Bereitstellen und Konfigurieren von Access Point

Unified Access Gateway 2.8

vmware®

Die neueste technische Dokumentation finden Sie auf der VMware-Website unter:

https://docs.vmware.com/de/

Falls Sie Anmerkungen zu dieser Dokumentation haben, senden Sie Ihre Kommentare und Vorschläge an:

docfeedback@vmware.com

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

VMware Global, Inc.
Zweigniederlassung Deutschland
Freisinger Str. 3
85716 Unterschleißheim/Lohhof
Germany
Tel.: +49 (0) 89 3706 17000
Fax: +49 (0) 89 3706 17333
www.vmware.com/de

Inhalt

Bereitstellen und Konfigurieren von VMware Access Point

Bereitstellen und Konfigurieren von Access Point bietet Informationen zum Konzipieren einer Bereitstellung von VMware Horizon®, VMware Identity Manager™ und VMware AirWatch®, die VMware Access Point™ verwendet, um einen sicheren externen Zugriff auf die Anwendungen Ihrer Organisation zu ermöglichen. Bei diesen Anwendungen kann es sich um Windows-Anwendungen, Software-as-a-Service(SaaS)-Anwendungen und Desktops handeln. Dieses Handbuch enthält auch Anleitungen für die Bereitstellung virtueller Access Point-Appliances und für die Änderung der Konfigurationseinstellungen nach der Bereitstellung.

Zielgruppe

Diese Informationen richten sich an Benutzer, die Access Pointbereitstellen und verwenden möchten. Die Informationen wurden für erfahrene Linux- und Windows-Systemadministratoren verfasst, die mit der Technologie virtueller Maschinen sowie mit Datencenter-Vorgängen vertraut sind.

Vorbereiten der Bereitstellung von Access Point

1

Access Point-Funktionen sind ein sicheres Gateway für Benutzer, die auf Remote-Desktops und -anwendungen von außerhalb der Unternehmens-Firewall zugreifen möchten.

Dieses Kapitel behandelt die folgenden Themen:

- Access Point als sicheres Gateway
- Verwendung von Access Point anstelle eines virtuellen privaten Netzwerks
- System- und Netzwerkanforderungen von Access Point
- Firewall-Regeln für Umkreisnetzwerk-basierte Access Point-Appliances
- Access Point-Topologien für den Lastausgleich
- DMZ-Design für Access Point mit mehreren Netzwerkkarten

Access Point als sicheres Gateway

Access Point ist eine Sicherheits-Appliance der Schicht 7, die normalerweise in einer demilitarisierten Netzwerkzone (DMZ) installiert ist. Access Point wird verwendet, um sicherzustellen, dass nur Datenverkehr in das Datencenter des Unternehmens gelangt, der zu einem sicher authentifizierten Remotebenutzer gehört.

Access Point leitet Authentifizierungsanfragen an den jeweiligen Server weiter und blockiert jede nicht authentifizierte Anfrage. Benutzer können nur auf Ressourcen zugreifen, für deren Zugriff sie berechtigt sind.

Außerdem sorgen virtuelle Access Point-Appliances dafür, dass der Datenverkehr für einen authentifizierten Benutzer nur an Desktop- und Anwendungsressourcen geleitet werden kann, für die der Benutzer auch berechtigt ist. Dieser Grad an Sicherheit erfordert eine genaue Untersuchung der Desktopprotokolle und Koordination von sich potenziell schnell verändernden Richtlinien und Netzwerkadressen, damit der Zugriff genauestens kontrolliert werden kann.

Access Point-Appliances befinden sich in der Regel in einer demilitarisierten Netzwerkzone (DMZ) und dienen als Proxy-Host für Verbindungen innerhalb des vertrauenswürdigen Netzwerks Ihres Unternehmens. Dieses Konzept bietet eine zusätzliche Schutzschicht durch Abschirmung der virtuellen Desktops, Anwendungshosts und Server gegenüber dem öffentlichen Internet.

Access Point ist eine speziell für DMZ entwickelte geschützte Sicherheits-Appliance. Die folgenden Schutzeinstellungen sind implementiert.

- Aktuelle Linux-Kernel- und Software-Patches
- Unterstützung mehrerer Netzwerkkarten (NICs) für Datenverkehr aus Internet und Intranet
- SSH deaktiviert
- FTP, Telnet, Rlogin oder Rsh-Dienste deaktiviert
- Nicht benötigte Dienste deaktiviert

Verwendung von Access Point anstelle eines virtuellen privaten Netzwerks

Access Point und generische VPN-Lösungen ähneln sich, da beide sicherstellen, dass Datenverkehr nur für sicher authentifizierte Benutzer in ein internes Netzwerk weitergeleitet wird.

Access Point bietet im Vergleich mit einem generischen VPN die folgenden Vorteile.

- Access Control Manager Access Point wendet Zugriffsregeln automatisch an. Access Point erkennt die Berechtigungen der Benutzer und die für die interne Verbindung erforderliche Adressierung, die sich schnell ändern kann. Ein VPN erreicht dasselbe, da bei den meisten VPNs ein Administrator Netzwerkverbindungsregeln für jeden Benutzer oder jede Benutzergruppe einzeln konfigurieren kann. Dies funktioniert zwar zunächst recht gut mit einem VPN, die Verwaltung der erforderlichen Regeln bringt aber erheblichen administrativen Arbeitsaufwand mit sich.
- Benutzeroberfläche Access Point nimmt keine Änderungen an der unkomplizierten Benutzeroberfläche von Horizon Client vor. Mit Access Point befinden sich authentifizierte Benutzer beim Start des Horizon Clients in ihrer View-Umgebung und haben kontrollierten Zugriff auf ihre Desktops und Anwendungen. Bei einem VPN müssen Sie zunächst die VPN-Software einrichten und dann separat die Authentifizierung durchführen, bevor der Horizon Client gestartet wird.
- Leistung Access Point ist für maximale Sicherheit und Leistung konzipiert. Mit Access Point sind PCoIP-, HTML Access- und WebSocket-Protokolle ohne zusätzliche Kapselung gesichert. VPNs werden als SSL-VPNs implementiert. Diese Implementierung entspricht den Sicherheitsanforderungen und gilt bei aktiviertem TLS (Transport Layer Security) als sicher, aber das zugrunde liegende Protokoll bei SSL/TLS ist lediglich TCP-basiert. Da moderne Video-Remoting-Protokolle verbindungslose UDP-basierte Transporte nutzen, können die Leistungsvorteile bei Durchsetzen eines TCP-basierten Transports erheblich gemindert werden. Dies gilt nicht für alle VPN-Technologien, da diejenigen, die mit DTLS oder IPsec anstelle von SSL/TLS betrieben werden können, gut mit View-Desktopprotokollen funktionieren können.

System- und Netzwerkanforderungen von Access Point

Damit Sie die Access Point-Appliance bereitstellen können, müssen Sie sicherstellen, dass Ihr System die Hardware- und Softwareanforderungen erfüllt.

Unterstützte VMware-Produktversionen

Sie müssen bestimmte Versionen der VMware-Produkte mit bestimmten Versionen von Access Point verwenden. Neueste Informationen zur Kompatibilität finden Sie in den Versionshinweisen zum Produkt und in der Interoperabilitätstabelle für VMware-Produkte unter http://www.vmware.com/resources/compatibility/sim/interop_matrix.php. Die Informationen in den Versionshinweisen und der Interoperabilitätstabelle sind gegenüber den Informationen in diesem Handbuch vorrangig.

Access Point 2.8 kann mit folgenden VMware-Produkten als sicheres Gateway verwendet werden.

- VMware AirWatch 8.4 und höher
- VMware Identity Manager 2.7 und höher
- VMware Horizon 6.2 und höher
- VMware Horizon Air Hybrid Mode 1.0 und höher
- VMware Horizon Air 15.3 und höher

Hardwareanforderungen für den ESXi-Server

Die Access Point-Appliance muss unter einer vSphere-Version bereitgestellt werden, die mit der Version identisch ist, die für die von Ihnen verwendeten Horizon-Produkte und Versionen unterstützt wird.

Wenn Sie vSphere Web Client verwenden, müssen Sie sicherstellen, dass das Client-Integrations-Plug-In installiert ist. Weitere Informationen dazu finden Sie in der vSphere-Dokumentation. Wenn Sie dieses Plug-in nicht vor dem Start des Bereitstellungsassistenten installieren, fordert Sie der Assistent zur Installation auf. Hierzu müssen Sie den Browser schließen und den Assistenten beenden.

Hinweis Konfigurieren Sie die Uhr (UTC) der Access Point-Appliance, damit diese über die korrekte Uhrzeit verfügt. Öffnen Sie z. B. ein Konsolenfenster auf der virtuellen Access Point-Maschine, und wählen Sie mit den Pfeilschaltflächen die erforderliche Zeitzone aus. Stellen Sie zudem sicher, dass die Uhrzeit des ESXi-Hosts mit dem NTP-Server synchronisiert ist und dass die VMware Tools, die auf der virtuellen Appliance-Maschine ausgeführt werden, die Uhrzeit auf der virtuellen Maschine mit der Uhrzeit auf dem ESXi-Host synchronisieren.

Anforderungen für die virtuelle Appliance

Das OVF-Paket für die Access Point-Appliance wählt automatisch die für Access Point erforderliche Konfiguration der virtuellen Maschine aus. Auch wenn Sie diese Einstellungen ändern können, empfiehlt VMware, den CPU-Arbeitsspeicher oder den Festplattenspeicherplatz nicht auf niedrigere Werte als die OVF-Standardeinstellungen einzustellen.

Stellen Sie sicher, dass der Datenspeicher, der für die Appliance verwendet werden soll, über ausreichend freien Festplattenspeicherplatz verfügt und die anderen Systemanforderungen erfüllt.

- Downloadgröße der virtuellen Appliance: 2,5 GB
- Minimal erforderlicher Festplattenspeicher bei schlanker Speicherzuweisung: 2,5 GB
- Minimal erforderlicher Festplattenspeicher bei starker Speicherzuweisung: 20 GB

Für die Bereitstellung der virtuellen Appliance sind folgende Informationen erforderlich

- Statische IP-Adresse
- IP-Adresse des DNS-Servers
- Kennwort für den Root-Benutzer
- URL der Serverinstanz des Lastausgleichsdienstes, auf den die Access Point-Appliance verweist

Anforderungen an die Netzwerkkonfiguration

Sie haben die Möglichkeit, eine, zwei oder drei Netzwerkschnittstellen zu verwenden. Access Point verlangt dabei für jede eine eigene statische IP-Adresse. Viele DMZ-Implementierungen verwenden getrennte Netzwerke zur Sicherung der verschiedenen Datenverkehrstypen. Konfigurieren Sie Access Point entsprechend dem Netzwerkdesign der DMZ, in der die Bereitstellung erfolgt.

- Eine Netzwerkschnittstelle ist für POCs (Proof of Concept, Machbarkeitsstudie) oder für Testvorgänge ausreichend. Bei einem NIC (Network Information Center) findet der gesamte externe, interne und Verwaltungsverkehr auf demselben Subnetz statt.
- Bei zwei Netzwerkschnittstellen befindet sich der externe Verkehr auf einem Subnetz und der interne bzw. der Verwaltungsverkehr auf einem anderen.
- Die Verwendung von drei Netzwerkschnittstellen ist die sicherste Variante. Bei einem dritten NIC verfügen der externe, der interne und der Verwaltungsverkehr über jeweils ein eigenes Subnetz.

Wichtig Stellen Sie sicher, dass jedem Netzwerk ein IP-Pool zugewiesen wurde. Die Access Point-Appliance kann dann zum Zeitpunkt der Bereitstellung die Einstellungen für Subnetzmaske und Gateway übernehmen. Um einen IP-Pool in vCenter Server hinzuzufügen, wenn Sie den systemeigenen vSphere Client verwenden, wechseln Sie zur Registerkarte **IP-Pools** des Rechenzentrums. Wenn Sie alternativ dazu den vSphere Web Client verwenden, können Sie ein Netzwerkprotokollprofil erstellen. Wechseln Sie zur Registerkarte **Verwalten** des Rechenzentrums und wählen Sie die Registerkarte **Netzwerkprotokollprofile** aus. Weitere Informationen finden Sie unter Konfigurieren von Benutzerprofilen für Netzwerke mit virtuellen Maschinen.

Anforderungen für die Protokollspeicherung

Für die Protokolldateien ist standardmäßig ein bestimmter Teil des Speicherplatzes im Aggregat vorgesehen. Die Protokolle für Access Point werden standardmäßig archiviert. Um diese Protokolleinträge beizubehalten, speichern Sie diese mit Syslog. Siehe Sammeln von Protokollen der Access Point-Appliance.

Firewall-Regeln für Umkreisnetzwerk-basierte Access Point -Appliances

Für Umkreisnetzwerk-basierte Access Point-Appliances müssen für die Front-End- und Back-End-Firewall bestimmte Firewall-Regeln aktiviert sein. Während der Installation werden Access Point-Dienste standardmäßig für die Überwachung an bestimmten Netzwerkports eingerichtet.

Die Bereitstellung einer Umkreisnetzwerk-basierten Access Point-Appliance beinhaltet in der Regel zwei Firewalls.

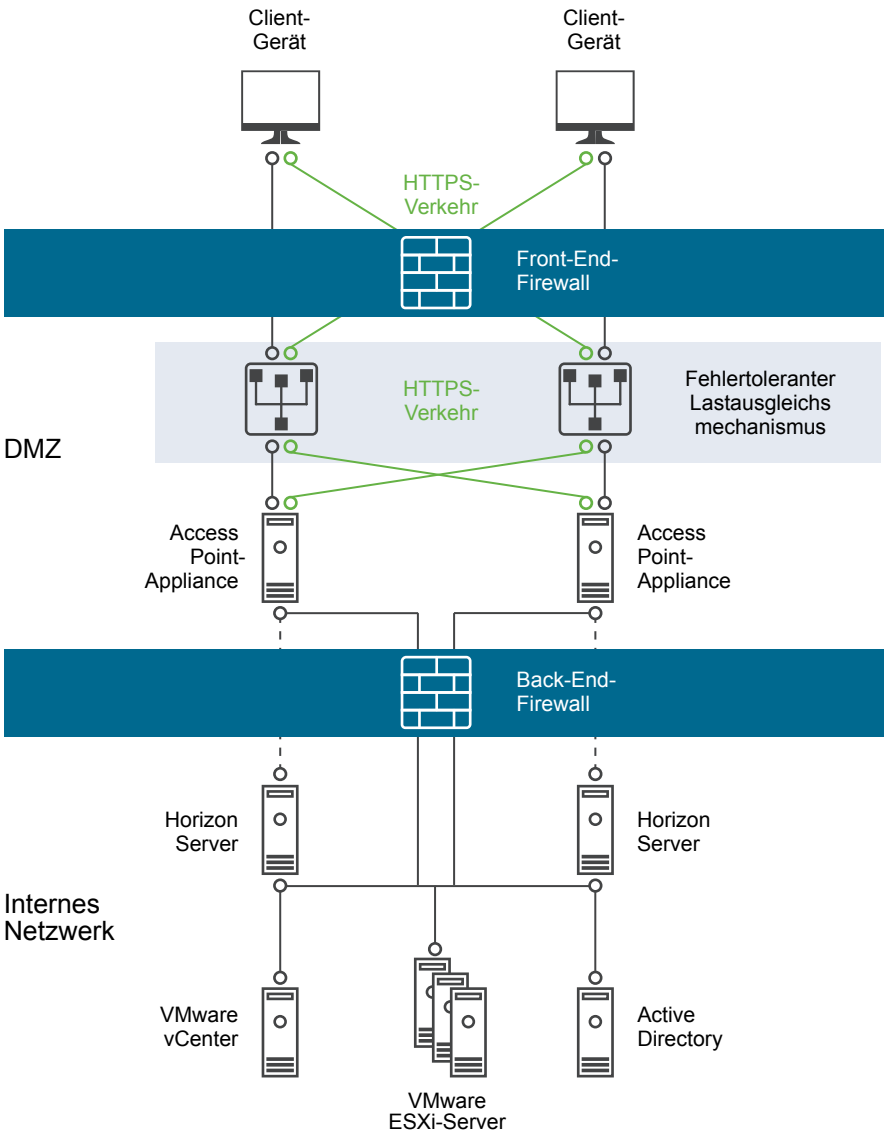
- Eine externe, dem Netzwerk vorgelagerte Front-End-Firewall ist erforderlich, um sowohl das Umkreisnetzwerk als auch das interne Netzwerk zu schützen. Diese Firewall wird so konfiguriert, dass externer Netzwerkdatenverkehr das Umkreisnetzwerk erreichen kann.
- Eine Back-End-Firewall zwischen dem Umkreisnetzwerk und dem internen Netzwerk dient zum Bereitstellen einer zweiten Schutzschicht. Diese Firewall wird so konfiguriert, dass nur Datenverkehr zugelassen wird, der von Diensten innerhalb des Umkreisnetzwerks stammt.

Mithilfe von Firewall-Richtlinien wird die von Diensten im Umkreisnetzwerk eingehende Kommunikation streng kontrolliert, wodurch das Risiko einer Gefährdung des internen Netzwerks stark vermindert wird.

Damit sich externe Clientgeräte in der DMZ mit einer Access Point-Appliance verbinden können, muss die Front-End-Firewall Datenverkehr an bestimmten Ports zulassen. Standardmäßig werden die externen Clientgeräte und externen Webclients (HTML Access) mit einer Access Point-Appliance in der DMZ an TCP-Port 443 verbunden. Wenn Sie das Blast-Protokoll verwenden, muss Port 443 in der Firewall geöffnet sein. Wenn Sie das PCOIP-Protokoll verwenden, muss Port 4172 in der Firewall geöffnet sein.

Die folgende Abbildung zeigt eine Beispielkonfiguration mit Front-End- und Back-End-Firewall.

Abbildung 1-1. Zwei-Firewall-Topologie



Access Point -Topologien für den Lastausgleich

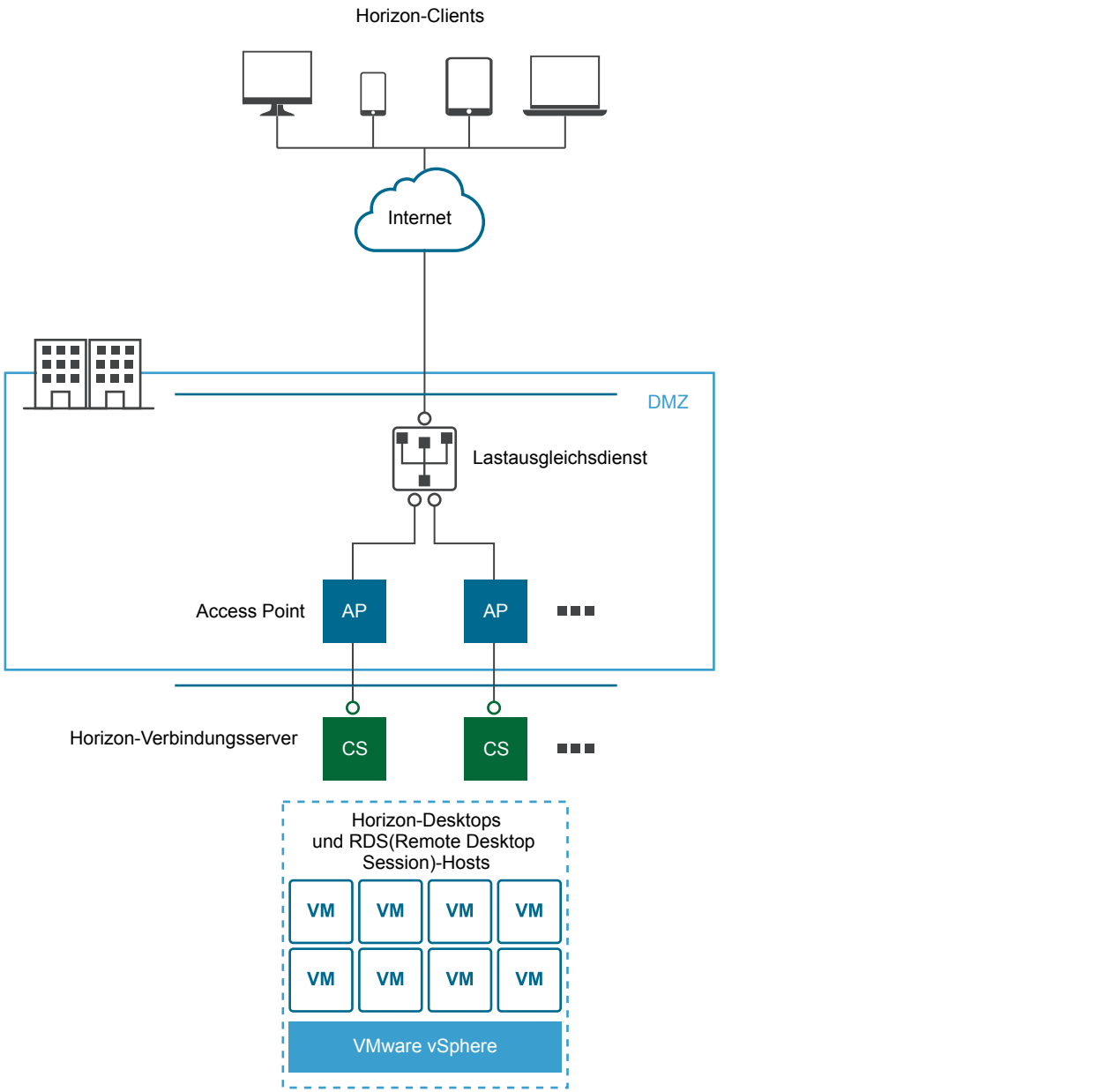
Sie können jede der verschiedenen vorhandenen Topologien implementieren.

