Bereitstellen und Konfigurieren von VMware Unified Access Gateway

Unified Access Gateway 2.9

Dieses Dokument unterstützt die aufgeführten Produktversionen sowie alle folgenden Versionen, bis das Dokument durch eine neue Auflage ersetzt wird. Die neuesten Versionen dieses Dokuments finden Sie unter http://www.vmware.com/de/support/pubs.

DE-002471-00

vmware®

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

http://www.vmware.com/de/support/

Auf der VMware-Website finden Sie auch die aktuellen Produkt-Updates.

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 Unified Access Gateway

Bereitstellen und Konfigurieren von Unified Access Gateway bietet Informationen zum Konzipieren einer Bereitstellung von VMware Horizon®, VMware Identity Manager™ und VMware AirWatch®, die VMware Unified Access Gateway™ 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 Unified Access Gateway-Appliances und für die Änderung der Konfigurationseinstellungen nach der Bereitstellung.

Zielgruppe

Diese Informationen richten sich an Benutzer, die Unified Access Gatewaybereitstellen 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 VMware Unified Access Gateway 1

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

Hinweis VMware Unified Access Gateway® hieß früher VMware Access Point.

Dieses Kapitel behandelt die folgenden Themen:

Unified Access Gateway als sicheres Gateway

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

Unified Access Gateway 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 sorgt Unified Access Gateway dafür, dass der Datenverkehr für einen authentifizierten Benutzer nur an Desktop- und Anwendungsressourcen geleitet werden kann. Hierbei verfügt der Benutzer über entsprechende Berechtigungen. 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.

Unified Access Gateway dient als Proxy-Host für Verbindungen innerhalb des vertrauenswürdigen Netzwerks eines Unternehmens. Dieses Konzept bietet eine zusätzliche Schutzschicht durch Abschirmung der virtuellen Desktops, Anwendungshosts und Server gegenüber dem öffentlichen Internet.

Unified Access Gateway ist speziell auf die DMZ ausgelegt. 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

Verwenden von Unified Access Gateway anstelle eines Virtual Private Network

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

Unified Access Gateway bietet im Vergleich zu einem generischen VPN die folgenden Vorteile.

- Access Control Manager Unified Access Gateway wendet Zugriffsregeln automatisch an. Unified Access Gateway erkennt die Berechtigungen der Benutzer und die zur internen Verbindung erforderliche Adressierung. 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 Unified Access Gateway nimmt keine Änderungen an der unkomplizierten Benutzeroberfläche von Horizon Client vor. Mit Unified Access Gateway 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 Unified Access Gateway ist für maximale Sicherheit und Leistung konzipiert. Mit Unified Access Gateway 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 Unified Access Gateway

Damit Sie die Unified Access Gateway-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 Unified Access Gateway 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.

Hardwareanforderungen für den ESXi-Server

Die Unified Access Gateway-Appliance muss unter einer vSphere-Version bereitgestellt werden, die mit der Version identisch ist, die für die von Ihnen verwendeten VMware-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 Unified Access Gateway-Appliance, damit diese über die korrekte Uhrzeit verfügt. Öffnen Sie z. B. ein Konsolenfenster auf der virtuellen Unified Access Gateway-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 Unified Access Gateway-Appliance wählt automatisch die für Unified Access Gateway 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: 1,4 GB
- Minimal erforderlicher Festplattenspeicher bei schlanker Speicherzuweisung: 2,3 GB
- Minimal erforderlicher Festplattenspeicher bei starker Speicherzuweisung: 20 GB

Für die Bereitstellung der virtuellen Appliance sind folgende Informationen erforderlich:

- Statische IP-Adresse (empfohlen)
- IP-Adresse des DNS-Servers
- Kennwort für den Root-Benutzer
- Kennwort für den Administratorbenutzer
- URL der Serverinstanz des Lastausgleichsdiensts, auf die die Unified Access Gateway-Appliance verweist

Hardwareanforderungen bei Verwendung von Windows Hyper-V Server

Bei Verwendung von Unified Access Gateway in einer AirWatch-Bereitstellung für App-spezifische Tunnel können Sie die Unified Access Gateway-Appliance auf einem Microsoft Hyper-V-Server installieren.

Die Microsoft-Server Windows Server 2012 R2 und Windows Server 2016 werden unterstützt.

Anforderungen an die Netzwerkkonfiguration

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

- Eine Netzwerkschnittstelle ist für POCs (Proof of Concept, Machbarkeitsstudie) oder für Testvorgänge ausreichend. Bei einer NIC 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 Unified Access Gateway-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.

Unified Access Gateway kann ohne IP-Pools (vCenter Server) erfolgreich bereitgestellt werden. Wenn Sie jedoch versuchen, im Browser über die Verwaltungsoberfläche auf Unified Access Gateway zuzugreifen, wird die Verwaltungsoberfläche nicht gestartet.

Anforderungen für die Protokollspeicherung

Für die Protokolldateien ist standardmäßig ein bestimmter Teil des Speicherplatzes im Aggregat vorgesehen. Die Protokolle für Unified Access Gateway werden standardmäßig archiviert. Um diese Protokolleinträge beizubehalten, speichern Sie diese mit Syslog. Siehe „Erfassen von Protokollen auf der Unified Access Gateway-Appliance“, auf Seite 77.

Firewall-Regeln für Umkreisnetzwerk-basierte Unified Access Gateway -Appliances

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

Die Bereitstellung einer Umkreisnetzwerk-basierten Unified Access Gateway-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 (in der demilitarisierten Netzwerkzone/DMZ) eingehende Kommunikation streng kontrolliert, wodurch das Risiko einer Gefährdung des internen Netzwerks stark vermindert wird.

Damit sich externe Client-Geräte in der DMZ mit einer Unified Access Gateway-Appliance verbinden können, muss die Front-End-Firewall Datenverkehr an bestimmten Ports zulassen. Standardmäßig werden die externen Client-Geräte und externen Webclients (HTML Access) mit einer Unified Access Gateway-Appliance in der DMZ an TCP-Port 443 verbunden. Wenn Sie das Blast-Protokoll verwenden, muss Port 8443 in der Firewall geöffnet sein, Sie können Blast jedoch auch für Port 443 konfigurieren.

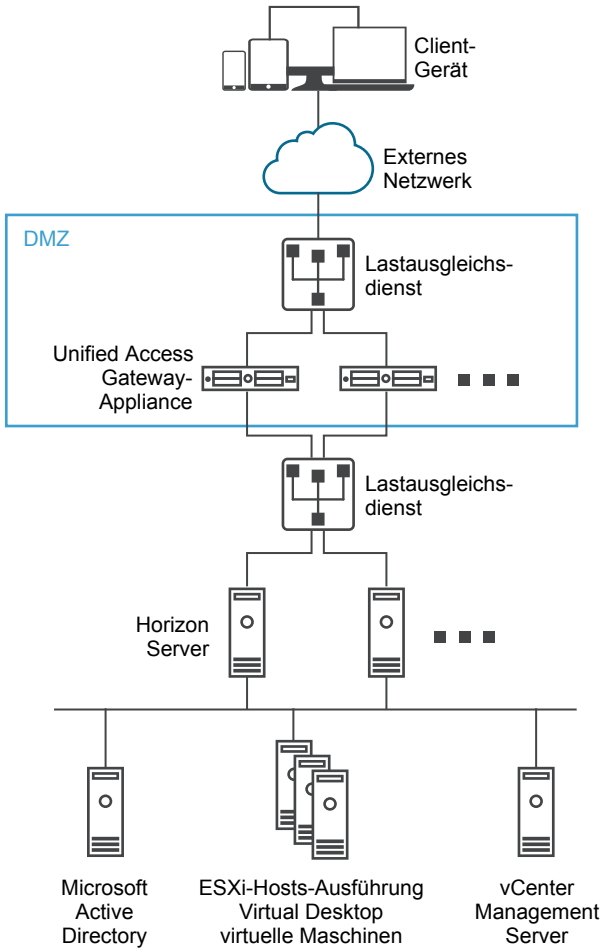
Tabelle 1-1. Port-Anforderungen

Port	Portal	Quelle	Ziel	Beschreibung
443	TCP	Internet	Unified Access Gateway	Datenverkehr aus dem Internet, Horizon Client XML-API, Horizon Tunnel und Blast Extreme
443	UDP	Internet	Unified Access Gateway	UDP (optional)
8443	UDP	Internet	Unified Access Gateway	Blast Extreme (optional)
8443	TCP	Internet	Unified Access Gateway	Blast Extreme
4172	TCP und UDP	Internet	Unified Access Gateway	PCoIP (optional)
443	TCP	Unified Access Gateway	Horizon Broker	Horizon Client XML-API
22443	TCP und UDP	Unified Access Gateway	Desktops und RDS-Hosts	Blast Extreme
4172	TCP und UDP	Unified Access Gateway	Desktops und RDS-Hosts	PCoIP (optional)
32111	TCP	Unified Access Gateway	Desktops und RDS-Hosts	Framework-Kanal für USB-Umleitung
9427	TCP	Unified Access Gateway	Desktops und RDS-Hosts	MMR und CDR
9443	TCP	Verwaltungsoberfläche	Unified Access Gateway	Schnittstelle zur Verwaltung

Hinweis Für alle UDP-Ports müssen Weiterleitungs- und Antwort-Datagramme erlaubt sein.

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

Abbildung 1-1. Unified Access Gateway in einer DMZ-Topologie



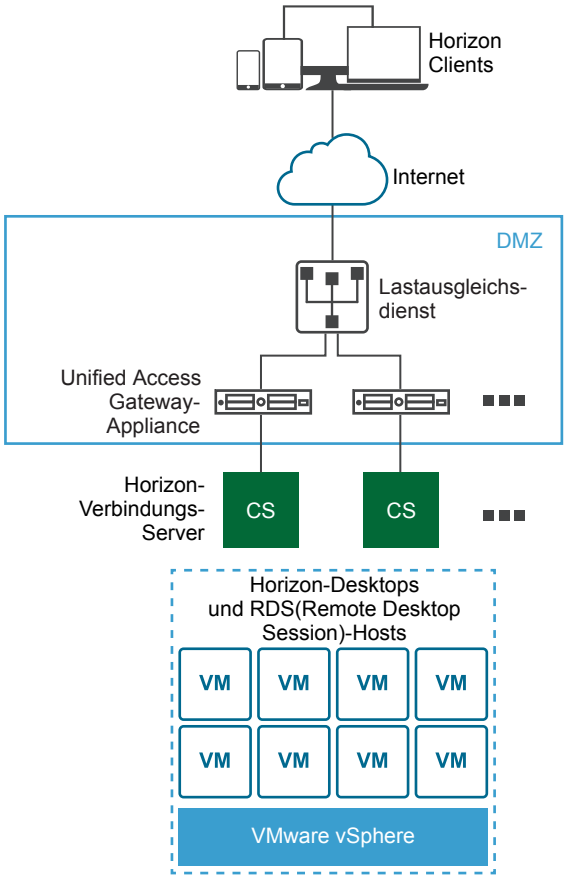
Unified Access Gateway -Topologien für den Lastausgleich

Eine Unified Access Gateway-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. Unified Access Gateway-Appliances können mit Standardlösungen von Drittanbietern für den Lastausgleichsdienst verwendet werden, die für HTTPS konfiguriert sind.

Wenn die Unified Access Gateway-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 Unified Access Gateway haben Sie die Möglichkeit, mit der Unified Access Gateway-Appliance auf denselben Lastausgleichsdienst zu verweisen, der des öfteren bereits verwendet wird.

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

Abbildung 1-2. Mehrere Unified Access Gateway -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. Das Protokoll verwendet strukturierte XML-Nachrichten über HTTPS. Dieses Protokoll wird teilweise als Horizon XML-API-Steuerungsprotokoll bezeichnet. In einer Umgebung mit Lastausgleich, wie sie in der Abbildung „Mehrere Unified Access Gateway-Appliances hinter einem Lastausgleichsdienst“ dargestellt ist, leitet der Lastausgleichsdienst diese Verbindung an eine der Unified Access Gateway-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 Unified Access Gateway-Appliances.

- Sekundäre Horizon-Protokolle

Nachdem der Horizon Client eine sichere Kommunikation mit einer der Unified Access Gateway-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, TCP 8443, UDP 443 und UDP 8443)
- PCoIP-Anzeigeprotokoll (TCP 443, UDP 443).

Diese sekundären Horizon-Protokolle müssen zu derselben Access Point-Appliance weitergeleitet werden, zu der das primäre Horizon-Protokoll weitergeleitet wurde. Unified Access Gateway kann die sekundären Protokolle dann auf der Grundlage der authentifizierten Benutzersitzung autorisieren. Eine wichtige Sicherheitsfunktion von Unified Access Gateway besteht darin, dass Unified Access Gateway nur dann Datenverkehr in das Datencenter des Unternehmens weiterleitet, wenn der Datenverkehr zu einem authentifizierten Benutzer gehört. Wenn das sekundäre Protokoll fälschlicherweise an eine andere Unified Access Gateway-Appliance weitergeleitet wird als das primäre Protokoll, werden Benutzer nicht autorisiert und in der 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 Unified Access Gateway mit mehreren Netzwerkschnittstellenkarten

Eine der Konfigurationseinstellungen für Unified Access Gateway betrifft die Anzahl der zu verwendenden virtuellen NICs (Network Interface Cards). Wenn Sie Unified Access Gateway bereitstellen, wählen Sie eine Bereitstellungskonfiguration für Ihr Netzwerk aus.

