

Access Point 배포 및 구 성

Unified Access Gateway 2.8



vmware®

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

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

Copyright © 2016 VMware, Inc. 판권 소유. [저작권 및 상표 정보](#).

목차

VMware Access Point 배포 및 구성 5

1 Access Point 배포 준비 6

- 보안 게이트웨이로서의 Access Point 6
- VPN(Virtual Private Network) 대신 Access Point 사용 7
- Access Point 시스템 및 네트워크 요구 사항 7
- DMZ 기반 Access Point 장치의 방화벽 규칙 9
- Access Point 로드 밸런싱 토폴로지 11
- 다중 네트워크 인터페이스 카드가 있는 Access Point의 DMZ 설계 13

2 Access Point 장치 배포 17

- OVF 템플릿 마법사를 사용하여 Access Point 배포 17
 - Access Point 배포 속성 18
 - OVF 템플릿 마법사를 사용하여 Access Point 배포 19
- 관리 구성 페이지에서 Access Point 구성 22
 - Access Point 시스템 설정 구성 23
- SSL 서버 서명된 인증서 업데이트 24

3 PowerShell을 사용하여 Access Point 배포 26

- PowerShell을 사용하여 Access Point를 배포하기 위한 시스템 요구 사항 26
- PowerShell을 사용하여 Access Point 장치 배포 27

4 배포 사용 사례 29

- Horizon View 및 Horizon Air Hybrid-Mode를 사용하여 Access Point 배포 29
 - Horizon 설정 구성 33
- 역방향 프록시로 Access Point 배포 35
 - VMware Identity Manager용 역방향 프록시 구성 37
- AirWatch Tunnel을 사용한 Access Point 배포 38
 - AirWatch에 대한 터널 프록시 배포 39
 - AirWatch를 사용한 애플리케이션별 Tunnel 배포 39
 - AirWatch에 대한 애플리케이션별 Tunnel 및 프록시 설정 구성 40

5 TLS/SSL 인증서를 사용하여 Access Point 구성 42

- Access Point 장치용 TLS/SSL 인증서 구성 42
 - 올바른 인증서 유형 선택 42
 - 인증서 파일을 한 줄 PEM 형식으로 변환 43
 - Access Point 의 기본 TLS/SSL 서버 인증서 교체 45
 - TLS 또는 SSL 통신에 사용되는 보안 프로토콜 및 암호 제품군 변경 46

6 DMZ에서 인증 구성 48

- Access Point 장치에서 인증서 또는 스마트 카드 인증 구성 48
 - Access Point에서 인증서 인증 구성 49
 - 인증 기관 인증서 가져오기 50
 - Access Point에서 RSA SecurID 인증 구성 52
 - Access Point에 대한 RADIUS 구성 53
 - RADIUS 인증 구성 53
 - Access Point에서 RSA 어댑티브 인증 구성 54
 - Access Point에서 RSA 어댑티브 인증 구성 55
 - Access Point SAML 메타데이터 생성 57
 - 다른 서비스 제공자가 사용하는 SAML 인증자 만들기 58
 - 서비스 제공자 SAML 메타데이터를 Access Point에 복사 58

7 Access Point 배포 문제 해결 59

- 배포 오류 해결 59
- Access Point 장치에서 로그 수집 61
- 디버그 모드 사용 62

VMware Access Point 배포 및 구성

Access Point 배포 및 구성에서는 조직 애플리케이션에 대한 보안 외부 액세스를 사용할 수 있도록 하기 위해 VMware Access Point™를 사용하는 VMware Horizon®, VMware Identity Manager™ 및 VMware AirWatch® 배포를 설계하는 방법에 대한 정보를 제공합니다. 이러한 애플리케이션은 Windows 애플리케이션, SaaS(Software as a Service) 애플리케이션 및 데스크톱일 수 있습니다. 이 가이드에서는 또한 Access Point 가상 장치를 배포하고 배포 후에 구성 설정을 변경하는 방법에 대한 지침을 제공합니다.

대상

이 정보는 Access Point 장치를 배포하고 사용하려는 모든 사용자를 대상으로 합니다. 이 정보는 가상 시스템 기술과 데이터 센터 운영을 잘 아는 숙련된 Linux 및 Windows 시스템 관리자를 대상으로 작성되었습니다.

Access Point 배포 준비

Access Point는 회사 방화벽 외부에서 원격 데스크톱 및 애플리케이션에 액세스하려는 사용자에게 보안 게이트웨이로 사용됩니다.

이 장에서는 다음 주제에 대해 설명합니다.

- 보안 게이트웨이로서의 Access Point
- VPN(Virtual Private Network) 대신 Access Point 사용
- Access Point 시스템 및 네트워크 요구 사항
- DMZ 기반 Access Point 장치의 방화벽 규칙
- Access Point 로드 밸런싱 토폴로지
- 다중 네트워크 인터페이스 카드가 있는 Access Point의 DMZ 설계

보안 게이트웨이로서의 Access Point

Access Point는 일반적으로 DMZ(예외 구역)에 설치되는 계층 7 보안 장치입니다. Access Point는 강력하게 인증된 원격 사용자에게 대한 트래픽만 회사 데이터 센터로 유입되도록 하는 데 사용됩니다.

Access Point에서는 인증 요청을 적절한 서버로 보내고 인증되지 않은 요청을 모두 삭제합니다. 사용자는 액세스 권한을 부여받은 리소스에만 액세스할 수 있습니다.

또한 Access Point 가상 장치는 인증된 사용자에게 대한 트래픽이 사용자에게 실제로 사용 권한이 있는 데스크톱 및 애플리케이션 리소스로만 전송될 수 있도록 합니다. 이러한 수준의 보호에는 액세스를 정확히 제어하기 위해 데스크톱 프로토콜의 특정 조사 기능 및 빨리 바뀔 수 있는 정책 및 네트워크 주소 조정 기능이 포함됩니다.

Access Point 장치는 일반적으로 네트워크 DMZ(예외 구역) 내에 있으며 회사의 신뢰할 수 있는 네트워크에서 연결에 대한 프록시 호스트로 작동합니다. 이 설계에서는 가상 데스크톱, 애플리케이션 호스트 및 서버를 공용 인터넷으로부터 보호하여 추가 보안 계층을 제공합니다.

Access Point는 DMZ용으로 특수하게 디자인된 보안 강화 장치입니다. 다음 보안 강화 설정이 구현됩니다.

- 최신 Linux 커널 및 소프트웨어 패치
- 인터넷 및 인트라넷 트래픽에 대한 다중 NIC 지원
- SSH 사용 안 함

- FTP, 텔넷, Rlogin 또는 Rsh 서비스 사용 안 함
- 원치 않는 서비스 사용 안 함

VPN(Virtual Private Network) 대신 Access Point 사용

Access Point 및 일반 VPN 솔루션은 강력하게 인증된 사용자에게 대한 트래픽만 내부 네트워크로 전달되도록 한다는 측면에서 서로 유사합니다.

일반 VPN보다 더 나은 Access Point의 장점은 다음과 같습니다.

- Access Control Manager. Access Point는 액세스 규칙을 자동으로 적용합니다. Access Point는 사용자의 사용 권한 및 내부적으로 연결하는 데 필요한 주소(빠르게 변경될 수 있음)를 인식합니다. 대부분의 VPN은 관리자가 모든 사용자 또는 사용자 그룹에 대한 네트워크 연결 규칙을 개별적으로 구성할 수 있도록 하므로 VPN 하나로도 동일한 역할을 합니다. 처음에는 VPN 하나로 충분하지만 나중에는 필요한 규칙을 유지 관리하기 위해 상당한 관리 노력이 필요합니다.
- 사용자 인터페이스. Access Point는 직관적인 Horizon Client 사용자 인터페이스를 변경하지 않습니다. Access Point를 사용하면 Horizon Client를 실행할 때 인증된 사용자가 View 환경에서 작업하게 되며 데스크톱 및 애플리케이션에 대한 액세스를 제어할 수 있습니다. VPN은 사용자가 먼저 VPN 소프트웨어를 설치한 다음 별도로 인증을 받고 Horizon Client를 실행하도록 요구합니다.
- 성능: Access Point는 보안 및 성능을 최대화하도록 디자인되었습니다. Access Point를 사용하면 추가 캡슐화 없이도 PCoIP, HTML Access 및 WebSocket 프로토콜 보안이 유지됩니다. VPN은 SSL VPN으로 구현됩니다. 이러한 구현은 보안 요구 사항을 충족하며, TLS(Transport Layer Security)가 설정되면 안전한 것으로 간주됩니다. 하지만 SSL/TLS를 사용한 기본 프로토콜은 TCP만을 기반으로 합니다. 연결 없는 UDP 기반 전송을 활용하는 최신 비디오 원격 프로토콜을 사용하면 TCP 기반 전송을 통해 실행될 경우 성능상의 이점이 크게 줄어들 수 있습니다. SSL/TLS 대신 DTLS 또는 IPsec으로도 작동할 수 있는 VPN 기술은 View 데스크톱 프로토콜에서도 잘 작동할 수 있기 때문에 이러한 특성이 모든 VPN 기술에 해당되는 것은 아닙니다.

Access Point 시스템 및 네트워크 요구 사항

Access Point 장치를 배포하려면 시스템이 하드웨어 및 소프트웨어 요구 사항을 충족하는지 확인합니다.

지원되는 VMware 제품 버전

특정 버전의 VMware 제품을 특정 버전의 Access Point와 함께 사용해야 합니다. 호환성에 대한 최신 정보를 보려면 제품 릴리스 노트를 참조하십시오. 그리고

http://www.vmware.com/resources/compatibility/sim/interop_matrix.php에 있는 VMware 제품 상호 운용성 매트릭스를 참조하십시오. 릴리스 노트와 상호 운용성 매트릭스에 있는 정보가 이 가이드의 정보보다 우선적으로 적용됩니다.

Access Point 2.8을 다음 VMware 오픈링에서 보안 게이트웨이로 사용할 수 있습니다.

- VMware AirWatch 8.4 이상
- VMware Identity Manager 2.7 이상

- VMware Horizon 6.2 이상
- VMware Horizon Air Hybrid-Mode 1.0 이상
- VMware Horizon Air 15.3 이상

ESXi Server에 대한 하드웨어 요구 사항

Access Point 장치는 사용 중인 Horizon 제품 및 버전에 대해 지원되는 것과 같은 버전의 vSphere에 배포되어 있어야 합니다.

vSphere Web Client를 사용하려면 클라이언트 통합 플러그인이 설치되어 있는지 확인합니다. 자세한 내용은 vSphere 설명서를 참조하십시오. 배포 마법사를 시작하기 전에 이 플러그인을 설치하지 않으면 플러그인을 설치하라는 메시지가 표시됩니다. 이 경우 브라우저를 닫고 마법사를 종료해야 합니다.

참고 장치의 시간이 올바르게 설정되도록 Access Point 장치에서 시계(UTC)를 구성합니다. 예를 들어 Access Point 가상 시스템에서 콘솔 창을 열고 화살표 버튼을 사용하여 올바른 시간대를 선택합니다. 또한 ESXi 호스트의 시간이 NTP 서버와 동기화되는지 확인하고 장치 가상 시스템에서 실행 중인 VMware Tools가 ESXi 호스트의 시간과 가상 시스템의 시간을 동기화하는지 확인합니다.

가상 장치 요구 사항

Access Point 장치의 OVF 패키지에서는 Access Point에 필요한 가상 시스템 구성을 자동으로 선택합니다. 이러한 설정을 변경할 수 있지만 CPU, 메모리 또는 디스크 공간은 기본 OVF 설정보다 더 작은 값으로 변경하지 않는 것이 좋습니다.

장치에 사용할 데이터스토어에 사용 가능한 디스크 공간이 충분하며 다른 시스템 요구 사항을 충족하는지 확인합니다.

- 가상 장치 다운로드 크기는 2.5GB입니다.
- 썸 프로비저닝된 디스크 최소 요구 사항은 2.5GB입니다.
- 씹 프로비저닝된 디스크 최소 요구 사항은 20GB입니다.

가상 장치를 배포하려면 다음 정보가 필요합니다.

- 정적 IP 주소
- DNS 서버의 IP 주소
- 루트 사용자 암호
- Access Point 장치가 가리키는 서버 인스턴스 또는 로드 밸런서의 URL

네트워킹 구성 요구 사항

1~3개의 네트워크 인터페이스를 사용할 수 있으며 Access Point에서는 각각 별도의 고정 IP 주소를 필요로 합니다. 많은 DMZ 구현에서 별도의 네트워크를 사용하여 서로 다른 여러 트래픽 유형을 보호합니다. 배포된 DMZ의 네트워크 설계에 따라 Access Point를 구성합니다.

- 개념 증명(PoC)이나 테스트에는 네트워크 인터페이스를 하나만 사용하는 것이 적절합니다. NIC가 하나이면 외부, 내부 및 관리 트래픽이 모두 동일한 서브넷에 있습니다.
- 네트워크 인터페이스가 두 개인 경우에는 외부 트래픽이 한 서브넷에 있고 내부 및 관리 트래픽이 다른 서브넷에 있습니다.
- 가장 안전한 옵션은 세 개의 네트워크 인터페이스를 사용하는 것입니다. NIC가 세 개인 경우 외부, 내부 및 관리 트래픽에는 모두 별도의 서브넷이 사용됩니다.

중요 각 네트워크에 IP 풀을 할당했는지 확인합니다. 그러면 배포 시에 Access Point 장치에서 서브넷 마스크 및 게이트웨이 설정을 가져올 수 있습니다. vSphere Client를 사용하는 경우에 IP 풀을 추가하려면 vCenter Server에서 데이터 센터의 **IP 풀** 탭으로 이동합니다. 또는 vSphere Web Client를 사용하는 경우 네트워크 프로토콜 프로파일을 생성할 수 있습니다. 데이터 센터의 **관리** 탭으로 이동하여 **네트워크 프로토콜 프로파일** 탭을 선택합니다. 자세한 내용은 [가상 시스템 네트워킹용으로 프로토콜 프로파일 구성](#)을 참조하십시오.

로그 보존 요구 사항

로그 파일은 기본적으로 집계에 있는 전체 디스크 크기보다 작은 특정 공간을 사용하도록 구성됩니다. Access Point에 대한 로그는 기본적으로 순환됩니다. 이러한 로그 항목을 보존하려면 syslog를 사용해야 합니다. [Access Point 장치에서 로그 수집](#)의 내용을 참조하십시오.

DMZ 기반 Access Point 장치의 방화벽 규칙

DMZ 기반 Access Point 장치는 프론트엔드와 백엔드 방화벽에 대해 특정 방화벽 규칙을 필요로 합니다. 설치 도중 기본적으로 특정 네트워크 포트에서 수신하도록 Access Point 서비스가 설정됩니다.

DMZ 기반 Access Point 장치의 배치에는 일반적으로 두 개의 방화벽이 포함되어 있습니다.

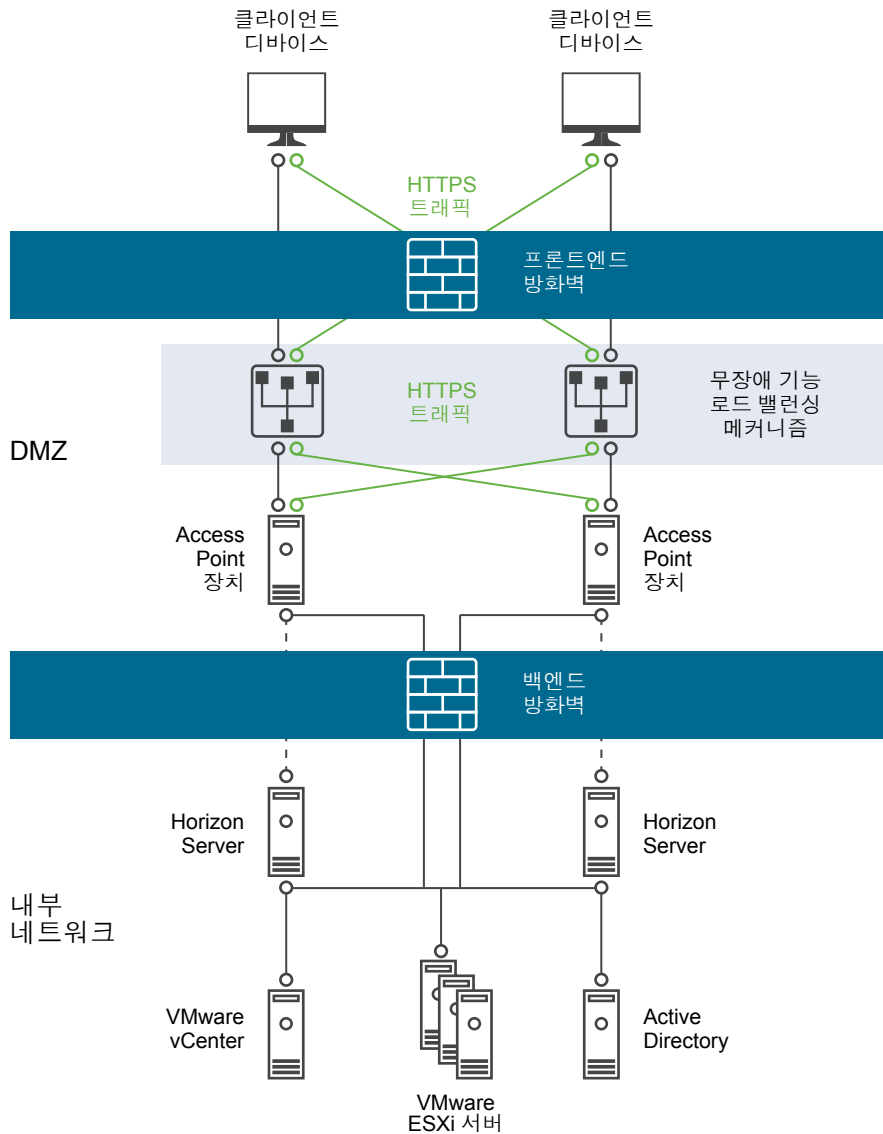
- 외부 네트워크 지향 프론트엔드 방화벽은 DMZ와 내부 네트워크를 보호해야 합니다. 외부 네트워크 트래픽이 DMZ에 도달할 수 있도록 방화벽을 구성합니다.
- DMZ와 내부 네트워크 사이의 백엔드 방화벽은 두 번째 보안 계층을 제공하기 위해 필요합니다. DMZ 내에 있는 서비스에서 발생한 트래픽만 허용하도록 방화벽을 구성합니다.

방화벽 정책은 DMZ 서비스의 인바운드 통신을 철저하게 제어하여 내부 네트워크 손상 위험을 크게 줄입니다.

외부 클라이언트 디바이스가 DMZ 내에 있는 Access Point 장치에 연결할 수 있도록 허용하려면 프론트엔드 방화벽에서 특정 포트에 대한 트래픽을 허용해야 합니다. 기본적으로 외부 클라이언트 디바이스 및 외부 웹 클라이언트(HTML Access)는 TCP 포트 443에서 DMZ 내의 Access Point 장치에 연결합니다. Blast 프로토콜을 사용할 경우 방화벽에서 포트 443이 열려 있어야 합니다. PCOIP 프로토콜을 사용할 경우 방화벽에서 포트 4172가 열려 있어야 합니다.

다음 그림에서는 프론트엔드 및 백엔드 방화벽을 포함하는 구성의 예를 보여줍니다.

