

Déploiement et configuration de VMware Unified Access Gateway

Unified Access Gateway 3.0

vmware[®]

Vous trouverez la documentation technique la plus récente sur le site Web de VMware à l'adresse :

<https://docs.vmware.com/fr/>

Le site Web de VMware propose également les dernières mises à jour des produits.

N'hésitez pas à nous transmettre tous vos commentaires concernant cette documentation à l'adresse suivante :

docfeedback@vmware.com

Copyright © 2016, 2017 VMware, Inc. Tous droits réservés. [Copyright et informations sur les marques.](#)

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

VMware, Inc.
100-101 Quartier Boieldieu
92042 Paris La Défense
France
www.vmware.com/fr

Table des matières

Déploiement et configuration de VMware Unified Access Gateway	5
1 Préparation au déploiement de VMware Unified Access Gateway	7
Unified Access Gateway comme une passerelle sécurisée	7
Utilisation d' Unified Access Gateway au lieu d'un réseau privé virtuel	8
Configuration requise pour le système et le réseau Unified Access Gateway	8
Règles de pare-feu pour les dispositifs Unified Access Gateway basés sur une zone DMZ	10
Topologies d'équilibrage de charge Unified Access Gateway	12
Conception de la DMZ pour Unified Access Gateway avec plusieurs cartes d'interface réseau	14
Mettre à niveau sans interruption	17
2 Déploiement du dispositif Unified Access Gateway	19
Utilisation de l'assistant de modèle OVF pour déployer Unified Access Gateway	19
Déploiement d' Unified Access Gateway au moyen de l'assistant de modèle OVF	20
Configuration d' Unified Access Gateway à partir des pages de configuration d'administration	24
Configurer les paramètres système d' Unified Access Gateway	24
Mise à jour des certificats signés du serveur SSL	26
3 Utilisation de PowerShell pour déployer Unified Access Gateway	27
Configuration système requise pour déployer Unified Access Gateway à l'aide de PowerShell	27
Utilisation de PowerShell pour déployer le dispositif Unified Access Gateway	28
4 Cas d'utilisation de déploiement d'Unified Access Gateway	31
Déploiement avec Horizon View et Horizon Cloud avec infrastructure sur site	31
Configuration des paramètres Horizon	35
Options de configuration des URL externes Blast TCP et UDP	37
Déploiement en tant que proxy inverse	38
Configurer le proxy inverse	40
Déploiement pour l'accès avec Single Sign-On à des applications Web héritées sur site	43
Scénarios de déploiement du pontage d'identité	44
Configuration des paramètres du pontage d'identité	46
Configurer un proxy inverse Web pour le pontage d'identité	49
Ajouter le fichier de métadonnées de fournisseur de services d' Unified Access Gateway au service VMware Identity Manager	50
Tunnel VMware sur Unified Access Gateway	51
Configurer les paramètres de VMware Tunnel pour AirWatch	52
Déploiement de VMware Tunnel pour AirWatch avec PowerShell	53

5	Configuration d' Unified Access Gateway à l'aide de certificats TLS/SSL	55
	Configuration de certificats TLS/SSL pour les dispositifs Unified Access Gateway	55
	Sélection du type de certificat correct	55
	Convertir des fichiers de certificat au format PEM sur une ligne	56
	Remplacer le certificat de serveur TLS/SSL par défaut pour Unified Access Gateway	58
	Modifier les protocoles de sécurité et les suites de chiffrement utilisés pour la communication TLS ou SSL	59
6	Configuration de l'authentification dans la zone DMZ	61
	Configuration de l'authentification par certificat ou carte à puce sur le dispositif Unified Access Gateway	61
	Configurer l'authentification par certificat sur Unified Access Gateway	62
	Obtenir des certificats d'autorités de certification	64
	Configurer l'authentification RSA SecurID dans Unified Access Gateway	65
	Configuration de RADIUS pour Unified Access Gateway	66
	Configuration de l'authentification RADIUS	66
	Configuration de RSA Adaptive Authentication dans Unified Access Gateway	68
	Configurer RSA Adaptive Authentication dans Unified Access Gateway	69
	Générer des métadonnées SAML Unified Access Gateway	70
	Création d'un authentificateur SAML utilisé par d'autres fournisseurs de services	71
	Copier les métadonnées SAML du fournisseur de services sur Unified Access Gateway	71
7	Dépannage du déploiement d' Unified Access Gateway	73
	Contrôle de la santé des services déployés	73
	Dépannage des erreurs de déploiement	74
	Collecte de journaux depuis le dispositif Unified Access Gateway	75
	Index	77

Déploiement et configuration de VMware Unified Access Gateway

Déploiement et configuration d'Unified Access Gateway fournit des informations sur la conception du déploiement de VMware Horizon[®], de VMware Identity Manager[™] et de VMware AirWatch[®] qui utilise VMware Unified Access Gateway[™] pour un accès externe sécurisé aux applications de votre organisation. Ces applications peuvent être des applications Windows, des applications SaaS (Software as a Service) et des postes de travail. Ce guide contient également des instructions sur le déploiement de dispositifs virtuels Unified Access Gateway et sur la modification des paramètres de configuration après le déploiement.

Public cible

Ces informations sont destinées à toute personne souhaitant déployer et utiliser des dispositifs Unified Access Gateway. Les informations sont rédigées pour des administrateurs système Linux et Windows expérimentés qui connaissent bien la technologie des machines virtuelles et les opérations de centre de données.

Préparation au déploiement de VMware Unified Access Gateway

1

Unified Access Gateway fonctionne comme une passerelle sécurisée pour les utilisateurs qui veulent accéder à des applications et des postes de travail distants depuis l'extérieur du pare-feu d'entreprise.

REMARQUE VMware Unified Access Gateway[®] était appelé auparavant VMware Access Point.

Ce chapitre aborde les rubriques suivantes :

- [« Unified Access Gateway comme une passerelle sécurisée », page 7](#)
- [« Utilisation d'Unified Access Gateway au lieu d'un réseau privé virtuel », page 8](#)
- [« Configuration requise pour le système et le réseau Unified Access Gateway », page 8](#)
- [« Règles de pare-feu pour les dispositifs Unified Access Gateway basés sur une zone DMZ », page 10](#)
- [« Topologies d'équilibrage de charge Unified Access Gateway », page 12](#)
- [« Conception de la DMZ pour Unified Access Gateway avec plusieurs cartes d'interface réseau », page 14](#)
- [« Mettre à niveau sans interruption », page 17](#)

Unified Access Gateway comme une passerelle sécurisée

Unified Access Gateway est un dispositif qui est normalement installé dans une zone démilitarisée (DMZ). Unified Access Gateway est utilisé pour s'assurer que le trafic entrant dans le centre de données d'entreprise est effectué uniquement pour le compte d'un utilisateur distant à authentification élevée.

Unified Access Gateway redirige les demandes d'authentification vers le serveur approprié et rejette toute demande non authentifiée. Les utilisateurs ne peuvent accéder qu'aux ressources dont l'accès leur est autorisé.

Unified Access Gateway garantit également que le trafic d'un utilisateur authentifié peut être dirigé uniquement vers les ressources de poste de travail et d'application auxquelles l'utilisateur est autorisé à accéder. Ce niveau de protection implique une inspection spécifique des protocoles de poste de travail et une coordination des stratégies et des adresses réseau susceptibles de changer rapidement pour pouvoir contrôler l'accès de façon précise.

Unified Access Gateway agit comme un hôte proxy pour les connexions à l'intérieur du réseau approuvé de votre entreprise. Cette conception offre une couche de sécurité supplémentaire en protégeant les postes de travail virtuels, les hôtes d'application et les serveurs vis-à-vis des sites Internet publics.

Unified Access Gateway est conçu spécifiquement pour la zone DMZ. Les paramètres de renforcement suivants sont implémentés.

- Noyau Linux et correctifs logiciels à jour

- Prise en charge de plusieurs cartes réseau pour le trafic sur Internet et l'intranet
- SSH désactivé
- Services FTP, Telnet, Rlogin ou Rsh désactivés
- Services indésirables désactivés

Utilisation d' Unified Access Gateway au lieu d'un réseau privé virtuel

Unified Access Gateway et les solutions VPN génériques sont similaires, puisqu'elles s'assurent que le trafic est transmis à un réseau interne uniquement pour le compte d'utilisateurs à authentification élevée.

Avantages d'Unified Access Gateway par rapport aux solutions VPN génériques :

- Access Control Manager. Unified Access Gateway applique des règles d'accès automatiquement. Unified Access Gateway reconnaît les droits des utilisateurs et l'adressage requis pour se connecter en interne. Un VPN fait la même chose, car la plupart des VPN autorisent un administrateur à configurer des règles de connexion réseau pour chaque utilisateur ou groupe d'utilisateurs individuellement. Au début, cela fonctionne bien avec un VPN, mais exige un travail administratif important pour appliquer les règles requises.
- Interface utilisateur. Unified Access Gateway ne modifie pas l'interface utilisateur Horizon Client simple. Avec Unified Access Gateway, lorsque Horizon Client est lancé, les utilisateurs authentifiés sont dans leur environnement View et disposent d'un accès contrôlé à leurs postes de travail et applications. Un VPN exige que vous configuriez le logiciel VPN, puis que vous vous authentifiez séparément avant de lancer Horizon Client.
- Performances. Unified Access Gateway est conçu pour maximiser la sécurité et les performances. Avec Unified Access Gateway, les protocoles PCoIP, HTML Access et WebSocket sont sécurisés sans qu'une encapsulation supplémentaire soit nécessaire. Des VPN sont implémentés en tant que VPN SSL. Cette implémentation répond aux exigences de sécurité et, avec TLS (Transport Layer Security) activé, elle est considérée comme sûre, mais le protocole sous-jacent avec SSL/TLS est simplement basé sur TCP. Avec des protocoles modernes de vidéo à distance exploitant des transports UDP sans connexion, les avantages de performance peuvent être considérablement réduits lorsque l'on force le transport TCP. Cela ne s'applique pas à toutes les technologies de VPN, car celles qui peuvent également fonctionner avec DTLS ou IPsec au lieu de SSL/TLS peuvent fonctionner correctement avec des protocoles de poste de travail View.

Configuration requise pour le système et le réseau Unified Access Gateway

Pour déployer le dispositif Unified Access Gateway, assurez-vous que votre système répond à la configuration matérielle et logicielle requise.

Versions de produit VMware prises en charge

Vous devez utiliser des versions spécifiques des produits VMware avec des versions spécifiques d'Unified Access Gateway. Consultez les notes de mise à jour des produits pour voir les dernières informations sur la compatibilité et consultez la matrice d'interopérabilité des produits VMware à l'adresse http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

Exigences matérielles d'ESXi Server

Le dispositif Unified Access Gateway doit être déployé sur une version de vSphere identique à celle prise en charge pour les produits et versions de VMware que vous utilisez.

Si vous prévoyez d'utiliser vSphere Web Client, vérifiez que le plug-in d'intégration du client est installé. Pour plus d'informations, voir la documentation vSphere. Si vous n'installez pas ce plug-in avant de démarrer l'assistant de déploiement, ce dernier vous invite à le faire. Pour cela, vous devez fermer le navigateur et quitter l'assistant.

REMARQUE Configurez l'horloge (UTC) sur le dispositif Unified Access Gateway pour qu'il soit à l'heure exacte. Par exemple, ouvrez une fenêtre de console sur la machine virtuelle Unified Access Gateway et utilisez les flèches pour sélectionner le bon fuseau horaire. Vérifiez également que l'heure de l'hôte ESXi est synchronisée avec un serveur NTP et que VMware Tools, qui est exécuté dans la machine virtuelle de dispositif, synchronise l'heure de la machine virtuelle avec celle de l'hôte ESXi.

Exigences du dispositif virtuel

Le package OVF du dispositif Unified Access Gateway sélectionne automatiquement la configuration de machine virtuelle dont Unified Access Gateway a besoin. Même si vous pouvez modifier ces paramètres, VMware vous recommande de ne pas modifier le CPU, la mémoire ou l'espace disque par des valeurs inférieures aux paramètres OVF par défaut.

- Vitesse d'horloge minimale du CPU : 2 000 MHz
- Mémoire minimale : 4 Go

Vérifiez que la banque de données que vous utilisez pour le dispositif dispose d'un espace disque libre suffisant et qu'elle répond aux autres spécifications système.

- Taille de téléchargement du dispositif virtuel : 1,4 Go
- Espace disque minimal requis à provisionnement dynamique : 2,6 Go
- Espace disque minimal requis à provisionnement statique : 20 Go

Les informations suivantes sont requises pour déployer le dispositif virtuel.

- Adresse IP statique (recommandé)
- Adresse IP du serveur DNS
- Mot de passe de l'utilisateur racine
- Mot de passe de l'utilisateur administrateur
- URL de l'instance de serveur de l'équilibrage de charge vers laquelle le dispositif Unified Access Gateway pointe

Versions de navigateurs prises en charge

Chrome, Firefox et Internet Explorer sont les navigateurs permettant de lancer l'interface utilisateur d'administration. Utilisez la version la plus récente du navigateur.

Exigences matérielles lors de l'utilisation de Windows Hyper-V Server

Lorsque vous utilisez Unified Access Gateway pour un déploiement de tunnel par application avec AirWatch, vous pouvez installer le dispositif Unified Access Gateway sur Microsoft Hyper-V Server.

Les serveurs Microsoft pris en charge sont Windows Server 2012 R2 et Windows Server 2016.

Configuration requise pour le réseau

Vous pouvez utiliser une, deux ou trois interfaces réseau, et Unified Access Gateway requiert une adresse IP statique séparée pour chacune d'entre elles. De nombreuses implémentations de zone DMZ utilisent des réseaux distincts pour sécuriser les différents types de trafic. Configurez Unified Access Gateway en fonction de la conception de réseau de la zone DMZ dans laquelle il est déployé.

- Une interface réseau est appropriée pour la validation de principe ou les tests. Avec une carte réseau, les trafics externe, interne et de gestion sont tous sur le même sous-réseau.
- Avec deux interfaces réseau, le trafic externe est sur un sous-réseau, et les trafics interne et de gestion sont sur un autre sous-réseau.
- L'option la plus sûre consiste à utiliser les trois interfaces réseau. Avec une troisième carte réseau, les trafics externe, interne et de gestion ont chacun leur propre sous-réseau.

IMPORTANT Vérifiez que vous avez attribué un pool IP à chaque réseau. Le dispositif Unified Access Gateway peut choisir les paramètres du masque de sous-réseau et de la passerelle au moment du déploiement. Pour ajouter un pool IP, dans vCenter Server, si vous utilisez le vSphere Client natif, accédez à l'onglet **Pools IP** du centre de données. Si vous utilisez vSphere Web Client, vous pouvez également créer un profil de protocole réseau. Accédez à l'onglet **Gérer** du centre de données et sélectionnez l'onglet **Profils de protocole réseau**. Pour plus d'informations, reportez-vous à la section [Configurer les profils de protocole pour la mise en réseau des machines virtuelles](#).

Si Unified Access Gateway est déployé sans pool d'adresses IP (vCenter Server), le déploiement réussit, mais lorsque vous tentez d'accéder à Unified Access Gateway avec l'interface utilisateur d'administration depuis le navigateur, le service Interface utilisateur d'administration ne se lance pas.

Exigences de conservation des journaux

Les fichiers journaux sont configurés par défaut pour utiliser une certaine quantité d'espace qui est inférieure à la taille totale de disque dans l'agrégation. Les journaux pour Unified Access Gateway sont alternés par défaut. Vous devez utiliser Syslog pour conserver ces entrées de journal. Reportez-vous à la section « [Collecte de journaux depuis le dispositif Unified Access Gateway](#) », page 75.

Règles de pare-feu pour les dispositifs Unified Access Gateway basés sur une zone DMZ

Les dispositifs Unified Access Gateway basés sur une zone DMZ requièrent certaines règles de pare-feu sur les pare-feu frontaux et principaux. Lors de l'installation, les services Unified Access Gateway sont configurés pour écouter sur certains ports réseau par défaut.

En général, un déploiement de dispositif Unified Access Gateway basé sur une zone DMZ inclut deux pare-feu.

- Un pare-feu frontal externe en réseau est nécessaire pour protéger la zone DMZ et le réseau interne. Vous configurez ce pare-feu pour permettre au trafic réseau externe d'atteindre la zone DMZ.
- Un pare-feu principal, entre la zone DMZ et le réseau interne, est requis pour fournir un deuxième niveau de sécurité. Vous configurez ce pare-feu pour accepter uniquement le trafic qui provient des services dans la zone DMZ.

La règle de pare-feu contrôle exclusivement les communications entrantes provenant du service de la zone DMZ, ce qui réduit considérablement le risque que le réseau interne soit compromis.

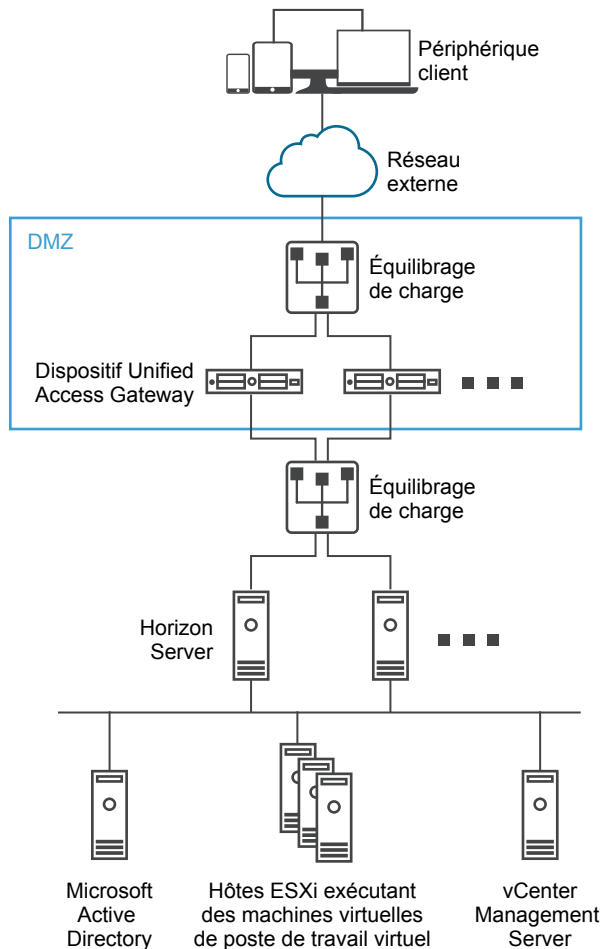
Pour autoriser des périphériques clients externes à se connecter à un dispositif Unified Access Gateway dans la zone DMZ, le pare-feu frontal doit autoriser le trafic sur certains ports. Par défaut, les périphériques clients externes et les clients Web externes (HTML Access) se connectent à un dispositif Unified Access Gateway dans la zone DMZ sur le port TCP 443. Si vous utilisez le protocole Blast, le port 8443 doit être ouvert sur le pare-feu, mais vous pouvez également configurer Blast pour le port 443.

Tableau 1-1. Exigences du port

Port	Portail	Source	Cible	Description
443	TCP	Internet	Unified Access Gateway	Pour le trafic Web, Horizon Client XML - API, Horizon Tunnel et Blast Extreme
443	UDP	Internet	Unified Access Gateway	UDP (facultatif)
8443	UDP	Internet	Unified Access Gateway	Blast Extreme (facultatif)
8443	TCP	Internet	Unified Access Gateway	Blast Extreme
4172	TCP et UDP	Internet	Unified Access Gateway	PCoIP (facultatif)
443	TCP	Unified Access Gateway	Horizon Broker	Horizon Client XML-API
22443	TCP et UDP	Unified Access Gateway	Postes de travail et hôtes RDS	Blast Extreme
4172	TCP et UDP	Unified Access Gateway	Postes de travail et hôtes RDS	PCoIP (facultatif)
32111	TCP	Unified Access Gateway	Postes de travail et hôtes RDS	Canal d'infrastructure pour la redirection USB
9427	TCP	Unified Access Gateway	Postes de travail et hôtes RDS	MMR et CDR
9443	TCP	Interface utilisateur d'administration	Unified Access Gateway	Interface de gestion

REMARQUE Tous les ports UDP requièrent que les datagrammes de transfert et les datagrammes de réponse soient autorisés.

La figure suivante montre un exemple de configuration qui comporte des pare-feu frontal et principal.

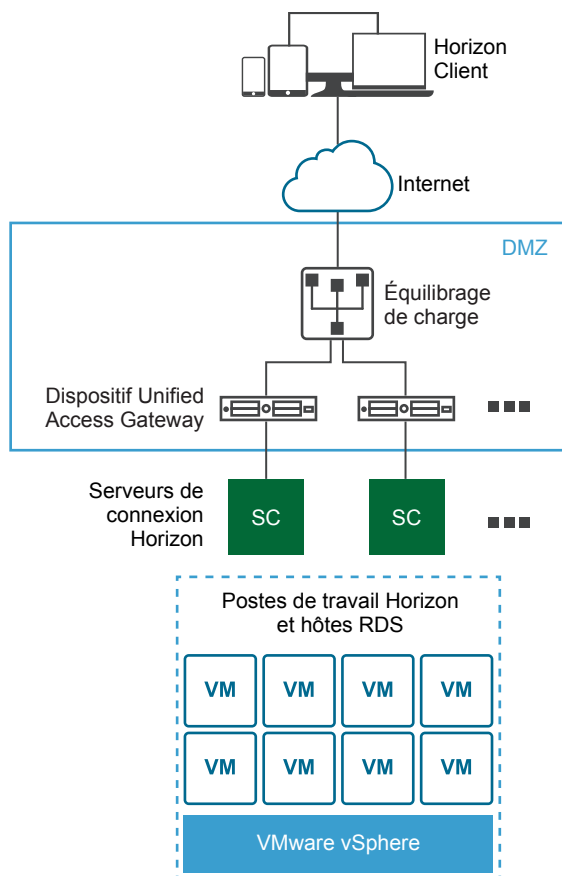
Figure 1-1. Unified Access Gateway dans la topologie de la zone DMZ

Topologies d'équilibrage de charge Unified Access Gateway

Un dispositif Unified Access Gateway dans la zone DMZ peut être configuré pour pointer vers un serveur ou vers un équilibreur de charge qui fait face à un groupe de serveurs. Les dispositifs Unified Access Gateway fonctionnent avec des solutions d'équilibrage de charge tierces standard qui sont configurées pour HTTPS.

Si le dispositif Unified Access Gateway pointe vers un équilibreur de charge devant des serveurs, la sélection de l'instance du serveur est dynamique. Par exemple, l'équilibreur de charge peut faire une sélection en fonction de la disponibilité et de sa connaissance du nombre de sessions en cours sur chaque instance du serveur. En général, les instances du serveur dans le pare-feu d'entreprise contiennent un équilibreur de charge pour prendre en charge l'accès interne. Avec Unified Access Gateway, vous pouvez pointer le dispositif Unified Access Gateway vers ce même équilibreur de charge qui est souvent déjà en cours d'utilisation.

Vous pouvez également avoir un ou plusieurs dispositifs Unified Access Gateway qui pointent vers une instance individuelle du serveur. Avec les deux approches, utilisez un équilibreur de charge devant deux dispositifs Unified Access Gateway ou plus dans la zone DMZ.

Figure 1-2. Plusieurs dispositifs Unified Access Gateway derrière un équilibrage de charge

Protocoles Horizon

Lorsqu'un utilisateur Horizon Client se connecte à un environnement Horizon, plusieurs protocoles différents sont utilisés. La première connexion est toujours le protocole XML-API principal sur HTTPS. Après une authentification réussie, un ou plusieurs protocoles secondaires sont également utilisés.