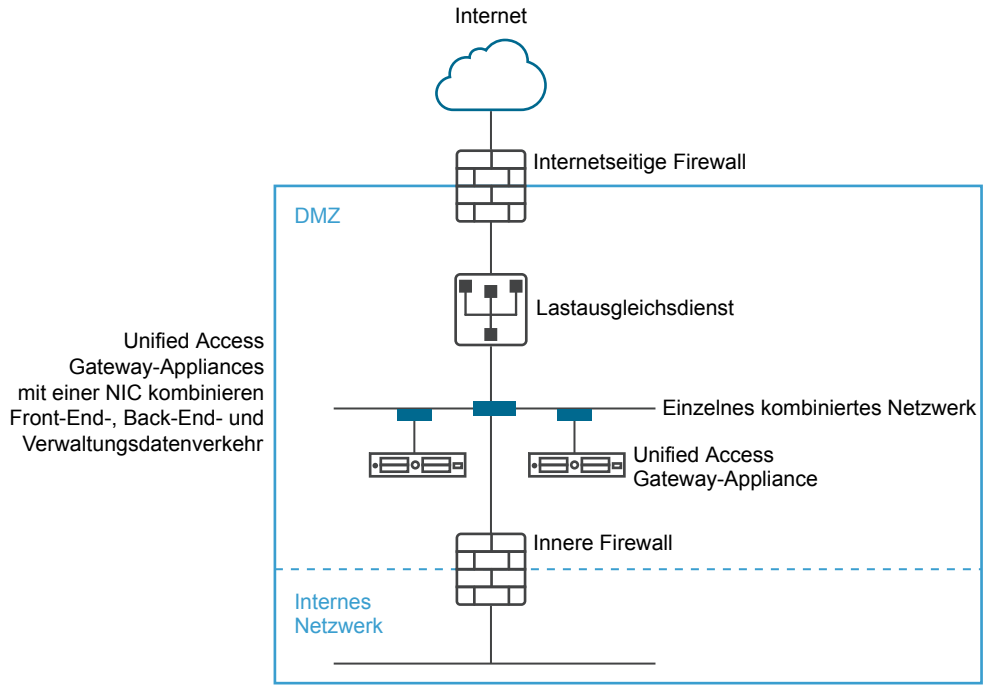
Sie können eine, zwei oder drei NICs festlegen, die mit „onenic“, „twonic“ oder „threenic“ angegeben werden.

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 Unified Access Gateway 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 Unified Access Gateway-Appliances geleitet. Unified Access Gateway leitet den autorisierten Datenverkehr dann durch die innere Firewall an Ressourcen im internen Netzwerk. Unified Access Gateway blockiert nicht autorisierten Datenverkehr.

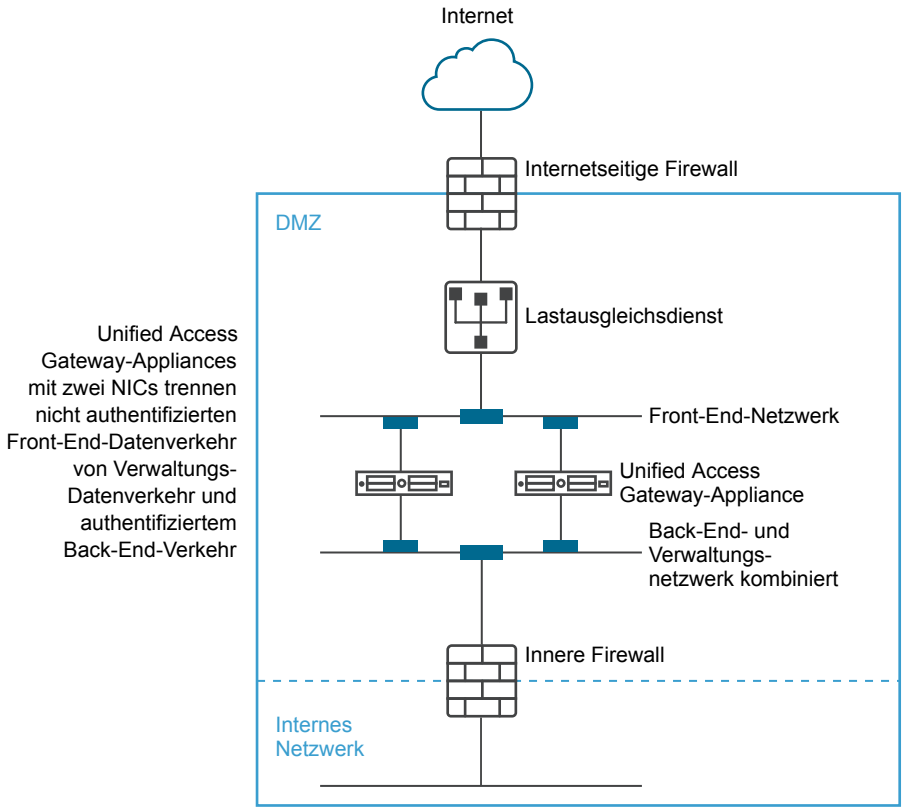
Abbildung 1-3. Unified Access Gateway mit einer NIC



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. Unified Access Gateway mit zwei NICs



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

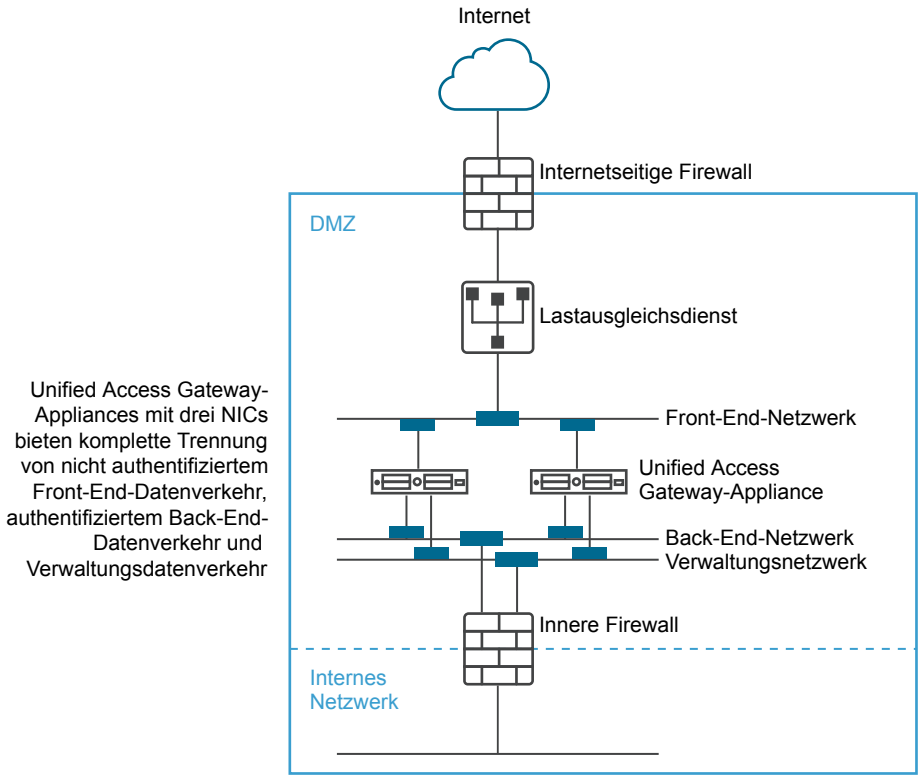
Wenn ein Gerät, z. B. der Lastausgleichsdienst, im nicht authentifizierten Front-End-Netzwerk kompromittiert wurde, dann ist es in einer Bereitstellung mit zwei NICs nicht möglich, das Gerät so umzukonfigurieren, dass Unified Access Gateway umgangen wird. Firewall-Regeln der Schicht 4 sind mit der Unified Access Gateway-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 Unified Access Gateway 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 können Sie zusätzliche Infrastruktursysteme wie DNS-Server oder RSA SecurID-Authentifizierungsmanager-Server so konfigurieren, dass sie sich im Back-End-Netzwerk innerhalb der DMZ befinden und 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 Unified Access Gateway-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.

Unified Access Gateway 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. Unified Access Gateway mit drei NICs



Upgrade ohne Ausfallzeit

Durch Upgrades ohne Ausfallzeit können Sie ein Upgrade für Unified Access Gateway durchführen, ohne dass die Verfügbarkeit für Benutzer unterbrochen wird. Bevor Sie ein Upgrade für eine Unified Access Gateway-Appliance durchführen, wird der Stilllegungsmodus der Unified Access Gateway-Systemkonfigurationsseiten von NEIN zu JA geändert.

Wenn der Wert für den Stilllegungsmodus „Ja“ lautet, wird bei der Integritätsprüfung durch den Lastausgleichsdienst die Unified Access Gateway-Appliance als nicht verfügbar angezeigt. Anforderungen, die den Lastausgleichsdienst erreichen, werden an die nächste Unified Access Gateway-Appliance hinter dem Lastausgleich gesendet.

Voraussetzungen

- Mindestens zwei Unified Access Gateway-Appliances, die hinter dem Lastausgleichsdienst konfiguriert sind
- Eine für die Einstellung „URL für Integritätsprüfung“ konfigurierte URL, mit der der Lastausgleichsdienst eine Verbindung herstellt, um die Integrität der Unified Access Gateway-Appliance zu prüfen.
- Prüfen Sie die Integrität der Appliance im Lastausgleichsdienst. Geben Sie den REST-API-Befehl `GET https://mycoUnifiedAccessGateway.com:443/favicon.ico` ein.

  Die Antwort lautet `HTTP/1.1 200 OK`, wenn für den Stilllegungsmodus „Nein“ eingestellt ist. Sie lautet `HTTP/1.1 503`, wenn für den Stilllegungsmodus „Ja“ eingestellt ist.

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 Aktivieren Sie in der Zeile **Stilllegungsmodus** den Wert **Ja**, um die Unified Access Gateway-Appliance anzuhalten.

   Wenn die Appliance angehalten wird, werden bestehende Sitzungen, für die die Appliance verwendet wird, 10 Stunden lang aufrechterhalten, bevor sie geschlossen werden.

4 Klicken Sie auf **Speichern**.

Neue Anforderungen an den Lastausgleichsdienst werden an die nächste Unified Access Gateway-Appliance gesendet.

Weiter

Exportieren Sie die Einstellungen der angehaltenen Unified Access Gateway-Appliance. Stellen Sie eine neue Unified Access Gateway-Version bereit und importieren Sie die Einstellungen. Die neue Version der Unified Access Gateway-Appliance kann dem Lastausgleichsdienst hinzugefügt werden.

Bereitstellen der Unified Access Gateway -Appliance 2

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

Zur Installation der Unified Access Gateway-Appliance auf einem vSphere ESX- oder ESXi-Host können primär zwei Methoden verwendet werden. Microsoft Server 2012 und 2016 Hyper-V-Rollen werden unterstützt.

- Die Unified Access Gateway-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 Unified Access Gateway-Verwaltungsoberfläche an, um die Unified Access Gateway-Systemeinstellungen zu konfigurieren, die sicheren Edgedienste für mehrere Anwendungsfälle einzurichten und die Authentifizierung in der DMZ zu konfigurieren. Siehe „Bereitstellen von Unified Access Gateway mit dem OVF-Vorlagenassistenten“, auf Seite 20.
- PowerShell-Skripte können eingesetzt werden, um Unified Access Gateway 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 Unified Access Gateway bereitzustellen. Siehe „Verwenden von PowerShell zur Bereitstellung der Unified Access Gateway-Appliance“, auf Seite 28.

Hinweis Bei Verwendung der Unified Access Gateway-Appliance in einer AirWatch-Umgebung für App-spezifische Tunnel- und Proxy-Bereitstellungen können Sie Unified Access Gateway auf einer virtuellen Windows Hyper-V-Maschine installieren.

Dieses Kapitel behandelt die folgenden Themen:

Bereitstellen von Unified Access Gateway mit dem OVF-Vorlagenassistenten

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

Wenn Sie die OVF-Vorlage bereitstellen, konfigurieren Sie, wie viele Netzwerkschnittstellen (Network Interfaces/NIC) erforderlich sind, und legen die IP-Adresse sowie die Kennwörter für den Administrator und den Root-Benutzer fest.

Nach der Bereitstellung von Unified Access Gateway wechseln Sie zur Benutzeroberfläche für die Verwaltung, um die Unified Access Gateway-Umgebung einzurichten. Konfigurieren Sie auf der Verwaltungsoberfläche Desktop- und Anwendungsressourcen sowie die in der DMZ zu verwendenden Authentifizierungsmethoden. Rufen Sie `https://<mycoUnifiedGatewayAppliance>.com:9443/admin/index.html` zur Anmeldung auf den Seiten der Verwaltungsoberfläche auf.

Bereitstellen von Unified Access Gateway mit dem OVF-Vorlagenassistenten

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

Zwei Versionen der Unified Access Gateway-OVA-Datei sind verfügbar: eine standardmäßige OVA und eine FIPS-Version der OVA. Die FIPS 140-2-Version wird mit einem Satz durch FIPS zertifizierter Verschlüsselungen und Hashes ausgeführt, wobei einschränkende Dienste aktiviert sind, die durch FIPS zertifizierte Bibliotheken unterstützen. Wenn Unified Access Gateway im FIPS-Modus bereitgestellt wird, kann die Appliance nicht in den standardmäßigen OVA-Bereitstellungsmodus wechseln.

