1 vSphere Client 또는 vSphere Web Client에서 **파일 > OVF 템플릿 배포**를 선택합니다.

2 마법사에 따라 템플릿을 배포합니다.

페이지	설명
소스	OVA 패키지 위치를 찾아보거나 특정 URL을 입력합니다.
OVA 템플릿 세부 정보	올바른 버전을 선택했는지 확인합니다.
라이센스	최종 사용자 라이센스 계약을 읽고 **동의**를 클릭합니다.
이름 및 위치	가상 장치의 이름을 입력합니다. 이 이름은 인벤토리 폴더 내에서 고유해야 하고 최대 80까지 가능합니다. 이름은 대/소문자를 구분합니다. 가상 장치의 위치를 선택합니다.
호스트/클러스터	배포된 템플릿을 실행할 호스트 또는 클러스터를 선택합니다.
리소스 풀	리소스 풀을 선택합니다.
스토리지	가상 시스템 파일을 저장할 위치를 선택합니다.
디스크 형식	파일의 디스크 형식을 선택합니다. 운영 환경의 경우 **씩 프로비저닝** 형식을 선택합니다. 평가 및 테스트의 경우 **씬 프로비저닝** 형식을 사용합니다.
네트워크 매핑	사용 환경의 네트워크를 OVF 템플릿의 네트워크에 매핑합니다.
속성	a **시간대 설정** 필드에서 올바른 시간대를 선택합니다. b [고객 환경 향상 프로그램] 확인란은 기본적으로 선택되어 있습니다. VMware는 사용자 요구 사항에 대한 응답을 개선하기 위해 배포에 관한 익명 데이터를 수집합니다. 데이터가 수집되는 것을 원하지 않으면 이 확인란을 선택 취소합니다. c [호스트 이름] 텍스트 상자에 사용할 호스트 이름을 입력합니다. 이 상자를 비워 두면 역방향 DNS가 호스트 이름 조회에 사용됩니다. d connector에 대한 정적 IP 주소를 구성하려면 기본 게이트웨이, DNS, IP 주소 및 넷마스크 각각에 대해 주소를 입력합니다. **중요** 호스트 이름을 포함하여 네 주소 필드 중 하나라도 비워 두면 DHCP가 사용됩니다. DHCP를 구성하려면 주소 필드를 비워 둡니다.
완료 준비	선택 사항을 검토하고 **완료**를 클릭합니다.

네트워크 속도에 따라 배포하는 데 몇 분 정도 걸릴 수 있습니다. 진행률 대화상자에서 진행 상태를 확인할 수 있습니다.

3 배포가 완료되면 connector 장치를 선택하고 마우스 오른쪽 버튼으로 클릭한 후 **전원 > 전원 켜기**를 선택합니다.

connector 장치가 초기화됩니다. **콘솔** 탭으로 이동하여 세부 정보를 볼 수 있습니다. 가상 장치 초기화가 완료되면 콘솔 화면에 connector 설정 마법사에 로그인하기 위한 connector 버전 및 URL이 표시됩니다.

4 설정 마법사를 실행하려면 브라우저에 [콘솔] 탭에 표시되는 connector URL을 지정합니다.

5 [시작] 페이지에서 **계속**을 클릭합니다.

6 다음 connector 가상 장치 관리자 계정에 대해 강력한 암호를 만듭니다.

강력한 암호는 8자 이상이고 대문자와 소문자를 포함하며 1개 이상의 숫자나 특수 문자를 포함해야 합니다.

옵션	설명
장치 관리자	장치 관리자 암호를 만듭니다. 사용자 이름은 **admin**이며 변경할 수 없습니다. 이 계정 및 암호를 사용하여 connector 서비스에 로그인한 후 인증서, 장치 암호 및 syslog 구성을 관리합니다. **중요** **관리자** 암호는 6자 이상이어야 합니다.
루트 계정	기본 VMware 루트 암호는 connector 장치를 설치하는 데 사용되었습니다. 새 루트 암호를 만듭니다.
sshuser 계정	커넥터 장치에 대한 원격 액세스에 사용할 암호를 만듭니다.

7 **계속**을 클릭합니다.

8 [커넥터 활성화] 페이지에서 활성화 코드를 붙여넣은 후 **계속**을 클릭합니다.

활성화 코드가 확인되고 VMware Identity Manager 서비스와 connector 인스턴스 간 통신이 설정됩니다.

connector 설정이 완료되었습니다.

후속 작업

[설치 완료] 페이지의 링크를 클릭하여 관리 콘솔로 이동합니다. 그런 다음 디렉토리 연결을 설정합니다.

디렉토리 설정

커넥터 가장 장치를 배포한 후에 VMware Identity Manager 관리 콘솔에서 디렉토리를 설정합니다. 엔터프라이즈 디렉토리의 사용자 및 그룹을 VMware Identity Manager 서비스와 동기화할 수 있습니다.

VMware Identity Manager에서는 다음 유형의 디렉토리 통합을 지원합니다.

- LDAP를 통한 Active Directory
- Active Directory, Windows 통합 인증
- LDAP 디렉토리

자세한 내용은 엔터프라이즈 디렉토리와 통합을 참조하십시오.

