Déploiement et configuration de VMware Unified Access Gateway

09 juillet 2020

Unified Access Gateway 3.10

vmware by Broadcom

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

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

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

Table des matières

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 Workspace ONE Access et de Unified Access GatewayWorkspace ONE UEM qui utilise VMware™ 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.

Note VMware Unified Access Gateway® était appelé auparavant VMware Access Point.

Lisez les sections suivantes :

- Unified Access Gateway comme une passerelle sécurisée
- Utilisation d'Unified Access Gateway au lieu d'un réseau privé virtuel
- Configuration requise pour le système et le réseau Unified Access Gateway
- Règles de pare-feu pour les dispositifs Unified Access Gateway basés sur une zone DMZ
- Configuration système requise pour le déploiement de VMware Tunnel avec Unified Access Gateway
- Topologies d'équilibrage de charge Unified Access Gateway
- Haute disponibilité d'Unified Access Gateway
- Conception de la DMZ pour Unified Access Gateway avec plusieurs cartes d'interface réseau
- Mettre à niveau sans interruption
- Déploiement d'Unified Access Gateway sans profil de protocole réseau (NPP)
- Participer au programme d'amélioration du produit ou le quitter

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 Horizon Connection Server 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 authentifiiez 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 Horizon Connection Server.

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.

Pour plus d'informations sur la stratégie de prise en charge du cycle de vie d'Unified Access Gateway, consultez le site https://kb.vmware.com/s/article/2147313.

Exigences matérielles d'ESXi Server

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

Si vous prévoyez d'utiliser vSphere Web client, vérifiez que le plug-in d'intégration de client est installé. Pour plus d'informations, consultez 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.

Note 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. Bien que vous puissiez modifier ces paramètres, il est recommandé 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

Important Unified Access Gateway est un dispositif virtuel VMware. La sécurité et les correctifs généraux sont distribués par VMware en tant que fichiers image de dispositif virtuel mis à jour. La personnalisation d'un dispositif Unified Access Gateway ou la mise à niveau de composants individuels n'est pas prise en charge, à l'exception de l'augmentation de la mémoire et du nombre de vCPU qui peut être effectuée via les paramètres **Modifier** de vCenter Server.

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

- Taille de téléchargement du dispositif virtuel : 2,6 Go
- Espace disque minimal requis à provisionnement dynamique : 3,5 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

Options de dimensionnement d'Unified Access Gateway

- **Standard :** cette configuration est recommandée pour le déploiement d'Horizon prenant en charge jusqu'à 2 000 connexions d'Horizon, selon la capacité du serveur de connexion. Elle est également recommandée pour les déploiements de Workspace ONE UEM (cas d'utilisation mobiles) jusqu'à 10 000 connexions simultanées.
- **Grand :** cette configuration est recommandée pour les déploiements de Workspace ONE UEM, où Unified Access Gateway doit prendre en charge plus de 50 000 connexions simultanées. Cette taille permet à Content Gateway, Tunnel par application et Proxy et Proxy inverse d'utiliser le même dispositif Unified Access Gateway.

- **Extra grand** : cette configuration est recommandée pour les déploiements de Workspace ONE UEM. Cette taille permet à Content Gateway, Tunnel par application et Proxy et Proxy inverse d'utiliser le me^me dispositif Unified Access Gateway.

- **Note** Options de VM pour les déploiements Standard, Grand et Extra grand :
  - Standard : 2 cœurs et 4 Go de RAM
  - Grand : 4 cœurs et 16 Go de RAM
  - Extra grand : 8 cœurs et 32 Go de RAM

  Pour plus d'informations sur les recommandations de dimensionnement d'Unified Access Gateway, vous pouvez afficher l'option Nombre maximal de configurations VMware.

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 de Workspace ONE UEM, 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.

DNS multidiffusion et noms d'hôte `.local`

UAG (Unified Access Gateway) 3.7 et les versions ultérieures prennent en charge le DNS multidiffusion ainsi que le DNS monodiffusion. Les noms d'appellations multiples ayant le suffixe de domaine `.local` sont routés vers toutes les interfaces locales compatibles avec la multidiffusion IP en utilisant le protocole DNS multidiffusion.

Évitez de définir `.local` dans un serveur DNS monodiffusion, car RFC6762 réserve l'utilisation de ce domaine pour le DNS multidiffusion. Par exemple, si vous utilisez un nom d'hôte `hostname.example.local` dans un paramètre de configuration, tel qu'URL de destination du proxy sur UAG, le nom d'hôte n'est pas résolu à l'aide du DNS monodiffusion, car `.local` est réservé pour le DNS multidiffusion.

Vous pouvez également utiliser l'une des méthodes suivantes dans lesquelles le suffixe de domaine `.local` n'est pas requis :

- Spécifiez une adresse IP au lieu d'un nom d'hôte `.local`.
- Vous pouvez ajouter un autre enregistrement DNS A secondaire dans le serveur DNS.

  Dans l'exemple précédent de nom d'hôte, vous pouvez ajouter `hostname.example.int` à la même adresse IP que `hostname.example.local` et l'utiliser dans la configuration d'UAG.
- Vous pouvez définir une entrée du fichier `hosts` locale.

  Dans l'exemple précédent, une entrée `hosts` locale peut être définie pour `hostname.example.local`.

  Les entrées du fichier `hosts` spécifient les noms et adresses IP et peuvent être définies à l'aide de l'interface utilisateur d'administration d'UAG via les paramètres du fichier `.ini` de PowerShell.

  Important Vous ne devez pas modifier le fichier `/etc/hosts` sur UAG.

  Sur UAG, les entrées du fichier `hosts` locales sont recherchées avant d'effectuer une recherche DNS. Cette recherche vérifie que si le nom d'hôte se trouve dans le fichier `hosts`, vous pouvez utiliser les noms `.local` sans effectuer de recherche DNS.

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.

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.

Les tableaux suivants répertorient la configuration requise des ports pour les différents services dans Unified Access Gateway.

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

Tableau 1-1. Configuration requise des ports pour Secure Email Gateway

Port	Protocole	Source	Cible/Destination	Description
443* ou tout port supérieur à 1 024	HTTPS	Périphériques (depuis Internet et Wi-Fi)	Unified Access Gateway Point de terminaison de Secure Email Gateway	Secure Email Gateway écoute le port 11 443
443* ou tout port supérieur à 1 024	HTTPS	Workspace ONE UEM Console	Unified Access Gateway Point de terminaison de Secure Email Gateway	Secure Email Gateway écoute le port 11 443
443* ou tout port supérieur à 1 024	HTTPS	Service de notification par e-mail (en cas d'activation)	Unified Access Gateway Point de terminaison de Secure Email Gateway	Secure Email Gateway écoute le port 11 443
5 701	HTTP	Secure Email Gateway	Secure Email Gateway	Utilisé pour le cache distribué Hazelcast

Tableau 1-1. Configuration requise des ports pour Secure Email Gateway (suite)

Port	Protocole	Source	Cible/Destination	Description
41 232	HTTPS	Secure Email Gateway	Secure Email Gateway	Utilisé pour la gestion des clusters Vertx
44 444	HTTPS	Secure Email Gateway	Secure Email Gateway	Utilisé pour les fonctionnalités de diagnostic et d'administration

Note Comme le service Secure Email Gateway (SEG) s'exécute en tant qu'utilisateur non racine dans Unified Access Gateway, SEG ne peut pas s'exécuter sur les ports système. Par conséquent, les ports personnalisés doivent être supérieurs au port 1 024.

Tableau 1-2. Configuration requise des ports pour le serveur de connexion Horizon

Port	Protocole	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 443 est transféré en interne vers UDP 9 443 sur le service du serveur de tunnel UDP sur Unified Access Gateway.
8443	UDP	Internet	Unified Access Gateway	Blast Extreme (facultatif)
8443	TCP	Internet	Unified Access Gateway	Blast Extreme (facultatif)
4172	TCP et UDP	Internet	Unified Access Gateway	PCoIP (facultatif)
443	TCP	Unified Access Gateway	Serveur de connexion Horizon	Horizon Client XML-API, Blast Extreme HTML Access, Horizon Air Console Access (HACA)
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)

Tableau 1-2. Configuration requise des ports pour le serveur de connexion Horizon (suite)

Port	Protocole	Source	Cible	Description
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

Note 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 terminaux 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 1-3. Configuration requise des ports pour le proxy inverse Web

Port	Protocole	Source	Cible	Description
443	TCP	Internet	Unified Access Gateway	Pour le trafic Web
quelconque	TCP	Unified Access Gateway	Site intranet	N'importe quel port personnalisé configuré sur lequel l'intranet écoute. Par exemple, 80, 443, 8 080, etc.
88	TCP	Unified Access Gateway	Serveur KDC/Serveur AD	Requis pour le pontage d'identité afin d'accéder à AD si SAML sur Kerberos/ Certificat sur Kerberos est configuré.
88	UDP	Unified Access Gateway	Serveur KDC/Serveur AD	Requis pour le pontage d'identité afin d'accéder à AD si SAML sur Kerberos/ Certificat sur Kerberos est configuré.

Tableau 1-4. Configuration requise des ports pour l'interface utilisateur d'administration

Port	Protocole	Source	Cible	Description
9443	TCP	Interface utilisateur d'administration	Unified Access Gateway	Interface de gestion

Tableau 1-5. Configuration requise des ports pour la configuration du point de terminaison de base de Content Gateway

Port	Protocole	Source	Cible	Description
443* ou n'importe quel port > 1 024	HTTPS	Périphériques (depuis Internet et Wi-Fi)	Point de terminaison de Unified Access Gateway Content Gateway	Si 443 est utilisé, Content Gateway écoutera sur le port 10 443.
443* ou n'importe quel port > 1 024	HTTPS	Services de terminaux Workspace ONE UEM	Point de terminaison de Unified Access Gateway Content Gateway	
443* ou n'importe quel port > 1 024	HTTPS	Console Workspace ONE UEM	Point de terminaison de Unified Access Gateway Content Gateway	Si 443 est utilisé, Content Gateway écoutera sur le port 10 443.
443* ou n'importe quel port > 1 024	HTTPS	Point de terminaison de Unified Access Gateway Content Gateway	Workspace ONE UEM API Server	
N'importe quel port sur lequel le référentiel écoute.	HTTP ou HTTPS	Point de terminaison de Unified Access Gateway Content Gateway	Référentiels de contenu Web tels que (SharePoint/ WebDAV/CMIS, etc.	N'importe quel port personnalisé configuré sur lequel le site intranet écoute.
137–139 et 445	Protocole CIFS ou SMB	Point de terminaison de Unified Access Gateway Content Gateway	Référentiels basés sur un partage réseau (partages de fichiers Windows)	Partages d'intranet

Tableau 1-6. Configuration requise des ports pour la configuration du point de terminaison relais de Content Gateway

Port	Protocole	Source	Cible/Destination	Description
443* ou n'importe quel port > 1 024	HTTP/ HTTPS	Serveur relais Unified Access Gateway (relais Content Gateway)	Point de terminaison de Unified Access Gateway Content Gateway	Si 443 est utilisé, Content Gateway écoutera sur le port 10 443.
443* ou n'importe quel port > 1 024	HTTPS	Périphériques (depuis Internet et Wi-Fi)	Serveur relais Unified Access Gateway (relais Content Gateway)	Si 443 est utilisé, Content Gateway écoutera sur le port 10 443.
443* ou n'importe quel port > 1 024	TCP	Services de terminaux Workspace ONE UEM	Serveur relais Unified Access Gateway (relais Content Gateway)	Si 443 est utilisé, Content Gateway écoutera sur le port 10 443.
443* ou n'importe quel port > 1 024	HTTPS	Workspace ONE UEM Console		
443* ou n'importe quel port > 1 024	HTTPS	Relais Unified Access Gateway Content Gateway	Serveur API Workspace ONE UEM	
443* ou n'importe quel port > 1 024	HTTPS	Point de terminaison de Unified Access Gateway Content Gateway	Serveur API Workspace ONE UEM	
N'importe quel port sur lequel le référentiel écoute.	HTTP ou HTTPS	Point de terminaison de Unified Access Gateway Content Gateway	Référentiels de contenu Web tels que (SharePoint/ WebDAV/CMIS, etc.	N'importe quel port personnalisé configuré sur lequel le site intranet écoute.

Tableau 1-6. Configuration requise des ports pour la configuration du point de terminaison relais de Content Gateway (suite)

Port	Protocole	Source	Cible/Destination	Description
443* ou n'importe quel port > 1 024	HTTPS	Unified Access Gateway (relais Content Gateway)	Point de terminaison de Unified Access Gateway Content Gateway	Si 443 est utilisé, Content Gateway écoutera sur le port 10 443.
137–139 et 445	Protocole CIFS ou SMB	Point de terminaison de Unified Access Gateway Content Gateway	Référentiels basés sur un partage réseau (partages de fichiers Windows)	Partages d'intranet

Note Étant donné que le service Content Gateway est exécuté en tant qu'utilisateur non racine dans Unified Access Gateway, Content Gateway ne peut pas s'exécuter sur les ports système et, par conséquent, les ports personnalisés doivent être > 1 024.

Tableau 1-7. Configuration requise des ports pour VMware Tunnel

Port	Protocole	Source	Cible/Destination	Vérification	Remarque (voir la section Remarque au bas de la page)
2 020 *	HTTPS	Périphériques (depuis Internet et Wi-Fi)	Proxy de VMware Tunnel	Exécutez la commande suivante après l'installation : `netstat -tlpn | grep [Port]`	
8443 *	TCP, UDP	Périphériques (depuis Internet et Wi-Fi)	Tunnel par application de VMware Tunnel	Exécutez la commande suivante après l'installation : `netstat -tlpn | grep [Port]`	1

Tableau 1-8. Configuration de point de terminaison de base de VMware Tunnel

Port	Protocole	Source	Cible/Destination	Vérification	Remarque (voir la section Remarque au bas de la page)
SaaS : 443 : 2001 *	HTTPS	VMware Tunnel	Serveur Workspace ONE UEM Cloud Messaging	`curl -Ivv https://<AWCM URL>:<port>/awcm/status/ping` La réponse attendue est HTTP 200 OK.	2
SaaS : 443 Sur site : 80 ou 443	HTTP ou HTTPS	VMware Tunnel	Point de terminaison REST API de Workspace ONE UEM ■ SaaS : `https://asXXX.awmdm.com` ou `https://asXXX.airwatchportals.com` ■ Sur site : plus couramment votre serveur DS ou de console	`curl -Ivv https://<API URL>/api/mdm/ping` La réponse attendue est HTTP 401 non autorisé.	5
80 443, n'importe quel port TCP	HTTP, HTTPS ou TCP	VMware Tunnel	Ressources internes	Confirmez que VMware Tunnel peut accéder aux ressources internes sur le port requis.	4
514 *	UDP	VMware Tunnel	Serveur Syslog		
Sur site : 2020	HTTPS	Console Workspace ONE UEM	Proxy de VMware Tunnel	Les utilisateurs sur site peuvent tester la connexion à l'aide de la commande `telnet` : `telnet <Tunnel Proxy URL> <port>`	6

Tableau 1-9. Configuration en cascade de VMware Tunnel

Port	Protocole	Source	Cible/Destination	Vérification	Remarque (voir la section Remarque au bas de la page)
SaaS : 443 Sur site : 2001 *	TLS v1.2	Serveur frontal VMware Tunnel	Serveur Workspace ONE UEM Cloud Messaging	Vérifiez en utilisant `wget` vers `https://<AWCM URL>:<port>/awcm/status` et en veillant à recevoir une réponse HTTP 200.	2
8443	TLS v1.2	Serveur frontal VMware Tunnel	Serveur principal VMware Tunnel	Connectez-vous par Telnet du serveur frontal VMware Tunnel au serveur principal VMware Tunnel sur le port.	3

Tableau 1-9. Configuration en cascade de VMware Tunnel (suite)

Port	Protocole	Source	Cible/Destination	Vérification	Remarque (voir la section Remarque au bas de la page)
SaaS : 443 Sur site : 2001	TLS v1.2	Serveur principal VMware Tunnel	Serveur Workspace ONE UEM Cloud Messaging	Vérifiez en utilisant `wget` vers `https://<AWCM URL>:<port>/awcm/status` et en veillant à recevoir une réponse HTTP 200.	2
80 ou 443	TCP	Serveur principal VMware Tunnel	Applications Web/ sites Web internes		4
80 443, n'importe quel port TCP	TCP	Serveur principal VMware Tunnel	Ressources internes		4
80 ou 443	HTTPS	Serveur frontal et principal VMware Tunnel	Point de terminaison REST API de Workspace ONE UEM ■ SaaS :`https://asXXX.awmdm.com` ou `https://asXXX.airwatchportals.com` ■ Sur site : plus couramment votre serveur DS ou de console	`curl -Ivv https://<API URL>/api/mdm/ping` La réponse attendue est HTTP 401 non autorisé.	5

Tableau 1-10. Configuration de serveur frontal et de serveur principal VMware Tunnel

Port	Protocole	Source	Cible/Destination	Vérification	Remarque (voir la section Remarque au bas de la page)
SaaS : 443 Sur site : 2001	HTTP ou HTTPS	Serveur frontal VMware Tunnel	Serveur Workspace ONE UEM Cloud Messaging	`curl -Ivv https://<AWCM URL>:<port>/awcm/status/ping` La réponse attendue est HTTP 200 OK.	2
80 ou 443	HTTPS ou HTTPS	Serveur principal et serveur frontal VMware Tunnel	Point de terminaison REST API de Workspace ONE UEM ■ SaaS :`https://asXXX.awmdm.com` ou `https://asXXX.airwatchportals.com` ■ Sur site : plus couramment votre serveur DS ou de console	`curl -Ivv https://<API URL>/api/mdm/ping` La réponse attendue est HTTP 401 non autorisé. Le point de terminaison de VMware Tunnel requiert l'accès au point de terminaison REST API uniquement lors du déploiement initial.	5
2 010 *	HTTPS	Serveur frontal VMware Tunnel	Serveur principal VMware Tunnel	Connectez-vous par Telnet du serveur frontal VMware Tunnel au serveur principal VMware Tunnel sur le port.	3
80 443, n'importe quel port TCP	HTTP, HTTPS ou TCP	Serveur principal VMware Tunnel	Ressources internes	Confirmez que VMware Tunnel peut accéder aux ressources internes sur le port requis.	4
514 *	UDP	VMware Tunnel	Serveur Syslog		
Sur site : 2 020	HTTPS	Workspace ONE UEM	Proxy de VMware Tunnel	Les utilisateurs sur site peuvent tester la connexion à l'aide de la commande `telnet` : `telnet <Tunnel Proxy URL> <port>`	6

Les points suivants sont valides pour la configuration requise de VMware Tunnel.