Hinweis 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

- Überprüfen Sie die Bereitstellungsoptionen, die im Assistenten verfügbar sind. Siehe „System- und Netzwerkanforderungen von Unified Access Gateway“, auf Seite 8.
- Legen Sie fest, wie viele Netzwerkschnittstellen und statische IP-Adressen für die Unified Access Gateway-Appliance konfiguriert werden sollen. Siehe „Anforderungen an die Netzwerkkonfiguration“, auf Seite 9.
- Laden Sie die `.ova`-Installationsdatei für die Unified Access Gateway-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“ zur `OVA`-Datei, die Sie heruntergeladen haben, oder geben Sie eine URL ein und klicken Sie auf **Weiter**.

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
Name und Speicherort	Geben Sie den Namen der virtuellen Unified Access Gateway-Appliance ein. Der Name muss innerhalb des Bestandsordners eindeutig sein. Bei Namen wird die Groß-/Kleinschreibung beachtet. Wählen Sie einen Speicherort für die virtuelle Appliance aus.
Bereitstellungskonfiguration	Für ein IPv4-Netzwerk können Sie eine, zwei oder drei Netzwerkschnittstellen (NICs) verwenden. Für ein IPv6-Netzwerk verwenden Sie drei Netzwerkschnittstellen (NICs). Unified Access Gateway erfordert eine eigene statische IP-Adresse für jede NIC. Viele DMZ-Implementierungen verwenden getrennte Netzwerke zur Sicherung der verschiedenen Datenverkehrstypen. Konfigurieren Sie Unified Access Gateway entsprechend dem Netzwerkdesign der DMZ, in der die Bereitstellung erfolgt.
Host/Cluster	Wählen Sie den Host oder Cluster aus, auf dem die virtuelle Appliance ausgeführt werden soll.
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.

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. Ordnen Sie die Netzwerke in der OVF-Vorlage den Netzwerken in Ihrer Bestandsliste zu. 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 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.
Anpassen von Netzwerkeigenschaften	Die Textfelder auf der Eigenschaftenseite sind speziell für Unified Access Gateway 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. ■ **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** ■ **NIC 1 (eth0) 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 Unified Access Gateway-Appliance ein. Trennen Sie diese jeweils durch Leerzeichen. Beispiel für einen IPv4-Eintrag: 192.0.2.1 192.0.2.2. Beispiel für einen IPv6-Eintrag: fc00:10:112:54::1 ■ **NIC 2 (eth1) IPv4-Adresse**. Geben Sie die IPv4-Adresse für die NIC ein, wenn Sie für den NIC-Modus STATICV4 festgelegt haben.

Option	Beschreibung
	■ **Kommagetrennte Liste mit benutzerdefinierten IPv4-Routen für NIC 2 (eth1) im Formular ipv4-network-address/bits.ipv4-gateway-address** ■ **NIC 2 (eth1) IPv6-Adresse**. Geben Sie die IPv6-Adresse für die NIC ein, wenn Sie für den NIC-Modus STATICV6 festgelegt haben. ■ **NIC 3 (eth2) 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 3 (eth2) im Formular ipv4-network-address/bits.ipv4-gateway-address** ■ **NIC 3 (eth2) IPv6-Adresse**. Geben Sie die IPv6-Adresse für die NIC ein, wenn Sie für den NIC-Modus STATICV6 festgelegt haben. ■ **Kennwortoptionen**. Geben Sie das Kennwort für den Root-Benutzer dieser VM und das Kennwort für den Admin-Benutzer ein, der auf die Verwaltungskonsole zugreift und den REST-API-Zugriff aktiviert. ■ **Kennwortoptionen**. Geben Sie das Kennwort für den Admin-Benutzer ein, der sich zum Konfigurieren von Unified Access Gateway bei der Verwaltungsoberfläche anmeldet und den REST-API-Zugriff aktivieren kann. Die anderen Einstellungen sind entweder optional oder bereits mit einer Standardeinstellung vorausgefüllt.

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_UAG_appliance`

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

Wenn die Bereitstellung erfolgreich war, erscheint die bereitgestellte Webseite des Servers, auf den Unified Access Gateway 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 Unified Access Gateway-Appliance ist bereitgestellt und startet automatisch.

Weiter

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

Hinweis Wenn Sie nicht auf die Verwaltungsoberfläche zugreifen können, überprüfen Sie, ob die virtuelle Maschine die IP-Adresse aufweist, die während der Installation der OVA angezeigt wurde. Wenn die IP-Adresse nicht konfiguriert wurde, verwenden Sie den auf der Benutzeroberfläche angegebenen vami-Befehl, um die NICs neu zu konfigurieren. Führen Sie den Befehl `" cd /opt/vmware/share/vami"` und dann den Befehl `"./vami_config_net"` aus.

Konfigurieren von Unified Access Gateway auf den Verwaltungsseiten für die Konfiguration

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

Die Seiten „Allgemeine Einstellungen“ und „Erweiterte Einstellungen“ enthalten Nachfolgendes.

- Unified Access Gateway-Systemkonfiguration und SSL-Server-Zertifikat
- 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
- Identity Bridging-Einstellungskonfiguration

Auf den Seiten für Support-Einstellungen haben Sie folgende Möglichkeiten.

- Herunterladen der Unified Access Gateway-Protokolldateien als ZIP-Dateien
- Exportieren der Unified Access Gateway-Einstellungen zum Abrufen der Konfigurationseinstellungen
- Festlegen der Einstellungen für die Protokollebene
- Importieren der Unified Access Gateway-Einstellungen zum Erstellen und Aktualisieren der gesamten Unified Access Gateway-Konfiguration

Konfigurieren der Unified Access Gateway -Systemeinstellungen

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

Die URL der Unified Access Gateway-Verwaltungsoberfläche hat das Format `https://<mycoUnifiedAccess–Gatewayappliance.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 Unified Access Gateway-Bereitstellungseigenschaften. Die folgenden Informationen sind erforderlich
  - Statische IP-Adresse für die Unified Access Gateway-Appliance

- IP-Adresse des DNS-Servers
- Kennwort für die Verwaltungskonsole
- URL der Serverinstanz des Lastausgleichsdienstes, auf den die Unified Access Gateway-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 Unified Access Gateway-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 ! @ # $ % * ( ).
Verschlüsselungssammlungen	In den meisten Fällen ist es nicht erforderlich, die Standardeinstellungen zu ändern. Dies sind die kryptografischen Algorithmen, mit denen die Kommunikation zwischen Clients und der Unified Access Gateway-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.
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 Unified Access Gateway-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 Unified Access Gateway überprüft. Beispiel: `https://mycoUnifiedAccessGateway.com:443/favicon.ico`
Cookies für Zwischenspeicherung	Der Satz Cookies, den Unified Access Gateway 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.

Option	Standardwert und Beschreibung
Stilllegungsmodus	Wenn Sie ein Upgrade durchführen, legen Sie für diesen Modus nur **JA** fest, wenn Unified Access Gateway mit einem Lastausgleichsdienst verwendet wird. Nachdem das Upgrade abgeschlossen ist, legen Sie für diesen Modus NEIN fest.
Überwachungsintervall	Der Standardwert ist **60**.
Zeitüberschreitung für Anforderung	Die Standardeinstellung ist **3000**.
Body-Receive-Zeitüberschreitung	Die Standardeinstellung ist **5000**.

4 Klicken Sie auf **Speichern**.

Weiter

Konfigurieren Sie die Edge-Diensteinstellungen für die Komponenten, mit denen Unified Access Gateway bereitgestellt wird. 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 Unified Access Gateway-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.

Bereitstellen von Unified Access Gateway mit PowerShell

3

Unified Access Gateway 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 Unified Access Gateway 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 Unified Access Gateway mit PowerShell

Um Unified Access Gateway 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 Unified Access Gateway eingesetzt. Achten Sie also darauf, dass die Werte korrekt sind.

Verwenden von PowerShell zur Bereitstellung der Unified Access Gateway -Appliance

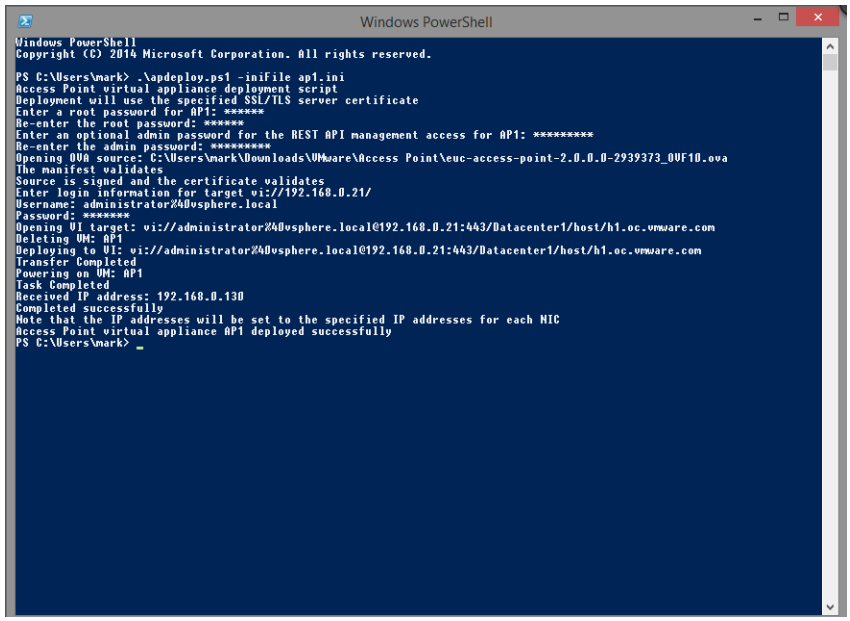
Anhand von PowerShell-Skripten können Sie die Umgebung mit allen Konfigurationseinstellungen einrichten. Wenn Sie das PowerShell-Skript zum Bereitstellen von Unified Access Gateway ausführen, kann die Lösung schon beim ersten Systemstart in der Produktion eingesetzt werden.

Voraussetzungen

- Stellen Sie sicher, dass die Systemanforderungen erfüllt sind.

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

  Abbildung 3-1. PowerShell-Beispielskript



Vorgehensweise

1 Laden Sie die Unified Access Gateway-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 Unified Access Gateway-Appliance.

  Beispiel: Stellen Sie eine neue Unified Access Gateway-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 Unified Access Gateway-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 Unified Access Gateway-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.

Anwendungsbeispiele für die Unified Access Gateway-Bereitstellung 4

Mithilfe der in diesem Kapitel beschriebenen Bereitstellungsszenarien können Sie die Unified Access Gateway-Bereitstellung für Ihre Umgebung identifizieren und organisieren.

Sie können Unified Access Gateway mit Horizon View, Horizon Cloud mit standortbasierter Infrastruktur, VMware Identity Manager und VMware AirWatch bereitstellen.

Dieses Kapitel behandelt die folgenden Themen:

Bereitstellung mit Horizon View und Horizon Cloud mit standortbasierter Infrastruktur

Sie können Unified Access Gateway mit Horizon View und Horizon Cloud mit standortbasierter Infrastruktur bereitstellen. Für die View-Komponente von VMware Horizon spielen Unified Access Gateway-Appliances die gleiche Rolle wie früher View-Sicherheitsserver.

Bereitstellungsszenario

Unified Access Gateway liefert sicheren Remote-Zugriff auf standortbasierte virtuelle Desktops und Anwendungen in einem Kunden-Datencenter. Dies wird mit einer standortbasierten Bereitstellung von Horizon View oder Horizon Cloud für einheitliches Management betrieben.

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

Virtuelle Unified Access Gateway-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 Unified Access Gateway-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.

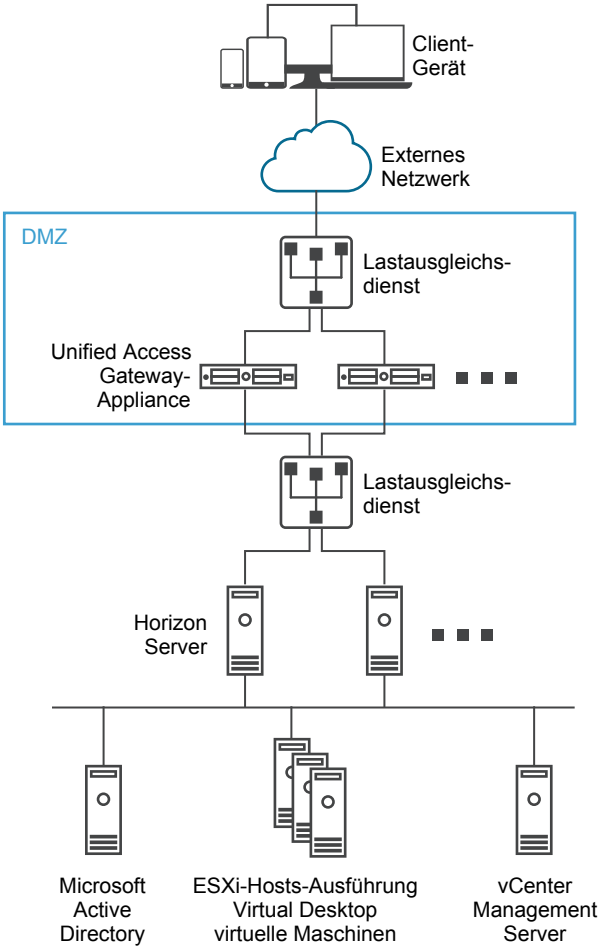
Sie müssen die Anforderungen einer nahtlosen Unified Access Gateway-Bereitstellung mit Horizon erfüllen.