그림 1-1. 이중 방화벽 토폴로지



Access Point 로드 밸런싱 토폴로지

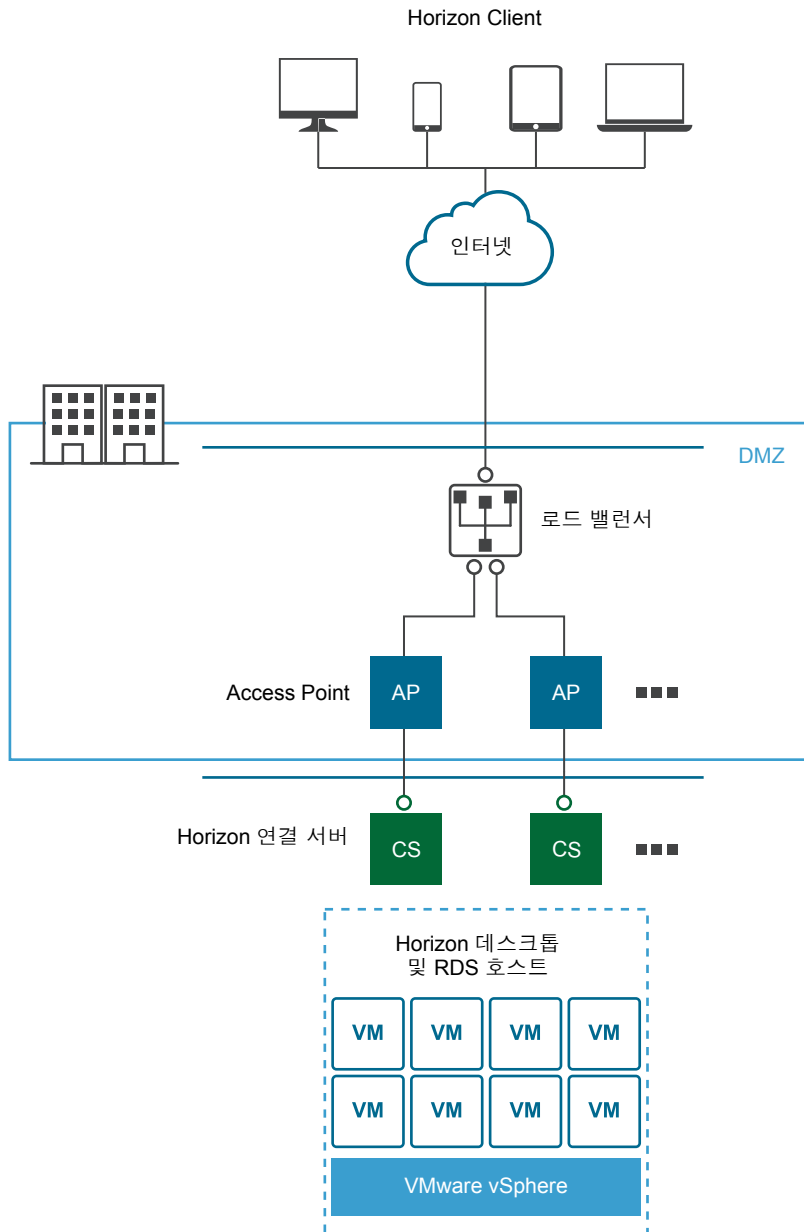
서로 다른 여러 토폴로지를 원하는 대로 구현할 수 있습니다.

DMZ에 있는 Access Point 장치는 서버 또는 서버 그룹의 앞에 있는 로드 밸런서를 가리키도록 구성할 수 있습니다. Access Point 장치는 HTTPS에 대해 구성된 표준 타사 로드 밸런싱 솔루션에서 작동합니다.

Access Point 장치가 서버 앞의 로드 밸런서를 가리키는 경우에는 서버 인스턴스의 선택이 동적으로 이루어집니다. 예를 들어, 로드 밸런서에서 각 서버 인스턴스의 현재 세션 수에 대한 정보와 가용성을 기준으로 선택할 수 있습니다. 회사 방화벽 내의 서버 인스턴스에는 보통 내부 액세스를 지원하기 위한 로드 밸런서가 있습니다. Access Point를 사용하면 Access Point 장치가 이미 자주 사용되고 있는 이 로드 밸런서를 가리키도록 할 수 있습니다.

또는 하나 이상의 Access Point 장치가 개별 서버 인스턴스를 가리키게 할 수도 있습니다. 두 가지 방법 모두 DMZ에서 두 개 이상의 Access Point 장치 앞에 있는 로드 밸런서를 사용합니다.

그림 1-2. 로드 밸런서 뒤에 있는 여러 Access Point 장치



Horizon 프로토콜

Horizon Client 사용자가 Horizon 환경에 연결할 때는 여러 다른 프로토콜이 사용됩니다. 첫 번째 연결은 항상 HTTPS를 통한 기본 XML-API 프로토콜입니다. 성공적인 인증 후에 하나 이상의 보조 프로토콜도 작성됩니다.

- 기본 Horizon 프로토콜

사용자가 Horizon Client에서 호스트 이름을 입력하면 기본 Horizon 프로토콜이 시작됩니다. 이는 인증 권한 부여 및 세션 관리를 위한 제어 프로토콜입니다. 이 프로토콜은 HTTPS를 통해 XML로 구조화된 메시지를 사용합니다(SSL을 통한 HTTP). 이 프로토콜은 경우에 따라 Horizon XML-API 제어 프로토콜로 알려져 있습니다. 위에 표시된 로드 밸런서 뒤에 있는 여러

Access Point 장치 그림처럼 로드 밸런싱된 환경에서 로드 밸런서는 이 연결을 Access Point 장치 중 하나로 라우팅합니다. 일반적으로 로드 밸런서는 먼저 가용성을 기준으로 장치를 선택한 다음 사용 가능한 장치 중에서 현재 세션 수가 가장 적은 장치를 기준으로 트래픽을 라우팅합니다. 이러한 구성은 여러 다른 클라이언트의 트래픽을 사용 가능한 Access Point 장치 집합으로 균일하게 분산합니다.

■ 보조 Horizon 프로토콜

Horizon Client가 Access Point 장치 중 하나에 대해 보안 통신을 설정하면 사용자가 인증을 받습니다. 이 인증 시도가 성공하면 Horizon 클라이언트로부터 하나 이상의 보조 연결이 설정됩니다. 이러한 보조 연결에는 다음이 포함될 수 있습니다.

- RDP, MMR/CDR과 같은 TCP 프로토콜을 캡슐화하는 데 사용되는 HTTPS 터널 및 클라이언트 프레임워크 채널. (TCP 443).
- Blast Extreme 디스플레이 프로토콜(TCP 443 및 UDP 443).
- PCoIP 디스플레이 프로토콜(TCP 4172 및 UDP 4172).

이러한 보조 Horizon 프로토콜은 기본 Horizon 프로토콜이 라우팅된 동일한 Access Point 장치로 라우팅되어야 합니다. 그런 다음 Access Point는 인증된 사용자 세션을 기준으로 보조 프로토콜을 인증할 수 있습니다. Access Point의 중요한 보안 기능은 트래픽이 인증된 사용자에 대한 것일 경우에만 Access Point가 회사 데이터 센터로 트래픽을 전달한다는 것입니다. 보조 프로토콜이 기본 프로토콜 장치가 아닌 다른 Access Point 장치로 잘못 라우팅되면 인증되지 않고 DMZ에 배치됩니다. 연결은 실패합니다. 로드 밸런서가 잘못 구성된 경우 보조 프로토콜을 잘못 라우팅하는 문제가 일반적으로 발생합니다.

다중 네트워크 인터페이스 카드가 있는 Access Point의 DMZ 설계

Access Point는 일반적으로 DMZ(예외 구역)에 설치되는 계층 7 보안 장치입니다. Access Point는 강력하게 인증된 원격 사용자에 대한 트래픽만 회사 데이터 센터로 유입되도록 하는 데 사용됩니다.

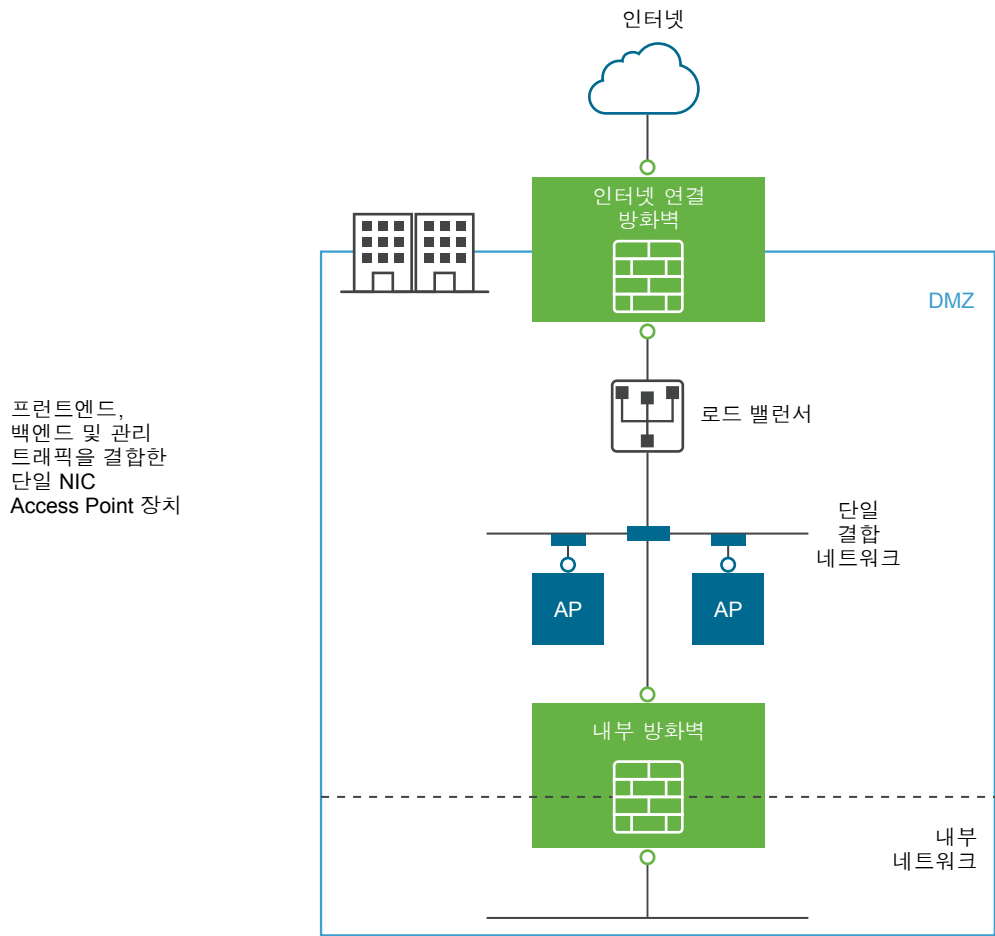
Access Point에 대한 구성 설정 중 하나는 사용할 가상 NIC(네트워크 인터페이스 카드) 번호입니다. Access Point를 배포할 때 네트워크에 대한 배포 구성을 선택합니다. onenic, twonic 또는 threonic으로 지정된 1개, 2개 또는 3개의 NICS 설정을 지정할 수 있습니다.

각 가상 LAN의 열린 포트 수를 줄이고 다른 유형의 네트워크 트래픽을 분리하면 보안을 크게 강화할 수 있습니다. 심층 방어 DMZ 보안 설계 전략의 일부로 다른 유형의 네트워크 트래픽을 분리하고 격리한다는 측면에서 이점을 얻을 수 있습니다. 이는 DMZ 내에 여러 가상 LAN을 두어 DMZ 내에 별도의 물리적 스위치를 구현하거나 전체 VMware NSX 관리 DMZ의 일부로 구현할 수 있습니다.

일반적인 단일 NIC DMZ 배포

가장 간단한 Access Point 배포는 모든 네트워크 트래픽이 단일 네트워크에 결합되는 단일 NIC를 통해 구현됩니다. 인터넷 연결 방화벽의 트래픽은 사용 가능한 Access Point 장치 중 하나로 전송됩니다. 그러면 Access Point는 내부 방화벽을 통해 내부 네트워크의 리소스로 인증된 트래픽을 전달합니다. Access Point는 인증되지 않은 트래픽을 삭제합니다.

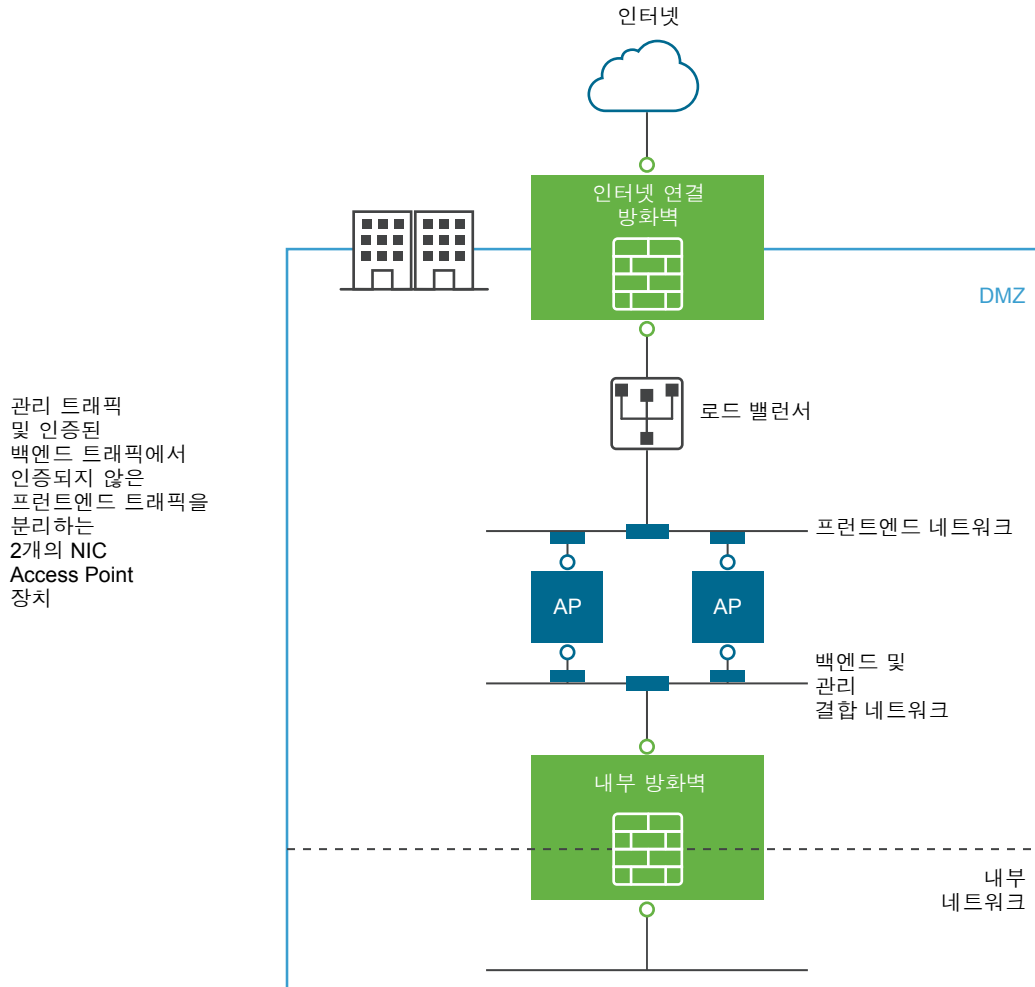
그림 1-3. Access Point의 단일 NIC 옵션



백엔드 및 관리 트래픽에서 인증되지 않은 사용자 트래픽 분리

단일 NIC 배포를 사용하는 것보다 2개의 NIC를 지정하는 것이 좋습니다. 첫 번째 NIC는 인터넷에 연결된 인증되지 않은 액세스에 계속 사용되지만 백엔드의 인증된 트래픽 및 관리 트래픽은 다른 네트워크로 분리됩니다.

그림 1-4. Access Point의 두 NIC 옵션



두 NIC 배포에서 내부 방화벽을 통해 내부 네트워크로 이동되는 트래픽은 Access Point에 의해 인증되어야 합니다. 인증되지 않은 트래픽은 이 백엔드 네트워크에 없습니다. Access Point용 REST API와 같은 관리 트래픽은 이 두 번째 네트워크에만 있습니다.

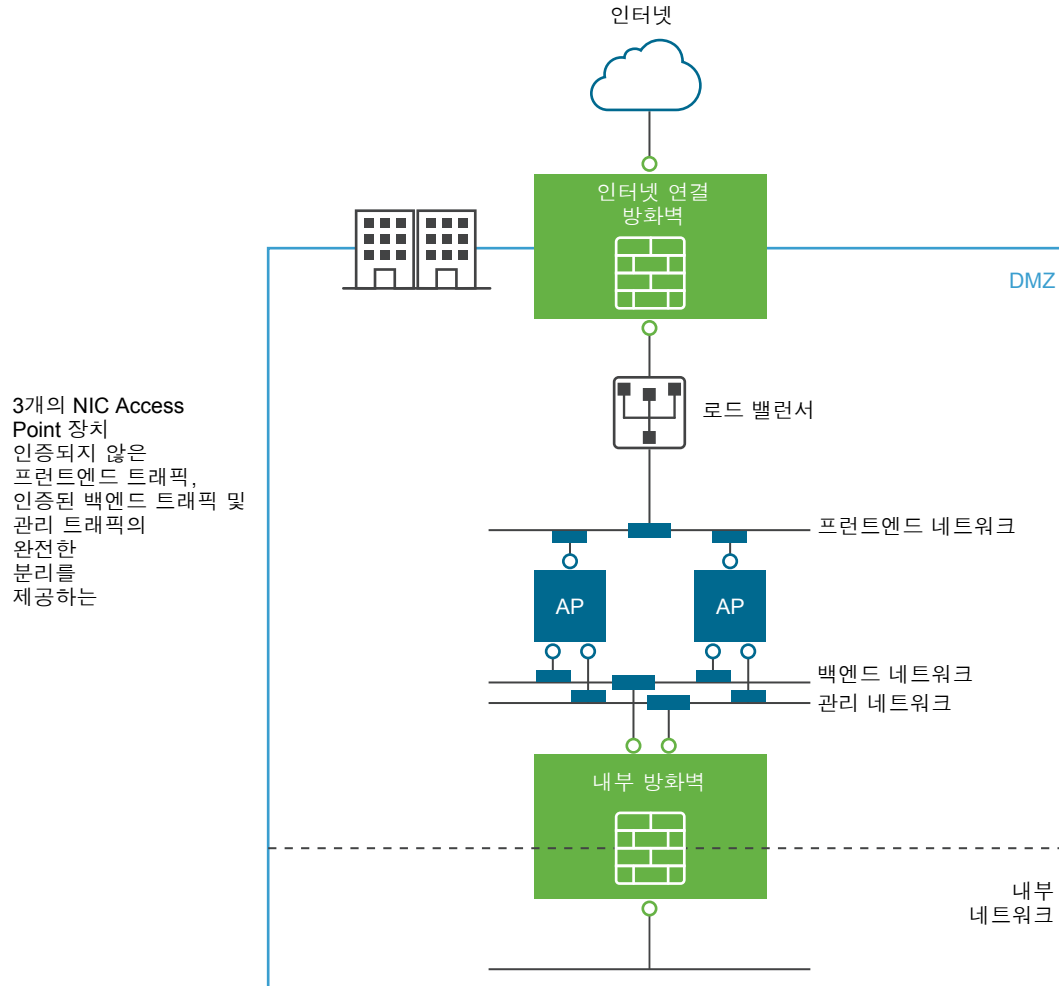
로드 밸런서와 같은 인증되지 않은 프런트엔드 네트워크의 디바이스가 손상된 경우 이러한 두 NIC 배포에서는 Access Point를 우회하도록 디바이스를 다시 구성할 수 없습니다. 계층 4 방화벽 규칙이 계층 7 Access Point 보안과 결합됩니다. 마찬가지로 인터넷 연결 방화벽이 TCP 포트 9443을 허용하도록 잘못 구성되면 Access Point 관리 REST API가 인터넷 사용자에게 노출되지 않습니다. 심층 방어 원리는 단일 구성 오류 또는 시스템 공격이 있을 때 반드시 전체적으로 취약성이 발생하는 것은 아니라는 점을 인식하는 것과 같은 여러 보호 수준을 사용합니다.