Eine Access Point-Appliance in der DMZ kann so konfiguriert werden, dass sie entweder auf einen Server oder auf einen Lastausgleichsdienst verweist, der einer Gruppe von Servern vorgelagert ist. Access Point-Appliances können mit Standardlösungen von Drittanbietern für den Lastausgleichsdienst verwendet werden, die für HTTPS konfiguriert sind.

Wenn die Access Point-Appliance auf einen Lastausgleichsdienst verweist, der Servern vorgelagert ist, erfolgt die Auswahl der Serverinstanz dynamisch. So kann beispielsweise der Lastausgleichsdienst auf Basis der Verfügbarkeit und der Anzahl der ihm bekannten aktuellen Sitzungen auf jeder Serverinstanz eine Auswahl treffen. In der Regel verfügen die Serverinstanzen innerhalb der Unternehmens-Firewall über einen Lastausgleichsdienst zur Unterstützung des internen Zugriffs. Mit Access Point haben Sie die Möglichkeit, mit der Access Point-Appliance auf denselben Lastausgleichsdienst zu verweisen, der des öfteren bereits verwendet wird.

Stattdessen können auch eine oder mehrere Access Point-Appliances auf eine einzelne Serverinstanz verweisen. Bei beiden Vorgehensweisen verwenden Sie einen den zwei oder mehr Access Point-Appliances in der DMZ vorgelagerten Lastausgleichsdienst.

Abbildung 1-2. Mehrere Access Point-Appliances hinter einem Lastausgleichsdienst



Horizon-Protokolle

Wenn ein Horizon Client-Benutzer eine Verbindung mit einer Horizon-Umgebung herstellt, werden verschiedene Protokolle eingesetzt. Die erste Verbindung ist immer das primäre XML-API-Protokoll über HTTPS. Nach der erfolgreichen Authentifizierung werden dann sekundäre Protokolle verwendet.

- Primäres Horizon-Protokoll

  Der Benutzer gibt auf dem Horizon Client einen Hostnamen ein. Dies startet das primäre Horizon-Protokoll. Dies ist ein Steuerungsprotokoll zur Authentifizierungsautorisierung und Sitzungsverwaltung. Es verwendet XML-strukturierte Nachrichten über HTTPS (HTTP über SSL). Dieses Protokoll wird teilweise als Horizon XML-API-Steuerungsprotokoll bezeichnet. In einer Umgebung mit Lastausgleich, wie sie in der obigen Abbildung „Mehrere Access Point-Appliances hinter einem Lastausgleichsdienst“ dargestellt ist, leitet der Lastausgleichsdienst diese Verbindung an eine der Access Point-Appliances weiter. Der Lastausgleichsdienst wählt die Appliance in der Regel zuerst anhand der Verfügbarkeit aus und leitet den Datenverkehr dann an die verfügbare Appliance mit der geringsten Anzahl aktueller Sitzungen weiter. Diese Konfiguration verteilt den Datenverkehr von verschiedenen Clients gleichmäßig auf die verfügbaren Access Point-Appliances.

- Sekundäre Horizon-Protokolle

  Nachdem der Horizon Client eine sichere Kommunikation mit einer der Access Point-Appliances hergestellt hat, wird der Benutzer authentifiziert. Wenn dieser Authentifizierungsversuch erfolgreich verläuft, werden eine oder mehrere sekundäre Verbindungen vom Horizon Client hergestellt. Zu diesen sekundären Verbindungen können folgende Verbindungen gehören:

  - HTTPS-Tunnel, die zum Kapseln von TCP-Protokollen wie RDP, MMR/CDR und dem Clientframework-Kanal verwendet werden. (TCP 443).
  - Blast Extreme-Anzeigeprotokoll (TCP 443 und UDP 443).
  - PCoIP-Anzeigeprotokoll (TCP 4172 und UDP 4172).

Diese sekundären Horizon-Protokolle müssen zu derselben Access Point-Appliance weitergeleitet werden, zu der das primäre Horizon-Protokoll weitergeleitet wurde. Access Point kann die sekundären Protokolle dann auf der Grundlage der authentifizierten Benutzersitzung autorisieren. Eine wichtige Sicherheitsfunktion von Access Point besteht darin, dass Access Point nur dann Datenverkehr in das Datencenter des Unternehmens weiterleitet, wenn der Datenverkehr zu einem authentifizierten Benutzer gehört. Wenn die sekundären Protokolle fälschlicherweise an eine andere Access Point-Appliance weitergeleitet werden als die des primären Protokolls, werden sie nicht autorisiert und in die DMZ verworfen. Die Verbindung schlägt fehl. Ein falsches Routing der sekundären Protokolle ist ein häufiges Problem, wenn der Lastausgleichsdienst nicht richtig konfiguriert ist.

DMZ-Design für Access Point mit mehreren Netzwerkkarten

Access Point ist eine Sicherheits-Appliance der Schicht 7, die normalerweise in einer demilitarisierten Netzwerkzone (DMZ) installiert ist. Access Point wird verwendet, um sicherzustellen, dass nur Datenverkehr in das Datencenter des Unternehmens gelangt, der zu einem sicher authentifizierten Remotebenutzer gehört.

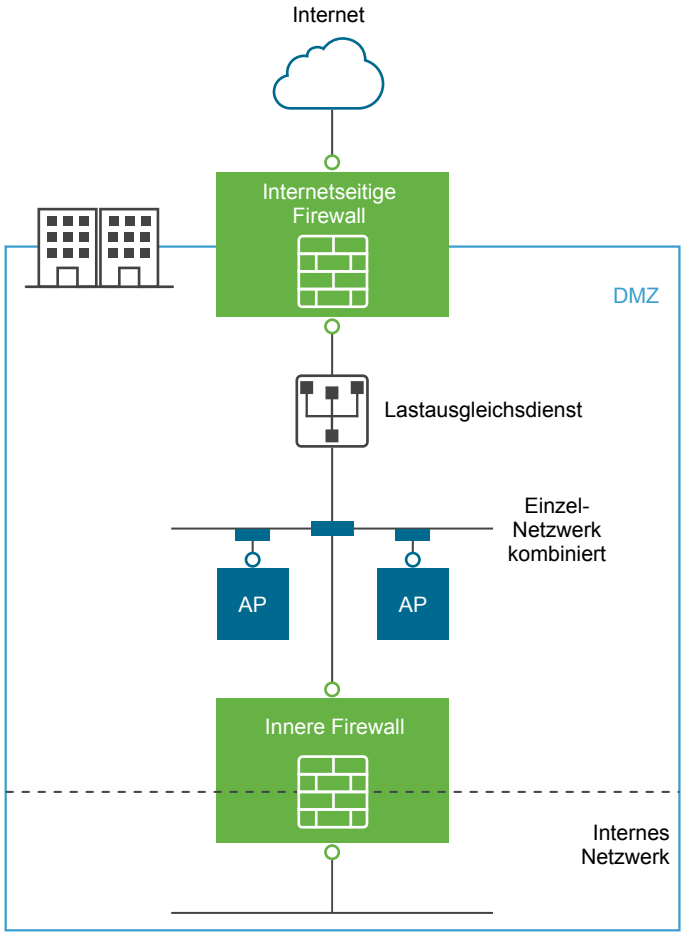
Eine der Konfigurationseinstellungen für Access Point betrifft die Anzahl der zu verwendenden virtuellen NICs (Network Interface Cards). Wenn Sie Access Point bereitstellen, wählen Sie eine Bereitstellungskonfiguration für Ihr Netzwerk aus. Sie können eine, zwei oder drei NICs festlegen, die mit „onenic“, „twonic“ oder „threenic“ angegeben werden.

Eine Verringerung der Anzahl der offenen Ports in den einzelnen virtuellen LANs und eine Trennung der verschiedenen Typen von Netzwerkdatenverkehr kann eine signifikante Verbesserung der Sicherheit bewirken. Die Vorteile ergeben sich hauptsächlich durch das Trennen und Isolieren der verschiedenen Typen von Netzwerkdatenverkehr im Zuge einer Defense-in-Depth-Sicherheitsstrategie für die DMZ. Dies kann entweder durch die Implementierung von separaten physischen Switches in der DMZ, durch mehrere virtuelle LANs in der DMZ oder durch eine vollständig durch VMware NSX verwaltete DMZ erreicht werden.

Typische DMZ-Bereitstellung mit einer NIC

Die einfachste Bereitstellung von Access Point erfolgt mit nur einer NIC, bei der der gesamte Netzwerkdatenverkehr in einem einzigen Netzwerk kombiniert ist. Datenverkehr von der Internet-seitigen Firewall wird an eine der verfügbaren Access Point-Appliances geleitet. Access Point leitet den autorisierten Datenverkehr dann durch die innere Firewall an Ressourcen im internen Netzwerk. Access Point blockiert nicht autorisierten Datenverkehr.

Abbildung 1-3. Access Point mit einer NIC

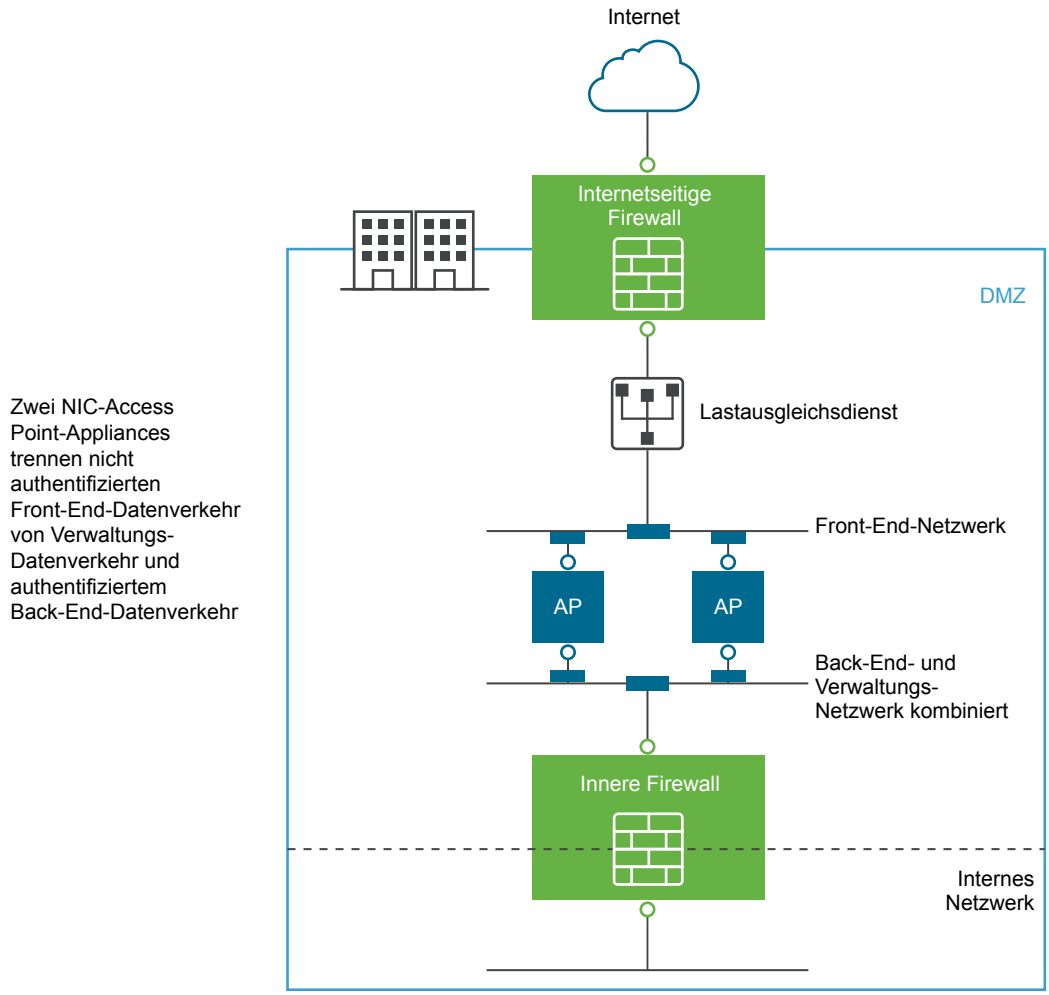


Einzel-NIC-Access Point-Appliances kombinieren Front-End-, Back-End- und Verwaltungsdatenverkehr

Trennung von nicht authentifiziertem Benutzerdatenverkehr von Back-End- und Verwaltungsdatenverkehr

Besser als eine Bereitstellung mit einer NIC ist eine Bereitstellung mit zwei NICs. Die erste NIC wird weiterhin für Internet-seitige nicht authentifizierte Zugriffe verwendet, der authentifizierte Back-End-Datenverkehr und der Verwaltungsdatenverkehr befinden sich jedoch separat in einem anderen Netzwerk.

Abbildung 1-4. Access Point mit zwei NICs



In einer Bereitstellung mit zwei NICs muss der Datenverkehr, der durch die innere Firewall in das interne Netzwerk gelangt, durch Access Point autorisiert werden. Nicht autorisierter Datenverkehr gelangt nicht in dieses Back-End-Netzwerk. Verwaltungsdatenverkehr wie die REST-API für Access Point befindet sich ausschließlich in diesem zweiten Netzwerk.

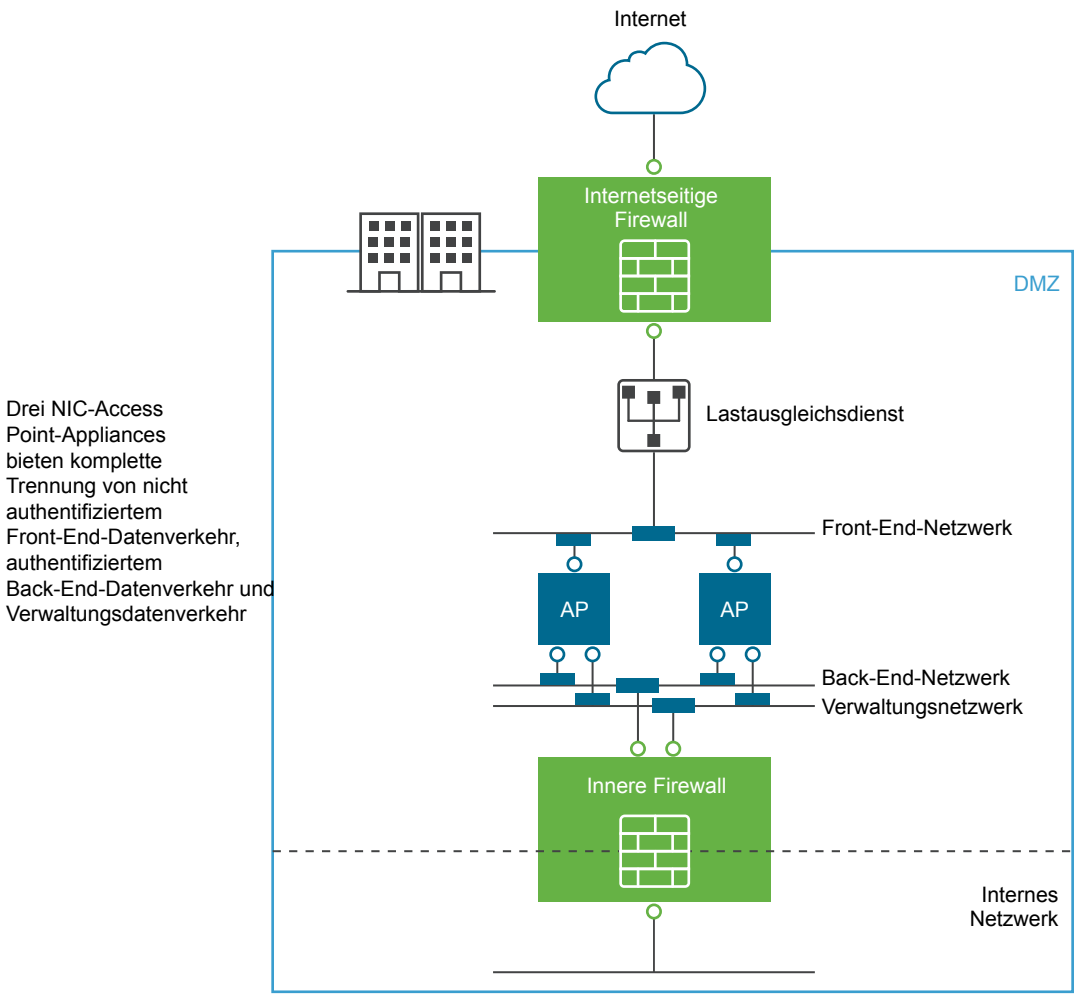
Wenn ein Gerät, z. B. der Lastausgleichsdienst, im nicht authentifizierten Front-End-Netzwerk kompromittiert wurde, dann ist es in einer Bereitstellung mit zwei NICs nicht möglich, das Gerät so umzukonfigurieren, dass Access Point umgangen wird. Firewall-Regeln der Schicht 4 sind mit der Access Point-Sicherheit der Schicht 7 kombiniert. Ähnlich verhält es sich, wenn die Internet-seitige Firewall dahingehend falsch konfiguriert wurde, dass TCP-Port 9443 geöffnet ist. In diesem Fall wird die REST-API für die Verwaltung von Access Point nicht für Internetbenutzer verfügbar. Bei einem Defense-in-Depth-Prinzip kommen mehrere Sicherheitsstufen zum Einsatz, wodurch ein einzelner Konfigurationsfehler oder Systemangriff nicht zwingend zu einer allgemeinen Gefährdung führt.

In einer Bereitstellung mit zwei NICs befinden sich zusätzliche Infrastruktursysteme, wie DNS-Server oder RSA SecurID-Authentifizierungsmanager-Server in der Regel im Back-End-Netzwerk innerhalb der DMZ, sodass diese Server im Internet-seitigen Netzwerk nicht sichtbar sind. Wenn sich Infrastruktursysteme in der DMZ befinden, schützt dies vor Angriffen der Schicht 2, die aus dem Internet-seitigen LAN von einem kompromittierten Front-End-System stammen, und sorgt für eine effektive Verringerung der Gesamtangriffsfläche.

Der größte Teil des Access Point-Netzwerkdatenverkehrs betrifft die Anzeigeprotokolle für Blast und PCoIP. Mit einer einzigen NIC wird der Anzeigeprotokolldatenverkehr in das und aus dem Internet mit dem Datenverkehr in die und aus den Back-End-Systemen kombiniert. Wenn zwei oder mehr NICs verwendet werden, wird der Datenverkehr auf die Front-End- und Back-End-NICs und -Netzwerke verteilt. Dies beseitigt den potenziellen Engpass einer einzigen NIC und bietet Leistungsvorteile.

Access Point unterstützt eine weitere Trennung, indem auch der Verwaltungsdatenverkehr in ein spezifisches Verwaltungs-LAN verlagert werden kann. HTTPS-Verwaltungsdatenverkehr an Port 9443 kann dann nur aus dem Verwaltungs-LAN stammen.

Abbildung 1-5. Access Point mit drei NICs



Bereitstellen der Access Point - Appliance 2

Access Point wird als OVF-Paket geliefert und auf einem vSphere ESX- oder ESXi-Host als vorkonfigurierte virtuelle Appliance bereitgestellt.

Für die Installation der Access Point-Appliance können zwei Verfahren genutzt werden.

- Die Access Point-OVF-Vorlage kann mit dem vSphere Client oder dem vSphere Web Client bereitgestellt werden. Sie werden aufgefordert, die grundlegenden Einstellungen vorzunehmen, wie die Konfiguration der NIC-Bereitstellung, die IP-Adresse und die Kennwörter der Verwaltungsoberfläche. Melden Sie sich nach der OVF-Bereitstellung bei der Access Point-Verwaltungsoberfläche an, um die Access Point-Systemeinstellungen zu konfigurieren, die sicheren Edgedienste für mehrere Anwendungsfälle einzurichten und die Authentifizierung in der DMZ zu konfigurieren. Siehe Bereitstellen von Access Point mit dem OVF-Vorlagenassistenten.
- PowerShell-Skripte können eingesetzt werden, um Access Point bereitzustellen und die sicheren Edgedienste für mehrere Anwendungsfälle einzurichten. Laden Sie die ZIP-Datei herunter, konfigurieren Sie das PowerShell-Skript für Ihre Umgebung und führen Sie das Skript aus, um Access Point bereitzustellen. Siehe Verwenden von PowerShell zur Bereitstellung der Access Point-Appliance.

Dieses Kapitel behandelt die folgenden Themen:

- Bereitstellen von Access Point mit dem OVF-Vorlagenassistenten
- Konfigurieren von Access Point auf den Verwaltungsseiten für die Konfiguration
- Aktualisieren von signierten SSL-Serverzertifikaten

Bereitstellen von Access Point mit dem OVF-Vorlagenassistenten

Um Access Point bereitzustellen, müssen Sie die OVF-Vorlage mit dem vSphere Client oder dem vSphere Web Client bereitstellen, die Appliance einschalten und die Einstellungen konfigurieren.

Nachdem Access Point bereitgestellt wurde, richten Sie in der Verwaltungsoberfläche die Access Point-Umgebung ein und konfigurieren die Desktop- und Anwendungsressourcen und die Authentifizierungsmethoden, die in der DMZ verwendet werden.