■ Protocole Horizon principal

L'utilisateur entre un nom d'hôte sur Horizon Client, ce qui démarre le protocole Horizon principal. Il s'agit d'un protocole de contrôle pour la gestion des authentifications, des autorisations et des sessions. Le protocole utilise des messages structurés XML sur HTTPS. Ce protocole est également connu sous le nom de protocole de contrôle XML-API Horizon. Dans un environnement avec équilibrage de charge comme indiqué dans l'illustration Plusieurs dispositifs Unified Access Gateway derrière un équilibrage de charge, l'équilibrage de charge achemine cette connexion vers l'un des dispositifs Unified Access Gateway. Généralement, l'équilibrage de charge sélectionne le dispositif d'abord en fonction de la disponibilité, puis, selon les dispositifs disponibles, achemine le trafic sur la base du nombre le moins élevé de sessions en cours. Cette configuration distribuée de façon uniforme le trafic en provenance de différents clients sur l'ensemble des dispositifs Unified Access Gateway disponibles.

■ Protocoles Horizon secondaires

Une fois qu'Horizon Client établit une communication sécurisée avec l'un des dispositifs Unified Access Gateway, l'utilisateur s'authentifie. Si cette tentative d'authentification réussit, une ou plusieurs connexions secondaires sont effectuées à partir d'Horizon Client. Ces connexions secondaires peuvent inclure ce qui suit :

- Le tunnel HTTPS utilisé pour l'encapsulation des protocoles TCP tels que RDP, MMR/CDR et le canal de framework client. (TCP 443)
- Protocole d'affichage Blast Extreme (TCP 443, TCP 8443, UDP 443 et UDP 8443)
- Protocole d'affichage PCoIP (TCP 443, UDP 443)

Ces protocoles Horizon secondaires doivent être acheminés vers le même dispositif Unified Access Gateway que le protocole Horizon principal. Unified Access Gateway peut ensuite autoriser les protocoles secondaires sur la base de la session de l'utilisateur authentifié. Au niveau de la sécurité Unified Access Gateway, il est important de noter qu'Unified Access Gateway n'achemine le trafic dans le centre de données d'entreprise que si le trafic s'effectue pour le compte d'un utilisateur authentifié. Si le protocole secondaire est acheminé de façon incorrecte vers un dispositif Unified Access Gateway différent de celui du dispositif de protocole principal, les utilisateurs ne sont pas autorisés et sont alors déplacés vers la zone DMZ. La connexion échoue. Le routage incorrect des protocoles secondaires est un problème courant si l'équilibrage de charge n'est pas configuré correctement.

Conception de la DMZ pour Unified Access Gateway avec plusieurs cartes d'interface réseau

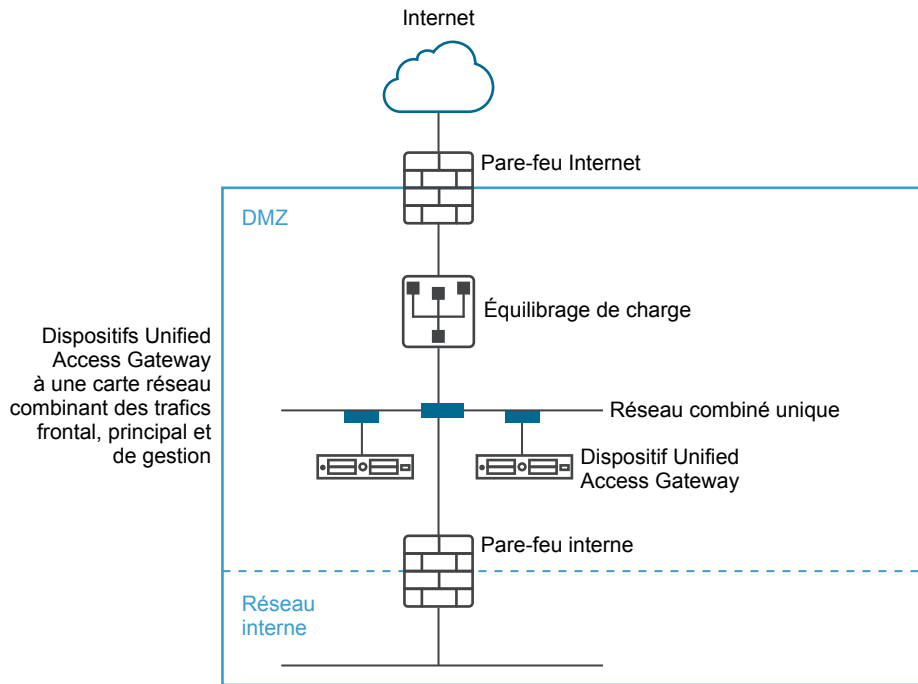
Un des paramètres de configuration pour Unified Access Gateway est le nombre de cartes réseau à utiliser. Lorsque vous déployez Unified Access Gateway, vous sélectionnez une configuration de déploiement pour votre réseau.

Vous pouvez spécifier un, deux ou trois paramètres de carte réseau, appelés onenic, twonic ou threenic.

La réduction du nombre de ports ouverts sur chaque LAN virtuel et la séparation des différents types de trafic réseau peuvent considérablement améliorer la sécurité. Les avantages concernent principalement la séparation et l'isolation des différents types de trafic réseau dans le cadre d'une stratégie de conception de sécurité DMZ en profondeur. Pour ce faire, vous pouvez implémenter des commutateurs physiques séparés au sein de la DMZ, employer plusieurs LAN virtuels au sein de la DMZ ou procéder via une DMZ complète gérée par VMware NSX.

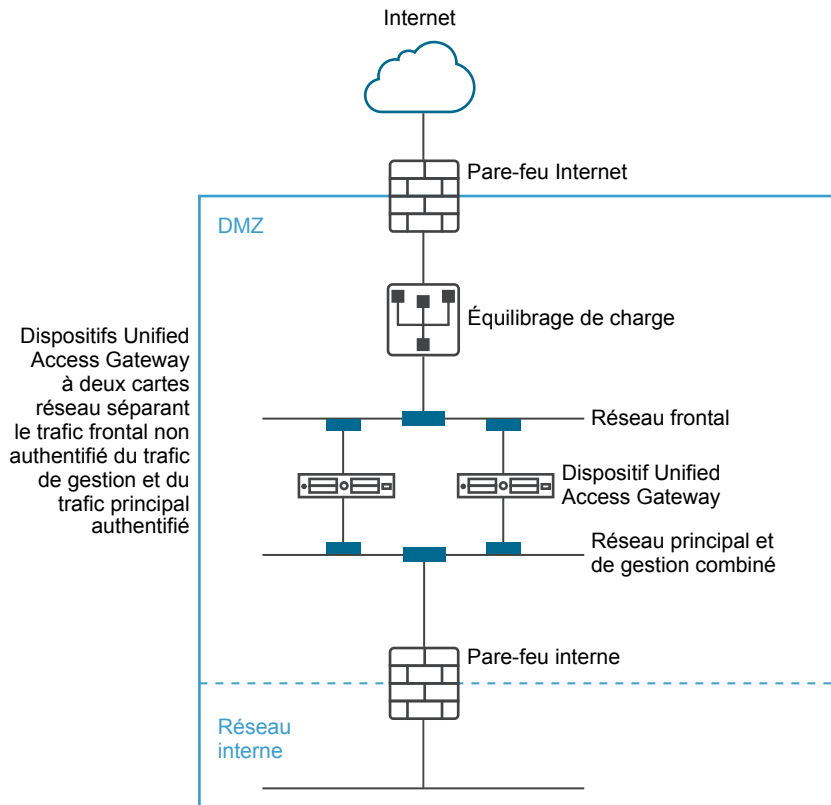
Déploiement DMZ typique avec une carte réseau unique

Le déploiement le plus simple d'Unified Access Gateway s'effectue avec une carte réseau unique sur laquelle l'ensemble du trafic réseau est combiné sur un réseau unique. Le trafic provenant du pare-feu Internet est redirigé vers l'un des dispositifs Unified Access Gateway disponibles. Unified Access Gateway achemine ensuite le trafic autorisé via le pare-feu interne vers les ressources sur le réseau interne. Unified Access Gateway ignore le trafic non autorisé.

Figure 1-3. Option à une seule carte réseau d' Unified Access Gateway

Séparation du trafic utilisateur non authentifié du réseau principal et du trafic de gestion

Une amélioration par rapport au déploiement d'une carte réseau unique consiste à spécifier deux cartes réseau. La première est toujours utilisée pour les accès non authentifiés provenant d'Internet, mais le trafic authentifié du réseau principal et le trafic de gestion sont séparés sur un réseau différent.

Figure 1-4. Option à deux cartes réseau d' Unified Access Gateway

Dans un déploiement à deux cartes réseau, Unified Access Gateway doit autoriser le trafic vers le réseau interne qui passe par le pare-feu interne. Le trafic non autorisé ne se trouve pas sur ce réseau principal. Le trafic de gestion tel que l'API REST pour Unified Access Gateway se trouve uniquement sur ce second réseau.

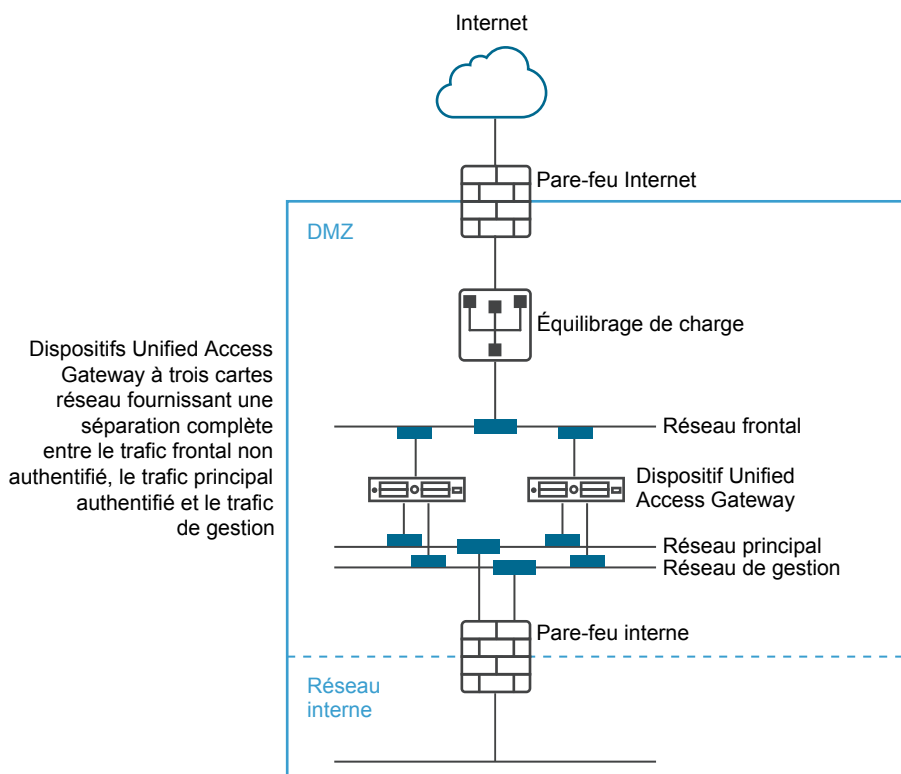
Si un périphérique sur le réseau frontal non authentifié, comme l'équilibrage de charge, a été compromis, il n'est pas possible de reconfigurer ce périphérique pour contourner Unified Access Gateway dans ce déploiement à deux cartes réseau. Il associe des règles de pare-feu de couche 4 à une sécurité Unified Access Gateway de couche 7. De la même façon, si le pare-feu Internet n'a pas été correctement configuré pour autoriser le port TCP 9443, cela n'expose toujours pas l'API REST de gestion d'Unified Access Gateway pour les utilisateurs Internet. Un principe de défense en profondeur fait appel à plusieurs niveaux de protection, comme le fait de savoir qu'une simple erreur de configuration ou attaque du système n'entraîne pas nécessairement une vulnérabilité générale.

Dans un déploiement à deux cartes réseau, vous pouvez introduire des systèmes d'infrastructure supplémentaires, tels que des serveurs DNS, des serveurs RSA SecurID Authentication Manager sur le réseau principal au sein de la zone DMZ de façon que ces serveurs ne soient pas visibles sur le réseau Internet. L'introduction de systèmes d'infrastructure au sein de la DMZ protège contre les attaques de couche 2 à partir du LAN Internet en cas de compromission du système frontal et limite efficacement la surface d'attaque générale.

La plupart du trafic réseau Unified Access Gateway concerne les protocoles d'affichage pour Blast et PCoIP. Avec une carte réseau unique, le trafic des protocoles d'affichage en direction et en provenance d'Internet est combiné au trafic en direction et en provenance des systèmes principaux. Lorsque deux ou plusieurs cartes réseau sont utilisées, le trafic est réparti sur l'ensemble des cartes réseaux et des réseaux frontaux et principaux. Cela limite le risque de goulots d'étranglement inhérent à une carte réseau unique et apporte des avantages en matière de performances.

Unified Access Gateway prend en charge une séparation supplémentaire en autorisant également la séparation du trafic de gestion sur un LAN de gestion spécifique. Le trafic de gestion HTTPS sur le port 9443 est alors uniquement possible à partir du LAN de gestion.

Figure 1-5. Option à trois cartes réseau d' Unified Access Gateway



Mettre à niveau sans interruption

Les mises à niveau sans interruption vous permettent de mettre Unified Access Gateway à niveau sans interruption pour les utilisateurs. Avant de mettre à niveau un dispositif Unified Access Gateway, le mode de mise au repos dans les pages de configuration système Unified Access Gateway passe de NON à OUI.

Lorsque la valeur du mode de mise au repos est OUI, le dispositif Unified Access Gateway apparaît comme étant non disponible lorsque l'équilibrage de charge contrôle la santé du dispositif. Les demandes qui parviennent à l'équilibrage de charge sont envoyées au dispositif Unified Access Gateway suivant qui se trouve derrière l'équilibrage de charge.

Prérequis

- Deux dispositifs Unified Access Gateway ou plus configurés derrière l'équilibrage de charge
- Paramètre URL de contrôle de santé configuré avec une URL à laquelle se connecte l'équilibrage de charge pour contrôler la santé du dispositif Unified Access Gateway
- Contrôlez la santé du dispositif dans l'équilibrage de charge. Tapez la commande API REST GET `https://mycoUnifiedAccessGateway.com:443/favicon.ico`.

La réponse est HTTP/1.1 200 OK, si le mode de mise au repos est défini sur Non, ou HTTP/1.1 503, si le mode de mise au repos est défini sur Oui.

Procédure

- 1 Dans la section Configuration manuelle de l'interface utilisateur d'administration, cliquez sur **Sélectionner**.
- 2 Dans la section Paramètres avancés, cliquez sur l'icône en forme d'engrenage **Configuration du système**.
- 3 Dans la ligne **Mode de mise au repos**, activez **OUI** pour suspendre le dispositif Unified Access Gateway.

Lorsque le dispositif est arrêté, les sessions existantes que le dispositif sert sont honorées pendant 10 heures, après quoi elles sont fermées.
- 4 Cliquez sur **Enregistrer**.

Les nouvelles demandes qui parviennent à l'équilibrage de charge sont envoyées au dispositif Unified Access Gateway suivant.

Suivant

Exportez les paramètres depuis le dispositif Unified Access Gateway suspendu. Déployez une nouvelle version d'Unified Access Gateway et importez les paramètres. La nouvelle version du dispositif Unified Access Gateway peut être ajoutée à l'équilibrage de charge.

Déploiement du dispositif Unified Access Gateway

2

Unified Access Gateway se présente sous la forme d'un fichier OVF et est déployé sur un hôte vSphere ESX ou ESXi en tant que dispositif virtuel préconfiguré.

Deux méthodes principales peuvent être utilisées pour installer le dispositif Unified Access Gateway sur un hôte vSphere ESX ou ESXi. Les rôles Microsoft Server 2012 et 2016 Hyper-V sont pris en charge.

- vSphere Client ou vSphere Web Client peuvent être utilisés pour déployer le modèle OVF Unified Access Gateway. Vous êtes invité à fournir les paramètres de base, y compris la configuration du déploiement de carte réseau, l'adresse IP et les mots de passe de l'interface de gestion. Une fois l'OVF déployé, connectez-vous à l'interface utilisateur d'administration d'Unified Access Gateway pour configurer les paramètres système d'Unified Access Gateway, configurer des services Edge sécurisés dans plusieurs cas d'utilisation et configurer l'authentification dans la DMZ. Reportez-vous à la section [« Déploiement d'Unified Access Gateway au moyen de l'assistant de modèle OVF »](#), page 20.
- Les scripts PowerShell peuvent être utilisés pour déployer Unified Access Gateway et configurer des services Edge sécurisés dans plusieurs cas d'utilisation. Téléchargez le fichier zip, configurez le script PowerShell pour votre environnement et exécutez le script pour déployer Unified Access Gateway. Reportez-vous à la section [« Utilisation de PowerShell pour déployer le dispositif Unified Access Gateway »](#), page 28.

REMARQUE Pour les cas d'utilisation de proxy et de tunnel par application AirWatch, vous pouvez déployer Unified Access Gateway dans des environnements ESXi ou Microsoft Hyper-V.

Ce chapitre aborde les rubriques suivantes :

- [« Utilisation de l'assistant de modèle OVF pour déployer Unified Access Gateway »](#), page 19
- [« Configuration d'Unified Access Gateway à partir des pages de configuration d'administration »](#), page 24
- [« Mise à jour des certificats signés du serveur SSL »](#), page 26

Utilisation de l'assistant de modèle OVF pour déployer Unified Access Gateway

Pour déployer Unified Access Gateway, déployez le modèle OVF à l'aide de vSphere Client ou vSphere Web Client, mettez le dispositif sous tension et configurez les paramètres.

Lorsque vous déployez OVF, vous configurez le nombre d'interfaces réseau nécessaires, et vous définissez l'adresse IP, ainsi que les mots de passe de l'administrateur et racine.

Une fois Unified Access Gateway déployé, allez dans l'interface utilisateur d'administration pour configurer l'environnement d'Unified Access Gateway. Dans l'interface utilisateur d'administration, configurez les ressources de poste de travail et d'application et les méthodes d'authentification à utiliser dans la zone DMZ. Pour vous connecter aux pages de l'interface utilisateur d'administration, accédez à <https://<mycoUnifiedGatewayAppliance>.com:9443/admin/index.html>.

Déploiement d' Unified Access Gateway au moyen de l'assistant de modèle OVF

Vous pouvez déployer le dispositif Unified Access Gateway en ouvrant une session sur vCenter Server et en utilisant l'assistant Déployer le modèle OVF.

Deux versions du fichier OVA d'Unified Access Gateway sont disponibles, OVA standard et une version FIPS de l'OVA. La version FIPS 140-2 s'exécute avec le jeu de chiffrements et de hachages certifié par FIPS et elle dispose de services restrictifs activés qui prennent en charge des bibliothèques certifiées par FIPS. Lorsqu'Unified Access Gateway est déployé en mode FIPS, le dispositif ne peut pas être passé en mode de déploiement OVA standard.

REMARQUE Si vous utilisez vSphere Client natif, vérifiez que vous avez affecté un pool IP à chaque réseau. Pour ajouter un pool IP dans vCenter Server au moyen du vSphere Client natif, accédez à l'onglet Pools IP du centre de données. Si vous utilisez vSphere Web Client, vous pouvez également créer un profil de protocole réseau. Accédez à l'onglet Gérer du centre de données et sélectionnez l'onglet Profils de protocole réseau.

Prérequis

- Examinez les options de déploiement qui sont disponibles dans l'assistant. Reportez-vous à la section « [Configuration requise pour le système et le réseau Unified Access Gateway](#) », page 8.
- Déterminez le nombre d'interfaces réseau et d'adresses IP statiques à configurer pour le dispositif Unified Access Gateway. Reportez-vous à la section « [Configuration requise pour le réseau](#) », page 10.
- Téléchargez le fichier de programme d'installation .ova pour le dispositif Unified Access Gateway sur le site Web VMware à l'adresse <https://my.vmware.com/web/vmware/downloads> ou déterminez l'URL à utiliser (exemple : http://example.com/vapps/euc-access-point-Y.Y.0.0-xxxxxxx_OVF10.ova), où Y.Y est le numéro de version et xxxxxx le numéro de build.

Procédure

- 1 Utilisez le vSphere Client natif ou vSphere Web Client pour ouvrir une session sur une instance de vCenter Server.

Pour un réseau IPv4, utilisez l'instance native de vSphere Client ou vSphere Web Client. Pour un réseau IPv6, utilisez vSphere Web Client.

- 2 Sélectionnez une commande de menu pour lancer l'assistant **Déployer le modèle OVF**.

Option	Commande de menu
vSphere Client	Sélectionnez Fichier > Déployer le modèle OVF .
vSphere Web Client	Sélectionnez un objet d'inventaire qui est un objet parent valide d'une machine virtuelle, tel qu'un centre de données, un dossier, un cluster, un pool de ressources ou un hôte et, dans le menu Actions , sélectionnez Déployer le modèle OVF .

- 3 Sur la page Sélectionner la source, accédez au fichier .ova que vous avez téléchargé ou entrez une URL et cliquez sur **Suivant**.

Examinez les détails du produit, la version et les exigences de taille.

- 4 Suivez les invites de l'assistant en tenant compte des conseils suivants.

Option	Description
Nom et emplacement	Saisissez un nom pour le dispositif virtuel Unified Access Gateway. Il doit être unique dans le dossier de l'inventaire. Les noms sont sensibles à la casse. Sélectionnez un emplacement pour le dispositif virtuel.
Configuration de déploiement	Pour un réseau IPv4, vous pouvez utiliser une, deux ou trois interfaces réseau (cartes réseau). Pour un réseau IPv6, utilisez trois cartes réseau. Unified Access Gateway requiert une adresse IP statique séparée pour chaque carte réseau. De nombreuses implémentations de zone DMZ utilisent des réseaux distincts pour sécuriser les différents types de trafic. Configurez Unified Access Gateway en fonction de la conception de réseau de la zone DMZ dans laquelle il est déployé.
Hôte/Cluster	Sélectionnez l'hôte ou le cluster sur lequel exécuter le dispositif virtuel.
Format de disque	Pour les environnements d'évaluation et de test, sélectionnez le format Provisionnement fin. Pour les environnements de production, sélectionnez l'un des formats Provisionnement statique. Provisionnement statique immédiatement mis à zéro est un type de format de disque virtuel statique qui prend en charge les fonctionnalités de cluster, telles que la tolérance aux pannes, mais qui prend beaucoup plus de temps pour créer d'autres types de disques virtuels.