두 NIC 배포에서는 DNS 서버, RSA SecurID 인증 관리자 서버와 같은 추가 인프라 시스템을 DMZ 내의 백엔드 네트워크에 추가하여 인터넷 연결 네트워크에서 이러한 서버를 보지 못하도록 하는 것이 일반적입니다. 인프라 시스템을 DMZ 내에 배치하면 손상된 프런트엔드 시스템의 인터넷 연결 LAN에서 발생하는 계층 2 공격으로부터 보호되며 전반적인 공격 영역이 효과적으로 줄어듭니다.

대부분의 Access Point 네트워크 트래픽은 Blast 및 PCoIP에 대한 디스플레이 프로토콜입니다. 단일 NIC를 사용할 경우 인터넷으로 들어오고 인터넷에서 나오는 디스플레이 프로토콜 트래픽이 백엔드 시스템으로 들어오고 백엔드 시스템에서 나오는 트래픽과 결합됩니다. 2개 이상의 NIC가 사용되면 트래픽이 프런트엔드 및 백엔드 NIC와 네트워크에서 분산됩니다. 이 경우 단일 NIC의 잠재적인 병목 현상이 감소하여 성능이 향상됩니다.

Access Point는 특정 관리 LAN에서 관리 트래픽을 분리하도록 하여 추가적인 격리를 지원합니다. 포트 9443에 대한 HTTPS 관리 트래픽은 관리 LAN에서만 가져올 수 있습니다.

그림 1-5. Access Point의 세 NIC 옵션



Access Point 장치 배포

Access Point는 OVF로 패키징되고 vSphere ESX 또는 ESXi 호스트에 미리 구성된 가상 장치로 배포됩니다.

Access Point 장치를 설치하는 데 두 가지 기본 방법을 사용할 수 있습니다.

- vSphere Client 또는 vSphere Web Client는 Access Point OVF 템플릿을 배포하는 데 사용할 수 있습니다. NIC 배포 구성, IP 주소 및 관리 인터페이스 암호를 비롯한 기본 설정을 지정하는 메시지가 표시됩니다. OVF가 배포된 후 Access Point 관리자 인터페이스에 로그인하여 Access Point 시스템 설정을 구성하고, 다중 사용 사례에서 보안 Edge 서비스를 설정하고, DMZ에서 인증을 구성합니다. [OVF 템플릿 마법사를 사용하여 Access Point 배포](#)의 내용을 참조하십시오.
- PowerShell 스크립트를 사용하여 다중 사용 사례에서 Access Point를 배포하고 보안 Edge 서비스를 설정할 수 있습니다. zip 파일을 다운로드하고, 작업 환경에 적합하게 PowerShell 스크립트를 구성하고, Access Point를 배포하는 스크립트를 실행합니다. [PowerShell을 사용하여 Access Point 장치 배포](#)의 내용을 참조하십시오.

이 장에서는 다음 주제에 대해 설명합니다.

- [OVF 템플릿 마법사를 사용하여 Access Point 배포](#)
- [관리 구성 페이지에서 Access Point 구성](#)
- [SSL 서버 서명된 인증서 업데이트](#)

OVF 템플릿 마법사를 사용하여 Access Point 배포

Access Point를 배포하려면 vSphere Client 또는 vSphere Web Client를 사용하여 OVF 템플릿을 배포하고 장치의 전원을 켜 후 설정을 구성합니다.

Access Point가 배포된 후 관리 UI(사용자 인터페이스)로 이동하여 Access Point 환경을 설정하고 DMZ에서 사용할 데스크톱 및 애플리케이션 리소스와 인증 방법을 구성합니다.

Access Point 배포 속성

OVF를 배포하는 경우 필요한 NIC(네트워크 인터페이스) 수, IP 주소를 구성하고 관리자 암호를 설정합니다. 다른 배포 속성은 Access Point 관리 페이지에서 설정할 수 있습니다.

표 2-1. 배포 옵션 Access Point

배포 속성	설명
배포 구성	Access Point 가상 시스템에서 사용할 수 있는 네트워크 인터페이스의 수를 지정합니다. 기본적으로는 이 속성이 설정되지 않으므로 한 개의 NIC(네트워크 인터페이스 컨트롤러)가 사용됩니다.
외부(인터넷 연결) IP 주소	(필수) 인터넷에서 이 가상 시스템에 액세스하는 데 사용되는 공용 IPv4 또는 IPv6 주소를 지정합니다. 참고 컴퓨터 이름은 이 인터넷 IPv4 또는 IPv6 주소의 DNS 쿼리를 통해 설정됩니다. 기본값: 없음.
관리 네트워크 IP 주소	관리 네트워크에 연결되는 인터페이스의 IP 주소를 지정합니다. 구성되지 않은 경우에는 관리 서버가 인터넷 연결 인터페이스에서 수신합니다. 기본값: 없음.
백엔드 네트워크 IP 주소	백엔드 네트워크에 연결되는 인터페이스의 IP 주소를 지정합니다. 구성되지 않은 경우에는 백엔드 시스템으로 전송되는 네트워크 트래픽이 다른 네트워크 인터페이스를 통해 라우팅됩니다. 기본값: 없음.
DNS 서버 주소	(필수) 이 가상 시스템에 대해 공백으로 구분된 하나 이상의 도메인 이름 서버 IPv4 주소를 지정합니다(예: 192.0.2.1 192.0.2.2). 최대 세 개의 서버를 지정할 수 있습니다. 기본적으로 이 속성은 설정되지 않으므로 시스템에서는 인터넷 연결 NIC와 연결된 DNS 서버를 사용합니다. 주의 이 옵션을 비워 둔 상태에서 인터넷 연결 NIC와 연결된 DNS 서버가 없는 경우에는 장치가 올바르게 배포되지 않습니다.
루트 사용자 암호	(필수) 이 가상 시스템의 루트 사용자 암호를 지정합니다. 암호는 유효한 Linux 암호여야 합니다. 기본값: 없음.
관리자 암호	(필수) 이 암호를 설정하지 않으면 Access Point 장치에서 관리 콘솔 및 REST API에 액세스할 수 없습니다. 암호는 길이가 8자 이상이어야 하며 대문자 하나, 소문자 하나, 숫자 하나, 특수 문자를 하나 이상씩 포함해야 하고, 사용할 수 있는 특수 문자는 ! @ # \$ % * ()입니다. 기본값: 없음.

표 2-1. 배포 옵션 Access Point (계속)

배포 속성	설명
현지화된 메시지에 사용할 로케일	(필수) 오류 메시지를 생성할 때 사용할 로케일을 지정합니다. <ul style="list-style-type: none"> ■ 영어의 경우 en_US ■ 일본어의 경우 ja_JP ■ 프랑스어의 경우 fr_FR ■ 독일어의 경우 de_DE ■ 중국어 간체의 경우 zh_CN ■ 중국어 번체의 경우 zh_TW ■ 한국어의 경우 ko_KR 기본값: en_US.
Syslog 서버 URL	Access Point 이벤트 로깅에 사용되는 Syslog 서버를 지정합니다. 이 값은 URL이나 호스트 이름 또는 IP 주소일 수 있습니다. 체계와 포트 번호는 선택 사항입니다(예: syslog://server.example.com:514). 기본적으로 이 속성은 설정되지 않으므로 syslog 서버에 이벤트가 기록되지 않습니다.

OVF 템플릿 마법사를 사용하여 Access Point 배포

vCenter Server에 로그인하여 OVF 템플릿 배포 마법사를 사용하면 Access Point 장치를 배포할 수 있습니다.

참고 vSphere Web Client를 사용하여 OVF를 배포하는 경우에는 각 네트워크의 DNS 서버, 게이트웨이 및 넷마스크 주소도 지정할 수 있습니다. 기본 vSphere Client를 사용하는 경우에는 각 네트워크에 IP 풀을 할당했는지 확인합니다. 기본 vSphere Client를 사용하여 vCenter Server에 IP 풀을 추가하려면 데이터 센터의 [IP 풀] 탭으로 이동합니다. 또는 vSphere Web Client를 사용하는 경우 네트워크 프로토콜 프로파일을 생성할 수 있습니다. 데이터 센터의 [관리] 탭으로 이동하여 [네트워크 프로토콜 프로파일] 탭을 선택합니다.

필수 조건

- 마법사에서 사용할 수 있는 배포 옵션을 숙지하십시오. [Access Point 시스템 및 네트워크 요구 사항](#)의 내용을 참조하십시오.
- Access Point 장치에 대해 구성할 네트워크 인터페이스와 고정 IP 주소의 수를 결정합니다. [네트워크 구성 요구 사항](#)의 내용을 참조하십시오.
- <https://my.vmware.com/web/vmware/downloads>의 VMware 웹 사이트에서 Access Point 장치에 대한 .ova 설치 관리자 파일을 다운로드하거나, 사용할 URL을 결정합니다 (예: http://example.com/vapps/euc-access-point-Y.Y.0.0-xxxxxxx_OVF10.ova, 여기서 Y.Y는 버전 번호이고 xxxxxxx는 빌드 번호).

프로시저

- 1 기본 vSphere Client 또는 vSphere Web Client를 사용하여 vCenter Server 인스턴스에 로그인합니다.

IPv4 네트워크의 경우에는 기본 vSphere Client 또는 vSphere Web Client를 사용하고 IPv6 네트워크의 경우에는 vSphere Web Client를 사용합니다.

2 OVF 템플릿 배포 마법사를 실행하는 메뉴 명령을 선택합니다.

옵션	메뉴 명령
vSphere Client	파일 > OVF 템플릿 배포를 선택합니다.
vSphere Web Client	데이터 센터, 폴더, 클러스터, 리소스 풀 또는 호스트와 같이 가상 시스템의 유효한 상위 개체인 인벤토리 개체를 선택하고 작업 메뉴에서 OVF 템플릿 배포 를 선택합니다.

3 마법사의 소스 선택 페이지에서 다운로드한 .ova 파일의 위치로 이동하거나 URL을 입력하고 다음을 클릭합니다.

세부 정보 페이지가 표시됩니다. 제품 세부 정보, 버전 및 크기 요구 사항을 검토합니다.

4 마법사의 메시지에 따르면 다음 지침을 고려하여 마법사를 완료합니다.

옵션	설명
배포 구성 선택	IPv4 네트워크의 경우에는 1~3개의 NIC(네트워크 인터페이스)를 사용할 수 있고 IPv6 네트워크의 경우에는 3개의 NIC를 사용합니다. Access Point에서는 각 NIC별로 별도의 고정 IP 주소가 필요합니다. 많은 DMZ 구현에서 별도의 네트워크를 사용하여 서로 다른 여러 트래픽 유형을 보호합니다. 배포된 DMZ의 네트워크 설계에 따라 Access Point를 구성합니다.
디스크 포맷	평가 및 테스트 환경에서는 썸 프로비저닝 형식을 선택합니다. 운영 환경에서는 썸 프로비저닝 형식 중 하나를 선택합니다. 빠르게 비워지는 썸 프로비저닝은 Fault Tolerance와 같은 클러스터링 기능을 지원하지만 다른 유형의 가상 디스크보다 생성 시간이 오래 걸리는 썸 가상 디스크 형식 유형입니다.
VM 스토리지 정책	(vSphere Web Client에만 해당) 이 옵션은 대상 리소스에서 스토리지 정책이 사용되도록 설정된 경우에 사용할 수 있습니다.

옵션	설명
<p>네트워크/네트워크 매핑 설정</p>	<p>vSphere Web Client를 사용하는 경우에는 네트워크 설정 페이지를 통해 각 NIC를 네트워크에 매핑하고 프로토콜 설정을 지정할 수 있습니다.</p> <p>a IP 프로토콜 드롭다운 목록에서 IPv4 또는 IPv6를 선택합니다.</p> <p>b 테이블에서 첫 번째 행 Internet을 선택한 다음 아래쪽 화살표를 클릭하여 대상 네트워크를 선택합니다. IP 프로토콜로 IPv6를 선택할 경우 IPv6 기능이 있는 네트워크를 선택해야 합니다.</p> <p>행을 선택한 후에 창의 아래쪽 부분에 DNS 서버, 게이트웨이 및 넷마스크의 IP 주소를 입력할 수도 있습니다.</p> <p>c 2개 이상의 NIC를 사용하는 경우에는 다음 행 ManagementNetwork를 선택하고 대상 네트워크를 선택하면 해당 네트워크의 DNS 서버, 게이트웨이 및 넷마스크 IP 주소를 입력할 수 있습니다.</p> <p>NIC를 하나만 사용하는 경우는 모든 행이 같은 네트워크에 매핑됩니다.</p> <p>d 세 번째 NIC가 있는 경우는 세 번째 행도 선택하고 설정을 완료합니다.</p> <p>2개의 NIC만 사용하는 경우는 이 세 번째 행 BackendNetwork에서 ManagementNetwork에 사용한 것과 같은 네트워크를 선택합니다.</p> <p>vSphere Web Client에서는 마법사를 완료한 후에 네트워크 프로토콜 프로파일이 없으면 이를 자동으로 생성합니다.</p> <p>Web Client가 아닌 기본 vSphere Client를 사용하는 경우에는 네트워크 매핑 페이지를 통해 각 NIC를 네트워크에 매핑할 수 있지만 DNS 서버, 게이트웨이 및 넷마스크 주소를 지정하는 필드는 없습니다. 전제 조건에 설명된 것과 같이, 이미 각 네트워크에 IP 풀을 할당했거나 네트워크 프로토콜 프로파일을 생성했어야 합니다.</p>
<p>속성 사용자화 템플릿</p>	<p>속성 페이지의 텍스트 상자는 Access Point와 관련되어 있으며 다른 유형의 가상 장치에는 필요하지 않을 수 있습니다. 각 마법사 페이지의 텍스트에서 각 설정에 대해 설명합니다. 마법사의 오른쪽에서 텍스트가 잘린 경우에는 오른쪽 하단 모서리를 끌어서 창의 크기를 조정합니다. 다음 텍스트 상자에 값을 입력해야 합니다.</p> <ul style="list-style-type: none"> ■ IPMode:STATICV4/STATICV6. STATICV4를 입력할 경우에는 NIC에 IPv4 주소를 입력해야 하고 STATICV6를 입력할 경우에는 NIC에 IPv6 주소를 입력해야 합니다. ■ 침표로 구분된 전달 규칙 목록 형식: {tcp udp}/listening-port-number/destination-ip-address:destination-port-number ■ NIC 1(ETH0) IPv4 주소. NIC 모드에 STATICV4를 입력한 경우 NIC에 IPv4 주소를 입력합니다. ■ NIC 1(eth0)에 대한 침표로 구분된 IPv4 사용자 지정 경로 목록 형식: ipv4-network-address/bits.ipv4-gateway-address ■ IPv6 주소. NIC 모드에 STATICV6를 입력한 경우 NIC에 IPv6 주소를 입력합니다. ■ DNS 서버 주소. VM용 도메인 이름 서버의 IPv4 또는 IPv6 주소를 공백으로 구분하여 입력합니다. ■ 2개의 NIC를 지정한 경우 관리 네트워크 IP 주소, 3개의 NIC를 지정한 경우 백엔드 네트워크 IP 주소 ■ 암호 옵션. 이 VM의 루트 사용자 암호와 관리 콘솔에 액세스하고 REST API 액세스를 사용하도록 설정하는 관리자의 암호를 입력합니다. <p>다른 모든 설정은 옵션이거나 이미 기본 설정이 입력되어 있습니다. 마법사 페이지에 나열된 암호 요구 사항에 주의하십시오. 모든 배포 속성에 대한 설명은 Access Point 배포 속성을 참조하십시오.</p>

5 완료 준비 페이지에서 배포 후 전원 켜기를 선택하고 마침을 클릭합니다.

배포를 모니터링할 수 있도록 vCenter Server 상태 영역에 OVF 템플릿 배포 작업이 나타납니다. 가상 시스템에서 콘솔을 열고 시스템 부팅 중에 표시되는 콘솔 메시지를 볼 수도 있습니다. /var/log/boot.msg 파일에서도 이러한 메시지의 로그를 사용할 수 있습니다.

6 배포가 완료되면 브라우저를 열고 다음 URL을 입력하여 최종 사용자가 장치에 연결할 수 있는지 확인합니다.

```
https://FQDN-of-AP-appliance
```

이 URL에서 FQDN-of-AP-appliance는 DNS 확인이 가능하며 정규화된 Access Point 장치 도메인 이름입니다.

배포에 성공하면 Access Point가 가리키는 서버에서 제공하는 웹 페이지가 표시됩니다. 배포에 성공하지 못한 경우에는 장치 가상 시스템을 삭제하고 장치를 다시 배포할 수 있습니다. 가장 일반적인 오류는 인증서 지문을 올바르게 입력하지 않는 것입니다.

Access Point 장치가 배포되고 자동으로 시작됩니다.

후속 작업

Access Point 관리 UI(사용자 인터페이스)에 로그인하고 Access Point를 통해 인터넷에서 원격으로 액세스하도록 데스크톱 및 애플리케이션 리소스를 구성하고 DMZ에서 사용할 인증 방법을 구성합니다. 관리 콘솔 URL은 `https://<mycoAccessPointappliance.com:9443/admin/index.html` 형식입니다.

관리 구성 페이지에서 Access Point 구성

OVF를 배포하고 Access Point 장치의 전원을 켜 후에 Access Point 관리 사용자 인터페이스에 로그인하여 다음 설정을 구성합니다.

- Access Point 시스템 구성 및 SSL 서버 인증서.
- Horizon에 대한 Edge 서비스 설정, 역방향 프록시, AirWatch에 대한 애플리케이션별 Tunnel 및 프록시 설정.
- RSA SecurID, RADIUS, X.509 인증서 및 RSA 어댑티브 인증에 대한 인증 설정.
- SAML ID 제공자 및 서비스 제공자 설정.

다음 옵션은 구성 페이지에서 액세스할 수 있습니다.

- Access Point 로그 zip 파일을 다운로드합니다.
- 구성 설정을 검색하려면 Access Point 설정을 내보냅니다.
- 전체 Access Point 구성을 생성 및 업데이트하려면 Access Point 설정을 가져옵니다.

Access Point 시스템 설정 구성

관리 구성 페이지에서 클라이언트와 Access Point 장치 간의 통신을 암호화하는 데 사용되는 보안 프로토콜 및 암호화 알고리즘을 구성할 수 있습니다.

Access Point 관리자 인터페이스 URL은 `https://<mycoAccessPointappliance.com>:9443/admin/index.html` 형식입니다. 로그인하려면 OVF를 배포할 때 구성한 관리자 이름 및 암호를 입력합니다.

필수 조건

- Access Point 배포 속성을 검토합니다. 다음 설정 정보가 필요합니다.
 - Access Point 장치에 대한 정적 IP 주소
 - DNS 서버의 IP 주소
 - 관리 콘솔의 암호
 - Access Point 장치가 가리키는 서버 인스턴스 또는 로드 밸런서의 URL
 - 이벤트 로그 파일을 저장할 Syslog 서버 URL

프로시저

- 1 [관리 UI 수동 구성] 섹션에서 **선택**을 클릭합니다.
- 2 [고급 설정] 섹션에서 **시스템 구성** 톱니 모양 아이콘을 클릭합니다.
- 3 다음 Access Point 장치 구성 값을 편집합니다.

옵션	기본값 및 설명
로케일	오류 메시지를 생성할 때 사용할 로케일을 지정합니다. <ul style="list-style-type: none"> ■ 영어의 경우 en_US ■ 일본어의 경우 ja_JP ■ 프랑스어의 경우 fr_FR ■ 독일어의 경우 de_DE ■ 중국어 간체의 경우 zh_CN ■ 중국어 번체의 경우 zh_TW ■ 한국어의 경우 ko_KR
관리자 암호	이 암호는 장치를 배포할 때 설정한 것입니다. 암호를 다시 설정할 수 있습니다. 암호는 길이가 8자 이상이어야 하며 대문자 하나, 소문자 하나, 숫자 하나, 특수 문자를 하나 이상씩 포함해야 하고, 사용할 수 있는 특수 문자는 ! @ # \$ % * ()입니다.
암호 제품군	대부분의 경우 기본 설정을 변경할 필요가 없습니다. 이는 클라이언트와 Access Point 장치 간의 통신을 암호화하는 데 사용되는 암호화 알고리즘입니다. 암호 설정은 다양한 보안 프로토콜을 사용하도록 설정하는 데 사용됩니다.
암호 순서 허용	기본값은 [아니오]입니다. TLS 암호 목록 순서 제어를 사용하도록 설정하려면 예 를 선택합니다.
SSL 3.0 사용	기본값은 [아니오]입니다. SSL 3.0 보안 프로토콜을 사용하도록 설정하려면 예 를 선택합니다.