Bereitstellungseigenschaften für Access Point

Wenn Sie OVF bereitstellen, konfigurieren Sie, wie viele Netzwerkschnittstellen (NIC) erforderlich sind und legen die IP-Adresse und das Administratorkennwort fest. Die übrigen Bereitstellungseigenschaften können auf den Access Point-Verwaltungsseiten festgelegt werden.

Tabelle 2-1. Bereitstellungsoptionen Access Point

Bereitstellungseigenschaft	Beschreibung
Bereitstellungskonfiguration	Legt fest, wie viele Netzwerkschnittstellen in der virtuellen Access Point-Maschine verfügbar sind. Standardmäßig ist diese Eigenschaft nicht festgelegt, d. h. es wird nur ein NIC (Network Interface Controller) verwendet.
Externe IP-Adresse (Verbindung über das Internet)	(Erforderlich) Legt die für den Zugriff auf diese virtuelle Maschine über das Internet verwendete IPv4- oder IPv6-Adresse fest. **Hinweis** Der Computername wird über eine DNS-Abfrage dieser Internet-IPv4- oder IPv6-Adresse festgelegt. Standardeinstellung: keine.
IP-Adresse des Verwaltungsnetzwerks	Legt die IP-Adresse der mit dem Verwaltungsnetzwerk verbundenen Schnittstelle fest. Wird diese nicht konfiguriert, erfolgt die Verbindung mit dem Verwaltungsserver über die Schnittstelle zum Internet. Standardeinstellung: keine.
IP-Adresse des Backend-Netzwerks	Legt die IP-Adresse der mit dem Backend-Netzwerk verbundenen Schnittstelle fest. Wird diese nicht konfiguriert, wird der zu den Backend-Systemen gesendete Netzwerkverkehr über andere Netzwerkschnittstellen geleitet. Standardeinstellung: keine.
DNS-Server-Adressen	(Erforderlich) Gibt eine oder mehrere durch Leerzeichen getrennte IPv4-Adressen des DNS-Servers für diese virtuelle Maschine an (Beispiel: 192.0.2.1 192.0.2.2). Sie können bis zu drei Server festlegen. Standardmäßig ist diese Eigenschaft nicht festgelegt, d. h. das System verwendet den DNS-Server, der dem mit dem Internet verbundenen NIC zugewiesen ist. **Vorsicht** Wird diese Option leer gelassen und ist dem mit dem Internet verbundenen NIC kein DNS-Server zugewiesen, wird die Appliance nicht korrekt bereitgestellt.
Kennwort für den Root-Benutzer	(Erforderlich) Legt das Kennwort für den Root-Benutzer dieser virtuellen Maschine fest. Beim Kennwort muss es sich um ein gültiges Linux-Kennwort handeln. Standardeinstellung: keine.
Kennwort für den Administratorbenutzer	(Erforderlich) Ohne Festlegung dieses Kennworts können Sie nicht auf die Verwaltungskonsole und die REST-API der Access Point-Appliance zugreifen. Kennwörter müssen mindestens acht Zeichen lang sein und mindestens einen Groß- sowie einen Kleinbuchstaben enthalten, eine Ziffer und ein Sonderzeichen enthalten. Zulässige Sonderzeichen sind ! @ # $ % * ( ). Standardeinstellung: keine.

Tabelle 2-1. Bereitstellungsoptionen Access Point (Fortsetzung)

Bereitstellungseigenschaft	Beschreibung
Gebietsschema für lokalisierte Meldungen	(Erforderlich) Legt das Gebietsschema für die Ausgabe von Fehlermeldungen fest. ■ **en_US** für Englisch ■ **ja_JP** für Japanisch ■ **fr_FR** für Französisch ■ **de_DE** für Deutsch ■ **zh_CN** für Vereinfachtes Chinesisch ■ **zh_TW** für Traditionelles Chinesisch ■ **ko_KR** für Koreanisch Standardeinstellung: en_US.
Syslog-Server-URL	Legt den für die Protokollierung von Access Point-Ereignissen verwendeten Syslog-Server fest. Bei diesem Wert kann es sich um eine URL, um einen Hostnamen oder um eine IP-Adresse handeln. Das Schema und die Portnummer sind optional (Beispiel: syslog://server.example.com:514). Standardmäßig ist diese Eigenschaft nicht festgelegt, d. h., es werden keine Ereignisse auf einem Syslog-Server protokolliert.

Bereitstellen von Access Point mit dem OVF-Vorlagenassistenten

Sie können die Access Point-Appliance bereitstellen, indem Sie sich in vCenter Server anmelden und den Assistenten zum Bereitstellen von OVF-Vorlagen verwenden.

Hinweis Wenn Sie den vSphere Web Client verwenden, um OVF bereitzustellen, müssen Sie auch den DNS-Server, das Gateway und die Netzmaskenadressen für jedes Netzwerk angeben. Bei Verwendung des nativen vSphere Client müssen Sie sicherstellen, dass jedem Netzwerk ein IP-Pool zugewiesen wurde. Um einen IP-Pool in vCenter Server hinzuzufügen, wenn Sie den systemeigenen vSphere Client verwenden, wechseln Sie zur Registerkarte „IP-Pools“ des Datencenters. Wenn Sie alternativ dazu den vSphere Web Client verwenden, können Sie ein Netzwerkprotokollprofil erstellen. Wechseln Sie zur Registerkarte „Verwalten“ des Datencenters und wählen Sie die Registerkarte „Netzwerkprotokollprofile“ aus.

Voraussetzungen

- Machen Sie sich mit den Bereitstellungsoptionen im Assistenten vertraut. Siehe System- und Netzwerkanforderungen von Access Point.
- Legen Sie fest, wie viele Netzwerkschnittstellen und statische IP-Adressen für die Access Point-Appliance konfiguriert werden sollen. Siehe Anforderungen an die Netzwerkkonfiguration.
- Laden Sie die `.ova`-Installationsdatei für die Access Point-Appliance von dieser VMware Website herunter: https://my.vmware.com/web/vmware/downloads. Oder geben Sie die URL an, die Sie verwenden möchten (Beispiel: `http://example.com/vapps/euc-access-point-`*`Y.Y`*`.0.0-`*`xxxxxxx`*`_OVF10.ova`), wobei *Y.Y* die Versionsnummer ist und *xxxxxxx* die Build-Nummer.

Vorgehensweise

1 Melden Sie sich mit dem nativen vSphere Client oder vSphere Web Client bei einer vCenter Server-Instanz an.

Für ein IPv4-Netzwerk verwenden Sie den nativen vSphere Client oder den vSphere Web Client. Für ein IPv6-Netzwerk verwenden Sie den vSphere Web Client.

2 Wählen Sie einen Menübefehl für den Start des Assistenten zum Bereitstellen von OVF-Vorlagen aus.

Option	Menübefehl
vSphere Client	Wählen Sie **Datei > OVF-Vorlage bereitstellen**.
vSphere Web Client	Wählen Sie ein Bestandslistenobjekt aus, das ein gültiges übergeordnetes Objekt einer virtuellen Maschine ist, z. B. ein Datencenter, einen Ordner, Cluster, Ressourcenpool oder Host, und wählen Sie aus dem Menü **Aktionen** die Option **OVF-Vorlage bereitstellen** aus.

3 Gehen Sie auf der Seite „Quelle auswählen“ des Bereitstellungsassistenten zum Ort der `.ova`-Datei, die Sie heruntergeladen haben, oder geben Sie eine URL ein und klicken Sie auf **Weiter**.

Die Seite mit den Details wird geöffnet. Überprüfen Sie die Produktdetails, Version und Größenanforderungen.

4 Folgen Sie den Aufforderungen des Assistenten und beachten Sie die folgenden Anleitungen für den Abschluss des Assistenten.

Option	Beschreibung
Eine Bereitstellungskonfiguration auswählen	Für ein IPv4-Netzwerk können Sie eine, zwei oder drei Netzwerkschnittstellen (NICs) verwenden. Für ein IPv6-Netzwerk verwenden Sie drei Netzwerkschnittstellen (NICs). Access Point erfordert eine eigene statische IP-Adresse für jede NIC. Viele DMZ-Implementierungen verwenden getrennte Netzwerke zur Sicherung der verschiedenen Datenverkehrstypen. Konfigurieren Sie Access Point entsprechend dem Netzwerkdesign der DMZ, in der die Bereitstellung erfolgt.
Festplattenformat	Für Evaluierungs- und Testumgebungen wählen Sie das Format für eine schlanke Speicherzuweisung („Thin Provisioning“). Für Produktionsumgebungen wählen Sie eines der Formate für eine starke Speicherzuweisung („Thick Provisioning“). „Thick Provision Eager Zeroed“ ist ein Typ eines Thick-Formats virtueller Festplatten, das Clustering-Funktionen wie die Fehlertoleranz unterstützt, aber sehr viel mehr Zeit benötigt, um andere Typen virtueller Festplatten zu erstellen.
VM-Speicherrichtlinie	(Nur vSphere Web Client) Diese Option ist verfügbar, wenn Speicherrichtlinien auf der Zielressource aktiviert wurden.

Option	Beschreibung
Einrichten von Netzwerken/Netzwerkzuordnung	Wenn Sie vSphere Web Client verwenden, können Sie auf der Seite „Netzwerke einrichten“ jede Netzwerkschnittstelle (NIC) einem Netzwerk zuordnen und die Protokolleinstellungen festlegen. a Wählen Sie in der Dropdown-Liste **IP-Protokoll** IPv4 oder IPv6 aus. b Wählen Sie die erste Zeile in der Tabelle **Internet** aus und klicken Sie dann auf den Abwärtspfeil, um das Zielnetzwerk auszuwählen. Wenn Sie als IP-Protokoll IPv6 ausgewählt haben, müssen Sie das Netzwerk mit IPv6-Funktion auswählen. Nach der Auswahl der Zeile können Sie auch die IP-Adressen für den DNS-Server, das Gateway und die Netzmaske im unteren Fensterabschnitt eingeben. c Wenn Sie mehr als eine NIC verwenden, wählen Sie die nächste Zeile **ManagementNetwork** und anschließend das Zielnetzwerk aus. Dann können Sie die IP-Adressen für den DNS-Server, das Gateway und die Netzmaske für dieses Netzwerk eingeben. Wenn Sie nur eine NIC verwenden, werden alle Zeilen demselben Netzwerk zugeordnet. d Wenn Sie über eine dritte NIC verfügen, müssen Sie auch die dritte Zeile auswählen und die Einstellungen vornehmen. Wenn Sie nur zwei NICs verwenden, wählen Sie für die dritte Zeile **BackendNetwork** dasselbe Netzwerk aus, das Sie bereits für **ManagementNetwork** verwendet haben. Beim vSphere Web Client wird automatisch eine Netzwerkprotokolldatei erstellt, nachdem Sie den Assistenten abgeschlossen haben, falls keine solche existiert. Wenn Sie den systemeigenen vSphere Client (anstelle von Web Client) verwenden, können Sie auf der Seite „Netzwerkzuordnung“ jede NIC einem Netzwerk zuordnen. Es gibt dort jedoch keine Felder zur Angabe der Adressen für den DNS-Server, das Gateway und die Netzmaske. Wie bei den Voraussetzungen beschrieben wurde, müssen Sie bereits jedem Netzwerk einen IP-Pool zugewiesen oder ein Netzwerkprotokollprofil erstellt haben.
Eigenschaftenvorlage personalisieren	Die Textfelder auf der Eigenschaftenseite sind speziell für Access Point vorgesehen und für andere Typen von virtuellen Appliances möglicherweise nicht erforderlich. Der Text auf der Seite des Assistenten erläutert jede Einstellung. Wird der Text auf der rechten Seite des Assistenten abgeschnitten, vergrößern Sie das Fenster durch Ziehen an der Ecke rechts unten. Sie müssen Werte in die folgenden Textfelder eingeben: ■ **IPMode:STATICV4/STATICV6**. Wenn Sie STATICV4 eingeben, müssen Sie für die NIC die IPv4-Adresse angeben. Wenn Sie STATICV6 eingeben, müssen Sie für die NIC die IPv6-Adresse angeben. ■ **Kommagetrennte Liste mit weitergegebenen Regeln im Formular {tcp|udp}/listening-port-number/destination-ip-address:destination-port-nu** ■ **NIC 1 (ETH0) IPv4-Adresse**. Geben Sie die IPv4-Adresse für die NIC ein, wenn Sie für den NIC-Modus STATICV4 festgelegt haben. ■ **Kommagetrennte Liste mit benutzerdefinierten IPv4-Routen für NIC 1 (eth0) im Formular ipv4-network-address/bits.ipv4-gateway-address** ■ **IPv6-Adresse**. Geben Sie die IPv6-Adresse für die NIC ein, wenn Sie für den NIC-Modus STATICV6 festgelegt haben. ■ **DNS-Server-Adressen**. Geben Sie IPv4- oder IPv6-Adressen des Domänennamensservers für die VM ein. Trennen Sie diese jeweils durch Leerzeichen.

Option	Beschreibung
	■ **IP-Adresse des Verwaltungsnetzwerks**, wenn Sie 2 NICs angegeben haben, und **IP-Adresse des Backend-Netzwerks**, wenn Sie 3 NICs angegeben haben ■ **Kennwortoptionen**. Geben Sie das Kennwort für den Root-Benutzer dieser VM und das Kennwort für den Administratorbenutzer ein, der auf die Verwaltungskonsole zugreift und den REST-API-Zugriff aktiviert. Alle anderen Einstellungen sind entweder optional oder bereits mit einer Standardeinstellung vorausgefüllt. Beachten Sie dabei die Kennwortanforderungen, die auf der Assistentenseite aufgelistet sind. Beschreibungen aller Bereitstellungseigenschaften finden Sie unter Bereitstellungseigenschaften für Access Point.

5 Auf der Seite „Bereit zum Abschließen“ wählen Sie **Nach Bereitstellung einschalten** aus und klicken Sie auf **Fertig stellen**.

Im Statusbereich von vCenter Server wird eine Aufgabe für den Assistenten zum Bereitstellen von OVF-Vorlagen zur Überwachung der Bereitstellung angezeigt. Sie haben auch die Möglichkeit, auf der virtuellen Maschine eine Konsole zur Darstellung der Konsolenmeldungen zu öffnen, die während des Systemstarts eingeblendet werden. Ein Protokoll dieser Meldungen ist auch in der Datei `/var/log/boot.msg` verfügbar.

6 Wenn die Bereitstellung abgeschlossen ist, müssen Sie sich vergewissern, dass Endbenutzer mit der Appliance durch Öffnen eines Browsers und Eingabe der folgenden URL eine Verbindung herstellen können.

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

In dieser URL ist *FQDN-of-AP-appliance* der durch das DNS auflösbare, vollqualifizierte Domänenname (FQDN) der Access Point-Appliance.

Wenn die Bereitstellung erfolgreich war, erscheint die bereitgestellte Webseite des Servers, auf den Access Point verweist. War die Bereitstellung nicht erfolgreich, können Sie die virtuelle Appliance-Maschine löschen und die Appliance erneut bereitstellen. Der häufigste Fehler ist die falsche Eingabe von Zertifikatfingerabdrücken.

Die Access Point-Appliance ist bereitgestellt und startet automatisch.

Weiter

Melden Sie sich bei der Administratorbenutzeroberfläche von Access Point an und konfigurieren Sie die Desktop- und Anwendungsressourcen, um den Remote-Zugriff aus dem Internet über Access Point und die in der DMZ verwendeten Authentifizierungsmethoden zuzulassen. Die URL der Verwaltungskonsole hat das Format `https://<mycoAccessPointappliance.com:9443/admin/index.html`.

Konfigurieren von Access Point auf den Verwaltungsseiten für die Konfiguration

Melden Sie sich nach der Bereitstellung des OVF-Pakets und dem Einschalten der Access Point-Appliance bei der Access Point-Verwaltungsoberfläche an, um die folgenden Einstellungen zu konfigurieren.

- Access Point-Systemkonfiguration und SSL-Serverzertifikat.
- Edgediensteinstellungen für Horizon, Reverse-Proxy, App-spezifische Tunnel und Proxy-Einstellungen für AirWatch.
- Authentifizierungseinstellungen für RSA SecurID, RADIUS, X.509-Zertifikat und adaptive RSA-Authentifizierung.
- Einstellungen für SAML-Identitätsanbieter und -Dienstanbieter.

Auf den Konfigurationsseiten haben Sie Zugriff auf die folgenden Optionen.

- Herunterladen der Access Point-Protokolldateien als ZIP-Dateien.
- Exportieren der Access Point-Einstellungen zum Abrufen der Konfigurationseinstellungen.
- Importieren der Access Point-Einstellungen zum Erstellen und Aktualisieren der gesamten Access Point-Konfiguration.

Konfigurieren der Access Point-Systemeinstellungen

Auf den Verwaltungsseiten können Sie konfigurieren, welche Sicherheitsprotokolle und kryptographischen Algorithmen zur Verschlüsselung der Kommunikation zwischen Clients und der Access Point-Appliance verwendet werden.

Die Access Point URL der Admin-Benutzeroberfläche ist im Format `https://<mycoAccessPointappliance.com>:9443/admin/index.html`. Geben Sie zum Anmelden den Administratorbenutzernamen und das Administratorkennwort ein, die Sie bei der Bereitstellung des OVF konfiguriert haben.

Voraussetzungen

- Überprüfen Sie die Access Point-Bereitstellungseigenschaften. Die folgenden Informationen sind erforderlich
  - Statische IP-Adresse für die Access Point-Appliance
  - IP-Adresse des DNS-Servers
  - Kennwort für die Verwaltungskonsole
  - URL der Serverinstanz des Lastausgleichsdienstes, auf den die Access Point-Appliance verweist
  - Syslog-Server-URL für das Speichern der Ereignisprotokolldateien

Vorgehensweise

1 Klicken Sie auf der Verwaltungsoberfläche im Bereich „Manuell konfigurieren“ auf **Auswählen**.

2 Klicken Sie im Bereich „Erweiterte Einstellungen“ auf das Zahnradsymbol für die **Systemkonfiguration**.

3 Bearbeiten Sie die folgenden Konfigurationswerte für die Access Point-Appliance.

Option	Standardwert und Beschreibung
Gebietsschema	Legt das Gebietsschema für die Ausgabe von Fehlermeldungen fest. ■ **`en_US`** für Englisch ■ **`ja_JP`** für Japanisch ■ **`fr_FR`** für Französisch ■ **`de_DE`** für Deutsch ■ **`zh_CN`** für Vereinfachtes Chinesisch ■ **`zh_TW`** für Traditionelles Chinesisch ■ **`ko_KR`** für Koreanisch
Administratorkennwort	Dieses Kennwort wurde bei der Bereitstellung der Appliance festgelegt. Sie können es zurücksetzen. Kennwörter müssen mindestens acht Zeichen lang sein und mindestens einen Groß- sowie einen Kleinbuchstaben enthalten, eine Ziffer und ein Sonderzeichen enthalten. Zulässige Sonderzeichen sind ! @ # $ % * ( ).
Cipher Suites	In den meisten Fällen ist es nicht erforderlich, die Standardeinstellungen zu ändern. Dies sind die kryptographischen Algorithmen, mit denen die Kommunikation zwischen Clients und der Access Point-Appliance verschlüsselt wird. Mit den Verschlüsselungseinstellungen werden verschiedene Sicherheitsprotokolle aktiviert.
Cipher-Reihenfolge beachten	Die Standardeinstellung ist NEIN. Wählen Sie **JA** aus, um die Beachtung der Reihenfolge der TLS-Cipher-Liste zu aktivieren.
SSL 3.0 aktiviert	Die Standardeinstellung ist NEIN. Wählen Sie **JA** aus, um das Sicherheitsprotokoll SSL 3.0 zu aktivieren.
TLS 1.0 aktiviert	Die Standardeinstellung ist NEIN. Wählen Sie **JA** aus, um das Sicherheitsprotokoll TLS 1.0 zu aktivieren.
TLS 1.1 aktiviert	Die Standardeinstellung ist JA. Das Sicherheitsprotokoll TLS 1.1 ist aktiviert.
TLS 1.2 aktiviert	Die Standardeinstellung ist JA. Das Sicherheitsprotokoll TLS 1.2 ist aktiviert.
Syslog-URL	Geben Sie die Syslog-Server-URL ein, die für die Protokollierung von Access Point-Ereignissen verwendet wird. Bei diesem Wert kann es sich um eine URL, um einen Hostnamen oder um eine IP-Adresse handeln. Wenn Sie keine Syslog-Server-URL angeben, werden keine Ereignisse protokolliert. Geben Sie diese in folgender Form ein: `syslog://server.example.com:514`.
URL für Integritätsprüfung	Geben Sie eine URL ein, mit der der Lastausgleichsdienst eine Verbindung herstellt und den Zustand von Access Point überprüft.
Cookies für Zwischenspeicherung	Der Satz Cookies, den Access Point zwischenspeichert. Der Standardwert ist „keine“.
IP-Modus	Wählen Sie den statischen IP-Modus aus, entweder STATICV4 oder STATICV6.
Zeitüberschreitung der Sitzung	Der Standardwert ist **36000000** Millisekunden.
Stilllegungsmodus	Aktivieren Sie **JA**, um die Access Point-Appliance anzuhalten, damit ein konsistenter Zustand für Wartungsaufgaben erreicht wird
Überwachungsintervall	Der Standardwert ist **60**.

4 Klicken Sie auf **Speichern**.

Weiter

Konfigurieren Sie die Edgediensteinstellungen für die Komponenten, mit denen Access Point bereitgestellt ist. Konfigurieren Sie nach den Edgeeinstellungen die Authentifizierungseinstellungen.

Aktualisieren von signierten SSL-Serverzertifikaten

Sie können Ihre signierten Zertifikate bei Ablauf ersetzen.