Note * : vous pouvez modifier ce port si nécessaire en fonction des restrictions de votre environnement.

1 Si le port 443 est utilisé, Tunnel par application écoutera sur le port 8 443.

   Note Lorsque les services VMware Tunnel et Content Gateway sont activés sur le même dispositif, et que le partage de port TLS est activé, les noms DNS doivent être uniques pour chaque service. Lorsque TLS n'est pas activé, seul un nom DNS peut être utilisé pour les deux services, car le port différenciera le trafic entrant. (Pour Content Gateway,si le port 443 est utilisé, Content Gateway écoutera sur le port 10 443.)

2 Pour que VMware Tunnel interroge la console Workspace ONE UEM à des fins de conformité et de suivi.

3 Pour que les topologies de serveur frontal VMware Tunnel transmettent les demandes de terminaux vers le point de terminaison VMware Tunnel interne uniquement.

4 Pour que les applications utilisant VMware Tunnel accèdent aux ressources internes.

5 VMware Tunnel doit communiquer avec l'API pour l'initialisation. Assurez-vous qu'il existe une connectivité entre REST API et le serveur VMware Tunnel. Accédez à **Groupes et paramètres > Tous les paramètres > Système > Avancé > URL de sites** pour définir l'URL de serveur REST API. Cette page n'est pas disponible pour les clients SaaS. L'URL de REST API pour les clients SaaS est plus couramment l'URL du serveur de console ou de services de terminaux.

6 Cela est requis pour une « Connexion de test » réussie au proxy de VMware Tunnel depuis la console Workspace ONE UEM. La configuration requise est facultative et peut être omise sans perte de fonctionnalité aux terminaux. Pour les clients SaaS, il est possible que la console Workspace ONE UEM ait déjà établi une connectivité entrante au proxy de VMware Tunnel sur le port 2 020 en raison de la configuration requise du trafic Internet entrant sur le port 2 020.

Configuration système requise pour le déploiement de VMware Tunnel avec Unified Access Gateway

Pour déployer VMware Tunnel avec Unified Access Gateway, assurez-vous que votre système répond à la configuration requise suivante :

Exigences de l'hyperviseur

L'instance de Unified Access Gateway qui déploie VMware Tunnel nécessite un hyperviseur pour déployer le dispositif virtuel. Vous devez disposer d'un compte d'administration dédié avec des privilèges complets pour déployer le modèle OVF.

Hyperviseurs pris en charge

- VMware vSphere web client

  Note Vous devez utiliser des versions spécifiques des produits VMware avec des versions spécifiques d'Unified Access Gateway. Le dispositif Unified Access Gateway doit être déployé sur une version de VMware vSphere identique à celle prise en charge pour les produits et versions de VMware, respectivement.

- Microsoft Hyper-V sur Windows Server 2012 R2 ou Windows Server 2016

Exigences logicielles

Vérifiez que vous disposez de la version la plus récente d'Unified Access Gateway. VMware Tunnel prend en charge la compatibilité en amont entre Unified Access Gateway et Workspace ONE UEM Console. La compatibilité en amont vous permet de mettre à niveau votre serveur VMware Tunnel peu après la mise à niveau de votre dispositif Workspace ONE UEM Console. Pour garantir la parité entre Workspace ONE UEM Console et VMware Tunnel, envisagez de planifier une mise à niveau anticipée.

Configuration matérielle requise

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

Pour modifier les paramètres par défaut, mettez la machine virtuelle hors tension dans vCenter. Cliquez avec le bouton droit sur la machine virtuelle et sélectionnez **Modifier les paramètres**.

La configuration par défaut utilise 4 Go de RAM et de 2 CPU. Vous devez modifier la configuration par défaut pour répondre à la configuration matérielle requise. Pour gérer toutes les charges des périphériques et les exigences de maintenance, envisagez d'exécuter un minimum de deux serveurs de VMware Tunnel.

Tableau 1-11. Configuration matérielle requise

Nombre de périphériques	Jusqu'à 40 000	40 000 à 80 000	80 000 à 120 000	120 000 à 160 000
Nombre de serveurs	2	3	4	5
Cœurs de CPU	4 cœurs de CPU*	4 cœurs de CPU chacun	4 cœurs de CPU chacun	4 cœurs de CPU chacun
RAM (GO)	8	8	8	8

Tableau 1-11. Configuration matérielle requise (suite)

Nombre de périphériques	Jusqu'à 40 000	40 000 à 80 000	80 000 à 120 000	120 000 à 160 000
Espace disponible sur le disque dur (Go)	10 Go pour la distribution (Linux uniquement) 400 Mo pour le programme d'installation ~ 10 Go d'espace de fichier journal**			

* Il est possible de ne déployer qu'un seul dispositif VMware Tunnel dans le cadre d'un déploiement plus petit. Toutefois, envisagez de déployer au moins deux serveurs équilibrés en charge avec quatre cœurs de CPU chacun, quel que soit le nombre de périphériques, pour optimiser les performances et les temps d'activité.

**10 Go pour un déploiement standard. Redimensionnez le fichier journal en fonction de votre utilisation du journal et de la configuration requise pour stocker les journaux.

Configuration requise des ports pour le proxy VMware Tunnel

Le proxy VMware Tunnel peut être configuré à l'aide de l'un des deux modèles de configuration suivants :

- point de terminaison de base (un seul niveau) à l'aide d'un point de terminaison de proxy VMware Tunnel ;
- point de terminaison relais (multiniveaux) à l'aide d'un relais de proxy VMware Tunnel et d'un point de terminaison de proxy VMware Tunnel.

Tableau 1-12. Configuration requise des ports pour la Configuration de point de terminaison de base de proxy VMware Tunnel

Source	Cible ou Destination	Protocole	Port	Vérification	Remarques
Périphériques (depuis Internet et Wi-Fi)	Point de terminaison de proxy VMware Tunnel	HTTPS	2020*	Exécutez la commande suivante après l'installation : `netstat -tlpn | grep [Port]`	Les périphériques se connectent au DNS public configuré pour VMware Tunnel sur le port spécifié.
Point de terminaison de proxy VMware Tunnel	Serveur Workspace ONE UEM Cloud Messaging	HTTPS	SaaS : 443 Sur-site : 2001*	`curl -Ivv https://<AWCM URL>:<port>/awcm/status/ping` La réponse attendue est `HTTP 200 OK`.	Pour que le proxy VMware Tunnel interroge la console Workspace ONE UEM à des fins de conformité et de suivi. La version TLS 1.2 au minimum est requise.

Tableau 1-12. Configuration requise des ports pour la Configuration de point de terminaison de base de proxy VMware Tunnel (suite)

Source	Cible ou Destination	Protocole	Port	Vérification	Remarques
Point de terminaison de proxy VMware Tunnel	UEM REST API ■ SaaS‡ : https://asXXX.awmdm.com ou https://asXXX.airwatchportals.com ■ Sur site† : plus couramment les services du périphérique ou le serveur de la console	HTTP ou HTTPS	SaaS : 443 Sur-site : 2001*	`curl -Ivv https://<API URL>/api/mdm/ping` La réponse attendue est `HTTP 401 unauthorized`	Le proxy VMware Tunnel doit communiquer avec UEM REST API pour l'initialisation. Dans la console Workspace ONE UEM, accédez à **Groupes & paramètres > Tous les paramètres > Système > Avancé > URL du Site** pour définir **l'URL de REST API**. Cette page n'est pas disponible pour les utilisateurs SaaS de Workspace ONE UEM. Pour les utilisateurs SaaS de Workspace ONE UEM, l'**URL de REST API** est plus couramment l'**URL de la console** ou l'**URL des services de périphérique**.
Point de terminaison de proxy VMware Tunnel	Ressources internes	HTTP, HTTPS ou TCP	80 443, n'importe quel port TCP	Confirmez que le point de terminaison de périphérique VMware Tunnel peut accéder aux ressources internes sur le port requis.	Pour que les applications utilisant le proxy VMware Tunnel accèdent aux ressources internes. Les points de terminaison ou ports exacts sont déterminés en fonction de l'emplacement de ces ressources.

Tableau 1-12. Configuration requise des ports pour la Configuration de point de terminaison de base de proxy VMware Tunnel (suite)

Source	Cible ou Destination	Protocole	Port	Vérification	Remarques
Point de terminaison de proxy VMware Tunnel	Serveur Syslog	UDP	514*		
Workspace ONE UEM console	Point de terminaison de proxy VMware Tunnel	HTTPS	2020*	Les utilisateurs sur site† peuvent tester la connexion à l'aide de la commande telnet : `telnet <Tunnel ProxyURL><port>`	Cela est nécessaire pour une « connexion de test » réussie au point de terminaison de proxy VMware Tunnel à partir de Workspace ONE UEM Console.

Tableau 1-13. Configuration requise des ports pour la configuration de point de terminaison relais de proxy VMware Tunnel

Source	Cible ou Destination	Protocole	Port	Vérification	Remarques
Périphériques (depuis Internet et Wi-Fi)	Relais de proxy VMware Tunnel	HTTPS	2020*	Exécutez la commande suivante après l'installation : `netstat -tlpn | grep [Port]`	Les périphériques se connectent au DNS public configuré pour VMware Tunnel sur le port spécifié.
Relais de proxy VMware Tunnel	Serveur Workspace ONE UEM Cloud Messaging	HTTP ou HTTPS	SaaS : 443 Sur-site : 2001*	`curl -Ivv https://<AWCM URL>:<port>/awcm/status/ping` La réponse attendue est `HTTP 200 OK`.	Pour que le proxy VMware Tunnel interroge la console Workspace ONE UEM à des fins de conformité et de suivi. La version TLS 1.2 au minimum est requise.

Tableau 1-13. Configuration requise des ports pour la configuration de point de terminaison relais de proxy VMware Tunnel (suite)

Source	Cible ou Destination	Protocole	Port	Vérification	Remarques
Relais de proxy VMware Tunnel	UEM REST API ■ SaaS‡ : https://asXXX.awmdm.com ou https://asXXX.airwatchportals.com ■ Sur site† : plus couramment les services du périphérique ou le serveur de la console	HTTP ou HTTPS	SaaS : 443 Sur-site : 2001*	`curl -Ivv https://<API URL>/api/mdm/ping` La réponse attendue est `HTTP 401 unauthorized` Le relais de proxy VMware Tunnel requiert UEM REST API uniquement lors du déploiement initial.	Le proxy VMware Tunnel doit communiquer avec UEM REST API pour l'initialisation. Dans la console Workspace ONE UEM, accédez à **Groupes & paramètres > Tous les paramètres > Système > Avancé > URL du Site** pour définir **l'URL de REST API**. Cette page n'est pas disponible pour les utilisateurs SaaS de Workspace ONE UEM. Pour les utilisateurs SaaS de Workspace ONE UEM, l'**URL de REST API** est plus couramment l'**URL de la console** ou l'**URL des services de périphérique**.

Tableau 1-13. Configuration requise des ports pour la configuration de point de terminaison relais de proxy VMware Tunnel (suite)

Source	Cible ou Destination	Protocole	Port	Vérification	Remarques
Point de terminaison de proxy VMware Tunnel	UEM REST API ■ SaaS‡ : https://asXXX.awmdm.com ou https://asXXX.airwatchportals.com ■ Sur site† : plus couramment les services du périphérique ou le serveur de la console	HTTP ou HTTPS	SaaS : 443 Sur-site : 2001*	`curl -Ivv https://<API URL>/api/mdm/ping` La réponse attendue est `HTTP 401 unauthorized` Le relais de proxy VMware Tunnel requiert UEM REST API uniquement lors du déploiement initial.	Le proxy VMware Tunnel doit communiquer avec UEM REST API pour l'initialisation. Dans la console Workspace ONE UEM, accédez à **Groupes & paramètres > Tous les paramètres > Système > Avancé > URL du Site** pour définir **l'URL de REST API**. Cette page n'est pas disponible pour les utilisateurs SaaS de Workspace ONE UEM. Pour les utilisateurs SaaS de Workspace ONE UEM, l'**URL de REST API** est plus couramment l'**URL de la Console** ou l'**URL des services de périphériques**.
Relais de proxy VMware Tunnel	Point de terminaison de proxy VMware Tunnel	HTTPS	2010*	Telnet à partir du relais de proxy VMware Tunnel au point de terminaison de proxy VMware Tunnel sur le port 2010.	Pour transférer les demandes du périphérique à partir du relais jusqu'au serveur de point de terminaison. La version TLS 1.2 au minimum est requise.

Tableau 1-13. Configuration requise des ports pour la configuration de point de terminaison relais de proxy VMware Tunnel (suite)

Source	Cible ou Destination	Protocole	Port	Vérification	Remarques
Point de terminaison de proxy VMware Tunnel	Ressources internes	HTTP, HTTPS ou TCP	80 443, n'importe quel port TCP	Confirmez que le point de terminaison de périphérique VMware Tunnel peut accéder aux ressources internes sur le port requis.	Pour que les applications utilisant le proxy VMware Tunnel accèdent aux ressources internes. Les points de terminaison ou ports exacts sont déterminés en fonction de l'emplacement de ces ressources.
Point de terminaison de proxy VMware Tunnel	Serveur Syslog	UDP	514*		
Console Workspace ONE UEM	Relais de proxy VMware Tunnel	HTTPS	2020*	Les utilisateurs sur site† peuvent tester la connexion à l'aide de la commande telnet : `telnet <Tunnel ProxyURL><port>`	Cela est nécessaire pour une « connexion de test » réussie au relais de proxy VMware Tunnel à partir de Workspace ONE UEM Console.

REMARQUES

- * Vous pouvez modifier ce port en fonction des restrictions de votre environnement.
- † Sur site signifie l'emplacement de la console Workspace ONE UEM.
- ‡ Pour les clients SaaS qui doivent ajouter les communications sortantes à la liste blanche, reportez-vous à l'article de la Base de connaissances VMware qui répertorie les plages d'adresses IP à jour : https://support.workspaceone.com/articles/115001662168-.

Configuration requise des ports pour le tunnel VMware par application

Le tunnel VMware par application peut être configuré à l'aide de l'un des deux modèles de configuration suivants :

- point de terminaison de base (un seul niveau) à l'aide d'un point de terminaison de base de tunnel VMware par application ;

- en cascade (multiniveaux), à l'aide d'un tunnel VMware par application frontal et d'un tunnel VMware par application principal.

Tableau 1-14. Configuration requise des ports pour la configuration de base du point de terminaison de tunnel VMware par application

Source	Destination	Protocole	Port	Vérification	Remarques
Périphériques (depuis Internet et Wi-Fi)	Point de terminaison de base de tunnel VMware par application	TCP, UDP	8443*	Exécutez la commande suivante après l'installation : `netstat -tlpn | grep [Port]`	Les périphériques se connectent au DNS public configuré pour VMware Tunnel sur le port spécifié. Si le port 443 est utilisé, le composant du tunnel par application écoutera sur le port 8 443.
Point de terminaison de base de tunnel VMware par application	Serveur Workspace ONE UEM Cloud Messaging	HTTPS	SaaS : 443 Sur-site : 2001*	Vérifiez en utilisant `wget` vers `https://<AWCM URL>:<port>/awcm/status` et en veillant à recevoir une réponse `HTTP 200`.	Pour que le tunnel VMware par application interroge la console Workspace ONE UEM à des fins de conformité et de suivi. La version TLS 1.2 au minimum est requise.