옵션	기본값 및 설명
TLS 1.0 사용	기본값은 [아니요]입니다. TLS 1.0 보안 프로토콜을 사용하도록 설정하려면 예를 선택합니다.
TLS 1.1 사용	기본값은 [예]입니다. TLS 1.1 보안 프로토콜이 사용되도록 설정됩니다.
TLS 1.2 사용	기본값은 [예]입니다. TLS 1.2 보안 프로토콜이 사용되도록 설정됩니다.
Syslog URL	Access Point 이벤트를 로깅하는 데 사용되는 Syslog 서버 URL을 입력합니다. 이 값은 URL이나 호스트 이름 또는 IP 주소일 수 있습니다. Syslog 서버 URL을 설정하지 않으면 이벤트가 로깅되지 않습니다. syslog://server.example.com:514로 입력합니다.
상태 점검 URL	로드 밸런서에서 연결하여 Access Point의 상태를 확인하는 URL을 입력합니다.
캐시할 쿠키	Access Point에서 캐시하는 쿠키 집합입니다. 기본값은 [없음]입니다.
IP 모드	STATICV4 또는 STATICV6 중에서 정적 IP 모드를 선택합니다.
세션 시간 초과	기본값은 36000000밀리초입니다.
중지 모드	Access Point 장치를 일시 중지하여 일관된 상태에서 유지 보수 작업을 수행하도록 하려면 예로 설정합니다.
모니터 간격	기본값은 60입니다.

4 저장을 클릭합니다.

후속 작업

Access Point와 함께 배포된 구성 요소에 대한 Edge 서비스 설정을 구성합니다. Edge 설정이 구성된 후에 인증 설정을 구성합니다.

SSL 서버 서명된 인증서 업데이트

서명된 인증서가 만료되면 이를 교체할 수 있습니다.

VMware는 운영 환경에서 가능한 한 빨리 기본 인증서를 교체할 것을 권장합니다. Access Point 장치를 배포할 때 생성되는 기본 TLS/SSL 서버 인증서는 신뢰할 수 있는 CA(인증 기관)에서 서명되지 않았습니다.

필수 조건

- 액세스할 수 있는 컴퓨터에 저장된 새로 서명된 인증서 및 개인 키
- 인증서를 PEM 형식 파일로 변환하고 .pem 파일을 한 줄 형식으로 변환합니다. "인증서 파일을 한 줄 PEM 형식으로 변환"을 참조하십시오.

프로시저

- 1 관리 콘솔에서 **선택**을 클릭합니다.
- 2 [고급 설정] 섹션에서 SSL 서버 인증서 설정 톱니 모양 아이콘을 클릭합니다.
- 3 [개인 키] 행에서 **선택**을 클릭하고 개인 키 파일로 이동합니다.
- 4 **열기**를 클릭하여 파일을 업로드합니다.
- 5 [인증서 체인] 행에서 [선택]을 클릭하고 인증서 체인 파일로 이동합니다.

6 열기를 클릭하여 파일을 업로드합니다.

7 저장을 클릭합니다.

후속 작업

인증서에 서명한 CA가 잘 알려져 있지 않다면 루트 및 중간 인증서를 신뢰하도록 클라이언트를 구성하십시오.

PowerShell을 사용하여 Access Point 배포

3

PowerShell 스크립트는 Access Point를 배포하는 데 사용될 수 있습니다. PowerShell 스크립트는 환경별 요구에 맞게 조정할 수 있는 샘플 스크립트로 전달됩니다.

PowerShell 스크립트를 사용하여 Access Point를 배포할 경우 스크립트는 OVF Tool 명령을 호출하고 설정의 유효성을 검사하여 올바른 명령줄 구문을 자동으로 구성합니다. 이 방법을 사용하면 배포 시에 TLS/SSL 서버 인증서 구성과 같은 고급 설정을 이용할 수도 있습니다.

이 장에서는 다음 주제에 대해 설명합니다.

- PowerShell을 사용하여 Access Point를 배포하기 위한 시스템 요구 사항
- PowerShell을 사용하여 Access Point 장치 배포

PowerShell을 사용하여 Access Point를 배포하기 위한 시스템 요구 사항

PowerShell 스크립트를 사용하여 Access Point를 배포하려면 특정 버전의 VMware 제품을 사용해야 합니다.

- vCenter Server가 있는 vSphere ESX 호스트.
- PowerShell 스크립트는 Windows 8.1 이상 시스템 또는 Windows Server 2008 R2 이상에서 실행됩니다.
또한 시스템은 Windows에서 실행되는 vCenter Server 또는 별도의 Windows 시스템일 수 있습니다.
- 이 스크립트가 실행되는 Windows 시스템에는 VMware OVF Tool 명령이 설치되어 있어야 합니다.

<https://www.vmware.com/support/developer/ovf/>에서 OVF Tool 4.0.1 이상을 설치해야 합니다.

사용할 vSphere 데이터스토어 및 네트워크를 선택해야 합니다.

vSphere 네트워크 프로토콜 프로파일이 참조된 모든 네트워크 이름에 연결되어 있어야 합니다. 이 네트워크 프로토콜 프로파일은 IPv4 서브넷 마스크, 게이트웨이 등과 같은 네트워크 설정을 지정합니다. Access Point의 배포에서는 이러한 값을 사용하여 값을 올바르게 유지합니다.

PowerShell을 사용하여 Access Point 장치 배포

PowerShell 스크립트는 모든 구성 설정을 사용하여 환경을 준비합니다. PowerShell 스크립트를 실행하여 Access Point를 배포할 경우 첫 번째 시스템 부팅 시 솔루션의 프로덕션 사용 준비가 완료됩니다.

필수 조건

- 시스템 요구 사항이 적절한지와 사용 가능한지 확인합니다.

다음은 사용자 환경에 Access Point를 배포하기 위한 샘플 스크립트입니다.

그림 3-1. 샘플 PowerShell 스크립트

```

Windows PowerShell
Copyright (C) 2014 Microsoft Corporation. All rights reserved.

PS C:\Users\mark> .\apdeploy.ps1 -inifile ap1.ini
Access Point virtual appliance deployment script
Deployment will use the specified SSL/TLS server certificate
Enter a root password for AP1: *****
Re-enter the root password: *****
Enter an optional admin password for the REST API management access for AP1: *****
Re-enter the admin password: *****
Opening OVA source: C:\Users\mark\Downloads\VMware\Access Point\apc-access-point-2.0.0-2939373_00F10.ova
The manifest validates
Source is signed and the certificate validates
Enter login information for target vi://192.168.0.21/
Username: administrator@40vsphere.local
Password: *****
Opening UI target: vi://administrator@40vsphere.local@192.168.0.21:443/Datacenter1/host/h1.oc.vmware.com
Deleting VM: AP1
Deploying to UI: vi://administrator@40vsphere.local@192.168.0.21:443/Datacenter1/host/h1.oc.vmware.com
Transfer Completed
Powering on VM: AP1
Task Completed
Received IP address: 192.168.0.130
Completed successfully
Note that the IP addresses will be set to the specified IP addresses for each NIC
Access Point virtual appliance AP1 deployed successfully
PS C:\Users\mark>
    
```

프로시저

- 1 [My VMware]에서 Windows 시스템으로 Access Point OVA를 다운로드합니다.
- 2 ap-deploy-XXX.zip 파일을 Windows 시스템의 폴더로 다운로드합니다.

이 zip 파일은 <https://communities.vmware.com/docs/DOC-30835>에서 다운로드할 수 있습니다.

- 3 PowerShell 스크립트를 열고 디렉토리를 스크립트의 위치로 수정합니다.
- 4 Access Point 가상 장치에 대한 .INI 구성 파일을 생성합니다.

예: 새 Access Point 장치 AP1를 배포합니다. 구성 파일 이름은 ap1.ini입니다. 이 파일에는 AP1에 대한 모든 구성 설정이 포함됩니다. apdeploy .ZIP 파일의 샘플 .INI 파일을 사용하여 .INI 파일을 생성하고 설정을 적절히 수정할 수 있습니다.

참고 환경의 여러 Access Point 배포에 대해 고유한 INI 파일이 있을 수 있습니다. 여러 장치를 배포하려면 .INI 파일의 IP 주소 및 이름 매개 변수를 적절히 변경해야 합니다.

수정할 .INI 파일 예.

```
name=AP1
source=C:\WAPs\weuc-access-point-2.8.0.0-000000000_0VF10.ova
target=vi://administrator@vsphere.local:PASSWORD@192.168.0.21/Datacenter1/host/esx1.myco.int
ds=Local Disk 1
netInternet=VM Network
netManagementNetwork=VM Network
netBackendNetwork=VM Network

[Horizon/WebReverseProxy/AirwatchTunnel]
proxyDestinationUrl=https://192.168.0.209

# For IPv4, proxydestinationURL=https://192.168.0.209
# For IPv6, proxyDEstinationUrI=[fc00:10:112:54::220]
```

- 5 스크립트를 성공적으로 실행하려면 PowerShell set-executionpolicy 명령을 입력합니다.

```
set-executionpolicy -scope currentuser unrestricted
```

이 명령은 현재 제한된 경우에만 한 번 실행해야 합니다.

스크립트에 대한 경고가 표시되면 다음 명령을 실행하여 주의를 차단 해제합니다.

```
unblock-file -path .\Wapdeploy.ps1
```

- 6 이 명령을 실행하여 배포를 시작합니다. .INI 파일을 지정하지 않으면 스크립트는 기본적으로 ap.ini가 됩니다.

```
.\Wapdeploy.ps1 -iniFile ap1.ini
```

- 7 자격 증명을 입력하라는 메시지가 표시되면 입력하고 스크립트를 완료합니다.

참고 대상 시스템에 대한 지문을 추가하라는 메시지가 표시되면 **yes**를 입력합니다.

Access Point 장치가 배포되고 프로덕션용으로 사용 가능합니다.

PowerShell 스크립트에 대한 자세한 내용은

<https://communities.vmware.com/docs/DOC-30835>를 참조하십시오.

배포 사용 사례

이 장에 설명된 배포 시나리오는 작업 환경에서 Access Point 배포를 식별하고 구성하는 데 도움이 될 수 있습니다.

Horizon View, Horizon Air Hybrid-Mode, VMware Identity Manager 및 VMware AirWatch를 사용하여 Access Point를 배포할 수 있습니다.

이 장에서는 다음 주제에 대해 설명합니다.

- [Horizon View 및 Horizon Air Hybrid-Mode를 사용하여 Access Point 배포](#)
- [역방향 프록시로 Access Point 배포](#)
- [AirWatch Tunnel을 사용한 Access Point 배포](#)

Horizon View 및 Horizon Air Hybrid-Mode를 사용하여 Access Point 배포

Horizon View 및 Horizon Air Hybrid-Mode를 사용하여 Access Point를 배포할 수 있습니다. VMware Horizon의 View 구성 요소에서, Access Point 장치는 이전의 View 보안 서버와 동일한 역할을 수행합니다.

배포 시나리오

Access Point에서는 고객 데이터 센터의 온-프레미스 가상 데스크톱 및 애플리케이션에 대한 보안 원격 액세스를 제공합니다. 이 기능은 통합 관리를 위해 Horizon View 또는 Horizon Air Hybrid-Mode 온-프레미스 배포에서 작동합니다.

Access Point를 사용하면 기업에서는 사용자 ID를 명확히 확인하고 사용 권한이 있는 데스크톱 및 애플리케이션에 대한 액세스를 정밀하게 제어할 수 있습니다.

Access Point 가상 장치는 일반적으로 네트워크 DMZ(예외 구역)에 배포됩니다. DMZ에 배포하면 강력하게 인증된 사용자에 대한 트래픽만 데스크톱 및 애플리케이션 리소스에 대한 데이터 센터로 들어 갑니다. Access Point 가상 장치는 인증된 사용자에 대한 트래픽이 사용자에게 사용 권한이 부여된 데스크톱 및 애플리케이션 리소스로만 전송될 수 있도록 합니다. 이러한 수준의 보호에는 액세스를 정확히 제어하기 위해 데스크톱 프로토콜의 특정 조사 기능 및 빨리 바뀔 수 있는 정책 및 네트워크 주소 조정 기능이 포함됩니다.

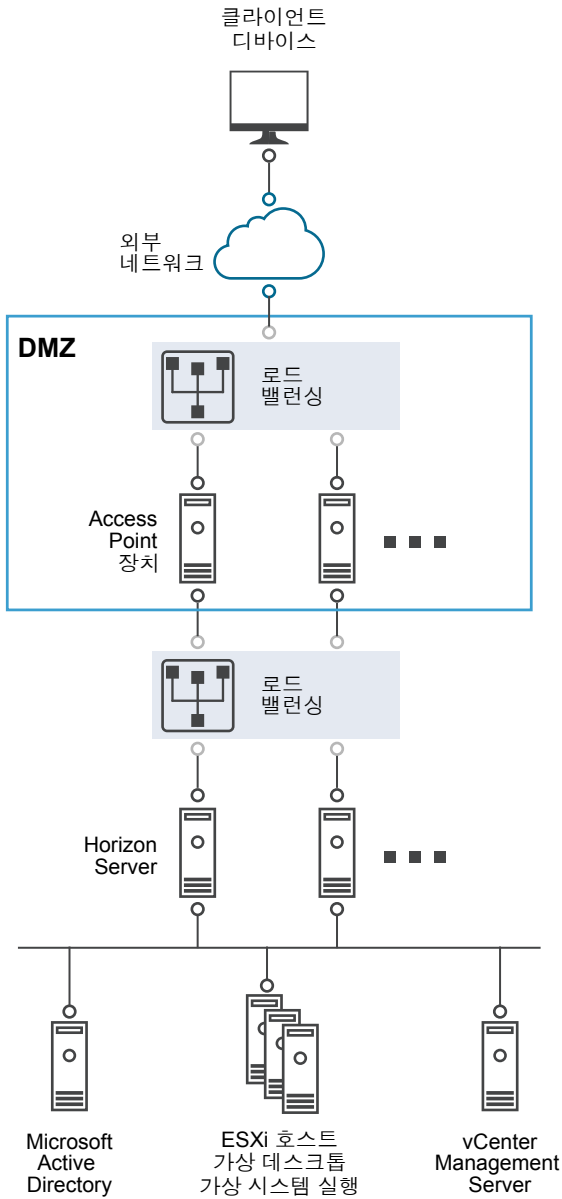
Horizon을 사용하여 원활하게 Access Point 배포를 수행하기 위한 요구 사항을 확인해야 합니다.

- Access Point 장치는 Horizon server 앞의 로드 밸런서를 가리키며 서버 인스턴스의 선택이 동적으로 이루어집니다.
- Access Point는 Horizon 보안 서버를 대신합니다.
- Blast TCP/UDP에 대해 포트 443을 사용할 수 있어야 합니다.
- Horizon을 사용하여 Access Point를 배포할 때는 Blast 보안 게이트웨이 및 PCoIP 보안 게이트웨이를 사용하도록 설정해야 합니다. 디스플레이 프로토콜은 Access Point를 통해 자동으로 프록시로 사용될 수 있습니다. BlastExternalURL 및 pcoipExternalURL 설정은 Horizon Client에서 Access Point의 해당 게이트웨이를 통해 이러한 디스플레이 프로토콜 연결을 라우팅하는 데 사용되는 연결 주소를 지정합니다. 이러한 게이트웨이는 인증된 사용자 대신 디스플레이 프로토콜 트래픽을 제어하여 보안이 향상됩니다. 허가되지 않은 디스플레이 프로토콜 트래픽은 Access Point에서 무시됩니다.
- View 연결 서버 인스턴스에서 보안 게이트웨이를 사용하지 않도록 설정하고 Access Point 장치에서 이러한 게이트웨이를 사용하도록 설정합니다.

View 보안 서버와의 주요 차이점은 Access Point가 다음과 같다는 점입니다.

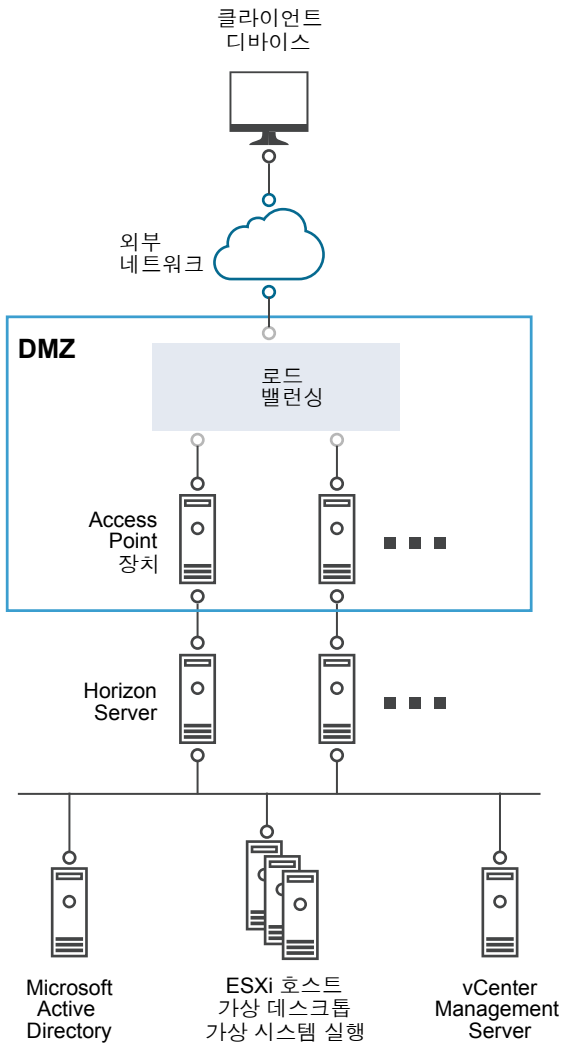
- 보안 배포입니다. Access Point는 보안이 강화되고 잠겨 있고 미리 구성된 Linux 기반 가상 시스템으로 구현됩니다.
- 확장 가능합니다. Access Point를 개별 View 연결 서버에 연결하거나 여러 View 연결 서버 앞의 로드 밸런서를 통해 연결하여 고가용성을 크게 향상시킬 수 있습니다. Horizon Client와 백엔드 View 연결 서버 간의 계층으로 작동합니다. 신속하게 배포되므로 빠르게 변화하는 엔터프라이즈의 요구를 충족하도록 빠르게 확장 또는 축소할 수 있습니다.

그림 4-1. Access Point 장치가 로드 밸런서를 가리킴



또는 하나 이상의 Access Point 장치가 개별 서버 인스턴스를 가리키도록 할 수 있습니다. 두 가지 방법 모두 DMZ에서 두 개 이상의 Access Point 장치 앞에 있는 로드 밸런서를 사용합니다.

그림 4-2. Access Point 장치가 Horizon Server 인스턴스를 가리킴



인증

사용자 인증은 View 보안 서버와 매우 유사합니다. Access Point의 지원되는 사용자 인증 방법에는 다음이 포함됩니다.

- Active Directory 사용자 이름 및 암호
- 키오스크 모드. 키오스크 모드에 대한 자세한 내용은 Horizon 설명서를 참조하십시오.
- SecurID용 RSA에 의해 공식적으로 인증되는 RSA SecurID 2단계 인증
- 다양한 타사의 2 요소 보안 벤더 솔루션을 통한 RADIUS
- 스마트 카드, CAC 또는 PIV X.509 사용자 인증
- SAML

이러한 인증 방법은 View 연결 서버와 함께 지원됩니다. Access Point는 Active Directory와 직접 통신하지 않아도 됩니다. 이러한 통신은 Active Directory에 직접 액세스할 수 있는 View 연결 서버를 통해 프록시로 작동합니다. 사용자 세션이 인증 정책에 따라 인증된 후에 Access Point는 사용 권한 정보에 대한 요청, 데스크톱 및 애플리케이션 실행 요청을 View 연결 서버로 전달할 수 있습니다. 또한 Access Point는 해당 데스크톱 및 애플리케이션 프로토콜 처리기를 관리하여 허가된 프로토콜 트래픽만 전달할 수 있도록 합니다.