Option	Description
Configuration des réseaux/Mappage réseau	<p>Si vous utilisez vSphere Web Client, la page Configuration des réseaux vous permet de mapper chaque carte réseau vers un réseau et de spécifier des paramètres de protocole.</p> <p>Mappez les réseaux utilisés dans ce modèle OVF aux réseaux de votre inventaire.</p> <ol style="list-style-type: none"> Sélectionnez IPv4 ou IPv6 dans la liste déroulante Protocole IP. Sélectionnez la première ligne du tableau Internet et cliquez sur la flèche vers le bas pour sélectionner le réseau de destination. Si vous sélectionnez IPv6 comme protocole IP, vous devez sélectionner le réseau avec des capacités IPv6. <p>Après avoir sélectionné la ligne, vous pouvez également entrer des adresses IP pour le serveur DNS, la passerelle et le masque de réseau dans la partie inférieure de la fenêtre.</p> <ol style="list-style-type: none"> Si vous utilisez plusieurs cartes réseau, sélectionnez la ligne suivante ManagementNetwork, sélectionnez le réseau de destination ; vous pouvez ensuite entrer les adresses IP pour le serveur DNS, la passerelle et le masque de réseau pour ce réseau. <p>Si vous n'utilisez qu'une seule carte réseau, toutes les lignes sont mappées vers le même réseau.</p> <ol style="list-style-type: none"> Si vous avez une troisième carte réseau, sélectionnez également la troisième ligne et remplissez les paramètres. <p>Si vous n'utilisez que deux cartes réseau, pour cette troisième ligne BackendNetwork, sélectionnez le réseau que vous avez utilisé pour ManagementNetwork.</p> <p>Avec vSphere Web Client, s'il n'existe pas encore de profil de protocole réseau, il est automatiquement créé lorsque l'assistant est terminé.</p> <p>Si vous utilisez le vSphere Client natif, la page Mappage réseau vous permet de mapper chaque carte réseau à un réseau, mais il n'y a pas de champ pour spécifier les adresses du serveur DNS, de la passerelle et du masque de réseau. Comme décrit dans les conditions préalables, vous devez déjà avoir attribué un pool IP à chaque réseau ou avoir créé un profil de protocole réseau.</p>
Personnaliser les propriétés réseau	<p>Les cases sur la page Propriétés sont spécifiques à Unified Access Gateway et il est probable qu'elles ne soient pas requises pour d'autres types de dispositifs virtuels. Le texte sur la page de l'assistant explique chaque paramètre. Si le texte est tronqué sur le côté droit de l'assistant, redimensionnez la fenêtre en faisant glisser le curseur à partir de l'angle inférieur droit.</p> <ul style="list-style-type: none"> ■ IPMode:STATICV4/STATICV6. Si vous entrez STATICV4, vous devez entrer l'adresse IPv4 de la carte réseau. Si vous entrez STATICV6, vous devez entrer l'adresse IPv6 de la carte réseau. ■ Liste de règles de transfert séparées par une virgule au format {tcp udp}/listening-port-number/destination-ip-address:destination-port-number ■ Adresse IPv4 de la carte réseau 1 (ETH0). Entrez l'adresse IPv4 de la carte réseau si vous avez entré STATICV4 pour le mode de carte réseau. ■ Liste d'itinéraires personnalisés IPv4 séparés par une virgule pour la carte réseau 1 (eth0) au format ipv4-network-address/bits.ipv4-gateway-address ■ Adresse IPv6 de la carte réseau 1 (eth0). Entrez l'adresse IPv6 de la carte réseau si vous avez entré STATICV6 pour le mode de carte réseau. ■ Adresses de serveur DNS. Entrez les adresses IPv4 ou IPv6, séparées par des espaces, des serveurs de nom de domaine du dispositif Unified Access Gateway. Exemple d'entrée IPv4 : 192.0.2.1 192.0.2.2. Exemple d'entrée IPv6 : fc00:10:112:54::1

Option	Description
	<ul style="list-style-type: none"> ■ Passerelle par défaut Entrez une valeur par défaut définie par les profils de protocole réseau vSphere (Remarque : entrez une valeur de passerelle par défaut uniquement si le mode IP est STATICV4/STATICV6). ■ Adresse IPv4 de la carte réseau 2 (eth1). Entrez l'adresse IPv4 de la carte réseau si vous avez entré STATICV4 pour le mode de carte réseau. ■ Liste d'itinéraires personnalisés IPv4 séparés par une virgule pour la carte réseau 2 (eth1) au format ipv4-network-address/bits.ipv4-gateway-address ■ Adresse IPv6 de la carte réseau 2 (eth1). Entrez l'adresse IPv6 de la carte réseau si vous avez entré STATICV6 pour le mode de carte réseau. ■ Adresse IPv4 de la carte réseau 3 (eth2). Entrez l'adresse IPv4 de la carte réseau si vous avez entré STATICV4 pour le mode de carte réseau. ■ Liste d'itinéraires personnalisés IPv4 séparés par une virgule pour la carte réseau 3 (eth2) au format ipv4-network-address/bits.ipv4-gateway-address ■ Adresse IPv6 de la carte réseau 3 (eth2). Entrez l'adresse IPv6 de la carte réseau si vous avez entré STATICV6 pour le mode de carte réseau. ■ Options de mot de passe. Entrez le mot de passe de l'utilisateur racine de cette VM et le mot de passe de l'administrateur qui accède à la console d'administration et qui active l'accès à l'API REST. ■ Options de mot de passe. Entrez le mot de passe de l'administrateur qui se connecte à l'interface utilisateur d'administration pour configurer Unified Access Gateway et qui peut activer l'accès à l'API REST.
	Les autres paramètres sont facultatifs ou ont déjà un paramètre par défaut.

- 5 Sur la page Prêt à terminer, sélectionnez **Mettre sous tension après le déploiement** et cliquez sur **Terminer**.

Une tâche Déployer le modèle OVF apparaît dans la zone d'état de vCenter Server pour que vous puissiez contrôler le déploiement. Vous pouvez également ouvrir une console sur la machine virtuelle pour afficher les messages de console qui sont affichés lors du démarrage du système. Un journal de ces messages est également disponible dans le fichier `/var/log/boot.msg`.

- 6 Lorsque le déploiement est terminé, vérifiez que les utilisateurs finaux peuvent se connecter au dispositif en ouvrant un navigateur et en entrant l'URL suivante :

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

Dans cette URL, *FQDN-of-UAG-appliance* est le nom de domaine complet pouvant être résolu par DNS du dispositif Unified Access Gateway.

En cas de réussite du déploiement, la page Web fournie par le serveur vers laquelle pointe Unified Access Gateways'affiche. Si le déploiement échoue, vous pouvez supprimer la machine virtuelle de dispositif et déployer de nouveau le dispositif. L'erreur la plus courante est l'entrée erronée des empreintes numériques de certificat.

Le dispositif Unified Access Gateway est déployé et démarre automatiquement.

Suivant

Connectez-vous à l'interface utilisateur d'administration d'Unified Access Gateway et configurez les ressources de poste de travail et d'application pour permettre un accès distant à partir d'Internet par le biais d'Unified Access Gateway et les méthodes d'authentification à utiliser dans la zone DMZ. L'URL de la console d'administration présente le format `https://<myco>Unified Access Gatewayappliance.com:9443/admin/index.html`.

REMARQUE Si vous ne pouvez pas accéder à l'écran de connexion de l'interface utilisateur d'administration, vérifiez si l'adresse IP de la machine virtuelle est affichée lors de l'installation du fichier OVA. Si l'adresse IP n'est pas configurée, utilisez la commande vami mentionnée dans l'interface utilisateur pour reconfigurer les cartes réseau. Exécutez la commande `cd /opt/vmware/share/vami`, puis la commande `./vami_config_net`.

Configuration d' Unified Access Gateway à partir des pages de configuration d'administration

Après le déploiement de l'OVF et la mise sous tension du dispositif Unified Access Gateway, connectez-vous à l'interface utilisateur d'administration d'Unified Access Gateway afin de configurer les paramètres.

Les pages Paramètres généraux et Paramètres avancés incluent ce qui suit.

- Configuration système d'Unified Access Gateway et certificat de serveur SSL
- Paramètres du service Edge pour Horizon, proxy inverse et VMware Tunnel
- Paramètres d'authentification pour RSA SecurID, RADIUS, certificat X.509 et RSA Adaptive Authentication
- Paramètres du fournisseur d'identité SAML et du fournisseur de services
- Configuration des paramètres de pontage d'identité

Les options suivantes sont accessibles à partir des pages Paramètres de prise en charge.

- Télécharger des fichiers zip de journal d'Unified Access Gateway
- Exporter les paramètres d'Unified Access Gateway pour récupérer les paramètres de configuration
- Définir les paramètres de niveau de journal
- Importer les paramètres d'Unified Access Gateway pour créer et mettre à jour une configuration Unified Access Gateway complète

Configurer les paramètres système d' Unified Access Gateway

Vous pouvez configurer les protocoles de sécurité et les algorithmes cryptographiques qui sont utilisés pour chiffrer les communications entre les clients et le dispositif Unified Access Gateway à partir des pages de configuration d'administration.

Prérequis

- Passez en revue les propriétés de déploiement Unified Access Gateway. Les informations de paramétrage suivantes sont requises :
 - Adresse IP statique pour le dispositif Unified Access Gateway
 - Adresse IP du serveur DNS
 - Mot de passe pour la console d'administration
 - URL de l'instance de serveur ou de l'équilibrage de charge vers laquelle le dispositif Unified Access Gateway pointe.

- URL du serveur Syslog permettant d'enregistrer les fichiers journaux des événements

Procédure

- 1 Dans la section Configuration manuelle de l'interface utilisateur d'administration, cliquez sur **Sélectionner**.
- 2 Dans la section Paramètres avancés, cliquez sur l'icône en forme d'engrenage **Configuration du système**.
- 3 Modifiez les valeurs suivantes de configuration du dispositif Unified Access Gateway.

Option	Valeur par défaut et description
Paramètre régional	Spécifie le paramètre régional à utiliser pour générer les messages d'erreur. <ul style="list-style-type: none"> ■ en_US pour l'anglais ■ ja_JP pour le japonais ■ fr_FR pour le français ■ de_DE pour l'allemand ■ zh_CN pour le chinois simplifié ■ zh_TW pour le chinois traditionnel ■ ko_KR pour le coréen
Mot de passe Admin	Ce mot de passe a été défini lorsque vous avez déployé le dispositif. Vous pouvez le réinitialiser. Les mots de passe doivent contenir au moins 8 caractères, au moins une majuscule et une minuscule, un chiffre et un caractère spécial, qui inclut ! @ # \$ % * ().
Suites de chiffrement	Dans la plupart des cas, les paramètres par défaut ne doivent pas être modifiés. Il s'agit des algorithmes cryptographiques qui sont utilisés pour chiffrer les communications entre les clients et le dispositif Unified Access Gateway. Les paramètres de chiffement permettent d'activer différents protocoles de sécurité.
Respecter l'ordre de chiffement	La valeur par défaut est NO. Sélectionnez YES pour activer le contrôle d'ordre de liste de chiffement TLS.
SSL 3.0 activé	La valeur par défaut est NO. Sélectionnez YES pour activer le protocole de sécurité SSL 3.0.
TLS 1.0 activé	La valeur par défaut est NO. Sélectionnez YES pour activer le protocole de sécurité TLS 1.0.
TLS 1.1 activé	La valeur par défaut est YES. Le protocole de sécurité TLS 1.1 est activé.
TLS 1.2 activé	La valeur par défaut est YES. Le protocole de sécurité TLS 1.2 est activé.
URL Syslog	Entrez l'URL du serveur Syslog qui est utilisée pour la journalisation des événements Unified Access Gateway. Cette valeur peut être une URL, un nom d'hôte ou une adresse IP. Si vous ne définissez pas l'URL du serveur Syslog, aucun événement n'est journalisé. Utilisez le format <code>syslog://server.example.com:514</code> .
URL de contrôle de santé	Entrez une URL à laquelle l'équilibrage de charge se connecte et vérifie la santé d'Unified Access Gateway.
Cookies à mettre en cache	Ensemble de cookies mis en cache par Unified Access Gateway. La valeur par défaut est aucun.
Mode IP	Sélectionnez le mode IP statique : STATICV4 ou STATICV6.
Délai d'expiration de session	La valeur par défaut est de 36 000 000 millisecondes.
Mode de mise au repos	Choisissez YES pour mettre en pause le dispositif Unified Access Gateway afin d'obtenir un état cohérent permettant d'effectuer les tâches de maintenance.
Surveiller l'intervalle	La valeur par défaut est 60.

- 4 Cliquez sur **Enregistrer**.

Suivant

Configurez les paramètres du service Edge pour les composants avec lesquels Unified Access Gateway est déployé. Une fois les paramètres Edge configurés, configurez les paramètres d'authentification.

Mise à jour des certificats signés du serveur SSL

Vous pouvez remplacer vos certificats signés lorsqu'ils arrivent à échéance.

Pour les environnements de production, VMware vous recommande de remplacer le certificat par défaut dès que possible. Le certificat de serveur TLS/SSL par défaut qui est généré lorsque vous déployez un dispositif Unified Access Gateway n'est pas signé par une autorité de certification approuvée.

Prérequis

- Nouveau certificat signé et nouvelle clé privée enregistrés sur un ordinateur auquel vous avez accès.
- Convertissez le certificat en fichiers au format PEM et convertissez les fichiers .pem au format sur une seule ligne. Voir [Convertir des fichiers de certificat au format PEM sur une ligne](#)

Procédure

- 1 Dans la console d'administration, cliquez sur **Sélectionner**.
- 2 Dans la section Paramètres avancés, cliquez sur l'icône en forme d'engrenage Paramètres de certificat du serveur SSL.
- 3 Sélectionnez le type de certificat **PEM** ou **PFX**.
- 4 Si le type de certificat est **PEM** :
 - a Dans la ligne Clé privée, cliquez sur **Sélectionner** et accédez au fichier de clé privée.
 - b Cliquez sur **Ouvrir** pour télécharger le fichier.
 - c Dans la ligne Chaîne de certificats, cliquez sur **Sélectionner** et accédez au fichier de chaîne de certificats.
 - d Cliquez sur **Ouvrir** pour télécharger le fichier.
- 5 Si le type de certificat est **PFX** :
 - a Dans la ligne Télécharger PFX, cliquez sur **Sélectionner** et accédez au fichier pfx.
 - b Cliquez sur **Ouvrir** pour télécharger le fichier.
 - c Entrez le mot de passe du certificat PFX.
 - d Entrez l'alias du certificat PFX. Cette fonction est utilisée lorsque plusieurs certificats sont présents dans le magasin de certificats.
- 6 Cliquez sur **Enregistrer**.

Suivant

Si l'autorité de certification qui a signé le certificat n'est pas reconnue, configurez les clients pour qu'ils approuvent les certificats racine et intermédiaires.

Utilisation de PowerShell pour déployer Unified Access Gateway

3

Un script PowerShell peut être utilisé pour déployer Unified Access Gateway. Le script PowerShell est fourni à titre d'exemple et vous pouvez le modifier en fonction de vos besoins spécifiques en matière d'environnement.

Lorsque vous utilisez le script PowerShell pour déployer Unified Access Gateway, le script appelle la commande OVF Tool et valide les paramètres pour créer automatiquement la syntaxe de ligne de commande correcte. Cette méthode permet également de définir des paramètres avancés, tels que la configuration du certificat de serveur TLS/SSL à appliquer au moment du déploiement.

Ce chapitre aborde les rubriques suivantes :

- « Configuration système requise pour déployer Unified Access Gateway à l'aide de PowerShell », page 27
- « Utilisation de PowerShell pour déployer le dispositif Unified Access Gateway », page 28

Configuration système requise pour déployer Unified Access Gateway à l'aide de PowerShell

Pour déployer Unified Access Gateway à l'aide d'un script PowerShell, vous devez utiliser des versions spécifiques de produits VMware.

- Hôte vSphere ESX avec vCenter Server.
- Le script PowerShell s'exécute sur des machines Windows 8.1 ou version ultérieure ou sur Windows Server 2008 R2 ou version ultérieure.

La machine peut également être un serveur vCenter Server exécuté sur Windows ou une machine Windows séparée.

- La commande VMware OVF Tool doit être installée sur la machine Windows exécutant le script.

Vous devez installer OVF Tool 4.0.1 ou version ultérieure à partir de <https://www.vmware.com/support/developer/ovf/>.

Vous devez sélectionner la banque de données vSphere et le réseau à utiliser.

Un profil de protocole de réseau vSphere doit être associé à chaque nom de réseau référencé. Ce profil de protocole réseau spécifie des paramètres de réseau, tels que le masque de sous-réseau IPv4, la passerelle, etc. Le déploiement d'Unified Access Gateway utilise ces valeurs pour s'assurer qu'elles sont correctes.

Utilisation de PowerShell pour déployer le dispositif Unified Access Gateway

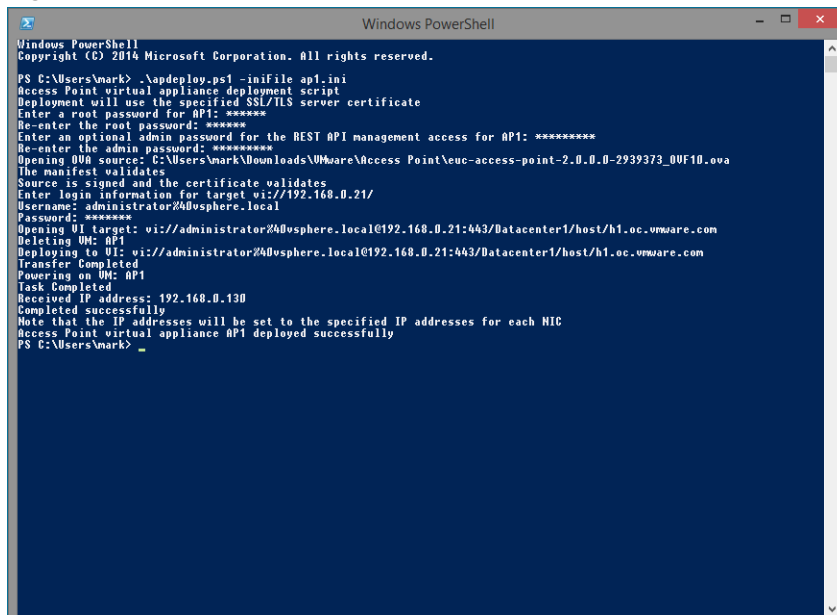
Les scripts PowerShell préparent votre environnement avec tous les paramètres de configuration. Lorsque vous exécutez le script PowerShell pour déployer Unified Access Gateway, la solution est prête pour la production lors du premier démarrage système.

Prérequis

- Vérifiez que la configuration système requise est appropriée et disponible.

Il s'agit d'un exemple de script pour déployer Unified Access Gateway dans votre environnement.

Figure 3-1. Exemple de script PowerShell



```

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

PS C:\Users\mark> .\apdeploy.ps1 -inifile ap1.ini
Access Point virtual appliance deployment script
Deployment will use the specified SSL/TLS server certificate
Enter a root password for AP1: *****
Re-enter the root password: *****
Enter an optional admin password for the REST API management access for AP1: *****
Re-enter the admin password: *****
Opening OVA source: C:\Users\mark\Downloads\VMware\Access Point\uc-access-point-2.0.0.0-2939373_0UF10.ova
The manifest validates
Source is signed and the certificate validates
Enter login information for target vi://192.168.0.21/
Username: administrator@bosphere.local
Password: *****
Opening UI target: vi://administrator@bosphere.local@192.168.0.21:443/Datacenter1/host/h1.oc.vmware.com
Deleting VM: AP1
Deploying to UI: vi://administrator@bosphere.local@192.168.0.21:443/Datacenter1/host/h1.oc.vmware.com
Transfer Completed
Powering on VM: AP1
Task Completed
Received IP address: 192.168.0.130
Completed successfully
Note that the IP addresses will be set to the specified IP addresses for each NIC
Access Point virtual appliance AP1 deployed successfully
PS C:\Users\mark>
  
```

Procédure

- 1 Téléchargez le fichier OVA Unified Access Gateway à partir de My VMware sur votre ordinateur Windows.
- 2 Téléchargez les fichiers ap-deploy-XXX.zip dans un dossier sur la machine Windows.

Les fichiers compressés sont disponibles à l'adresse <https://communities.vmware.com/docs/DOC-30835>.

- 3 Ouvrez un script PowerShell et modifiez le répertoire vers l'emplacement de votre script.
- 4 Créez un fichier de configuration .INI pour le dispositif virtuel Unified Access Gateway.

Par exemple : déployez un nouveau dispositif Unified Access Gateway AP1. Le fichier de configuration s'appelle ap1.ini. Ce fichier contient tous les paramètres de configuration pour AP1. Vous pouvez utiliser les fichiers .INI fournis en exemple dans le fichier .ZIP apdeploy pour créer le fichier .INI et modifier les paramètres en conséquence.

REMARQUE Vous pouvez disposer de fichiers .INI uniques pour plusieurs déploiements d'Unified Access Gateway dans votre environnement. Vous devez modifier les adresses IP et les paramètres de nom dans le fichier .INI de façon appropriée pour déployer plusieurs dispositifs.