Tableau 1-14. Configuration requise des ports pour la configuration de base du point de terminaison de tunnel VMware par application (suite)

Source	Destination	Protocole	Port	Vérification	Remarques
Point de terminaison de base de tunnel VMware par application	Applications ou ressources Web/sites Web internes	HTTP, HTTPS ou TCP	80, 443, n'importe quel port TCP requis		Pour que les applications utilisant le tunnel VMware par application accèdent aux ressources internes. Les points de terminaison ou ports exacts sont déterminés en fonction de l'emplacement de ces ressources.
Point de terminaison de base de tunnel VMware par application	UEM REST API ■ SaaS‡ : https://asXXX.awmdm.com ou https://asXXX.airwatchportals.com ■ Sur site† : plus couramment les services du périphérique ou le serveur de la console	HTTP ou HTTPS	80 ou 443	`curl -Ivv https://<API URL>/api/mdm/ping` La réponse attendue est `HTTP 401 unauthorized`	Le tunnel VMware par application doit communiquer avec UEM REST API pour l'initialisation. Dans la console Workspace ONE UEM, accédez à **Groupes & paramètres > Tous les paramètres > Système > Avancé > URL du Site** pour définir **l'URL de REST API**. Cette page n'est pas disponible pour les utilisateurs SaaS de Workspace ONE UEM. Pour les utilisateurs SaaS de Workspace ONE UEM, l'**URL de REST API** est plus couramment l'**URL de la console** ou l'**URL**

Tableau 1-14. Configuration requise des ports pour la configuration de base du point de terminaison de tunnel VMware par application (suite)

Source	Destination	Protocole	Port	Vérification	Remarques
					des services de périphérique.

Tableau 1-15. Configuration requise des ports pour la configuration en cascade du tunnel VMware par application

Source	Destination	Protocole	Port	Vérification	Remarques
Périphériques (depuis Internet et Wi-Fi)	Tunnel VMware par application frontal	TCP, UDP	8443*	Exécutez la commande suivante après l'installation : `netstat -tlpn | grep [Port]`	Les périphériques se connectent au DNS public configuré pour VMware Tunnel sur le port spécifié. Si le port 443 est utilisé, le composant du tunnel par application écoutera sur le port 8 443.
Tunnel VMware par application frontal	Serveur Workspace ONE UEM Cloud Messaging	HTTPS	SaaS : 443 Sur-site : 2001*	Vérifiez en utilisant `wget` vers `https://<AWCM URL>:<port>/awcm/status` et en veillant à recevoir une réponse `HTTP 200`.	Pour que le tunnel VMware par application interroge la console Workspace ONE UEM à des fins de conformité et de suivi. La version TLS 1.2 au minimum est requise.
Tunnel VMware par application frontal	Tunnel VMware par application principal	TCP	8443	Telnet à partir du Tunnel VMware par application frontal vers le tunnel VMware par application principal sur le port 8443.	Pour transférer les demandes du périphérique depuis le serveur frontal vers le serveur principal. La version TLS 1.2 au minimum est requise.

Tableau 1-15. Configuration requise des ports pour la configuration en cascade du tunnel VMware par application (suite)

Source	Destination	Protocole	Port	Vérification	Remarques
Tunnel VMware par application principal	Serveur Workspace ONE UEM Cloud Messaging	HTTPS	SaaS : 443 Sur-site : 2001*	Vérifiez en utilisant `wget` vers `https://<AWCM URL>:<port>/awcm/status` et en veillant à recevoir une réponse `HTTP 200`.	Pour que le tunnel VMware par application interroge la console Workspace ONE UEM à des fins de conformité et de suivi. La version TLS 1.2 au minimum est requise.
VMware Tunnel principal	Applications ou ressources Web/sites Web internes	HTTP, HTTPS ou TCP	80, 443, n'importe quel port TCP requis		Pour que les applications utilisant le tunnel VMware par application accèdent aux ressources internes. Les points de terminaison ou ports exacts sont déterminés en fonction de l'emplacement de ces ressources.

Tableau 1-15. Configuration requise des ports pour la configuration en cascade du tunnel VMware par application (suite)

Source	Destination	Protocole	Port	Vérification	Remarques
Tunnel VMware par application frontal	UEM REST API ■ SaaS‡ : https://asXXX.awmdm.com ou https://asXXX.airwatchportals.com ■ Sur site† : plus couramment les services du périphérique ou le serveur de la console	HTTP ou HTTPS	80 ou 443	`curl -Ivv https://<API URL>/api/mdm/ping` La réponse attendue est `HTTP 401 unauthorized`	Le tunnel VMware par application doit communiquer avec UEM REST API pour l'initialisation. Dans la console Workspace ONE UEM, accédez à **Groupes & paramètres > Tous les paramètres > Système > Avancé > URL du Site** pour définir **l'URL de REST API**. Cette page n'est pas disponible pour les utilisateurs SaaS de Workspace ONE UEM. Pour les utilisateurs SaaS de Workspace ONE UEM, l'**URL de REST API** est plus couramment l'**URL de la console** ou l'**URL des services de périphérique**.
Tunnel VMware par application principal	UEM REST API ■ SaaS‡ : https://asXXX.awmdm.com ou https://asXXX.airwatchportals.com ■ Sur site† : plus	HTTP ou HTTPS	80 ou 443	`curl -Ivv https://<API URL>/api/mdm/ping` La réponse attendue est `HTTP 401 unauthorized`	Le tunnel VMware par application doit communiquer avec UEM REST API pour l'initialisation. Dans la console Workspace ONE UEM, accédez à **Groupes & paramètres > Tous les paramètres > Système > Avancé > URL**

Tableau 1-15. Configuration requise des ports pour la configuration en cascade du tunnel VMware par application (suite)

Source	Destination	Protocole	Port	Vérification	Remarques
	couramment les services du périphérique ou le serveur de la console				**du Site** pour définir **l'URL de REST API**. Cette page n'est pas disponible pour les utilisateurs SaaS de Workspace ONE UEM. Pour les utilisateurs SaaS de Workspace ONE UEM, l'**URL de REST API** est plus couramment l'**URL de la console** ou l'**URL des services de périphérique**.

REMARQUES

- * Vous pouvez modifier ce port en fonction des restrictions de votre environnement.
- † Sur site signifie l'emplacement de la console Workspace ONE UEM.
- ‡ Pour les clients SaaS qui doivent ajouter la communications sortante à la liste blanche, reportez-vous à l'article de la Base de connaissances VMware qui répertorie les plages d'adresses IP à jour : ..

Pour les clients SaaS qui doivent ajouter la communication sortante à la liste blanche, reportez-vous à l'article de la Base de connaissances suivante qui répertorie les plages d'adresses IP à jour que VMware possède actuellement : Plages d'adresses IP de VMware Workspace ONE pour centres de données de SaaS.

Exigences de connexion de l'interface réseau

Vous pouvez utiliser une, deux ou trois interfaces réseau. Une adresse IP distincte doit être attribuée à chaque interface. De nombreuses implémentations de zone DMZ sécurisée utilisent des réseaux distincts pour identifier les différents types de trafic.

Configurez le dispositif virtuel en fonction de la conception de réseau de la zone DMZ dans laquelle il est déployé. Consultez votre administrateur réseau pour plus d'informations concernant la zone DMZ de votre réseau.

- Avec une interface 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.

- Avec une troisième interface réseau, les trafics externe, interne et de gestion ont chacun leur propre sous-réseau.

Note Avec plusieurs déploiements d'interfaces réseau, chacune doit se trouver sur un sous-réseau distinct.

Topologies d'équilibrage de charge Unified Access Gateway

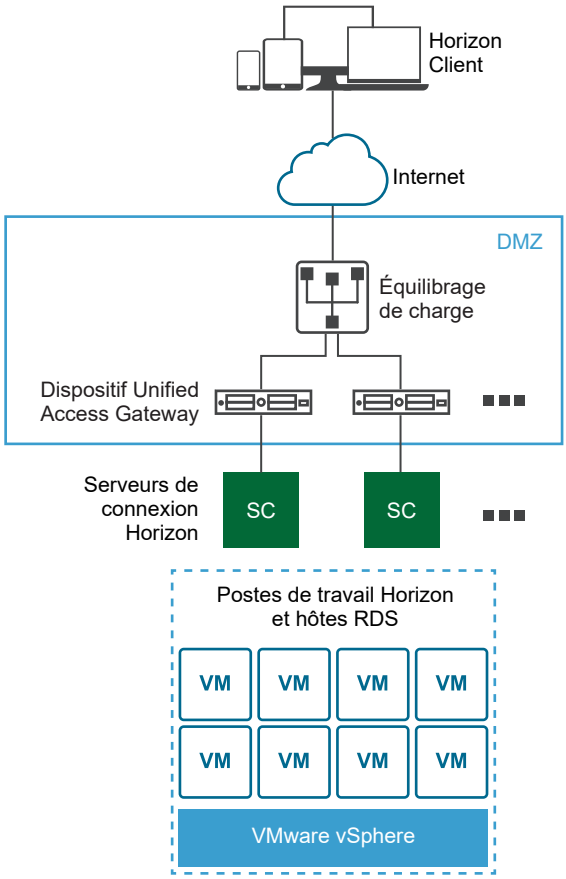
Un dispositif Unified Access Gateway dans la zone DMZ peut être configuré pour pointer vers un serveur ou vers un équilibrage de charge qui fait face à un groupe de serveurs. Les dispositifs Unified Access Gateway fonctionnent avec des solutions d'équilibrage de charge tierces standard qui sont configurées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

Note Unified Access Gateway est certifié pour une utilisation avec des équilibrages de charge Avi Vantage lorsque Unified Access Gateway est déployé en tant que proxy inverse Web.

Si le dispositif Unified Access Gateway pointe vers un équilibrage de charge devant des serveurs, la sélection de l'instance du serveur est dynamique. Par exemple, l’équilibrage 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 équilibrage de charge pour prendre en charge l'accès interne. Avec Unified Access Gateway, vous pouvez pointer le dispositif Unified Access Gateway vers ce même équilibrage 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 équilibrage de charge devant deux dispositifs Unified Access Gateway ou plus dans la zone DMZ.

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



Protocoles Horizon

Lorsqu'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 distribue 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 4172, UDP 4172)

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.

Considérations relatives à l'équilibrage de charge pour Content Gateway et le Proxy tunnel

Gardez les éléments suivants à l’esprit lorsque vous utilisez un équilibrage de charge avec Content Gateway et le Proxy tunnel :

- Configurez les équilibrages de charge pour envoyer des en-têtes HTTP d’origine afin d'éviter tout problème de connectivité des périphériques. Content Gateway et le Proxy tunnel utilisent des informations dans l’en-tête HTTP de la demande pour authentifier les périphériques.
- Le composant Tunnel par application requiert l'authentification de chaque client après qu’une connexion est établie. Lorsque la connexion est établie, une session est créée pour le client et stockée dans la mémoire. La même session est alors utilisée pour chaque élément de données client afin que les données puissent être chiffrées et déchiffrées à l’aide de la même clé. Lorsque vous concevez une solution d’équilibrage de charge, l’équilibrage de charge doit être configuré avec la persistance basée sur l'adresse IP/la session activée. Une solution alternative peut consister à utiliser la permutation circulaire DNS du côté client, ce qui signifie que le client peut sélectionner un serveur différent pour chaque connexion.

Surveillance de la santé

Un équilibrage de charge surveille la santé de chaque dispositif Unified Access Gateway en envoyant régulièrement une demande `HTTPS GET /favicon.ico`. Par exemple, `https://uag1.myco-dmz.com/favicon.ico`. Cette surveillance est configurée sur l'équilibrage de charge. Il exécutera cette demande `HTTPS GET` et attendra une réponse `"HTTP/1.1 200 OK"` d'Unified Access Gateway pour savoir s'il est « sain ». S'il obtient une réponse autre que `"HTTP/1.1 200 OK"` ou s'il n'obtient aucune réponse, il marquera le dispositif Unified Access Gateway spécifique comme étant hors service et ne tentera pas d'y acheminer les demandes client. Il poursuivra la vérification pour pouvoir détecter si le dispositif est disponible.

Unified Access Gateway peut passer en mode « repos », après quoi il ne répondra pas à la demande de surveillance de santé de l'équilibrage de charge avec une réponse `"HTTP/1.1 200 OK"`. Au lieu de cela, il répondra avec `"HTTP/1.1 503"` pour indiquer que le service Unified Access Gateway est temporairement indisponible. Ce paramètre est souvent utilisé avant une maintenance planifiée, une reconfiguration planifiée ou une mise à niveau planifiée d'un dispositif Unified Access Gateway. Dans ce mode, l'équilibrage de charge ne dirigera pas de nouvelles sessions vers ce dispositif, car il sera marqué comme non disponible, mais vous pouvez autoriser les sessions existantes à poursuivre jusqu'à ce que l'utilisateur se déconnecte ou que la durée maximale de session soit atteinte. Par conséquent, cette opération ne va pas perturber les sessions utilisateur existantes. Le dispositif sera alors disponible pour la maintenance après la durée maximale globale de session, qui est généralement de 10 heures. Cette fonctionnalité peut être utilisée pour effectuer une mise à niveau continue d'un ensemble de dispositifs Unified Access Gateway dans une stratégie, évitant ainsi toute interruption de service pour l'utilisateur.

Configurer AVI Vantage pour l'équilibrage de charge d'UAG (lors d'une utilisation en tant que proxy inverse Web)

Les informations présentées ici vous aideront à configurer Avi Vantage, lorsqu'il est utilisé comme solution d'équilibrage de charge, pour Unified Access Gateway lorsque celui-ci est déployé en tant que proxy inverse Web. La configuration implique un ensemble de tâches qui doivent être effectuées à l'aide du contrôleur Avi.

À l'aide de l'interface utilisateur d'Avi, vous devez créer un groupe d'adresses IP, créer un profil de surveillant de la santé personnalisé, créer un pool, installer le certificat SSL requis pour l'adresse IP virtuelle et créer un service virtuel.

À l'aide de l'adresse IP virtuelle utilisée dans le service virtuel, vous pouvez accéder au proxy inverse Web.

Conditions préalables

- Assurez-vous d'avoir déjà déployé Unified Access Gateway en tant que proxy inverse Web.

  Déploiement en tant que proxy inverse
- Assurez-vous que le contrôleur Avi est déployé et que vous avez accès au contrôleur et à l'interface utilisateur d'Avi.

Pour plus d'informations sur Avi Vantage, consultez la documentation relative à Avi.

Procédure

1 Créer un groupe d'adresses IP

Créez un groupe d'adresses IP qui contient une liste des serveurs Unified Access Gateway qui doivent être utilisés pour l'équilibrage de charge.

2 Créer un profil de surveillant de la santé personnalisé

Créez un profil de surveillant de la santé pour Unified Access Gateway sur Avi Vantage. Le profil de surveillant de la santé est utilisé pour surveiller la santé d'Unified Access Gateway.

3 Créer des pools

Les pools contiennent la liste des serveurs Unified Access Gateway et le profil de surveillant de la santé pour Unified Access Gateway. Les pools sont ensuite ajoutés au service virtuel.

4 Installer le certificat SSL requis pour l'adresse IP virtuelle

La connexion SSL s'arrête sur le service virtuelAvi. Par conséquent, le certificat SSL doit être attribué au service virtuel. Pour que cette attribution se produise, il est nécessaire d'installer le certificat SSL sur Avi Vantage.

5 Créer un service virtuel

Créez un service virtuel avec l'adresse IP virtuelle du serveur Unified Access Gateway. Il s'agit de l'adresse IP virtuelle à laquelle les périphériques clients se connectent.

Créer un groupe d'adresses IP

Créez un groupe d'adresses IP qui contient une liste des serveurs Unified Access Gateway qui doivent être utilisés pour l'équilibrage de charge.

Étant donné que les mêmes serveurs Unified Access Gateway sont utilisés comme membres de deux pools différents, les groupes d'adresses IP peuvent être attachés au pool plutôt que d'attacher directement les serveurs au pool. Toute modification de la configuration des membres du pool, par exemple l'ajout ou la suppression de serveurs, doit être effectuée au niveau du groupe d'adresses IP.

Procédure

1 Dans l'interface utilisateur d'Avi Vantage, accédez à **Modèles > Groupes**.

2 Cliquez sur **Créer un groupe d'adresses IP**.

3 Entrez le **Nom du groupe d'adresses IP**.

4 Dans la section **Informations sur l'adresse IP**, entrez l'adresse IP des serveurs Unified Access Gateway.

5 Cliquez sur **Ajouter**.

6 Cliquez sur **Enregistrer**.

Étape suivante

Créer un profil de surveillant de la santé personnalisé

Créer un profil de surveillant de la santé personnalisé

Créez un profil de surveillant de la santé pour Unified Access Gateway sur Avi Vantage. Le profil de surveillant de la santé est utilisé pour surveiller la santé d'Unified Access Gateway.

Pour plus d'informations sur le profil de surveillant de la santé, reportez-vous à la documentation d'Avi.

Procédure

1. Dans l'interface utilisateur d'Avi Vantage, accédez à **Modèles > Profils > Surveillants de la santé**.
2. Cliquez sur **Créer**.
3. Dans la fenêtre **Nouveau surveillant de la santé**, entrez les informations de profil pour Unified Access Gateway.
   a. Pour la valeur **Port du surveillant de la santé**, entrez `443`.
   b. Pour la valeur **Données de demande client**, entrez `GET /favicon.ico HTTP/1.1`.
   c. Pour le **Code de réponse**, sélectionnez `2XX`.
   d. Activez **Attributs SSL**.
   e. Pour **Profil SSL**, sélectionnez `System-Standard`.
   f. Pour la valeur **Code de réponse de maintenance**, entrez `503`.
4. Cliquez sur **Enregistrer**.