Access Point는 스마트 카드 인증 자체를 처리합니다. 여기에는 Access Point에서 OCSP(온라인 인증서 상태 프로토콜) 서버와 통신하여 X.509 인증서 해지 등을 확인할 수 있는 옵션이 포함됩니다.

Horizon 설정 구성

Horizon View 및 Horizon Air Hybrid-Mode에서 Access Point를 배포할 수 있습니다. VMware Horizon의 View 구성 요소의 경우 Access Point 장치는 이전의 View 보안 서버와 동일한 역할을 수행합니다.

프로시저

- 1 [관리 UI 수동 구성] 섹션에서 **선택**을 클릭합니다.
- 2 [일반 설정] > [Edge 서비스 설정] 줄에서 **표시**를 클릭합니다.
- 3 **Horizon 설정** 톱니 모양 아이콘을 클릭합니다.
- 4 Horizon을 사용하도록 설정하려면 [Horizon 설정] 페이지에서 [아니요]를 **예**로 변경합니다.
- 5 Horizon에 대해 다음 Edge 서비스 설정 리소스를 구성합니다.

옵션	설명
식별자	기본적으로 View로 설정됩니다. Access Point는 View 연결 서버, Horizon Air, Horizon Air Hybrid-Mode와 같이 View XML 프로토콜을 사용하는 서버와 통신할 수 있습니다.
연결 서버 URL	Horizon Server 또는 로드 밸런서의 주소를 입력합니다. https://00.00.00.00으로 입력합니다.
프록시 대상 URL 지문	Horizon Server 지문 목록을 입력합니다. 지문 목록을 제공하지 않은 경우에는 신뢰할 수 있는 CA에서 서버 인증서를 발급해야 합니다. 16진수 지문 숫자를 입력합니다. 예를 들어 sha=C3 89 A2 19 DC 7A 48 2B 85 1C 81 EC 5E 8F 6A 3C 33 F2 95 C3과 같습니다.

6 인증 방법 규칙 및 기타 고급 설정을 구성하려면 **자세히**를 클릭합니다.

옵션	설명
인증 방법	<p>사용할 인증 방법을 선택합니다.</p> <p>기본값은 사용자 이름 및 암호의 패스스루 인증을 사용하는 것입니다. Access Point에서 구성한 인증 방법은 드롭다운 메뉴에 표시됩니다.</p> <p>첫 번째 인증 시도가 실패하는 경우 두 번째 인증 방법을 사용하는 인증을 구성하려면 다음을 수행합니다.</p> <ul style="list-style-type: none"> a 첫 번째 드롭다운 메뉴에서 인증 방법을 하나 선택합니다. b +를 클릭하고 [AND] 또는 [OR]를 선택합니다. c 세 번째 드롭다운 메뉴에서 두 번째 인증 방법을 선택합니다. <p>사용자가 2가지 인증 방법을 통해 인증을 받도록 하려면 드롭다운에서 [OR]를 [AND]로 변경합니다.</p>
상태 점검 URL	로드 밸런서가 구성된 경우 로드 밸런서가 연결 및 Access Point 장치의 상태를 확인하는 데 사용하는 URL을 입력합니다.
SAML SP	View XMLAPI 브로커에 대한 SAML 서비스 제공자의 이름을 입력합니다. 이 이름은 구성된 서비스 제공자 메타데이터의 이름과 일치하거나 특수 값 [DEMO]여야 합니다.
PCoIP 사용	PCoIP 보안 게이트웨이를 사용하도록 설정하려면 [아니요]를 예 로 변경합니다.
프록시 외부 URL	Access Point 장치의 외부 URL을 입력합니다. 클라이언트는 PCoIP 보안 게이트웨이를 통한 보안 연결에 이 URL을 사용합니다. 이 연결은 PCoIP 트래픽에 사용됩니다. 기본값은 Access Point IP 주소 및 포트 4172입니다.
스마트 카드 힌트 프롬프트	스마트 카드 사용자 이름 힌트 기능을 지원하도록 Access Point 장치를 설정하려면 [아니요]를 예 로 변경합니다. 스마트 카드 힌트 기능을 사용하여 사용자의 스마트 카드 인증서를 여러 Active Directory 도메인 사용자 계정에 매핑할 수 있습니다.
Blast 사용	Blast 보안 게이트웨이를 사용하려면 [아니요]를 예 로 변경합니다.
Blast 외부 URL	최종 사용자가 Blast 보안 게이트웨이를 통해 웹 브라우저에서 보안 연결을 설정하는 데 사용하는 Access Point 장치의 FQDN URL을 입력합니다. https://exampleappliance:443 으로 입력합니다.
터널 사용	View 보안 터널이 사용되는 경우 [아니요]를 예 로 변경합니다. 클라이언트는 View 보안 게이트웨이를 통한 터널 연결을 위해 외부 URL을 사용합니다. 터널은 RDP, USB 및 MMR(멀티미디어 리디렉션) 트래픽에 사용됩니다.
터널 외부 URL	Access Point 장치의 외부 URL을 입력합니다. 설정하지 않으면 Access Point 기본값이 사용됩니다.
Windows 사용자 이름 일치	RSA SecurID 및 Windows 사용자 이름을 일치시키려면 [아니요]를 예 로 변경합니다. [예]로 설정하면 securID-auth가 [true]로 설정되고 securID 및 Windows 사용자 이름 일치가 적용됩니다.
게이트웨이 위치	요청이 시작된 위치를 사용하도록 설정하려면 [아니요]를 예 로 변경합니다. 보안 서버 및 Access Point는 게이트웨이 위치를 설정합니다. 위치는 외부 또는 내부일 수 있습니다.
Windows SSO 사용	RADIUS 인증을 사용하도록 설정하려면 [아니요]를 예 로 변경합니다. Windows 로그인에서 처음으로 RADIUS 액세스 요청에 성공한 자격 증명을 사용합니다.

7 **저장**을 클릭합니다.

역방향 프록시로 Access Point 배포

Access Point는 Web Reverse Proxy로 사용될 수 있으며 DMZ에서 일반 역방향 프록시 또는 인증 역방향 프록시로 작동할 수 있습니다.

배포 시나리오

Access Point는 VMware Identity Manager의 온-프레미스 배포에 대한 보안 원격 액세스를 제공합니다. Access Point 장치는 일반적으로 네트워크 DMZ(예외 구역)에 배포됩니다.

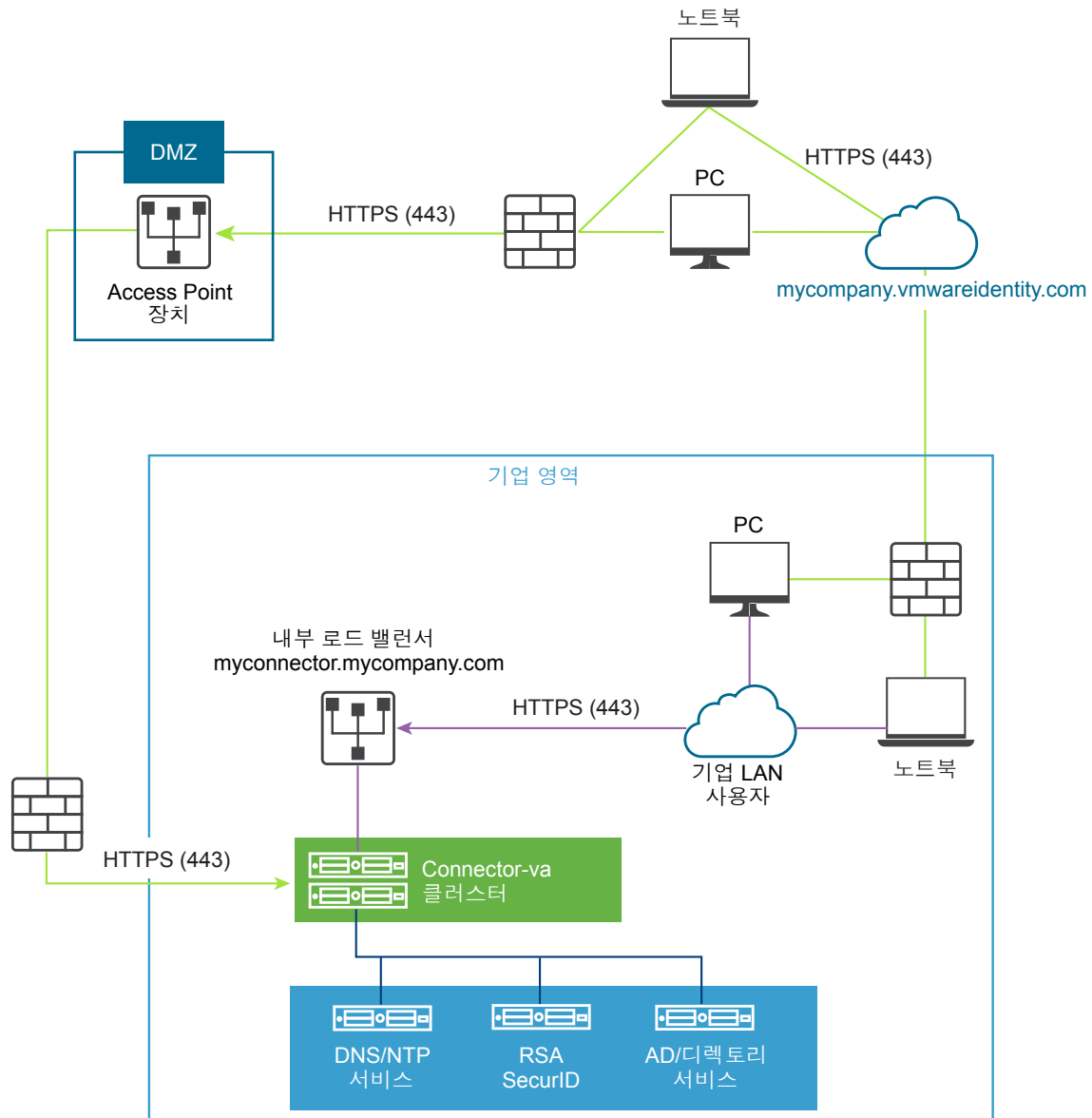
VMware Identity Manager를 사용할 경우 Access Point 장치는 사용자의 브라우저와 데이터 센터의 VMware Identity Manager 서비스 간에 Web Reverse Proxy로 작동합니다. 또한 Access Point를 사용하면 VMware Identity Manager 카탈로그에 원격으로 액세스하여 Horizon 애플리케이션을 실행할 수 있습니다.

VMware Identity Manager를 사용한 Access Point 배포의 요구 사항

- 분할 DNS
- VMware Identity Manager 장치는 호스트 이름으로 FQDN(정규화된 도메인 이름)을 갖고 있어야 합니다.

- Access Point가 내부 DNS를 사용해야 합니다. 이는 proxyDestinationURL이 FQDN을 사용해야 함을 의미합니다.

그림 4-3. 커넥터를 가리키는 Access Point 장치



역방향 프록시의 이해

솔루션으로 사용되는 Access Point는 원격 사용자가 앱 포털에 액세스하여 Single Sign-On을 수행하고 리소스에 액세스할 수 있도록 합니다. Edge Service Manager에서 인증 역방향 프록시를 사용하도록 설정합니다. 현재 RSA SecurID 및 RADIUS 인증 방법이 지원됩니다.

참고 Web Reverse Proxy에서 인증을 사용하도록 설정하기 전에 ID 제공자 메타데이터를 생성해야 합니다.

Access Point는 브라우저 기반 클라이언트의 인증이 있거나 없는 상태로 VMware Identity Manager 및 웹 애플리케이션에 원격으로 액세스할 수 있도록 하고 Horizon 데스크톱을 실행합니다.

- 브라우저 기반 클라이언트는 인증 방법으로 RADIUS 및 RSA SecurID를 사용하도록 지원합니다.

Access Point 2.8 릴리스에서는 역방향 프록시 지원이 VMware Identity Manager 및 내부 웹 리소스(예: Confluence 및 WIKI)로 제한됩니다. 앞으로 이러한 리소스 목록이 확장될 예정입니다.

참고 authCookie 및 unSecurePattern 속성은 인증 역방향 프록시에 유효하지 않습니다. authMethods 속성을 사용하여 인증 방법을 정의해야 합니다.

VMware Identity Manager용 역방향 프록시 구성

Web Reverse Proxy 서비스에서 Access Point를 VMware Identity Manager와 함께 사용하도록 구성할 수 있습니다.

필수 조건

VMware Identity Manager를 포함하는 Access Point 배포에 대한 요구 사항

- 분할 DNS
- VMware Identity Manager 서비스는 호스트 이름으로 FQDN(정규화된 도메인 이름)을 갖고 있어야 합니다.
- Access Point가 내부 DNS를 사용해야 합니다. 즉, proxyDestination URL이 FQDN을 사용해야 합니다.

프로시저

- 1 [관리 UI 수동 구성] 섹션에서 **선택**을 클릭합니다.
- 2 [일반 설정] > [Edge 서비스 설정] 줄에서 **표시**를 클릭합니다.
- 3 **역방향 프록시 설정** 톱니 모양 아이콘을 클릭합니다.
- 4 역방향 프록시를 사용하도록 설정하려면 [역방향 프록시 설정] 페이지에서 [아니오]를 **예**로 변경합니다.
- 5 Horizon에 대해 다음 Edge 서비스 설정 리소스를 구성합니다.

옵션	설명
식별자	Edge 서비스 식별자는 WEB_REVERSE_PROXY로 설정됩니다.
프록시 대상 URL	VMware Identity Manager 서버의 주소를 입력합니다. 예를 들어 https://vmwareidentitymgr.example.com 으로 입력합니다.

옵션	설명
프록시 대상 URL 지문	proxyDestination URL에 대해 허용 가능한 SSL 서버 인증서 지문 목록을 입력합니다. 와일드카드 *를 포함하면 모든 인증서가 허용됩니다. 지문은 [alg=]xx:xx 형식입니다. 여기서 alg는 sha1, 기본값 또는 md5일 수 있습니다. 'xx'는 16진수입니다. 예를 들어 sha=C3 89 A2 19 DC 7A 48 2B 85 1C 81 EC 5E 8F 6A 3C 33 F2 95 C3과 같습니다. 지문을 구성하지 않은 경우에는 신뢰할 수 있는 CA에서 서버 인증서를 발급해야 합니다.
프록시 패턴	대상 URL로 전달되는 일치하는 URI 경로를 입력합니다. 예를 들어 (//SAAS(.*) hc(.*) web(.*) catalog-portal(.*))로 입력합니다.

6 기타 고급 설정을 구성하려면 **자세히**를 클릭합니다.

옵션	설명
인증 방법	기본값은 사용자 이름 및 암호의 패스스루 인증을 사용하는 것입니다. Access Point에서 구성한 인증 방법은 드롭다운 메뉴에 표시됩니다. Access Point에서 구성한 인증 방법은 드롭다운 메뉴에 표시됩니다.
상태 점검 URL	로드 밸런서가 구성된 경우 로드 밸런서가 연결 및 Access Point 장치의 상태를 확인하는 데 사용하는 URL을 입력합니다.
SAML SP	View XML API 브로커에 대한 SAML 서비스 제공자의 이름을 입력합니다. 이 이름은 구성된 서비스 제공자 메타데이터의 이름과 일치하거나 특수 값 DEMO여야 합니다.
활성화 코드	VMware Identity Manager 및 Access Point 간에 신뢰를 설정하기 위해 VMware Identity Manager 서비스가 생성하고 Access Point로 가져온 코드를 입력합니다.
외부 URL	기본값은 Access Point 호스트 URL, 포트 443입니다. 다른 외부 URL을 입력할 수 있습니다. https://<host:port>.로 입력합니다.

7 **저장**을 클릭합니다.

AirWatch Tunnel을 사용한 Access Point 배포

Access Point 장치는 DMZ에 배포됩니다. 배포 중에는 Access Point 구성 요소와 AirWatch 구성 요소(예: 에이전트 및 터널 프록시 서비스)가 설치됩니다.

AirWatch 환경에서 AirWatch Tunnel을 배포하는 과정에는 초기 하드웨어 설정, AirWatch 관리 콘솔에서 서버 정보 및 애플리케이션 설정 구성, 설치 관리자 다운로드 및 AirWatch Tunnel 서버에서 설치 관리자 실행이 포함됩니다.

OVF 설치가 완료되고 값이 변경되면 각 Edge 서비스를 수동으로 구성할 수 있습니다.

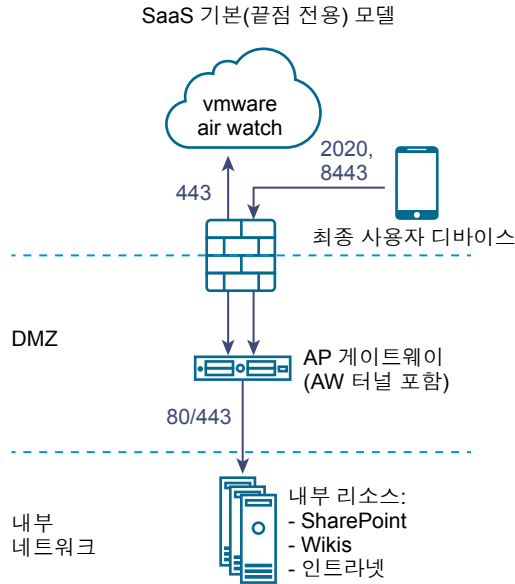
AirWatch를 사용한 Access Point 배포에 대한 자세한 내용은 <https://resources.airwatch.com/view/vb7zp7wwhpw756m2pfx> 를 참조하십시오.

AirWatch에 대한 터널 프록시 배포

터널 프록시 배포는 AirWatch에서 VMware 브라우저 모바일 애플리케이션을 통해 최종 사용자 디바이스와 웹 사이트 간 네트워크 트래픽의 보안을 유지합니다.

모바일 애플리케이션은 터널 프록시 서버와의 보안 HTTPS 연결을 생성하고 중요한 데이터를 보호합니다. AirWatch Tunnel 프록시에서 내부 애플리케이션을 사용하려면 AirWatch SDK를 애플리케이션에 내장하여 이 구성 요소의 터널링 기능을 사용할 수 있도록 합니다.

그림 4-4. 터널 프록시 배포

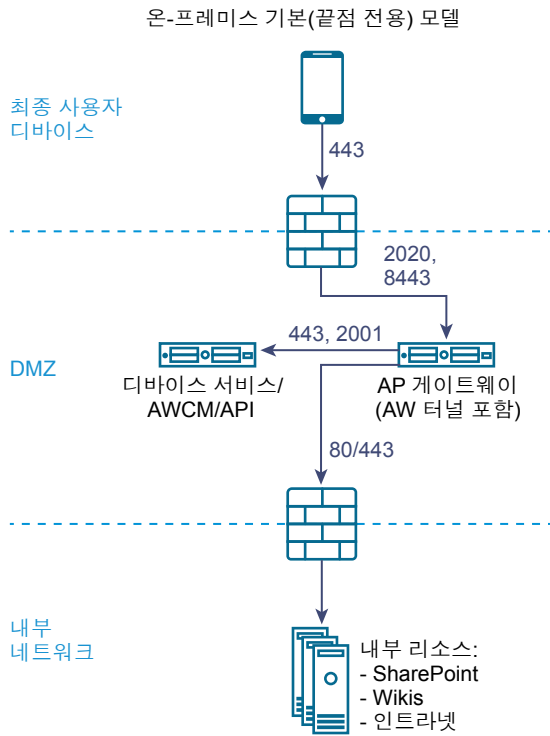


AirWatch를 사용한 애플리케이션별 Tunnel 배포

애플리케이션별 Tunnel 배포를 사용하면 내부 및 공용 애플리케이션에서 보안 내부 네트워크에 있는 회사 리소스에 안전하게 액세스할 수 있습니다.