Exemple de fichier .INI à modifier.

```
name=AP1
source=C:\APs\auc-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 Pour vérifier la réussite de l'exécution du script, tapez la commande PowerShell `set-executionpolicy`.
`set-executionpolicy -scope currentuser unrestricted`

Vous devez exécuter cette commande une seule fois si elle est actuellement limitée.

S'il existe un avertissement pour le script, exécutez la commande pour débloquer l'avertissement :

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

- 6 Exécutez la commande pour démarrer le déploiement. Si vous ne spécifiez pas le fichier .INI, le script est défini par défaut sur `ap.ini`.
`.\apdeploy.ps1 -iniFile ap1.ini`
- 7 Entrez les informations d'identification lorsque vous y êtes invité et terminez le script.

REMARQUE Si vous êtes invité à ajouter l'empreinte numérique de la machine cible, entrez **yes**.

Le dispositif Unified Access Gateway est déployé et disponible pour la production.

Pour plus d'informations sur les scripts PowerShell, consultez

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

Cas d'utilisation de déploiement d'Unified Access Gateway

4

Les scénarios de déploiement décrits dans ce chapitre peuvent vous aider à identifier et à organiser le déploiement d'Unified Access Gateway dans votre environnement.

Vous pouvez déployer Unified Access Gateway avec Horizon View, Horizon Cloud avec infrastructure sur site, VMware Identity Manager et VMware AirWatch.

Ce chapitre aborde les rubriques suivantes :

- [« Déploiement avec Horizon View et Horizon Cloud avec infrastructure sur site », page 31](#)
- [« Déploiement en tant que proxy inverse », page 38](#)
- [« Déploiement pour l'accès avec Single Sign-On à des applications Web héritées sur site », page 43](#)
- [« Tunnel VMware sur Unified Access Gateway », page 51](#)

Déploiement avec Horizon View et Horizon Cloud avec infrastructure sur site

Vous pouvez déployer Unified Access Gateway avec Horizon View et Horizon Cloud avec infrastructure sur site. Pour le composant View de VMware Horizon, les dispositifs Unified Access Gateway jouent le même rôle que celui précédemment joué par les serveurs de sécurité View.

Scénario de déploiement

Unified Access Gateway fournit un accès distant sécurisé à des applications et des postes de travail virtuels sur site dans un centre de données de client. Cela fonctionne avec un déploiement sur site d'Horizon View ou Horizon Cloud pour une gestion unifiée.

Unified Access Gateway garantit à l'entreprise l'identité de l'utilisateur et il contrôle précisément l'accès à ses applications et postes de travail autorisés.

En général, les dispositifs virtuels Unified Access Gateway sont déployés dans une zone démilitarisée (DMZ) de réseau. Le déploiement dans la DMZ permet de s'assurer que l'ensemble du trafic entrant dans le centre de données à destination des ressources de poste de travail et d'application s'effectue pour le compte d'un utilisateur fortement authentifié. Les dispositifs virtuels Unified Access Gateway garantissent également que le trafic d'un utilisateur authentifié ne puisse être dirigé que vers des ressources de poste de travail et d'application auxquelles l'utilisateur est autorisé à accéder. Ce niveau de protection implique une inspection spécifique des protocoles de poste de travail et une coordination des stratégies et des adresses réseau susceptibles de changer rapidement pour pouvoir contrôler l'accès de façon précise.

Vous devez vérifier les exigences pour un déploiement transparent d'Unified Access Gateway avec Horizon.

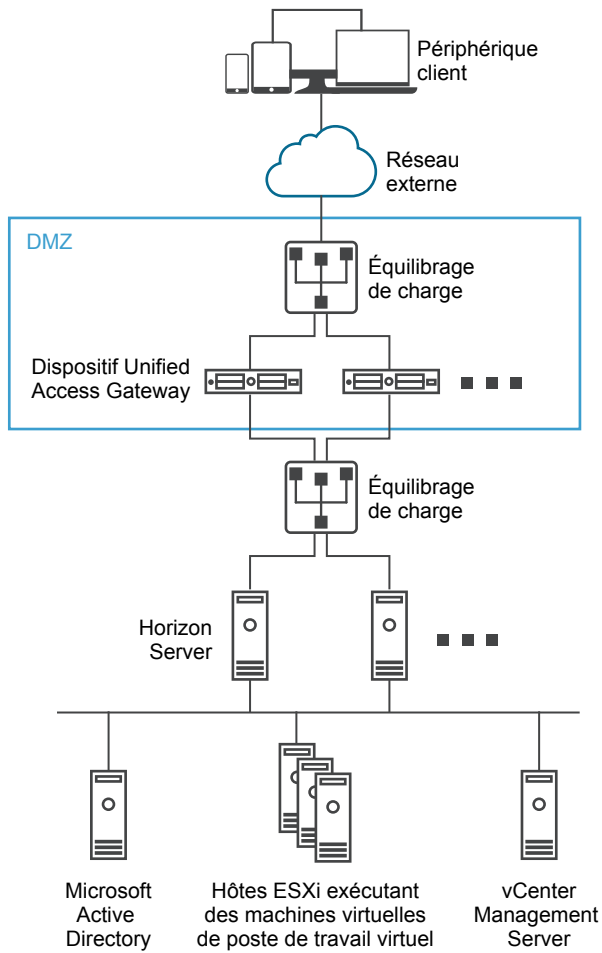
- Si le dispositif Unified Access Gateway pointe vers un équilibrage de charge devant les serveurs Horizon Server, la sélection de l'instance du serveur est dynamique.

- Unified Access Gateway remplace le serveur de sécurité Horizon.
- Par défaut, le port 8443 doit être disponible pour Blast TCP/UDP. Toutefois, le port 443 peut également être configuré pour Blast TCP/UDP.
- Blast Secure Gateway et PCoIP Secure Gateway doivent être activés lorsqu'Unified Access Gateway est déployé avec Horizon. Cela garantit que les protocoles d'affichage peuvent servir de proxy automatiquement via Unified Access Gateway. Les paramètres BlastExternalURL et pcoipExternalURL spécifient des adresses de connexion utilisées par les instances d'Horizon Client pour acheminer ces connexions de protocole d'affichage via les passerelles appropriées sur Unified Access Gateway. Cela améliore la sécurité, car ces passerelles garantissent que le trafic du protocole d'affichage est contrôlé pour le compte d'un utilisateur authentifié. Le trafic de protocole d'affichage non autorisé est ignoré par Unified Access Gateway.
- Désactivez les passerelles sécurisées (Blast Secure Gateway et PCoIP Secure Gateway) sur les instances Serveur de connexion View et activez ces passerelles sur les dispositifs Unified Access Gateway.

La principale différence par rapport au serveur de sécurité View réside dans le fait qu'Unified Access Gateway offre les avantages suivants.

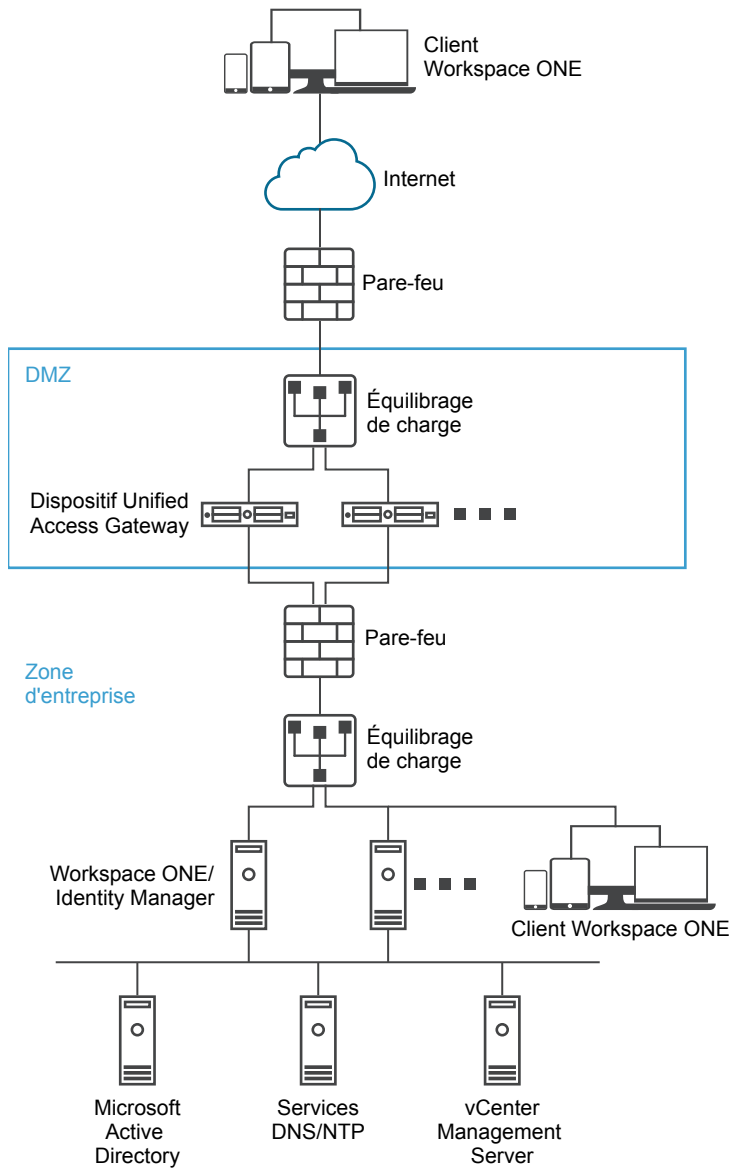
- Déploiement sécurisé. Unified Access Gateway est implémenté en tant que machine virtuelle basée sur Linux, préconfigurée, verrouillée et à sécurité renforcée.
- Évolutivité. Vous pouvez connecter Unified Access Gateway à un Serveur de connexion View individuel ou via un équilibrage de charge devant plusieurs Serveurs de connexion View, ce qui améliore la haute disponibilité. Il fait office de couche entre les instances d'Horizon Client et les Serveurs de connexion View principaux. Dans la mesure où le déploiement est rapide, il peut rapidement être mis à l'échelle vers le haut ou vers le bas pour répondre aux exigences des entreprises à évolution rapide.

Figure 4-1. Dispositif Unified Access Gateway pointant vers un équilibrage de charge



Vous pouvez également diriger un ou plusieurs dispositifs Unified Access Gateway vers une instance de serveur individuelle. Avec les deux approches, utilisez un équilibrage de charge devant deux dispositifs Unified Access Gateway ou plus dans la zone DMZ.

Figure 4-2. Dispositif Unified Access Gateway pointant vers une instance d'Horizon Server



Authentification

L'authentification utilisateur est semblable au serveur de sécurité View. Voici les méthodes d'authentification utilisateur prises en charge dans Unified Access Gateway :

- Nom d'utilisateur et mot de passe Active Directory
- Mode kiosque. Pour plus d'informations sur le mode kiosque, consultez la documentation d'Horizon.
- Authentification à deux facteurs SecurID, certifiée formellement par RSA pour SecurID
- RADIUS via diverses solutions de fournisseurs de sécurité à deux facteurs tiers
- Carte à puce, CAC ou certificats utilisateur PIV X.509
- SAML

Ces méthodes d'authentification sont prises en charge avec le Serveur de connexion View. Unified Access Gateway n'a pas besoin de communiquer directement avec Active Directory. Cette communication sert de proxy via le Serveur de connexion View, qui peut accéder directement à Active Directory. Une fois que la session utilisateur est authentifiée selon la stratégie d'authentification, Unified Access Gateway peut transmettre des demandes d'informations de droit, ainsi que des demandes de lancement de poste de travail et d'application, au Serveur de connexion View. Unified Access Gateway gère également ses gestionnaires de protocole de poste de travail et d'application pour leur permettre de ne transmettre que le trafic de protocole autorisé.

Unified Access Gateway gère lui-même l'authentification par carte à puce. Cela inclut des options pour qu'Unified Access Gateway puisse communiquer avec des serveurs OCSP (Online Certificate Status Protocol) afin de vérifier la révocation des certificats X.509, etc.

Configuration des paramètres Horizon

Vous pouvez déployer Unified Access Gateway à partir d'Horizon View et Horizon Cloud with On-Premises Infrastructure. Pour le composant View de VMware Horizon, le dispositif Unified Access Gateway joue le même rôle que celui précédemment joué par le serveur de sécurité View.

Procédure

- 1 Dans la section Configuration manuelle de l'interface utilisateur d'administration, cliquez sur **Sélectionner**.
- 2 Dans Paramètres généraux > ligne Paramètres du service Edge, cliquez sur **Afficher**.
- 3 Cliquez sur l'icône d'engrenage **Paramètres Horizon**.
- 4 Dans la page Paramètres Horizon, remplacez NO par YES pour activer Horizon.
- 5 Configurez les ressources des paramètres de service Edge suivantes pour Horizon.

Option	Description
Identifiant	Définissez par défaut sur View. Unified Access Gateway peut communiquer avec des serveurs qui utilisent le protocole View XML, tels que le Serveur de connexion View, Horizon Cloud et Horizon Cloud with On-Premises Infrastructure.
URL du Serveur de connexion	Entrez l'adresse de Horizon Server ou de l'équilibrage de charge. Entrez-la sous la forme https://00.00.00.00
Empreintes numériques de l'URL de destination du proxy	Entrez la liste des empreintes numériques Horizon Server. Si vous ne fournissez pas une liste d'empreintes numériques, les certificats de serveur doivent être émis par une autorité de certification approuvée. Entrez les chiffres d'empreintes numériques au format hexadécimal. Par exemple, sha1= C3 89 A2 19 DC 7A 48 2B 85 1C 81 EC 5E 8F 6A 3C 33 F2 95 C3

- 6 Pour configurer la règle de la méthode d'authentification et les autres paramètres avancés, cliquez sur **Autres**.

Option	Description
Méthodes d'authentification	<p>Sélectionnez les méthodes d'authentification à utiliser.</p> <p>La méthode par défaut est l'utilisation d'une authentification directe du nom d'utilisateur et du mot de passe. Les méthodes d'authentification que vous avez configurées dans Unified Access Gateway figurent dans les menus déroulants.</p> <p>Pour configurer l'authentification qui inclut l'application d'une seconde méthode d'authentification si la première tentative échoue :</p> <ol style="list-style-type: none"> Sélectionnez une méthode d'authentification dans le premier menu déroulant. Cliquez sur + et sélectionnez ET ou OU. Sélectionnez la seconde méthode d'authentification dans le troisième menu déroulant. <p>Pour obliger les utilisateurs à s'authentifier par le biais de deux méthodes d'authentification, remplacez OU par ET dans la liste déroulante.</p>
URL de contrôle de santé	Si l'équilibrage de charge est configuré, entrez l'URL que l'équilibrage de charge utilise pour se connecter et contrôler la santé du dispositif Unified Access Gateway.
SP SAML	Entrez le nom du fournisseur de services SAML pour le Broker View XMLAPI. Ce nom doit correspondre à celui des métadonnées du fournisseur de services configuré ou à la valeur spéciale DEMO.
PCoIP activé	Remplacez NON par OUI pour spécifier si PCoIP Secure Gateway est activé.
URL externe du proxy	Entrez l'URL externe du dispositif Unified Access Gateway. Les clients utilisent cette URL pour des connexions sécurisées via la passerelle sécurisée PCoIP. Cette connexion est utilisée pour le trafic PCoIP. La valeur par défaut est l'adresse IP d'Unified Access Gateway et le port 4172.
Invite de conseil de carte à puce	Remplacez NON par OUI pour permettre au dispositif Unified Access Gateway de prendre en charge la fonctionnalité des conseils de nom d'utilisateur pour la carte à puce. Avec la fonctionnalité de conseils de nom d'utilisateur de carte à puce, le certificat de carte à puce d'un utilisateur peut effectuer un mappage vers plusieurs comptes d'utilisateur de domaine Active Directory.
Blast activé	Pour utiliser la passerelle sécurisée Blast, Remplacez NO par YES .
URL externe Blast	Entrez l'URL du nom de domaine complet du dispositif Unified Access Gateway que les utilisateurs finaux emploient pour établir une connexion sécurisée à partir des navigateurs Web via la passerelle sécurisée Blast. Entrez-la sous la forme https://exampleappliance:443
Serveur de tunnel UDP activé	Activez cette option si les instances d'Horizon Client utilisent un réseau de mauvaise qualité.
Tunnel activé	Si le tunnel sécurisé View est utilisé, Remplacez NO par YES . Le client utilise l'URL externe pour les connexions de tunnel via la passerelle sécurisée View. Le tunnel est utilisé pour le trafic RDP, USB et de redirection multimédia (MMR).
URL externe de tunnel	Entrez l'URL externe du dispositif Unified Access Gateway. La valeur par défaut est utilisée si cette URL n'est pas définie.
Modèle de proxy	Entrez l'expression régulière qui correspond aux URI liés à l'URL d'Horizon Server (proxyDestinationUrl). Pour le Serveur de connexion View, une barre oblique (/) est une valeur classique pour la redirection vers le client Web HTML Access lorsque vous utilisez le dispositif Unified Access Gateway.
Faire correspondre au nom d'utilisateur Windows	Remplacez NO par YES pour faire correspondre le RSA SecurID et le nom d'utilisateur Windows. Lorsqu'il est défini sur YES, securID-auth est défini sur true et la correspondance de securID et du nom d'utilisateur Windows est appliquée.

Option	Description
Emplacement de la passerelle	Remplacez NO par YES pour activer l'emplacement à partir duquel sont issues les demandes. Le serveur de sécurité et Unified Access Gateway définissent l'emplacement de la passerelle. L'emplacement peut être externe ou interne.
Windows SSO activé	Remplacez NO par YES pour activer l'authentification RADIUS. La connexion Windows utilise les informations d'identification utilisées dans la première demande d'accès RADIUS réussie.
Entrées de l'hôte	Entrez une liste d'entrées d'hôte séparées par des virgules à ajouter au fichier /etc/hosts. Chaque entrée inclut une adresse IP, un nom d'hôte et un alias de nom d'hôte facultatif dans cet ordre, séparés par un espace. Par exemple, 10.192.168.1 example1.com, 10.192.168.2 example2.com example-alias.

7 Cliquez sur **Enregistrer**.

Options de configuration des URL externes Blast TCP et UDP

Blast Secure Gateway inclut la mise en réseau Blast Extreme Adaptive Transport (BEAT), qui s'ajuste dynamiquement aux conditions du réseau, comme les vitesses variables et les pertes de paquets. Dans Unified Access Gateway, vous pouvez configurer les ports utilisés par le protocole BEAT.

Blast utilise les ports standard TCP 8443 et UDP 8443. Le port UDP 443 peut également être utilisé pour accéder à un poste de travail via le serveur tunnel UDP. La configuration de port est définie via la propriété URL externe Blast.

Tableau 4-1. Options du port BEAT

URL externe Blast	Port TCP utilisé par le client	Port UDP utilisé par le client	Description
https://ap1.myco.com	8443	8443	Il s'agit du formulaire par défaut qui requiert que le port TCP 8443, et éventuellement le port UDP 8443, soit ouvert au niveau du pare-feu pour autoriser les connexions entre Internet et Unified Access Gateway
https://ap1.myco.com:443	443	8443	Utilisez ce formulaire lorsque les ports TCP 443 ou UDP 8443 doivent être ouverts.
https://ap1.myco.com:xxxx	xxxx	8443	
https://ap1.myco.com:xxx x/?UDPPort=yyyy	xxxx	yyyy	

Pour configurer des ports autres que celui par défaut, une règle de transfert d'adresse IP interne doit être ajoutée pour le protocole respectif lors du déploiement. Les règles de transfert doivent être spécifiées sur le déploiement dans le modèle OVF ou via les fichiers INI entrés via les commandes PowerShell.

Déploiement en tant que proxy inverse

Unified Access Gateway peut être utilisé comme proxy inverse Web et faire office de simple proxy inverse ou de proxy inverse d'authentification dans la DMZ.

Scénario de déploiement

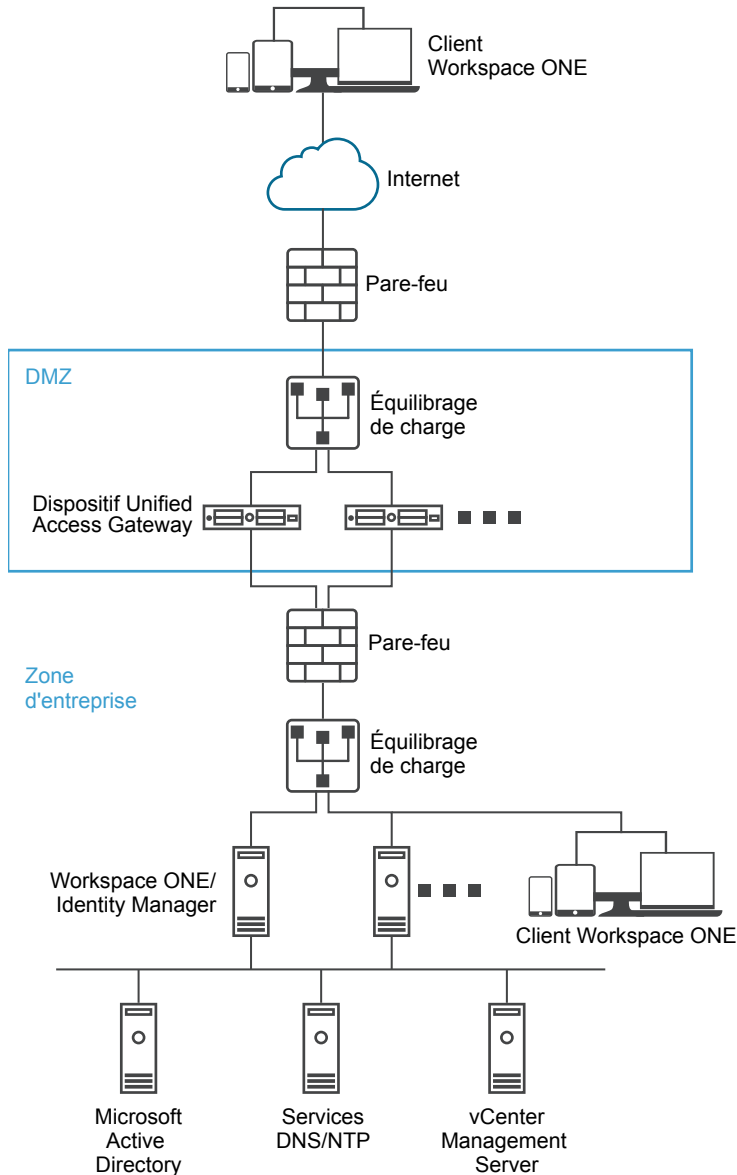
Unified Access Gateway fournit un accès à distance sécurisé pour un déploiement sur site de VMware Identity Manager. En général, les dispositifs Unified Access Gateway sont déployés dans une zone démilitarisée (DMZ) de réseau. Avec VMware Identity Manager, le dispositif Unified Access Gateway agit en tant que proxy inverse Web entre le navigateur d'un utilisateur et le service VMware Identity Manager dans le centre de données. Unified Access Gateway active également l'accès à distance au catalogue Workspace ONE pour lancer des applications Horizon.

Exigences du déploiement d'Unified Access Gateway avec VMware Identity Manager.

- DNS fractionné
- Le dispositif VMware Identity Manager doit avoir un nom de domaine complet (FQDN) comme nom d'hôte.

- Unified Access Gateway doit utiliser un DNS interne. Cela signifie que proxyDestinationURL doit utiliser un FQDN.

Figure 4-3. Dispositif Unified Access Gateway pointant vers VMware Identity Manager



Comprendre le proxy inverse

Unified Access Gateway, en tant que solution, fournit aux utilisateurs distants un accès au portail des applications pour leur permettre de s'authentifier et d'accéder à leurs ressources. Vous activez le proxy inverse authn sur un gestionnaire de services Edge. Actuellement, les méthodes d'authentification RSA SecurID et RADIUS sont prises en charge.

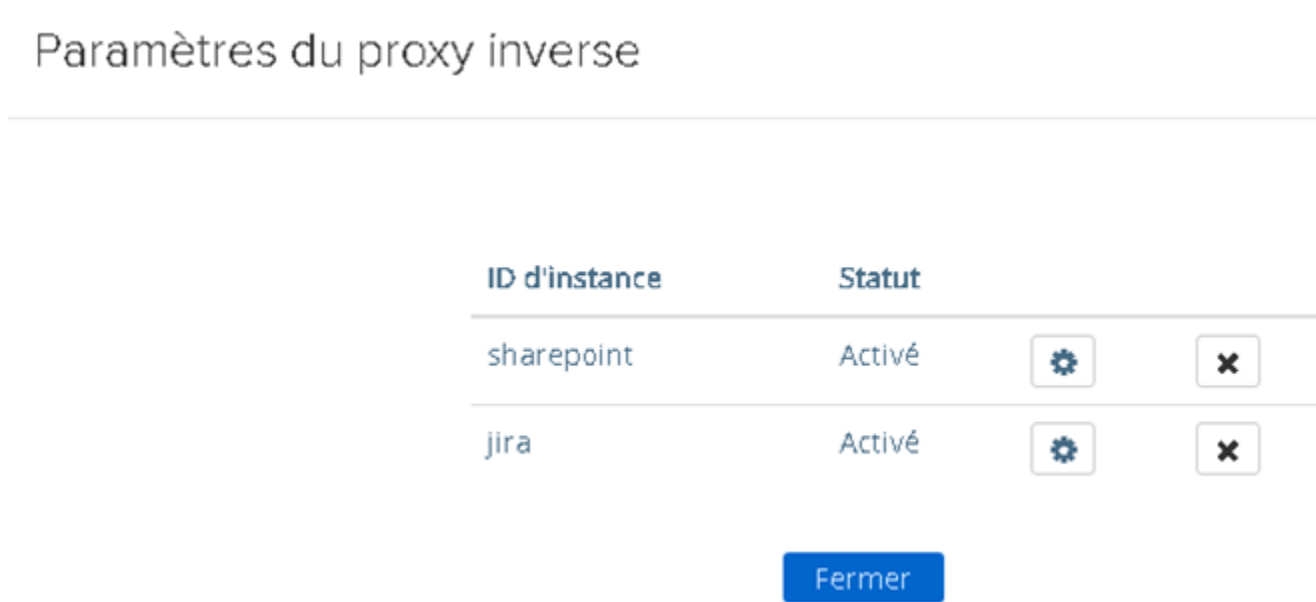
REMARQUE Vous devez générer les métadonnées de fournisseur d'identité avant d'activer l'authentification sur le proxy inverse Web.

Unified Access Gateway fournit un accès distant à VMware Identity Manager et aux applications Web avec ou sans authentification à partir d'un client basé sur un navigateur, puis il lance un poste de travail Horizon.

- Les clients basés sur un navigateur sont pris en charge au moyen des méthodes d'authentification RADIUS et RSA SecurID.

Vous pouvez configurer plusieurs instances du proxy inverse, chacune d'elles peut en outre être supprimée.

Figure 4-4. Plusieurs proxys inverses configurés



Configurer le proxy inverse

Vous pouvez configurer le service de proxy inverse Web pour utiliser Unified Access Gateway avec VMware Identity Manager.

Prérequis

Configuration requise pour un déploiement avec VMware Identity Manager.

- DNS fractionné. Le DNS fractionné peut être utilisé pour résoudre le nom en différentes adresses IP selon que l'adresse IP est interne ou externe.
- Le service VMware Identity Manager doit avoir un nom de domaine complet (FQDN) comme nom d'hôte.
- Unified Access Gateway doit utiliser un DNS interne. Cela signifie que l'URL de destination du proxy doit utiliser un FQDN.

Procédure

- 1 Dans la section Configuration manuelle de l'interface utilisateur d'administration, cliquez sur **Sélectionner**.
- 2 Dans Paramètres généraux > ligne Paramètres du service Edge, cliquez sur **Afficher**.
- 3 Cliquez sur l'icône d'engrenage **Paramètres de proxy inverse**.
- 4 Sur la page Paramètre du proxy inverse, cliquez sur **Ajouter**

- 5 Dans la section Activer les paramètres du proxy inverse, remplacez NON par OUI pour activer le proxy inverse.
- 6 Configurez les paramètres de service Edge suivants.

Option	Description
Identifiant	L'identifiant du service Edge est défini sur le proxy inverse Web.
ID d'instance	Nom unique pour identifier et différencier une instance du proxy inverse Web de toutes les autres instances du proxy inverse Web.
URL de destination du proxy	Entrez l'adresse de l'application Web.
Empreintes numériques de l'URL de destination du proxy	Entrez une liste des empreintes numériques de certificat serveur SSL acceptables pour l'URL proxyDestination. Si vous incluez le caractère générique *, n'importe quel certificat est autorisé. Une empreinte numérique est au format [alg=]xx:xx, où alg peut correspondre à sha1, la valeur par défaut, ou à md5. Les « xx » correspondent à des chiffres hexadécimaux. Le séparateur « : » peut également être un espace ou un caractère manquant. La casse est ignorée dans les empreintes numériques. Par exemple : sha1=B6 77 DC 9C 19 94 2E F1 78 F0 AD 4B EC 85 D1 7A F8 8B DC 34, sha256=ad:5c:f1:48:47:94:7e:80:82:73:13:6c:83:52:be:78:ed:ff: 50:23:56:a8:42:8a:d9:30:fc:3a:33:d6:c6:db Si vous ne configurez pas les empreintes numériques, les certificats de serveur doivent être émis par une autorité de certification approuvée.
Modèle de proxy	Entrez les chemins d'URI correspondants qui assurent la transmission à l'URL de destination. Par exemple, entrez <code>(/ /SAAS(.*) /hc(.*) /web(.*) /catalog-portal(.*)).</code> REMARQUE Lorsque vous configurez plusieurs proxys inverses, fournissez le nom d'hôte dans le modèle d'hôte de proxy.

- 7 Pour configurer d'autres paramètres avancés, cliquez sur **Autres**.

Option	Description
Méthodes d'authentification	La méthode par défaut est l'utilisation d'une authentification directe du nom d'utilisateur et du mot de passe. Les méthodes d'authentification que vous avez configurées dans Unified Access Gateway figurent dans les menus déroulants.
Chemin d'accès à l'URI de contrôle de santé	Unified Access Gateway se connecte à ce chemin d'accès à l'URI pour vérifier la santé de votre application Web.
SP SAML	Ce champ est requis lors de la configuration d'UAG en tant que proxy inverse authentifié pour VMware Identity Manager. Entrez le nom du fournisseur de services SAML pour le broker API XML View. Ce nom doit correspondre à celui du fournisseur de services configuré avec Unified Access Gateway ou à la valeur spéciale DEMO . S'il existe plusieurs fournisseurs de services configurés avec Unified Access Gateway, leurs noms doivent être uniques.
Code d'activation	Entrez le code d'activation généré par le service VMware Identity Manager et importé dans Unified Access Gateway pour établir la confiance entre VMware Identity Manager et Unified Access Gateway. Notez que le code d'activation n'est pas requis pour les déploiements sur site. Pour plus d'informations sur la génération d'un code d'activation, consultez la section <i>Déploiement de Cloud de VMware Identity Manager</i> .
URL externe	La valeur par défaut est l'URL de l'hôte Unified Access Gateway, le port 443. Vous pouvez entrer une autre URL externe. Utilisez le format <code>https://<host>:port</code> .

Option	Description
Modèle non sécurisé	Entrez le modèle de redirection de VMware Identity Manager connu. Par exemple : <code>/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/oauth2token(.*) 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(.*)</code>
Cookie d'authentification	Entrez le nom du cookie d'authentification. Par exemple : HZN
URL de redirection de connexion	Si l'utilisateur se déconnecte du portail, entrez l'URL de redirection pour la reconnexion. Par exemple : /SAAS/auth/Login?dest=%s
Modèle d'hôte de proxy	Nom d'hôte externe utilisé pour vérifier l'hôte entrant et voir s'il correspond au modèle de cette instance particulière. Le modèle d'hôte est facultatif lors de la configuration d'instances du proxy inverse Web.
Entrées de l'hôte	Entrez une liste d'entrées d'hôte séparées par des virgules à ajouter au fichier <code>/etc/hosts</code> . Chaque entrée inclut une adresse IP, un nom d'hôte et un alias de nom d'hôte facultatif dans cet ordre, séparés par un espace. Par exemple, 10.192.168.1 example1.com, 10.192.168.2 example2.com example-alias.

REMARQUE Les options Modèle non sécurisé, Cookie d'authentification et URL de redirection de connexion ne s'appliquent qu'avec VMware Identity Manager. Les valeurs fournies ici s'appliquent également à Access Point 2.8 et Unified Access Gateway 2.9.

REMARQUE Les propriétés Cookie d'authentification et Modèle non sécurisé ne sont pas valides pour le proxy inverse authn. Vous devez utiliser la propriété Méthodes d'authentification pour définir la méthode d'authentification.

8 Cliquez sur **Enregistrer**.

Suivant

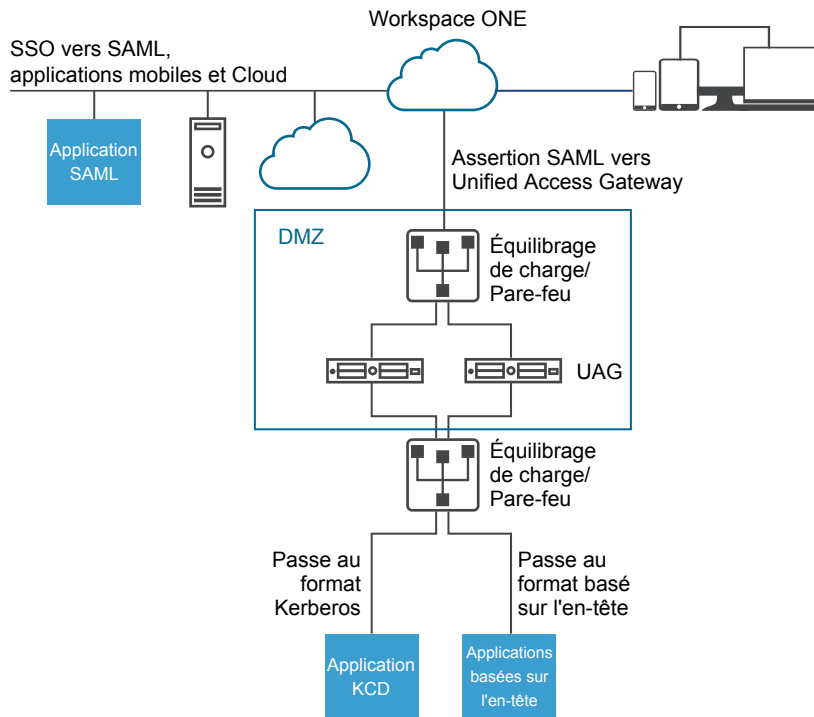
Pour activer le pontage d'identité, consultez « [Configuration des paramètres du pontage d'identité](#) », page 46.

Déploiement pour l'accès avec Single Sign-On à des applications Web héritées sur site

La fonctionnalité de pontage d'identité d'Unified Access Gateway peut être configurée pour fournir l'authentification unique (SSO) à des applications Web héritées qui utilisent la délégation Kerberos contrainte (KCD) ou l'authentification basée sur l'en-tête.

Unified Access Gateway en mode de pontage d'identité agit en tant que fournisseur de services qui transmet l'authentification utilisateur aux applications héritées configurées. VMware Identity Manager agit en tant que fournisseur d'identité et fournit SSO dans des applications SAML. Lorsque des utilisateurs accèdent à des applications héritées qui requièrent KCD ou l'authentification basée sur l'en-tête, Identity Manager authentifie l'utilisateur. Une assertion SAML avec les informations de l'utilisateur est envoyée à Unified Access Gateway. Unified Access Gateway utilise cette authentification pour autoriser les utilisateurs à accéder à l'application.

Figure 4-5. Mode de pontage d'identité d' Unified Access Gateway



Scénarios de déploiement du pontage d'identité

Le mode de pontage d'identité d'Unified Access Gateway peut être configuré pour fonctionner avec VMware Workspace[®] ONE[®] dans le Cloud ou dans un environnement sur site.

Utilisation du pontage d'identité d' Unified Access Gateway avec des clients Workspace ONE dans le Cloud

Le mode de pontage d'identité peut être configuré pour fonctionner avec Workspace ONE dans le Cloud pour authentifier des utilisateurs. Lorsqu'un utilisateur demande l'accès à une application Web héritée, le fournisseur d'identité applique des stratégies d'authentification et d'autorisation applicables.

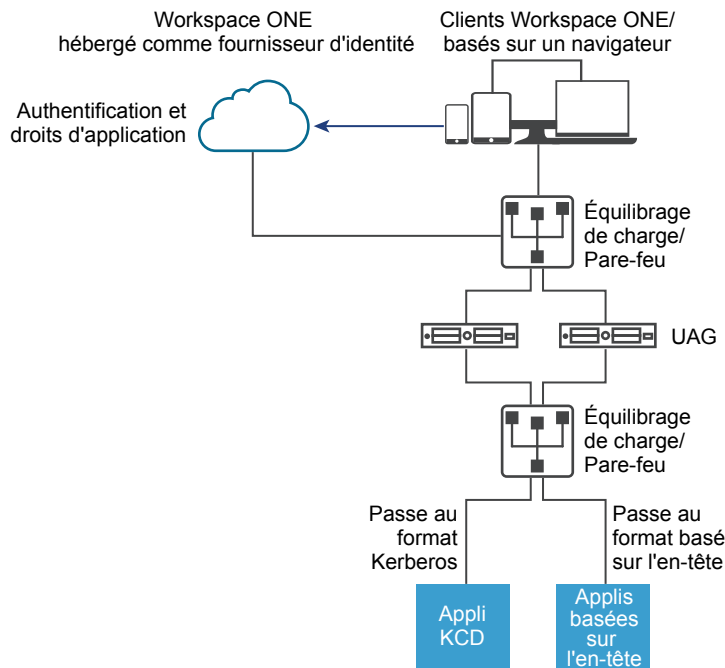
Si l'utilisateur est validé, le fournisseur d'identité crée un jeton SAML et l'envoie à l'utilisateur. L'utilisateur transmet le jeton SAML à Unified Access Gateway dans la zone DMZ. Unified Access Gateway valide le jeton SAML et récupère le nom principal de l'utilisateur à partir du jeton.

Si la demande concerne l'authentification Kerberos, la délégation Kerberos contrainte est utilisée pour négocier avec le serveur Active Directory. Unified Access Gateway emprunte l'identité de l'utilisateur pour récupérer le jeton Kerberos pour s'authentifier avec l'application.

Si la demande concerne l'authentification basée sur l'en-tête, le nom d'en-tête de l'utilisateur est envoyé au serveur Web pour demander l'authentification avec l'application.

L'application renvoie la réponse à Unified Access Gateway. La réponse est renvoyée à l'utilisateur.

Figure 4-6. Pontage d'identité d' Unified Access Gateway avec Workspace ONE dans le Cloud



Utilisation du pontage d'identité avec des clients Workspace ONE sur site

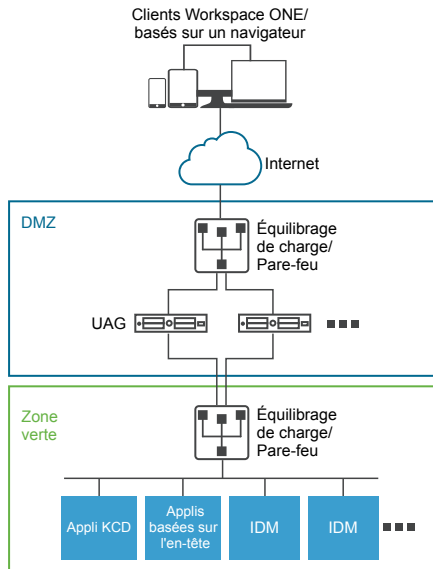
Lorsque le mode de pontage d'identité est configuré pour authentifier des utilisateurs avec Workspace ONE dans un environnement sur site, les utilisateurs entrent l'URL pour accéder à l'application Web héritée sur site via le proxy Unified Access Gateway. Unified Access Gateway redirige la demande vers le fournisseur d'identité à des fins d'authentification. Le fournisseur d'identité applique des stratégies d'authentification et d'autorisation à la demande. Si l'utilisateur est validé, le fournisseur d'identité crée un jeton SAML et l'envoie à l'utilisateur.

L'utilisateur transmet le jeton SAML à Unified Access Gateway. Unified Access Gateway valide le jeton SAML et récupère le nom principal de l'utilisateur à partir du jeton.

Si la demande concerne l'authentification Kerberos, la délégation Kerberos contrainte est utilisée pour négocier avec le serveur Active Directory. Unified Access Gateway emprunte l'identité de l'utilisateur pour récupérer le jeton Kerberos pour s'authentifier avec l'application.

Si la demande concerne l'authentification basée sur l'en-tête, le nom d'en-tête de l'utilisateur est envoyé au serveur Web pour demander l'authentification avec l'application.

L'application renvoie la réponse à Unified Access Gateway. La réponse est renvoyée à l'utilisateur.

Figure 4-7. Pontage d'identité d' Unified Access Gateway sur site

Configuration des paramètres du pontage d'identité