참고 VMware Identity Manager 서비스에서 로컬 디렉토리를 생성할 수도 있습니다. 로컬 디렉토리 사용을 참조하십시오.

프로시저

1 커넥터를 활성화한 후에 표시되는 [설치 완료] 페이지에 있는 링크를 클릭합니다.

ID 및 액세스 관리 > 디렉토리 탭이 표시됩니다.

2 **디렉토리 추가**를 클릭하고 추가하려는 디렉토리 유형을 선택합니다.

3 마법사에 따라 디렉토리 구성 정보를 입력하고, 동기화할 그룹 및 사용자를 선택한 후 사용자를 VMware Identity Manager 서비스와 동기화합니다.

디렉토리 설정 방법에 대한 자세한 내용은 엔터프라이즈 디렉토리와 통합을 참조하십시오.

후속 작업

사용자 및 그룹 탭을 클릭하고 사용자가 동기화되었는지 확인합니다.

커넥터에서 인증 어댑터 사용

PasswordIdpAdapter, RSAAIdpAdapter, SecurIDAdapter 및 RadiusAuthAdapter를 포함하는 몇 가지 인증 어댑터를 아웃바운드 모드에서 커넥터에 사용할 수 있습니다. 사용하려는 어댑터를 구성하고 사용하도록 설정합니다.

프로시저

1 VMware Identity Manager 관리 콘솔에서 **ID 및 액세스 관리** 탭을 클릭합니다.

2 **설정**을 클릭한 다음 **커넥터** 탭을 클릭합니다.

배포한 커넥터가 나열됩니다.

3 **작업자** 열에서 링크를 클릭합니다.

4 **인증 어댑터** 탭을 클릭합니다.

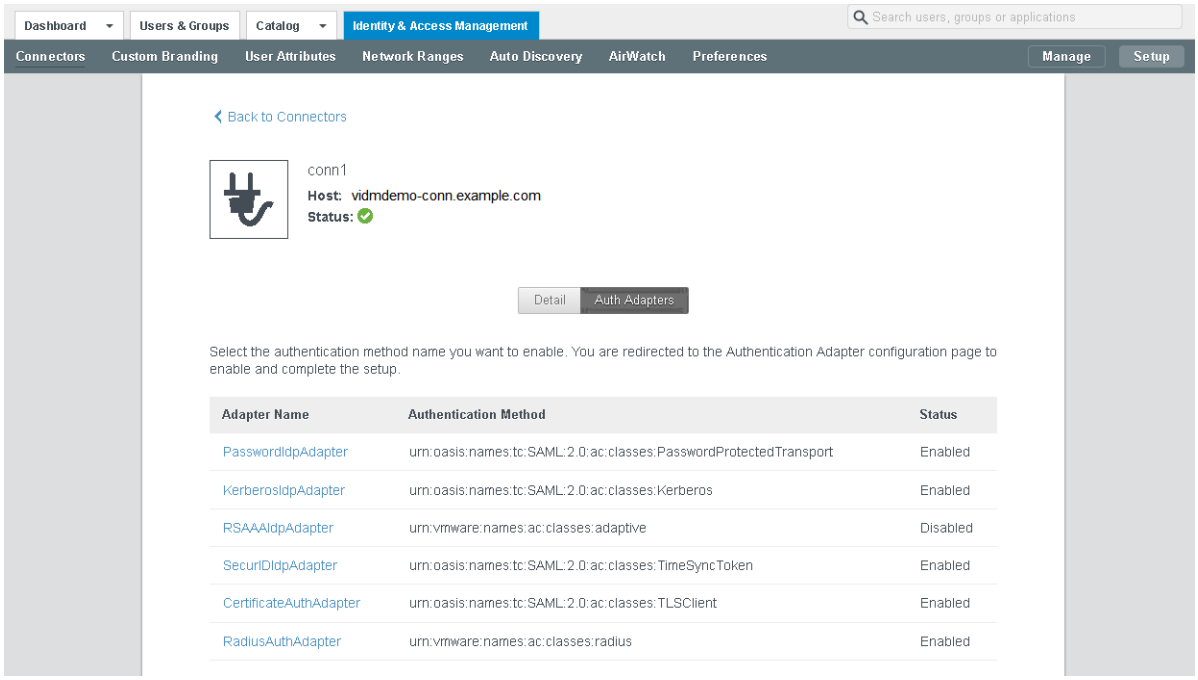
커넥터에 대해 사용 가능한 모든 인증 어댑터가 표시됩니다.

디렉토리를 이미 설정했으면 디렉토리를 생성하는 동안 지정한 구성 정보를 사용하여 PasswordIdpAdapter가 이미 구성되고 사용되도록 설정되어 있습니다.

5 각각에 대한 링크를 클릭하고 구성 정보를 입력하여 사용하려는 인증 어댑터를 구성하고 사용하도록 설정합니다. 하나 이상의 인증 어댑터를 사용하도록 설정해야 합니다.

특정 인증 어댑터 구성에 대한 자세한 내용은 VMware Identity Manager 관리 가이드를 참조하십시오.