이는 iOS 7+ 또는 Android 5.0+와 같은 운영 체제가 제공하는 애플리케이션별 기능을 사용합니다. 이러한 운영 체제는 모바일 관리자가 승인한 특정 애플리케이션별로 내부 리소스에 액세스할 수 있도록 합니다. 이 솔루션을 사용할 때의 이점은 모바일 애플리케이션의 코드를 변경할 필요가 없다는 것입니다. 이러한 운영 체제의 지원을 통해 다른 사용자 지정 솔루션을 사용할 때보다 원활한 사용자 환경 및 강화된 보안을 누릴 수 있습니다.

그림 4-5. 애플리케이션별 Tunnel 배포



AirWatch에 대한 애플리케이션별 Tunnel 및 프록시 설정 구성

터널 프록시 배포는 VMware 브라우저 모바일 애플리케이션을 통해 최종 사용자 디바이스와 웹 사이트 간 네트워크 트래픽의 보안을 유지합니다.

프로시저

- 1 [관리 UI 수동 구성] 섹션에서 **선택**을 클릭합니다.
- 2 [일반 설정] > [Edge 서비스 설정] 줄에서 **표시**를 클릭합니다.
- 3 **애플리케이션별 Tunnel 및 프록시 설정** 톱니 모양 아이콘을 클릭합니다.
- 4 터널 프록시를 사용하도록 설정하려면 [아니요]를 **예**로 변경합니다.
- 5 다음 Edge 서비스 설정 리소스를 구성합니다.

옵션	설명
식별자	기본적으로 View로 설정됩니다. Access Point는 View 연결 서버, Horizon Air, Horizon Air Hybrid-Mode와 같이 View XML 프로토콜을 사용하는 서버와 통신할 수 있습니다.
API 서버 URL	AirWatch API 서버 URL을 입력합니다. 예를 들어 https://example.com:<포트>로 입력합니다.
API 서버 사용자 이름	API 서버에 로그인하기 위한 사용자 이름을 입력합니다.
API 서버 암호	API 서버에 로그인하기 위한 암호를 입력합니다.

옵션	설명
조직 그룹 코드	사용자의 조직을 입력합니다.
AirWatch 서버 호스트 이름	AirWatch 서버 호스트 이름을 입력합니다.

6 기타 고급 설정을 구성하려면 **자세히**를 클릭합니다.

옵션	설명
AirWatch 아웃바운드 프록시	터널 프록시 서비스를 초기화하려면 [아니요]를 예로 변경합니다.
아웃바운드 프록시 호스트	아웃바운드 프록시가 설치되는 호스트 이름을 입력합니다. 참고 이는 터널 프록시가 아닙니다.
아웃바운드 프록시 포트	아웃바운드 프록시의 포트 번호를 입력합니다.
아웃바운드 프록시 사용자 이름	아웃바운드 프록시에 로그인하기 위한 사용자 이름을 입력합니다.
아웃바운드 프록시 암호	아웃바운드 프록시에 로그인하기 위한 암호를 입력합니다.
NTLM 인증	아웃바운드 프록시 요청에 NTLM 인증이 필요하도록 지정하려면 [아니요]를 예로 변경합니다.
AirWatch Tunnel 프록시에 사용	이 프록시를 AirWatch Tunnel에 대한 아웃바운드 프록시로 사용하려면 [아니요]를 예로 변경합니다. 사용하지 않도록 설정하면 Access Point는 초기 API 호출에 이 프록시를 사용하여 AirWatch 관리 콘솔의 구성을 가져옵니다.

7 **저장**을 클릭합니다.

TLS/SSL 인증서를 사용하여 Access Point 구성

5

Access Point 장치에 대해 TLS/SSL 인증서를 구성해야 합니다.

참고 Access Point 장치에 대한 TLS/SSL 인증서를 구성하면 Horizon View, Horizon Air Hybrid-Mode 및 Web Reverse Proxy에만 적용됩니다.

Access Point 장치용 TLS/SSL 인증서 구성

TLS/SSL은 Access Point 장치에 대한 클라이언트 연결에 필요합니다. 클라이언트 연결 Access Point 장치와 TLS/SSL 연결을 종료하는 중간 서버에는 TLS/SSL 서버 인증서가 필요합니다.

TLS/SSL 서버 인증서는 CA(인증 기관)에서 서명합니다. CA는 인증서와 작성자의 ID를 보증하는 신뢰할 수 있는 엔터티입니다. 신뢰할 수 있는 CA에서 인증서에 서명한 경우, 사용자에게 인증서 확인을 묻는 메시지가 더 이상 표시되지 않으며, 추가 구성 없이 썬 클라이언트 디바이스에 연결할 수 있습니다.

기본 TLS/SSL 서버 인증서는 Access Point 장치를 배포할 때 생성됩니다. VMware는 운영 환경에서 가능한 한 빨리 기본 인증서를 교체할 것을 권장합니다. 기본 인증서는 신뢰할 수 있는 CA에서 서명하지 않습니다. 기본 인증서는 운영 환경이 아닌 경우에만 사용하십시오.

올바른 인증서 유형 선택

Access Point에서 다양한 유형의 TLS/SSL 인증서를 사용할 수 있습니다. 배포에 적합한 인증서 유형을 선택하는 것이 중요합니다. 인증서를 사용할 수 있는 서버의 수에 따라 인증서 유형의 비용이 다릅니다.

선택한 유형이 무엇이든 인증서에 FQDN(정규화된 도메인 이름)을 사용하여 VMware 보안 권장 사항에 따릅니다. 내부 도메인에서의 통신에도 단순한 서버 이름이나 IP 주소를 사용하지 마십시오.

단일 서버 이름 인증서

특정 서버의 대상 이름이 있는 인증서를 생성할 수 있습니다. 예: dept.example.com.

이러한 유형의 인증서는 한 Access Point 장치만 인증해야 하는 등의 경우에 유용합니다.

CA에 인증서 서명 요청을 제출할 때 인증서와 연결되는 서버 이름을 제공합니다. Access Point 장치에서 인증서에 연결된 이름과 일치하도록 제공된 서버 이름을 확인할 수 있어야 합니다.

제목 대체 이름

SAN(제목 대체 이름)은 인증서를 발급할 때 추가할 수 있는 특성입니다. 이 특성을 사용하여 인증서에서 두 개 이상의 서버를 유효성 검사할 수 있도록 대상 이름(URL)을 추가할 수 있습니다.

예를 들어, 로드 밸런서 뒤에 있는 Access Point 장치에 대해 ap1.example.com, ap2.example.com 및 ap3.example.com의 세 인증서를 발급할 수 있습니다. 로드 밸런서 호스트 이름을 나타내는 제목 대체 이름을 추가한 경우는(이 예에서는 horizon.example.com) 인증서가 클라이언트에서 지정한 호스트 이름과 일치하므로 유효합니다.

와일드카드 인증서

와일드카드 인증서는 여러 서비스에서 사용할 수 있도록 생성됩니다. 예: *.example.com.

여러 서버에 인증서가 필요한 경우에는 와일드카드 인증서가 유용합니다. Access Point 장치 외에도 환경에 있는 다른 애플리케이션에 TLS/SSL 인증서가 필요한 경우에는 해당 서버에도 와일드카드 인증서를 사용할 수 있습니다. 그러나 다른 서비스에서 공유되는 와일드카드 인증서를 사용하는 경우 이러한 다른 서비스의 보안도 VMware Horizon 제품 보안에 영향을 미칩니다.

참고 와일드카드 인증서는 단일 도메인 수준에만 사용할 수 있습니다. 예를 들어, 대상 이름이 *.example.com인 와일드카드 인증서는 하위 도메인 dept.example.com에서 사용할 수 있지만 dept.it.example.com에서는 사용할 수 없습니다.

Access Point 장치로 가져오는 인증서는 클라이언트 시스템에서 신뢰해야 하며 와일드카드나 SAN(제목 대체 이름) 인증서를 사용하여 Access Point의 모든 인스턴스와 모든 로드 밸런서에 적용해야 합니다.

인증서 파일을 한 줄 PEM 형식으로 변환

Access Point REST API를 사용하여 인증서 설정을 구성하거나 PowerShell 스크립트를 사용하려면 인증서 체인과 개인 키에 대해 인증서를 PEM 형식 파일로 변환해야 하며, 그 뒤에 .pem 파일을 줄 바꿈 문자가 포함된 한 줄 형식으로 변환해야 합니다.

Access Point를 구성할 때 변환해야 할 수 있는 인증서 유형에는 세 가지가 있습니다.

- 항상 Access Point 장치에 대해 TLS/SSL 서버 인증서를 설치 및 구성해야 합니다.
- 스마트 카드 인증을 사용하려면 스마트 카드에 넣을 인증서에 대해 신뢰할 수 있는 CA 발급자 인증서를 설치 및 구성해야 합니다.
- 스마트 카드 인증을 사용하려면 Access Point 장치에 설치되는 SAML 서버 인증서의 서명 CA에 대해 루트 인증서를 설치 및 구성하는 것이 좋습니다.

이러한 모든 유형의 인증서에 대해 같은 절차를 수행하여 인증서를 인증서 체인이 포함된 PEM 형식 파일로 변환할 수 있습니다. TLS/SSL 서버 인증서 및 루트 인증서의 경우 각 파일을 개인 키가 포함된 PEM 파일로 변환할 수도 있습니다. 그 후에는 각 .pem 파일을 JSON 문자열로 Access Point REST API에 전달할 수 있는 한 줄 형식으로 변환해야 합니다.

필수 조건

- 인증서 파일이 있는지 확인합니다. 파일은 PKCS#12(.p12 또는 .pfx) 형식이나 Java JKS 또는 JCEKS 형식으로 되어 있을 수 있습니다.
- 인증서 변환에 사용할 openssl 명령줄 도구를 숙지합니다.
<https://www.openssl.org/docs/apps/openssl.html>의 내용을 참조하십시오.
- 인증서가 Java JKS 또는 JCEKS 형식으로 되어 있는 경우에는 Java keytool 명령줄 도구를 숙지하고 먼저 인증서를 .p12 또는 .pks 형식으로 변환한 후 .pem 파일로 변환합니다.

프로시저

- 1 인증서가 Java JKS 또는 JCEKS 형식으로 되어 있는 경우에는 keytool을 사용하여 인증서를 .p12 또는 .pks 형식으로 변환합니다.

중요 이 변환을 수행하는 동안 같은 소스 및 대상 암호를 사용하십시오.

- 2 인증서가 PKCS#12(.p12 또는 .pfx) 형식이거나 인증서가 PKCS#12 형식으로 이미 변환된 경우에는 openssl을 사용하여 인증서를 .pem 파일로 변환합니다.

예를 들어, 인증서의 이름이 mycaservercert.pfx인 경우에는 다음 명령을 사용하여 인증서를 변환합니다.

```
openssl pkcs12 -in mycaservercert.pfx -nokeys -out mycaservercert.pem
openssl pkcs12 -in mycaservercert.pfx -nodes -nocerts -out mycaservercert.pem
openssl rsa -in mycaservercertkey.pem -check -out mycaservercertkeyrsa.pem
```

- 3 mycaservercert.pem을 편집하여 불필요한 인증서 항목을 모두 제거합니다. SSL 서버 인증서 하나를 포함하고 그 뒤에 필요한 중간 CA 인증서와 루트 CA 인증서를 포함해야 합니다.
- 4 다음 UNIX 명령을 사용하여 각 .pem 파일을 JSON 문자열로 Access Point REST API에 전달할 수 있는 값으로 변환합니다.

```
awk 'NF {sub(/Wr/, ""); printf "%s\\n", $0;}' cert-name.pem
```

이 예에서 *cert-name.pem*은 인증서 파일의 이름입니다.

새로운 형식에서는 줄바꿈 문자를 포함하여 모든 인증서 정보를 한 줄에 넣습니다. 중간 인증서가 있는 경우에는 두 인증서가 같은 줄에 있도록 중간 인증서도 한 줄 형식이어야 하며, 첫 번째 인증서에 추가해야 합니다.

이제 <https://communities.vmware.com/docs/DOC-30835>에 있는 블로그 게시물 "Using PowerShell to Deploy VMware Access Point"(PowerShell을 사용하여 VMware Access Point 배포)에 첨부된 PowerShell 스크립트와 함께 이 .pem 파일을 사용하여 Access Point에 대한 인증서를 구성할 수 있습니다. 또는, JSON 요청을 생성 및 사용하여 인증서를 구성할 수 있습니다.

후속 작업

TLS/SSL 서버 인증서를 변환한 경우에는 [Access Point의 기본 TLS/SSL 서버 인증서 교체](#)의 내용을 참조하십시오. 스마트 카드 인증서의 경우에는 [Access Point 장치에서 인증서 또는 스마트 카드 인증 구성](#)의 내용을 참조하십시오.

Access Point 의 기본 TLS/SSL 서버 인증서 교체

신뢰할 수 있는 CA에서 서명된 TLS/SSL 서버 인증서를 Access Point 장치에 저장하려면 인증서를 올바른 형식으로 변환하고 PowerShell 스크립트나 Access Point REST API를 사용하여 인증서를 구성해야 합니다.

VMware는 운영 환경에서 가능한 한 빨리 기본 인증서를 교체할 것을 권장합니다. Access Point 장치를 배포할 때 생성되는 기본 TLS/SSL 서버 인증서는 신뢰할 수 있는 인증 기관에서 서명되지 않았습니다.

중요 인증서가 만료되기 전에 신뢰할 수 있는 CA에서 서명한 인증서를 정기적으로 교체하는 경우에도 이 절차를 사용합니다. 주기는 2년일 수 있습니다.

이 절차에서는 REST API를 사용하여 인증서를 교체하는 방법을 설명합니다. 쉬운 대체 방법은 <https://communities.vmware.com/docs/DOC-30835>에 있는 블로그 게시물 "Using PowerShell to Deploy VMware Access Point"(PowerShell을 사용하여 VMware Access Point 배포)에 첨부된 샘플 PowerShell 스크립트를 사용하는 것입니다. 명명된 Access Point 장치를 이미 배포한 경우 스크립트를 다시 실행하면 장치의 전원이 꺼지고 장치가 삭제되며, 지정된 현재 설정으로 장치가 다시 배포됩니다.

필수 조건

- 이미 올바른 TLS/SSL 서버 인증서와 개인 키가 없으면 인증 기관에서 새로 서명된 인증서를 가져옵니다. CSR(인증서 서명 요청)을 생성하여 인증서를 가져올 때 개인 키도 생성되었는지 확인하십시오. 1024 미만인 KeyLength 값을 사용하여 서버의 인증서를 생성하지 마십시오.

CSR을 생성하려면 클라이언트 디바이스에서 Access Point 장치에 연결할 때 사용할 FQDN(정규화된 도메인 이름)과 주체 이름을 완성하기 위한 조직 단위, 조직, 구/군/시 및 국가를 알고 있어야 합니다.

- 인증서를 PEM 형식 파일로 변환하고 .pem 파일을 한 줄 형식으로 변환합니다. [인증서 파일을 한 줄 PEM 형식으로 변환](#)의 내용을 참조하십시오.
- Access Point REST API를 숙지합니다. 이 API의 사양은 Access Point가 설치된 가상 시스템의 URL(<https://access-point-appliance.example.com:9443/rest/swagger.yaml>)에서 확인할 수 있습니다.

프로시저

- 1 Access Point 장치의 인증서를 제출하기 위한 JSON 요청을 생성합니다.

```
{
  "privateKeyPem": "string",
  "certChainPem": "string"
}
```

이 예에서 string 값은 전체 조건에 설명된 대로 생성한 JSON 한 줄 PEM 값입니다.

- 2 JSON 요청을 사용하여 Access Point REST API를 호출하고 Access Point 장치에 인증서와 키를 저장하려면 curl 또는 postman과 같은 REST 클라이언트를 사용합니다.

다음 예에서는 curl 명령을 사용합니다. 예에서 access-point-appliance.example.com은 Access Point 장치의 정규화된 도메인 이름이고 cert.json은 이전 단계에서 생성한 JSON 요청입니다.

```
curl -k -d @- -u 'admin' -H "Content-Type: application/json" -X PUT https://access-point-appliance.example.com:9443/rest/v1/config/certs/ssl < ~/cert.json
```

후속 작업

인증서에 서명한 CA가 잘 알려져 있지 않다면 루트 및 중간 인증서를 신뢰하도록 클라이언트를 구성하십시오.

TLS 또는 SSL 통신에 사용되는 보안 프로토콜 및 암호 제품군 변경

대부분의 경우에는 기본 설정을 변경할 필요가 없지만, 클라이언트와 Access Point 장치 사이에서 통신을 암호화하는 데 사용되는 보안 프로토콜 및 암호화 알고리즘을 구성할 수 있습니다.

기본 설정에는 익명 DH 알고리즘을 제외한 128비트 또는 256비트 AES 암호화를 사용하는 암호 제품군이 포함되고, 이 제품군을 강도에 따라 정렬합니다. 기본적으로 TLS v1.1 및 TLS v1.2가 사용되도록 설정되어 있습니다. TLS v1.0 및 SSL v3.0이 사용되도록 설정되어 있지 않습니다.

필수 조건

- Access Point REST API를 숙지합니다. 이 API의 사양은 Access Point가 설치된 가상 시스템의 URL(<https://access-point-appliance.example.com:9443/rest/swagger.yaml>)에서 확인할 수 있습니다.
- 암호 제품군 및 프로토콜을 구성하는 데 필요한 특정 속성 cipherSuites, ssl30Enabled, tls10Enabled, tls11Enabled 및 tls12Enabled를 숙지합니다.

프로시저

- 1 사용할 프로토콜과 암호 제품군을 지정하는 JSON 요청을 생성합니다.

다음 예에서 기본 설정을 확인할 수 있습니다.

```
{
  "cipherSuites": "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,SSL_RSA_WITH_RC4_128_SHA",
  "ssl30Enabled": "false",
  "tls10Enabled": "false",
  "tls11Enabled": "true",
  "tls12Enabled": "true"
}
```

- 2 curl 또는 postman과 같은 REST 클라이언트를 사용하여 JSON 요청으로 Access Point REST API를 호출하고 프로토콜 및 암호 제품군을 구성합니다.

예에서 `access-point-appliance.example.com`은 Access Point 장치의 정규화된 도메인 이름입니다.

```
curl -k -d @- -u 'admin' -H "Content-Type: application/json" -X PUT https://access-point-
appliance.example.com:9443/rest/v1/config/system < ~/ciphers.json
```

`ciphers.json`은 이전 단계에서 생성한 JSON 요청입니다.

지정한 암호 제품군과 프로토콜이 사용됩니다.

DMZ에서 인증 구성

처음에 VMware Access Point를 배포할 때 기본적으로 Active Directory 암호 인증이 설정됩니다. 사용자는 Active Directory 사용자 이름 및 암호를 입력하며, 이러한 자격 증명이 인증을 위해 백엔드 시스템을 통해 전송됩니다.

인증서/스마트 카드 인증, RSA SecurID 인증, RADIUS 인증 및 RSA 어댑티브 인증을 수행하도록 Access Point 서비스를 구성할 수 있습니다.

참고 Active Directory를 사용하는 암호 인증은 AirWatch 배포에서 사용할 수 있는 유일한 인증 방법입니다.

이 장에서는 다음 주제에 대해 설명합니다.

- [Access Point 장치에서 인증서 또는 스마트 카드 인증 구성](#)
- [Access Point에서 RSA SecurID 인증 구성](#)
- [Access Point에 대한 RADIUS 구성](#)
- [Access Point에서 RSA 어댑티브 인증 구성](#)
- [Access Point SAML 메타데이터 생성](#)

Access Point 장치에서 인증서 또는 스마트 카드 인증 구성

클라이언트가 데스크톱 또는 모바일 디바이스에서 인증서로 인증을 받거나 인증을 위해 스마트 카드 어댑터를 사용할 수 있도록 Access Point에서 x509 인증서 인증을 구성할 수 있습니다.