Lorsque Kerberos est configuré dans l'application principale, pour configurer le pontage d'identité dans Unified Access Gateway, vous téléchargez les métadonnées du fournisseur d'identité ainsi que le fichier keytab et vous configurez les paramètres de domaine KCD.

REMARQUE Cette version de pontage d'identité prend en charge uniquement une configuration de domaine unique. Cela signifie que l'utilisateur et le SPN doivent être dans le même domaine.

Lorsque le pontage d'identité est activé avec l'authentification basée sur l'en-tête, les paramètres du fichier keytab et les paramètres de domaine KCD ne sont pas requis.

Avant de configurer les paramètres du pontage d'identité pour l'authentification Kerberos, assurez-vous que les éléments suivants sont disponibles.

- Un fournisseur d'identité est configuré et les métadonnées SAML du fournisseur d'identité sont enregistrées. Le fichier de métadonnées SAML est téléchargé vers Unified Access Gateway (scénarios SAML uniquement).
- Pour l'authentification Kerberos, un serveur sur lequel Kerberos est activé avec les noms de domaine des centres de distribution de clés à utiliser identifiés.
- Pour l'authentification Kerberos, téléchargez le fichier keytab Kerberos sur Unified Access Gateway. Le fichier keytab inclut les informations d'identification du compte de service Active Directory qui est configuré pour obtenir le ticket Kerberos au nom d'un utilisateur du domaine pour un service principal donné.

Télécharger des métadonnées du fournisseur d'identité

Pour configurer la fonctionnalité de pontage d'identité, vous devez télécharger le fichier XML de métadonnées de certificat SAML du fournisseur d'identité sur Unified Access Gateway.

Prérequis

Fichier XML de métadonnées SAML enregistré sur un ordinateur auquel vous avez accès.

Si vous utilisez VMware Identity Manager comme fournisseur d'identité, téléchargez et enregistrez le fichier de métadonnées SAML à partir de la console d'administration de VMware Identity Manager, Catalogue > Métadonnées SAML de paramètres > lien de métadonnées Fournisseur d'identité (IdP).

Procédure

- 1 Dans la section Configuration manuelle de l'interface utilisateur d'administration, cliquez sur **Sélectionner**.
- 2 Dans la section **Paramètres avancés > Paramètres du pontage d'identité**, sélectionnez l'icône d'engrenage **Télécharger les métadonnées du fournisseur d'identité**.
- 3 Entrez l'ID d'entité du fournisseur d'identité dans la zone de texte **ID d'entité**.

Si vous n'entrez pas de valeur dans la zone de texte ID d'entité, le nom du fournisseur d'identité dans le fichier de métadonnées est analysé et utilisé comme ID d'entité du fournisseur d'identité.

- 4 Dans la section **Métadonnées du fournisseur d'identité**, cliquez sur **Sélectionner** et accédez au fichier de métadonnées que vous avez enregistré. Cliquez sur **Ouvrir**.
- 5 Cliquez sur **Enregistrer**.

Suivant

Pour l'authentification KDC, configurez les paramètres du domaine et les paramètres du fichier keytab.

Pour l'authentification basée sur l'en-tête, lorsque vous configurez la fonctionnalité de pontage d'identité, complétez l'option Nom d'en-tête de l'utilisateur avec le nom de l'en-tête HTTP qui inclut l'ID utilisateur.

Configurer des paramètres de domaine

Configurez le nom de domaine, les centres de distribution de clés pour le domaine et le délai d'expiration du KDC.

Le domaine est le nom d'une entité administrative qui conserve des données d'authentification. Il est important de sélectionner un nom descriptif pour le domaine d'authentification Kerberos. Configurez le domaine, appelé aussi nom de domaine, et le service KDC correspondant dans Unified Access Gateway. Lorsqu'une demande UPN parvient à un domaine spécifique, Unified Access Gateway résout en interne le KDC pour utiliser le ticket en service Kerberos.

L'usage consiste à utiliser un nom de domaine identique au FQDN, mais écrit en majuscules. Par exemple, un nom de domaine est EXAMPLE.NET. Le nom de domaine est utilisé par un client Kerberos pour générer des noms DNS.

À partir d'UAG 3.0, vous pouvez supprimer les domaines précédemment définis.

Prérequis

Un serveur sur lequel Kerberos est activé avec les noms de domaine des centres de distribution de clés à utiliser identifiés.

Procédure

- 1 Dans la section Configuration manuelle de l'interface utilisateur d'administration, cliquez sur **Sélectionner**.
- 2 Dans la section **Paramètres avancés > Paramètres du pontage d'identité**, sélectionnez l'icône d'engrenage **Paramètres de domaine**.
- 3 Cliquez sur **Ajouter**.

- Renseignez le formulaire.

Étiquette	Description
Nom du domaine	Entrez le domaine avec le nom de domaine. Entrez le domaine en majuscules. Le domaine doit correspondre au nom de domaine configuré dans Active Directory.
Centres de distribution de clés	Entrez les serveurs KDC pour le domaine. Séparez la liste par des virgules si vous ajoutez plusieurs serveurs.
Délai d'expiration du KDC (en secondes)	Entrez la durée d'attente pour la réponse du KDC. La valeur par défaut est de 3 secondes.

- Cliquez sur **Enregistrer**.

Suivant

Configurez les paramètres du fichier keytab.

Télécharger les paramètres Keytab

Un fichier keytab est un fichier contenant des paires de principaux et de clés chiffrées Kerberos. Un fichier keytab est créé pour les applications qui requièrent l'authentification unique. Le pontage d'identité d'Unified Access Gateway utilise un fichier keytab pour s'authentifier sur des systèmes distants à l'aide de Kerberos sans entrer de mot de passe.

Lorsqu'un utilisateur est authentifié sur Unified Access Gateway à partir du fournisseur d'identité, Unified Access Gateway demande un ticket Kerberos au contrôleur de domaine Kerberos pour authentifier l'utilisateur.

Unified Access Gateway utilise le fichier keytab pour emprunter l'identité de l'utilisateur à authentifier au domaine Active Directory interne. Unified Access Gateway doit posséder un compte de service d'utilisateur de domaine sur le domaine Active Directory. Unified Access Gateway n'est pas directement joint au domaine.

REMARQUE Si l'administrateur génère de nouveau le fichier keytab pour un compte de service, le fichier keytab doit être téléchargé de nouveau sur Unified Access Gateway.

Prérequis

Accédez au fichier keytab Kerberos à télécharger sur Unified Access Gateway. Le fichier keytab est un fichier binaire. Si possible, utilisez SCP ou une autre méthode sécurisée pour transférer le fichier keytab entre des ordinateurs.

Procédure

- Dans la section Configuration manuelle de l'interface utilisateur d'administration, cliquez sur **Sélectionner**.
- Dans la section **Paramètres avancés > Paramètres du pontage d'identité**, sélectionnez l'icône d'engrenage **Télécharger les paramètres Keytab**.
- (Facultatif) Entrez le nom du principal Kerberos dans la zone de texte **Nom du principal**.

Chaque principal est toujours complété du nom du domaine. Le domaine doit être en majuscules.

Vérifiez que le nom du principal entré ici est le premier principal trouvé dans le fichier keytab. Si le même nom du principal ne se trouve pas dans le fichier keytab téléchargé, le téléchargement du fichier keytab échoue.

- 4 Dans le champ **Sélectionner un fichier Keytab**, cliquez sur **Sélectionner** et accédez au fichier keytab que vous avez enregistré. Cliquez sur **Ouvrir**.

Si vous n'avez pas entré le nom du principal, le premier principal trouvé dans le fichier keytab est utilisé. Vous pouvez fusionner plusieurs fichiers keytab en un seul.

- 5 Cliquez sur **Enregistrer**.

Suivant

Configurez le proxy inverse Web pour le pontage d'identité d'Unified Access Gateway.

Configurer un proxy inverse Web pour le pontage d'identité

Activez le pontage d'identité, configurez le nom d'hôte externe pour le service et téléchargez le fichier de métadonnées de fournisseur de services d'Unified Access Gateway.

Ce fichier de métadonnées est téléchargé sur la page de configuration de l'application Web dans le service VMware Identity Manager.

Prérequis

Paramètres de pontage d'identité configurés dans l'interface utilisateur d'administration d'Unified Access Gateway, section Paramètres avancés. Les paramètres suivants doivent être configurés.

- Métadonnées de fournisseur d'identité téléchargées sur Unified Access Gateway.
- Nom du principal Kerberos configuré et fichier keytab téléchargé sur Unified Access Gateway.
- Nom de domaine et informations sur le centre de distribution de clés.

Procédure

- 1 Dans la section Configuration manuelle de l'interface utilisateur d'administration, cliquez sur **Sélectionner**.
- 2 Dans Paramètres généraux > ligne Paramètres du service Edge, cliquez sur **Afficher**.
- 3 Cliquez sur l'icône d'engrenage **Paramètres de proxy inverse**.
- 4 Sur la page Paramètres du proxy inverse, cliquez sur **Ajouter** pour créer un paramètre du proxy.
- 5 Configurez les paramètres de service Edge suivants.

Option	Description
Identifiant	L'identifiant du service Edge est défini sur le proxy inverse Web.
ID d'instance	Nom unique de l'instance du proxy inverse Web.
URL de destination du proxy	Spécifiez l'URI interne de l'application Web. Unified Access Gateway doit pouvoir résoudre et accéder à cette URL.
Empreintes numériques de l'URL de destination du proxy	Entrez l'URI pour correspondre à ce paramètre du proxy. Une empreinte numérique est au format [alg=]xx:xx, où alg peut correspondre à sha1, la valeur par défaut, ou md5. Les « xx » correspondent à des chiffres hexadécimaux. Par exemple, sha=C3 89 A2 19 DC 7A 48 2B 85 1C 81 EC 5E 8F 6A 3C 33 F2 95 C3 Si vous ne configurez pas les empreintes numériques, les certificats de serveur doivent être émis par une autorité de certification approuvée.
Modèle de proxy	(Facultatif) Spécifiez un modèle d'hôte. Le modèle d'hôte indique à Unified Access Gateway à quel moment transmettre le trafic à l'aide de ce paramètre du proxy si le modèle de proxy n'est pas unique. Ce moment est décidé à l'aide de l'URL utilisée par le navigateur Web du client. Par exemple, entrez <code>(/ /SAAS(.*) /hc(.*) /web(.*) /catalog-portal(.*)).</code>

- 6 Dans la section Activer le pontage d'identité, remplacez NON par OUI.
- 7 Configurez les paramètres de pontage d'identité suivants.

Option	Description
Fournisseur d'identité	Dans le menu déroulant, sélectionnez le fournisseur d'identité à utiliser.
Keytab	Dans le menu déroulant, sélectionnez le fichier keytab configuré pour ce proxy inverse.
Nom du principal de service cible	Entrez le nom du principal de service Kerberos. Chaque principal est toujours complété du nom du domaine. Par exemple, myco_hostname@MYCOMPANY . Tapez le nom du domaine en majuscules. Si vous n'ajoutez pas de nom dans la zone de texte, le nom du principal de service est dérivé du nom d'hôte de l'URL de destination du proxy.
Page d'accueil du service	Entrez la page vers laquelle les utilisateurs sont redirigés dans le fournisseur d'identité après la validation de l'assertion. Le paramètre par défaut est /.
Nom d'en-tête de l'utilisateur	Pour l'authentification basée sur l'en-tête, entrez le nom de l'en-tête HTTP qui inclut l'ID d'utilisateur dérivé de l'assertion.

- 8 Dans la section Télécharger des métadonnées SP, cliquez sur **Télécharger**.
Enregistrez le fichier de métadonnées de fournisseur de services.
- 9 Cliquez sur **Enregistrer**.

Suivant

Ajoutez le fichier de métadonnées de fournisseur de services d'Unified Access Gateway sur la page de configuration de l'application Web dans le service VMware Identity Manager.

Ajouter le fichier de métadonnées de fournisseur de services d'Unified Access Gateway au service VMware Identity Manager

Le fichier de métadonnées de fournisseur de services d'Unified Access Gateway que vous avez téléchargé doit être téléchargé sur la page de configuration de l'application Web dans le service VMware Identity Manager.

Le certificat SSL utilisé doit être le même sur tous les serveurs Unified Access Gateway à équilibrage de charge.

Prérequis

Fichier de métadonnées de fournisseur de services d'Unified Access Gateway enregistré sur l'ordinateur

Procédure

- 1 Connectez-vous à la console d'administration de VMware Identity Manager.
- 2 Dans l'onglet Catalogue, cliquez sur **Ajouter une application** et sélectionnez **créer une application**.
- 3 Sur la page Détails de l'application, entrez un nom convivial dans la zone de texte Nom.
- 4 Sélectionnez le profil d'authentification **SAML 2.0 POST**.
Vous pouvez également ajouter une description de cette application et une icône à afficher aux utilisateurs finaux dans le portail Workspace ONE.
- 5 Cliquez sur **Suivant** et, sur la page Configuration de l'application, faites défiler la section **Configurer via**.
- 6 Sélectionnez la case d'option Métadonnées XML et collez le texte des métadonnées de fournisseur de services d'Unified Access Gateway dans la zone de texte Métadonnées XML.

- 7 (Facultatif) Dans la section Mappage d'attribut, mappez les noms d'attribut suivants aux valeurs de profil d'utilisateur. La valeur du champ FORMAT est Basique. Les noms d'attribut doivent être entrés en minuscules.

Nom	Valeur configurée
upn	userPrincipalName
userid	ID d'utilisateur Active Directory

- 8 Cliquez sur **Enregistrer**.

Suivant

Attribuez cette application à des utilisateurs et des groupes.

REMARQUE Unified Access Gateway ne prend en charge que les utilisateurs avec un seul domaine. Si le fournisseur d'identité est configuré avec plusieurs domaines, l'application peut être autorisée uniquement pour les utilisateurs dans un seul domaine.

Tunnel VMware sur Unified Access Gateway

Le déploiement du tunnel VMware à l'aide du dispositif Unified Access Gateway offre aux applications un moyen sécurisé et efficace d'accéder aux ressources d'entreprise. Unified Access Gateway prend en charge le déploiement dans les environnements ESXi ou Microsoft Hyper-V.

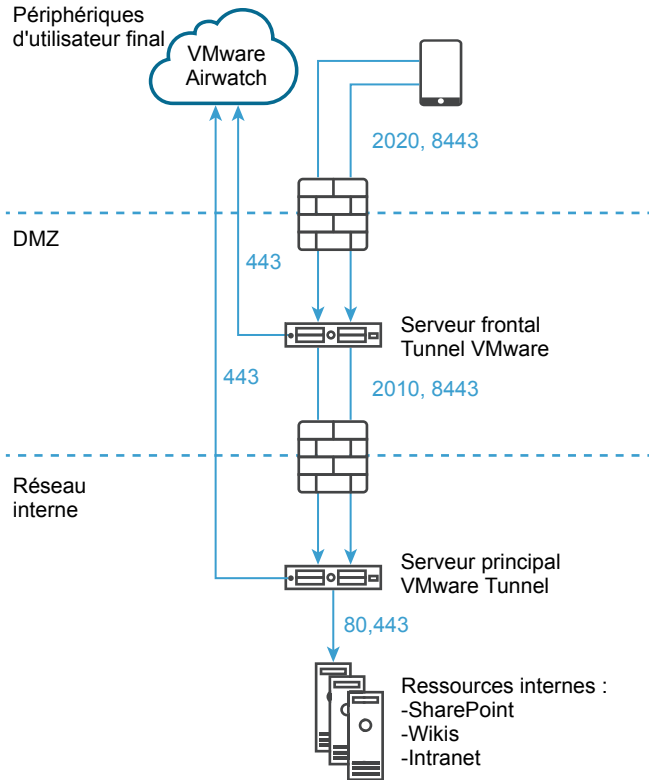
Le tunnel VMware comprend deux composants indépendants : le proxy tunnel et le tunnel par application. Pour déployer le tunnel VMware, vous disposez de deux modèles d'architecture réseau : à niveau unique ou multinationnel.

Les modèles de déploiement du proxy tunnel et du tunnel par application peuvent tous deux être utilisés pour un réseau multinationnel sur le dispositif UAG. Le déploiement se compose d'un serveur Unified Access Gateway frontal déployé dans la zone DMZ et d'un serveur principal déployé dans le réseau interne.

Le composant Proxy tunnel sécurise le trafic réseau entre un périphérique utilisateur et un site Web via l'application VMware Browser ou n'importe quelle application compatible avec le SDK AirWatch déployée à partir d'AirWatch. L'application mobile crée une connexion HTTPS sécurisée avec le serveur Tunnel Proxy et protège les données sensibles. Les périphériques sont authentifiés auprès du proxy tunnel avec un certificat émis via le SDK tel que configuré dans la Console d'administration AirWatch. En général, ce composant doit être utilisé lorsque plusieurs périphériques non gérés nécessitent un accès sécurisé aux ressources internes.

Pour les périphériques totalement inscrits, le composant Tunnel par application permet aux périphériques de se connecter aux ressources internes sans avoir besoin du SDK AirWatch. Ce composant s'appuie sur les capacités natives de VPN par application des systèmes d'exploitation iOS, Android, Windows 10 et macOS. Pour plus d'informations sur ces plateformes et les capacités du composant Tunnel VMware, reportez-vous au *Guide du tunnel VMware*, à l'adresse <https://resources.air-watch.com/view/yr8n5s2b9d6qqbcfjbrw/en> (en anglais)

Le déploiement du tunnel VMware pour votre environnement AirWatch comprend l'installation du matériel de départ, la configuration des informations du nom d'hôte et du port du tunnel VMware dans la Console d'administration AirWatch, le téléchargement et le déploiement du modèle OVF de Unified Access Gateway et la configuration manuelle du tunnel VMware. Reportez-vous à la section « [Configurer les paramètres de VMware Tunnel pour AirWatch](#) », page 52 pour plus d'informations.

Figure 4-8. Déploiement multiniveau du tunnel VMware : tunnel proxy et tunnel par application

AirWatch 9.1 et versions ultérieures prend en charge le mode cascade en tant que modèle de déploiement multiniveau du tunnel VMware. Le mode cascade nécessite un port entrant dédié pour chaque composant Tunnel entre Internet et le serveur Tunnel frontal. Les serveurs frontal et principal doivent être en mesure de communiquer avec les serveurs API AirWatch et AWCM. Le mode cascade du tunnel VMware prend en charge l'architecture multiniveau pour le composant Tunnel par application.

Pour plus de détails, notamment sur le déploiement de point de terminaison de relais utilisable avec le composant Proxy tunnel, consultez la documentation du *tunnel VMware* à l'adresse <https://resources.air-watch.com/view/yr8n5s2b9d6qqbcfjbrw/en>

Configurer les paramètres de VMware Tunnel pour AirWatch

Le déploiement du proxy tunnel sécurise le trafic réseau entre un périphérique utilisateur et un site Web via l'application mobile VMware Browser.

Procédure

- 1 Dans la section Configuration manuelle de l'interface utilisateur d'administration, cliquez sur **Sélectionner**.
- 2 Dans Paramètres généraux > ligne Paramètres du service Edge, cliquez sur **Afficher**.
- 3 Cliquez sur l'icône d'engrenage **Paramètres de VMware Tunnel**.
- 4 Remplacez NO par YES pour activer le proxy tunnel.

- 5 Configurez les ressources des paramètres de service Edge suivantes.

Option	Description
URL du serveur API	Entrez l'URL du serveur d'API AirWatch. Par exemple, entrez-la sous la forme <code>https://example.com:<port></code> .
Nom d'utilisateur du serveur API	Entrez le nom d'utilisateur pour vous connecter au serveur API.
Mot de passe du serveur API	Entrez le mot de passe pour vous connecter au serveur API.
ID du groupe Organisation	Entrez l'organisation de l'utilisateur.
Nom d'hôte du serveur du tunnel	Saisissez le nom d'hôte externe de VMware Tunnel configuré dans la console d'administration AirWatch.

- 6 Pour configurer d'autres paramètres avancés, cliquez sur **Autres**.

Option	Description
Hôte de proxy sortant	Entrez le nom d'hôte sur lequel le proxy sortant est installé. REMARQUE Il ne s'agit pas de Tunnel Proxy.
Port de proxy sortant	Entrez le numéro de port du proxy sortant.
Nom d'utilisateur du proxy sortant	Entrez le nom d'utilisateur pour vous connecter au proxy sortant.
Mot de passe de proxy sortant	Entrez le mot de passe pour vous connecter au proxy sortant.
Authentification NTLM	Remplacez NO par YES pour spécifier que la demande de proxy sortant nécessite une authentification NTLM.
Utiliser pour le proxy VMware Tunnel	Remplacez NO par YES pour utiliser ce proxy en tant que proxy sortant pour VMware Tunnel. S'il n'est pas activé, Unified Access Gateway utilise ce proxy pour l'appel d'API initial afin d'obtenir la configuration de la console d'administration d'AirWatch.
Entrées de l'hôte	Entrez une liste d'entrées d'hôte séparées par des virgules à ajouter au fichier <code>/etc/hosts</code> . Chaque entrée inclut une adresse IP, un nom d'hôte et un alias de nom d'hôte facultatif dans cet ordre, séparés par un espace. Par exemple, 10.192.168.1 example1.com, 10.192.168.2 example2.com example-alias
Certificats approuvés	Sélectionnez les fichiers de certificat approuvés à ajouter au magasin d'approbations.

- 7 Cliquez sur **Enregistrer**.

Pour plus d'informations sur le déploiement d'Unified Access Gateway avec AirWatch, consultez la documentation de VMware Tunnel https://my.airwatch.com/help/9.1/en/Content/Expert_Guides/EI/AW_Tunnel/C/Tunnel_Introduction.htm.

Déploiement de VMware Tunnel pour AirWatch avec PowerShell

Vous pouvez utiliser PowerShell pour déployer VMware Tunnel pour AirWatch.

Pour plus d'informations sur le déploiement de VMware Tunnel avec PowerShell, regardez cette vidéo :



Déploiement de VMware AirWatch Tunnel avec PowerShell
(http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_airwatch_tunnel_powershell)

Configuration d'Unified Access Gateway à l'aide de certificats TLS/SSL

5

Vous devez configurer les certificats TLS/SSL pour les dispositifs Unified Access Gateway.

REMARQUE La configuration des certificats TLS/SSL pour le dispositif Unified Access Gateway s'applique à Horizon View, Horizon Cloud et proxy inverse Web uniquement.

Configuration de certificats TLS/SSL pour les dispositifs Unified Access Gateway

TLS/SSL est requis pour les connexions client à des dispositifs Unified Access Gateway. Les dispositifs face au client Unified Access Gateway et les serveurs intermédiaires qui mettent fin aux connexions TLS/SSL requièrent des certificats de serveur TLS/SSL.

Les certificats de serveur TLS/SSL sont signés par une autorité de certification. Une autorité de certification est une entité approuvée qui garantit l'identité du certificat et de son créateur. Lorsque le certificat est signé par une autorité de certification approuvée, les utilisateurs ne reçoivent plus de messages leur demandant de vérifier le certificat, et les périphériques de client léger peuvent se connecter sans demander de configuration supplémentaire.

Un certificat de serveur TLS/SSL par défaut est généré lorsque vous déployez un dispositif Unified Access Gateway. Pour les environnements de production, VMware vous recommande fortement de remplacer le certificat par défaut dès que possible. Le certificat par défaut n'est pas signé par une autorité de certification approuvée. Utilisez le certificat par défaut uniquement dans un environnement hors production.

Sélection du type de certificat correct

Vous pouvez utiliser divers types de certificats TLS/SSL avec Unified Access Gateway. La sélection du type de certificat correct pour votre déploiement est cruciale. Les types de certificat ont des coûts différents, en fonction du nombre de serveurs sur lesquels ils peuvent être utilisés.

Suivez les recommandations de sécurité de VMware en utilisant des noms de domaine complets (FQDN) pour vos certificats, quel que soit le type que vous sélectionnez. N'utilisez pas un nom de serveur simple ou une adresse IP, même pour les communications effectuées à l'intérieur de votre domaine interne.

Certificat de nom de serveur unique

Vous pouvez générer un certificat avec un nom d'objet pour un serveur spécifique. Par exemple : `dept.example.com`.

Ce type de certificat est utile si, par exemple, un seul dispositif Unified Access Gateway a besoin d'un certificat.

Lorsque vous soumettez une demande de signature de certificat à une autorité de certification, fournissez le nom de serveur à associer au certificat. Vérifiez que le dispositif Unified Access Gateway peut résoudre le nom de serveur que vous fournissez pour qu'il corresponde au nom associé au certificat.

Autres noms de l'objet

Un autre nom de l'objet (SAN) est un attribut pouvant être ajouté à un certificat lors de son émission. Vous utilisez cet attribut pour ajouter des noms d'objet (URL) à un certificat pour qu'il puisse valider plusieurs serveurs.

Par exemple, trois certificats peuvent être émis pour les dispositifs Unified Access Gateway qui se trouvent derrière un équilibrage de charge : `ap1.example.com`, `ap2.example.com` et `ap3.example.com`. En ajoutant un autre nom de l'objet qui représente le nom d'hôte de l'équilibrage de charge, tel que `horizon.example.com` dans cet exemple, le certificat est valide, car il correspond au nom d'hôte spécifié par le client.

Lorsque vous soumettez une demande de signature de certificat à une autorité de certification, fournissez l'adresse IP virtuelle (VIP) d'équilibrage de charge d'interface externe comme nom commun et le nom du SAN. Vérifiez que le dispositif Unified Access Gateway peut résoudre le nom de serveur que vous fournissez pour qu'il corresponde au nom associé au certificat.

Le certificat est utilisé sur le port 443.

Certificat de caractère générique

Un certificat de caractère générique est généré pour pouvoir être utilisé pour plusieurs services. Par exemple : `*.example.com`.

Un certificat de caractère générique est utile si plusieurs serveurs ont besoin d'un certificat. Si d'autres applications dans votre environnement en plus des dispositifs Unified Access Gateway ont besoin de certificats TLS/SSL, vous pouvez utiliser un certificat de caractère générique pour ces serveurs. Toutefois, si vous utilisez un certificat de caractère générique partagé avec d'autres services, la sécurité du produit VMware Horizon dépend également de la sécurité de ces autres services.

REMARQUE Vous ne pouvez utiliser un certificat de caractère générique que sur un seul niveau de domaine. Par exemple, un certificat de caractère générique avec le nom d'objet `*.example.com` peut être utilisé pour le sous-domaine `dept.example.com`, mais pas `dept.it.example.com`.

Les certificats que vous importez dans le dispositif Unified Access Gateway doivent être approuvés par des machines clientes et doivent également être applicables à toutes les instances d'Unified Access Gateway et à tout équilibrage de charge, en utilisant des certificats de caractère générique ou des certificats avec l'autre nom de l'objet (SAN).

Convertir des fichiers de certificat au format PEM sur une ligne

Pour utiliser l'API REST Unified Access Gateway afin de configurer des paramètres de certificat, ou pour utiliser les scripts PowerShell, vous devez convertir le certificat en fichiers au format PEM pour la chaîne de certificats et la clé privée, et vous devez ensuite convertir les fichiers `.pem` en un format sur une seule ligne qui inclut des caractères de saut de ligne intégrés.

Lors de la configuration d'Unified Access Gateway, vous pouvez avoir à convertir trois types possibles de certificat.

- Vous devez toujours installer et configurer un certificat de serveur TLS/SSL pour le dispositif Unified Access Gateway.
- Si vous prévoyez d'utiliser l'authentification par carte à puce, vous devez installer et configurer le certificat de l'émetteur d'autorité de certification approuvée pour le certificat qui sera placé sur la carte à puce.

- Si vous prévoyez d'utiliser l'authentification par carte à puce, VMware vous recommande d'installer et de configurer un certificat racine pour l'autorité de certification de signature pour le certificat du serveur SAML installé sur le dispositif Unified Access Gateway.

Pour tous ces types de certificats, vous effectuez la même procédure pour convertir le certificat en un fichier au format PEM qui contient la chaîne de certificats. Pour les certificats de serveur TLS/SSL et les certificats racine, vous convertissez également chaque fichier en un fichier PEM qui contient la clé privée. Vous devez ensuite convertir chaque fichier `.pem` en un format sur une seule ligne pouvant être transmis dans une chaîne JSON à l'API REST Unified Access Gateway.

Prérequis

- Vérifiez que vous disposez du fichier de certificat. Le fichier peut être au format PKCS#12 (`.p12` ou `.pfx`) ou au format Java JKS ou JCEKS.
- Familiarisez-vous avec l'outil de ligne de commande `openssl` que vous utiliserez pour convertir le certificat. Reportez-vous à la section <https://www.openssl.org/docs/apps/openssl.html>.
- Si le certificat est au format Java JKS ou JCEKS, familiarisez-vous avec l'outil de ligne de commande `keytool` de Java pour d'abord convertir le certificat au format `.p12` ou `.pks` avant de convertir en fichiers `.pem`.

Procédure

- 1 Si votre certificat est au format Java JKS ou JCEKS, utilisez `keytool` pour convertir le certificat au format `.p12` ou `.pks`.

IMPORTANT Utilisez le même mot de passe source et de destination lors de cette conversion.

- 2 Si votre certificat est au format PKCS#12 (`.p12` ou `.pfx`), ou après la conversion du certificat au format PKCS#12, utilisez `openssl` pour convertir le certificat en fichiers `.pem`.

Par exemple, si le nom du certificat est `mycaservercert.pfx`, utilisez les commandes suivantes pour convertir le certificat :