- Die Unified Access Gateway-Appliance verweist auf einen Load Balancer, der Horizon-Servern vorgelagert ist, und die Auswahl der Serverinstanz erfolgt dynamisch.
- Unified Access Gateway ersetzt den Horizon-Sicherheitsserver.
- Standardmäßig muss Port 8443 für Blast TCP/UDP verfügbar sein. Es ist jedoch auch möglich, Port 443 für Blast TCP/UDP zu konfigurieren.
- Das Blast Secure Gateway und PCoIP Secure Gateway müssen aktiviert sein, wenn Unified Access Gateway mit Horizon bereitgestellt wird. So wird sichergestellt, dass die Anzeigeprotokolle automatisch über Unified Access Gateway als Proxys dienen können. Die Einstellungen BlastExternalURL und pcoipExternalURL geben Verbindungsadressen an, mit denen die Horizon-Clients diese Anzeigeprotokollverbindungen über die jeweiligen Gateways bei Unified Access Gateway 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 Unified Access Gateway ignoriert.
- Deaktivieren Sie die sicheren Gateways auf den Instanzen des View-Verbindungsservers und aktivieren Sie diese Gateways auf den Unified Access Gateway-Appliances.

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

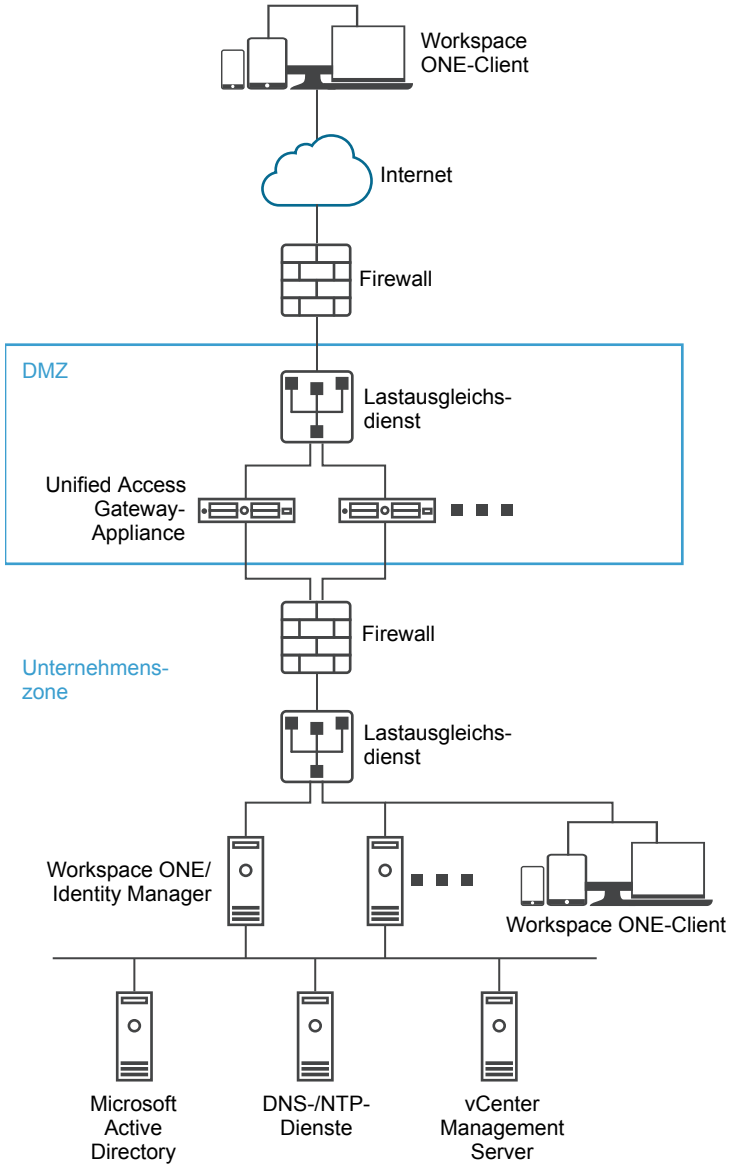
- Sichere Bereitstellung. Unified Access Gateway ist als geschützte, gesperrte, vorkonfigurierte Linux-basierte virtuelle Maschine implementiert.
- Skalierbar. Sie können Unified Access Gateway mit einem individuellen View-Verbindungsserver verbinden oder eine Verbindung über einen Lastausgleichsdienst, der mehreren View-Verbindungsservern vorgelagert ist, herstellen und so für Hochverfügbarkeit sorgen. 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. Verweisen der Unified Access Gateway -Appliance auf einen Lastausgleichsdienst



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

Abbildung 4-2. Verweisen der Unified Access Gateway -Appliance auf eine Horizon Server-Instanz



Authentifizierung

Die Benutzerauthentifizierung erfolgt ähnlich wie beim View-Sicherheitsserver. Die folgenden Benutzer-Authentifizierungsmethoden werden in Unified Access Gateway 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 verschiedene Zwei-Faktor-Sicherheitslösungen von Drittanbietern
- Smartcard, CAC oder PIV X.509-Benutzerzertifikate
- SAML

Diese Authentifizierungsmethoden werden beim View-Verbindungsserver unterstützt.
Unified Access Gateway 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 Unified Access Gateway Anforderungen für Berechtigungsinformationen sowie Anforderungen zum Desktop- und Anwendungsstart an View-Verbindungsserver weiterleiten. Unified Access Gateway verwaltet darüber hinaus die zugehörigen Desktop- und Anwendungsprotokoll-Handler, damit diese nur autorisierten Protokolldatenverkehr weiterleiten.

Unified Access Gateway führt die Smartcard-Authentifizierung eigenständig durch. Dazu gehören Optionen für die Kommunikation zwischen Unified Access Gateway und Online Certificate Status Protocol(OCSP)-Servern zur Suche nach entzogenen X.509-Zertifikaten usw.

Konfigurieren der Horizon-Einstellungen

Sie können Unified Access Gateway über Horizon View und Horizon Cloud with On-Premises Infrastructure bereitstellen. Für die View-Komponente von VMware Horizon spielt die Unified Access Gateway-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. Unified Access Gateway kann mit Servern kommunizieren, die das View XML-Protokoll verwenden – etwa dem View-Verbindungsserver, Horizon Cloud und Horizon Cloud with On-Premises Infrastructure.
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: sha1 = 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 Unified Access Gateway 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 Unified Access Gateway-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 zu **JA**, um festzulegen, dass PCoIP Secure Gateway aktiviert ist.
Externe Proxy-URL	Geben Sie die externe URL der Unified Access Gateway-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 Unified Access Gateway-IP-Adresse und Port 4172 angegeben.
Aufforderung für Smart Card-Hinweis	Ändern Sie NEIN zu **JA**, um die Unterstützung der Funktion für den Benutzernamenshinweis für Smartcards durch die Unified Access Gateway-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 Unified Access Gateway-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
UDP-Tunnel-Server aktiviert	Aktivieren Sie diese Option bei schlechten Netzwerkbedingungen für Horizon Clients.
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 Unified Access Gateway-Appliance ein. Wenn nicht anders angegeben, wird der Standardwert verwendet.
Proxy-Muster	Geben Sie den regulären Ausdruck ein, mit dem die URIs, die mit der Horizon Server-URL verbunden sind (proxyDestinationUrl), abgeglichen werden. Für den View-Verbindungsserver ist ein Schrägstrich (/) der typische Wert für die Angabe der Umleitung an den HTML Access-Webclient bei Nutzung der Unified Access Gateway-Appliance.

Option	Beschreibung
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.
Gateway-Standort	Ändern Sie NEIN in **JA**, um den Standort zu aktivieren, von dem die Anforderungen stammen. Der Sicherheitsserver und Unified Access Gateway 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.
Hosteinträge	Geben Sie eine durch Komma getrennte Liste von Hostnamen ein, die der /etc/hosts-Datei hinzugefügt werden. Jeder Eintrag enthält eine IP, einen Hostnamen und einen optionalen Hostnamensalias (in dieser Reihenfolge), die durch ein Leerzeichen getrennt sind. Beispiel: **`10.192.168.1 example1.com, 10.192.168.2 example2.com example_alias`**.

7 Klicken Sie auf **Speichern**.

Externe URL-Konfigurationsoptionen für Blast TCP und UDP

Blast Secure Gateway beinhaltet das BEAT-Netzwerkprotokoll (Blast Extreme Adaptive Transport), das sich dynamisch an die jeweiligen Netzwerkbedingungen wie unterschiedliche Geschwindigkeiten und Paketverluste anpasst. In Unified Access Gateway können Sie die vom BEAT-Protokoll verwendeten Ports konfigurieren.

Blast verwendet die Standard-Ports TCP 8443 und UDP 8443. UDP 443 kann auch für den Zugriff auf einen Desktop über den UDP-Tunnel-Server verwendet werden. Die Port-Konfiguration wird über die Eigenschaft „Externe Blast-URL“ eingestellt.

Tabelle 4-1. Optionen für den BEAT-Port

Externe Blast-URL	Vom Client verwendeter TCP-Port	Vom Client verwendeter UDP-Port	Beschreibung
https://ap1.myco.com	8443	8443	Dies ist das Standardformular, für das TCP 8443 und optional UDP 8443 in der Firewall geöffnet werden müssen, um Verbindungen mit Unified Access Gateway über das Internet zuzulassen.
https://ap1.myco.com:443	443	8443	Verwenden Sie dieses Formular, wenn TCP 443 oder UDP 8443 geöffnet werden muss.
https://ap1.myco.com:xxxx	xxxx	8443	
https://ap1.myco.com:xxxx/?UDP-Port=yyyy	xxxx	yyyy	

Um andere Ports als die Standardports zu konfigurieren, muss bei der Bereitstellung eine interne IP-Weiterleitungsregel für das entsprechende Protokoll hinzugefügt werden. Die Weiterleitungsregeln können in der OVF-Vorlage der Bereitstellung oder über die in den PowerShell-Befehlen eingegebenen INI-Dateien festgelegt werden.

Bereitstellung als Reverse-Proxy

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

Bereitstellungsszenario

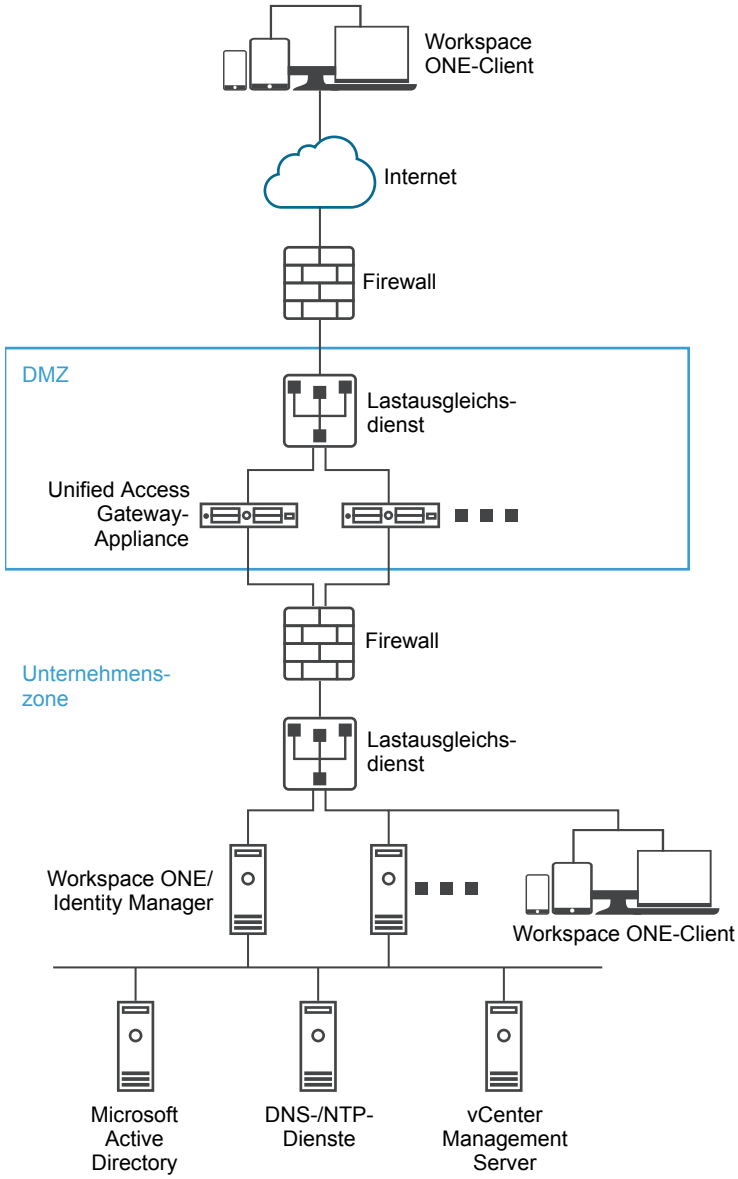
Unified Access Gateway bietet sicheren Remote-Zugriff auf eine standortbasierte Bereitstellung von VMware Identity Manager. Unified Access Gateway-Appliances werden üblicherweise in einer demilitarisierten Netzwerkzone (DMZ) bereitgestellt. Mit VMware Identity Manager arbeitet die Unified Access Gateway-Appliance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

Anforderungen zur Unified Access Gateway-Bereitstellung mit VMware Identity Manager

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

- Unified Access Gateway muss das interne DNS verwenden. Die proxyDestinationURL muss also FQDN verwenden.