예:



커넥터에 대해 아웃바운드 모드 사용

커넥터에 대해 아웃바운드 전용 연결 모드를 사용하도록 설정하려면 커넥터를 내장 ID 제공자에 연결합니다.

내장 ID 제공자는 기본적으로 VMware Identity Manager 서비스에서 사용할 수 있으며 VMware Verify와 같은 추가 내장 인증 방법을 제공합니다. 내장 ID 제공자에 대한 자세한 내용은 VMware Identity Manager 관리 가이드를 참조하십시오.

참고 해당 커넥터를 아웃바운드 및 일반 모드에서 동시에 사용할 수 있습니다. 아웃바운드 모드를 사용하도록 설정하더라도 여전히 인증 방법 및 정책을 사용하여 내부 사용자에 대한 Kerberos 인증을 구성할 수 있습니다.

프로시저

1 관리 콘솔의 **ID 및 액세스 관리** 탭에서 **관리**를 클릭합니다.

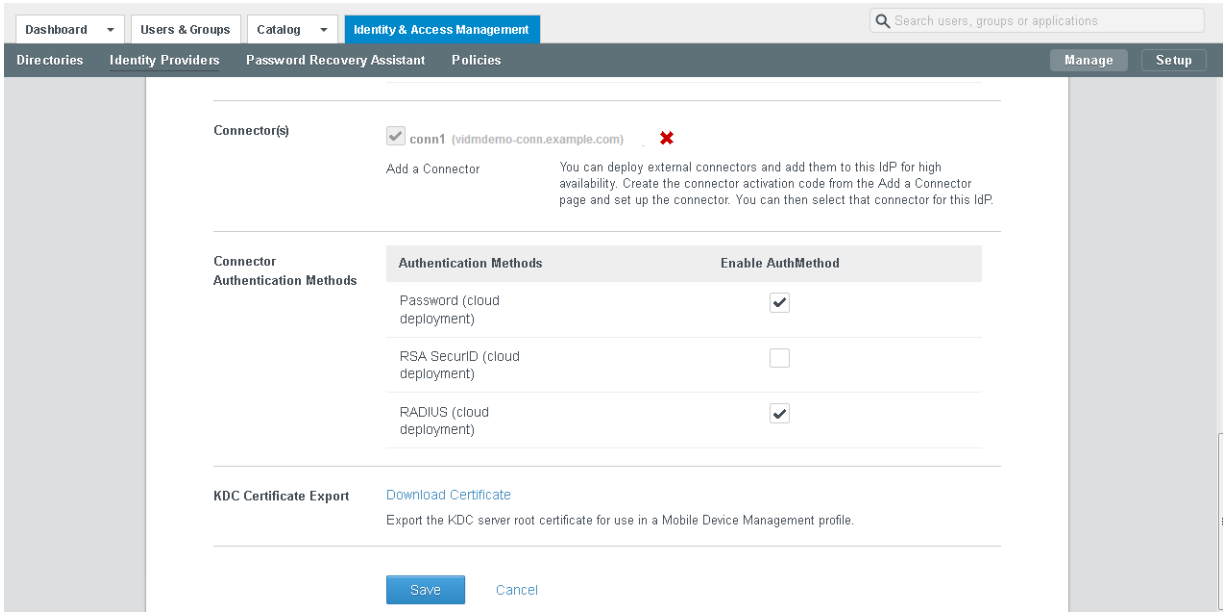
2 **ID 제공자** 탭을 클릭합니다.

3 **기본 제공** 링크를 클릭합니다.

4 다음 정보를 입력합니다.

옵션	설명
사용자	내장 ID 제공자를 사용할 디렉토리 또는 도메인을 선택합니다.
네트워크	내장 ID 제공자를 사용할 네트워크 범위를 선택합니다.
커넥터	설정한 커넥터를 선택합니다. **참고** 나중에 고가용성을 위해 추가 커넥터를 추가할 때 여기에서 커넥터를 선택한 후 추가하고 내장 ID 제공자에 연결합니다. VMware Identity Manager는내장 ID 제공자와 연결된 모든 커넥터에 트래픽을 자동으로 분산합니다. 따라서 로드 밸런서는 필요하지 않습니다.
커넥터 인증 방법	커넥터에 대해 사용하도록 설정한 배포 방법이 나열됩니다. 사용할 인증 방법을 선택합니다. 디렉토리를 생성할 때 자동으로 구성되고 사용되도록 설정된 PasswordIdpAdapter가 이 페이지에 **암호(클라우드 배포)**로 표시되어, 아웃바운드 모드에서 커넥터와 함께 사용됨을 나타냅니다.

예:



5 **저장**을 클릭하여 내장 ID 제공자 구성을 저장합니다.

6 사용하도록 설정한 인증 방법을 사용하도록 정책을 편집합니다.

a **ID 및 액세스 관리** 탭에서 **관리**를 클릭합니다.

b **정책** 탭을 클릭하고 편집하려는 정책을 클릭합니다.

c **정책 규칙**에서 편집하려는 규칙에 대해 **인증 방법** 열의 링크를 클릭합니다.

d [정책 규칙 편집] 페이지에서 이 규칙에 사용할 인증 방법을 선택합니다.

e **확인**을 클릭합니다.

f **저장**을 클릭합니다.