Für Produktionsumgebungen empfiehlt VMware ausdrücklich, das Standardzertifikat so schnell wie möglich zu ersetzen. Das Standard-TLS/SSL-Serverzertifikat, das bei der Bereitstellung einer Access Point-Appliance generiert wird, ist nicht von einer vertrauenswürdigen Zertifizierungsstelle signiert.

Voraussetzungen

- Das neue signierte Zertifikat und der private Schlüssel sind auf einem Computer gespeichert, auf den Sie Zugriff haben.
- Konvertieren Sie das Zertifikat in PEM-Dateien und diese .pem-Dateien dann in ein einzeiliges Format. Siehe „Konvertieren von Zertifikatdateien in das einzeilige PEM-Format“

Vorgehensweise

1. Klicken Sie in der Verwaltungskonsole auf **Auswählen**.
2. Klicken Sie im Bereich „Erweiterte Einstellungen“ auf das Zahnradsymbol für die Einstellungen des SSL-Serverzertifikats.
3. Klicken Sie in der Zeile des privaten Schlüssels auf **Auswählen** und suchen Sie nach der Datei mit dem privaten Schlüssel.
4. Klicken Sie auf **Öffnen**, um die Datei hochzuladen.
5. Klicken Sie in der Zeile der Zertifikatkette auf „Auswählen“ und suchen Sie nach der Datei der Zertifikatkette.
6. Klicken Sie auf **Öffnen**, um die Datei hochzuladen.
7. Klicken Sie auf **Speichern**.

Weiter

Wenn die Zertifizierungsstelle, die das Zertifikat erstellt hat, nicht bekannt ist, konfigurieren Sie Clients so, dass sie dem Stammzertifikat und den Zwischenzertifikaten vertrauen.

Verwenden von PowerShell zur Bereitstellung von Access Point 3

Access Point kann über ein PowerShell-Skript bereitgestellt werden. Das PowerShell-Skript wird als Musterskript geliefert, das Sie für Ihre Umgebung anpassen können.

Wenn Sie das PowerShell-Skript verwenden, um Access Point bereitzustellen, ruft das Skript das OVF-Tool auf und validiert die Einstellungen, um automatisch die korrekte Befehlszeilensyntax zu erzeugen. Diese Methode ermöglicht auch erweiterte Einstellungen wie die Konfiguration des TLS/SSL-Serverzertifikats, das während der Bereitstellung angewendet werden soll.

Dieses Kapitel behandelt die folgenden Themen:

- Systemanforderungen zur Bereitstellung von Access Point mit PowerShell
- Verwenden von PowerShell zur Bereitstellung der Access Point-Appliance

Systemanforderungen zur Bereitstellung von Access Point mit PowerShell

Um Access Point mit dem PowerShell-Skript bereitzustellen, müssen Sie bestimmte Versionen von VMware-Produkten verwenden.

- vSphere ESX-Host mit einem vCenter Server.
- Das PowerShell-Skript kann auf Computern mit Windows 8.1 oder höher bzw. Windows Server 2008 R2 oder höher ausgeführt werden.

  Der Computer kann auch ein vCenter Server sein, der unter Windows ausgeführt wird, oder ein separater Windows-Computer.
- VMware OVF Tool muss auf dem Windows-Computer installiert sein, auf dem das Skript ausgeführt wird.

  Installieren Sie OVF Tool 4.0.1 oder höher von https://www.vmware.com/support/developer/ovf/.

Sie müssen den vSphere-Datenspeicher und das zu verwendende Netzwerk auswählen.

Ein vSphere-Netzwerkprotokollprofil muss mit jedem referenzierten Netzwerknamen verknüpft sein. Dieses Netzwerkprotokollprofil gibt Netzwerkeinstellungen wie IPv4-Subnetzmaske, Gateway usw. an. Diese Werte werden bei der Bereitstellung von Access Point eingesetzt. Achten Sie also darauf, dass die Werte korrekt sind.

Verwenden von PowerShell zur Bereitstellung der Access Point -Appliance

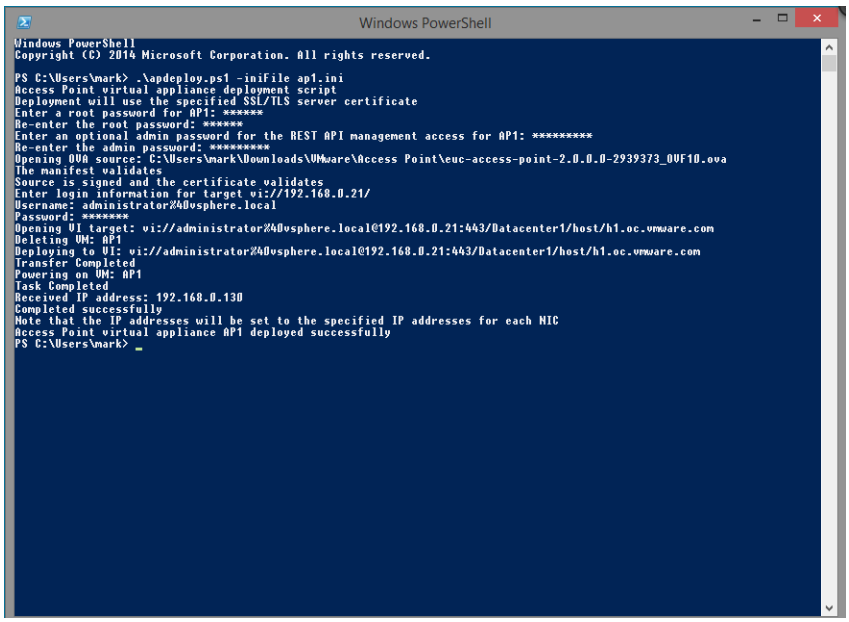
Anhand von PowerShell-Skripten können Sie die Umgebung mit allen Konfigurationseinstellungen einrichten. Wenn Sie das PowerShell-Skript zum Bereitstellen von Access Point ausführen, kann die Lösung schon beim ersten Systemstart in der Produktion eingesetzt werden.

Voraussetzungen

- Stellen Sie sicher, dass die Systemanforderungen erfüllt sind.

  Dies ist ein Beispielskript zum Bereitstellen von Access Point in Ihrer Umgebung.

  Abbildung 3-1. PowerShell-Beispielskript



Vorgehensweise

1. Laden Sie die Access Point-OVA-Datei von My VMware auf Ihren Windows-Computer herunter.
2. Laden Sie die ap-deploy-XXX.zip-Dateien in einen Ordner auf dem Windows-Computer herunter.

   Sie finden die ZIP-Dateien unter https://communities.vmware.com/docs/DOC-30835.
3. Öffnen Sie ein PowerShell-Skript und ändern Sie das Verzeichnis in den Speicherort des Skripts.

4 Erstellen Sie eine .INI-Konfigurationsdatei für die virtuelle Access Point-Appliance.

Beispiel: Stellen Sie eine neue Access Point-Appliance AP1 bereit. Die Konfigurationsdatei hat den Namen ap1.ini. Diese Datei enthält alle Konfigurationseinstellungen für AP1. Sie können mit den Beispiel-INI-Dateien in der Datei apdeploy.zip die .INI-Datei erstellen und die Einstellungen entsprechend ändern.

Hinweis Sie können eindeutige .INI-Dateien für mehrere Access Point-Bereitstellungen in Ihrer Umgebung verwenden. Um mehrere Appliances bereitzustellen, müssen Sie die IP-Adressen und die Namensparameter in der .INI-Datei entsprechend ändern.

Beispiel für die anzupassende .INI-Datei.

```
name=AP1
source=C:\APs\euc-access-point-2.8.0.0-000000000_OVF10.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, proxyDEstinationUrl=[fc00:10:112:54::220]
```

5 Geben Sie den PowerShell-Befehl „set-executionpolicy“ ein, um eine erfolgreiche Ausführung des Skripts sicherzustellen.

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

Führen Sie diesen Befehl einmal aus und nur dann, wenn die Ausführung derzeit eingeschränkt ist.

Wenn eine Warnung für das Skript angezeigt wird, führen Sie diesen Befehl aus, um die Warnung aufzuheben:

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

6 Führen Sie den Befehl aus, um die Bereitstellung zu starten. Wenn Sie die .INI-Datei nicht angeben, verwendet das Skript standardmäßig ap.ini.

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

7 Geben Sie die Anmeldedaten ein, wenn Sie dazu aufgefordert werden, und schließen Sie das Skript ab.

Hinweis Wenn Sie aufgefordert werden, den Fingerabdruck für den Zielcomputer hinzuzufügen, geben Sie **Ja** ein.

Die Access Point-Appliance ist bereitgestellt und kann in der Produktion eingesetzt werden.

Weitere Informationen zu PowerShell-Skripten finden Sie unter https://communities.vmware.com/docs/DOC-30835.

Anwendungsfälle für die Bereitstellung

4

Mithilfe der in diesem Kapitel beschriebenen Bereitstellungsszenarien können Sie die in Ihrer Umgebung passende Access Point-Bereitstellung identifizieren und organisieren.

Sie können Access Point mit Horizon View, Horizon Air Hybrid-Mode, VMware Identity Manager und VMware AirWatch bereitstellen.

Dieses Kapitel behandelt die folgenden Themen:

Access Point-Bereitstellung mit Horizon View und Horizon Air Hybrid-Mode

Sie können Access Point mit Horizon View und Horizon Air Hybrid-Mode bereitstellen. Für die View-Komponente von VMware Horizon spielen Access Point-Appliances die gleiche Rolle wie früher View-Sicherheitsserver.

Bereitstellungsszenario

Access Point liefert sicheren Remote-Zugriff auf standortbasierte virtuelle Desktops und Anwendungen in einem Kunden-Datencenter. Dies wird mit einer On-Premise-Bereitstellung von Horizon View oder Horizon Air Hybrid-Mode für einheitliches Management betrieben.

Dank Access Point kann das Unternehmen die Identität des Benutzers sicherstellen und den Zugriff auf seine zulässigen Desktops und Anwendungen steuern.

Virtuelle Access Point-Appliances werden üblicherweise in einer demilitarisierten Netzwerkzone (DMZ) bereitgestellt. Durch die Bereitstellung in einer DMZ wird sichergestellt, dass der gesamte Datenverkehr, der für Desktop- und Anwendungsressourcen in das Datencenter gelangt, Datenverkehr ist, der zu einem sicher authentifizierten Benutzer gehört. Außerdem sorgen virtuelle Access Point-Appliances dafür, dass der Datenverkehr für einen authentifizierten Benutzer nur an Desktop- und Anwendungsressourcen geleitet werden kann, für die der Benutzer berechtigt ist. Dieser Grad an Sicherheit erfordert eine genaue Untersuchung der Desktopprotokolle und Koordination von sich potenziell schnell verändernden Richtlinien und Netzwerkadressen, damit der Zugriff genauestens kontrolliert werden kann.

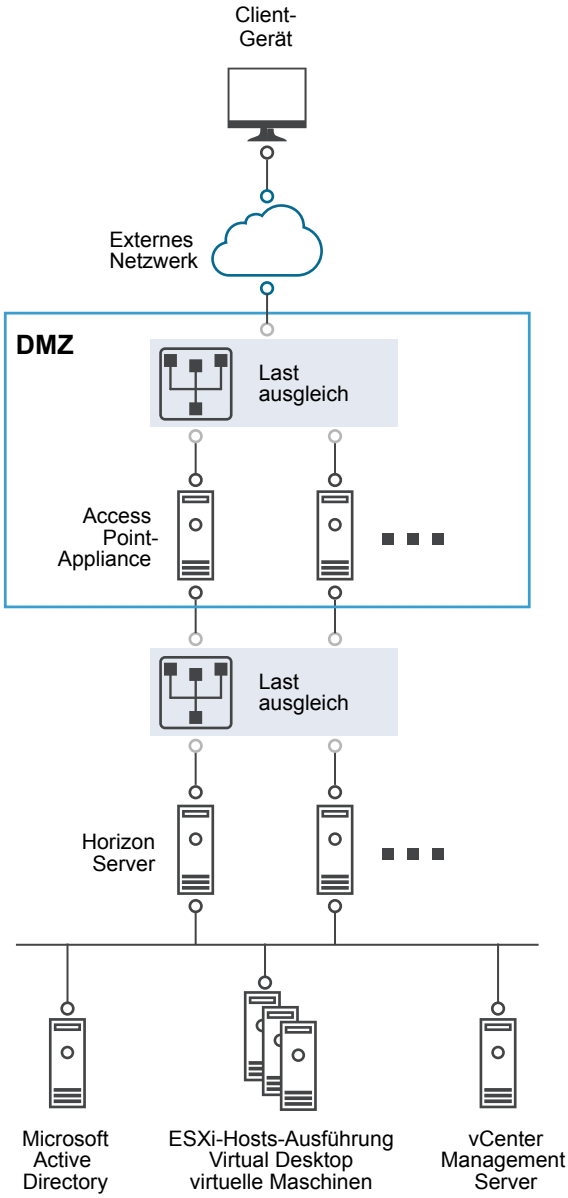
Sie müssen die Anforderungen einer nahtlosen Access Point-Bereitstellung mit Horizon erfüllen.

- Die Access Point-Appliance verweist auf einen Load Balancer, der Horizon-Servern vorgelagert ist, und die Auswahl der Serverinstanz erfolgt dynamisch.
- Access Point ersetzt den Horizon-Sicherheitsserver.
- Port 443 muss für Blast TCP/UDP verfügbar sein.
- Das Blast Secure Gateway und PCoIP Secure Gateway müssen aktiviert sein, wenn Access Point mit Horizon bereitgestellt wird. So wird sichergestellt, dass die Anzeigeprotokolle automatisch über Access Point als Proxys dienen können. Die Einstellungen BlastExternalURL und pcoipExternalURL geben Verbindungsadressen an, mit denen die Horizon-Clients diese Anzeigeprotokollverbindungen über die jeweiligen Gateways bei Access Point weiterleiten. Dadurch wird die Sicherheit verbessert, da diese Gateways sicherstellen, dass der Anzeigeprotokoll-Datenverkehr im Namen eines authentifizierten Benutzers gesteuert wird. Unautorisierter Anzeigeprotokoll-Datenverkehr wird von Access Point ignoriert.
- Deaktivieren Sie die sicheren Gateways auf den View-Verbindungsserverinstanzen und aktivieren Sie diese Gateways auf den Access Point-Appliances.

Den Hauptunterschied zum View-Sicherheitsserver bilden folgende Eigenschaften von Access Point.

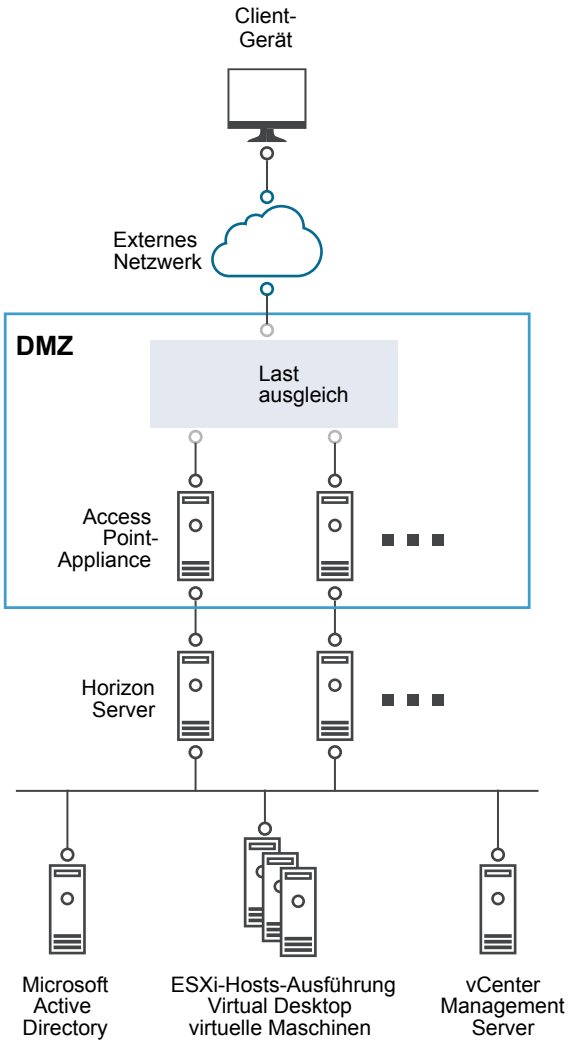
- Sichere Bereitstellung. Access Point ist als geschützte, gesperrte, vorkonfigurierte Linux-basierte virtuelle Maschine implementiert.
- Skalierbar. Sie können Access Point mit einem individuellen View-Verbindungsserver verbinden oder über einen Load Balancer, der mehreren View-Verbindungsservern vorgelagert ist, und so Hochverfügbarkeit erhalten. Access Point agiert als Ebene zwischen Horizon Clients und Backend-View-Verbindungsservern. Da die Bereitstellung schnell verläuft, kann sie schnell vergrößert oder verkleinert werden, um die wechselnden Anforderungen dynamischer Unternehmen zu erfüllen.

Abbildung 4-1. Access Point-Appliance mit Verweis auf einen Load Balancer



Alternativ dazu können auch eine oder mehrere Access Point-Appliances auf eine einzelne Serverinstanz verweisen. Bei beiden Vorgehensweisen verwenden Sie einen Load Balancer, der zwei oder mehr Access Point-Appliances in der DMZ vorgelagert ist.

Abbildung 4-2. Access Point-Appliance mit Verweis auf eine Horizon-Server-Instanz



Authentifizierung

Die Benutzerauthentifizierung erfolgt sehr ähnlich wie beim View-Sicherheitsserver. Die folgenden Benutzer-Authentifizierungsmethoden werden in Access Point unterstützt.

- Active Directory-Benutzername und -Kennwort
- Kiosk-Modus. Detaillierte Informationen zum Kiosk-Modus finden Sie in der Horizon-Dokumentation.
- Zwei-Faktor-Authentifizierung mit RSA SecurID, offiziell zertifiziert durch RSA für SecurID
- RADIUS über mehrere zweistufige Lösungen von externen Sicherheitsanbietern
- Smartcard, CAC oder PIV X.509-Benutzerzertifikate
- SAML

Diese Authentifizierungsmethoden werden in Kombination mit View-Verbindungsserver unterstützt. Access Point erfordert keine direkte Kommunikation mit Active Directory. Diese Kommunikation dient als Proxy über den View-Verbindungsserver, der direkt auf Active Directory zugreifen kann. Nach der Authentifizierung der Benutzersitzung entsprechend der Authentifizierungsrichtlinie kann Access Point Anforderungen für Berechtigungsinformationen sowie Anforderungen zum Desktop- und Anwendungsstart an View-Verbindungsserver weiterleiten. Access Point verwaltet darüber hinaus die zugehörigen Anwendungsprotokoll-Handler, damit diese nur autorisierten Protokolldatenverkehr weiterleiten.

Die Smartcard-Authentifizierung wird von Access Point selbst verarbeitet. Dazu gehören Optionen für die Kommunikation zwischen Access Point und Online Certificate Status Protocol-(OCSP-)Servern, um nach entzogenen X.509-Zertifikaten zu suchen usw.

Konfigurieren der Horizon-Einstellungen

Access Point kann mit Horizon View und Horizon Air Hybrid-Mode bereitgestellt werden. Für die View-Komponente von VMware Horizon spielt die Access Point-Appliance die gleiche Rolle wie früher der View-Sicherheitsserver.

Vorgehensweise

1. Klicken Sie auf der Verwaltungsoberfläche im Bereich „Manuell konfigurieren“ auf **Auswählen**.
2. Klicken Sie unter „Allgemeine Einstellungen“ in der Zeile mit den Einstellungen des Edgedienstes auf **Anzeigen**.
3. Klicken Sie auf das Zahnradsymbol für die **Horizon-Einstellungen**.
4. Ändern Sie auf der Seite der Horizon-Einstellungen NEIN in **JA**, um Horizon zu aktivieren.
5. Konfigurieren Sie die folgenden Edgediensteinstellungen für Horizon.