Abbildung 4-3. Auf VMware Identity Manager verweisende Unified Access Gateway -Appliance



Wissenswertes zum Reverse-Proxy

Unified Access Gateway bietet als Lösung Zugriff auf das App-Portal, in dem Remote-Benutzer über eine einmalige Anmeldung auf ihre Ressourcen zugreifen können. Sie aktivieren den Authn-Reverse-Proxy auf einem Edge Service Manager. Aktuell werden die Authentifizierungsmethoden RSA SecurID und RADIUS unterstützt.

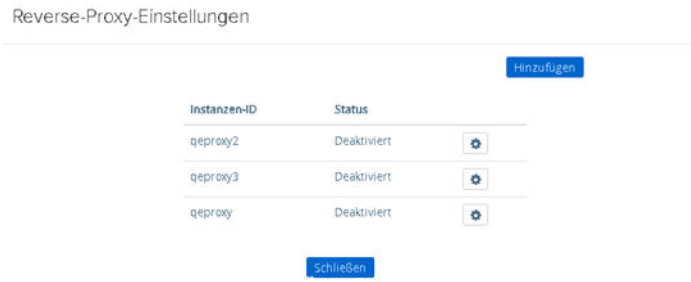
Hinweis Sie müssen Identitätsanbieter-Metadaten generieren, bevor Sie die Authentifizierung auf dem Web-Reverse-Proxy aktivieren.

Unified Access Gateway bietet 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.

Sie können mehrere Reverse-Proxy-Instanzen konfigurieren.

Abbildung 4-4. Mehrere konfigurierte Reverse-Proxys



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

Konfigurieren des Reverse-Proxy

Sie können den Web-Reverse-Proxy-Dienst zur Verwendung von Unified Access Gateway mit VMware Identity Manager konfigurieren.

Voraussetzungen

Anforderungen für die Bereitstellung mit VMware Identity Manager.

- Aufgeteiltes DNS. Bei einem aufgeteilten DNS kann der Name auf verschiedene IP-Adressen aufgelöst werden – abhängig davon, ob es sich um eine interne oder externe IP handelt.
- Der VMware Identity Manager-Dienst muss einen vollqualifizierten Domänennamen (FQDN) als Hostnamen aufweisen.
- Unified Access Gateway muss das interne DNS verwenden. Die Proxy-Ziel-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. Klicken Sie auf der Seite „Reverse-Proxy-Einstellungen“ auf **Hinzufügen**.
5. Ändern Sie im Abschnitt „Reverse-Proxy-Einstellungen aktivieren“ NEIN zu **JA**, um den Reverse-Proxy zu aktivieren.

6 Konfigurieren Sie die folgenden Edgediensteinstellungen.

Option	Beschreibung
Bezeichner	Für den Bezeichner des Edgedienstes wird der Web-Reverse-Proxy festgelegt.
Instanzen-ID	Der eindeutige Name, um eine Instanz des Web-Reverse-Proxy zu identifizieren und von allen anderen Instanzen des Web-Reverse-Proxy zu unterscheiden.
Proxy-Ziel-URL	Geben Sie die Adresse der Webanwendung ein.
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(.*))`. **Hinweis** Wenn Sie mehrere Reverse-Proxys konfigurieren, geben Sie den Hostnamen im Proxy-Host-Muster an.

7 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 Unified Access Gateway 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 Unified Access Gateway-Appliance herzustellen und eine Integritätsprüfung durchzuführen.
SAML SP	Dieses Feld ist erforderlich, wenn UAG als authentifizierter Reverse-Proxy für VMware Identity Manager konfiguriert wird. Geben Sie den Namen des SAML-Dienstanbieters für den View XML API-Broker ein. Dieser Name muss entweder mit dem Namen eines mit Unified Access Gateway konfigurierten Dienstanbieters übereinstimmen oder der spezielle Wert **`DEMO`** sein. Wenn mehrere Dienstanbieter mit Unified Access Gateway konfiguriert wurden, müssen ihre Namen eindeutig sein.
Aktivierungscode	Geben Sie den vom VMware Identity Manager-Dienst generierten und in Unified Access Gateway importierten Code ein, um eine Vertrauensbeziehung zwischen VMware Identity Manager und Unified Access Gateway aufzubauen. Beachten Sie, dass für lokale Bereitstellungen der Aktivierungscode nicht erforderlich ist. Ausführliche Informationen zur Generierung eines Aktivierungscodes finden Sie unter *VMware Identity Manager-Cloud-Bereitstellung*.
Externe URL	Standardmäßig ist die Unified Access Gateway-Host-URL, Port 443, angegeben. Sie können eine weitere externe URL eingeben. Geben Sie diese in folgender Form ein: `https://<host:port>.`

Option	Beschreibung
UnSecure-Muster	Geben Sie das bekannte Muster der VMware Identity Manager-Umleitung ein. Beispiel: `(/catalog-portal(.)|/|/SAAS/|/SAAS|/SAAS/API/1.0/GET/image(.)|/SAAS/horizon/css(.)|/SAAS/horizon/angular(.)|/SAAS/horizon/js(.)|/SAAS/horizon/js-lib(.)|/SAAS/auth/login(.)|/SAAS/jersey/manager/api/branding|/SAAS/horizon/images/(.)|/SAAS/jersey/manager/api/images/(.)|/hc/(.)/authenticate/(.)|/hc/static/(.)|/SAAS/auth/saml/response|/SAAS/auth/authenticatedUserDispatcher|/web(.)|/SAAS/apps/|/SAAS/horizon/portal/(.)|/SAAS/horizon/fonts(.)|/SAAS/API/1.0/POST/sso(.)|/SAAS/API/1.0/REST/system/info(.)|/SAAS/API/1.0/REST/auth/cert(.)|/SAAS/API/1.0/REST/oauth2/activate(.)|/SAAS/API/1.0/GET/user/devices/register(.)|/SAAS/API/1.0/oauth2/token(.)|/SAAS/API/1.0/REST/oauth2/session(.)|/SAAS/API/1.0/REST/user/resources(.)|/hc/t/(.)/(.)/authenticate(.)|/SAAS/API/1.0/REST/auth/logout(.)|/SAAS/auth/saml/response(.)|/SAAS/(.)/(.)auth/login(.)|/SAAS/API/1.0/GET/apps/launch(.)|/SAAS/API/1.0/REST/user/applications(.)|/SAAS/auth/federation/sso(.)|/SAAS/auth/oauth2/authorize(.)|/hc/prepareSaml/failure(.)|/SAAS/auth/oauthtoken(.)|/SAAS/API/1.0/GET/metadata/idp.xml|/SAAS/auth/saml/artifact/resolve(.)|/hc/(.)/authAdapter(.)|/hc/authenticate/(.)|/SAAS/auth/logout|/SAAS/common.js|/SAAS/auth/launchInput(.)|/SAAS/launchUsersApplication.do(.)|/hc/API/1.0/REST/thinapp/download(.)|/hc/t/(.)/(.)/logout(.*))`
Authentifizierungs-Cookie	Geben Sie den Namen des Authentifizierungs-Cookies ein. Beispiel: **`HZN`**
URL für Anmeldungsumleitung	Wenn der Benutzer sich beim Portal abmeldet, geben Sie die Umleitungs-URL für die erneute Anmeldung ein. Beispiel: **`/SAAS/auth/login?dest=%s`**
Proxy-Host-Muster	Externer Hostname, mit dem geprüft wird, ob der eingehende Host dem Muster für diese bestimmte Instanz entspricht. Beim Konfigurieren der Instanzen des Web-Reverse-Proxys ist das Host-Muster optional.
Hosteinträge	Geben Sie eine durch Komma getrennte Liste von Hostnamen ein, die der /etc/hosts-Datei hinzugefügt werden. Jeder Eintrag enthält eine IP, einen Hostnamen und einen optionalen Hostnamensalias (in dieser Reihenfolge), die durch ein Leerzeichen getrennt sind. Beispiel: **`10.192.168.1 example1.com, 10.192.168.2 example2.com example-alias`**.

Hinweis Die Optionen „UnSecure-Muster“, „Authentifizierungs-Cookie“ und „URL für Anmeldungsumleitung“ können nur mit VMware Identity Manager anwendet werden. Die hier bereitgestellten Werte gelten auch für Access Point 2.8 und Access Point 2.9.

Hinweis Das Authentifizierungs-Cookie und die Eigenschaften für UnSecure-Muster gelten nicht für den Authentifizierungs-Reverse-Proxy. Sie müssen die Authentifizierungsmethode mit der Eigenschaft für Authentifizierungsmethoden definieren.

8 Klicken Sie auf **Speichern**.

Weiter

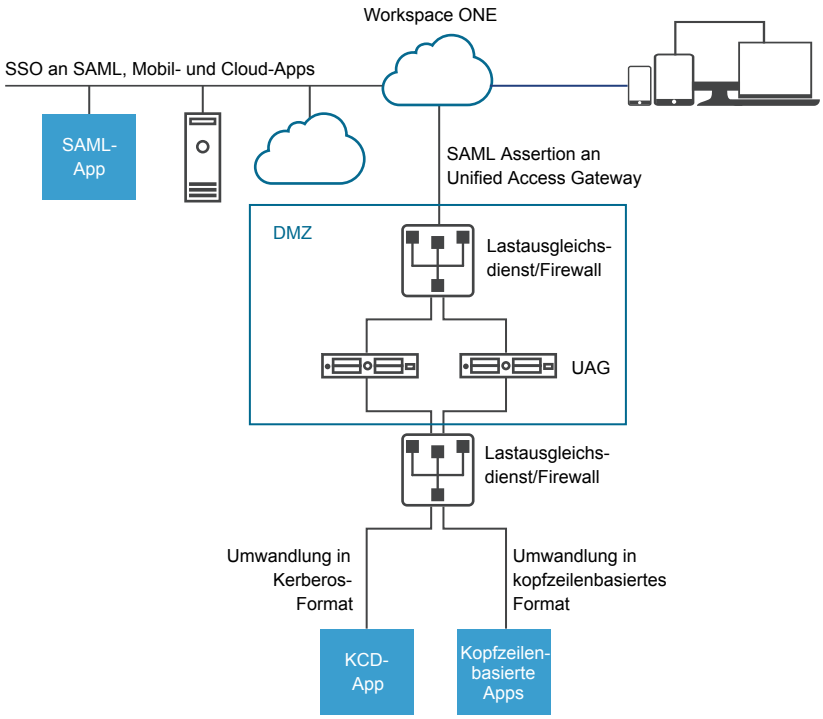
Informationen zum Aktivieren von Identity Bridging finden Sie unter „Konfigurieren der Identity Bridging-Einstellungen“, auf Seite 46.

Bereitstellung für Single Sign-on-Zugriff auf standortbasierte ältere Webanwendungen

Die Identity Bridging-Funktion von Unified Access Gateway kann so konfiguriert werden, dass Single Sign-on (SSO) bei älteren Webanwendungen ermöglicht wird, die Kerberos Constrained Delegation (KCD) oder die kopfzeilenbasierte Authentifizierung nutzen.

Im Identity Bridging-Modus verhält sich Unified Access Gateway als Dienstanbieter, der die Benutzerauthentifizierung an die konfigurierten älteren Anwendungen übergibt. VMware Identity Manager agiert als Identitätsanbieter und ermöglicht SSO für SAML-Anwendungen. Beim Zugriff auf ältere Anwendungen, die KCD oder die kopfzeilenbasierte Authentifizierung nutzen, authentifiziert Identity Manager den Benutzer. Eine SAML-Assertion mit den Informationen des Benutzers wird an Unified Access Gateway gesendet. Unified Access Gateway nutzt diese Authentifizierung, um Benutzern den Zugriff auf die Anwendung zu erlauben.

Abbildung 4-5. Identity Bridging-Modus von Unified Access Gateway



Identity Bridging-Bereitstellungsszenarien

Der Identity Bridging-Modus von Unified Access Gateway kann zur Verwendung von VMware Workspace® ONE® in der Cloud oder in einer standortbasierten Umgebung konfiguriert werden.

Verwenden von Unified Access Gateway Identity Bridging mit Workspace ONE Clients in der Cloud

Der Identity Bridging-Modus kann für Workspace ONE in der Cloud eingerichtet werden, um Benutzer zu authentifizieren. Wenn ein Benutzer Zugriff auf eine ältere Webanwendung anfordert, wendet der Identitätsanbieter die betreffenden Authentifizierungs- und Autorisierungsrichtlinien an.

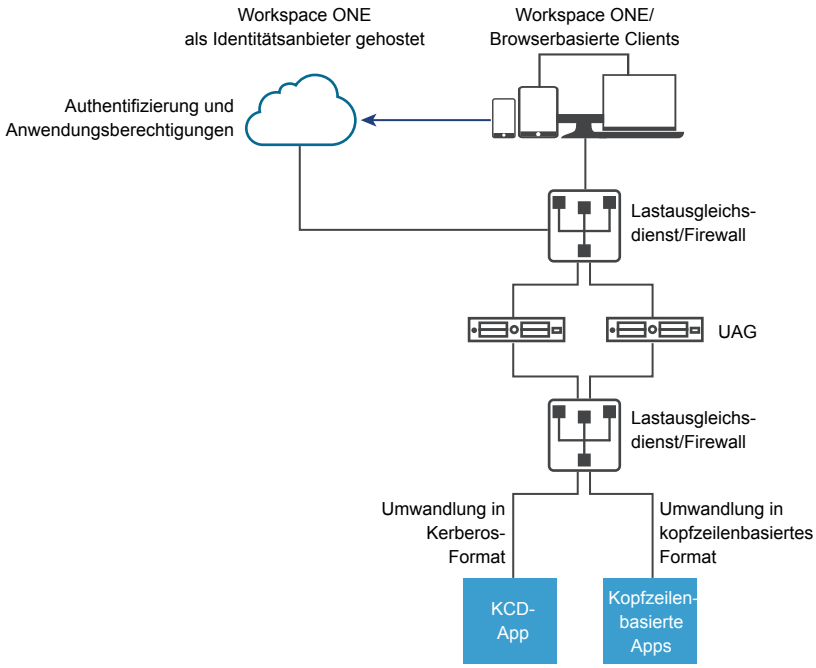
Wird der Benutzer validiert, so erstellt der Identitätsanbieter ein SAML-Token und sendet es dem Benutzer zu. Der Benutzer übergibt das SAML-Token an Unified Access Gateway in der DMZ.
Unified Access Gateway validiert das SAML-Token und ruft den Benutzerprinzipalnamen aus dem Token ab.