Étape suivante

Créer des pools

Créer des pools

Les pools contiennent la liste des serveurs Unified Access Gateway et le profil de surveillant de la santé pour Unified Access Gateway. Les pools sont ensuite ajoutés au service virtuel.

Un service virtuel pointe généralement vers un pool.

Procédure

1. Dans l'interface utilisateur d'Avi Vantage, accédez à **Applications > Pools**.
2. Cliquez sur **Créer un pool**.

3 Dans la fenêtre **Sélectionner un Cloud**, sélectionnez le Cloud qui appartient au type d'infrastructure du Cloud VMware vCenter/vSphere ESX.

   Le type d'infrastructure du Cloud est configuré dans le cadre du déploiement du contrôleur Avi.

4 Cliquez sur **Suivant**.

5 Dans la fenêtre **Nouveau pool**, entrez les informations requises, ainsi que les éléments suivants :

   a Dans le champ **Équilibrage de charge**, choisissez `Consistent Hash` avec `Source IP Address` en tant que clé de hachage.

   b Dans la section **Surveillants de la santé**, cliquez sur **Ajouter un surveillant actif**.

   c Sélectionnez le surveillant de la santé précédemment créé pour Unified Access Gateway.

6 Sélectionnez **Activer SSL**.

7 Pour **Profil SSL**, choisissez `System-Standard`.

8 Cliquez sur **Suivant**.

9 Dans l'onglet **Serveurs**, ajoutez le groupe d'adresses IP créé précédemment des serveurs Unified Access Gateway.

10 Cliquez sur **Suivant**.

11 Accédez à **Avancé > Vérifier**.

12 Cliquez sur **Enregistrer**.

Étape suivante

Installer le certificat SSL requis pour l'adresse IP virtuelle

Installer le certificat SSL requis pour l'adresse IP virtuelle

La connexion SSL s'arrête sur le service virtuelAvi. Par conséquent, le certificat SSL doit être attribué au service virtuel. Pour que cette attribution se produise, il est nécessaire d'installer le certificat SSL sur Avi Vantage.

Note Il est recommandé d'installer un certificat signé par une autorité de certification valide plutôt que d'utiliser des certificats auto-signés.

Pour plus d'informations sur l'installation du certificat SSL, reportez-vous à la documentation d'Avi.

Étape suivante

Créer un service virtuel

Créer un service virtuel

Créez un service virtuel avec l'adresse IP virtuelle du serveur Unified Access Gateway. Il s'agit de l'adresse IP virtuelle à laquelle les périphériques clients se connectent.

Procédure

1. Dans l'interface utilisateur d'Avi Vantage, accédez à **Applications > Services virtuels**.
2. Cliquez sur **Créer un service virtuel > Configuration avancée**.
3. Dans la fenêtre **Sélectionner un Cloud**, sélectionnez le Cloud qui appartient au type d'infrastructure du Cloud VMware vCenter/vSphere ESX.

   Le type d'infrastructure du Cloud est configuré dans le cadre du déploiement du contrôleur Avi.
4. Dans la fenêtre **Nouveau service virtuel**, configurez le service virtuel.
   a. Entrez le nom du service virtuel.
   b. Entrez l'adresse IP virtuelle.
   c. Sous **Services**, entrez le numéro de port `443`.
   d. Pour le numéro de port `443`, cochez la case **SSL**.

      SSL est activé pour le port `443`.
   e. Pour **Profil d'application**, sélectionnez `System-Secure-HTTP`.
   f. Sélectionnez le **Pool** précédemment créé pour Unified Access Gateway.
   g. Pour **Profil SSL**, sélectionnez `System-Standard`.
   h. Sélectionnez le certificat SSL précédemment installé.
5. Cliquez sur **Suivant**.
6. Accédez à l'onglet **Avancé**.
7. Cliquez sur **Enregistrer**.

Étape suivante

Accédez au proxy inverse Web à l'aide de l'adresse IP virtuelle.

Haute disponibilité d'Unified Access Gateway

Unified Access Gateway pour les produits informatiques et les services d'utilisateurs finaux nécessite une haute disponibilité pour les déploiements de Workspace ONE et de VMware Horizon sur site. En revanche, l'utilisation d'équilibrages de charge tiers augmente la complexité du processus de déploiement et de dépannage. Cette solution réduit le besoin d'un équilibrage de charge tiers dans la zone DMZ se trouvant devant Unified Access Gateway.

Note Cette solution n'est pas un équilibrage de charge générique.

Unified Access Gateway continue à prendre en charge les équilibrages de charge tiers devant, pour les utilisateurs qui préfèrent ce mode de déploiement. Pour plus d'informations, consultez le document Topologies d'équilibrage de charge Unified Access Gateway. La haute disponibilité d'Unified Access Gateway n'est pas prise en charge pour les déploiements d'Amazon AWS et de Microsoft Azure.

Implémentation

Unified Access Gateway nécessite l'adresse IP virtuelle IPv4 et un ID de groupe provenant de l'administrateur. Unified Access Gateway attribue l'adresse IP virtuelle à l'un des nœuds seulement dans le cluster configuré avec la même adresse IP virtuelle et le même ID de groupe. En cas d'échec de l'instance d'Unified Access Gateway contenant l'adresse IP virtuelle, celle-ci est réattribuée automatiquement à l'un des nœuds disponibles dans le cluster. La distribution de la haute disponibilité et des charges se produit entre les nœuds du cluster configuré avec le même ID de groupe.

Plusieurs connexions provenant de la même adresse IP source sont envoyées à la même instance d'Unified Access Gateway qui traite la première connexion à partir de ce client pour Horizon et le proxy inverse Web. Cette solution prend en charge 10 000 connexions simultanées dans le cluster.

Note L'affinité de session est requise pour ces cas spécifiques.

Pour les services VMware Tunnel (VPN par application), Secure Email Gateway et Content Gateway, la distribution de la haute disponibilité et des charges s'effectue à l'aide de l'algorithme Least Connection.

Note Ces connexions sont sans état et l'affinité de session n'est pas nécessaire.

Mode et Affinité

Des services différents d'Unified Access Gateway requièrent des algorithmes différents.

- Pour VMware Horizon et le proxy inverse Web : l'affinité d'adresse IP source est utilisée avec l'algorithme Round Robin pour la distribution.
- Pour VMware Tunnel (VPN par application) et Content Gateway : il n'existe aucune affinité de session et l'algorithme Least Connection est utilisé pour la distribution.

Méthodes permettant de distribuer le trafic entrant :

1. Affinité d'adresse IP source : gère l'affinité entrez la connexion client et le nœud Unified Access Gateway. Toutes les connexions ayant la même adresse IP source sont envoyées au même nœud Unified Access Gateway.
2. Mode Round Robin avec haute disponibilité : les demandes de connexion entrante sont distribuées séquentiellement dans le groupe de nœuds Unified Access Gateway.

3 Mode Least Connection avec haute disponibilité : une nouvelle demande de connexion est envoyée au nœud Unified Access Gateway avec le nombre minimal de connexions actives des clients.

Note L'affinité d'adresse IP source fonctionne uniquement si l'adresse IP de la connexion entrante est unique pour chaque connexion client. Exemple : s'il y a un composant réseau, tel qu'une passerelle SNAT entre les clients et Unified Access Gateway, l'affinité d'adresse IP source ne fonctionne pas, car le trafic entrant depuis plusieurs clients différents vers Unified Access Gateway utilise la même adresse IP source.

Note L'adresse IP virtuelle doit appartenir au même sous-réseau que l'interface `eth0`.

Conditions préalables

- L'adresse IP virtuelle utilisée pour la haute disponibilité doit être unique et disponible. Unified Access Gateway ne confirme pas si elle est unique lors de la configuration. L'adresse IP peut s'afficher comme étant attribuée, mais elle peut ne pas être accessible si une machine virtuelle ou physique est associée à l'adresse IP.
- ID de groupe doit être unique dans un sous-réseau donné. Si l'ID de groupe n'est pas unique, une adresse IP virtuelle incompatible peut être attribuée au groupe. Par exemple, au minimum deux nœuds Unified Access Gateway peuvent finir par obtenir la même adresse IP virtuelle. Cela peut provoquer le basculement de l'adresse IP virtuelle entre plusieurs nœuds Unified Access Gateway.
- Pour configurer la haute disponibilité d'Horizon ou du proxy inverse Web, assurez-vous que le certificat de serveur TLS sur tous les nœuds d'Unified Access Gateway sont identiques.

Limites

- IPv4 est pris en charge pour l'adresse IP virtuelle flottante. IPv6 n'est pas pris en charge.
- Seule la haute disponibilité de TCP est prise en charge.
- La haute disponibilité d'UDP n'est pas prise en charge.
- Avec le cas d'utilisation de VMware Horizon, seul le trafic de l'API XML vers le Serveur de connexion Horizon utilise la haute disponibilité. La haute disponibilité n'est pas utilisée pour distribuer la charge du trafic de protocole (affichage) tel que Blast, PCoIP, RDP. Par conséquent, les adresses IP individuelles (ainsi que l'adresse IP virtuelle) des nœuds Unified Access Gateway doivent être également accessibles aux clients de VMware Horizon.

Configuration requise pour la haute disponibilité dans chaque instance d'Unified Access Gateway

Pour la configuration de la haute disponibilité dans Unified Access Gateway, consultez la section Configurer les paramètres de la haute disponibilité.

Configurer les paramètres de la haute disponibilité

Pour utiliser la haute disponibilité d'Unified Access Gateway, activez et configurez les **Paramètres de la haute disponibilité** dans l'interface utilisateur d'administration.

Procédure

1 Dans la section **Configurer manuellement** de l'interface utilisateur d'administration, cliquez sur **Sélectionner**.

2 Dans la section **Paramètres avancés**, cliquez sur l'icône en forme d'engrenage **Paramètres de la haute disponibilité**.

3 Sur la page **Paramètres de la haute disponibilité**, remplacez **DISABLED** par **ENABLED** pour activer la haute disponibilité.

4 Configurez les paramètres.

Option	Description
Adresse IP virtuelle	Adresse IP virtuelle valide utilisée par la haute disponibilité. **Note** L'adresse IP virtuelle utilisée pour la haute disponibilité doit être unique et disponible. Si aucune adresse IP unique n'est définie, l'adresse IP peut s'afficher comme étant attribuée, mais elle peut ne pas être accessible si une machine virtuelle ou physique est associée à l'adresse IP.
ID de groupe	ID de groupe pour la haute disponibilité. Entrez une valeur numérique comprise entre 1 et 255. **Note** ID de groupe doit être unique dans un sous-réseau donné. Si aucun ID de groupe unique n'est défini, une adresse IP virtuelle incompatible peut être attribuée au groupe. Par exemple, lorsque l'adresse IP d'au moins deux passerelles Unified Access Gateway peut finir par essayer obtenir la même adresse IP virtuelle.

5 Cliquez sur **Enregistrer**.

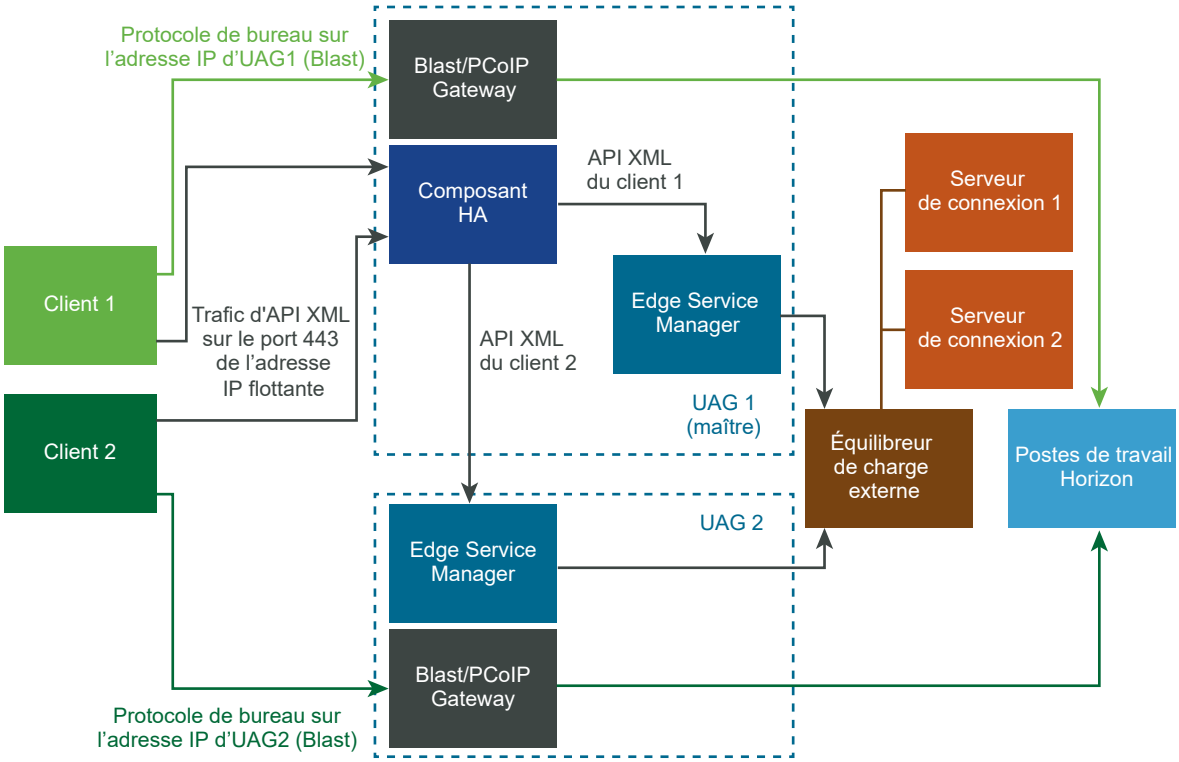
- Les différents états de **Paramètres de la haute disponibilité** indiquent les éléments suivants :
- **Non configuré** : indique que les **Paramètres de la haute disponibilité** ne sont pas configurés.
- **Traitement** : indique que les **Paramètres de la haute disponibilité** sont en cours de traitement pour prendre effet.
- **Maître** : indique que le nœud est choisi comme maître dans le cluster et qu'il répartit le trafic.
- **Sauvegarde** : indique que le nœud est dans l'état de sauvegarde dans le cluster.
- **Erreur** : indique que le nœud peut contenir des erreurs de configuration du proxy haute disponibilité.

Unified Access Gateway configuré avec Horizon

Plusieurs instances d'Unified Access Gateway sont configurées avec les mêmes paramètres d'Horizon, et la haute disponibilité est activée sur chaque instance d'Unified Access Gateway.

Un nom d'hôte externe commun est utilisé pour le protocole API XML. Ce nom d'hôte externe commun est mappé à l'adresse IP flottante configurée dans les paramètres de la haute disponibilité sur les nœuds d'Unified Access Gateway. Le trafic du poste de travail n'utilise pas la haute disponibilité, et la charge n'est pas distribuée. Cette solution nécessite ainsi VIP N + 1 pour Horizon où N est le nombre de nœuds Unified Access Gateway déployés. Sur chaque instance d'Unified Access Gateway, l'URL externe de Blast, de PCoIP et de Tunnel doit être le mappage des adresses IP externes ou des noms d'hôte à l'adresse IP eth0 correspondante d'Unified Access Gateway. Les clients qui utilisent un réseau insuffisant pour se connecter en UDP à l'API XML accèdent à la même instance d'Unified Access Gateway, celle qui a reçu la première connexion UDP à l'API XML.

Figure 1-2. Unified Access Gateway configuré à l'aide d'Horizon



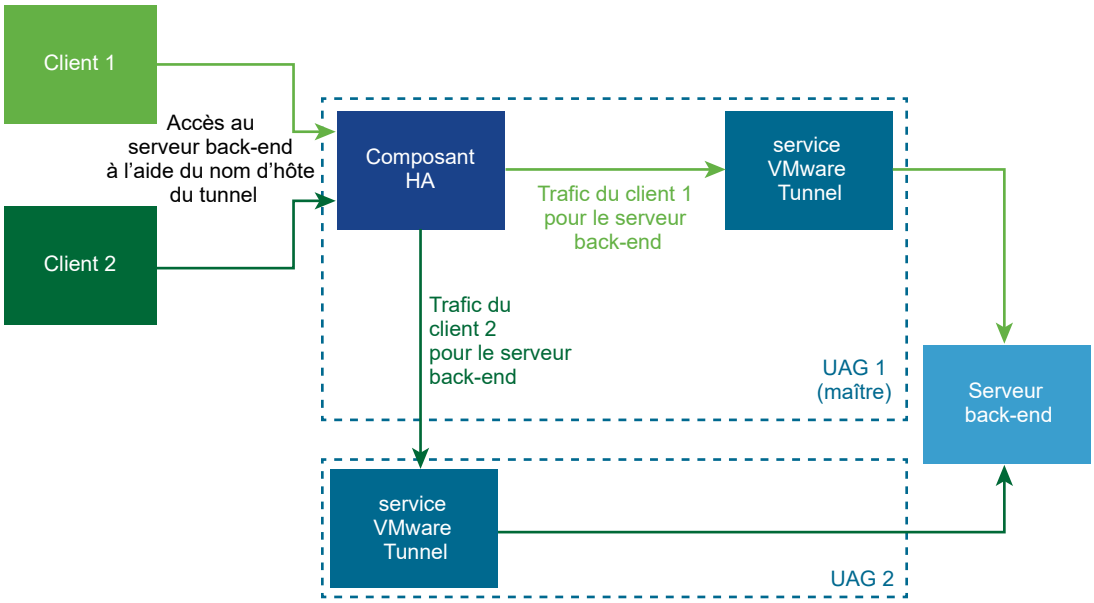
Mode et affinité : l'affinité est basée sur l'adresse IP source. La première connexion à partir du client est distribuée à l'aide du mécanisme Round Robin. Cependant, les connexions suivantes à partir du même client sont envoyées à la même instance d'Unified Access Gateway qui a géré la première connexion.