인증서 기반 인증은 사용자가 보유한 항목(개인 키 또는 스마트 카드) 및 알고 있는 사항(개인 키 암호 또는 스마트 카드 PIN)을 기준으로 합니다. 스마트 카드 인증은 사용자가 가진 정보(스마트 카드)와 사용자가 아는 정보(PIN)를 모두 확인하여 2 요소 인증을 제공합니다. 최종 사용자는 스마트 카드를 사용하여 원격 View 데스크톱 운영 체제에 로그인하고, 보낸 사람의 신원을 증명하기 위해 인증서를 사용하여 이메일에 서명하는 이메일 애플리케이션과 같은 스마트 카드 지원 애플리케이션에 액세스합니다.

이 기능을 사용할 경우 Access Point 서비스에 대해 스마트 카드 인증서 인증이 수행됩니다.

Access Point에서는 SAML 어설션을 사용하여 최종 사용자의 X.509 인증서 및 스마트 카드 PIN에 대한 정보를 Horizon Server로 전달합니다.

사용자 인증서가 있는 사용자가 인증이 해지되지 않도록 인증서 해지 검사를 구성할 수 있습니다. 인증서는 사용자가 조직을 떠나거나 스마트 카드를 분실하거나 부서를 다른 부서로 이동할 경우 해지되기도 합니다. CRL(인증서 해지 목록) 및 OCSP(온라인 인증서 상태 프로토콜)를 사용하는 인증서 해지 검사가 지원됩니다. CRL은 인증서를 발행한 CA에서 게시한 해지된 인증서 목록입니다. OCSP는 인증서의 해지 상태를 가져오는 데 사용되는 인증서 유효성 검사 프로토콜입니다.

동일한 인증서 인증 어댑터 구성에서 CRL 및 OCSP를 둘 다 구성할 수 있습니다. 두 가지 유형의 인증서 해지 검사를 구성하고 [OCSP 실패 시 CRL 사용] 확인란을 선택한 경우, OCSP가 먼저 검사되고 OCSP가 실패한 경우 해지 검사가 CRL로 폴백됩니다. CRL이 실패해도 해지 검사 중에 OCSP로 폴백되지 않습니다.

Access Point에 스마트 카드 인증이 필요하지만 인증이 서버를 통해서도 전달되도록 인증을 구성할 수 있으며, 이 경우 Active Directory 인증이 필요할 수 있습니다.

참고 VMware Identity Manager의 경우 인증이 항상 Access Point를 통해 VMware Identity Manager 서비스로 전달됩니다. Access Point를 Horizon 7에서 사용하는 경우에만 Access Point 장치에서 스마트 카드 인증을 수행하도록 구성할 수 있습니다.

Access Point에서 인증서 인증 구성

Access Point 관리 콘솔에서 인증서 인증을 사용하도록 설정하고 구성합니다.

필수 조건

- 사용자가 제공한 인증서를 서명한 CA에서 루트 인증서와 중간 인증서를 가져옵니다. [인증 기관 인증서 가져오기](#)의 내용을 참조하십시오.
- Access Point SAML 메타데이터가 서비스 제공자에 추가되고 서비스 제공자 SAML 메타데이터가 Access Point 장치로 복사되는지 확인합니다.
- (선택 사항) 인증서 인증을 위한 유효한 인증서 정책의 OID(개체 식별자) 목록.
- 해지 검사의 경우 CRL의 파일 위치 및 OCSP 서버의 URL.
- (선택 사항) OCSP 응답 서명 인증서 파일 위치.
- 인증 전에 동의 양식이 표시되는 경우, 동의 양식 콘텐츠.

프로시저

- 1 [관리 UI 수동 구성] 섹션에서 **선택**을 클릭합니다.
- 2 [일반 설정 인증 설정] 섹션에서 **표시**를 클릭합니다.
- 3 X.509 인증서 줄에서 톱니 모양을 클릭합니다.
- 4 X.509 인증서 양식을 구성합니다.

별표는 필수 텍스트 상자를 나타냅니다. 다른 모든 텍스트 상자는 선택 사항입니다.

옵션	설명
X.509 인증서 사용	인증서 인증을 사용하도록 설정하려면 [아니요]를 예로 변경합니다.
*이름	이 인증 방법의 이름을 지정합니다.

옵션	설명
*루트 및 중간 CA 인증서	업로드할 인증서 파일을 선택하려면 선택 을 클릭합니다. DER 또는 PEM으로 인코딩된 여러 루트 CA 및 중간 CA 인증서를 선택할 수 있습니다.
CRL 캐시 크기	인증서 해지 목록 캐시 크기를 입력합니다. 기본값은 100입니다.
인증서 해지 사용	인증서 해지 검사를 사용하도록 설정하려면 [아니요]를 예 로 변경합니다. 해지 검사는 사용자 인증서를 해지한 사용자의 인증을 방지합니다.
인증서의 CRL 사용	인증서를 발급한 CA에서 게시한 CRL(인증서 해지 목록)을 사용하여 인증서 상태(해지됨 또는 해지 안 됨)에 대한 유효성을 검사하려면 이 확인란을 선택합니다.
CRL 위치	CRL을 검색할 서버 파일 경로 또는 로컬 파일 경로를 입력합니다.
OCSP 해지 사용	OCSP(온라인 인증서 상태 프로토콜) 인증서 유효성 검사 프로토콜을 사용하여 인증서의 해지 상태를 가져오려면 이 확인란을 선택합니다.
OCSP 실패 시 CRL 사용	CRL 및 OCSP를 둘 다 구성한 경우, 이 확인란을 선택하여 OCSP 검사를 사용할 수 없는 경우 CRL 사용으로 폴백할 수 있습니다.
OCSP Nonce 전송	OCSP 요청의 고유한 식별자를 응답에서 전송하려면 이 확인란을 선택합니다.
OCSP URL	OCSP 해지를 사용하도록 설정한 경우 해지 검사를 위한 OCSP 서버 주소를 입력합니다.
OCSP 응답자의 서명 인증서	응답자에 대한 OCSP 인증서 경로 /path/to/file.cer을 입력합니다.
인증 전 동의 양식 사용	사용자가 인증서 인증을 사용하여 Workspace ONE 포털에 로그인하기 전에 표시할 동의 양식 페이지를 포함하려면 이 확인란을 선택합니다.
동의 양식 콘텐츠	콘텐츠 양식에 표시되는 텍스트를 여기에 입력합니다.

5 **저장**을 클릭합니다.

후속 작업

X.509 인증서 인증이 구성되고 Access Point 장치가 로드 밸런서 뒤에 설정되면 Access Point를 로드 밸런서에 SSL 패스스루로 구성해야 하며, 로드 밸런서에서 SSL을 종료하도록 구성하면 안 됩니다. 이 구성을 사용하면 인증서가 Access Point로 전달되도록 Access Point와 클라이언트 간에 SSL 핸드셰이크가 사용됩니다.

인증 기관 인증서 가져오기

사용자와 관리자가 제공한 스마트 카드의 신뢰할 수 있는 모든 사용자 인증서에 대해 적용 가능한 모든 CA(인증 기관) 인증서를 가져와야 합니다. 이러한 인증서에는 루트 인증서가 포함되며, 사용자의 스마트 카드 인증서가 중간 인증 기관에서 발급된 경우에는 중간 인증서도 포함될 수 있습니다.

사용자와 관리자가 제공한 스마트 카드에 있는 인증서를 서명한 CA의 루트 또는 중간 인증서가 없는 경우 인증서가 들어 있는 스마트 카드 또는 CA 서명 사용자 인증서에서 해당 인증서를 내보낼 수 있습니다. [Windows에서 CA 인증서 가져오기](#)의 내용을 참조하십시오.

프로시저

- ◆ 다음 소스 중 하나에서 CA 인증서를 가져오십시오.
 - Microsoft Certificate Services를 실행 중인 Microsoft IIS 서버. Microsoft IIS 설치, 인증서 발행 및 조직의 인증서 배포에 대한 정보는 Microsoft TechNet 웹사이트를 참조하십시오.
 - 신뢰된 CA의 공용 루트 인증서. 이는 이미 스마트 카드 인프라가 있는 환경에서 루트 인증서의 가장 일반적인 소스이며 스마트 카드 분산 및 인증에 대한 표준화된 접근법입니다.

Windows에서 CA 인증서 가져오기

CA 서명이 있는 사용자 인증서 또는 이 인증서가 포함된 스마트 카드가 있으면 Windows가 루트 인증서를 신뢰하기 때문에 Windows에서 루트 인증서를 내보낼 수 있습니다. 사용자 인증서의 발급자가 중간 인증 기관인 경우에는 해당 인증서를 내보낼 수 있습니다.

프로시저

- 1 스마트 카드에 사용자 인증서가 있는 경우 개인 저장소에 사용자 인증서를 추가하려면 판독기에 스마트 카드를 삽입하십시오.

개인 저장소에 사용자 인증서가 표시되지 않는 경우에는 판독기 소프트웨어를 사용해 사용자 인증서로 파일로 내보내십시오. 이 파일은 이 절차의 4단계에서 사용됩니다.
- 2 Internet Explorer에서 **도구 > 인터넷 옵션**을 선택합니다.
- 3 **내용** 탭에서 **인증서**를 클릭합니다.
- 4 **개인** 탭에서 사용할 인증서를 선택하고 **보기**를 클릭합니다.

목록에 사용자 인증서가 표시되지 않으면 **가져오기**를 클릭해 파일에서 수동으로 인증서를 가져오십시오. 인증서를 가져온 후에 목록에서 인증서를 선택할 수 있습니다.
- 5 **인증 경로** 탭에서 트리 맨 위에 있는 인증서를 선택하고 **인증서 보기**를 클릭합니다.

사용자 인증서가 트러스트 계층 구조의 일부로 서명된 경우에는 다른 고수준 인증서에서 서명 인증서에 서명했을 수 있습니다. 상위 인증서(실제로 사용자 인증서에 서명한 인증서)를 루트 인증서로 선택합니다. 경우에 따라 발급자가 중간 CA일 수도 있습니다.
- 6 **세부 정보** 탭에서 **파일에 복사**를 클릭합니다.

인증서 내보내기 마법사가 나타납니다.
- 7 **다음 > 다음**을 클릭하고 내보낼 파일의 이름과 위치를 입력합니다.
- 8 파일을 지정한 위치로 루트 인증서로 저장하려면 **다음**을 클릭합니다.

Access Point에서 RSA SecurID 인증 구성

Access Point 장치가 RSA SecurID 서버에서 인증 에이전트로 구성된 후에 Access Point 장치에 RSA SecurID 구성 정보를 추가해야 합니다.

필수 조건

- RSA 인증 관리자(RSA SecurID 서버)가 설치되어 있고 제대로 구성되어 있는지 확인합니다.
- RSA SecurID 서버에서 압축된 `sdconf.rec` 파일을 다운로드하고 서버 구성 파일의 압축을 풉니다.

프로시저

- 1 [관리 UI 수동 구성] 섹션에서 **선택**을 클릭합니다.
- 2 [일반 설정 인증 설정] 섹션에서 **표시**를 클릭합니다.
- 3 RSA SecurID 줄에서 톱니 모양을 클릭합니다.
- 4 RSA SecurID 페이지를 구성합니다.

RSA SecurID 서버에서 사용되는 정보 및 생성된 파일은 SecurID 페이지를 구성할 때 필요합니다.

옵션	조치
RSA SecurID 사용	SecurID 인증을 사용하도록 설정하려면 [아니요]를 예 로 변경합니다.
*이름	이름은 <code>securid-auth</code> 입니다.
*반복 횟수	허용되는 인증 시도 횟수를 입력합니다. 이는 RSA SecurID 토큰을 사용하여 로그인할 경우 최대 로그인 시도 실패 횟수입니다. 기본값은 5회입니다. 참고 둘 이상의 디렉토리가 구성되어 있고 추가 디렉토리를 사용하여 RSA SecurID 인증을 구현하는 경우 각 RSA SecurID 구성에 대해 동일한 값을 사용하여 허용된 인증 시도 횟수 를 구성합니다. 이 값이 동일하지 않은 경우 SecurID 인증이 실패합니다.
*외부 호스트 이름	Access Point 인스턴스의 IP 주소를 입력합니다. Access Point 장치를 인증 에이전트로 RSA SecurID 서버에 추가할 때 사용한 값과 입력한 값이 일치해야 합니다.
*내부 호스트 이름	RSA SecurID 서버에서 IP 주소 프로프트에 할당된 값을 입력합니다.
*서버 구성	[변경]을 클릭하여 RSA SecurID 서버 구성 파일을 업로드합니다. 먼저 RSA SecurID 서버에서 압축된 파일을 다운로드하고 기본 이름이 <code>sdconf.rec</code> 인 서버 구성 파일을 추출해야 합니다.
*이름 ID 접미사	View에서 TrueSSO 환경을 제공할 수 있도록 하는 <code>nameId</code> 를 입력합니다.

Access Point에 대한 RADIUS 구성

사용자에게 RADIUS 인증 사용을 요구하도록 Access Point를 구성할 수 있습니다. Access Point 장치에서 RADIUS 서버 정보를 구성합니다.

RADIUS 지원은 다양한 대체 2 요소 토큰 기반 인증 옵션을 제공합니다. RADIUS와 같은 2단계 인증 솔루션은 별도 서버에 설치된 인증 관리자에서 작동하므로 RADIUS 서버를 구성하고 ID 관리자 서비스에서 액세스할 수 있도록 설정해야 합니다.

사용자가 로그인하고 RADIUS 인증이 사용되도록 설정된 경우 브라우저에 특별한 로그인 대화상자가 표시됩니다. 사용자는 [로그인] 대화상자에 RADIUS 인증 사용자 이름 및 암호를 입력합니다.

RADIUS 서버가 액세스 챌린지를 생성하면 Access Point에서 두 번째 암호를 묻는 대화상자를 표시합니다. 현재 RADIUS 챌린지에는 텍스트 입력을 요구하는 메시지만 지원됩니다.

사용자가 이 대화상자에서 자격 증명을 입력하면 RADIUS 서버는 SMS 문자 메시지나 이메일 또는 다른 대역 외 메커니즘을 사용하는 텍스트를 코드와 함께 사용자의 휴대 전화로 전송할 수 있습니다. 사용자가 [로그인] 대화상자에 이 텍스트와 코드를 입력하면 인증이 완료됩니다.

RADIUS 서버가 Active Directory에서 사용자를 가져오는 기능을 제공하기 때문에 RADIUS 인증 사용자 이름과 암호를 묻기 전에 Active Directory 자격 증명을 묻는 메시지부터 표시될 수 있습니다.

RADIUS 인증 구성

Access Point 장치에서 RADIUS 인증을 사용하도록 설정하고, RADIUS 서버에서 구성 설정을 입력하고, 인증 유형을 RADIUS 인증으로 변경해야 합니다.

필수 조건

- 인증 관리자 서버로 사용할 서버에 RADIUS 소프트웨어가 설치되어 있고 구성되어 있는지 확인합니다. RADIUS 서버를 설정한 다음 Access Point에서 RADIUS 요청을 구성합니다. RADIUS 서버 설정에 대한 자세한 내용은 RADIUS 벤더의 설정 가이드를 참조하십시오.

다음 RADIUS 서버 정보가 필요합니다.

- RADIUS 서버의 IP 주소 또는 DNS 이름.
- 인증 포트 번호. 인증 포트는 일반적으로 1812입니다.
- 인증 유형. 인증 유형에는 PAP(Password Authentication Protocol), CHAP(Challenge Handshake Authentication Protocol), MSCHAP1, MSCHAP2(Microsoft Challenge Handshake Authentication Protocol, 버전 1 및 2)가 포함됩니다.
- RADIUS 프로토콜 메시지에서 암호화 및 암호 해독에 사용되는 RADIUS 공유 암호입니다.
- RADIUS 인증에 필요한 특정 시간 초과 및 다시 시도 값

프로시저

- [관리 UI 수동 구성] 섹션에서 **선택**을 클릭합니다.
- [일반 설정 인증 설정] 섹션에서 **표시**를 클릭합니다.

3 RADIUS 줄에서 톱니 모양을 클릭합니다.

옵션	조치
RADIUS 사용	RADIUS 인증을 사용하도록 설정하려면 [아니요]를 예 로 변경합니다.
이름*	이름은 radius-auth입니다.
인증 유형*	RADIUS 서버에서 지원되는 인증 프로토콜을 입력합니다. PAP, CHAP, MSCHAP1 또는 MSCHAP2 중 하나를 입력합니다.
공유 암호*	RADIUS 공유 암호를 입력합니다.
허용된 인증 시도 횟수*	RADIUS를 사용하여 로그인할 경우 최대 로그인 시도 실패 횟수를 입력합니다. 기본값은 3회입니다.
RADIUS 서버에 대한 시도 횟수*	총 다시 시도 횟수를 입력합니다. 기본 서버가 응답하지 않을 경우 다시 시도하기 전에 서비스는 구성된 시간 동안 대기합니다.
서버 시간 초과(초)*	RADIUS 서버가 응답하지 않을 경우 다시 시도가 전송되기까지 경과되는 RADIUS 서버 시간 초과(초)를 입력합니다.
RADIUS 서버 호스트 이름*	RADIUS 서버의 호스트 이름 또는 IP 주소를 입력합니다.
인증 포트*	RADIUS 인증 포트 번호를 입력합니다. 포트는 일반적으로 1812입니다.
영역 접두사	(선택 사항) 사용자 계정 위치를 영역이라고 합니다. 영역 접두사 문자열을 지정하면 RADIUS 서버로 보내는 사용자 이름 앞에 해당 문자열이 추가됩니다. 예를 들어 입력한 사용자 이름이 jdoe이고, 지정한 영역 접두사가 DOMAIN-A\이면 DOMAIN-A\jdoe 라는 사용자 이름이 RADIUS 서버에 전송됩니다. 이러한 필드를 구성하지 않으면 입력된 사용자 이름만 전송됩니다.
영역 접미사	(선택 사항) 영역 접미사를 구성하는 경우 사용자 이름 끝에 해당 문자열이 추가됩니다. 예를 들어 접미사가 @myco.com이면 사용자 이름 jdoe@myco.com이 RADIUS 서버로 전송됩니다.
이름 ID 접미사	View에서 True SSO 환경을 제공할 수 있도록 하는 nameId를 입력합니다.
로그인 페이지 암호 힌트	사용자가 올바른 RADIUS 암호를 입력하도록 하기 위해 사용자 로그인 페이지의 메시지에 표시할 텍스트 문자열을 입력합니다. 예를 들어 이 필드가 먼저 AD 암호, 그다음 SMS 암호 로 구성되면 로그인 페이지 메시지 먼저 AD 암호를 입력한 다음 SMS 암호를 입력하십시오. 가 표시됩니다. 기본 텍스트 문자열은 RADIUS 암호 입니다.
보조 서버 사용	고가용성을 위해 보조 RADIUS 서버를 구성하려면 [아니요]를 예 로 변경합니다. 3단계에 설명된 대로 보조 서버 정보를 구성합니다.

4 저장을 클릭합니다.

Access Point에서 RSA 어댑티브 인증 구성

RSA 어댑티브 인증은 사용자 이름 및 암호만으로 Active Directory에 대해 인증하는 것보다 더 강력한 다단계 인증을 제공하도록 구현할 수 있습니다. 어댑티브 인증은 위험 수준 및 정책에 따라 사용자의 로그인 시도를 모니터링하고 로그인을 인증합니다.

어댑티브 인증을 사용하도록 설정한 경우 RSA 정책 관리 애플리케이션에 설정된 위험 정책에 지정된 위험 표시기와 Access Point의 어댑티브 인증 구성이 사용자 이름 및 암호로 사용자를 인증할지 여부 또는 사용자를 인증하기 위해 추가 정보가 필요한지 여부를 결정하는 데 사용됩니다.