Bei einer Anforderung mit Kerberos-Authentifizierung übernimmt Kerberos Constrained Delegation die Aushandlung mit dem Active Directory-Server. Unified Access Gateway nimmt die Identität des Benutzers an, um das Kerberos-Token für die Authentifizierung bei der Anwendung abzurufen.

Bei einer Anforderung mit kopfzeilenbasierter Authentifizierung wird der Name der Benutzer-Kopfzeile an den Webserver gesendet, um die Authentifizierung bei der Anwendung einzuleiten.

Die Anwendung sendet die Antwort zurück an Unified Access Gateway. Die Antwort wird an den Benutzer gesendet.

Abbildung 4-6. Unified Access Gateway Identity Bridging mit Workspace ONE in der Cloud



Verwenden von Identity Bridging mit standortbasierten Workspace ONE-Clients

Wenn der Identity Bridging-Modus zur Authentifizierung von Benutzern mit Workspace ONE in einer standortbasierten Umgebung eingerichtet ist, geben Benutzer die URL ein, um über den Unified Access Gateway-Proxy auf die standortbasierte, ältere Webanwendung zuzugreifen.
Unified Access Gateway leitet die Anforderung an den Identitätsanbieter zur Authentifizierung um. Der Identitätsanbieter wendet Authentifizierungs- und Autorisierungsrichtlinien auf die Anforderung an. Wird der Benutzer validiert, so erstellt der Identitätsanbieter ein SAML-Token und sendet das Token dem Benutzer zu.

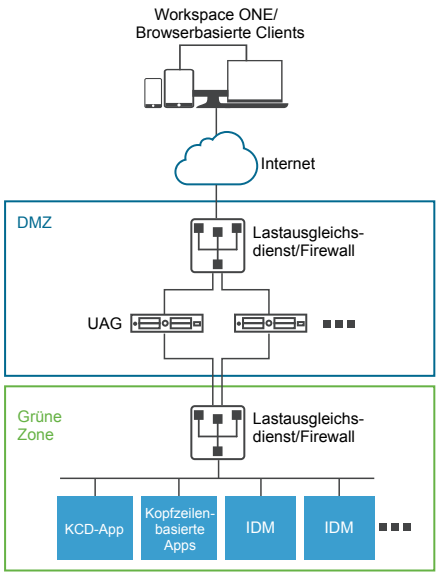
Der Benutzer übergibt das SAML-Token an Unified Access Gateway. Unified Access Gateway validiert das SAML-Token und ruft den Benutzerprinzipalnamen aus dem Token ab.

Bei einer Anforderung mit Kerberos-Authentifizierung übernimmt Kerberos Constrained Delegation die Aushandlung mit dem Active Directory-Server. Unified Access Gateway nimmt die Identität des Benutzers an, um das Kerberos-Token für die Authentifizierung bei der Anwendung abzurufen.

Bei einer Anforderung mit kopfzeilenbasierter Authentifizierung wird der Name der Benutzer-Kopfzeile an den Webserver gesendet, um die Authentifizierung bei der Anwendung einzuleiten.

Die Anwendung sendet die Antwort zurück an Unified Access Gateway. Die Antwort wird an den Benutzer gesendet.

Abbildung 4-7. Standortbasiertes Unified Access Gateway Identity Bridging



Konfigurieren der Identity Bridging-Einstellungen

Wenn Kerberos in der Back-End-Anwendung konfiguriert ist, müssen Sie zum Einrichten von Identity Bridging in Unified Access Gateway die Identitätsanbieter-Metadaten- und die Keytab-Datei hochladen und die KCD-Bereichseinstellungen konfigurieren.

Wenn Identity Bridging in Verbindung mit einer kopfzeilenbasierten Authentifizierung aktiviert ist, werden keine Keytab-Einstellungen und KCD-Bereichseinstellungen benötigt.

Stellen Sie vor dem Konfigurieren der Identity Bridging-Einstellungen für die Kerberos-Authentifizierung sicher, dass folgende Voraussetzungen erfüllt sind.

- Ein Identitätsanbieter wurde konfiguriert und die SAML-Metadaten des Identitätsanbieters wurden gespeichert. Die SAML-Metadatendatei wurde in Unified Access Gateway hochgeladen.
- Für die Kerberos-Authentifizierung muss ein Server vorhanden sein, auf dem Kerberos aktiviert ist und die Bereichsnamen für die zu verwendenden Key Distribution Centers angegeben sind.
- Laden Sie für die Kerberos-Authentifizierung die Kerberos-Keytab-Datei in Unified Access Gateway hoch. Die Keytab-Datei enthält die Anmeldedaten für das Active Directory-Dienstkonto, das eingerichtet wurde, um das Kerberos-Ticket eines beliebigen Benutzers in der Domäne für einen gegebenen Back-End-Dienst zu erhalten.

Metadaten des Identitätsanbieters hochladen

Um die Identity Bridging-Funktion zu konfigurieren, müssen Sie die Metadaten-XML-Datei für das SAML-Zertifikat des Identitätsanbieters in Unified Access Gateway hochladen.

Voraussetzungen

XML-Datei mit SAML-Metadaten, die auf einem Computer gespeichert ist, auf den Sie Zugriff haben.

Wenn Sie VMware Identity Manager als Identitätsanbieter verwenden, laden Sie die SAML-Metadatendatei herunter und speichern Sie sie, indem Sie in der Verwaltungskonsole von VMware Identity Manager die Optionen „Katalog“ > „Einstellungen SAML-Metadaten“ > Link „Metadaten des Identitätsanbieters (IdP)“ auswählen.

Vorgehensweise

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

2 Wählen Sie im Abschnitt **Erweiterte Einstellungen > Einstellungen für Identity Bridging** das Zahnradsymbol **Metadaten des Identitätsanbieters hochladen**.

3 Geben Sie die Element-ID für den Identitätsanbieter im Textfeld **Element-ID** ein.

   Wenn Sie im Textfeld „Element-ID“ keinen Wert eingeben, wird der Name des Identitätsanbieters in der Metadatendatei gesucht und als Element-ID für den Identitätsanbieter verwendet.

4 Klicken Sie im Abschnitt **IDP-Metadaten** auf **Auswählen** und suchen Sie die Metadatendatei, die Sie gespeichert haben. Klicken Sie auf **Öffnen**.

5 Klicken Sie auf **Speichern**.

Weiter

Konfigurieren Sie zur KDC-Authentifizierung die Einstellungen für den Bereich und die Keytab-Datei.

Füllen Sie zur kopfzeilenbasierten Authentifizierung beim Konfigurieren der Identity Bridging-Funktion die Option „Name der Benutzer-Kopfzeile“ mit dem Namen der HTTP-Kopfzeile aus, die die Benutzer-ID enthält.

Konfigurieren der Bereichseinstellungen

Konfigurieren Sie den Domänenbereichsnamen, die Key Distribution Centers für den Bereich und die KDC-Zeitüberschreitung.

Der Bereich ist der Name einer administrativen Einheit, die Authentifizierungsdaten verwaltet. Für den Bereich der Kerberos-Authentifizierung sollte unbedingt ein beschreibender Name gewählt werden. Konfigurieren Sie den Bereich, der auch Domänenname genannt wird, sowie den entsprechenden KDC-Dienst in Unified Access Gateway. Wenn eine UPN-Anforderung einen bestimmten Bereich erreicht, löst Unified Access Gateway das KDC intern auf, um das Kerberos-Ticket zu verwenden.

Der Bereichsname sollte grundsätzlich derselbe sein wie der Name Ihrer Domäne (in Großbuchstaben eingegeben). Ein Bereichsname lautet beispielsweise EXAMPLE.NET. Der Bereichsname wird von einem Kerberos-Client zum Generieren der DNS-Namen verwendet.

Voraussetzungen

Ein Server, auf dem Kerberos aktiviert ist und die Bereichsnamen für die zu verwendenden Key Distribution Centers angegeben sind.

Vorgehensweise

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

2 Wählen Sie im Abschnitt **Erweiterte Einstellungen > Einstellungen für Identity Bridging** das Zahnradsymbol **Bereichseinstellungen**.

3 Klicken Sie auf **Hinzufügen**.

4 Füllen Sie das Formular aus.

Bezeichnung	Beschreibung
Bereichsname	Geben Sie den Domänennamen für den Bereich ein. Geben Sie den Bereich in Großbuchstaben ein. Der Bereich muss dem in Active Directory eingerichteten Domänennamen entsprechen.
Key Distribution Centers	Geben Sie die KDC-Server für den Bereich ein. Trennen Sie mehrere Server durch ein Komma.
KDC-Zeitüberschreitung (in Sekunden)	Geben Sie die Zeit ein, die auf eine KDC-Antwort gewartet werden soll. Die Standardeinstellung ist 3 Sekunden.

5 Klicken Sie auf **Speichern**.

Weiter

Konfigurieren Sie die Keytab-Einstellungen.

Keytab-Einstellungen hochladen

Eine Keytab-Datei ist eine Datei, die Paare aus Kerberos-Prinzipalen und verschlüsselten Schlüsseln enthält. Eine Keytab-Datei wird für Anwendungen erstellt, die eine Anmeldung per Single Sign-on erfordern. Unified Access Gateway Identity Bridging nutzt eine Keytab-Datei zur Authentifizierung bei Remote-Systemen, die Kerberos verwenden, ohne dass ein Kennwort eingegeben werden muss.

Wenn ein Benutzer über den Identitätsanbieter bei Unified Access Gateway authentifiziert wird, fordert Unified Access Gateway ein Kerberos-Ticket beim Kerberos Domain Controller an, um den Benutzer zu authentifizieren.

Zur Authentifizierung bei der internen Active Directory-Domäne nimmt Unified Access Gateway mithilfe der Keytab-Datei die Identität des Benutzers an. Unified Access Gateway benötigt ein Dienstkonto eines Domänenbenutzers in der Active Directory-Domäne. Unified Access Gateway ist nicht direkt mit der Domäne verknüpft.

Hinweis Wenn der Administrator die Keytab-Datei für ein Dienstkonto neu generiert, muss die Keytab-Datei in Unified Access Gateway nochmals hochgeladen werden.

Voraussetzungen

Greifen Sie auf die Kerberos-Keytab-Datei zu, die in Unified Access Gateway hochgeladen werden soll. Bei einer Keytab-Datei handelt es sich um eine binäre Datei. Wenn möglich, verwenden Sie SCP oder eine andere sichere Methode, um die Keytab-Datei zwischen Computern zu übertragen.

Vorgehensweise

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

2 Wählen Sie im Abschnitt **Erweiterte Einstellungen > Einstellungen für Identity Bridging** das Zahnradsymbol **Keytab-Einstellungen hochladen**.

3 (Optional) Geben Sie den Kerberos-Prinzipalnamen im Textfeld **Name des Prinzipals** ein.

   Jeder Prinzipal ist stets durch den Namen des Bereichs vollständig qualifiziert. Der Bereich muss in Großbuchstaben eingegeben werden.

   Stellen Sie sicher, dass der hier eingegebene Prinzipalname der erste in der Keytab-Datei gefundene Prinzipalname ist. Wenn sich dieser Prinzipalname nicht in der Keytab-Datei befindet, die hochgeladen wird, schlägt das Hochladen der Keytab-Datei fehl.

4 Klicken Sie im Feld **Keytab-Datei auswählen** auf **Auswählen** und suchen Sie die Keytab-Datei, die Sie gespeichert haben. Klicken Sie auf **Öffnen**.

   Wenn Sie den Namen des Prinzipals nicht eingegeben haben, wird der erste in der Keytab-Datei gefundene Prinzipal verwendet. Sie können mehrere Keytab-Dateien in einer Datei zusammenführen.

5 Klicken Sie auf **Speichern**.

Weiter

Konfigurieren Sie den Web-Reverse-Proxy für Unified Access Gateway Identity Bridging.

Konfigurieren eines Web-Reverse-Proxys für Identity Bridging

Aktivieren Sie Identity Bridging, konfigurieren Sie den externen Hostnamen für den Dienst und laden Sie die Unified Access Gateway-Dienstanbieter-Metadatendatei herunter.

Diese Metadatendatei wird auf die Konfigurationsseite der Webanwendung im VMware Identity Manager-Dienst hochgeladen.

Voraussetzungen

In der Unified Access Gateway-Verwaltungsoberfläche im Abschnitt „Erweiterte Einstellungen“ konfigurierte Identity Bridging-Einstellungen. Die folgenden Einstellungen müssen konfiguriert sein.