Connexion de VMware Tunnel (VPN par application) à l'aide de la configuration de base

VMware Tunnel (VPN par application) est configuré avec les paramètres de base dans la console Workspace ONE UEM.

Le nom d'hôte du serveur Tunnel configuré dans la console Workspace ONE UEM des paramètres VMware Tunnel (VPN par application) est résolu à l'adresse IP flottante configurée pour la haute disponibilité dans Unified Access Gateway. Les connexions sur cette adresse IP flottante sont distribuées entre les nœuds configurés dans Unified Access Gateway.

Figure 1-3. Connexion de VMware Tunnel (VPN par application) à l'aide de la configuration de base



Mode et affinité : l'algorithme Least Connections est utilisé pour la distribution de la haute disponibilité et des charges. Une nouvelle demande est envoyée au serveur avec le nombre minimal de connexions actuelles aux clients. L'affinité de session n'est pas nécessaire, car il s'agit de connexions sans état.

Connexions de VMware Tunnel (VPN par application) en mode cascade

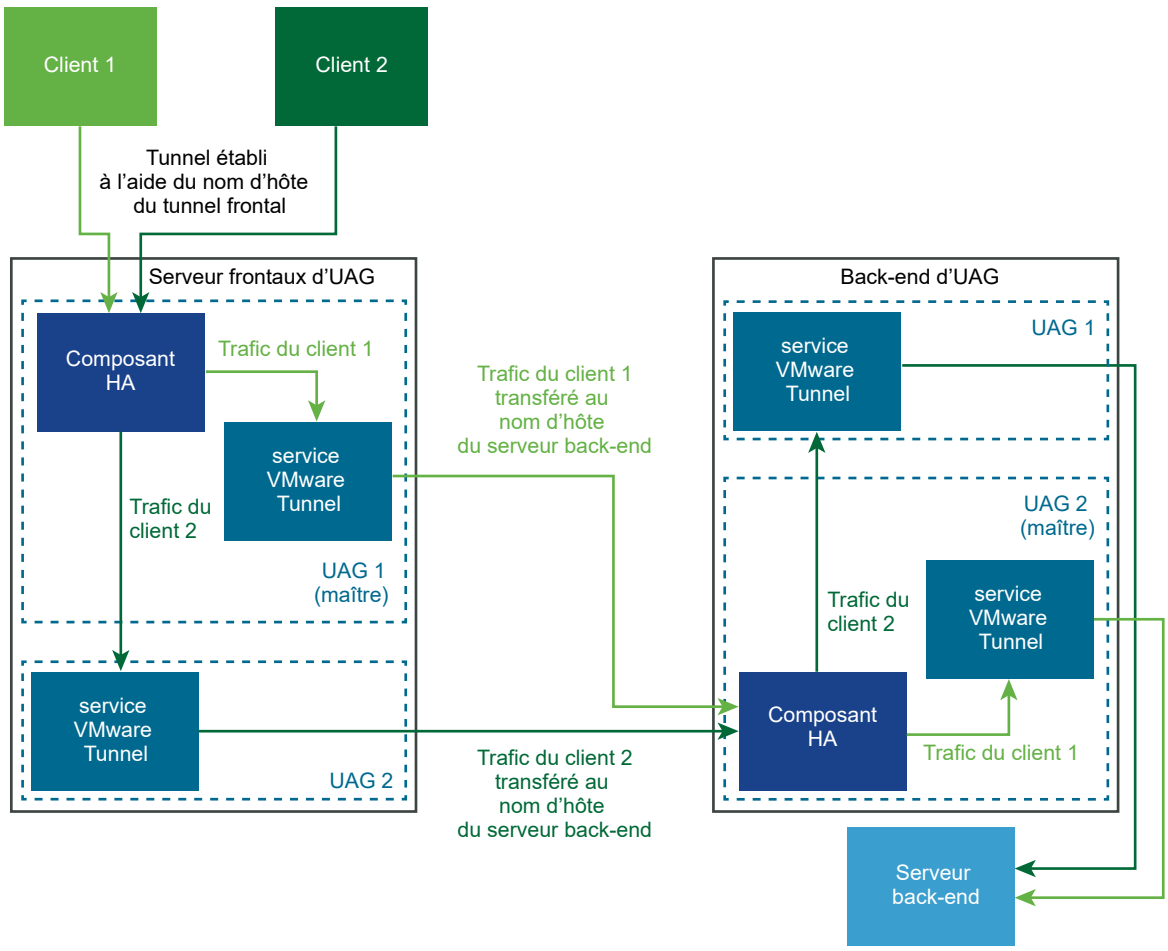
VMware Tunnel (VPN par application) est configuré avec des paramètres de cascade dans la console Workspace ONE UEM.

Deux noms d'hôte de serveur Tunnel sont configurés dans la console Workspace ONE UEM pour le serveur frontal et pour le back-end. Nous pouvons déployer respectivement deux jeux de nœuds dans Unified Access Gateway pour le serveur frontal et le back-end.

Les nœuds frontaux dans Unified Access Gateway sont configurés avec un nom d'hôte du serveur Tunnel frontal. Les paramètres de la haute disponibilité sur les nœuds frontaux dans Unified Access Gateway sont configurés avec une adresse IP flottante externe. Le nom d'hôte du serveur Tunnel frontal est résolu à l'adresse IP flottante externe. Les connexions sur cette adresse IP flottante externe sont distribuées parmi les nœuds frontaux dans Unified Access Gateway.

Les nœuds back-end dans Unified Access Gateway sont configurés avec le nom d'hôte du serveur Tunnel back-end. Les paramètres de la haute disponibilité sur les nœuds back-end dans Unified Access Gateway sont configurés avec une adresse IP flottante interne. Le service VMware Tunnel (VPN par application) sur les nœuds frontaux dans Unified Access Gateway achemine le trafic vers le back-end à l'aide du nom d'hôte du serveur Tunnel back-end. Le nom d'hôte du serveur Tunnel back-end est résolu à l'adresse IP flottante interne. Les connexions sur cette adresse IP flottante interne sont distribuées parmi les nœuds back-end dans Unified Access Gateway.

Figure 1-4. Connexions de VMware Tunnel (VPN par application) en mode cascade



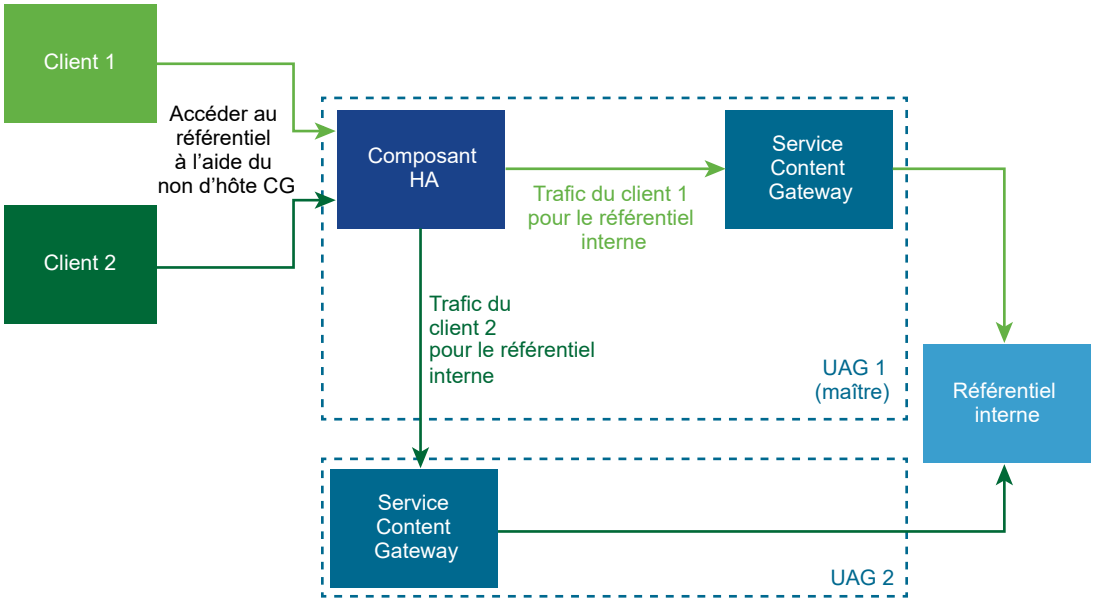
Mode et affinité : l'algorithme Least Connections est utilisé pour la distribution de la haute disponibilité et des charges. Une nouvelle demande est envoyée au serveur avec le nombre minimal de connexions actuelles aux clients. L'affinité de session n'est pas nécessaire, car il s'agit de connexions sans état.

Configuration de base de Content Gateway

Content Gateway est configuré avec des paramètres de base dans la console Workspace ONE UEM.

Le nom d'hôte du serveur Content Gateway configuré dans la console Workspace ONE UEM pour les paramètres de Content Gateway est résolu à l'adresse IP flottante configurée pour la haute disponibilité dans Unified Access Gateway. Les connexions sur cette adresse IP flottante sont équilibrées en charge entre les nœuds configurés dans Unified Access Gateway.

Figure 1-5. Configuration de base de Content Gateway



Mode et affinité : l'algorithme Least Connections est utilisé pour la distribution de la haute disponibilité et des charges. Une nouvelle demande est envoyée au serveur avec le nombre minimal de connexions actuelles aux clients. L'affinité de session n'est pas nécessaire, car il s'agit de connexions sans état.

Content Gateway avec configuration du relais et du point de terminaison

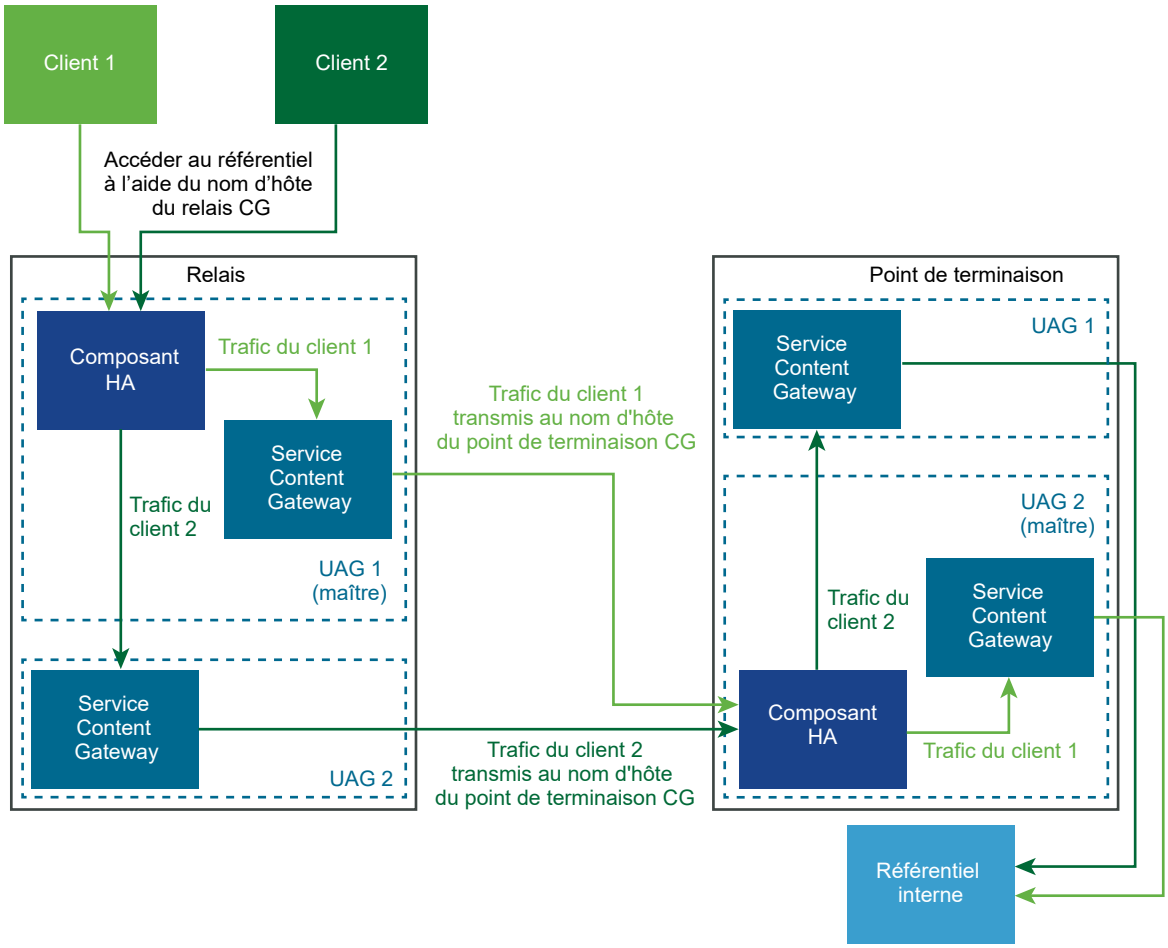
Content Gateway est définie avec la configuration du relais et du point de terminaison dans la console Workspace ONE UEM.

Deux noms d'hôte du serveur Content Gateway sont configurés dans la console Workspace ONE UEM pour le relais et le point de terminaison. Deux jeux de nœuds dans Unified Access Gateway sont déployés pour le relais et le point de terminaison.

Les nœuds de relais dans Unified Access Gateway sont configurés avec le nom d'hôte du serveur Content Gateway de relais. Les paramètres de la haute disponibilité sur les nœuds de relais dans Unified Access Gateway sont configurés à l'aide d'une adresse IP flottante externe. Le nom d'hôte du serveur Content Gateway de relais est résolu à l'adresse IP flottante externe. Les connexions sur cette adresse IP flottante externe sont équilibrées en charge entre les nœuds de relais dans Unified Access Gateway.

Les nœuds de point de terminaison dans Unified Access Gateway sont configurés avec le nom d'hôte du serveur Tunnel de point de terminaison. Les paramètres de la haute disponibilité sur les nœuds de point de terminaison dans Unified Access Gateway sont configurés à l'aide d'une adresse IP flottante interne. Le service Content Gateway devant Unified Access Gateway achemine le trafic au point de terminaison à l'aide du nom d'hôte du serveur Content Gateway de point de terminaison. Le nom d'hôte du serveur Content Gateway de point de terminaison est résolu à l'adresse IP flottante interne. Les connexions sur cette adresse IP flottante interne sont équilibrées en charge entre les nœuds de point de terminaison dans Unified Access Gateway.

Figure 1-6. Content Gateway avec configuration du relais et du point de terminaison



Mode et affinité : l'algorithme Least Connections est utilisé pour la distribution de la haute disponibilité et des charges. Une nouvelle demande est envoyée au serveur avec le nombre minimal de connexions actuelles aux clients. L'affinité de session n'est pas nécessaire, car il s'agit de connexions sans état.

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.

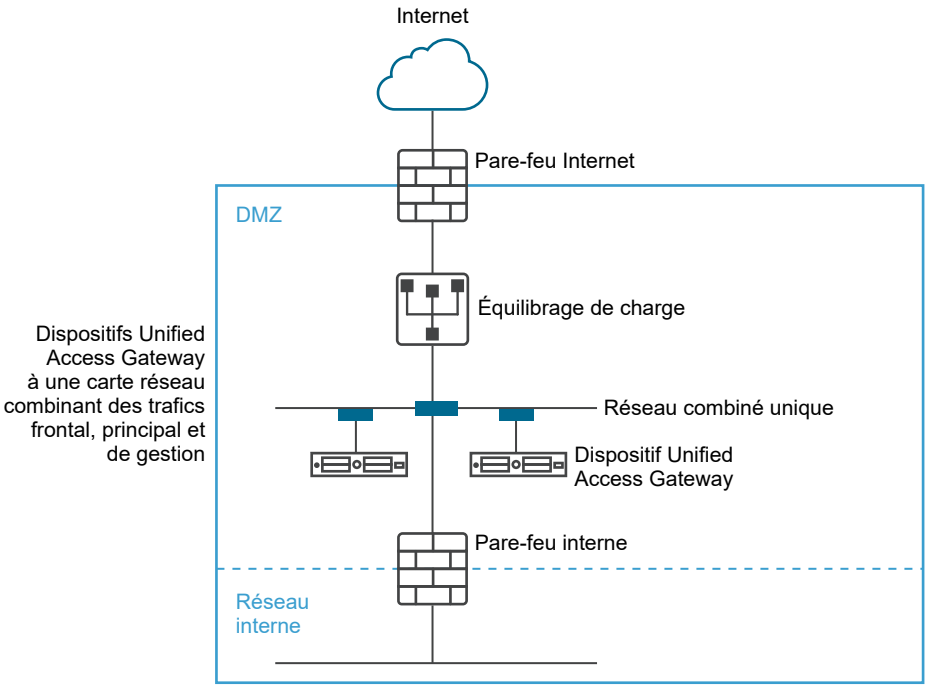
Vous pouvez spécifier un, deux ou trois paramètres de carte réseau, appelés onenic, twonic ou threenic.