정책 구성에 대한 자세한 내용은 VMware Identity Manager 관리 가이드를 참조하십시오.

이제 커넥터의 아웃바운드 모드가 사용하도록 설정됩니다. 사용자가 [내장 ID 제공자] 페이지에서 커넥터에 대해 사용하도록 설정한 인증 방법 중 하나를 사용하여 로그인할 때 커넥터에 대한 HTTP 리디렉션이 필요하지 않습니다.

VMware Identity Manager 커넥터에 대해 고가용성 구성

클러스터에 여러 커넥터 가상 장치를 추가하여 고가용성 및 페일오버에 대해 VMware Identity Manager 커넥터를 설정할 수 있습니다. 어떤 이유로든 가상 장치 중 하나가 사용할 수 없게 되어도 다른 커넥터는 계속 사용할 수 있습니다.

클러스터를 생성하려면 새 커넥터 가상 장치를 설치하고, 첫 번째 커넥터를 설정할 때와 정확히 동일한 방식으로 구성합니다.

그런 다음 모든 커넥터 인스턴스를 기본 제공 ID 제공자에 연결합니다. VMware Identity Manager 서비스는 기본 제공 ID 제공자와 연결된 모든 커넥터에 트래픽을 자동으로 분산합니다. 따라서 로드 밸런서는 필요하지 않습니다. 네트워크 문제로 인해 커넥터 중 하나를 사용할 수 없게 되면 서비스는 해당 커넥터로 트래픽을 보내지 않습니다. 연결이 복원되면 서비스는 커넥터로 트래픽을 다시 보내기 시작합니다.

커넥터 클러스터를 설정한 후에는 커넥터에서 사용하도록 설정한 인증 방법이 고가용성으로 구성됩니다. 커넥터 인스턴스 중 하나를 사용할 수 없게 되어도 인증을 계속 사용할 수 있습니다. 그렇지만 디렉토리 동기화의 경우, 커넥터 인스턴스에 오류가 발생하면 수동으로 다른 커넥터 인스턴스를 동기화 커넥터로 선택해야 합니다. 디렉토리 동기화는 한 번에 한 커넥터에 대해서만 사용하도록 설정할 수 있습니다.

참고 Kerberos 인증의 고가용성에는 이 섹션이 적용되지 않습니다. "VMware Identity Manager Connector 배포에 Kerberos 인증 지원 추가," (25 페이지)의 내용을 참조하십시오.

추가 커넥터 인스턴스 설치

첫 번째 커넥터 인스턴스를 설치 및 구성한 후에 고가용성을 위해 커넥터를 더 추가할 수 있습니다. 새 커넥터 가상 장치를 설치하고, 첫 번째 커넥터 인스턴스와 정확히 같은 방식으로 구성합니다.

필수 조건

"VMware Identity Manager 커넥터 배포," (16 페이지)에 설명된 것처럼 첫 번째 커넥터 인스턴스를 설치하고 구성했습니다.

프로시저

1 다음 지침에 따라 새 커넥터 인스턴스를 설치 및 구성합니다.

   - "커넥터에 대한 활성화 코드 생성," (18 페이지)
   - "커넥터 가상 장치 설치 및 구성," (18 페이지)

2 새 커넥터를 첫 번째 커넥터 인스턴스의 WorkspaceIDP에 연결합니다.

   a 관리 콘솔에서 **ID 및 액세스 관리** 탭을 선택하고 **ID 제공자** 탭을 선택합니다.

   b [ID 제공자] 페이지에서 첫 번째 커넥터 인스턴스의 WorkspaceIDP를 찾은 후 링크를 클릭합니다.

   c **커넥터** 필드에서 새 커넥터를 선택합니다.

   d 바인딩 DN 암호를 입력하고 **커넥터 추가**를 클릭합니다.

   e **저장**을 클릭합니다.

3 첫 번째 커넥터 인스턴스에서 Active Directory 도메인에 가입한 경우 새 커넥터 인스턴스에서도 도메인에 가입해야 합니다.

a **ID 및 액세스 관리** 탭에서 **설정**을 클릭합니다.

새 커넥터 인스턴스가 [커넥터] 페이지에 나열됩니다.

b 새 커넥터 옆에 있는 **도메인 가입**을 클릭하고 도메인 정보를 지정합니다.

참고 IWA(Windows 통합 인증) 유형의 디렉토리에 대해 다음 작업을 수행해야 합니다.

a 새 커넥터 인스턴스를 원래 커넥터 인스턴스의 IWA 디렉토리가 가입된 도메인에 가입시킵니다.

1 **ID 및 액세스 관리** 탭을 선택하고 **설정**을 클릭합니다.

새 커넥터 인스턴스가 [커넥터] 페이지에 나열됩니다.

2 **도메인 가입**을 클릭하고 도메인 정보를 지정합니다.

b IWA 디렉토리 구성을 저장합니다.

1 **ID 및 액세스 관리** 탭을 선택합니다.

2 [디렉토리] 페이지에서 IWA 디렉토리 링크를 클릭합니다.