Option	Beschreibung
Bezeichner	Standardmäßig ist hier „View“ eingestellt. Access Point kann mit Servern kommunizieren, die das View XML-Protokoll verwenden, wie View-Verbindungsserver, Horizon Air und Horizon Air Hybrid-Mode.
Verbindungsserver-URL	Geben Sie die Adresse des Horizon Servers oder des Lastausgleichsdienstes ein. Geben Sie diesen in folgender Form ein: https://00.00.00.00
Fingerabdrücke für Proxy-Ziel-URL	Geben Sie die Liste der Horizon Server-Fingerabdrücke ein. Wenn Sie keine Fingerabdruckliste zur Verfügung stellen, müssen die Serverzertifikate durch eine vertrauenswürdige Zertifizierungsstelle ausgestellt worden sein. Geben Sie die Fingerabdrücke als Hexadezimalzahlen ein. Beispiel: sha = C3 89 A2 19 DC 7A 48 2B 85 1C 81 EC 5E 8F 6A 3C 33 F2 95 C3

6 Klicken Sie auf **Mehr**, um die Authentifizierungsmethodenregel und andere erweiterte Einstellungen zu konfigurieren.

Option	Beschreibung
Authentifizierungsmethoden	Wählen Sie die zu verwendenden Authentifizierungsmethoden aus. Standardmäßig wird die Passthrough-Authentifizierung des Benutzernamens und des Kennworts verwendet. In den Dropdown-Menüs sind die von Ihnen in Access Point konfigurierten Authentifizierungsmethoden aufgeführt. Sie können eine Authentifizierung konfigurieren, bei der eine zweite Authentifizierungsmethode verwendet wird, sofern der erste Authentifizierungsversuch fehlschlägt: a Wählen Sie im ersten Dropdown-Menü eine Authentifizierungsmethode aus. b Klicken Sie auf **+** und wählen Sie UND oder ODER aus. c Wählen Sie im dritten Dropdown-Menü die zweite Authentifizierungsmethode aus. Damit Benutzer sich über beide Authentifizierungsmethoden authentifizieren müssen, ändern Sie im Dropdown-Menü ODER in UND.
URL für Integritätsprüfung	Wenn ein Lastausgleichsdienst konfiguriert ist, geben Sie die URL ein, die der Lastausgleichsdienst verwendet, um eine Verbindung mit der Access Point-Appliance herzustellen und eine Integritätsprüfung durchzuführen.
SAML SP	Geben Sie den Namen des SAML-Dienstanbieters für den View XMLAPI-Broker ein. Dieser Name muss entweder mit dem Namen in den Metadaten eines konfigurierten Dienstanbieters übereinstimmen oder der spezielle Wert DEMO sein.
PCOIP aktiviert	Ändern Sie NEIN in **JA**, um festzulegen, dass PCoIP Secure Gateway aktiviert ist.
Externe Proxy-URL	Geben Sie die externe URL der Access Point-Appliance ein. Diese URL wird von Clients für sichere Verbindungen über das PCoIP Secure Gateway verwendet. Diese Verbindung wird für den PCoIP-Verkehr verwendet. Standardmäßig sind die Access Point-IP-Adresse und Port 4172 angegeben.
Aufforderung für Smart Card-Hinweis	Ändern Sie NEIN in **JA**, um die Unterstützung der Funktion für den Benutzernamenhinweis für Smartcards durch die Access Point-Appliance zu aktivieren. Durch Hinweise für Smartcards kann das Smartcard-Zertifikat eines Benutzers mehreren Active Directory-Domänenbenutzerkonten zugeordnet werden.
Blast aktiviert	Ändern Sie NEIN in **JA**, um das Blast Secure Gateway zu verwenden.
Externe Blast-URL:	Geben Sie die FQDN-URL der Access Point-Appliance ein, die Endbenutzer verwenden, um im Webbrowser eine sichere Verbindung über das Blast Secure Gateway herzustellen. Geben Sie diese in folgender Form ein: https://exampleappliance:443
Tunnel aktiviert	Wenn der sichere View-Tunnel verwendet wird, ändern Sie NEIN in **JA**. Der Client verwendet die externe URL für Tunnelverbindungen über das View Secure Gateway. Der Tunnel wird für den Verkehr von RDP, USB und MMR (Multimedia-Umleitung) benutzt.
Externe Tunnel-URL	Geben Sie die externe URL der Access Point-Appliance ein. Falls keine Angabe erfolgt, wird der Access Point-Standardwert verwendet.
Übereinstimmung mit Windows-Benutzername	Ändern Sie NEIN in **JA**, damit RSA SecurID und Windows-Benutzername übereinstimmen. Wenn JA festgelegt ist, wird „securID-auth“ auf „wahr“ gesetzt und die Übereinstimmung von SecurID und Windows-Benutzername wird erzwungen.

Option	Beschreibung
Gateway-Standort	Ändern Sie NEIN in **JA**, um den Standort zu aktivieren, von dem die Anforderungen stammen. Der Sicherheitsserver und Access Point legen den Gateway-Standort fest. Es kann sich um einen externen oder um einen internen Standort handeln.
Windows-SSO aktiviert	Ändern Sie NEIN in **JA**, um die RADIUS-Authentifizierung zu aktivieren. Die Windows-Anmeldung benutzt dann die Anmeldeinformationen, die bei der ersten erfolgreichen Anforderung des RADIUS-Zugriffs verwendet werden.

7 Klicken Sie auf **Speichern**.

Access Point-Bereitstellung als Reverse-Proxy

Access Point kann als Web-Reverse-Proxy genutzt und entweder als normaler Reverse-Proxy oder als authentifizierender Reverse-Proxy in der DMZ eingesetzt werden.

Bereitstellungsszenario

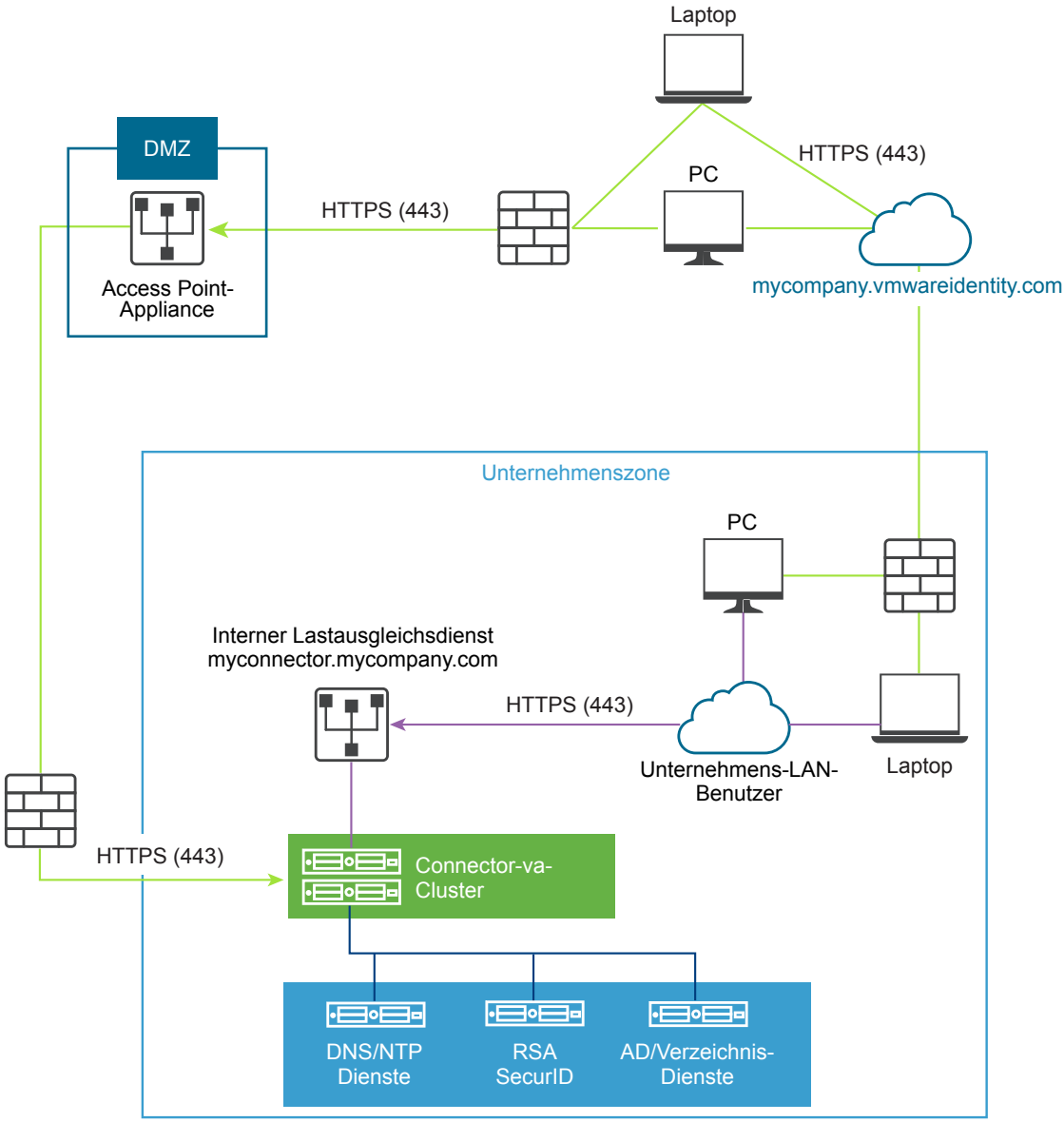
Access Point bietet sicheren Remote-Zugriff auf eine On-Premise-Bereitstellung von VMware Identity Manager. Access Point-Appliances werden üblicherweise in einer demilitarisierten Netzwerkzone (DMZ) bereitgestellt. Mit VMware Identity Manager arbeitet die Access Point-Appliance als Web-Reverse-Proxy zwischen dem Browser eines Benutzers und dem VMware Identity Manager-Dienst im Datencenter. Access Point ermöglicht außerdem den Remote-Zugriff auf den VMware Identity Manager-Katalog, um Horizon-Anwendungen zu starten.

Anforderungen für Access Point-Bereitstellung mit VMware Identity Manager

- DNS aufteilen
- Die VMware Identity Manager-Appliance muss einen vollqualifizierten Domänennamen (FQDN) als Hostnamen aufweisen.

- Der Access Point muss interne DNS verwenden. Die proxyDestinationURL muss also FQDN verwenden.

Abbildung 4-3. Access Point-Appliance mit Verweis auf Connector



Wissenswertes zum Reverse-Proxy

Access Point bietet Zugriff auf das App-Portal, wo Remote-Benutzer über eine einmalige Anmeldung auf ihre Ressourcen zugreifen können. Sie aktivieren den Authn-Reverse-Proxy auf einem Edgedienst-Manager. Aktuell werden die Authentifizierungsmethoden RSA SecurID und RADIUS unterstützt.

Hinweis Sie müssen Identitätsanbieter-Metadaten generieren, bevor Sie die Authentifizierung auf dem Web-Reverse-Proxy aktivieren.

Access Point liefert Remote-Zugriff auf VMware Identity Manager und Webanwendungen mit oder ohne Authentifizierung über einen browserbasierten Client und anschließenden Start von Horizon-Desktop.

- Browserbasierte Clients werden unter Verwendung der Authentifizierungsmethoden RADIUS und RSA SecurID unterstützt.

Die Reverse-Proxy-Unterstützung ist mit Access Point 2.8 auf VMware Identity Manager und interne Webressourcen, wie Confluence und WIKI, eingeschränkt. Diese Ressourcenliste wird in Zukunft noch erweitert.

Hinweis Die Eigenschaften `authCookie` und `unSecurePattern` sind für Authn-Reverse-Proxy nicht gültig. Sie müssen die Authentifizierungsmethode mit der Eigenschaft `authMethods` definieren.

Konfigurieren des Reverse-Proxys für VMware Identity Manager

Sie können den Web-Reverse-Proxy-Dienst für die Verwendung von Access Point mit VMware Identity Manager konfigurieren.

Voraussetzungen

Anforderungen für die Access Point-Bereitstellung mit VMware Identity Manager.

- DNS aufteilen
- Der VMware Identity Manager-Dienst muss einen vollqualifizierten Domänennamen (FQDN) als Hostnamen aufweisen.
- Der Access Point muss interne DNS verwenden. Die proxyDestination-URL muss also FQDN verwenden.

Vorgehensweise

1. Klicken Sie auf der Verwaltungsoberfläche im Bereich „Manuell konfigurieren“ auf **Auswählen**.
2. Klicken Sie unter „Allgemeine Einstellungen“ in der Zeile mit den Einstellungen des Edgedienstes auf **Anzeigen**.
3. Klicken Sie auf das Zahnradsymbol für die **Reverse-Proxy-Einstellungen**.
4. Ändern Sie auf der Seite der Reverse-Proxy-Einstellungen NEIN in **JA**, um den Reverse-Proxy zu aktivieren.
5. Konfigurieren Sie die folgenden Edgediensteinstellungen für Horizon.

Option	Beschreibung
Bezeichner	Für den Bezeichner des Edgedienstes ist WEB_REVERSE_PROXY festgelegt.
Proxy-Ziel-URL	Geben Sie die Adresse des VMware Identity Manager-Servers ein. Geben Sie beispielsweise **`https://vmwareidentitymgr.example.com`** ein.

Option	Beschreibung
Fingerabdrücke für Proxy-Ziel-URL	Geben Sie eine Liste annehmbarer Fingerabdrücke von SSL-Server-Zertifikaten für die proxyDestination-URL ein. Wenn Sie das Platzhalterzeichen * einfügen, werden alle Zertifikate zugelassen. Ein Fingerabdruck hat das Format [alg=]xx:xx, wobei „alg“ der Standardwert „sha1“ oder „md5“ sein kann. „xx“ steht für Hexadezimalzahlen. Beispiel: sha = C3 89 A2 19 DC 7A 48 2B 85 1C 81 EC 5E 8F 6A 3C 33 F2 95 C3 Wenn Sie die Fingerabdrücke nicht konfigurieren, müssen die Serverzertifikate durch eine vertrauenswürdige Zertifizierungsstelle ausgestellt worden sein.
Proxy-Muster	Geben Sie die entsprechenden URI-Pfade ein, die an die Ziel-URL weitergegeben werden. Beispiel: **`(/|/SAAS(.*)|/hc(.*)|/web(.*)|/catalog-portal(.*))`**.

6 Klicken Sie auf **Mehr**, um erweiterte Einstellungen zu konfigurieren.

Option	Beschreibung
Authentifizierungsmethoden	Standardmäßig wird die Passthrough-Authentifizierung des Benutzernamens und des Kennworts verwendet. In den Dropdown-Menüs sind die von Ihnen in Access Point konfigurierten Authentifizierungsmethoden aufgeführt. Im Dropdown-Menü sind die von Ihnen in Access Point konfigurierten Authentifizierungsmethoden aufgeführt.
URL für Integritätsprüfung	Wenn ein Lastausgleichsdienst konfiguriert ist, geben Sie die URL ein, die der Lastausgleichsdienst verwendet, um eine Verbindung mit der Access Point-Appliance herzustellen und eine Integritätsprüfung durchzuführen.
SAML SP	Geben Sie den Namen des SAML-Dienstanbieters für den View XML API-Broker ein. Dieser Name muss entweder mit dem Namen in den Metadaten eines konfigurierten Dienstanbieters übereinstimmen oder der spezielle Wert **`DEMO`** sein.
Aktivierungscode	Geben Sie den vom VMware Identity Manager-Dienst generierten Aktivierungscode ein, der in Access Point importiert wird, um eine Vertrauensbeziehung zwischen VMware Identity Manager und Access Point aufzubauen.
Externe URL	Standardmäßig ist die Access Point-Host-URL, Port 443, angegeben. Sie können eine weitere externe URL eingeben. Geben Sie diese in folgender Form ein: `https://<host:port>`.

7 Klicken Sie auf **Speichern**.

Access Point-Bereitstellung mit AirWatch-Tunnel

Die Access Point-Appliance wird in der DMZ bereitgestellt. Zur Bereitstellung gehört die Installation der Access Point-Komponenten und der AirWatch-Komponenten, wie Agent- und Tunnel-Proxy-Dienste.

Zum Bereitstellen des AirWatch Tunnel für Ihre AirWatch-Umgebung gehören die Einrichtung der anfänglichen Hardware, die Konfiguration der Serverinformationen und der App-Einstellungen in der AirWatch-Admin-Konsole, das Herunterladen einer Installationsdatei und die Ausführung des Installationsprogramms in Ihrem AirWatch Tunnel-Server.

Sie können jeden der Edgedienste nach Abschluss der OVF-Installation und Änderung der Werte manuell konfigurieren.

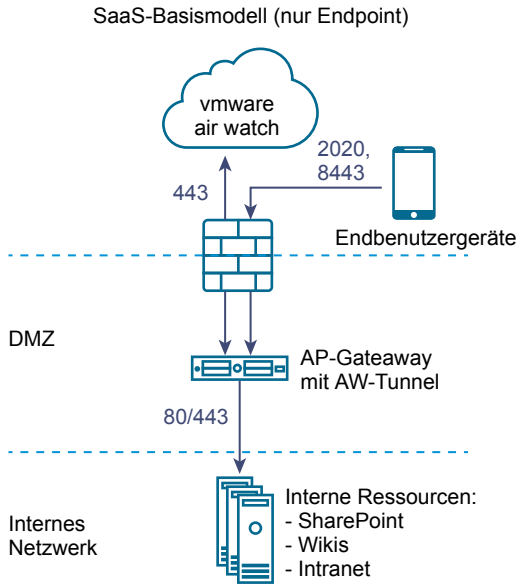
Weitere Informationen zum Bereitstellen von Access Point mit AirWatch finden Sie unter https://resources.air-watch.com/view/vb7zp7wwhpw756m2pfxy .

Tunnel-Proxy-Bereitstellung für AirWatch

Bei der Tunnel-Proxy-Bereitstellung wird der Netzwerkdatenverkehr zwischen einem Endbenutzergerät und einer Website über die VMware Browser-Mobilanwendung aus AirWatch gesichert.

Die Mobilanwendung baut eine sichere HTTPS-Verbindung zum Tunnel Proxy-Server auf und schützt die sensiblen Daten. Um eine interne Anwendung mit AirWatch Tunnel-Proxy zu verwenden, müssen Sie sicherstellen, dass das AirWatch-SDK in die Anwendung eingebettet ist. Dadurch erhalten Sie Tunneling-Funktionen mit dieser Komponente.

Abbildung 4-4. Tunnel-Proxy-Bereitstellung

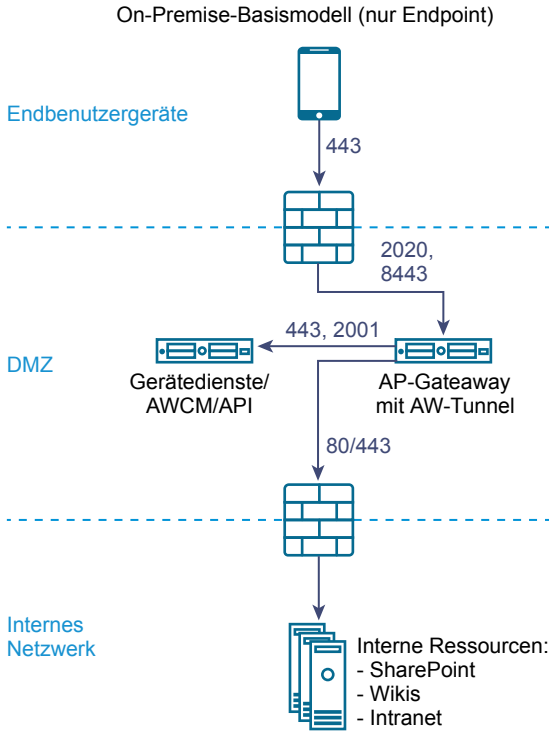


App-spezifische Tunnel-Bereitstellung mit AirWatch

Mit der App-spezifischen Tunnel-Bereitstellung können sowohl interne als auch öffentliche Anwendungen sicher auf Unternehmensressourcen zugreifen, die sich in Ihrem sicheren internen Netzwerk befinden.

Dabei werden die von Betriebssystemen wie iOS 7 oder höher und Android 5.0 oder höher bereitgestellten App-spezifischen Funktionen eingesetzt. Unter diesen Betriebssystemen können spezielle, von den Mobilitätsadministratoren genehmigte Anwendungen auf interne Ressourcen zugreifen. Vorteil hierbei ist, dass kein Code für die mobilen Anwendungen geändert werden muss. Die Unterstützung durch das Betriebssystem liefert eine nahtlose Nutzungserfahrung und mehr Sicherheit als bei jeder anderen benutzerdefinierten Lösung.

Abbildung 4-5. App-spezifische Tunnel-Bereitstellung



Konfigurieren der App-spezifischen Tunnel- und Proxy-Einstellungen für AirWatch

Durch die Tunnel-Proxy-Bereitstellung wird der Netzwerkdatenverkehr zwischen einem Endbenutzergerät und einer Website über die VMware Browser-Mobilanwendung gesichert.

Vorgehensweise

1. Klicken Sie auf der Verwaltungsoberfläche im Bereich „Manuell konfigurieren“ auf **Auswählen**.
2. Klicken Sie unter „Allgemeine Einstellungen“ in der Zeile mit den Einstellungen des Edgedienstes auf **Anzeigen**.
3. Klicken Sie auf das Zahnradsymbol für die **App-spezifischen Tunnel- und Proxy-Einstellungen**.
4. Ändern Sie NEIN in **JA**, um den Tunnel-Proxy zu aktivieren.
5. Konfigurieren Sie die folgenden Edgediensteinstellungen.

Option	Beschreibung
Bezeichner	Standardmäßig ist hier „View“ eingestellt. Access Point kann mit Servern kommunizieren, die das View XML-Protokoll verwenden, wie View-Verbindungsserver, Horizon Air und Horizon Air Hybrid-Mode.
URL für API-Server	Geben Sie die URL des AirWatch-API-Servers ein. Beispiel: https://example.com:<port>.
Benutzername für API-Server	Geben Sie den Benutzernamen für die Anmeldung beim API-Server ein.
Kennwort für API-Server	Geben Sie das Kennwort für die Anmeldung beim API-Server ein.

Option	Beschreibung
Gruppencode für Organisation	Geben Sie die Organisation des Benutzers ein.
Hostname für AirWatch-Server	Geben Sie den AirWatch-Serverhostnamen ein.