- Die Identitätsanbieter-Metadaten müssen auf Unified Access Gateway hochgeladen sein.
- Der Kerberos-Prinzipalname muss konfiguriert und die Keytab-Datei muss auf Unified Access Gateway hochgeladen sein.
- Der Bereichsname und die Key Distribution Center-Informationen.

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 Klicken Sie auf der Seite „Reverse-Proxy-Einstellungen“ auf **Hinzufügen**, um eine neue Proxy-Einstellung zu erstellen.

5 Konfigurieren Sie die folgenden Edgediensteinstellungen.

Option	Beschreibung
Bezeichner	Für den Bezeichner des Edgedienstes wird der Web-Reverse-Proxy festgelegt.
Instanzen-ID	Eindeutiger Name für die Instanz des Web-Reverse-Proxys.
Proxy-Ziel-URL	Geben Sie die interne URI für die Webanwendung an. Unified Access Gateway muss diese URL auflösen und auf sie zugreifen können.

Option	Beschreibung
Fingerabdrücke für Proxy-Ziel-URL	Geben Sie den entsprechenden URI für diese Proxy-Einstellung an. 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	(Optional) Geben Sie ein Host-Muster an. Das Host-Muster teilt Unified Access Gateway mit, wann Datenverkehr unter Verwendung dieser Proxy-Einstellung weitergeleitet werden muss, falls das Proxy-Muster nicht eindeutig ist. Dies wird anhand der URL entschieden, die vom Webbrowser des Clients verwendet wird. Beispiel: **`(/|/SAAS(.*)|/hc(.*)|/web(.*)|/catalog-portal(.*))`**.

6 Ändern Sie im Abschnitt „Identity Bridging aktivieren“ den Wert NEIN zu **JA**.

7 Konfigurieren Sie die folgenden Identity Bridging-Einstellungen.

Option	Beschreibung
Identitätsanbieter	Wählen Sie im Dropdown-Menü den zu verwendenden Identitätsanbieter aus.
Keytab	Wählen Sie im Dropdown-Menü die für diesen Reverse-Proxy konfigurierte Keytab-Datei.
Name des Prinzipals des Zieldiensts	Geben Sie den Prinzipalnamen des Kerberos-Diensts ein. Jeder Prinzipal ist stets durch den Namen des Bereichs vollständig qualifiziert. Beispiel: **`myco_hostname@MYCOMPANY`**. Geben Sie den Bereichsnamen in Großbuchstaben ein. Wenn Sie keinen Namen in das Textfeld eingeben, wird der Name des Prinzipals aus dem Hostnamen der Proxy-Ziel-URL abgeleitet.
Landingpage des Dienstes	Geben Sie die Seite ein, auf die Benutzer nach Validierung der Assertion im Identitätsanbieter geleitet werden. Die Standardeinstellung lautet `/`.
Name der Benutzer-Kopfzeile	Zur kopfzeilenbasierten Authentifizierung geben Sie den Namen der HTTP-Kopfzeile ein, die die aus der Assertion abgeleitete Benutzer-ID enthält.

8 Klicken Sie im Abschnitt „SP-Metadaten herunterladen“ auf **Herunterladen**.

Speichern Sie die Dienstanbieter-Metadatendatei.

9 Klicken Sie auf **Speichern**.

Weiter

Fügen Sie die Unified Access Gateway-Dienstanbieter-Metadatendatei auf der Konfigurationsseite der Webanwendung im VMware Identity Manager-Dienst hinzu.

Hinzufügen der Unified Access Gateway -Dienstanbieter-Metadatendatei zum VMware Identity Manager-Dienst

Die von Ihnen heruntergeladene Unified Access Gateway-Dienstanbieter-Metadatendatei muss auf die Konfigurationsseite der Webanwendung im VMware Identity Manager-Dienst hochgeladen werden.

Für mehrere Unified Access Gateway-Server mit Lastausgleich muss das gleiche SSL-Zertifikat verwendet werden.

Voraussetzungen

Auf dem Computer gespeicherte Unified Access Gateway-Dienstanbieter-Metadatendatei

Vorgehensweise

1 Melden Sie sich bei der Verwaltungskonsole von VMware Identity Manager an.

2 Klicken Sie auf der Registerkarte „Katalog“ auf **Anwendung hinzufügen** und wählen Sie **Neu erstellen**.

3 Geben Sie auf der Seite „Anwendungsdetails“ einen benutzerfreundlichen Namen im Textfeld „Name“ ein.

4 Wählen Sie das Authentifizierungsprofil **SAML 2.0 POST** aus.

Sie können auch eine Beschreibung dieser Anwendung und ein Symbol, das Endbenutzern im Workspace ONE-Portal angezeigt werden soll, hinzufügen.

5 Klicken Sie auf **Weiter** und führen Sie auf der Seite „Anwendungskonfiguration“ einen Bildlauf zum Abschnitt **Konfigurieren über** durch.

6 Wählen Sie das Optionsfeld „Metadaten-XML“ aus und fügen Sie den Metadatentext des Unified Access Gateway-Dienstanbieters in das Textfeld „Metadaten-XML“ ein.

7 (Optional) Ordnen Sie im Abschnitt „Attributzuordnung“ die folgenden Attributnamen den Werten des Benutzerprofils zu. Der Wert im FORMAT-Feld lautet „Einfach“. Die Attributnamen müssen in Kleinbuchstaben eingegeben werden.

Name	Konfigurierter Wert
upn	userPrincipalName
userid	Active Directory-Benutzer-ID

8 Klicken Sie auf **Speichern**.

Weiter

Erteilen Sie Benutzern und Gruppen Berechtigungen für diese Anwendung.

Hinweis Unified Access Gateway unterstützt nur Benutzer einer Domäne. Wenn mehrere Domänen für den Dienstanbieter eingerichtet sind, kann nur Benutzern in einer einzigen Domäne der Zugriff auf die Anwendung erteilt werden.

Bereitstellung mit AirWatch Tunnel

Die Unified Access Gateway-Appliance wird in der DMZ bereitgestellt. Zur Bereitstellung gehört die Installation der Unified Access Gateway-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.

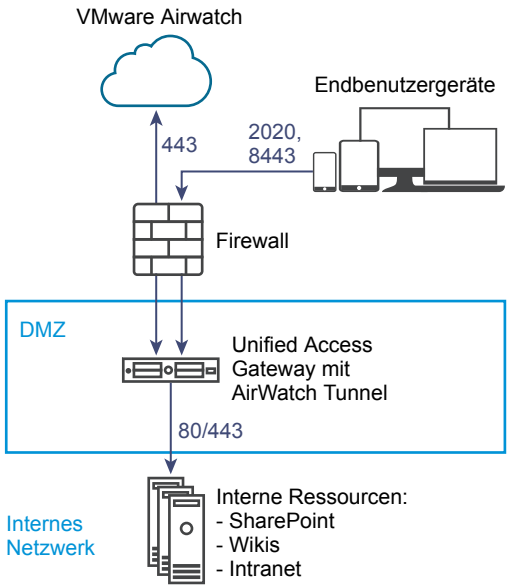
Weitere Informationen zum Bereitstellen von Unified Access Gateway mit AirWatch finden Sie unter https://resources.air-watch.com/view/vb7zp7wwhpw756m2pfxy .

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 4-8. Tunnel-Proxy-Bereitstellung



Relay Endpoint-Bereitstellungsmodell

Die Architektur des Relay-Endpoint-Bereitstellungsmodells umfasst zwei AirWatch Tunnel-Instanzen mit separaten Rollen.

Der AirWatch Tunnel-Relay-Server befindet sich in der demilitarisierten Netzwerkzone (DMZ). Vom öffentlichen DNS kann über die konfigurierten Ports darauf zugegriffen werden.

Die Ports für den Zugriff auf den öffentlichen DNS sind 8443 (über den App-spezifischen Tunnel) und Port 2020 (Proxy). Der AirWatch Tunnel-Endpoint-Server wird in dem internen Netzwerk installiert, das Intranetsites und Webanwendungen hostet. Der AirWatch Tunnel-Endpoint-Server benötigt einen internen DNS-Eintrag, der vom Relay-Server aufgelöst werden kann. Dieses Bereitstellungsmodell trennt den öffentlich verfügbaren Server von dem Server, der direkt mit den internen Ressourcen verbunden ist, und bietet so eine zusätzliche Schutzschicht.

Die Rolle des Relay-Servers umfasst die Kommunikation mit der AirWatch-API, den AWCM-Komponenten und den Authentifizierungsgeräten, wenn Anforderungen an AirWatch Tunnel gesendet werden. In diesem Bereitstellungsmodell unterstützt AirWatch Tunnel einen ausgehenden Proxy zur Kommunikation mit API und AWCM über das Relay. Der App-spezifische Tunneldienst muss direkt mit der API und AWCM kommunizieren. Wenn ein Gerät eine Anforderung an AirWatch Tunnel sendet, ermittelt der Relay-Server, ob das Gerät für den Zugriff auf den Dienst autorisiert ist. Nach der Authentifizierung wird die Anforderung sicher über HTTPS und einen einzigen Port an den AirWatch Tunnel-Endpoint-Server weitergeleitet.

Hinweis Der Standardport lautet 2010.

Die Rolle des Endpoint-Servers besteht darin, eine Verbindung zum internen DNS oder zu der vom Gerät angeforderten IP herzustellen. Der Endpoint-Server kommuniziert nur mit der API oder AWCM, wenn für **Enable API and AWCM outbound calls via proxy** (Ausgehende API- und AWCM-Aufrufe über Proxy aktivieren) in den AirWatch Tunnel-Einstellungen der AirWatch-Konsole **Aktiviert** festgelegt ist. Der Relay-Server führt regelmäßig Integritätsprüfungen durch, um sicherzustellen, dass der Endpoint aktiv und verfügbar ist.

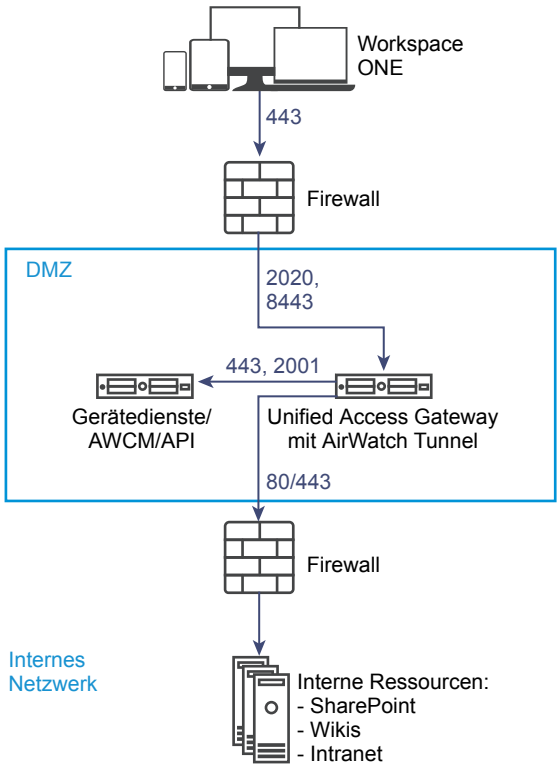
Diese Komponenten können auf gemeinsam genutzten oder dedizierten Servern installiert werden. Installieren Sie AirWatch Tunnel auf dedizierten Linux-Servern, um sicherzustellen, dass die Leistung nicht durch andere Anwendungen beeinträchtigt wird, die auf demselben Server ausgeführt werden. Für eine Relay-Endpoint-Bereitstellung werden Proxy- und App-spezifische Tunnelkomponenten auf demselben Relay-Server installiert. Nur die Proxy-Komponente wird auf dem Endpoint-Server installiert. Die App-spezifische Relay-Komponente verwendet den Proxy-Endpoint, um eine Verbindung zu internen Anwendungen herzustellen, sodass die Komponenten einen gemeinsamen Relay-Endpoint-Port und denselben Endpoint-Hostnamen nutzen.

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 4-9. 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. Unified Access Gateway kann mit Servern kommunizieren, die das View XML-Protokoll verwenden – etwa dem 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.
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
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 Unified Access Gateway diesen Proxy für den anfänglichen API-Aufruf, um die Konfiguration aus der AirWatch-Verwaltungskonsole abzurufen.
Hosteinträge	Geben Sie eine durch Komma getrennte Liste von Hostnamen ein, die der /etc/hosts-Datei hinzugefügt werden. Jeder Eintrag enthält eine IP, einen Hostnamen und einen optionalen Hostnamensalias (in dieser Reihenfolge), die durch ein Leerzeichen getrennt sind. Beispiel: `10.192.168.1 example1.com, 10.192.168.2 example2.com example-alias`
Vertrauenswürdige Zertifikate	Wählen Sie die vertrauenswürdigen Zertifikatdateien aus, die dem Trust Store hinzugefügt werden sollen.

7 Klicken Sie auf **Speichern**.

Konfigurieren von Unified Access Gateway mit TLS-/SSL-Zertifikaten

5

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

Hinweis Die Konfiguration der TLS-/SSL-Zertifikate für die Unified Access Gateway-Appliance gilt nur für Horizon View, Horizon Cloud und Web-Reverse-Proxy.