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.

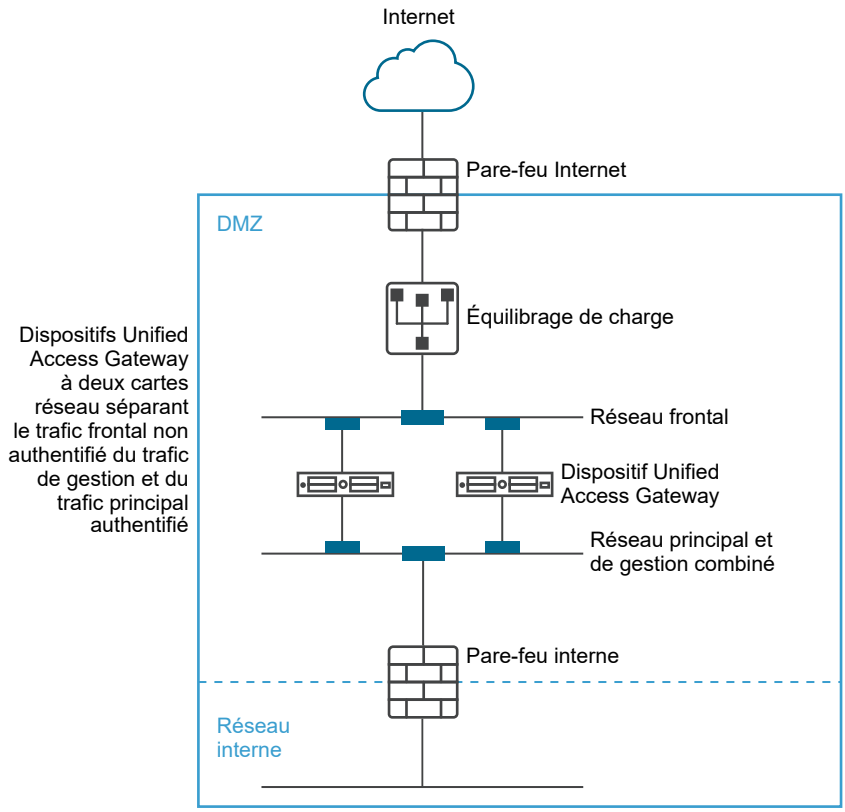
Figure 1-7. Option à une seule carte réseau d'Unified Access Gateway



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

Une option alternative 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 1-8. 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.

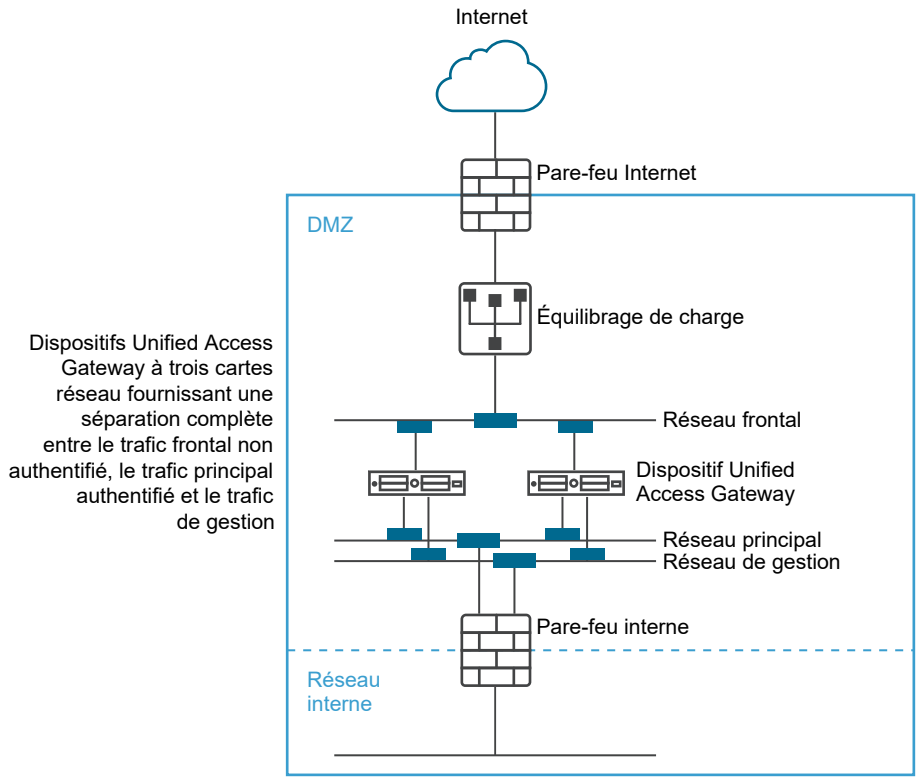
Si un périphérique sur le réseau frontal non authentifié, comme l'équilibrage de charge, a été compromis, il n'est pas possible de reconfigurer ce périphérique pour contourner Unified Access Gateway dans ce déploiement à deux cartes réseau. Il associe des règles de pare-feu de couche 4 à une sécurité 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 1-9. Option à trois cartes réseau d'Unified Access Gateway



Mettre à niveau sans interruption

La mise à niveau sans interruption vous permet de mettre Unified Access Gateway à niveau sans interruption pour les utilisateurs.

Lorsque la valeur **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.

Conditions préalables

- 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 REST API `GET https://UAG-IP-Address: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.

  Note
  - N'utilisez pas une autre URL que `GET https://UAG-IP-Address:443/favicon.ico`. Cela entraînerait une réponse d'état incorrect et une fuite des ressources.
  - Si le paramètre **Haute disponibilité** est activé, l'option **Mode de mise au repos (sans interruption)** s'applique uniquement au proxy inverse Web et à Horizon.
  - Si des équilibrages de charge tiers sont utilisés, l'option **Mode de mise au repos (sans interruption)** est applicable s'ils sont configurés pour effectuer un contrôle de santé en utilisant `GET /favicon.ico`.

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 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.

Étape suivante

- Pour un déploiement vSphere :
  a. Sauvegardez le fichier JSON en exportant le fichier.
  b. Supprimez l'ancien dispositif Unified Access Gateway.
  c. Déployez la nouvelle version du dispositif Unified Access Gateway.
  d. Importez le fichier JSON que vous avez précédemment exporté.

- Pour un déploiement PowerShell :
  a Supprimez le dispositif Unified Access Gateway.
  b Redéployez Unified Access Gateway avec le même fichier INI qui a été utilisé lors du premier déploiement. Reportez-vous à la section Utilisation de PowerShell pour déployer le dispositif Unified Access Gateway.

Note Si un message d'erreur relatif au certificat de serveur Tunnel s'affiche après la réactivation de l'équilibrage de charge, appliquez le même certificat de serveur SSL et les fichiers PEM de clé privée qui ont été utilisés précédemment sur le dispositif Unified Access Gateway. Cela est nécessaire, car le fichier JSON ou INI ne peut pas contenir de clés privées associées à un certificat de serveur SSL, étant donné que les clés privées ne peuvent pas être exportées pour des raisons de sécurité. Avec un déploiement de PowerShell, cette opération s'effectue automatiquement et il n'est pas nécessaire de réappliquer le certificat.

Déploiement d'Unified Access Gateway sans profil de protocole réseau (NPP)

La dernière version d'Unified Access Gateway n'accepte pas les valeurs de masque de réseau ou de préfixe et les paramètres de passerelle par défaut du profil de protocole réseau.

Vous devez fournir ces informations de mise en réseau lors du déploiement de votre instance d'Unified Access Gateway.

Dans le cas d'un déploiement statique, lors de la configuration de votre instance d'Unified Access Gateway, spécifiez l'adresse IPv4 ou IPv6, le masque de réseau ou le préfixe des cartes réseau respectives ainsi que la passerelle par défaut IPv4/IPv6. Si vous ne fournissez pas ces informations, l'allocation d'adresses IP utilise par défaut DHCPV4 + DHCPV6.

Tenez compte des points suivants lorsque vous configurez les propriétés de la mise en réseau :

- Si vous sélectionnez STATICV4 pour l'`IPMode` d'une carte réseau, vous devez spécifier l'adresse IPv4 et le masque de réseau de cette carte réseau.
- Si vous sélectionnez STATICV6 pour l'`IPMode` d'une carte réseau, vous devez spécifier l'adresse IPv6 et le masque de réseau de cette carte réseau.
- Si vous sélectionnez STATICV4 et STATIC V6 pour l'`IPMode` d'une carte réseau, vous devez spécifier l'adresse IPv4 et IPv6 ainsi que le masque de réseau de cette carte réseau.
- Si vous ne fournissez pas les informations d'adresse et de masque de réseau, c'est le serveur DHCP qui alloue les valeurs.
- Les propriétés de la passerelle IPv4 et IPv6 par défaut sont facultatives et doivent être spécifiées si Unified Access Gateway doit communiquer avec une adresse IP qui ne se trouve pas sur un segment local d'une carte réseau dans Unified Access Gateway.

Reportez-vous à la section Déploiement d'Unified Access Gateway au moyen de l'assistant de modèle OVF pour plus d'informations sur la configuration des propriétés de la mise en réseau.

Participer au programme d'amélioration du produit ou le quitter

Le programme d'amélioration du produit (CEIP) VMware fournit des informations que VMware utilise pour améliorer ses produits et services, pour résoudre des problèmes et pour vous conseiller sur la meilleure façon de déployer et d'utiliser ses produits.

Ce produit participe au programme d'amélioration du produit VMware (CEIP). Des informations détaillées sur les données collectées dans le cadre du CEIP et sur le but dans lequel VMware les utilise sont définies dans le Centre de confiance et d'assurance disponible sur le site https://www.vmware.com/fr/solutions/trustvmware/ceip.html.

Vous pouvez rejoindre ou quitter le CEIP pour ce produit à tout moment à partir de l'interface utilisateur d'administration.

Procédure

1 Dans **Paramètres avancés > Configuration système**, sélectionnez Oui ou Non.

   Si vous sélectionnez Oui, la boîte de dialogue Programme d'amélioration du produit s'affiche avec la case cochée pour indiquer que vous rejoignez le programme.

2 Passez en revue les informations dans la boîte de dialogue et cliquez sur **Fermer**.

3 Cliquez sur **Enregistrer** sur la page Configuration système pour enregistrer vos modifications.

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.
- 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.

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

Note Dans les deux méthodes de déploiement ci-dessus, si vous ne fournissez pas le mot de passe de l'interface utilisateur d'administration, vous ne pouvez pas ajouter ultérieurement un utilisateur de l'interface utilisateur d'administration pour permettre l'accès à celle-ci ou à l'API. Si vous souhaitez le faire, vous devez redéployer votre instance Unified Access Gateway à l'aide d'un mot de passe valide.

Lisez les sections suivantes :

- Utilisation de l'assistant de modèle OVF pour déployer Unified Access Gateway
- Configuration d'Unified Access Gateway à partir des pages de configuration d'administration
- Mise à jour des certificats signés du serveur SSL

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 de 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 de l'OVA prend en charge les services Edge suivants :

- Horizon (authentification relais et authentification par certificat)

  Note L'authentification par certificat inclut l'authentification par carte à puce et l'authentification par certificat de périphérique.

- Tunnel par application avec VMware

Important 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. L'authentification d'Horizon Edge n'est pas disponible dans la version FIPS.

Options de dimensionnement d'Unified Access Gateway

Pour simplifier le déploiement du dispositif Unified Access Gateway en tant que passerelle de sécurité Workspace ONE, les options de dimensionnement sont ajoutées aux configurations de déploiement dans le dispositif. La configuration de déploiement propose un choix entre une machine virtuelle standard, grande et extra grande.

- **Standard :** cette configuration est recommandée pour le déploiement d'Horizon prenant en charge jusqu'à 2 000 connexions d'Horizon, selon la capacité du serveur de connexion. Elle est également recommandée pour les déploiements de Workspace ONE UEM (cas d'utilisation mobiles) jusqu'à 10 000 connexions simultanées.
- **Grand :** cette configuration est recommandée pour les déploiements de Workspace ONE UEM, où Unified Access Gateway doit prendre en charge plus de 50 000 connexions simultanées. Cette taille permet à Content Gateway, Tunnel par application et Proxy et Proxy inverse d'utiliser le même dispositif Unified Access Gateway.
- **Extra grand** : cette configuration est recommandée pour les déploiements de Workspace ONE UEM. Cette taille permet à Content Gateway, Tunnel par application et Proxy et Proxy inverse d'utiliser le me^me dispositif Unified Access Gateway.

- **Note** Options de VM pour les déploiements Standard, Grand et Extra grand :
  - Standard : 2 cœurs et 4 Go de RAM
  - Grand : 4 cœurs et 16 Go de RAM
  - Extra grand : 8 cœurs et 32 Go de RAM

Pour plus d'informations sur les recommandations de dimensionnement d'Unified Access Gateway, vous pouvez afficher l'option Nombre maximal de configurations VMware.

Conditions préalables

- 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.
- 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.
- 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 *xxxxxxx* le numéro de build.
- En cas de déploiement Hyper-V, si vous mettez à niveau Unified Access Gateway avec une adresse IP statique, supprimez le dispositif antérieur avant de déployer l'instance d'Unified Access Gateway plus récente.

- Pour mettre à niveau un dispositif antérieur vers une nouvelle instance d'Unified Access Gateway sans interruption de service pour les utilisateurs, reportez-vous à la section Mettre à niveau sans interruption.

Procédure

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

Pour un réseau IPv4, utilisez le client natif vSphere ou le client Web vSphere. 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. Les déploiements ESXi et Hyper-V disposent de deux options pour définir l'attribution IP d'Unified Access Gateway. Si vous effectuez une mise à niveau pour Hyper-V, supprimez l'ancienne zone avec la même adresse IP avant de déployer la zone avec la nouvelle adresse. Pour ESXi, vous pouvez désactiver l'ancienne zone et en déployer une nouvelle avec la même adresse IP à l'aide de l'attribution statique.

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 ou IPV6, vous pouvez utiliser une, deux ou trois interfaces réseau (cartes 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. Parallèlement au nombre de cartes réseau, vous pouvez également choisir les options de déploiement **Standard** ou **Grand** pour Unified Access Gateway. **Note** Options de VM pour les déploiements **Standard** et **Grand** : ■ **Standard** - 2 cœurs et 4 Go de RAM ■ **Grand** - 4 cœurs et 16 Go de RAM

Option	Description
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.
Configuration des réseaux/Mappage réseau	Si vous utilisez vSphere Web Client, la page Configuration des réseaux vous permet de mapper chaque carte réseau à un réseau et de spécifier des paramètres de protocole. Mappez les réseaux utilisés dans ce modèle OVF aux réseaux de votre inventaire. a 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. 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. b 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. Si vous n'utilisez qu'une seule carte réseau, toutes les lignes sont mappées vers le même réseau. c Si vous avez une troisième carte réseau, sélectionnez également la troisième ligne et remplissez les paramètres. Si vous n'utilisez que deux cartes réseau, pour cette troisième ligne **BackendNetwork**, sélectionnez le réseau que vous avez utilisé pour **ManagementNetwork**. **Note** Si le menu déroulant **Protocole IP** s'affiche, ignorez-le et n'y faites aucune sélection. La sélection réelle du protocole IP (IPv4, IPv6 ou les deux) est liée au mode IP qui a été défini dans l'IPMode des cartes réseau 1 (eth0), 2 (eth1) et 3 (eth2) lors de la personnalisation des propriétés de la mise en réseau.

Option	Description

Personnaliser les propriétés réseau	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. En regard de chacune des cartes réseau, pour STATICV4, vous devez entrer l'adresse IPv4 de la carte réseau. Pour STATICV6, vous devez entrer l'adresse IPv6 de la carte réseau. Si vous ne renseignez pas les cases, l'allocation d'adresses IP prend par défaut les valeurs DHCPV4 + DHCPV6.
	
	Important La dernière version d'Unified Access Gateway n'accepte pas les valeurs de masque de réseau ou de préfixe et les paramètres de passerelle par défaut du profil de protocole réseau (NPP). Pour configurer Unified Access Gateway avec l'allocation d'adresses IP statiques, vous devez configurer le masque de réseau ou un préfixe sous Propriétés du réseau. Les valeurs suivantes ne sont pas renseignées depuis NPP.
	
	Note Les valeurs sont sensibles à la casse.
	