6 Klicken Sie auf **Mehr**, um erweiterte Einstellungen zu konfigurieren.

Option	Beschreibung
AirWatch – ausgehender Proxy	Ändern Sie NEIN in **JA**, um den Tunnel-Proxy-Dienst zu initialisieren.
HOST für ausgehenden Proxy	Geben Sie den Namen des Hosts ein, auf dem der ausgehende Proxy installiert ist. **Hinweis** Dies ist nicht der Tunnel-Proxy.
PORT für ausgehenden Proxy	Geben Sie die Portnummer des ausgehenden Proxy ein.
Benutzername für ausgehenden Proxy	Geben Sie den Benutzernamen für die Anmeldung beim ausgehenden Proxy ein.
Kennwort für ausgehenden Proxy	Geben Sie das Kennwort für die Anmeldung beim ausgehenden Proxy ein.
NTLM-Authentifizierung	Ändern Sie NEIN in **JA**, um festzulegen, dass für Anforderungen für den ausgehenden Proxy eine NTLM-Authentifizierung erforderlich ist.
Für AirWatch-Tunnel-Proxy verwenden	Ändern Sie NEIN in **JA**, um diesen Proxy als ausgehenden Proxy für AirWatch-Tunnel zu verwenden. Wenn diese Einstellung nicht aktiviert ist, verwendet Access Point diesen Proxy für den anfänglichen API-Aufruf, um die Konfiguration aus der AirWatch-Verwaltungskonsole abzurufen.

7 Klicken Sie auf **Speichern**.

Konfigurieren von Access Point mit TLS/SSL-Zertifikaten

5

Sie müssen die TLS/SSL-Zertifikate für Access Point-Appliances konfigurieren.

Hinweis Die Konfiguration der TLS/SSL-Zertifikate für die Access Point-Appliance gilt nur für Horizon View, Horizon Air Hybrid-Mode und Web-Reverse-Proxy.

Konfigurieren von TLS/SSL-Zertifikaten für Access Point-Appliances

TLS/SSL ist für Clientverbindungen mit Access Point-Appliances erforderlich. Clientverbundene Access Point-Appliances und Zwischenserver, die TLS/SSL-Verbindungen beenden, benötigen TLS/SSL-Serverzertifikate.

TLS/SSL-Zertifikate werden durch eine Zertifizierungsstelle (CA, Certificate Authority) signiert. Eine Zertifizierungsstelle ist eine vertrauenswürdige Instanz, welche die Identität des Zertifikats und seines Erstellers bestätigt. Wenn ein Zertifikat durch eine vertrauenswürdige Zertifizierungsstelle signiert wurde, werden die Benutzer nicht länger über Meldungen aufgefordert, das Zertifikat zu überprüfen, und Thin Client-Geräte können ohne zusätzliche Konfiguration eine Verbindung herstellen.

Beim Bereitstellen einer Access Point-Appliance wird ein Standard-TLS/SSL-Serverzertifikat erstellt. Für Produktionsumgebungen empfiehlt VMware, das Standardzertifikat so schnell wie möglich zu ersetzen. Das Standardzertifikat ist nicht von einer vertrauenswürdigen Zertifizierungsstelle signiert. Verwenden Sie das Standardzertifikat nur in einer Nicht-Produktionsumgebung.

Auswählen des korrekten Zertifikattyps

Sie können für Access Point verschiedene Typen von TLS/SSL-Zertifikaten verwenden. Die Auswahl des korrekten Zertifikattyps ist entscheidend für Ihre Bereitstellung. Die Kosten der verschiedenen Zertifikattypen sind unterschiedlich, je nach der Anzahl der Server, auf denen diese verwendet werden können.

Folgen Sie den VMware-Sicherheitsempfehlungen und verwenden Sie vollqualifizierte Domänennamen (FQDN) für Ihre Zertifikate, unabhängig vom ausgewählten Typ. Verwenden Sie selbst für die Kommunikation innerhalb Ihrer internen Domäne keinen einfachen Servernamen bzw. keine einfache IP-Adresse.

Namenszertifikat für Einzelserver

Sie können ein Zertifikat mit einem Antragstellernamen für einen bestimmten Server generieren. Beispiel: `dept.example.com`.

Dieser Zertifikattyp ist beispielsweise hilfreich, wenn nur eine Access Point-Appliance ein Zertifikat benötigt.

Wenn Sie eine Zertifikatsignieranforderung an eine Zertifizierungsstelle übermitteln, geben Sie den Servernamen an, der mit dem Zertifikat verknüpft ist. Stellen Sie sicher, dass die Access Point-Appliance den bereitgestellten Servernamen auflösen kann und dieser mit dem Namen identisch ist, der dem Zertifikat zugeordnet wurde.

Alternative Antragstellernamen

Ein alternativer Antragstellername (Subject Alternative Name, SAN) ist ein Attribut, das einem Zertifikat bei der Ausstellung hinzugefügt werden kann. Mit diesem Attribut können Sie einem Zertifikat Antragstellernamen (URLs) hinzufügen, damit es mehr als einen Server validieren kann.

Beispielsweise lassen sich für die Access Point-Appliances hinter einem Lastausgleichsdienst drei Zertifikate ausstellen: `ap1.example.com`, `ap2.example.com` und `ap3.example.com`. Durch Hinzufügen eines alternativen Antragstellernamens, der für den Hostnamen des Lastausgleichsdienstes steht (z. B. `horizon.example.com` in diesem Beispiel) wird das Zertifikat gültig, da es dem durch den Client angegebenen Hostnamen entspricht.

Platzhalterzertifikat

Ein Platzhalterzertifikat wird für Verwendung für mehrere Dienste generiert. Beispiel: `*.example.com`.

Ein Platzhalterzertifikat ist sinnvoll, wenn für viele Server ein Zertifikat nötig ist. Wenn andere Anwendungen in Ihrer Umgebung zusätzlich zu den Access Point-Appliances TLS/SSL-Zertifikate benötigen, können Sie ein Platzhalterzertifikat auch für diese Server verwenden. Wenn Sie allerdings ein Platzhalterzertifikat benutzen, das mit anderen Diensten gemeinsam verwendet wird, richtet sich die Sicherheit des VMware Horizon-Produkts auch nach der Sicherheit der anderen Dienste.

Hinweis Ein Platzhalterzertifikat lässt sich nur auf einer Ebene einer Domäne verwenden. Beispielsweise kann ein Platzhalterzertifikat mit dem Antragstellernamen `*.example.com` für die Unterdomäne `dept.example.com`, aber nicht für `dept.it.example.com` eingesetzt werden.

In die Access Point-Appliance importierte Zertifikate müssen von den Clientcomputern als vertrauenswürdig eingestuft werden und für alle Instanzen von Access Point sowie für jeden Lastausgleichsdienst verwendet werden können, entweder durch Verwendung von Platzhaltern oder von SAN-Zertifikaten (Alternativer Antragstellername).

Konvertieren von Zertifikatdateien in das einzeilige PEM-Format

Um Zertifikateinstellungen mit der Access Point-REST-API zu konfigurieren oder um PowerShell-Skripts zu verwenden, müssen Sie das Zertifikat für die Zertifikatkette sowie für den privaten Schlüssel in Dateien im PEM-Format und dann die `.pem`-Dateien in ein einzeiliges Format mit eingebetteten Zeilenendemarken konvertieren.

Für das Konfigurieren von Access Point stehen drei mögliche Arten von Zertifikaten zur Verfügung, die eventuell konvertiert werden müssen.

- Sie müssen immer ein TLS/SSL-Serverzertifikat für die Access Point-Appliance installieren und konfigurieren.
- Wenn Sie die Smartcard-Authentifizierung benutzen möchten, müssen Sie das von einer Zertifizierungsstelle herausgegebene vertrauenswürdige Zertifikat für das Zertifikat installieren und konfigurieren, das für die Smartcard verwendet werden soll.
- Für die Verwendung der Smartcard-Authentifizierung empfiehlt VMware die Installation und Konfiguration eines Stammzertifikats der Signatur-Zertifizierungsstelle für das SAML-Serverzertifikat, das in der Access Point-Appliance installiert ist.

Für alle Arten von Zertifikaten ist das Verfahren zur Konvertierung des Zertifikats in eine PEM-Datei mit der Zertifikatkette identisch. Für TLS/SSL-Server- und Stammzertifikate konvertieren Sie jede Datei auch in eine PEM-Datei mit dem privaten Schlüssel. Sie müssen dann auch jede `.pem`-Datei in ein einzeiliges Format konvertieren, das in einer JSON-Zeichenfolge in die Access Point-REST-API übernommen werden kann.

Voraussetzungen

- Stellen Sie sicher, das die Zertifikatdatei vorhanden ist. Die Datei kann im PKCS#12-Format (`.p12` oder `.pfx`) oder im Java-JKS- bzw. JCEKS-Format vorliegen.
- Machen Sie sich mit dem `openssl`-Befehlszeilentool für die Konvertierung des Zertifikats vertraut. Siehe https://www.openssl.org/docs/apps/openssl.html.
- Liegt das Zertifikat im Java-JKS- oder im JCEKS-Format vor, informieren Sie sich über das Java-`keytool`-Befehlszeilentool, um zuerst das Zertifikat in das `.p12`- oder in das `.pks`-Format und dann in `.pem`-Dateien zu konvertieren.

Vorgehensweise

1 Liegt Ihr Zertifikat im Java-JKS- oder JCEKS-Format vor, konvertieren Sie das Zertifikat mit `keytool` in das `.p12`- oder `.pks`-Format.

> **Wichtig** Verwenden Sie für diese Umwandlung dasselbe Quell- und Zielkennwort.

2 Liegt Ihr Zertifikat im PKCS#12-Format (`.p12` oder `.pfx`) vor oder wurde das Zertifikat in das PKCS#12-Format konvertiert, verwenden Sie `openssl`, um das Zertifikat in `.pem`-Dateien konvertieren.

   Wenn der Name des Zertifikats beispielsweise `mycaservercert.pfx` lautet, konvertieren Sie das Zertifikat mit den folgenden Befehlen:

```
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 Bearbeiten Sie `mycaservercert.pem` und entfernen Sie nicht erforderliche Zertifikateinträge. Es sollte das eine SSL-Server-Zertifikat enthalten, gefolgt von den erforderlichen Zwischen-CA-Zertifikaten und dem Stamm-CA-Zertifikat.

4 Mit dem folgenden UNIX-Befehl können Sie jede `.pem`-Datei in einen Wert konvertieren, der in einer JSON-Zeichenfolge in die Access Point-REST-API übernommen werden kann:

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

   In diesem Beispiel ist *`cert–name`*`.pem` der Name der Zertifikatdatei.

   Das neue Format platziert alle Zertifikatinformationen in einzelne Zeilen mit eingebetteten Zeilenendemarken. Wenn Sie über ein Zwischenzertifikat verfügen, muss dieses Zertifikat auch im einzeiligen Format vorliegen und dem ersten Zertifikat hinzugefügt werden, sodass sich beide Zertifikate in derselben Zeile befinden.

Sie können die Zertifikate nun für Access Point konfigurieren, indem Sie diese `.pem`-Dateien mit dem PowerShell-Skript verwenden, das dem unter https://communities.vmware.com/docs/DOC-30835 verfügbaren Blog-Beitrag „Using PowerShell to Deploy VMware Access Point“ (Verwenden von PowerShell zur Bereitstellung von VMware Access Point) angehängt ist. Alternativ können Sie eine JSON-Anfrage erstellen und mit dieser das Zertifikat konfigurieren.

Weiter

Informationen zu einem konvertierten TLS/SSL-Serverzertifikat finden Sie unter Ersetzen des Standard-TLS/SSL-Serverzertifikats für Access Point. Erläuterungen zu Smartcard-Zertifikaten erhalten Sie unter Konfigurieren der Zertifikat- oder Smartcard-Authentifizierung in der Access Point-Appliance.

Ersetzen des Standard-TLS/SSL-Serverzertifikats für Access Point

Um ein vertrauenswürdiges, von einer Zertifizierungsstelle signiertes TLS/SSL-Serverzertifikat in der Access Point-Appliance zu speichern, müssen Sie das Zertifikat in das erforderliche Format konvertieren und mit PowerShell-Skripts oder mit der Access Point-REST-API konfigurieren.

Für Produktionsumgebungen empfiehlt VMware ausdrücklich, das Standardzertifikat so schnell wie möglich zu ersetzen. Das Standard-TLS/SSL-Serverzertifikat, das bei der Bereitstellung einer Access Point-Appliance generiert wird, ist nicht von einer vertrauenswürdigen Zertifizierungsstelle signiert.

Wichtig Mit dieser Vorgehensweise können Sie auch regelmäßig ein Zertifikat ersetzen, das von einer vertrauenswürdigen Zertifizierungsstelle signiert wurde, bevor das Zertifikat abläuft (meist alle zwei Jahre).

Diese Vorgehensweise beschreibt, wie mit der REST-API das Zertifikat ersetzt wird. Eine einfachere Alternative ist eventuell die Verwendung der PowerShell-Skripts, die dem unter https://communities.vmware.com/docs/DOC-30835 verfügbaren Blog-Beitrag „Using PowerShell to Deploy VMware Access Point“ (Verwenden von PowerShell zur Bereitstellung von VMware Access Point) angehängt ist. Wenn Sie die benannte Access Point-Appliance bereits bereitgestellt haben, wird durch erneute Ausführung des Skripts die Appliance ausgeschaltet, gelöscht und mit den von Ihnen angegebenen aktuellen Einstellungen erneut bereitgestellt.

Voraussetzungen

- Sofern Sie nicht bereits über ein gültiges TLS/SSL-Serverzertifikat und dessen privaten Schlüssel verfügen, verwenden Sie ein neu signiertes Zertifikat der Zertifizierungsstelle. Wenn Sie eine Zertifikatsignieranforderung (CSR, Certificate Signing Request) für ein Zertifikat generieren, müssen Sie sicherstellen, dass auch ein privater Schlüssel generiert wird. Erstellen Sie keine Zertifikate für Server mithilfe eines KeyLength-Wertes unter 1024.

  Um die CSR zu generieren, müssen Sie über den vollqualifizierten Domänennamen (FQDN) verfügen, mit dem Clientgeräte eine Verbindung zur Access Point-Appliance und zur organisatorischen Einheit, zur Organisation, zur Stadt, zum Bundesland und zum Land für die Vervollständigung des Antragstellernamens herstellen.

- Konvertieren Sie das Zertifikat in PEM-Dateien und diese `.pem`-Dateien dann in ein einzeiliges Format. Siehe Konvertieren von Zertifikatdateien in das einzeilige PEM-Format.

- Machen Sie sich mit der Access Point-REST-API vertraut. Die Spezifikation für diese API ist über die folgende URL auf der virtuellen Maschine verfügbar, auf der Access Point installiert ist: `https://access-point-appliance.example.com:9443/rest/swagger.yaml`.

Vorgehensweise

1 Erstellen Sie eine JSON-Anfrage für die Weitergabe des Zertifikats an die Access Point-Appliance.

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

In diesem Beispiel stellen die *Zeichenfolge*-Werte die einzeiligen JSON-PEM-Werte dar, die Sie wie in den Voraussetzungen beschrieben erstellt haben.

2 Verwenden Sie für die JSON-Anfrage einen REST-Client wie `curl` oder `postman`, um die Access Point-REST-API aufzurufen und das Zertifikat sowie den Schlüssel in der Access Point-Appliance zu speichern.

Das folgende Beispiel verwendet einen `curl`-Befehl. In diesem Beispiel ist *access-point-appliance.example.com* der vollqualifizierte Domänenname (FQDN) der Access Point-Appliance und *cert*.json die im vorherigen Schritt erstellte JSON-Anfrage.

```
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
```

Weiter

Wenn die Zertifizierungsstelle, die das Zertifikat erstellt hat, nicht bekannt ist, konfigurieren Sie Clients so, dass sie dem Stammzertifikat und den Zwischenzertifikaten vertrauen.

Ändern der Sicherheitsprotokolle und Verschlüsselungssammlungen für die TLS- oder SSL-Kommunikation

Auch wenn die Standardeinstellungen in den meisten Fällen nicht geändert werden müssen, können Sie die Sicherheitsprotokolle und Verschlüsselungssammlungen, die für die Verschlüsselung der Kommunikation zwischen Clients und der Access Point-Appliance verwendet werden, konfigurieren.

Die Standardeinstellung enthält Verschlüsselungssammlungen, die entweder die 128-Bit- oder 256-Bit-AES-Verschlüsselung verwenden (mit Ausnahme von anonymen DH-Algorithmen) und nach der Verschlüsselungsstärke sortiert sind. TLS v1.1 und TLS v1.2 sind standardmäßig aktiviert. TLS v1.0 und SSL v3.0 sind deaktiviert.

Voraussetzungen

- Machen Sie sich mit der Access Point-REST-API vertraut. Die Spezifikation für diese API ist über die folgende URL auf der virtuellen Maschine verfügbar, auf der Access Point installiert ist: `https://access–point–appliance.example.com:9443/rest/swagger.yaml`.
- Informieren Sie sich über die speziellen Eigenschaften für die Konfiguration der Verschlüsselungssammlungen und Protokolle: `cipherSuites`, `ssl30Enabled`, `tls10Enabled`, `tls11Enabled` und `tls12Enabled`.

Vorgehensweise

1 Erstellen Sie eine JSON-Anfrage für die Angabe der zu verwendenden Protokolle und Verschlüsselungssammlungen.

Für das folgende Beispiel gelten die Standardeinstellungen.

```
{
"cipherSuites": "TLS_ECD-
HE_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 Verwenden Sie für die JSON-Anfrage einen REST-Client wie `curl` oder `postman`, um die Access Point-REST-API aufzurufen und die Protokolle sowie Verschlüsselungssammlungen zu konfigurieren.

Im Beispiel stellt *access-point-appliance.example.com* den vollqualifizierten Domänennamen (FQDN) der Access Point-Appliance dar.

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

ciphers.json ist die JSON-Anforderung, die Sie im vorhergehenden Schritt erstellt haben.

Es werden die von Ihnen angegebenen Verschlüsselungssammlungen und Protokolle verwendet.

Konfigurieren der Authentifizierung in DMZ

6

Bei der ersten Bereitstellung von VMware Access Point wird die Active Directory-Kennwortauthentifizierung als Standard eingerichtet. Benutzer geben ihren Benutzernamen und ihr Kennwort für Active Directory ein. Diese Anmeldedaten werden zur Authentifizierung an ein Back-End-System weitergeleitet.

Sie können den Access Point-Dienst so konfigurieren, dass eine Zertifikat-/Smartcard-Authentifizierung, eine RSA SecurID-Authentifizierung, eine RADIUS-Authentifizierung und eine adaptive RSA-Authentifizierung durchgeführt wird.

Hinweis Für eine AirWatch-Bereitstellung kann mit Active Directory nur die Kennwortauthentifizierung als Authentifizierungsmethode genutzt werden.

Dieses Kapitel behandelt die folgenden Themen:

Konfigurieren der Zertifikat- oder Smartcard-Authentifizierung in der Access Point -Appliance

Sie können die x509-Zertifikatauthentifizierung in Access Point so konfigurieren, dass Clients sich mithilfe von Zertifikaten auf Desktops oder mobilen Geräten authentifizieren oder einen Smartcard-Adapter für die Authentifizierung verwenden können.

Die zertifikatbasierte Authentifizierung beruht auf etwas, was der Benutzer besitzt (dem privaten Schlüssel oder der Smartcard) und auf etwas, was die Person weiß (dem Kennwort für den privaten Schlüssel oder der PIN der Smartcard). Die Smartcard-Authentifizierung bietet eine zweistufige Authentifizierung, indem einerseits überprüft wird, ob die Person im Besitz der Smartcard ist, und andererseits, ob die Person die erforderliche PIN kennt. Endbenutzer haben die Möglichkeit, Smartcards für die Anmeldung bei einem View-Remote-Desktop-Betriebssystem und für den Zugriff auf Smartcard-fähige Anwendungen zu verwenden, wie z. B. E-Mail-Anwendungen, die das Zertifikat für das Signieren von E-Mails zur Bestätigung der Absenderidentität einsetzen.

Mit dieser Funktion wird die Smartcard-Zertifikatauthentifizierung im Access Point-Dienst ausgeführt. Access Point verwendet eine SAML-Zusicherung, um Informationen zum X.509-Zertifikat und der Smartcard-PIN des Endbenutzers an den Horizon-Server zu übermitteln.

Sie können die Zertifikatsperrüberprüfung konfigurieren, um zu verhindern, dass sich Benutzer authentifizieren, deren Benutzerzertifikate gesperrt sind. Wenn Benutzer eine Organisation verlassen, eine Smartcard verlieren oder die Abteilung wechseln, werden Zertifikate häufig gesperrt. Es wird sowohl eine Zertifikatsperrüberprüfung mit Zertifikatsperrlisten (CRL, Certificate Revocation Lists) als auch mit dem Online Certificate Status Protocol (OCSP) unterstützt. Eine Zertifikatsperrliste ist eine Liste mit gesperrten Zertifikaten, die von der Zertifizierungsstelle veröffentlicht wird, die das Zertifikat ausgestellt hat. Bei OCSP handelt es sich um ein Zertifikatüberprüfungsprotokoll zur Ermittlung des Sperrstatus eines Zertifikats.

Sie können CRL und OCSP in derselben Zertifikat-Authentifizierungsadapter-Konfiguration festlegen. Wenn Sie beide Arten der Zertifikatsperrüberprüfung konfiguriert haben und das Kontrollkästchen „CRL im Falle eines OCSP-Fehlers verwenden“ aktiviert ist, wird OCSP zuerst überprüft und bei einem Scheitern die Sperrüberprüfung an CRL weitergegeben. Beachten Sie, dass umgekehrt bei einem Scheitern der CRL-Überprüfung die Sperrüberprüfung nicht an OCSP zurückgegeben wird.

Sie können die Authentifizierung auch so einrichten, dass für Access Point die Smartcard-Authentifizierung erforderlich ist, die Authentifizierung dann aber auch an den Server weitergegeben wird, für den eventuell die Active Directory-Authentifizierung durchgeführt werden muss.