3 **저장**을 클릭하여 디렉토리 구성을 저장합니다.

---

4 새 커넥터에 대해 인증 어댑터를 구성하고 사용하도록 설정합니다.

중요 클러스터의 모든 커넥터에 대해 인증 어댑터를 동일하게 구성해야 합니다. 모든 커넥터에 대해 동일한 인증 방법을 사용하도록 설정해야 합니다.

---

a **ID 및 액세스 관리** 탭에서 **설정**을 클릭한 다음 **커넥터**탭을 클릭합니다.

b 새 커넥터의 **작업자** 열에 있는 링크를 클릭합니다.

c **인증 어댑터** 탭을 클릭합니다.

커넥터에 대해 사용 가능한 모든 인증 어댑터가 표시됩니다.

새 커넥터를 첫 번째 커넥터와 연결된 디렉토리에 연결했으므로 PasswordIdpAdapter가 이미 구성되고 사용되도록 설정되어 있습니다.

d 첫 번째 커넥터와 동일한 방식으로 다른 인증 어댑터도 구성하고 사용하도록 설정합니다. 구성 정보가 동일한지 확인합니다.

인증 어댑터 구성에 대한 자세한 내용은 VMware Identity Manager 관리 가이드를 참조하십시오.

후속 작업

"기본 제공 ID 제공자에 새 커넥터 추가," (24 페이지)

기본 제공 ID 제공자에 새 커넥터 추가

새 커넥터 인스턴스를 배포 및 구성한 후에 기본 제공 ID 제공자에 이를 추가하고 첫 번째 커넥터에서 사용하도록 설정한 동일한 인증 방법을 사용하도록 설정합니다. VMware Identity Manager는 기본 제공 ID 제공자와 연결된 모든 커넥터에 트래픽을 자동으로 분산합니다.

프로시저

1 관리 콘솔의 **ID 및 액세스 관리** 탭에서 **관리**를 클릭합니다.

2 **ID 제공자** 탭을 클릭합니다.

3 **기본 제공** 링크를 클릭합니다.

4 **커넥터** 필드의 드롭다운 목록에서 새 커넥터를 선택하고 **커넥터 추가**를 클릭합니다.

5 **커넥터 인증 방법** 섹션에서 첫 번째 커넥터에 대해 선택한 것과 동일한 인증 방법을 사용하도록 설정합니다.

암호(클라우드 배포) 인증 방법이 자동으로 구성되고 사용되도록 설정됩니다. 다른 인증 방법을 사용하도록 설정해야 합니다.

중요 클러스터의 모든 커넥터에 대해 인증 어댑터를 동일하게 구성해야 합니다. 모든 커넥터에 대해 동일한 인증 방법을 사용하도록 설정해야 합니다.

특정 인증 어댑터 구성에 대한 자세한 내용은 VMware Identity Manager 관리 가이드를 참조하십시오.

6 **저장**을 클릭하여 내장 ID 제공자 구성을 저장합니다.

실패할 경우 다른 커넥터에서 디렉토리 동기화 사용

커넥터 인스턴스 실패가 발생할 경우에는 다른 커넥터 인스턴스에서 인증을 자동으로 처리합니다. 하지만 디렉토리 동기화의 경우에는 VMware Identity Manager 서비스에서 원래 커넥터 인스턴스 대신 다른 커넥터 인스턴스를 사용하도록 디렉토리 설정을 수정해야 합니다. 디렉토리 동기화는 한 번에 한 커넥터에 대해서만 사용하도록 설정할 수 있습니다.

프로시저

1 VMware Identity Manager 관리 콘솔에 로그인합니다.

2 **ID 및 액세스 관리** 탭을 클릭한 후 **디렉토리**를 클릭합니다.

3 원래 커넥터 인스턴스와 연결된 디렉토리를 클릭합니다.

팁 **설정 > 커넥터** 페이지에서 이 정보를 볼 수 있습니다.

4 디렉토리 페이지의 **디렉토리 동기화 및 인증** 섹션에 있는 **커넥터 동기화** 드롭다운 목록에서 다른 커넥터 인스턴스를 선택합니다.

5 **바인딩 DN 암호** 텍스트 상자에서 Active Directory 바인딩 계정 암호를 입력합니다.

6 **저장**을 클릭합니다.

VMware Identity Manager Connector 배포에 Kerberos 인증 지원 추가

인바운드 연결 모드가 필요한 내부 사용자용 Kerberos 인증을 아웃바운드 전용 연결 모드 커넥터를 기반으로 하는 배포에 추가할 수 있습니다. 내부 네트워크에서 오는 사용자를 위해 Kerberos 인증을 사용하고 외부에서 들어오는 사용자를 위해 다른 인증 방법을 사용하도록 동일한 커넥터를 구성할 수 있습니다. 이 작업은 네트워크 범위를 기준으로 인증 정책을 정의하여 수행할 수 있습니다.

참고 Kerberos 인증에 대해 고가용성을 설정하려면 로드 밸런서가 필요합니다.

Kerberos 인증 어댑터 구성 및 사용

VMware Identity Manager 커넥터에서 KerberosIdpAdapter를 구성하고 사용하도록 설정합니다. 고가용성을 위해 클러스터를 배포한 경우 클러스터의 모든 커넥터에 대해 어댑터를 구성하고 사용하도록 설정합니다.