인증에 지원되는 RSA 어댑티브 인증 방법

Access Point에서 지원되는 RSA 어댑티브 인증의 강력한 인증 방법은 전화, 이메일 또는 SMS 문자 메시지와 보안 질문을 통한 대역 외 인증입니다. 제공될 수 있는 RSA 어댑티브 인증 방법을 서비스에서 사용하도록 설정합니다. RSA 어댑티브 인증 정책에 따라 사용되는 보조 인증 방법이 결정됩니다.

대역 외 인증은 사용자 이름 및 암호와 함께 추가 확인을 전송하도록 요구하는 프로세스입니다. 사용자는 RSA 어댑티브 인증 서버에 등록할 때 서버 구성에 따라 이메일 주소나 전화 번호 또는 둘 다를 제공합니다. 추가 확인이 필요하면 RSA 어댑티브 인증 서버는 제공된 채널을 통해 일회용 암호를 전송합니다. 사용자는 사용자 이름 및 원래 암호 외에 이 암호도 입력합니다.

보안 질문 기능은 사용자가 RSA 어댑티브 인증 서버에 등록할 때 몇 가지 질문에 답변하도록 요구합니다. 답변할 등록 질문 수와 로그인 페이지에 나타나는 보안 질문 수를 구성할 수 있습니다.

RSA 어댑티브 인증 서버에 사용자 등록

사용자는 인증을 위해 어댑티브 인증을 사용하려면 RSA 어댑티브 인증 데이터베이스에 프로비저닝되어야 합니다. 사용자는 해당 사용자 이름 및 암호를 사용하여 처음 로그인할 때 RSA 어댑티브 인증 데이터베이스에 추가됩니다. 서비스에서 RSA 어댑티브 인증을 구성한 방식에 따라 사용자는 로그인할 때 이메일 주소, 전화 번호, 문자 메시지 서비스 번호(SMS)를 제공하도록 요구되거나 보안 질문에 대한 답변을 설정하도록 요구될 수 있습니다.

참고 RSA 어댑티브 인증은 사용자 이름에서 국제 문자를 허용하지 않습니다. 사용자 이름에서 다중 바이트 문자를 허용하려면 RSA 지원 서비스에 문의하여 RSA 어댑티브 인증 및 RSA 인증 관리자를 구성하십시오.

Access Point에서 RSA 어댑티브 인증 구성

서비스에 대해 RSA 어댑티브 인증을 구성하려면 RSA 어댑티브 인증을 사용하도록 설정합니다. 이를 위해 적용할 어댑티브 인증 방법을 선택하고 Active Directory 연결 정보 및 인증서를 추가합니다.

필수 조건

- RSA 어댑티브 인증이 보조 인증에 사용할 인증 방법으로 올바르게 구성되어 있습니다.
- SOAP 끝점 주소 및 SOAP 사용자 이름에 대한 세부 정보.
- 사용 가능한 Active Directory 구성 정보 및 Active Directory SSL 인증서.

프로시저

- 1 [관리 UI 수동 구성] 섹션에서 **선택**을 클릭합니다.
- 2 [일반 설정 인증 설정] 섹션에서 **표시**를 클릭합니다.
- 3 RSA 어댑티브 인증 줄에서 톱니 모양을 클릭합니다.

4 사용자 환경에 적합한 설정을 선택합니다.

참고 별표는 필수 필드를 나타냅니다. 다른 필드는 선택 사항입니다.

옵션	설명
RSA AA 어댑터 사용 이름*	RSA 어댑티브 인증을 사용하도록 설정하려면 [아니요]를 예로 변경합니다. 이름은 rsaaa-auth입니다.
SOAP 끝점*	RSA 어댑티브 인증 어댑터 및 서비스 간 통합을 위한 SOAP 끝점 주소를 입력합니다.
SOAP 사용자 이름*	SOAP 메시지에 서명하는 데 사용되는 사용자 이름 및 암호를 입력합니다.
SOAP 암호*	RSA 어댑티브 인증 SOAP API 암호를 입력합니다.
RSA 도메인	어댑티브 인증 서버의 도메인 주소를 입력합니다.
OOB 이메일 사용	이메일 메시지를 통해 최종 사용자에게 일회용 암호를 전송하는 대역 외 인증을 사용하도록 설정하려면 [예]를 선택합니다.
OOB SMS 사용	SMS 문자 메시지를 통해 최종 사용자에게 일회용 암호를 전송하는 대역 외 인증을 사용하도록 설정하려면 [예]를 선택합니다.
SecurID 사용	SecurID를 사용하도록 설정하려면 [예]를 선택합니다. RSA 토큰 및 암호를 입력하라는 메시지가 표시됩니다.
본인 확인 질문 사용	인증을 위해 등록 및 보안 질문을 사용하려면 [예]를 선택합니다.
등록 질문 수*	인증 어댑터 서버에 등록할 때 사용자가 설정해야 하는 질문 수를 입력합니다.
보안 질문 수*	사용자가 로그인하기 위해 올바르게 답변해야 하는 보안 질문 수를 입력합니다.
허용된 인증 시도 횟수*	인증이 실패하기 전에 로그인을 시도하는 사용자에게 보안 질문을 표시하는 횟수를 입력합니다.
디렉토리 유형*	지원되는 유일한 디렉토리는 Active Directory입니다.
SSL 사용	디렉토리 연결에 SSL을 사용하려면 [예]를 선택합니다. [디렉토리 인증서] 필드에 Active Directory SSL 인증서를 추가합니다.
서버 호스트*	Active Directory 호스트 이름을 입력합니다.
서버 포트	Active Directory 포트 번호를 입력합니다.
DNS 서비스 위치 사용	DNS 서비스 위치가 디렉토리 연결에 사용되는 경우 [예]를 선택합니다.
기본 DN	계정 검색을 시작할 DN을 입력합니다. 예를 들어 OU=myUnit,DC=myCorp,DC=com을 입력합니다.
바인딩 DN*	사용자를 검색할 수 있는 계정을 입력합니다. 예를 들어 CN=binduser,OU=myUnit,DC=myCorp,DC=com을 입력합니다.
바인딩 암호	바인딩 DN 계정의 암호를 입력합니다.
검색 특성	사용자 이름을 포함하는 계정 특성을 입력합니다.
디렉토리 인증서	보안 SSL 연결을 설정하려면 텍스트 상자에 디렉토리 서버 인증서를 추가합니다. 여러 서버가 있는 경우 CA(인증 기관)의 루트 인증서를 추가합니다.
STARTTLS 사용	STARTTLS를 사용하려면 [아니요]를 예로 변경합니다.

5 저장을 클릭합니다.

Access Point SAML 메타데이터 생성

Access Point 장치에서 SAML 메타데이터를 생성하고 서버와 메타데이터를 교환하여 스마트 카드 인증에 필요한 상호 신뢰를 형성해야 합니다.

SAML(Security Assertion Markup Language)은 여러 보안 도메인 간에 인증 및 권한 부여 정보를 설명하고 교환하는 데 사용되는 XML 기반 표준입니다. SAML은 SAML 어설션이라는 XML 문서로 ID 공급자와 서비스 공급자 간에 사용자 정보를 전달합니다. 이 시나리오에서 Access Point 는 ID 공급자이고 서버는 서버 제공자입니다.

필수 조건

- 장치의 시간이 올바르게 설정되도록 Access Point 장치에서 시계(UTC)를 구성합니다. 예를 들어, Access Point 가상 시스템에서 콘솔 창을 열고 화살표 버튼을 사용하여 올바른 시간대를 선택합니다. 또한 ESXi 호스트의 시간이 NTP 서버와 동기화되는지 확인하고 장치 가상 시스템에서 실행 중인 VMware Tools가 ESXi 호스트의 시간과 가상 시스템의 시간을 동기화하는지 확인합니다.

중요 Access Point 장치의 시계가 서버 호스트의 시계와 일치하지 않는 경우에는 스마트 카드 인증이 작동하지 않을 수도 있습니다.

- Access Point 메타데이터에 서명하는 데 사용할 수 있는 SAML 서명 인증서를 가져옵니다.

참고 VMware에서는 설정에 두 개 이상의 Access Point 장치가 있는 경우에 특정 SAML 서명 인증서를 생성하여 사용할 것을 권장합니다. 이 경우 서버에서 모든 Access Point 장치의 어설션을 승인할 수 있도록 같은 서명 인증서를 사용하여 모든 장치를 구성해야 합니다. 특정 SAML 서명 인증서에서 모든 장치의 SAML 메타데이터는 동일합니다.

- 아직 SAML 서명 인증서를 PEM 형식 파일로 변환하고 .pem 파일을 한 줄 형식으로 변환하지 않은 경우에는 지금 변환합니다. [인증서 파일을 한 줄 PEM 형식으로 변환](#)의 내용을 참조하십시오.

프로시저

- [관리 UI 수동 구성] 섹션에서 **선택**을 클릭합니다.
- [고급 설정] 섹션에서 **SAML ID 제공자 설정** 톱니 모양 아이콘을 클릭합니다.
- 인증서 제공** 확인란을 선택합니다.
- 개인 키 파일을 추가하려면 **선택**을 클릭하고 인증서에 대한 개인 키 파일로 이동합니다.
- 인증서 체인 파일을 추가하려면 **선택**을 클릭하고 인증서 체인 파일로 이동합니다.
- 저장**을 클릭합니다.
- [호스트 이름] 텍스트 상자에 호스트 이름을 입력하고 ID 제공자 설정을 다운로드합니다.

다른 서비스 제공자가 사용하는 SAML 인증자 만들기

Access Point 장치에 SAML 메타데이터를 생성한 후에 해당 데이터를 백엔드 서비스 제공자로 다시 복사할 수 있습니다. 이 데이터를 서비스 제공자에 복사하는 것은 Access Point를 ID 공급자로 사용하도록 SAML 인증자를 만드는 프로세스의 일부입니다.

Horizon Air Hybrid 모드 서버에 대한 내용은 특정 지침이 있는 제품 설명서를 참조하십시오.

서비스 제공자 SAML 메타데이터를 Access Point에 복사

Access Point를 ID 공급자로 사용할 수 있도록 SAML 인증자를 만들고 사용하도록 설정하려는 경우에는 백엔드 시스템에서 SAML 메타데이터를 생성하고 그 메타데이터를 사용하여 Access Point 장치에 서비스 제공자를 생성합니다. 이 데이터 교환에서는 ID 공급자(Access Point)와 백엔드 서비스 제공자(View 연결 서버 등) 사이의 신뢰를 형성합니다.

필수 조건

Access Point에 대한 SAML 인증자를 백엔드 서비스 제공자 서버에 만들었는지 확인합니다.

프로시저

- 1 보통 XML 파일 형태로 되어 있는 서비스 제공자 SAML 메타데이터를 검색합니다.

지침은 서비스 제공자에 대한 설명서를 참조하십시오.

서비스 제공자에 따라 절차가 다릅니다. 예를 들어 브라우저를 열고 URL(예: <https://connection-server.example.com/SAML/metadata/sp.xml>)을 입력합니다.

그리고 **다른 이름으로 저장** 명령을 사용하여 웹 페이지를 XML 파일로 저장합니다. 이 파일의 내용은 다음 텍스트로 시작합니다.

```
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" ...
```

- 2 [Access Point 관리 UI 수동 구성] 섹션에서 **선택**을 클릭합니다.
- 3 [고급 설정] 섹션에서 **SAML 서버 제공자 설정** 톱니 모양 아이콘을 클릭합니다.
- 4 [서비스 제공자 이름] 텍스트 상자에 서비스 제공자 이름을 입력합니다.
- 5 [메타데이터 XML] 텍스트 상자에 1단계에서 생성한 메타데이터 파일을 붙여 넣습니다.
- 6 **저장**을 클릭합니다.

Access Point와 서비스 제공자가 이제 인증 및 권한 부여 정보를 교환할 수 있습니다.

Access Point 배포 문제 해결

사용자 환경에 Access Point를 배포할 때 발생하는 문제를 진단하고 수정하기 위해 다양한 절차를 사용할 수 있습니다.

문제 해결 절차를 사용하여 해당 문제의 원인을 조사하고 직접 수정하거나 VMware 기술 지원에서 도움을 받을 수 있습니다.

이 장에서는 다음 주제에 대해 설명합니다.

- 배포 오류 해결
- Access Point 장치에서 로그 수집
- 디버그 모드 사용

배포 오류 해결

사용자 환경에 Access Point를 배포할 때 문제를 겪을 수 있습니다. 배포에 다양한 문제 진단 및 해결 절차를 사용할 수 있습니다.

인터넷에서 다운로드한 스크립트를 실행할 때 보안 경고 발생

PowerShell 스크립트가 실행하려고 의도한 스크립트가 맞는지 확인한 후 PowerShell 콘솔에서 다음 명령을 실행합니다.

```
unblock-file .\wapdeploy.ps1
```

ovftool 명령을 찾을 수 없음

OVFTool 소프트웨어가 스크립트에서 요구하는 위치에 맞게 Windows 시스템에 설치되어 있는지 확인합니다.

netmask1 속성의 잘못된 네트워크

- 메시지에 netmask0, netmask1 또는 netmask2가 언급될 수 있습니다. 세 개 네트워크 각각의 .INI 파일에 netInternet, netManagementNetwork 및 netBackendNetwork와 같은 값이 설정되어 있는지 확인합니다.

- vSphere 네트워크 프로토콜 프로파일이 참조된 모든 네트워크 이름에 연결되어 있는지 확인합니다. 이 경우 IPv4 서브넷 마스크, 게이트웨이 등과 같은 네트워크 설정이 지정됩니다. 연결된 네트워크 프로토콜 프로파일이 각 설정에 대해 올바른 값을 갖는지 확인합니다.

운영 체제 식별자가 지원되지 않는다는 경고 메시지 표시

경고 메시지는 지정된 운영 체제 식별자 SUSE Linux Enterprise Server 12.0 64비트(id:85)가 선택된 호스트에서 지원되지 않는다고 표시됩니다. 이 식별자는 다음 OS 식별자: 기타 Linux(64비트)에 해당됩니다.

이 경고 메시지는 무시하십시오. 지원되는 운영 체제에 자동으로 매핑되기 때문입니다.

RSA SecurID 인증을 위한 Access Point 구성

.INI 파일의 Horizon 섹션에 다음 줄을 추가합니다.

```
authMethods=securid-auth && sp-auth  
matchWindowsUserName=true
```

.INI 파일 맨 끝에 새 섹션을 추가합니다.

```
[SecurIDAuth]  
serverConfigFile=C:\Temp\sdconf.rec  
externalHostName=192.168.0.90  
internalHostName=192.168.0.90
```

IP 주소는 Access Point의 IP 주소로도 설정되어야 합니다. sdconf.rec 파일은 RSA Authentication Manager에서 가져오며 완전히 구성되어야 합니다. Access Point 2.5 이상 버전을 사용하고 있으며 Access Point에서 네트워크의 RSA Authentication Manager 서버에 액세스할 수 있는지 확인합니다. apdeploy Powershell 명령을 다시 실행하여 RSA SecurID용으로 구성된 Access Point를 다시 배포합니다.

로케이터가 개체를 참조하지 않음 오류

이 오류는 vSphere OVF Tool에서 사용되는 target= 값이 사용 중인 vCenter 환경에 올바르지 않음을 나타냅니다. vCenter 호스트 또는 클러스터를 참조하는 데 사용되는 대상 형식의 예로 <https://communities.vmware.com/docs/DOC-30835>의 표를 사용하십시오. 최상위 개체는 다음과 같이 지정됩니다.

```
target=vi://administrator@vsphere.local:PASSWORD@192.168.0.21/
```

이제 개체는 다음 수준에서 사용할 수 있는 이름을 표시합니다.

```
target=vi://administrator@vsphere.local:PASSWORD@192.168.0.21/Datacenter1/
target=vi://administrator@vsphere.local:PASSWORD@192.168.0.21/Datacenter1/host
target=vi://administrator@vsphere.local:PASSWORD@192.168.0.21/Datacenter1/host/Cluster1/
or
target=vi://administrator@vsphere.local:PASSWORD@192.168.0.21/Datacenter1/host/esxhost1
```

대상에 사용되는 폴더 이름, 호스트 이름 및 클러스터 이름은 대/소문자를 구분합니다.

Access Point 장치에서 로그 수집

브라우저에 URL을 입력하여 Access Point 장치에서 로그가 포함된 ZIP 파일을 가져올 수 있습니다.

다음 URL을 사용하여 Access Point 장치에서 로그를 수집합니다.

```
https://access-point-appliance.example.com:9443/rest/v1/monitor/support-archive
```

이 예에서 access-point-appliance.example.com은 Access Point 장치의 정규화된 도메인 이름입니다.

이러한 로그 파일은 장치의 /opt/vmware/gateway/logs 디렉토리에서 수집되었습니다.

다음 표에는 ZIP 파일에 포함된 다양한 파일에 대한 설명이 나와 있습니다.

표 7-1. 문제 해결에 도움이 되는 시스템 정보가 포함된 파일

파일 이름	설명
df.log	디스크 공간 사용에 대한 정보가 포함되어 있습니다.
netstat.log	네트워크 연결에 대한 정보가 포함되어 있습니다.
ap_config.json	Access Point 장치의 현재 구성 설정이 포함되어 있습니다.
ps.log	프로세스 목록이 포함되어 있습니다.
ifconfig.log	네트워크 인터페이스에 대한 정보가 포함되어 있습니다.
free.log	메모리 사용에 대한 정보가 포함되어 있습니다.

표 7-2. Access Point 의 로그 파일

파일 이름	설명
esmanager.log	포트 443 및 80에서 수신하는 Edge Service Manager 프로세스의 로그 메시지가 포함되어 있습니다.
authbroker.log	인증 어댑터를 처리하는 AuthBroker 프로세스의 로그 메시지가 포함되어 있습니다.
admin.log	포트 9443에서 Access Point REST API를 제공하는 프로세스의 로그 메시지가 포함되어 있습니다.
admin-zookeeper.log	Access Point 구성 정보를 저장하는 데 사용되는 데이터 계층과 관련된 로그 메시지가 포함되어 있습니다.
tunnel.log	XML API 처리의 일부로서 사용되는 터널 프로세스의 로그 메시지가 포함되어 있습니다.

표 7-2. Access Point 의 로그 파일 (계속)

파일 이름	설명
bsg.log	Blast 보안 게이트웨이의 로그 메시지가 포함되어 있습니다.
SecurityGateway_*.log	PCoIP 보안 게이트웨이의 로그 메시지가 포함되어 있습니다.

“-std-out.log”로 끝나는 로그 파일은 다양한 프로세스의 stdout에 기록되는 정보를 포함하며 일반적으로 빈 파일입니다.

AirWatch에 대한 Access Point 로그 파일

- /var/log/airwatch/tunnel/vpnd
tunnel-init.log 및 tunnel.log는 다음 디렉토리에서 캡처됩니다.
- /var/log.airwatch/proxy
proxy.log는 다음 디렉토리에서 캡처됩니다.
- /var/log/airwatch/appliance-agent
appliance-agent.log는 다음 디렉토리에서 캡처됩니다.

디버그 모드 사용

Access Point 장치에 대해 디버그 모드를 사용하도록 설정하여 장치의 내부 상태를 보거나 조작할 수 있습니다. 디버그 모드에서는 사용자 환경의 배포 시나리오를 테스트할 수 있습니다.

필수 조건

- Access Point 장치가 사용되고 있지 않은지 확인합니다.

참고 작동되지 않는 Access Point 장치에 대한 로깅 정보를 수집하는 것이 도움이 될 수 있습니다. 이 로그는 일반적인 방법으로 구할 수 있습니다.

프로시저

- 1 Access Point 시스템에 로그인합니다.
- 2 명령줄 인터페이스에 다음 명령을 입력합니다.
`cd /opt/vmare/gateway/conf`
- 3 로그 속성 파일을 확인합니다.
`vi log4j-esmanager.properties`
- 4 속성 파일에서 다음 줄을 찾은 후 편집합니다. info를 debug로 바꿉니다.

```
log4j.logger.com.vmware=info,default
```

- 5 임의 경로의 로깅 구성을 변경하려면 이 명령을 입력합니다.
`supervisorctl restart esmanager`