Konfigurieren von TLS-/SSL-Zertifikaten für Unified Access Gateway - Appliances

TLS/SSL ist für Clientverbindungen mit Unified Access Gateway-Appliances erforderlich. Clientverbundene Unified Access Gateway-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 Unified Access Gateway-Appliance wird ein standardmäßiges 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 Unified Access Gateway 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 einen einzelnen Server

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

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

Wenn Sie eine Zertifikatsignieranforderung an eine Zertifizierungsstelle übermitteln, geben Sie den Servernamen an, der mit dem Zertifikat verknüpft werden soll. Stellen Sie sicher, dass die Unified Access Gateway-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 Unified Access Gateway-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 (wie `horizon.example.com` in diesem Beispiel) ist das Zertifikat gültig, da es dem durch den Client angegebenen Hostnamen entspricht.

Wenn Sie eine Zertifikatsignieranforderung an eine Zertifizierungsstelle übermitteln, geben Sie die virtuelle IP-Adresse (VIP) des Lastausgleichsdiensts der externen Schnittstelle als Common Name und den SAN-Namen an. Stellen Sie sicher, dass die Unified Access Gateway-Appliance den bereitgestellten Servernamen auflösen kann und dieser mit dem Namen identisch ist, der dem Zertifikat zugeordnet wurde.

Das Zertifikat wird auf Port 443 verwendet.

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 Unified Access Gateway-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 Unified Access Gateway-Appliance importierte Zertifikate müssen von den Clientcomputern als vertrauenswürdig eingestuft werden und für alle Instanzen von Unified Access Gateway 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 Unified Access Gateway-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 Unified Access Gateway stehen drei mögliche Arten von Zertifikaten zur Verfügung, die eventuell konvertiert werden müssen.

- Sie müssen immer ein TLS/SSL-Serverzertifikat für die Unified Access Gateway-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 Unified Access Gateway-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 Unified Access Gateway-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 mycaservercertkey.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 Unified Access Gateway-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 Zertifikat sieht ähnlich wie in diesem Beispiel aus.

Abbildung 5-1. Zertifikatdatei im einzeiligen Format

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 Unified Access Gateway 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 Unified Access Gateway“, auf Seite 60. Erläuterungen zu Smartcard-Zertifikaten erhalten Sie unter „Konfigurieren der Zertifikat- oder Smartcard-Authentifizierung in der Unified Access Gateway-Appliance“, auf Seite 63.

Ersetzen des Standard-TLS/SSL-Serverzertifikats für Unified Access Gateway

Um ein vertrauenswürdiges, von einer Zertifizierungsstelle signiertes TLS-/SSL-Serverzertifikat in der Unified Access Gateway-Appliance zu speichern, müssen Sie das Zertifikat in das korrekte Format konvertieren und mit der Verwaltungsoberfläche oder PowerShell-Skripten konfigurieren.

Für Produktionsumgebungen empfiehlt VMware ausdrücklich, das Standardzertifikat so schnell wie möglich zu ersetzen. Das Standard-TLS/SSL-Serverzertifikat, das bei der Bereitstellung einer Unified Access Gateway-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.

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 Unified Access Gateway-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“, auf Seite 58.

Vorgehensweise

1. Klicken Sie auf der Verwaltungsoberfläche im Bereich „Manuell konfigurieren“ auf „Auswählen“.
2. Klicken Sie unter „Erweiterte Einstellungen“ > „Einstellungen für TLS-Serverzertifikat“ auf das Zahnradsymbol.
3. Klicken Sie für den privaten Schlüssel auf **Auswählen** und suchen Sie nach der Datei mit dem privaten Schlüssel. Klicken Sie auf **Öffnen**, um die Datei hochzuladen.
4. Klicken Sie für die Zertifikatkette auf **Auswählen** und suchen Sie nach der Zertifikatdatei. Klicken Sie auf **Öffnen**, um die Datei hochzuladen.
5. Klicken Sie auf **Speichern**.

   Wenn das Zertifikat akzeptiert wird, wird eine Erfolgsmeldung angezeigt.

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 Unified Access Gateway-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 Unified Access Gateway-REST-API vertraut. Die Spezifikation für diese API ist über die folgende URL auf der virtuellen Maschine verfügbar, auf der Unified Access Gateway 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 Unified Access Gateway-REST-API aufzurufen und die Protokolle sowie Verschlüsselungssammlungen zu konfigurieren.

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

```
curl -k -d @- -u 'admin' -H "Content-Type: application/json" -X PUT https://access-point-ap-
pliance.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 Unified Access Gateway 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 Unified Access Gateway-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 Unified Access Gateway -Appliance

Sie können die x509-Zertifikatauthentifizierung in Unified Access Gateway 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 Unified Access Gateway-Dienst ausgeführt. Unified Access Gateway 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 Unified Access Gateway 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 Unified Access Gateway an den VMware Identity Manager-Dienst weitergeleitet. Die Smartcard-Authentifizierung für die Unified Access Gateway-Appliance kann nur konfiguriert werden, wenn Unified Access Gateway mit Horizon 7 verwendet wird.

Konfigurieren der Zertifikatauthentifizierung auf Unified Access Gateway

Sie aktivieren und konfigurieren die Zertifikatauthentifizierung über die Unified Access Gateway-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“, auf Seite 66.
- Prüfen Sie, ob die SAML-Metadaten von Unified Access Gateway zum Dienstanbieter hinzugefügt und die SAML-Metadaten des Dienstanbieters in die Unified Access Gateway-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 Unified Access Gateway-Appliance hinter einem Lastausgleichsdienst eingerichtet ist, müssen Sie sicherstellen, dass Unified Access Gateway 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 Unified Access Gateway und Client stattfindet, damit das Zertifikat an Unified Access Gateway 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“, auf Seite 66.

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.

Weiter

Fügen Sie das Stammzertifikat oder das Zwischenzertifikat oder beide zu einer Server-Vertrauensspeicherdatei hinzu.

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.

Weiter

Fügen Sie das CA-Zertifikat einer Server-Vertrauensspeicherdatei hinzu.

Konfigurieren der RSA SecurID-Authentifizierung in Unified Access Gateway

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

Option	Aktion
*Externer HOST-Name	Geben Sie die IP-Adresse der Unified Access Gateway-Instanz ein. Der eingegebene Wert muss mit dem Wert übereinstimmen, den Sie beim Hinzufügen der Unified Access Gateway-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 Unified Access Gateway

Sie können Unified Access Gateway so konfigurieren, dass Benutzer die RADIUS-Authentifizierung nutzen müssen. Sie können die Informationen des RADIUS-Servers in der Unified Access Gateway-Appliance konfigurieren.

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 Access Challenge-Meldung ausgibt, zeigt Unified Access Gateway 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 Unified Access Gateway-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 Unified Access Gateway. 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.
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.

Option	Aktion
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 Unified Access Gateway

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 Unified Access Gateway-Konfiguration der adaptiven Authentifizierung aufgeführt sind, um festzulegen, ob ein Benutzer mit Benutzernamen 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 Unified Access Gateway

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“.
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.

Option	Beschreibung
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 Unified Access Gateway -SAML-Metadaten

Sie müssen SAML-Metadaten in der Unified Access Gateway-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 Unified Access Gateway der Identitätsanbieter und der Server der Dienstanbieter.

Voraussetzungen

- Konfigurieren Sie die Uhr (UTC) der Unified Access Gateway-Appliance, damit diese über die korrekte Uhrzeit verfügt. Öffnen Sie z. B. ein Konsolenfenster auf der virtuellen Unified Access Gateway-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 Unified Access Gateway-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 Unified Access Gateway-Metadaten.

  Hinweis VMware empfiehlt die Erstellung und Verwendung eines spezifischen SAML-Signaturzertifikats, wenn in Ihrer Installation mehr als eine Unified Access Gateway-Appliance vorhanden ist. In diesem Fall müssen alle Appliances mit demselben Signaturzertifikat konfiguriert werden, damit der Server Assertions von jeder Unified Access Gateway-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“, auf Seite 58.

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 Unified Access Gateway-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 Unified Access Gateway als Dienstanbieter verwendet werden kann.

Für einen Horizon Cloud-Server finden Sie spezielle Anweisungen in der Produktdokumentation.

Kopieren von SAML-Metadaten für einen Dienstanbieter in Unified Access Gateway

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

Voraussetzungen

Stellen Sie sicher, dass ein SAML-Authentifikator für Unified Access Gateway 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 Verwaltungsoberfläche von Unified Access Gateway 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**.

Unified Access Gateway und der Dienstanbieter können nun Authentifizierungs- und Autorisierungsinformationen austauschen.

Fehlerbehebung bei der Unified Access Gateway - Bereitstellung

7

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

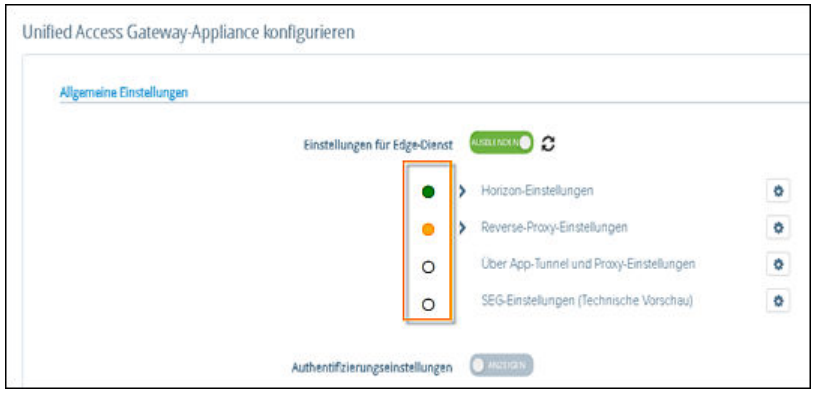
Sie können die Vorgehensweisen zur Fehlerbehebung nutzen, um die Ursachen dieser Probleme zu ermitteln. Anschließend können Sie versuchen, die Probleme selbst zu behandeln, oder sich an den technischen Support von VMware wenden, um Unterstützung zu erhalten.

Dieses Kapitel behandelt die folgenden Themen:

Überwachen der Integrität von bereitgestellten Diensten

Über die Verwaltungsoberfläche für die Edge-Einstellungen können Sie schnell erkennen, ob die von Ihnen bereitgestellten Dienste konfiguriert und gestartet sind und erfolgreich ausgeführt werden.

Abbildung 7-1. Integritätsprüfung



Vor dem Dienst wird ein Kreis angezeigt. Die Farbcodierung hat die nachfolgende Bedeutung.

- Ein leerer Kreis bedeutet, dass die Einstellung nicht konfiguriert ist.
- Ein roter Kreis bedeutet, dass der Dienst nicht aktiv ist.
- Ein gelber Kreis bedeutet, dass der Dienst teilweise ausgeführt wird.
- Ein grüner Kreis bedeutet, dass der Dienst ohne Probleme ausgeführt wird.

Fehlerbehebung bei Bereitstellungsfehlern

Möglicherweise treten Probleme beim Bereitstellen von Unified Access Gateway 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.

Konfigurieren von Unified Access Gateway für die RSA SecurID-Authentifizierung

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
```

Für beide IP-Adressen sollte die IP-Adresse von Unified Access Gateway eingestellt 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.

Erfassen von Protokollen auf der Unified Access Gateway -Appliance

Laden Sie die Datei AP-Log Archieve.zip über die Support-Einstellungen in der Verwaltungsoberfläche herunter. Die ZIP-Datei enthält alle Protokolle Ihrer Unified Access Gateway-Appliance.

Festlegen der Protokollierungsebene

Sie können die Einstellungen für die Protokollebene über die Verwaltungsoberfläche festlegen. Wechseln Sie zur Seite „Support-Einstellungen“ und wählen Sie „Einstellungen auf Protokollebene“ aus. Die folgenden Protokollebenen können generiert werden: INFO, WARNUNG, FEHLER und DEBUG. Standardmäßig ist die Protokollebene INFO eingestellt.

Im Folgenden wird der Typ der auf jeder Protokollebene erfassten Informationen beschrieben.

Tabelle 7-1. Protokollierungsebenen

Ebene	Typ der erfassten Informationen
INFO	Die INFO-Ebene umfasst Informationsmeldungen, die den Fortschritt des Diensts angeben.
FEHLER	Die FEHLER-Ebene umfasst Fehlerereignisse, wobei der Dienst möglicherweise trotzdem noch ausgeführt werden kann.
WARNUNG	Die Ebene WARNUNG umfasst potenziell gefährliche Situationen, die behoben oder ignoriert werden können.
DEBUG	Ereignisse, die für das Debugging im Allgemeinen nützlich sind. Sie können den Debug-Modus aktivieren, um den internen Status der Appliance anzuzeigen oder zu ändern. Anhand des Debug-Modus können Sie das Bereitstellungsszenario in Ihrer Umgebung testen.

Erfassen von Protokollen

Laden Sie die ZIP-Dateien mit den Protokollen über den Abschnitt „Support-Einstellungen“ in der Verwaltungsoberfläche herunter.

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 7-2. 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 Unified Access Gateway-Appliance.
`ps.log`	Enthält eine Verarbeitungsliste.
`ifconfig.log`	Enthält Informationen über Netzwerkschnittstellen.
`free.log`	Enthält Informationen über die Nutzung des Arbeitsspeichers.

Tabelle 7-3. Protokolldateien für Unified Access Gateway

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 Unified Access Gateway-REST-API auf Port 9443 bereitstellt.
`admin-zookeeper.log`	Enthält Protokollmeldungen zum Daten-Layer für das Speichern der Unified Access Gateway-Konfigurationsinformationen.
`tunnel.log`	Enthält Protokollmeldungen aus dem Tunnelprozess, der Teil der XML-API-Verarbeitung ist.
`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.

Unified Access Gateway-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.

Index

T

U

V

W

X

Z