	■ **IPMode de la carte réseau 1 (eth0) : STATICV4/STATICV6/DHCPV4/ DHCPV6/AUTOV6/STATICV4+STATICV6/STATICV4+DHCPV6/ STATICV4+AUTOV6/DHCPV4+AUTOV6/DHCPV4+STATICV6/ DHCPV4+DHCPV6/DHCPV4+AUTOV6** .
	■ **IPMode de la carte réseau 2 (eth1) : STATICV4/STATICV6/DHCPV4/ DHCPV6/AUTOV6/STATICV4+STATICV6/STATICV4+DHCPV6/ STATICV4+AUTOV6/DHCPV4+AUTOV6/DHCPV4+STATICV6/ DHCPV4+DHCPV6/DHCPV4+AUTOV6** .
	■ **IPMode de la carte réseau 3 (eth2) : STATICV4/STATICV6/DHCPV4/ DHCPV6/AUTOV6/STATICV4+STATICV6/STATICV4+DHCPV6/ STATICV4+AUTOV6/DHCPV4+AUTOV6/DHCPV4+STATICV6/ DHCPV4+DHCPV6/DHCPV4+AUTOV6** .
	■ **Liste de règles de transfert séparées par une virgule au format {tcp|udp}/listening-port-number/destination-ip-address:destination-port-nu**. Par exemple, pour IPv4, `tcp/5262/10.110.92.129:9443`, `tcp/5263/10.20.30.50:7443`.
	■ **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 de routes personnalisées IPv4 séparées par une virgule pour la carte réseau 1 (eth0) au format ipv4-network-address/bits ipv4-gateway-address**. Par exemple, `20.2.0.0/16 10.2.0.1,20.9.0.0/16 10.2.0.2,10.2.0.1/32`
	  Note Si la valeur **adresse-passerelle-ipv4** n'est pas spécifiée, la route respective qui est ajoutée dispose d'une passerelle de 0.0.0.0.
	■ **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.
	■ **Masque de réseau IPv4 de la carte réseau 1 (eth0)**. Entrez le masque de réseau IPv4 de la carte réseau.
	■ **Préfixe IPv6 de la carte réseau 1 (eth0)**. Entrez le préfixe IPv6 de la carte réseau.

Option	Description
	■ **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` ■ **Passerelle par défaut IPv4**. Entrez une passerelle IPv4 par défaut si Unified Access Gateway doit communiquer avec une adresse IP qui ne se trouve pas sur un segment local d'une carte réseau dans Unified Access Gateway. ■ **Passerelle par défaut IPv6**. Entrez une passerelle IPv6 par défaut si Unified Access Gateway doit communiquer avec une adresse IP qui ne se trouve pas sur un segment local d'une carte réseau dans Unified Access Gateway. ■ **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**. Par exemple, `20.2.0.0/16 10.2.0.1,20.9.0.0/16 10.2.0.2,10.2.0.1/32` **Note** Si la valeur **adresse-passerelle-ipv4** n'est pas spécifiée, la route respective qui est ajoutée dispose d'une passerelle de 0.0.0.0 ■ **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. ■ **Masque de réseau IPv4 de la carte réseau 2 (eth1)**. Entrez le masque de réseau IPv4 de cette carte réseau. ■ **Préfixe IPv6 de la carte réseau 2 (eth1)**. Entrez le préfixe IPv6 de cette 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**. Par exemple, `20.2.0.0/16 10.2.0.1,20.9.0.0/16 10.2.0.2,10.2.0.1/32` **Note** Si la valeur **adresse-passerelle-ipv4** n'est pas spécifiée, la route respective qui est ajoutée dispose d'une passerelle de 0.0.0.0 ■ **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. ■ **Masque de réseau IPv4 de la carte réseau 3 (eth2)**. Entrez le masque de réseau IPv4 de cette carte réseau. ■ **Préfixe IPv6 de la carte réseau 3 (eth2)**. Entrez le préfixe IPv6 de cette carte réseau. ■ **Mot de passe de l'utilisateur racine de la VM**. Entrez le mot de passe de l'utilisateur racine pour vous connecter à la console UAG. ■ **Mot de passe de l'interface utilisateur d'administration**. Entrez le mot de passe de l'utilisateur Admin pour configurer Unified Access Gateway à partir de l'interface utilisateur d'administration et également accéder aux REST API. Les autres paramètres sont facultatifs ou ont déjà un paramètre par défaut.
Activer SSH	Option permettant d'activer SSH pour l'accès à Unified Access Gateway.

Option	Description
Autoriser la connexion racine SSH à l'aide du mot de passe	Option permettant d'accéder à Unified Access Gateway à l'aide d'une connexion racine SSH et d'un mot de passe. Par défaut, la valeur de cette option est `true`.
Autoriser la connexion racine SSH à l'aide d'une paire de clés	Option permettant d'accéder à Unified Access Gateway à l'aide d'une connexion racine SSH et d'une paire de clés publique-privée. Par défaut, cette valeur est `false`. L'interface utilisateur d'administration d'Unified Access Gateway dispose d'un champ **Clés publiques SSH**, où un administrateur peut télécharger des clés publiques pour autoriser l'accès d'un utilisateur racine à Unified Access Gateway lors de l'utilisation de l'option de paire de clés publique-privée. Pour que ce champ soit disponible dans l'interface utilisateur d'administration, la valeur de cette option et **Activer SSH** doivent être `true` au moment du déploiement. Si l'une de ces options n'est pas `true`, le champ **Clés publiques SSH** n'est pas disponible dans l'interface utilisateur d'administration. Le champ **Clés publiques SSH** est un paramètre système avancé dans l'interface utilisateur d'administration. Reportez-vous à la section Configurer les paramètres système d'Unified Access Gateway.
Adhérer au CEIP	Sélectionnez **Participer au programme d'amélioration du produit VMware** pour adhérer au CEIP ou désélectionnez l'option pour quitter le CEIP.

Important Vous ne pouvez configurer les options SSH que lors du déploiement. Pour des raisons liées à la sécurité, vous ne pouvez pas modifier ces options après le déploiement via l'interface utilisateur d'administration ou l'API d'Unified Access Gateway.

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 la 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.

Résultats

Le dispositif Unified Access Gateway est déployé et démarre automatiquement.

Étape suivante

- 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://<mycoUnified Access Gatewayappliance.com:9443/admin/index.html`.

  Important Vous devez terminer la configuration d'Unified Access Gateway après le déploiement à l'aide de l'interface utilisateur d'administration. Si vous ne fournissez pas le mot de passe de l'interface utilisateur d'administration, vous ne pouvez pas ajouter ultérieurement un utilisateur de l'interface utilisateur d'administration pour permettre l'accès à celle-ci ou à l'API. Vous devez redéployer votre instance Unified Access Gateway avec un mot de passe de l'interface utilisateur d'administration valide si vous souhaitez ajouter un utilisateur de l'interface utilisateur d'administration.

  Note 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.

Note Lorsque vous lancez la console d'administration d'Unified Access Gateway pour la première fois, vous êtes invité à modifier le mot de passe que vous avez défini lorsque vous avez déployé le dispositif.

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

- Configuration système d'Unified Access Gateway et certificat de serveur TLS
- Paramètres du service Edge pour Horizon, proxy inversé et VMware Tunnel et Content Gateway (appelé également CG)
- 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

- Paramètres réseau
- Paramètres du fournisseur de vérification de la conformité du point de terminaison
- Configuration des paramètres de pontage d'identité
- Paramètres du compte

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

- Téléchargez les fichiers journaux d'Unified Access Gateway.
- Exportez les paramètres d' Unified Access Gateway pour extraire les paramètres de configuration.
- Définissez les paramètres de niveau de journal.
- Importez 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.

Conditions préalables

- 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
  - Adresses IP des serveurs DNS

    Note Vous pouvez spécifier un maximum de deux adresses IP de serveur DNS.

    Si aucune adresse IP de serveur DNS n'est spécifiée, Unified Access Gateway utilise les adresses DNS publiques de secours par défaut de la plate-forme.
  - 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 système**.

3 Modifiez les valeurs suivantes de configuration du dispositif Unified Access Gateway.

Option	Valeur par défaut et description
Nom UAG	Nom unique du dispositif UAG.
Paramètre régional	Spécifie le paramètre régional à utiliser pour générer les messages d'erreur. ■ **en_US** pour l'anglais américain. Il s'agit du réglage par défaut. ■ **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 ■ **es** pour l'espagnol ■ **pt_BR** pour le portugais du Brésil ■ **en_BR** pour l'anglais britannique
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.
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 `NO`. Sélectionnez **YES** pour activer le protocole de sécurité TLS 1.1.
TLS 1.2 activé	La valeur par défaut est `YES`. Le protocole de sécurité TLS 1.2 est activé.
TLS 1.3 activé	La valeur par défaut est `YES` Le protocole de sécurité TLS 1.3 est activé.
Type Syslog	Sélectionnez le type Syslog dans la liste déroulante. Les options sont les suivantes : ■ UDP : les messages Syslog sont envoyés sur le réseau en texte brut sur UDP. Il s'agit de l'option par défaut. ■ TLS : le chiffrement TLS est ajouté entre deux serveurs Syslog pour que les messages restent sécurisés. **Note** Cela s'applique à Unified Access Gateway 3.7 et versions ultérieures.

Option	Valeur par défaut et description
URL Syslog	Lorsque le type Syslog est défini sur UDP, cette option est activée. 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. Un nombre maximum de deux URL peut être fourni. Les URL sont séparées par une virgule. Exemple : `syslog://server1.example.com:514, syslog://server2.example.com:514` Par défaut, les événements des services Edge de Content Gateway et Secure Email Gateway sont journalisés. Pour consigner les événements sur le serveur Syslog pour le service Edge Tunnel Gateway configuré sur Unified Access Gateway, un administrateur doit configurer Syslog sur Workspace ONE UEM Console avec les informations.`Syslog Hostname=localhost and Port=514` Pour plus d'informations sur Syslog dans Workspace ONE UEM, reportez-vous à la section *Configurer VMware Tunnel* de la documentation *VMware Workspace ONE UEM Console* sur VMware Docs.
Serveurs Syslog	Lorsque le type Syslog est défini sur TLS, cette option est activée. 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. Un nombre maximum de deux URL peut être fourni. Les URL sont séparées par une virgule. Exemple : `syslog://server1.example.com:514, syslog://server2.example.com:514` Par défaut, les événements des services Edge de Content Gateway et Secure Email Gateway sont journalisés. Pour consigner les événements sur le serveur Syslog pour le service Edge Tunnel Gateway configuré sur Unified Access Gateway, un administrateur doit configurer Syslog sur Workspace ONE UEM Console avec les informations.`Syslog Hostname=localhost and Port=514` **Note** Cela s'applique à Unified Access Gateway 3.7 et versions ultérieures.
URL d'audit de Syslog	Entrez l'URL du serveur Syslog qui est utilisée pour la journalisation des événements d'audit d'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 d'audit n'est journalisé. Un nombre maximum de deux URL peut être fourni. Les URL sont séparées par une virgule. Exemple : `syslog://server1.example.com:514, syslog://server2.example.com:514`
Certificat d'autorité de certification	Cette option est activée lorsqu'un serveur Syslog est ajouté. Sélectionnez un certificat d'autorité de certification Syslog valide.
Certificat client Syslog	**Note** Cette option est activée uniquement en cas d'ajout d'un serveur Syslog dans l'interface utilisateur d'administration d'Unified Access Gateway. Sélectionnez un certificat client Syslog valide au format PEM.

Option	Valeur par défaut et description
Clé du certificat client Syslog	**Note** Cette option est activée uniquement en cas d'ajout d'un serveur Syslog dans l'interface utilisateur d'administration d'Unified Access Gateway. Sélectionnez une clé de certificat client Syslog valide au format PEM. **Note** Lorsque le dispositif Unified Access Gateway est déployé à l'aide de PowerShell, si un certificat ou une clé non valide ou expiré(e) est fourni(e), l'instance de l'interface utilisateur d'administration ne sera pas disponible.
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.
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**.
Âge du mot de passe	Nombre de jours de validité du mot de passe de l'administrateur actuel. La valeur par défaut est de 90 jours. Spécifiez zéro (0) si le mot de passe n'expire jamais.
Délai d'expiration de la demande	Indique le temps maximal qu'Unified Access Gateway attend pour recevoir une demande. La valeur par défaut est `3000`. Ce délai d'expiration doit être spécifié en millisecondes.
Délai d'expiration de réception du corps	Indique le temps maximal qu'Unified Access Gateway attend pour recevoir un corps de demande. L'option par défaut est `5000`. Ce délai d'expiration doit être spécifié en millisecondes.
Nombre maximal de connexions par session	Nombre maximal de connexions TCP autorisées par session TLS. La valeur par défaut est `16`. Pour n'appliquer aucune limite au nombre de connexions TCP autorisées, définissez la valeur de ce champ sur `0`. **Note** Une valeur du champ inférieure ou égale à `8` provoque des erreurs dans Horizon Client.
Délai d'expiration d'inactivité de connexion du client	Spécifiez la durée (en secondes) pendant laquelle une connexion client peut rester inactive avant la fermeture de la connexion. La valeur par défaut est de 360 secondes (6 minutes). Une valeur de 0 indique qu'il n'y a aucun délai d'inactivité.
Délai d'expiration d'authentification	Durée d'attente maximale, en millisecondes, avant laquelle l'authentification doit avoir lieu. La valeur par défaut est 300 000. Si 0 est spécifié, cela indique aucune limite de temps pour l'authentification.
Tolérance de variation d'horloge	Entrez la différence de temps autorisée en secondes entre une horloge d'Unified Access Gateway et les autres horloges sur le même réseau. La valeur par défaut est de 600 secondes.

Option	Valeur par défaut et description
Nombre maximal de CPU système autorisé	Indique l'utilisation moyenne maximale autorisée du CPU système en une minute. Lorsque la limite de CPU configurée est dépassée, les nouvelles sessions ne sont pas autorisées et le client reçoit une erreur HTTP 503 indiquant que le dispositif Unified Access Gateway est temporairement surchargé. En outre, la limite dépassée permet également à un équilibrage de charge de marquer le dispositif Unified Access Gateway comme étant inactif afin que les nouvelles demandes puissent être dirigées vers d'autres dispositifs Unified Access Gateway. La valeur est exprimée en pourcentage. La valeur par défaut est `100%`.
Adhérer au CEIP	Si l'option est activée, envoie des informations à VMware dans le cadre du Programme d'amélioration du produit (CEIP). Reportez-vous à la section Participer au programme d'amélioration du produit ou le quitter pour plus d'informations.
Activer SNMP	Basculez sur **OUI** pour activer le service SNMP. Le protocole de gestion de réseau simple (SNMP) collecte les statistiques système, de la mémoire et les informations MIB du service Edge Tunnel par Unified Access Gateway. **Note** Vous devez activer SNMP avant de configurer Tunnel. Si vous activez SNMP après la configuration de Tunnel, vous devez enregistrer à nouveau les paramètres de Tunnel afin que les paramètres SNMP prennent effet. Liste de la base d'informations de gestion (MIB, Management Information Base) disponible, ■ UCD-SNMP-MIB::systemStats ■ UCD-SNMP-MIB::memory ■ VMWARE-TUNNEL-SERVER-MIB::vmwTunnelServerMIB
Texte de clause de non-responsabilité de l'administrateur	Entrez le texte de clause de non-responsabilité en fonction de la politique de contrat d'utilisateur de votre entreprise. Pour qu'un administrateur se connecte à l'interface utilisateur d'administration Unified Access Gateway, l'administrateur doit accepter la politique de contrat. Le texte de clause de non-responsabilité peut être configuré via un déploiement PowerShell ou à l'aide de l'interface utilisateur d'administration Unified Access Gateway. Pour plus d'informations sur le paramètre PowerShell dans le fichier `INI`, reportez-vous à Utilisation de PowerShell pour déployer le dispositif Unified Access Gateway. Lors de l'utilisation de l'interface utilisateur d'administration Unified Access Gateway pour configurer cette zone de texte, l'administrateur doit d'abord se connecter à l'interface utilisateur d'administration, puis configurer le texte de clause de non-responsabilité. Lors des connexions suivantes de l'administrateur, le texte s'affiche pour permettre à l'administrateur d'accepter avant d'accéder à la page de connexion.
DNS	Entrez les adresses du système de noms de domaine qui sont ajoutées au fichier de configuration `/run/systemd/resolve/resolv.conf`. Il doit contenir une adresse de recherche DNS valide. Cliquez sur « + » pour ajouter une adresse DNS.

Option	Valeur par défaut et description
Recherche DNS	Entrez la recherche du système de noms de domaine qui est ajoutée au fichier de configuration `/etc/resolv.conf`. Il doit contenir une adresse de recherche DNS valide. Cliquez sur « + » pour ajouter une entrée de recherche DNS.
Serveurs NTP	Serveurs NTP pour la synchronisation du protocole de temps du réseau. Vous pouvez entrer des adresses IP et des noms d'hôte valides. Les serveurs NTP par interface obtenus depuis la configuration de `systemd-networkd.service` ou via DHCP auront priorité sur ces configurations. Cliquez sur « + » pour ajouter un serveur NTP.
Serveurs NTP de secours	Serveurs NTP de secours pour la synchronisation du protocole de temps du réseau. Si les informations de serveur NTP sont introuvables, ces noms d'hôte de serveur NTP de secours ou adresses IP seront utilisés. Cliquez sur « + » pour ajouter un serveur NTP de secours.
Clés publiques SSH	Chargez des clés publiques pour activer l'accès de l'utilisateur racine à Unified Access Gateway lors de l'utilisation de l'option de paire de clés publique/privée. Les administrateurs peuvent charger plusieurs clés publiques uniques sur Unified Access Gateway. Ce champ est visible sur l'interface utilisateur d'administration uniquement lorsque les options SSH suivantes sont définies sur `true` pendant le déploiement : **Activer SSH** et **Autoriser la connexion racine SSH à l'aide de la paire de clés**. Pour plus d'informations sur ces options, reportez-vous à la section Déploiement d'Unified Access Gateway au moyen de l'assistant de modèle OVF.