```
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 Modifiez `mycaservercert.pem` et supprimez les entrées inutiles du certificat. Il doit contenir le certificat de serveur SSL, ainsi que les certificats d'autorité de certification intermédiaires et racine nécessaires.
- 4 Utilisez la commande UNIX suivante pour convertir chaque fichier `.pem` en une valeur pouvant être transmise dans une chaîne JSON à l'API REST Unified Access Gateway :

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

Dans cet exemple, `cert-name.pem` est le nom du fichier de certificat. Le certificat ressemble à cet exemple.

Figure 5-1. Fichier de certificat sur une seule ligne

```

-----BEGIN CERTIFICATE-----
MIIFWjCCBEKgAwIBAgIQD6CcVzp5eV5FZjkgkpm5uzANBgkqhkiG9w0BAQ
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVI
d3cuZGlnaWN1cnQuY29tMS8wLQYDVQQDEyZEAWdpQ2VydCBTSEEyIEhpZjZl
dXJhbmNlIFN1cnZ1ciBDQTAeFw0xNjA0MDYwMDAwMDBaFw0xOTA0MTEyMj
AUBGqNVBAW...MwEQYDV...DYWxpZm9u...TWEAYDVI
bjYKw/. . . . .Q9B4VMs. . . . .OfSix4z. . . . .60kCixL.
ZCjWEcJOKT9ilagTx2Zyf0WCIOzhUmdNiwjSNPgLXFF5S4yUN0MMio/8yI
c9NchYmHqDOWHBoRtSYz4ZduKmYBJK2VylksBiuLIK0k9qhJKckhO+p96:
fjnSVrKhhYNojU/qlgQtBf9Qa1gpj3Q54DSchiZH
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIEsTCCA5mgAwIBAgIQBOHnpNxc8vNtwCtCuF0VnzANBgkqhkiG9w0BAQ
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVI
d3cuZGlnaWN1cnQuY29tMSswKQYDVQQDEyJEAWdpQ2VydCB1aWdoIEFzc:
ZSBFViBSb290IENBMB4XDTEzMTAyMjEyMDAwMFoXDTE0MTAyMjEyMDAwM

```

Le nouveau format place toutes les informations de certificat sur une seule ligne avec des caractères de saut de ligne intégrés. Si vous disposez d'un certificat intermédiaire, convertissez ce certificat en format sur une seule ligne et ajoutez-le au premier certificat pour que les deux se trouvent sur la même ligne.

Vous pouvez maintenant configurer des certificats pour Unified Access Gateway à l'aide de ces fichiers .pem avec les scripts PowerShell joints à l'article de blog « Using PowerShell to Deploy VMware United Access Gateway » (Utilisation de PowerShell pour déployer VMware United Access Gateway), disponible sur la page <https://communities.vmware.com/docs/DOC-30835>. Vous pouvez également créer et utiliser une demande JSON pour configurer le certificat.

Suivant

Si vous avez converti un certificat de serveur TLS/SSL, reportez-vous à la section « [Remplacer le certificat de serveur TLS/SSL par défaut pour Unified Access Gateway](#) », page 58. Pour les certificats de carte à puce, reportez-vous à la section « [Configuration de l'authentification par certificat ou carte à puce sur le dispositif Unified Access Gateway](#) », page 61.

Remplacer le certificat de serveur TLS/SSL par défaut pour Unified Access Gateway

Pour stocker un certificat de serveur TLS/SSL signé par une autorité de certification approuvée sur le dispositif Unified Access Gateway, vous devez convertir le certificat au bon format et utiliser l'interface utilisateur d'administration ou les scripts PowerShell pour configurer le certificat.

Pour les environnements de production, VMware vous recommande de remplacer le certificat par défaut dès que possible. Le certificat de serveur TLS/SSL par défaut qui est généré lorsque vous déployez un dispositif Unified Access Gateway n'est pas signé par une autorité de certification approuvée.

IMPORTANT Utilisez également cette procédure pour remplacer périodiquement un certificat qui a été signé par une autorité de certification approuvée avant que le certificat expire, ce qui peut se produire tous les deux ans.

Cette procédure décrit comment utiliser l'API REST pour remplacer le certificat.

Prérequis

- Sauf si vous disposez déjà d'un certificat de serveur TLS/SSL valide et de sa clé privée, obtenez un nouveau certificat signé auprès d'une autorité de certification. Lorsque vous générez une demande de signature de certificat (CSR) pour obtenir un certificat, vérifiez qu'une clé privée est également générée. Ne générez pas de certificats pour des serveurs à l'aide d'une valeur KeyLength inférieure à 1 024.