Hinweis Für VMware Identity Manager wird die Authentifizierung immer durch Access Point an den VMware Identity Manager-Dienst weitergeleitet. Die Smartcard-Authentifizierung für die Access Point-Appliance kann nur konfiguriert werden, wenn Access Point mit Horizon 7 verwendet wird.

Konfigurieren der Zertifikatauthentifizierung in Access Point

Sie aktivieren und konfigurieren die Zertifikatauthentifizierung über die Access Point-Verwaltungskonsole.

Voraussetzungen

- Rufen Sie das Stammzertifikat und Zwischen-Zertifikate von der Zertifizierungsstelle (CA) ab, die die Zertifikate der Benutzer signiert hat. Siehe Anfordern der Zertifizierungsstellenzertifikate.
- Prüfen Sie, ob die SAML-Metadaten von Access Point zum Dienstanbieter hinzugefügt wurden und ob die SAML-Metadaten des Dienstanbieters in die Access Point-Appliance kopiert wurden.
- (Optional) OID-Liste (Objektkennungsliste) der gültigen Zertifikatsrichtlinien für die Zertifikatsauthentifizierung.
- Für Sperrprüfungen: den CRL-Speicherort und die URL des OCSP-Servers.
- (Optional) Speicherort des OCSP-Antwortsignaturzertifikats.
- Inhalt des Zustimmungsformulars, wenn vor der Authentifizierung ein Zustimmungsformular angezeigt wird.

Vorgehensweise

1 Klicken Sie auf der Verwaltungsoberfläche im Bereich „Manuell konfigurieren“ auf **Auswählen**.

2 Klicken Sie unter „Allgemeine Einstellungen“ in der Zeile mit den Authentifizierungseinstellungen auf **Anzeigen**.

3 Klicken Sie in der Zeile des X.509-Zertifikats auf das Zahnradsymbol.

4 Konfigurieren Sie das X.509-Zertifikat.

Ein Asterisk (*) gibt an, welche Felder erforderlich sind. Alle anderen Textfelder sind optional.

Option	Beschreibung
X.509-Zertifikat aktivieren	Ändern Sie NEIN in **JA**, um die Zertifikatauthentifizierung zu aktivieren.
***Name**	Name bezeichnet die Authentifizierungsmethode.
***Stamm- und Zwischenzertifikate für CA**	Klicken Sie auf **Auswählen**, um die hochzuladenden Zertifikatdateien auszuwählen. Sie können mehrere Root- und Zwischen-CA-Zertifikate auswählen, die im DER- oder PEM-Format codiert sind.
CRL-Zwischenspeichergröße	Geben Sie die Größe des Zwischenspeichers für die Zertifikatsperrliste ein. Die Standardeinstellung ist 100.
Zurückrufen von Zertifikaten aktivieren	Ändern Sie NEIN in **JA**, um die Zertifikatssperrüberprüfung zu aktivieren. Durch die Aktivierung der Sperre wird verhindert, dass sich Benutzer authentifizieren können, die über gesperrte Zertifikate verfügen.
CRL aus Zertifikaten verwenden	Aktivieren Sie dieses Kontrollkästchen, um die von der Zertifizierungsstelle veröffentlichte Zertifikatsperrliste (Certificate Revocation Lists, CRL) zu verwenden, um den Status eines Zertifikats (gesperrt oder nicht gesperrt) zu validieren.
CRL-Speicherort	Geben Sie den Serverdateipfad oder den lokalen Dateipfad ein, von dem die CRL geladen werden kann.
OCSP-Sperrung aktivieren	Aktivieren Sie das Kontrollkästchen, um das Zertifikatvalidierungsprotokoll „Online Certificate Status Protocol (OCSP)“ zu verwenden, um den Sperrstatus des Zertifikats zu erfahren.
CRL bei OCSP-Fehler verwenden	Wenn Sie sowohl CRL als auch OCSP konfigurieren, können Sie dieses Kontrollkästchen aktivieren, um wieder CRL zu verwenden, wenn die OCSP-Prüfung nicht verfügbar ist.
OCSP-Nonce senden	Aktivieren Sie dieses Kontrollkästchen, wenn Sie den eindeutigen Bezeichner der OCSP-Anfrage in der Antwort übermitteln möchten.
OCSP-URL	Wenn Sie OCSP-Widerruf aktiviert haben, geben Sie die OCSP-Serveradresse für die Widerrufsprüfung ein.
Signaturzertifikat des OCSP-Antwortdienstes	Geben Sie den Pfad des OSCP-Zertifikats für den Antwortdienst: */path/to/file.cer* ein.
Zustimmungsformular vor Authentifizierung aktivieren	Aktivieren Sie dieses Kontrollkästchen, um eine Seite mit einem Zustimmungsformular anzuzeigen, bevor sich die Benutzer mit der Zertifikatauthentifizierung bei ihrem Workspace ONE-Portal anmelden.
Inhalt des Zustimmungsformulars	Geben Sie hier den Text ein, der im Zustimmungsformular angezeigt wird.

5 Klicken Sie auf **Speichern**.

Weiter

Wenn die X.509Zertifikatauthentifizierung konfiguriert ist und die Access Point-Appliance hinter dem Lastausgleichsdienst eingerichtet ist, müssen Sie sicherstellen, dass Access Point mit SSL-Durchleitung am Lastausgleichsdienst konfiguriert ist, d. h. SSL darf nicht im Lastausgleichsdienst beendet werden. Diese Konfiguration stellt sicher, dass das SSL-Handshake zwischen Access Point und dem Client stattfindet, damit das Zertifikat an Access Point übergeben wird.

Anfordern der Zertifizierungsstellenzertifikate

Sie müssen alle anwendbaren Zertifizierungsstellenzertifikate (CA-Zertifikate) für alle vertrauenswürdigen Benutzerzertifikate auf den Smartcards anfordern, die von Ihren Benutzern und Administratoren verwendet werden. Diese Zertifikate beinhalten Stammzertifikate und gegebenenfalls Zwischenzertifikate, wenn das Smartcard-Zertifikat des Benutzers von einer Zwischenzertifizierungsstelle ausgestellt wurde.

Wenn Sie nicht über das Stamm- oder Zwischenzertifikat der Zertifizierungsstelle verfügen, welche die Zertifikate auf den von Ihren Benutzern und Administratoren verwendeten Smartcards signiert hat, können Sie die Zertifikate auch aus einem von einer Zertifizierungsstelle signierten Benutzerzertifikat oder aus einer Smartcard mit Zertifikat exportieren. Siehe Anfordern des CA-Zertifikats von Windows.

Vorgehensweise

- Fordern Sie die CA-Zertifikate aus einer der nachfolgend aufgeführten Quellen an.
  - Microsoft IIS-Server, auf dem die Microsoft-Zertifikatdienste ausgeführt werden. Informationen zum Installieren von Microsoft IIS, Ausstellen von Zertifikaten und Verteilen von Zertifikaten in Ihrer Organisation finden Sie auf der Microsoft TechNet-Website.
  - Öffentliches Stammzertifikat einer vertrauenswürdigen Zertifizierungsstelle. Dies ist die gängigste Quelle eines Stammzertifikats in Umgebungen, die bereits über eine Smartcard-Infrastruktur und einen standardisierten Ansatz für die Smartcard-Verteilung und -Authentifizierung verfügen.

Anfordern des CA-Zertifikats von Windows

Wenn Sie über ein von einer Zertifizierungsstelle signiertes Benutzerzertifikat oder eine Smartcard mit Zertifikat verfügen und Windows dem Stammzertifikat vertraut, können Sie das Stammzertifikat aus Windows exportieren. Handelt es sich beim Aussteller des Benutzerzertifikats um eine Zwischenzertifizierungsstelle, können Sie dieses Zertifikat exportieren.

Vorgehensweise

1. Wenn das Benutzerzertifikat auf einer Smartcard vorhanden ist, führen Sie die Smartcard in den Leser ein, um das Benutzerzertifikat zu Ihrem persönlichen Speicher hinzuzufügen.

   Wenn das Benutzerzertifikat nicht im persönlichen Speicher angezeigt wird, exportieren Sie das Benutzerzertifikat über die Lesersoftware in eine Datei. Diese Datei wird in Schritt 4 dieser Vorgehensweise verwendet.
2. Wählen Sie in Internet Explorer **Tools > Internetoptionen** aus.
3. Klicken Sie auf der Registerkarte **Inhalte** auf **Zertifikate**.

4 Wählen Sie auf der Registerkarte **Eigene Zertifikate** das gewünschte Zertifikat aus und klicken Sie auf **Anzeigen**.

   Wenn das Benutzerzertifikat nicht in der Liste enthalten ist, klicken Sie auf **Importieren**, um das Zertifikat manuell aus einer Datei zu importieren. Nach dem Import können Sie das Zertifikat aus der Liste auswählen.

5 Wählen Sie auf der Registerkarte **Zertifizierungspfad** das oberste Zertifikat in der Struktur und klicken Sie auf **Zertifikat anzeigen**.

   Ein Benutzerzertifikat kann als Bestandteil einer Vertrauenshierarchie signiert werden – das Signaturzertifikat selbst kann durch ein anderes Zertifikat höherer Ebene signiert sein. Wählen Sie das übergeordnete Zertifikat (das Zertifikat, das zum Signieren des Benutzerzertifikats verwendet wurde) als Stammzertifikat aus. In einigen Fällen kann es sich beim Aussteller um eine Zwischenzertifizierungsstelle handeln.

6 Klicken Sie auf der Registerkarte **Details** auf **In Datei kopieren**.

   Der **Zertifikatexport-Assistent** wird geöffnet.

7 Klicken Sie auf **Weiter > Weiter** und geben Sie einen Namen sowie einen Speicherort für die Exportdatei an.

8 Klicken Sie auf **Weiter**, um die Datei am angegebenen Speicherort als Stammzertifikat zu speichern.

Konfigurieren der RSA SecurID-Authentifizierung in Access Point

Nachdem die Access Point-Appliance als Authentifizierungs-Agent auf dem RSA SecurID-Server konfiguriert wurde, müssen Sie der Access Point-Appliance RSA SecurID-Konfigurationsinformationen hinzufügen.

Voraussetzungen

- Vergewissern Sie sich, dass der RSA Authentication Manager (der RSA SecurID-Server) installiert und richtig konfiguriert ist.
- Laden Sie die komprimierte Datei „sdconf.rec“ vom RSA SecurID-Server herunter und extrahieren Sie die Serverkonfigurationsdatei.

Vorgehensweise

1 Klicken Sie auf der Verwaltungsoberfläche im Bereich „Manuell konfigurieren“ auf **Auswählen**.

2 Klicken Sie unter „Allgemeine Einstellungen“ in der Zeile mit den Authentifizierungseinstellungen auf **Anzeigen**.

3 Klicken Sie in der RSA SecurID-Zeile auf das Zahnradsymbol.

4 Konfigurieren Sie die RSA SecurID-Seite.

   Beim Konfigurieren der Seite SecurID werden die auf dem RSA SecurID-Server verwendeten Informationen und generierten Dateien benötigt.

Option	Aktion
RSA SecurID aktivieren	Ändern Sie NEIN in **JA**, um die SecurID-Authentifizierung zu aktivieren.
*Name	Der Name lautet „securid-auth“.
*Anzahl an Wiederholungen	Geben Sie die Anzahl der zulässigen Anmeldeversuche ein. Dies ist die maximal zulässige Anzahl fehlgeschlagener Anmeldungen mit dem RSA SecurID-Token. Die Standardeinstellung lautet 5 Versuche. **Hinweis** Wenn mehr als ein Verzeichnis konfiguriert und die RSA SecurID-Authentifizierung für zusätzliche Verzeichnisse implementiert ist, konfigurieren Sie die **Anzahl der zulässigen Authentifizierungsversuche** für jede RSA SecurID-Konfiguration mit demselben Wert. Wenn die Werte nicht identisch sind, scheitert die SecurID-Authentifizierung.
*Externer HOST-Name	Geben Sie die IP-Adresse der Access Point-Instanz ein. Der eingegebene Wert muss mit dem Wert übereinstimmen, den Sie beim Hinzufügen der Access Point-Appliance als Authentifizierungs-Agent zum RSA SecurID-Server verwendet haben.
*Interner HOST-Name	Geben Sie den für **IP-Adresse** auf dem RSA SecurID-Server festgelegten Wert ein.
*Serverkonfiguration	Klicken Sie auf „Ändern“, um die RSA SecurID-Serverkonfigurationsdatei hochzuladen. Zuerst müssen Sie die komprimierte Datei vom RSA SecurID-Server herunterladen und die Serverkonfigurationsdatei (standardmäßig `sdconf.rec` benannt) extrahieren.
*Suffix für Namens-ID	Geben Sie die Namens-ID ein, mit der View TrueSSO bereitstellen kann.

Konfigurieren von RADIUS für Access Point

Sie können Access Point so konfigurieren, dass Benutzer die RADIUS-Authentifizierung nutzen müssen. Die RADIUS-Serverinformationen konfigurieren Sie in der Access Point-Appliance.

RADIUS unterstützt ein breites Spektrum an alternativen tokenbasierten Zwei-Faktor-Authentifizierungsmöglichkeiten. Da Zwei-Faktor-Authentifizierungslösungen, wie z. B. RADIUS, mit Authentifizierungs-Managern arbeiten, die auf separaten Servern installiert sind, muss der RADIUS-Server konfiguriert und für den Identity Manager-Dienst zugänglich sein.

Wenn sich die Benutzer anmelden und die RADIUS-Authentifizierung aktiviert ist, wird ein besonderes Anmeldedialogfeld im Browser angezeigt. Die Benutzer geben den Benutzernamen und Passcode der RADIUS-Authentifizierung in das Anmeldedialogfeld ein. Wenn der RADIUS-Server eine Zugriffshürde ausgibt, zeigt Access Point ein Dialogfeld an, in dem nach einem zweiten Passcode gefragt wird. Die Unterstützung für RADIUS-Aufforderungen ist derzeit auf die Eingabeaufforderung für Texteingaben begrenzt.

Nachdem ein Benutzer die Anmeldedaten in das Dialogfeld eingegeben hat, kann der RADIUS-Server eine SMS-Textnachricht oder eine E-Mail oder einen Text mithilfe anderer Out-of-Band-Mechanismen mit einem Code an das Mobiltelefon des Benutzers senden. Der Benutzer kann diesen Text und Code in das Anmeldedialogfeld eingeben, um die Authentifizierung abzuschließen.

Wenn der RADIUS-Server die Möglichkeit zum Importieren von Benutzern aus Active Directory bietet, werden die Endbenutzer möglicherweise erst aufgefordert, ihre Anmeldedaten für Active Directory einzugeben, bevor sie nach dem Benutzernamen und Passcode für die RADIUS-Authentifizierung gefragt werden.

Konfigurieren der RADIUS-Authentifizierung

Bei der Access Point-Appliance müssen Sie die RADIUS-Authentifizierung aktivieren, die Konfigurationseinstellungen vom RADIUS-Server angeben und den Authentifizierungstyp in RADIUS-Authentifizierung ändern.

Voraussetzungen

- Vergewissern Sie sich, dass auf dem Server, der als Authentifizierungsmanager dienen soll, die RADIUS-Software installiert und konfiguriert ist. Richten Sie den RADIUS-Server ein und konfigurieren Sie dann die RADIUS-Anforderungen von Access Point. Informationen zum Einrichten des RADIUS-Servers finden Sie in den Einrichtungs-Handbüchern Ihres RADIUS-Händlers.

Die folgenden RADIUS-Serverinformationen sind erforderlich.

- IP-Adresse oder DNS-Name des RADIUS-Servers.
- Portnummern der Authentifizierung. Der Authentifizierungsport ist normalerweise 1812.
- Authentifizierungstyp. Zu den Authentifizierungstypen zählen PAP (Password Authentication Protocol), CHAP (Challenge Handshake Authentication Protocol), MSCHAP1, MSCHAP2 (Microsoft Challenge Handshake Authentication Protocol, Version 1 und 2).
- Der gemeinsame geheime Schlüssel von RADIUS, der für die Verschlüsselung und Entschlüsselung in RADIUS-Protokollmeldungen verwendet wird.
- Spezielle Timeout- und Wiederholungswerte, die für die RADIUS-Authentifizierung erforderlich sind.

Vorgehensweise

1. Klicken Sie auf der Verwaltungsoberfläche im Bereich „Manuell konfigurieren“ auf **Auswählen**.
2. Klicken Sie unter „Allgemeine Einstellungen“ in der Zeile mit den Authentifizierungseinstellungen auf **Anzeigen**.
3. Klicken Sie in der Zeile RADIUS auf das Zahnradsymbol.

Option	Aktion
RADIUS aktivieren	Ändern Sie NEIN in **JA**, um die RADIUS-Authentifizierung zu aktivieren.
Name*	Der Name lautet „radius-auth“
Authentifizierungstyp*	Geben Sie das vom RADIUS-Server unterstützte Authentifizierungsprotokoll ein. Entweder PAP, CHAP, MSCHAP1 oder MSCHAP2.
Gemeinsamer geheimer Schlüssel*	Geben Sie den gemeinsamen geheimen Schlüssel von RADIUS ein.

Option	Aktion
Anzahl der zulässigen Authentifizierungsversuche*	Geben Sie die maximale Anzahl fehlgeschlagener Anmeldeversuche ein, bei denen Sie RADIUS für die Anmeldung verwendet haben. Die Standardeinstellung lautet drei Versuche.
Anzahl der Versuche für RADIUS-Server*	Geben Sie die Gesamtanzahl der Wiederholungsversuche ein. Wenn der primäre Server nicht antwortet, wartet der Dienst die konfigurierte Zeit, bevor er es erneut versucht.
Server-Zeitlimit in Sekunden*	Geben Sie den Timeout des RADIUS-Servers in Sekunden ein, nach dem eine Wiederholung gesendet wird, wenn der RADIUS-Server nicht antwortet.
RADIUS-Serverhostname*	Geben Sie den Hostnamen oder die IP-Adresse des RADIUS-Servers ein.
Authentifizierungsport*	Geben Sie die Nummer des Radius-Authentifizierungsports ein. Dies ist normalerweise Port 1812.
Bereichspräfix	(Optional) Die Position des Benutzerkontos wird „Realm“ genannt. Wenn Sie einen Realm-Präfix-String angeben, wird der String am Anfang des Benutzernamens platziert, wenn der Name an den RADIUS-Server gesendet wird. Wenn der Benutzername beispielsweise mit „jdoe“ angegeben wird und das Realm-Präfix DOMAIN-A\ angegeben wird, wird der Benutzername DOMAIN-A\jdoe an den RADIUS-Server gesendet. Wenn Sie diese Felder nicht konfigurieren, wird nur der eingegebene Benutzername gesendet.
Bereichssuffix	(Optional) Wenn Sie ein Realm-Suffix konfigurieren, wird dieses am Ende des Benutzernamens platziert. Wenn das Suffix z. B. @myco.com ist, wird der Benutzername jdoe@myco.com an den RADIUS-Server gesendet.
Suffix für Namens-ID	Geben Sie die Namens-ID ein, mit der View True SSO bereitstellen kann.
Passphrase-Hinweis für Anmeldeseite	Geben Sie den Textstring ein, der in der Meldung auf der Anmeldeseite des Benutzers angezeigt werden soll und die Benutzer auffordert, den richtigen Radius-Passcode einzugeben. Wenn dieses Feld z. B. mit **AD-Kennwort zuerst und dann SMS-Passcode** konfiguriert wird, steht in der Meldung der Anmeldeseite **Geben Sie zuerst Ihr AD-Kennwort und dann den SMS-Passcode ein.** Der Standardtextstring ist **RADIUS-Passcode**.
Sekundären Server aktivieren	Ändern Sie NEIN in **JA**, um einen sekundären RADIUS-Server für Hochverfügbarkeit zu konfigurieren. Konfigurieren Sie den sekundären Server wie in Schritt 3 beschrieben.

4 Klicken Sie auf **Speichern**.

Konfigurieren der adaptiven RSA-Authentifizierung in Access Point

Die adaptive RSA-Authentifizierung kann eingeführt werden, um eine stärkere Mehr-Faktoren-Authentifizierung zu bieten, als die einfache Authentifizierung bei Active Directory mit Benutzername und Kennwort. Die adaptive Authentifizierung überwacht und authentifiziert Anmeldeversuche des Benutzers basierend auf Risikostufen und Richtlinien.

Wenn die adaptive Authentifizierung aktiviert ist, werden die in den Risikorichtlinien angegebenen Risikoindikatoren verwendet, die in der Anwendung RSA-Richtlinienverwaltung und der Access Point-Konfiguration der adaptiven Authentifizierung aufgeführt sind, um festzulegen, ob ein Benutzer mit Benutzername und Kennwort authentifiziert wird oder ob zusätzliche Informationen erforderlich sind, um den Benutzer zu authentifizieren.

Unterstützte Authentifizierungsmethoden der adaptiven RSA-Authentifizierung

Die starken Authentifizierungsmethoden der adaptiven RSA-Authentifizierung, die in Access Point unterstützt werden, sind die Out-of-Band-Authentifizierung per Telefon, E-Mail- oder SMS-Textnachricht und anhand von Sicherheitsfragen. Mithilfe des Dienstes aktivieren Sie die Methoden der adaptiven RSA-Authentifizierung, die bereitgestellt werden können. Die Richtlinien der adaptiven RSA-Authentifizierung legen fest, welche sekundäre Authentifizierungsmethode verwendet wird.