중요 클러스터의 모든 커넥터에 대해 인증 어댑터를 동일하게 구성해야 합니다. 모든 커넥터에 대해 동일한 인증 방법을 구성해야 합니다.

Kerberos 인증 구성에 대한 자세한 내용은 VMware Identity Manager 관리 가이드를 참조하십시오.

필수 조건

커넥터는 Active Directory 도메인에 가입되어야 합니다.

프로시저

1 VMware Identity Manager 관리 콘솔에서 **ID 및 액세스 관리** 탭을 클릭합니다.

2 **설정**을 클릭한 다음 **커넥터** 탭을 클릭합니다.

배포한 모든 연결이 나열됩니다.

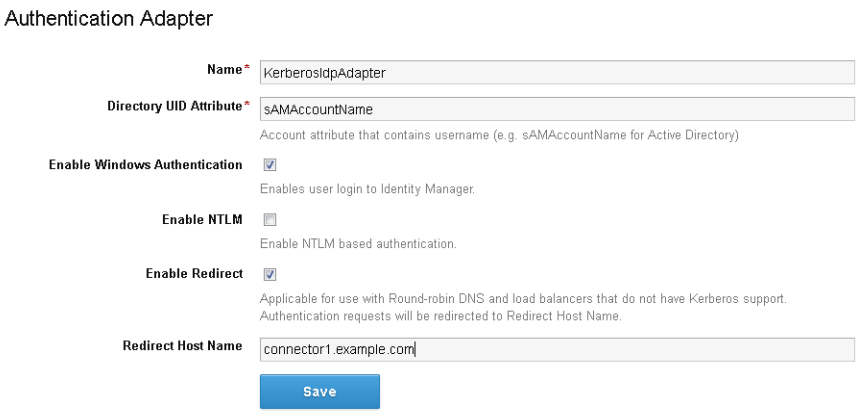
3 커넥터 중 하나의 **작업자** 열에 있는 링크를 클릭합니다.

4 **인증 어댑터** 탭을 클릭합니다.

5 KerberosIdpAdapter 링크를 클릭한 후 어댑터를 구성하고 사용하도록 설정합니다.

옵션	설명
이름	어댑터의 기본 이름은 KerberosIdpAdapter입니다. 이 이름은 변경할 수 있습니다.
디렉토리 UID 특성	사용자 이름을 포함하는 계정 특성입니다.
Windows 인증 사용	이 옵션을 선택합니다.
NTLM 사용	Active Directory 인프라가 NTLM 인증을 사용하지 않는 한, 이 옵션을 선택할 필요가 없습니다.
리디렉션 사용	클러스터에 여러 커넥터가 있고 로드 밸런서를 사용하여 Kerberos 고가용성을 설정하려는 경우 이 옵션을 선택하고 **리디렉션 호스트 이름**의 값을 지정합니다. 배포에 커넥터가 하나만 있으면 **리디렉션 사용** 및 **리디렉션 호스트 이름** 옵션을 사용할 필요가 없습니다.
리디렉션 호스트 이름	**리디렉션 사용** 옵션이 선택되면 값을 지정해야 합니다. 커넥터의 자체 호스트 이름을 입력합니다. 예를 들어 커넥터 호스트 이름이 connector1.example.com이면 텍스트 상자에 **connector1.example.com**을 입력합니다.

예:



KerberosIdPAdapter 구성에 대한 자세한 내용은 VMware Identity Manager 관리 가이드를 참조하십시오.

6 클러스터를 배포한 경우 클러스터의 모든 커넥터에 대해 KerberosIdPAdapter를 구성합니다.

모든 커넥터에 대해동일하게 어댑터를 구성해야 합니다.

후속 작업

필요한 경우 Kerberos 인증에 대해 고가용성을 설정합니다. Kerberos 인증은 로드 밸런서가 없으면 고가용성이 보장되지 않습니다.

Kerberos 인증에 대해 고가용성 구성

Kerberos 인증에 대해 고가용성을 구성하려면 방화벽 내부의 내부 네트워크에 로드 밸런서를 설치하고 여기에 커넥터 장치를 추가합니다.

또한 로드 밸런서에 대해 특정 설정을 구성하고, 로드 밸런서와 커넥터 간에 SSL 신뢰를 설정하고, 로드 밸런서 호스트 이름을 사용하도록 커넥터 인증 URL을 변경해야 합니다.

로드 밸런서 설정 구성

X-Forwarded-For 헤더 사용, 적절한 로드 밸런서 시간 초과 설정 및 엄격한 세션 사용 등 로드 밸런서에 대해 특정 설정을 구성해야 합니다.

다음 설정을 구성합니다.

- X-Forwarded-For 헤더

  로드 밸런서에서 X-Forwarded-For 헤더를 사용하도록 설정해야 합니다. 이를 통해 인증 방법이 결정됩니다. 자세한 정보는 로드 밸런서 공급업체에서 제공한 설명서를 참조하십시오.