Pour générer la CSR, vous devez connaître le nom de domaine complet (FQDN) que les périphériques client utiliseront pour se connecter au dispositif Unified Access Gateway, ainsi que l'unité d'organisation, l'entreprise, la ville, l'état et le pays pour remplir le nom de l'objet.

- Convertissez le certificat en fichiers au format PEM et convertissez les fichiers .pem au format sur une seule ligne. Reportez-vous à la section « [Convertir des fichiers de certificat au format PEM sur une ligne](#) », page 56.

Procédure

- 1 Dans la section Configurer manuellement de l'interface utilisateur d'administration, cliquez sur Sélectionner.
- 2 Dans Paramètres avancés > Paramètres du certificat de serveur TLS, cliquez sur l'icône d'engrenage.
- 3 Cliquez sur **Sélectionner** pour la clé privée et accédez au fichier de clé privée. Cliquez sur **Ouvrir** pour télécharger le fichier.
- 4 Cliquez sur **Sélectionner** pour la chaîne de certificats et accédez au fichier de certificat. Cliquez sur **Ouvrir** pour télécharger le fichier.
- 5 Cliquez sur **Enregistrer**.

Si le certificat est accepté, un message de réussite s'affiche.

Suivant

Si l'autorité de certification qui a signé le certificat n'est pas reconnue, configurez les clients pour qu'ils approuvent les certificats racine et intermédiaires.

Modifier les protocoles de sécurité et les suites de chiffrement utilisés pour la communication TLS ou SSL

Même si, dans quasiment tous les cas, les paramètres par défaut n'ont pas à être modifiés, vous pouvez configurer les protocoles de sécurité et les algorithmes cryptographiques qui sont utilisés pour chiffrer les communications entre les clients et le dispositif Unified Access Gateway.

Le paramètre par défaut inclut des suites de chiffrement qui utilisent le chiffrement AES sur 128 bits ou 256 bits, à l'exception des algorithmes DH anonymes, et les trie par niveau de sécurité. Par défaut, TLS v1.1 et TLS v1.2 sont activés. TLS v1.0 et SSL v3.0 sont désactivés.

Prérequis

- Familiarisez-vous avec l'API REST Unified Access Gateway. La spécification de cette API est disponible à l'adresse suivante sur la machine virtuelle sur laquelle Unified Access Gateway est installé : <https://access-point-appliance.example.com:9443/rest/swagger.yaml>.
- Familiarisez-vous avec les propriétés spécifiques relatives à la configuration des suites de chiffrement et des protocoles : `cipherSuites`, `ssl30Enabled`, `tls10Enabled`, `tls11Enabled` et `tls12Enabled`.

Procédure

- 1 Créez une demande JSON pour spécifier les protocoles et les suites de chiffrement à utiliser.

L'exemple suivant a les paramètres par défaut.

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

- 2 Utilisez un client REST, tel que `curl` ou `postman`, pour utiliser la demande JSON afin d'appeler l'API REST Unified Access Gateway et configurer les protocoles et les suites de chiffrement.

Dans l'exemple, *access-point-appliance.example.com* est le nom de domaine complet du dispositif Unified Access Gateway.

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

ciphers.json est la demande JSON que vous avez créée à l'étape précédente.

Les suites de chiffrement et les protocoles que vous avez spécifiés sont utilisés.

Configuration de l'authentification dans la zone DMZ

6

Lors du déploiement initial d'Unified Access Gateway, l'authentification par mot de passe Active Directory est configurée comme méthode par défaut. Les utilisateurs entrent leur nom d'utilisateur et mot de passe Active Directory, et ces informations d'identification sont envoyées via un système principal en vue de leur authentification.

Vous pouvez configurer le service Unified Access Gateway pour qu'il effectue l'authentification par certificat/carte à puce, l'authentification RSA SecurID, l'authentification RADIUS et l'authentification RSA Adaptive.

REMARQUE L'authentification par mot de passe avec Active Directory est la seule méthode d'authentification pouvant être utilisée avec un déploiement AirWatch.

Ce chapitre aborde les rubriques suivantes :

- [« Configuration de l'authentification par certificat ou carte à puce sur le dispositif Unified Access Gateway », page 61](#)
- [« Configurer l'authentification RSA SecurID dans Unified Access Gateway », page 65](#)
- [« Configuration de RADIUS pour Unified Access Gateway », page 66](#)
- [« Configuration de RSA Adaptive Authentication dans Unified Access Gateway », page 68](#)
- [« Générer des métadonnées SAML Unified Access Gateway », page 70](#)

Configuration de l'authentification par certificat ou carte à puce sur le dispositif Unified Access Gateway

Vous pouvez configurer l'authentification par certificat x509 dans Unified Access Gateway afin de permettre aux clients de s'authentifier avec des certificats sur leur poste de travail et périphériques mobiles ou d'utiliser un adaptateur de carte à puce pour l'authentification.

L'authentification par certificat est basée sur ce que possède l'utilisateur (la clé privée ou la carte à puce) et sur ce que la personne connaît (le mot de passe de la clé privée ou le code PIN de la carte à puce).

L'authentification par carte à puce fournit une authentification à deux facteurs en vérifiant à la fois ce que la personne a (la carte à puce) et ce qu'elle sait (le code PIN). Les utilisateurs finaux peuvent utiliser des cartes à puce pour ouvrir une session sur un système d'exploitation de poste de travail View distant et pour accéder à des applications compatibles avec les cartes à puce, telles qu'une application de messagerie électronique qui utilise le certificat pour signer des e-mails afin de prouver l'identité de l'expéditeur.

Avec cette fonctionnalité, l'authentification par certificat ou carte à puce est effectuée sur la base du service Unified Access Gateway. Unified Access Gateway utilise une assertion SAML pour communiquer des informations relatives au certificat X.509 de l'utilisateur final et le code PIN de la carte à puce à Horizon Server.

Vous pouvez configurer le contrôle de la révocation des certificats pour empêcher les utilisateurs dont les certificats d'utilisateur sont révoqués de s'authentifier. Les certificats sont souvent révoqués lorsqu'un utilisateur quitte une entreprise, perd une carte à puce ou passe d'un service à un autre. Le contrôle de la révocation des certificats à l'aide de listes de révocation de certificats (CRL) et du protocole OCSP est pris en charge. Une CRL est une liste de certificats révoqués publiée par l'autorité de certification qui a émis les certificats. OCSP est un protocole de validation des certificats utilisé pour obtenir le statut de révocation d'un certificat.

Il est possible de configurer la CRL et OCSP en configurant le même adaptateur d'authentification par certificat. Lorsque vous configurez les deux types de contrôle de révocation des certificats et que la case Utiliser la CRL en cas de défaillance d'OCSP est cochée, OCSP est contrôlé en premier et, s'il échoue, le contrôle de la révocation est effectué par la CRL. Le contrôle de la révocation ne revient pas à OCSP en cas d'échec de la CRL.

Vous pouvez également configurer l'authentification afin qu'Unified Access Gateway requière l'authentification par carte à puce, mais l'authentification est alors également transmise au serveur, ce qui peut nécessiter l'authentification Active Directory.

REMARQUE Pour VMware Identity Manager, l'authentification transite toujours par Unified Access Gateway vers le service VMware Identity Manager. Vous pouvez configurer l'authentification par carte à puce pour qu'elle soit exécutée sur le dispositif Unified Access Gateway uniquement si Unified Access Gateway est utilisé avec Horizon 7.

Configurer l'authentification par certificat sur Unified Access Gateway

Vous activez et configurez l'authentification par certificat dans la console d'administration d'Unified Access Gateway.

Prérequis

- Obtenez les certificats racines et intermédiaires auprès de l'autorité de certification ayant signé les certificats présentés par vos utilisateurs. Reportez-vous à la section « [Obtenir des certificats d'autorités de certification](#) », page 64.
- Vérifiez que les métadonnées SAML d'Unified Access Gateway sont ajoutées au fournisseur de services et que les métadonnées SAML du fournisseur de services sont copiées dans le dispositif Unified Access Gateway.
- (Facultatif) Une liste des identificateurs d'objets (OID) des stratégies de certificat valides pour l'authentification par certificat.
- Pour le contrôle de la révocation, l'emplacement du fichier du CRL et l'URL du serveur OCSP.
- (Facultatif) L'emplacement du fichier de la signature du certificat de la réponse OCSP.
- Le contenu du formulaire de consentement, si un tel formulaire s'affiche avant l'authentification.

Procédure

- 1 Dans la section Configuration manuelle de l'interface utilisateur d'administration, cliquez sur **Sélectionner**.
- 2 Dans Paramètres généraux, section Paramètres d'authentification, cliquez sur **Afficher**.
- 3 Cliquez sur l'engrenage dans la ligne du certificat X.509.

4 Configurez le formulaire du certificat X.509.

Les zones de texte obligatoires sont indiquées par un astérisque. Toutes les autres zones de texte sont facultatives.

Option	Description
Activer le certificat X.509	Remplacez NO par YES pour activer l'authentification par certificat.
*Nom	Attribuez un nom à cette méthode d'authentification.
*Certificats d'autorité de certification racine et intermédiaire	Cliquez sur Sélectionner pour sélectionner les fichiers de certificat à télécharger. Il est possible de sélectionner plusieurs certificats d'autorité de certification racine et intermédiaire qui utilisent l'encodage DER ou PEM.
Taille du cache CRL	Entrez la taille du cache de la liste de révocation de certificats. La valeur par défaut est 100.
Activer la révocation de certificat	Remplacez NO par YES pour activer le contrôle de révocation de certificat. Le contrôle de la révocation empêche les utilisateurs dont les certificats d'utilisateur sont révoqués de s'authentifier.
Utiliser la CRL des certificats	Cochez cette case pour utiliser la liste de révocation de certificats (CRL) publiée par l'autorité de certification qui a émis les certificats afin de valider le statut d'un certificat, révoqué ou non révoqué.
Emplacement de la CRL	Entrez le chemin d'accès au fichier de serveur ou local depuis lequel la CRL peut être récupérée.
Autoriser la révocation OCSP	Cochez la case pour utiliser le protocole de validation des certificats OCSP (Online Certificate Status Protocol) afin d'obtenir le statut de révocation d'un certificat.
Utiliser la CRL en cas de défaillance d'OCSP	Si vous configurez une CRL et OCSP, vous pouvez sélectionner cette zone pour basculer vers l'utilisation de la CRL si le contrôle OCSP n'est pas disponible.
Envoyer une valeur à usage unique OCSP	Cochez cette case si vous souhaitez que l'identificateur unique de la demande OCSP soit envoyée dans la réponse.
URL d'OCSP	Si vous avez activé la révocation OCSP, entrez l'adresse de serveur OCSP pour le contrôle de la révocation.
Certificat de signature du répondeur OCSP	Entrez le chemin du certificat OCSP pour le répondeur, <i>/path/to/file.cer</i> .
Activer le formulaire de consentement avant l'authentification	Cochez cette case pour inclure une page du formulaire de consentement qui s'affiche avant que les utilisateurs se connectent à leur portail Workspace ONE à l'aide de l'authentification par certificat.
Contenu du formulaire de consentement	Tapez ici le texte à afficher dans le formulaire de consentement.

5 Cliquez sur **Enregistrer**.**Suivant**

Lorsque l'authentification par certificat X.509 est configurée et que le dispositif Unified Access Gateway est configuré derrière un équilibrage de charge, assurez-vous qu'Unified Access Gateway est configuré avec une émulation SSL au niveau de l'équilibrage de charge et qu'il n'est pas configuré pour mettre fin à SSL au niveau de l'équilibrage de charge. Cette configuration permet de s'assurer que la négociation SSL a lieu entre Unified Access Gateway et le client afin de transmettre le certificat à Unified Access Gateway.

Obtenir des certificats d'autorités de certification

Vous devez obtenir tous les certificats d'autorités de certification applicables pour tous les certificats d'utilisateurs de confiance des cartes à puces présentées par vos utilisateurs et administrateurs. Ces certificats incluent des certificats racines et peuvent inclure des certificats intermédiaires si le certificat de carte à puce de l'utilisateur a été délivré par une autorité de certification intermédiaire.

Si vous ne disposez pas du certificat racine ou intermédiaire de l'autorité de certification qui a signé les certificats sur les cartes à puce présentées par vos utilisateurs et administrateurs, vous pouvez exporter les certificats à partir des certificats d'utilisateurs signés par une autorité de certification ou d'une carte à puce qui en contient un. Reportez-vous à la section « [Obtenir le certificat d'une autorité de certification de Windows](#) », page 64.

Procédure

- ◆ Obtenez les certificats d'autorités de certification à partir de l'une des sources suivantes.
 - Un serveur Microsoft IIS exécutant les services de certificats Microsoft. Pour plus d'informations sur l'installation de Microsoft IIS, l'émission des certificats et leur distribution dans votre entreprise, consultez le site Web Microsoft TechNet.
 - Le certificat racine public d'une autorité de certification approuvée. Il s'agit de la source la plus courante de certificat racine dans des environnements avec une infrastructure de carte à puce et une approche normalisée pour la distribution et l'authentification des cartes à puce.

Suivant

Ajoutez le certificat racine, le certificat intermédiaire ou les deux à un fichier du magasin d'approbations du serveur.

Obtenir le certificat d'une autorité de certification de Windows

Si vous disposez d'un certificat utilisateur signé par une autorité de certification ou d'une carte à puce en contenant un, et que Windows approuve le certificat racine, vous pouvez exporter ce dernier de Windows. Si l'émetteur du certificat de l'utilisateur est une autorité de certification intermédiaire, il est possible d'exporter ce certificat.

Procédure

- 1 Si le certificat utilisateur est sur une carte à puce, insérez la carte à puce dans le lecteur pour ajouter le certificat utilisateur à votre magasin personnel.

Si le certificat utilisateur n'apparaît pas dans votre magasin personnel, utilisez le logiciel du lecteur pour exporter le certificat utilisateur vers un fichier. Ce fichier est utilisé à l'étape 4 de cette procédure.

- 2 Dans Internet Explorer, sélectionnez **Outils > Options Internet**.
- 3 Sous l'onglet **Contenu**, cliquez sur **Certificats**.
- 4 Sous l'onglet **Personnel**, sélectionnez le certificat que vous voulez utiliser et cliquez sur **Affichage**.

Si le certificat utilisateur n'apparaît pas dans la liste, cliquez sur **Importer** pour l'importer manuellement à partir d'un fichier. Une fois le certificat importé, vous pouvez le sélectionner dans la liste.

- 5 Sous l'onglet **Chemin d'accès de certification**, sélectionnez le certificat en haut de l'arborescence et cliquez sur **Afficher le certificat**.

Si le certificat utilisateur est signé comme faisant partie d'une hiérarchie d'approbation, le certificat de signature peut être signé par un autre certificat de niveau plus élevé. Sélectionnez le certificat parent (celui qui est actuellement signé par le certificat utilisateur) comme votre certificat racine. Dans certains cas, l'émetteur peut être une autorité de certification intermédiaire.

- 6 Sous l'onglet **Détails**, cliquez sur **Copier dans un fichier**.
L'assistant Certificate Export (Exportation de certificat) apparaît.
- 7 Cliquez sur **Suivant** > **Suivant**, puis tapez un nom et un emplacement pour le fichier à exporter.
- 8 Cliquez sur **Suivant** pour enregistrer le fichier comme certificat racine dans l'emplacement spécifié.

Suivant

Ajoutez le certificat de l'autorité de certification à un fichier du magasin d'approbations du serveur.

Configurer l'authentification RSA SecurID dans Unified Access Gateway

Une fois le dispositif Unified Access Gateway configuré en tant qu'agent d'authentification sur le serveur RSA SecurID, vous devez ajouter les informations de configuration RSA SecureID au dispositif Unified Access Gateway.

Prérequis

- Vérifiez que RSA Authentication Manager (serveur RSA SecurID) est installé et correctement configuré.
- Téléchargez le fichier compressé sdconf.rec depuis le serveur RSA SecurID et extrayez le fichier de configuration du serveur.

Procédure

- 1 Dans la section Configuration manuelle de l'interface utilisateur d'administration, cliquez sur **Sélectionner**.
- 2 Dans Paramètres généraux, section Paramètres d'authentification, cliquez sur **Afficher**.
- 3 Cliquez sur l'engrenage dans la ligne RSA SecurID.
- 4 Configurez la page RSA SecurID.

Les informations utilisées et les fichiers générés sur le serveur RSA SecurID sont nécessaires lors de la configuration de la page SecurID.

Option	Action
Activer RSA SecurID	Remplacez NO par YES pour activer l'authentification SecurID.
*Nom	Le nom est securid-auth.
*Nombre d'itérations	Entrez le nombre de tentatives d'authentification autorisées. Il s'agit du nombre maximal d'échecs de tentatives de connexion à l'aide du jeton RSA SecurID. La valeur par défaut est de 5 tentatives. REMARQUE Lorsque plusieurs annuaires sont configurés et que vous implémentez l'authentification RSA SecurID avec des annuaires supplémentaires, configurez Nombre de tentatives d'authentification autorisées avec la même valeur pour chaque configuration RSA SecurID. Si la valeur est différente, l'authentification SecurID échoue.
*Nom d'HÔTE externe	Entrez l'adresse IP de l'instance Unified Access Gateway. La valeur que vous entrez doit correspondre à la valeur que vous avez utilisée lorsque vous avez ajouté le dispositif Unified Access Gateway en tant qu'agent d'authentification au serveur RSA SecurID.
*Nom d'HÔTE interne	Entrez la valeur attribuée à l'invite Adresse IP sur le serveur RSA SecurID.

Option	Action
*Configuration du serveur	Cliquez sur Modifier pour télécharger le fichier de configuration du serveur RSA SecurID. Vous devez d'abord télécharger le fichier compressé auprès du serveur RSA SecurID, puis extraire le fichier de configuration du serveur qui est appelé par défaut <code>sdconf.rec</code> .
*Suffixe d'ID de nom	Entrez le <code>nameId</code> qui permet à View d'offrir une expérience TrueSSO.

Configuration de RADIUS pour Unified Access Gateway

Vous pouvez configurer Unified Access Gateway de manière à obliger les utilisateurs à utiliser l'authentification RADIUS. Vous configurez les informations du serveur RADIUS sur le dispositif Unified Access Gateway.

La prise en charge de RADIUS offre une large gamme d'autres options d'authentification à deux facteurs basée sur des jetons. Comme les solutions d'authentification à deux facteurs, telles que RADIUS, fonctionnent avec des gestionnaires d'authentification installés sur des serveurs séparés, le serveur RADIUS doit être configuré et accessible par le service Identity Manager.

Lorsque les utilisateurs se connectent et que l'authentification RADIUS est activée, une boîte de dialogue de connexion spéciale apparaît dans le navigateur. Les utilisateurs entrent leur nom d'utilisateur et leur code secret d'authentification RADIUS dans la boîte de dialogue de connexion. Si le serveur RADIUS émet un challenge d'accès, Unified Access Gateway affiche une boîte de dialogue demandant un second code secret. Actuellement la prise en charge des challenges RADIUS est limitée à une invite d'entrée de texte.

Une fois que l'utilisateur a entré ses informations d'identification dans la boîte de dialogue, le serveur RADIUS peut envoyer un SMS ou un e-mail, ou du texte à l'aide d'un autre mécanisme hors bande sur le téléphone portable de l'utilisateur avec un code. L'utilisateur peut entrer ce texte et le code dans la boîte de dialogue de connexion pour terminer l'authentification.

Si le serveur RADIUS permet d'importer des utilisateurs depuis Active Directory, les utilisateurs finaux peuvent d'abord être invités à fournir des informations d'identification Active Directory avant d'être invités à fournir un nom d'utilisateur et un code secret d'authentification RADIUS.

Configuration de l'authentification RADIUS

Sur le dispositif Unified Access Gateway, vous devez activer l'authentification RADIUS, entrer les paramètres de configuration à partir du serveur RADIUS et définir le type d'authentification sur RADIUS.

Prérequis

- Vérifiez que le logiciel RADIUS est installé et configuré sur le serveur à utiliser comme serveur gestionnaire d'authentification. Configurez le serveur RADIUS, puis configurez les demandes RADIUS à partir d'Unified Access Gateway. Pour plus d'informations sur la configuration du serveur RADIUS, consultez les guides de configuration du fournisseur RADIUS.

Les informations de serveur RADIUS suivantes sont requises.

- Adresse IP ou nom DNS du serveur RADIUS.
- Numéros de port d'authentification. En général, le port d'authentification est le port 1812.
- Type d'authentification. Les types d'authentification incluent PAP (Password Authentication Protocol), CHAP (Challenge Handshake Authentication Protocol), MSCHAP1, MSCHAP2 (Microsoft Challenge Handshake Authentication Protocol, versions 1 et 2).
- Code secret partagé RADIUS utilisé pour le chiffrement et le déchiffrement dans les messages de protocole RADIUS.
- Valeurs du délai d'expiration et de nouvelle tentative nécessaires pour l'authentification RADIUS

Procédure

- 1 Dans la section Configuration manuelle de l'interface utilisateur d'administration, cliquez sur **Sélectionner**.
- 2 Dans Paramètres généraux, section Paramètres d'authentification, cliquez sur **Afficher**.
- 3 Cliquez sur l'engrenage dans la ligne RADIUS.

Option	Action
Activer RADIUS	Remplacez NO par YES pour activer l'authentification RADIUS.
Nom*	Le nom est radius-auth
Type d'authentification*	Entrez le protocole d'authentification pris en charge par le serveur RADIUS. PAP, CHAP, MSCHAP1 ou MSCHAP2.
Secret partagé*	Entrez le secret partagé RADIUS.
Nombre de tentatives d'authentification autorisées*	Entrez le nombre maximal de tentatives de connexion échouées lorsque vous utilisez RADIUS pour vous connecter. La valeur par défaut est de trois tentatives.
Nombre de tentatives sur le serveur RADIUS*	Spécifiez le nombre total de nouvelles tentatives. Si le serveur principal ne répond pas, le service attend le temps configuré avant de réessayer.
Délai d'attente du serveur en secondes*	Entrez le délai d'attente du serveur RADIUS en secondes, après lequel une nouvelle tentative est envoyée si le serveur RADIUS ne répond pas.
Nom d'hôte du serveur RADIUS*	Entrez le nom de l'hôte ou l'adresse IP du serveur RADIUS.
Port d'authentification*	Entrez le numéro de port d'authentification Radius. En général, il s'agit du port 1812.
Préfixe de domaine	(Facultatif) L'emplacement du compte d'utilisateur est appelé le domaine. Si vous spécifiez une chaîne de préfixe du domaine, la chaîne est placée au début du nom d'utilisateur lorsque le nom est envoyé au serveur RADIUS. Par exemple, si le nom d'utilisateur entré est jdoe et que le préfixe de domaine DOMAIN-A\ est spécifié, le nom d'utilisateur DOMAIN-A\jdoe est envoyé au serveur RADIUS. Si vous ne configurez pas ces champs, seul le nom d'utilisateur qui est entré est envoyé.
Suffixe de domaine	(Facultatif) Si vous configurez un suffixe du domaine, la chaîne est placée à la fin du nom d'utilisateur. Par exemple, si le suffixe est @myco.com, le nom d'utilisateur jdoe@myco.com est envoyé au serveur RADIUS.
Suffixe d'ID de nom	Entrez le nameId qui permet à View d'offrir une expérience True SSO.
Conseil de phrase secrète de la page de connexion	Entrez la chaîne de texte à afficher dans le message sur la page de connexion utilisateur pour demander aux utilisateurs d'entrer le bon code secret Radius. Par exemple, si ce champ est configuré avec Mot de passe AD en premier, puis code secret SMS , le message sur la page de connexion serait Entrez d'abord votre mot de passe AD, puis le code secret SMS . La chaîne de texte par défaut est RADIUS Passcode .
Activer le serveur secondaire	Remplacez NO par YES pour configurer un serveur RADIUS secondaire en vue d'une haute disponibilité. Configurez les informations du serveur secondaire comme décrit à l'étape 3.