Die Out-of-Band-Authentifizierung ist ein Prozess, bei dem zusammen mit dem Benutzernamen und dem Kennwort eine zusätzliche Überprüfung gesendet werden muss. Wenn sich die Benutzer beim adaptiven RSA-Authentifizierungsserver anmelden, geben sie eine E-Mail-Adresse, eine Telefonnummer oder beides an, je nach Serverkonfiguration. Wenn eine zusätzliche Überprüfung erforderlich ist, sendet der adaptive RSA-Authentifizierungsserver einen einmaligen Code über den bereitgestellten Kanal. Die Benutzer geben diesen Code zusammen mit ihrem Benutzernamen und dem Kennwort ein.

Bei der Anmeldung am adaptiven RSA-Authentifizierungsserver muss der Benutzer eine Reihe von Sicherheitsfragen beantworten. Sie können konfigurieren, wie viele Anmeldefragen gestellt werden und wie viele Sicherheitsfragen auf der Anmeldeseite angezeigt werden sollen.

Anmelden von Benutzern mit dem adaptiven RSA-Authentifizierungsserver

Die Benutzer müssen in der Datenbank des adaptiven RSA-Authentifizierungsservers registriert sein, um die adaptive Authentifizierung für die Authentifizierung zu nutzen. Bei der erstmaligen Anmeldung mit ihrem Benutzernamen und dem Kennwort werden die Benutzer der Datenbank des adaptiven RSA-Authentifizierungssystems hinzugefügt. Je nachdem, wie Sie die adaptive RSA-Authentifizierung im Dienst konfiguriert haben, werden die Benutzer bei der Anmeldung nach ihrer E-Mail-Adresse, der Telefonnummer oder der Nummer ihres SMS-Dienstes gefragt oder müssen Antworten auf Sicherheitsfragen eingeben.

Hinweis Die adaptive RSA-Authentifizierung lässt keine Benutzernamen zu, die internationale Zeichen enthalten. Wenn Sie Multi-Byte-Zeichen in den Benutzernamen zulassen möchten, wenden Sie sich an den RSA-Support, um die adaptive RSA-Authentifizierung und den RSA Authentication Manager zu konfigurieren.

Konfigurieren der adaptiven RSA-Authentifizierung in Access Point

Für die Konfiguration der adaptiven RSA-Authentifizierung in dem Dienst müssen Sie die adaptive RSA-Authentifizierung aktivieren. Wählen Sie die anzuwendende adaptive Authentifizierungsmethode aus und fügen Sie die Active Directory-Verbindungsinformationen und das Zertifikat hinzu.

Voraussetzungen

- Die adaptive RSA-Authentifizierung ist richtig mit den Authentifizierungsmethoden konfiguriert, die für die sekundäre Authentifizierung verwendet werden sollen.
- Einzelheiten zur SOAP-Endpunktadresse und zum SOAP-Endbenutzernamen.
- Active Directory-Konfigurationsinformationen und das verfügbare Active Directory-SSL-Zertifikat.

Vorgehensweise

1. Klicken Sie auf der Verwaltungsoberfläche im Bereich „Manuell konfigurieren“ auf **Auswählen**.
2. Klicken Sie unter „Allgemeine Einstellungen“ in der Zeile mit den Authentifizierungseinstellungen auf **Anzeigen**.
3. Klicken Sie in der Zeile der adaptiven RSA-Authentifizierung auf das Zahnradsymbol.
4. Wählen Sie die geeigneten Einstellungen für Ihre Umgebung aus.

   Hinweis Ein Asterisk (*) gibt an, welche Felder erforderlich sind. Die anderen Felder sind optional auszufüllen.

Option	Beschreibung
RSA AA-Adapter aktivieren	Ändern Sie NEIN in **JA**, um die adaptive RSA-Authentifizierung zu aktivieren.
Name*	Der Name lautet „rsaaa-auth“.

Option	Beschreibung
SOAP-Endpoint*	Geben Sie die SOAP-Endpunktadresse für die Integration zwischen dem Adapter der adaptiven RSA-Authentifizierung und dem Dienst ein.
SOAP-Benutzername*	Geben Sie den Benutzernamen und das Kennwort ein, die verwendet werden, um SOAP-Meldungen zu signieren.
SOAP-Kennwort*	Geben Sie das SOAP-API-Kennwort für die adaptive RSA-Authentifizierung ein.
RSA-Domäne	Geben Sie die Domänenadresse des adaptiven Authentifizierungsservers ein.
OOB-E-Mail aktivieren	Wählen Sie JA aus, um die Out-of-Band-Authentifizierung zu aktivieren, die einen einmaligen Code per E-Mail an den Endbenutzer sendet.
OOB-SMS aktivieren	Wählen Sie JA aus, um die Out-of-Band-Authentifizierung zu aktivieren, die einen einmaligen Code per SMS an den Endbenutzer sendet.
SecurID aktivieren	Wählen Sie JA aus, um SecurID zu aktivieren. Die Benutzer werden aufgefordert, ihren RSA-Token und den Passcode einzugeben.
Geheime Frage aktivieren	Wählen Sie JA aus, wenn Sie Anmeldefragen und Sicherheitsfragen für die Authentifizierung verwenden werden.
Anzahl der Anmeldefragen*	Geben Sie die Anzahl der Fragen ein, die die Benutzer einrichten müssen, wenn Sie sich beim Authentifizierungsadapterserver anmelden.
Anzahl der Sicherheitsfragen*	Geben Sie die Anzahl der Sicherheitsfragen an, die die Benutzer richtig beantworten müssen, um sich anmelden zu können.
Anzahl der zulässigen Authentifizierungsversuche*	Geben Sie an, wie häufig die Sicherheitsfragen einem Benutzer, der versucht sich anzumelden, angezeigt werden sollen, bevor die Authentifizierung fehlschlägt.
Verzeichnistyp*	Das einzige Verzeichnis, das unterstützt wird, ist Active Directory.
SSL verwenden	Wählen Sie JA aus, wenn Sie für Ihre Active Directory-Verbindung SSL verwenden. Sie fügen das Active Directory-SSL-Zertifikat im Feld „Verzeichniszertifikat“ hinzu.
Server-Host*	Geben Sie den Active Directory-Hostnamen ein.
Server-Port	Geben Sie die Active Directory-Portnummer ein.
DNS-Dienstspeicherort verwenden	Wählen Sie JA aus, wenn für die Verzeichnisverbindung der DNS-Dienstspeicherort verwendet wird.
Basis-DN	Geben Sie den DN ein, von dem aus Kontosuchvorgänge gestartet werden sollen. Beispiel: OU=MeineEinheit,DC=MeineFirma,DC=com.
Bind-DN*	Geben Sie das Konto ein, das nach Benutzern suchen darf. Beispiel: CN=binduser,OU=myUnit,DC=myCorp,DC=com
Bind-Kennwort	Geben Sie das Kennwort für das Bind-DN-Konto ein.
Suchattribut	Geben Sie das Kontoattribut ein, das den Benutzernamen enthält.
Verzeichniszertifikat	Fügen Sie das Serverzertifikat des Verzeichnisses zum Einrichten sicherer SSL-Verbindungen dem Textfeld hinzu. Fügen Sie im Falle mehrerer Server das Root-Zertifikat der Zertifizierungsstelle hinzu.
STARTTLS verwenden	Ändern Sie NEIN in **JA**, um STARTTLS zu verwenden.

5 Klicken Sie auf **Speichern**.

Generieren von Access Point -SAML-Metadaten

Sie müssen SAML-Metadaten in der Access Point-Appliance generieren und die Metadaten mit dem Server austauschen, um die erforderliche gegenseitige Vertrauensstellung für die Smartcard-Authentifizierung einzurichten.

Die Security Assertion Markup Language (SAML) ist ein XML-basierter Standard, der zur Beschreibung und zum Austausch von Authentifizierungs- und Autorisierungsinformationen zwischen unterschiedlichen Sicherheitsdomänen verwendet wird. SAML überträgt Informationen zu Benutzern zwischen Identitätsanbietern und Dienstanbietern in XML-Dokumenten namens SAML-Zusicherungen. In diesem Szenario ist Access Point der Identitätsanbieter und der Server der Dienstanbieter.

Voraussetzungen

- Konfigurieren Sie die Uhr (UTC) der Access Point-Appliance, damit diese über die korrekte Uhrzeit verfügt. Öffnen Sie z. B. ein Konsolenfenster auf der virtuellen Access Point-Maschine, und wählen Sie mit den Pfeilschaltflächen die erforderliche Zeitzone aus. Stellen Sie zudem sicher, dass die Uhrzeit des ESXi-Hosts mit einem NTP-Server synchronisiert ist. Prüfen Sie, ob die VMware Tools, die auf der virtuellen Appliance-Maschine ausgeführt werden, die Uhrzeit auf der virtuellen Maschine mit der Uhrzeit auf dem ESXi-Host synchronisieren.

  Wichtig Wenn die Uhr der Access Point-Appliance nicht der Uhr auf dem Serverhost entspricht, kann die Smartcard-Authentifizierung eventuell nicht durchgeführt werden.

- Verwenden Sie ein SAML-Signaturzertifikat für das Signieren der Access Point-Metadaten.

  Hinweis VMware empfiehlt die Erstellung und Verwendung eines spezifischen SAML-Signaturzertifikats, wenn in Ihrer Installation mehr als eine Access Point-Appliance vorhanden ist. In diesem Fall müssen alle Appliances mit demselben Signaturzertifikat konfiguriert werden, damit der Server Assertions von jeder Access Point-Appliance annehmen kann. Mit einem spezifischen SAML-Signaturzertifikat sind die SAML-Metadaten aller Appliances identisch.

- Sofern noch nicht geschehen, konvertieren Sie das SAML-Signaturzertifikat in PEM-Dateien und die `.pem`-Dateien in ein einzeiliges Format. Siehe Konvertieren von Zertifikatdateien in das einzeilige PEM-Format.

Vorgehensweise

1. Klicken Sie auf der Verwaltungsoberfläche im Bereich „Manuell konfigurieren“ auf **Auswählen**.
2. Klicken Sie im Bereich „Erweiterte Einstellungen“ auf das Zahnradsymbol für die **SAML-Identitätsanbietereinstellungen**.
3. Aktivieren Sie das Kontrollkästchen **Zertifikat bereitstellen**.
4. Um die Datei des privaten Schlüssels hinzuzufügen, klicken Sie auf **Auswählen** und suchen Sie nach der Datei mit dem privaten Schlüssel für das Zertifikat.

5 Um die Datei der Zertifikatkette hinzuzufügen, klicken Sie auf **Auswählen** und suchen Sie nach der Datei der Zertifikatkette.

6 Klicken Sie auf **Speichern**.

7 Geben Sie im Textfeld „Hostname“ den Hostnamen ein und laden Sie die Einstellungen des Identitätsanbieters herunter.

Erstellen eines SAML-Authentifikators für die Verwendung von anderen Dienstanbietern

Nachdem Sie die SAML-Metadaten in der Access Point-Appliance erstellt haben, kopieren Sie die Daten in den Backend-Dienstanbieter. Das Kopieren dieser Daten zum Dienstanbieter gehört zum Vorgang des Erstellens eines SAML-Authentifikators, damit Access Point als Dienstanbieter verwendet werden kann.

Für einen Horizon Air Hybrid-mode Server finden Sie spezielle Anweisungen in der Produktdokumentation.

Kopieren von SAML-Metadaten des Dienstanbieters nach Access Point

Nachdem Sie einen SAML-Authentifikator erstellt sowie aktiviert haben und Access Point sich damit als Identitätsanbieter verwenden lässt, können Sie auf diesem Backend-System SAML-Metadaten generieren und diese zum Erstellen eines Dienstanbieters in der Access Point-Appliance verwenden. Dieser Datenaustausch richtet eine Vertrauensstellung zwischen dem Identitätsanbieter (Access Point) und dem Backend-Dienstanbieter, zum Beispiel einem View-Verbindungsserver, ein.

Voraussetzungen

Stellen Sie sicher, dass ein SAML-Authentifikator für Access Point auf dem Backend-Dienstanbieter erstellt wurde.

Vorgehensweise

1 Rufen Sie die SAML-Metadaten vom Dienstanbieter ab. Diese liegen im Allgemeinen in Form einer XML-Datei vor.

   Anweisungen dazu finden Sie in der Dokumentation des Dienstanbieters.

   Für die einzelnen Dienstanbieter gelten verschiedene Vorgehensweisen. Sie müssen beispielsweise einen Browser öffnen und eine URL wie die folgende eingeben: https://*connection-server.example.com*/SAML/metadata/sp.xml

   Mit dem Befehl **Speichern unter** können Sie diese Webseite dann als XML-Datei speichern. Der Inhalt dieser Datei beginnt mit dem folgenden Text:

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

2 Klicken Sie auf der Access Point-Verwaltungsoberfläche im Bereich „Manuell konfigurieren“ auf **Auswählen**.

3 Klicken Sie im Bereich „Erweiterte Einstellungen“ auf das Zahnradsymbol für die **SAML-Serveranbietereinstellungen**.

4 Geben Sie im Textfeld für den Dienstanbieternamen den Namen des Dienstanbieters ein.

5 Geben Sie im Textfeld für Metadaten-XML die in Schritt 1 erstellte Metadatendatei ein.

6 Klicken Sie auf **Speichern**.

Access Point und der Dienstanbieter können nun Authentifizierungs- und Autorisierungsinformationen austauschen.

Fehlerbehebung bei der Access Point-Bereitstellung 7

Sie können Probleme, die bei der Bereitstellung von Access Point in Ihrer Umgebung auftreten, anhand verschiedener Verfahren diagnostizieren und korrigieren.

Sie können die Vorgehensweisen zur Fehlerbehebung nutzen, um die Ursachen dieser Probleme zu ermitteln. Anschließend können Sie versuchen, die Probleme selbst zu behandeln, oder sich an den technischen Support von VMware wenden, um Unterstützung zu erhalten.

Dieses Kapitel behandelt die folgenden Themen:

Fehlerbehebung bei Bereitstellungsfehlern

Möglicherweise treten Probleme beim Bereitstellen von Access Point in Ihrer Umgebung auf. Sie können diese Probleme bei der Bereitstellung anhand mehrerer Verfahren diagnostizieren und korrigieren.

Sicherheitswarnung beim Ausführen von Skripten, die aus dem Internet heruntergeladen wurden

Stellen Sie sicher, dass das PowerShell-Skript das gewünschte Skript ist, und führen Sie dann in der PowerShell-Konsole den folgenden Befehl aus:

```
unblock-file .\apdeploy.ps1
```

ovftool-Befehl nicht gefunden

Stellen Sie sicher, dass Sie die OVF Tool-Software auf dem Windows-Computer installiert haben und dass sie in dem vom Skript erwarteten Verzeichnis installiert ist.

Invalid-Netzwerk in Eigenschaft netmask1

- In der Meldung kann netmask0, netmask1 oder netmask2 angegeben werden. Stellen Sie sicher, dass ein Wert in der .INI-Datei für jedes der drei Netzwerke festgelegt wurde, wie netInternet, netManagementNetwork und netBackendNetwork.

- Stellen Sie sicher, dass ein vSphere-Netzwerkprotokollprofil mit jedem referenzierten Netzwerknamen verknüpft wurde. Dadurch werden Netzwerkeinstellungen wie IPv4-Subnetzmaske, Gateway usw. angegeben. Stellen Sie sicher, dass das verknüpfte Netzwerkprotokollprofil die richtigen Werte für jede der Einstellungen aufweist.

Warnmeldung, dass der Bezeichner des Betriebssystems nicht unterstützt wird

Mit der Warnmeldung wird darauf hingewiesen, dass der angegebene Betriebssystembezeichner SUSE Linux Enterprise Server 12.0 64-Bit (id:85) auf dem gewählten Host nicht unterstützt wird. Er ist dem folgenden OS-Bezeichner zugeordnet: Other Linux (64-Bit).

Ignorieren Sie diese Warnmeldung. Es erfolgt die automatische Zuordnung zu einem unterstützten Betriebssystem.

Access Point für RSA SecurID-Authentifizierung konfigurieren

Fügen Sie die folgenden Zeilen dem Horizon-Abschnitt der .INI-Datei hinzu.

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

Fügen Sie am Ende der .INI-Datei einen neuen Abschnitt hinzu.

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

Die IP-Adressen sollten beide auf die IP-Adresse von Access Point gesetzt werden. Die sdconf.rec-Datei wird von RSA Authentication Manager abgerufen, der vollständig konfiguriert sein muss. Stellen Sie sicher, dass Sie Access Point 2.5 oder höher verwenden und dass Access Point im Netzwerk auf den RSA Authentication Manager-Server zugreifen kann. Führen Sie den Powershell-Befehl „apdeploy“ erneut aus, um den für RSA SecurID konfigurierten Access Point erneut bereitzustellen.

Fehler: Locator verweist auf kein Objekt

Der Fehler gibt an, dass der von vSphere OVF Tool verwendete target=-Wert für Ihre vCenter-Umgebung nicht richtig ist. In der unter https://communities.vmware.com/docs/DOC-30835 aufgeführten Tabelle finden Sie Beispiele für das Zielformat zum Verweis auf einen vCenter-Host oder einen Cluster. Das Objekt der obersten Ebene wird wie folgt angegeben:

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

Das Objekt listet jetzt die möglichen Namen zur Verwendung auf der nächsten Ebene auf.

```
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
```

Bei den im Ziel verwendeten Ordner-, Host- und Clusternamen wird die Groß-/Kleinschreibung beachtet.

Sammeln von Protokollen der Access Point-Appliance

Um eine ZIP-Datei mit Protokollen Ihrer Access Point-Appliance zu erhalten, können Sie in einen Browser eine entsprechende URL eingeben.

Verwenden Sie für das Sammeln der Protokolle Ihrer Access Point-Appliance die folgende URL:

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

In diesem Beispiel stellt *access-point-appliance.example.com* den vollqualifizierten Domänennamen (FQDN) der Access Point-Appliance dar.

Diese Protokolldateien wurden aus dem Verzeichnis `/opt/vmware/gateway/logs` der Appliance erfasst.

Die folgende Tabelle enthält Beschreibungen der verschiedenen in der ZIP-Datei enthaltenen Dateien.

Tabelle 7-1. Dateien mit Systeminformationen für die Fehlerbehebung

Dateiname	Beschreibung
`df.log`	Enthält Informationen über die Nutzung des Festplattenspeichers.
`netstat.log`	Enthält Informationen über Netzwerkverbindungen.
`ap_config.json`	Enthält die aktuellen Konfigurationseinstellungen für die Access Point-Appliance.
`ps.log`	Enthält eine Verarbeitungsliste.
`ifconfig.log`	Enthält Informationen über Netzwerkschnittstellen.
`free.log`	Enthält Informationen über die Nutzung des Arbeitsspeichers.

Tabelle 7-2. Protokolldateien für Access Point

Dateiname	Beschreibung
`esmanager.log`	Enthält Protokollmeldungen des Edge Service Manager-Prozesses, der die Ports 443 und 80 abhört.
`authbroker.log`	Enthält Protokollmeldungen des AuthBroker-Prozesses, der die Authentifizierungsadapter steuert.
`admin.log`	Enthält Protokollmeldungen des Prozesses, der die Access Point-REST-API auf Port 9443 bereitstellt.
`admin-zookeeper.log`	Enthält Protokollmeldungen zum Daten-Layer für das Speichern der Access Point-Konfigurationsinformationen.
`tunnel.log`	Enthält Protokollmeldungen aus dem Tunnelprozess, der Teil der XML-API-Verarbeitung ist.

Tabelle 7-2. Protokolldateien für Access Point (Fortsetzung)

Dateiname	Beschreibung
`bsg.log`	Enthält Protokollmeldungen aus dem Blast Secure Gateway.
`SecurityGateway_*.log`	Enthält Protokollmeldungen aus dem PCoIP Secure Gateway.

Die Protokolldateien mit der Endung „`–std–out.log`“ enthalten Informationen für `stdout` von verschiedenen Prozessen und sind in der Regel leer.

Access Point-Protokolldateien für AirWatch

- `/var/log/airwatch/tunnel/vpnd`

  Die Dateien tunnel-init.log und tunnel.log werden in diesem Verzeichnis erfasst.

- `/var/log.airwatch/proxy`

  Die Datei proxy.log wird in diesem Verzeichnis erfasst.

- `/var/log/airwatch/appliance–agent`

  Die Datei appliance-agent.log wird in diesem Verzeichnis erfasst.

Aktivieren des Debug-Modus

Sie können den Debug-Modus für eine Access Point-Appliance aktivieren, um den internen Status der Appliance anzuzeigen oder zu ändern. Anhand des Debug-Modus können Sie das Bereitstellungsszenario in Ihrer Umgebung testen.

Voraussetzungen

- Stellen Sie sicher, dass die Access Point-Appliance nicht verwendet wird.

  Hinweis Es bietet sich an, Protokollierungsinformationen für eine nicht funktionsfähige Access Point-Appliance zu sammeln. Die Protokolle können auf die herkömmliche Art erfasst werden.

Vorgehensweise

1. Melden Sie sich beim Access Point-Computer an.
2. Geben Sie den folgenden Befehl in die Befehlszeilenschnittstelle ein.

   ```
   cd /opt/vmare/gateway/conf
   ```

3. Zeigen Sie die Protokolleigenschaftsdatei an.

   ```
   vi log4j–esmanager.properties
   ```

4. Suchen Sie die folgende Zeile in der Eigenschaftsdatei und bearbeiten Sie sie. Ersetzen Sie „info“ durch „debug“.

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

5 Geben Sie den Befehl ein, um die Protokollierungskonfiguration über jeden Pfad zu ändern.

```
supervisorctl restart esmanager
```