- 로드 밸런서 시간 초과

  connector가 올바르게 작동하게 하려면 로드 밸런서의 요청 시간 초과 값을 기본값보다 높게 설정해야 할 수도 있습니다. 분 단위로 값을 설정합니다. 시간 초과 설정이 너무 낮으면 다음 오류가 발생할 수 있습니다.

  502 오류: 현재 서비스를 사용할 수 없습니다.

- 스티키 세션 사용

  배포에 여러 커넥터 장치가 있는 경우 로드 밸런서에서 스티키 세션 설정을 사용하도록 설정해야 합니다. 그러면 로드 밸런서가 사용자의 세션을 특정 커넥터 인스턴스에 바인딩합니다.

로드 밸런서에 VMware Identity Manager Connector 루트 인증서 적용

로드 밸런서를 사용하여 VMware Identity Manager connector 가상 장치가 구성되면 로드 밸런서와 connector 간에 SSL 신뢰를 설정해야 합니다. connector 루트 인증서를 로드 밸런서에 복사해야 합니다.

connector 인증서는 커넥터 장치 관리 페이지(https://myconnector.mycompany:8443/cfg/ssl)에서 다운로드할 수 있습니다.

connector 도메인 이름이 로드 밸런서를 가리키는 경우 SSL 인증서가 해당 로드 밸런서에만 적용될 수 있습니다.

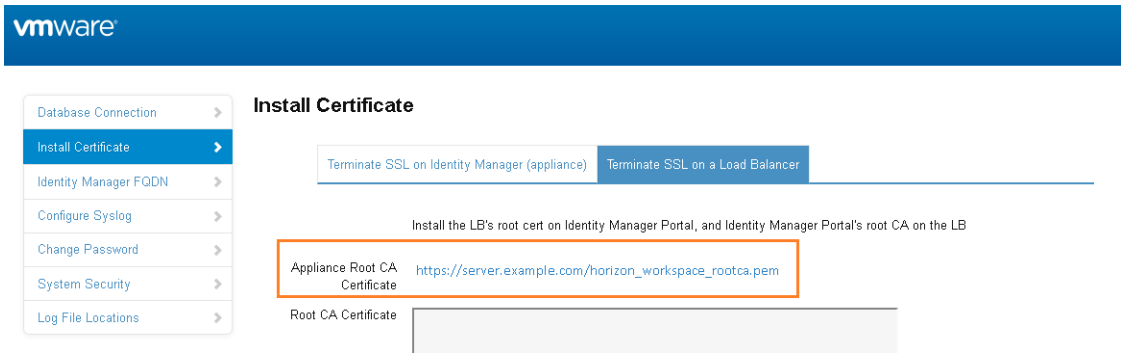
로드 밸런서가 connector 가상 장치와 통신하므로 connector 루트 CA 인증서를 신뢰할 수 있는 루트 인증서로 로드 밸런서에 복사해야 합니다.

프로시저

1 connector 장치 관리자 페이지(https://myconnector.mycompany:8443/cfg/ssl)에 관리자 권한으로 로그인합니다.

2 **인증서 설치**를 선택합니다.

3 **로드 밸런서에서 SSL 종료** 탭을 선택하고 **장치 루트 CA 인증서** 필드에서 링크 https://*hostname*/horizon_workspace_rootca.pem을 클릭합니다.



4 -----BEGIN CERTIFICATE----- 및 -----END CERTIFICATE---- 줄을 포함하여 사이의 모든 항목을 복사한 후 루트 인증서를 각 로드 밸런서의 올바른 위치에 붙여넣습니다. 로드 밸런서 설명서를 참조하십시오.

후속 작업

로드 밸런서 루트 인증서를 복사한 후 VMware Identity Managerconnector 장치에 붙여넣습니다.

VMware Identity Manager Connector에 로드 밸런서 루트 인증서 적용

로드 밸런서를 사용하여 VMware Identity Manager connector 가상 장치가 구성되면 로드 밸런서와 connector 간에 신뢰를 설정해야 합니다. 로드 밸런서에 connector 루트 인증서를 복사하는 것 외에, 로드 밸런서 루트 인증서를 connector에 복사해야 합니다.