- 4 Cliquez sur **Enregistrer**.

Configuration de RSA Adaptive Authentication dans Unified Access Gateway

RSA Adaptive Authentication peut être implémenté pour offrir une authentification multifacteur plus forte que l'authentification par nom d'utilisateur et mot de passe avec Active Directory. Adaptive Authentication surveille et authentifie les tentatives de connexion des utilisateurs selon des niveaux de risque et des stratégies.

Lorsqu'Adaptive Authentication est activé, les indicateurs de risque spécifiés dans les stratégies de risque configurées dans l'application RSA Policy Management et la configuration d'Adaptive Authentication dans Unified Access Gateway sont utilisés pour déterminer si un utilisateur est authentifié avec un nom d'utilisateur et un mot de passe ou si des informations supplémentaires sont nécessaires pour authentifier l'utilisateur.

Méthodes d'authentification prises en charge de RSA Adaptive Authentication

Les méthodes d'authentification forte de RSA Adaptive Authentication prises en charge dans Unified Access Gateway sont une authentification hors bande par téléphone, e-mail ou SMS et des questions de sécurité. Vous activez sur le service les méthodes de RSA Adaptive Authentication pouvant être fournies. Les stratégies de RSA Adaptive Authentication déterminent si une méthode d'authentification secondaire est nécessaire.

L'authentification hors bande est un processus qui nécessite l'envoi d'une vérification supplémentaire en complément du nom d'utilisateur et du mot de passe. Lorsque des utilisateurs s'inscrivent sur le serveur RSA Adaptive Authentication, ils fournissent une adresse e-mail, un numéro de téléphone, ou les deux, en fonction de la configuration du serveur. Lorsqu'une vérification supplémentaire est requise, le serveur RSA Adaptive Authentication envoie un code secret unique par le canal fourni. Les utilisateurs entrent ce code secret, ainsi que leur nom d'utilisateur et leur mot de passe.

Les questions de stimulation requièrent que l'utilisateur réponde à une série de questions lorsqu'il s'inscrit sur le serveur RSA Adaptive Authentication. Vous pouvez configurer le nombre de questions d'inscription à poser et le nombre de questions de sécurité à présenter sur la page de connexion.

Inscription d'utilisateurs avec le serveur RSA Adaptive Authentication

Les utilisateurs doivent être provisionnés dans la base de données RSA Adaptive Authentication pour pouvoir utiliser Adaptive Authentication pour l'authentification. Les utilisateurs sont ajoutés à la base de données RSA Adaptive Authentication la première fois qu'ils se connectent avec leur nom d'utilisateur et leur mot de passe. En fonction de la façon dont vous avez configuré RSA Adaptive Authentication dans le service, lorsque les utilisateurs se connectent, il peut leur être demandé de fournir leur adresse e-mail, leur numéro de téléphone, leur numéro de service de messagerie texte (SMS) ou de répondre à des questions de sécurité.

REMARQUE RSA Adaptive Authentication n'autorise pas les caractères internationaux dans les noms d'utilisateur. Si vous prévoyez d'autoriser les caractères multioctet dans les noms d'utilisateur, contactez le support RSA pour configurer RSA Adaptive Authentication et RSA Authentication Manager.

Configurer RSA Adaptive Authentication dans Unified Access Gateway

Pour configurer RSA Adaptive Authentication sur le service, activez RSA Adaptive Authentication, sélectionnez les méthodes d'authentification adaptative à appliquer et ajoutez les informations de connexion et le certificat Active Directory.

Prérequis

- RSA Adaptive Authentication correctement configuré avec les méthodes d'authentification à utiliser pour l'authentification secondaire.
- Détails sur l'adresse de point de terminaison SOAP et le nom d'utilisateur SOAP.
- Informations de configuration Active Directory et certificat SSL Active Directory disponibles.

Procédure

- 1 Dans la section Configuration manuelle de l'interface utilisateur d'administration, cliquez sur **Sélectionner**.
- 2 Dans Paramètres généraux, section Paramètres d'authentification, cliquez sur **Afficher**.
- 3 Cliquez sur l'engrenage dans la ligne RSA Adaptive Authentication.
- 4 Sélectionnez les paramètres appropriés pour votre environnement.

REMARQUE Les champs obligatoires sont indiqués par un astérisque. Les autres champs sont facultatifs.

Option	Description
Activer l'adaptateur RSA AA	Remplacez NO par YES pour activer RSA Adaptive Authentication.
Nom*	Le nom est rsaaa-auth.
Point de terminaison SOAP*	Entrez l'adresse du point de terminaison SOAP pour l'intégration entre l'adaptateur RSA Adaptive Authentication et le service.
Nom d'utilisateur SOAP*	Entrez le nom d'utilisateur et le mot de passe utilisés pour signer des messages SOAP.
Mot de passe SOAP*	Entrez le mot de passe SOAP API pour RSA Adaptive Authentication.
Domaine RSA	Entrez l'adresse de domaine du serveur Adaptive Authentication.
Activer l'e-mail OOB	Sélectionnez YES pour activer l'authentification hors bande qui envoie un code secret unique à l'utilisateur final par le biais d'un e-mail.
Activer le SMS OOB	Sélectionnez YES pour activer l'authentification hors bande qui envoie un code secret unique à l'utilisateur final par le biais d'un SMS.
Activer SecurID	Sélectionnez YES pour activer SecurID. Les utilisateurs sont invités à entrer leur jeton et leur code secret RSA.
Activer la question secrète	Sélectionnez YES pour utiliser des questions d'inscription et de sécurité pour l'authentification.
Nombre de questions d'inscription*	Entrez le nombre de questions que l'utilisateur devra configurer lorsqu'il s'inscrit sur le serveur de l'adaptateur d'authentification.
Nombre de questions de sécurité*	Entrez le nombre de questions de sécurité auxquelles les utilisateurs doivent répondre correctement pour se connecter.
Nombre de tentatives d'authentification autorisées*	Entrez le nombre de fois que les questions de sécurité seront affichées à un utilisateur essayant de se connecter avant que l'authentification échoue.
Type d'annuaire*	Le seul annuaire pris en charge est Active Directory.
Utiliser SSL	Sélectionnez YES si vous utilisez SSL pour la connexion à l'annuaire. Vous ajoutez le certificat SSL Active Directory dans le champ Certificat de l'annuaire.
Hôte du serveur*	Entrez le nom d'hôte Active Directory.

Option	Description
Port du serveur	Entrez le numéro de port Active Directory.
Utiliser l'emplacement de service DNS	Sélectionnez YES si l'emplacement du service DNS est utilisé pour la connexion à l'annuaire.
ND de base	Saisissez le ND à partir duquel effectuer les recherches de compte. Par exemple : OU=myUnit,DC=myCorp,DC=com.
Nom unique de liaison*	Entrez le compte pouvant rechercher des utilisateurs. Par exemple : CN=binduser,OU=myUnit,DC=myCorp,DC=com.
Mot de passe de liaison	Entrez le mot de passe du compte ND Bind.
Attribut de recherche	Entrez l'attribut du compte contenant le nom d'utilisateur.
Certificat de l'annuaire	Pour établir des connexions SSL sécurisées, ajoutez le certificat du serveur d'annuaire dans la zone de texte. S'il existe plusieurs serveurs, ajoutez le certificat racine de l'autorité de certification.
Utiliser STARTTLS	Remplacez NO par YES pour utiliser STARTTLS.

- 5 Cliquez sur **Enregistrer**.

Générer des métadonnées SAML Unified Access Gateway

Vous devez générer des métadonnées SAML sur le dispositif Unified Access Gateway et échanger des métadonnées avec le serveur afin d'établir l'approbation mutuelle requise pour l'authentification par carte à puce.

Le langage SAML (Security Assertion Markup Language) est une norme XML utilisée pour décrire et échanger des informations d'authentification et d'autorisation entre différents domaines de sécurité. SAML transmet des informations sur les utilisateurs entre les fournisseurs d'identité et les fournisseurs de services dans des documents XML nommés assertions SAML. Dans ce scénario, Unified Access Gateway est le fournisseur d'identité et le serveur est le fournisseur de services.

Prérequis

- Configurez l'horloge (UTC) sur le dispositif Unified Access Gateway pour qu'il soit à l'heure exacte. Par exemple, ouvrez une fenêtre de console sur la machine virtuelle Unified Access Gateway et utilisez les flèches pour sélectionner le bon fuseau horaire. De plus, vérifiez que l'heure de l'hôte ESXi est synchronisée avec un serveur NTP. Vérifiez que VMware Tools, qui est exécuté dans la machine virtuelle de dispositif, synchronise l'heure sur la machine virtuelle avec celle sur l'hôte ESXi.

IMPORTANT Si l'heure sur le dispositif Unified Access Gateway ne correspond pas à l'heure sur l'hôte du serveur, il est possible que l'authentification par carte à puce ne fonctionne pas.

- Obtenez un certificat de signature SAML que vous pouvez utiliser pour signer les métadonnées Unified Access Gateway.

REMARQUE VMware vous recommande de créer et d'utiliser un certificat de signature SAML spécifique lorsque vous avez plusieurs dispositifs Unified Access Gateway dans votre configuration. Dans ce cas, tous les dispositifs doivent être configurés avec le même certificat de signature pour que le serveur puisse accepter les assertions de n'importe quel dispositif Unified Access Gateway. Avec un certificat de signature SAML spécifique, les métadonnées SAML de tous les dispositifs sont identiques.

- Si vous ne l'avez pas déjà fait, convertissez le certificat de signature SAML en fichiers au format PEM et convertissez les fichiers .pem au format sur une seule ligne. Reportez-vous à la section « [Convertir des fichiers de certificat au format PEM sur une ligne](#) », page 56.

Procédure

- 1 Dans la section Configuration manuelle de l'interface utilisateur d'administration, cliquez sur **Sélectionner**.

- 2 Dans la section Paramètres avancés, cliquez sur l'icône en forme d'engrenage **Paramètres du fournisseur d'identité SAML**.
- 3 Activez la case à cocher **Fournir un certificat**.
- 4 Pour ajouter le fichier de clé privée, cliquez sur **Sélectionner** et accédez au fichier de clé privée du certificat.
- 5 Pour ajouter le fichier de chaîne de certificat, cliquez sur **Sélectionner** et accédez au fichier de chaîne de certificat.
- 6 Cliquez sur **Enregistrer**.
- 7 Dans la zone de texte Nom d'hôte, entrez le nom d'hôte et téléchargez les paramètres du fournisseur d'identité.

Création d'un authentificateur SAML utilisé par d'autres fournisseurs de services

Après avoir généré des métadonnées SAML sur le dispositif Unified Access Gateway, vous pouvez copier ces données sur le fournisseur de services principal. La copie de ces données sur le fournisseur de services fait partie du processus de création d'un authentificateur SAML pour qu'Unified Access Gateway puisse être utilisé en tant que fournisseur d'identité.

Pour un serveur Horizon Cloud, consultez la documentation du produit afin d'obtenir des instructions spécifiques.

Copier les métadonnées SAML du fournisseur de services sur Unified Access Gateway

Après avoir créé et activé un authentificateur SAML pour qu'Unified Access Gateway puisse être utilisé comme fournisseur d'identité, vous pouvez générer des métadonnées SAML sur le système principal et les utiliser pour créer un fournisseur de services sur le dispositif Unified Access Gateway. Cet échange de données établit l'approbation entre le fournisseur d'identité (Unified Access Gateway) et le fournisseur de services principal, tel que le Serveur de connexion View.

Prérequis

Vérifiez que vous avez créé un authentificateur SAML pour Unified Access Gateway sur le serveur du fournisseur de services principal.

Procédure

- 1 Récupérez les métadonnées SAML du fournisseur de services, qui prennent généralement la forme d'un fichier XML.

Pour obtenir des instructions, consultez la documentation du fournisseur de services.

Les fournisseurs de services ont des procédures différentes. Par exemple, vous devez ouvrir un navigateur et entrer une URL telle que : `https://connection-server.example.com/SAML/metadata/sp.xml`

Vous pouvez ensuite utiliser une commande **Enregistrer sous** pour enregistrer la page Web en tant que fichier XML. Le contenu de ce fichier commence par le texte suivant :

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

- 2 Dans la section Configurer manuellement de l'interface utilisateur d'administration d'Unified Access Gateway, cliquez sur **Sélectionner**.
- 3 Dans la section Paramètres avancés, cliquez sur l'icône en forme d'engrenage **Paramètres du fournisseur de serveur SAML**.
- 4 Entrez le nom du fournisseur de services dans la zone de texte correspondante.

- 5 Dans la zone de texte Métadonnées XML, collez le fichier de métadonnées que vous avez créé à l'étape 1.
- 6 Cliquez sur **Enregistrer**.

Unified Access Gateway et le fournisseur de services peuvent maintenant échanger des informations d'authentification et d'autorisation.

Dépannage du déploiement d' Unified Access Gateway

7

Vous pouvez utiliser diverses procédures pour diagnostiquer et corriger des problèmes rencontrés lorsque vous déployez Unified Access Gateway dans votre environnement.

Vous pouvez utiliser des procédures de dépannage pour rechercher les causes de tels problèmes et essayer de les corriger vous-même, ou vous pouvez obtenir de l'aide du support technique de VMware.

Ce chapitre aborde les rubriques suivantes :

- « [Contrôle de la santé des services déployés](#) », page 73
- « [Dépannage des erreurs de déploiement](#) », page 74
- « [Collecte de journaux depuis le dispositif Unified Access Gateway](#) », page 75

Contrôle de la santé des services déployés

Vous pouvez voir rapidement que les services que vous avez déployés sont configurés, actifs et en cours d'exécution à partir de l'interface utilisateur d'administration pour Paramètres Edge.

Figure 7-1. Contrôle de santé



Un cercle s'affiche devant le service. Le code couleur est le suivant.

- Un cercle vide signifie que le paramètre n'est pas configuré.
- Un cercle rouge signifie que le service est inactif.
- Un cercle orange signifie que le service est exécuté partiellement.
- Un cercle vert signifie que le service est exécuté sans problème.

Dépannage des erreurs de déploiement

Vous pouvez rencontrer des difficultés lorsque vous déployez Unified Access Gateway dans votre environnement. Vous pouvez utiliser diverses procédures pour diagnostiquer et corriger des problèmes avec votre déploiement.

Avertissement de sécurité lors de l'exécution de scripts téléchargés depuis Internet

Vérifiez que le script PowerShell est celui que vous voulez exécuter, puis exécutez la commande suivante depuis la console PowerShell :

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

Commande ovftool introuvable

Vérifiez que vous avez installé le logiciel OVF Tool sur votre machine Windows et qu'il est installé à l'emplacement attendu par le script.

Réseau non valide dans la propriété netmask1

- Le message peut indiquer netmask0, netmask1 ou netmask2. Vérifiez qu'une valeur a été définie dans le fichier .INI pour chacun des trois réseaux, par exemple netInternet, netManagementNetwork et netBackendNetwork.
- Vérifiez qu'un profil de protocole de réseau vSphere a été associé à chaque nom de réseau référencé. Cela spécifie des paramètres réseau tels que le masque de sous-réseau IPv4, la passerelle, etc. Vérifiez que le profil de protocole réseau associé dispose des valeurs correctes pour chaque paramètre.

Message d'avertissement à propos de l'identifiant de système d'exploitation non pris en charge

Le message d'avertissement indique que l'identifiant de système d'exploitation spécifié de SUSE Linux Enterprise Server 12.0 64 bits (id:85) n'est pas pris en charge sur l'hôte sélectionné. Il est mappé vers l'identifiant de système d'exploitation suivant : Autre Linux (64 bits).

Ignorez ce message d'avertissement. Il est mappé vers un système d'exploitation pris en charge automatiquement.

Configurer Unified Access Gateway pour l'authentification RSA SecurID

Ajoutez les lignes suivantes à la section Horizon du fichier .INI.

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

Ajoutez une section en bas de votre fichier .INI.

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

Les deux adresses IP doivent être définies sur l'adresse IP d'Unified Access Gateway. Le fichier sdconf.rec est obtenu auprès de RSA Authentication Manager qui doit être complètement configuré. Vérifiez que vous utilisez Access Point 2.5 ou version ultérieure et que le serveur RSA Authentication Manager est accessible sur le réseau depuis Access Point. Réexécutez la commande Powershell apdeploy pour redéployer votre Access Point configuré pour RSA SecurID.

Le localisateur ne fait pas référence à une erreur d'objet

L'erreur indique que la valeur `target=` utilisée par vSphere OVF Tool n'est pas correcte pour votre environnement vCenter. Utilisez le tableau répertorié dans <https://communities.vmware.com/docs/DOC-30835> pour voir des exemples du format cible utilisé pour faire référence à un hôte ou un cluster vCenter. L'objet de premier niveau est spécifié comme suit :

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

L'objet indique désormais les noms possibles à utiliser au niveau suivant.

```
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
```

Les noms de dossier, d'hôte et de cluster utilisés dans la cible sont sensibles à la casse.

Collecte de journaux depuis le dispositif Unified Access Gateway

Téléchargez le fichier AP-Log Archive.zip depuis les paramètres de prise en charge dans l'interface utilisateur d'administration. Le fichier ZIP contient tous les journaux de votre dispositif Unified Access Gateway.

Définir le niveau de journalisation

Vous pouvez gérer les paramètres de niveau de journal à partir de l'interface utilisateur d'administration. Accédez à la page Paramètres de prise en charge et sélectionnez Paramètres de niveau de journal. Les niveaux de journal pouvant être générés sont INFO, AVERTISSEMENT, ERREUR et DÉBOGAGE. Le niveau de journalisation est défini par défaut sur INFO.

Voici une description du type d'informations que les niveaux de journal collectent.

Tableau 7-1. Niveaux de journalisation

Niveau	Type d'informations collectées
INFO	Le niveau INFO désigne les messages d'informations qui indiquent la progression du service.
ERREUR	Le niveau ERREUR désigne les événements d'erreur qui peuvent toujours autoriser l'exécution du service.
AVERTISSEMENT	Le niveau AVERTISSEMENT désigne les situations potentiellement dangereuses, mais qui sont normalement récupérables ou qui peuvent être ignorées.
DÉBOGAGE	Événements qui sont en général utiles pour déboguer des problèmes. Vous pouvez activer le mode de débogage afin d'afficher ou de modifier l'état interne du dispositif. Le mode de débogage vous permet de tester le scénario de déploiement dans votre environnement.

Collecter les journaux

Téléchargez les fichiers ZIP de journal dans la section Paramètres de prise en charge de l'interface utilisateur d'administration.

Ces fichiers journaux sont collectés depuis le répertoire `/opt/vmware/gateway/logs` sur le dispositif.

Les tableaux suivants contiennent des descriptions des divers fichiers inclus dans le fichier ZIP.

Tableau 7-2. Fichiers qui contiennent des informations système pour faciliter le dépannage

Nom de fichier	Description
df.log	Contient des informations sur l'utilisation de l'espace disque.
netstat.log	Contient des informations sur les connexions réseau.
ap_config.json	Contient les paramètres de configuration actuels du dispositif Unified Access Gateway.
ps.log	Inclut une liste de processus.
ifconfig.log	Contient des informations sur les interfaces réseau.
free.log	Contient des informations sur l'utilisation de la mémoire.

Tableau 7-3. Fichiers journaux d' Unified Access Gateway

Nom de fichier	Description
esmanager.log	Contient des messages de journal du processus Edge Service Manager, qui écoute sur les ports 443 et 80.
authbroker.log	Contient des messages de journal du processus AuthBroker, qui gère des adaptateurs d'authentification.
admin.log	Contient des messages de journal du processus qui fournit l'API REST Unified Access Gateway sur le port 9443.
admin-zookeeper.log	Contient des messages de journal liés à la couche de données utilisée pour stocker des informations de configuration d'Unified Access Gateway.
tunnel.log	Contient des messages de journal du processus de tunnel utilisé dans le cadre du traitement API XML.
bsg.log	Contient des messages de journal de Blast Secure Gateway.
SecurityGateway_*.log	Contient des messages de journal de PCoIP Secure Gateway.

Les fichiers journaux qui se terminent par « -std-out.log » contiennent les informations écrites sur stdout de divers processus et il s'agit généralement de fichiers vides.

Fichiers journaux Unified Access Gateway pour AirWatch

- /var/log/airwatch/tunnel/vpnd
Les fichiers tunnel-init.log et tunnel.log sont capturés à partir de ce répertoire.
- /var/log/airwatch/proxy
Le fichier proxy.log est capturé à partir de ce répertoire.
- /var/log/airwatch/appliance-agent
Le fichier appliance-agent.log est capturé à partir de ce répertoire.

Index

A

- AirWatch, configurer tunnel par application **52, 53**
- AirWatch, déploiement de Unified Access Gateway **51**
- assistant de déploiement **20**
- authentification **61**
- authentification du certificat **61**
- authentification par carte à puce, configurer **62**
- authentification RSA SecurID, configurer **65**

B

- BEAT **37**
- Blast, configuration BEAT **37**

C

- cartes à puce, exportation de certificats utilisateur **64**
- cartes réseau Internet **14**
- cas d'utilisation **31**
- certificat, remplacer **26**
- certificats de serveur SSL **58**
- certificats racine
 - exportation **64**
 - obtention **64**
- certificats TLS/SSL **55**
- clé privée, mise à jour du certificat **26**
- configuration d'Access Point **55**
- configuration matérielle requise **8**
- configuration requise **8**
- configuration système **8**
- configurer
 - authentification RSA SecurID **65**
 - Horizon **35**
 - proxy inverse **40**
- configurer les paramètres **24**
- configurer RSA Adaptive Authentication **69**
- console d'administration, configurer les paramètres système **24**
- contrôle de santé **73**

D

- dépannage de unified access gateway **73**
- dépannage des erreurs **74**
- déploiement, dispositif **19**

- déploiement au moyen d'OVF **19**
- déploiement avec Horizon **31**
- Déploiement d'OVF **19**
- DMZ, cartes réseau Internet **14**
- Documentation de Unified Access Gateway **5**

E

- exécution du script powershell **28**
- exigences logicielles **8**

F

- format PEM des certificats de sécurité **56**

H

- Horizon, configurer **35**

J

- journaux, collecte **75**

K

- keytab **48**

M

- métadonnées de fournisseur de services **50**
- métadonnées SAML pour fournisseurs de services **71**
- méthodes d'authentification **61**
- mettre à jour le certificat **26**
- mise à niveau, préparer **17**
- mode de mise au repos **17**

P

- paramètres de domaine pour le pontage d'identité **47**
- paramètres de pontage d'identité, configurer **46**
- passerelle **7**
- pontage d'identité, keytab **48**
- pontage d'identité, configurer **49**
- pontage d'identité, paramètres de domaine **47**
- pontage d'identité, scénarios de déploiement **44**
- pontage d'identité, présentation **43**
- PowerShell, utilisation **27**
- Présentation de Unified Access Gateway **7**
- protocoles de sécurité **59**
- proxy, configurer pour AirWatch **52, 53**

proxy inverse **38**
proxy inverse Web pour le pontage d'identité **49**
proxy inverse, configurer pour VMware Identity
Manager **40**

R

RADIUS, configuration **66**
règles de pare-feu **10**
remplacer les certificats signés **26**
révocation du certificat **61**
RSA Adaptive Authentication, configurer **69**
RSA Adaptive Authentication, inscription
d'utilisateurs **68**

S

SAML **70, 71**
suites de chiffrement **59**

T

topologies **12**
trafic de gestion, DMZ **14**
trafic sur le réseau principal, DMZ **14**
tunnel par application, configurer **52, 53**

U

une carte réseau dans la DMZ **14**

V

View, vpn **8**
VMware Identity Manager
configurer le proxy inverse **40**
proxy inverse **38**
VPN, avec View **8**

X

X.509 **62**