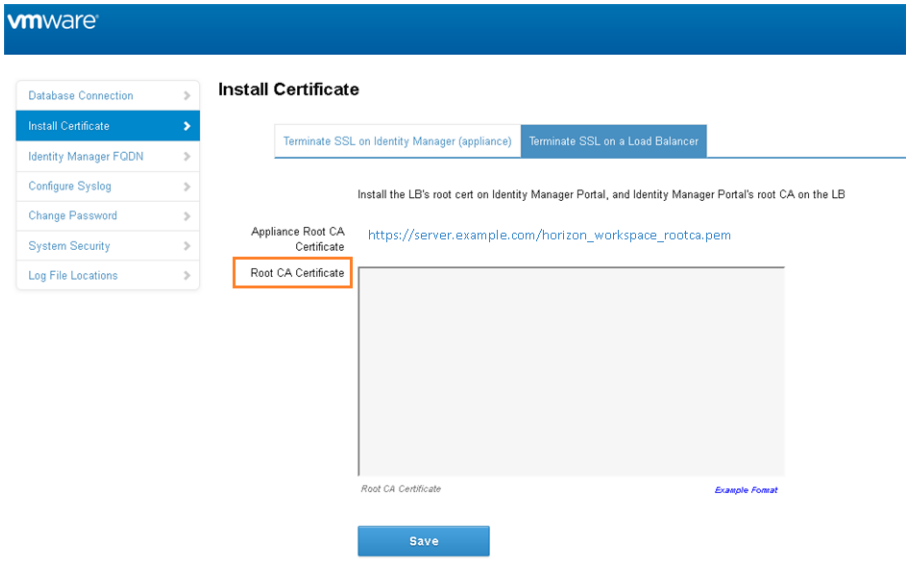
프로시저

1 로드 밸런서 루트 인증서를 가져옵니다.

2 connector 장치 관리 페이지(https://myconnector.mycompany:8443/cfg/ssl)로 이동한 후 관리자로 로그인합니다.

3 **인증서 설치** 페이지에서 **로드 밸런서에서 SSL 종료** 탭을 선택합니다.

4 로드 밸런서 인증서의 텍스트를 **루트 CA 인증서** 필드에 붙여넣습니다.



5 **저장**을 클릭합니다.

커넥터 IdP 호스트 이름을 로드 밸런서 호스트 이름으로 변경

로드 밸런서에 커넥터 가상 장치를 추가한 후에 각 커넥터의 Workspace IdP에 있는 IdP 호스트 이름을 로드 밸런서 호스트 이름으로 변경해야 합니다.

필수 조건

connector 가상 장치는 로드 밸런서 뒤에 구성해야 합니다. 로드 밸런서 포트가 443인지 확인합니다. 포트 번호 8443은 관리 포트이고 가상 장치마다 고유하므로 사용하면 안 됩니다.

프로시저

1 VMware Identity Manager 관리 콘솔에 로그인합니다.

2 **ID 및 액세스 관리** 탭을 클릭합니다.

3 **ID 제공자** 탭을 클릭합니다.

4 [ID 제공자] 페이지에서 connector 인스턴스에 대한 Workspace IdP 링크를 클릭합니다.

5 **IdP 호스트 이름** 텍스트 상자에서 connector 호스트 이름의 호스트 이름을 로드 밸런서 호스트 이름으로 변경합니다.

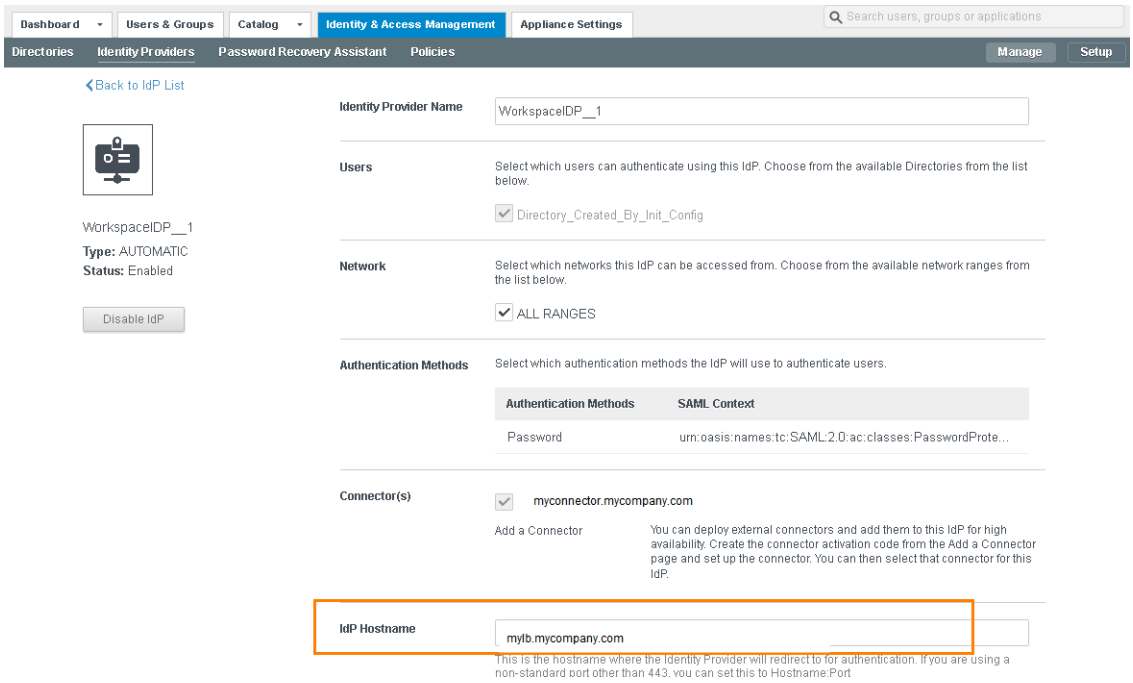
   예를 들어 connector 호스트 이름이 `myconnector`이고 로드 밸런서 호스트 이름이 `mylb`이면 다음 URL

   `myconnector.mycompany.com:포트`

   를

   다음으로 변경합니다.

   `mylb.mycompany.com:포트`



색인