4 Cliquez sur **Enregistrer**.

Étape suivante

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.

Modifier les paramètres réseau

Vous pouvez modifier les paramètres réseau, tels que l'adresse IP, le masque de sous-réseau, la passerelle par défaut et le mode d'allocation d'adresses IP pour les réseaux configurés à partir de l'interface utilisateur d'administration.

Notez les limitations suivantes lorsque vous modifiez les paramètres réseau :

- IPv4 est le seul mode d’adresse IP pris en charge. IPv6 n’est pas pris en charge.
- Lorsque l'adresse IP est modifiée dynamiquement sur une adresse IP de réseau de gestion, la redirection du navigateur n'est pas prise en charge vers la nouvelle adresse IP.
- Lorsque l'adresse IP, le masque de sous-réseau ou la passerelle par défaut est modifié pour une interface réseau orientée internet, toutes les sessions en cours sont perdues.

Conditions préalables

- Vérifiez que vous êtes connecté en tant qu'administrateur avec un rôle ROLE_ADMIN.
- Si vous remplacez l'adresse IP par une adresse IP statique, un masque de sous-réseau ou une passerelle par défaut, vous devez connaître au préalable ces éléments.

Procédure

1. Dans la section Configuration manuelle de l'interface utilisateur d'administration, cliquez sur **Sélectionner**.
2. Sous **Paramètres avancés**, cliquez sur l'icône d'engrenage en regard de **Paramètres réseau**.

   Une liste de réseaux configurés et de leurs paramètres s'affiche.
3. Dans la fenêtre Paramètres réseau, cliquez sur l'icône d'engrenage en regard du réseau dont vous souhaitez modifier les paramètres et entrez les informations suivantes :

   La configuration IPv4

Étiquette	Description
Mode d'allocation IPv4	Indiquez si l'adresse IP doit être allouée de manière statique ou dynamique. Vous devez spécifier ce paramètre pour l'allocation d'adresses IP statiques.
Adresse IPv4	Adresse IP du réseau. Vous n'avez pas besoin de spécifier l'adresse IP si vous sélectionnez l'allocation d'adresses IP dynamiques. Vous devez spécifier ce paramètre pour l'allocation d'adresses IP statiques.
Masque de réseau IPv4	Masque de réseau IPv4 du réseau. Il n'est pas nécessaire de spécifier le masque de réseau IPv4 si vous sélectionnez l'allocation d'adresses IP dynamiques.
Passerelle IPv4 par défaut	Adresse de passerelle IPv4 par défaut d'Unified Access Gateway. Il n'est pas nécessaire de spécifier l'adresse IP de passerelle par défaut si vous sélectionnez l'allocation d'adresses IP dynamiques.
Routes statiques IPv4	Routes IPv4 personnalisées pour le réseau. Cliquez sur « + » pour ajouter une route statique. Liste de routes personnalisées IPv4 de carte réseau séparées par des virgules, au format adresse-réseau-ipv4/bits adresse-passerelle-ipv4. Par exemple, 20.2.0.0/16 10.2.0.1,20.9.0.0/16 10.2.0.2,10.2.0.1/32. **Note** Si la valeur adresse-passerelle-ipv4 n'est pas spécifiée, la route respective qui est ajoutée dispose d'une passerelle de 0.0.0.0

   Les configurations IPv6 ne peuvent pas être modifiées.

Étiquette	Description
Mode d'allocation IPv6	Spécifie si l'adresse IP est allouée statiquement, dynamiquement ou automatiquement.
Adresse IPv6	Adresse IP du réseau.
Préfixe IPv6	Le préfixe IPv6 du réseau.
Passerelle IPv6 par défaut	Adresse de passerelle IPv6 par défaut d'Unified Access Gateway.

4 Cliquez sur **Enregistrer**.

Si les paramètres sont modifiés avec succès, un message de réussite s'affiche. Un message d'erreur s'affiche si les paramètres réseau ne peuvent pas être mis à jour.

Configuration des paramètres de compte utilisateur

En tant que super administrateur disposant d'un accès complet au système Unified Access Gateway, vous pouvez ajouter et supprimer des utilisateurs, modifier les mots de passe et les rôles des utilisateurs depuis les pages de configuration d'administration.

Les paramètres de compte, y compris les détails de l'administrateur avec privilèges limités, ne peuvent pas être exportés à partir des paramètres du dispositif ni importés vers ceux-ci. Pour configurer un nouveau compte avec privilèges limités sur une nouvelle instance de Unified Access Gateway, procédez à l'opération via l'interface utilisateur d'administration.

Expiration du mot de passe

Le super utilisateur et les administrateurs disposant de faibles privilèges peuvent afficher la période restante pour l'expiration du mot de passe. Sur la page **Paramètres du compte**, le champ **Le mot de passe expire dans (Jours)** fournit le compte à rebours en nombre de jours jusqu'à la date d'expiration du mot de passe. Ce champ aide les utilisateurs à rester informés de la date d'expiration du mot de passe et à prendre les mesures appropriées, telles que la réinitialisation de leur mot de passe.

Note La période d'expiration du mot de passe est arrondie au nombre entier inférieur immédiat.

Par exemple, si le nombre de jours restants pour l'expiration du mot de passe est de 1 jour 23 heures, la valeur indique 1 jour.

Ajouter un administrateur avec privilèges limités

Vous pouvez désormais configurer et ajouter un administrateur avec privilèges limités pouvant effectuer un nombre limité de tâches, telles que des opérations en lecture seule, la surveillance du système, etc.

Note Actuellement, vous ne pouvez ajouter qu'un seul administrateur avec privilèges limités à une instance de Unified Access Gateway.

Procédure

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

2 Sous Paramètres avancés, sélectionnez l'icône d'engrenage Paramètres du compte.

3 Dans la fenêtre Paramètres du compte, cliquez sur **Ajouter**.

Le rôle est automatiquement défini sur ROLE_MONITORING.

4 Dans la fenêtre Paramètres du compte, saisissez les informations suivantes :

   a Un nom d'utilisateur unique pour l'utilisateur.

   b (Facultatif) Cochez la case **Activé** si vous souhaitez activer l'utilisateur immédiatement après l'avoir ajouté.

   c Entrez un mot de passe pour l'utilisateur. 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 ! @ # $ % * ( ).

   d Confirmez le mot de passe.

5 Cliquez sur **Enregistrer**.

Résultats

L'administrateur que vous venez d'ajouter est répertorié sous Paramètres du compte.

Étape suivante

L'administrateur avec privilèges limités peut se connecter au système pour modifier son mot de passe ou effectuer des tâches de surveillance.

Modification des paramètres de compte d'utilisateur

En tant que super administrateur, vous pouvez modifier le mot de passe d'un utilisateur et activer ou désactiver un utilisateur.

Vous pouvez également modifier votre propre mot de passe, mais vous ne pouvez pas désactiver votre propre compte.

Procédure

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

2 Dans la section Paramètres avancés, cliquez sur Paramètres du compte.

   Une liste d'utilisateurs s'affiche.

3 Cliquez sur l'icône en forme d'engrenage en regard de l'utilisateur dont vous souhaitez modifier le compte.

4 Modifiez les valeurs suivantes.

   a Cochez ou décochez la case **Activer** selon que vous voulez activer ou désactiver l'utilisateur.

   b Pour réinitialiser le mot de passe utilisateur, entrez un nouveau mot de passe et confirmez-le. Si vous êtes connecté en tant qu'administrateur, vous devez également entrer votre ancien mot de passe.

      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 ! @ # $ % * ( ).

5 Cliquez sur **Enregistrer**.

Réinitialiser le mot de passe de l'administrateur à l'aide de la console Unified Access Gateway

En cas d'oubli du mot de passe de l'utilisateur Admin, l'utilisateur peut se connecter à la console Unified Access Gateway à l'aide des informations d'identification de l'utilisateur racine et réinitialiser le mot de passe de l'interface utilisateur d'administration.

Conditions préalables

Vous devez posséder le mot de passe pour vous connecter à la machine virtuelle en tant qu'utilisateur racine ou utilisateur disposant de privilèges racine. L'utilisateur doit faire partie du groupe *root*.

Pour plus d'informations sur le mot de passe racine, reportez-vous à la section Dépannage des problèmes de connexion racine.

Procédure

1 Connectez-vous au système d'exploitation de la console Unified Access Gateway en tant qu'utilisateur racine.

2 Entrez les commandes suivantes pour réinitialiser le mot de passe de l'administrateur.

```
adminpwd

New password for user "admin": ********

Retype new password: ********
```

Dans cet exemple, le mot de passe est composé d'au moins 8 caractères, contient au moins une majuscule et une minuscule, un chiffre et un caractère spécial, à savoir ! @ # $ % * ( ).

Le message suivant s'affiche.

```
adminpwd: password for "admin" updated successfully
```

3 Entrez les commandes suivantes pour réinitialiser le mot de passe d'un administrateur avec moins de privilèges.

```
adminpwd [-u <username>]

New password for user "jdoe": ********

Retype new password: ********
```

Le mot de passe de l'administrateur doit contenir au moins 8 caractères, au moins une majuscule et une minuscule, un chiffre et un caractère spécial, qui inclut ! @ # $ % * ( ).

Le message suivant s'affiche.

```
adminpwd: password for "jdoe" updated successfully
```

Résultats

Le mot de passe de l'utilisateur Admin est correctement réinitialisé.

Étape suivante

L'utilisateur peut désormais se connecter à l'interface d'Unified Access Gateway en utilisant le mot de passe de l'administrateur qui vient d'être défini. Il sera demandé à l'utilisateur de modifier le mot de passe lors de la première connexion après la réinitialisation du mot de passe en utilisant la commande `adminpwd` de la CLI.

Note Après avoir modifié le mot de passe, l'utilisateur doit se connecter lors de la première tentative.

Supprimer un utilisateur

En tant qu'utilisateur Super administrateur, vous pouvez supprimer un utilisateur non-racine.

Vous ne pouvez pas supprimer un administrateur racine.

Procédure

1. Dans la section Configuration manuelle de l'interface utilisateur d'administration, cliquez sur **Sélectionner**.
2. Sous Paramètres avancés, sélectionnez l’icône d’engrenage Paramètres du compte.

   Une liste d’utilisateurs s’affiche.
3. Cliquez sur le bouton « x » en regard de l’utilisateur que vous souhaitez supprimer.

   Attention L’utilisateur est immédiatement supprimé. Cette action ne peut pas être annulée.

Résultats

Le compte d’utilisateur est supprimé et un message s’affiche.

Configurer les paramètres de jeton Web JSON

UAG (Unified Access Gateway) prend en charge la validation du jeton Web JSON (JWT). Vous pouvez configurer les paramètres de jeton Web JSON pour valider un artefact SAML émis par Workspace ONE Access pendant l'opération Single Sign-On à Horizon et pour prendre en charge la fonctionnalité de redirection du protocole Horizon lorsqu'UAG est utilisé avec le broker universel Horizon.

Workspace ONE Access génère un artefact Horizon SAML encapsulé dans JWT lorsque la case **Encapsuler l'artefact dans JWT** est activée dans la configuration de Workspace ONE Access Horizon. Cela permet à UAG de bloquer les tentatives d'authentification, sauf si un jeton JWT approuvé est fourni avec la tentative d'authentification de l'artefact SAML.

Dans les deux cas d'utilisation, vous devez spécifier les paramètres de JWT pour permettre à UAG de faire confiance à l'émetteur des jetons JWT reçus.

Utilisez une URL de clé publique dynamique pour les paramètres JWT afin qu'UAG conserve automatiquement les dernières clés publiques pour cette approbation. Vous ne devez utiliser des clés publiques statiques que si UAG ne peut pas accéder à l'URL de la clé publique dynamique.

La procédure suivante décrit la configuration des paramètres de jeton Web JSON :

Procédure

1. Dans la section Configuration manuelle de l'interface utilisateur d'administration, cliquez sur **Sélectionner**.
2. Sous Paramètres avancés, sélectionnez l'icône en forme d'engrenage Paramètres JWT.
3. Dans la fenêtre Paramètres JWT, cliquez sur **Ajouter**.
4. Dans la fenêtre Paramètres du compte, saisissez les informations suivantes :

Option	Par défaut et description
Nom	Nom permettant d'identifier ce paramètre pour la validation.
Émetteur	Valeurs de l'émetteur de JWT spécifiées dans la réclamation émetteur du jeton entrant à valider. Par défaut, la valeur de ce champ est définie sur le champ **Nom**. **Note** L'option **Émetteur** n'est configurée que pour le cas d'utilisation de redirection du protocole de broker universel.
URL de clé publique dynamique	Entrez l'URL d'extraction dynamique de la clé publique.
Empreintes numériques d'URL de clé publique	Entrez la liste des empreintes numériques d'URL de clé publique. Si vous ne fournissez pas de liste d'empreintes numériques, assurez-vous que les certificats de serveur sont 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.
Certificats approuvés	Cliquez sur le signe « + » pour sélectionner un certificat au format PEM et l'ajouter au magasin des approbations. Cliquez sur le signe «- » pour supprimer un certificat du magasin d'approbations. Par défaut, le nom d'alias est le nom de fichier du certificat PEM. Pour fournir un nom différent, modifiez la zone de texte de l'alias.
Intervalle d'actualisation de clé publique	Intervalle de temps en secondes d'extraction périodique de clé publique de l'URL.
Clés publiques statiques	**Note** Si aucune URL de clé publique dynamique n'est disponible, définissez une clé publique statique. Cliquez sur **+** pour sélectionner et ajouter une clé publique à utiliser pour la validation de JWT. Le fichier doit être au format `PEM`.

5. Cliquez sur **Enregistrer**.

Résultats

Les détails des paramètres sont répertoriés sous Paramètres JWT.

Mise à jour des certificats signés du serveur SSL

Vous pouvez remplacer vos certificats signés lorsqu'ils expirent ou remplacer les certificats par défaut par des certificats signés par une autorité de certification.

Par défaut, Unified Access Gateway utilise un certificat de serveur TLS/SSL auto-signé. Pour les environnements de production, VMware vous recommande vivement de remplacer le certificat auto-signé par défaut par un certificat signé par une autorité de certification de confiance pour votre environnement.

Notez les points suivants lorsque vous importez un certificat :

- Vous pouvez remplacer le certificat par défaut par un certificat au format PEM pour l'administrateur et l'utilisateur.
- Lorsque vous importez un certificat signé par une autorité de certification sur l'interface d'administration, le connecteur SSL sur l'interface d'administration est mis à jour et redémarré pour que le certificat téléchargé prenne effet. Si le connecteur ne parvient pas à redémarrer avec le certificat signé par une autorité de certification importé, un certificat auto-signé est généré et appliqué sur l'interface d'administration, et l'utilisateur est informé que la tentative précédente d'importation d'un certificat a échoué.

  Note Avec le déploiement PowerShell de Unified Access Gateway, le certificat de serveur SSL peut être spécifié. Il n'est pas nécessaire de le remplacer manuellement.

Conditions préalables

- Nouveau certificat signé et nouvelle clé privée enregistrés sur un ordinateur auquel vous avez accès.
- Convertissez le certificat en fichiers au format PEM et le fichier `.pem` dans un format sur une seule ligne. Reportez-vous à la section Convertir des fichiers de certificat au format PEM sur une ligne.

Procédure

1. Dans la section **Configurer manuellement** de l'interface utilisateur d'administration Unified Access Gateway, cliquez sur **Sélectionner**.
2. Dans la section **Paramètres avancés**, cliquez sur l'icône en forme d'engrenage **Paramètres du certificat de serveur TLS**.
3. Sélectionnez **Interface d'administration** ou **Interface Internet** pour appliquer le certificat à l'une des deux interfaces. Vous pouvez également sélectionner les deux options pour appliquer le certificat aux deux interfaces.
4. Sélectionnez un **type de certificat** de `PEM` ou de `PFX`.

5 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.

6 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 un alias pour le certificat PFX.

   Vous pouvez utiliser l'alias pour les différencier lorsque plusieurs certificats sont présents.

7 Cliquez sur **Enregistrer**.

Résultats

Un message de confirmation s'affiche lorsque le certificat est mis à jour avec succès.

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.

Lisez les sections suivantes :

- Configuration système requise pour déployer Unified Access Gateway à l'aide de PowerShell
- Utilisation de PowerShell pour déployer le dispositif Unified Access Gateway

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.

- Le script PowerShell s'exécute sur des machines Windows 8.1 ou version ultérieure ou sur Windows Server 2008 R2 ou version ultérieure.
- Hôte VMware vSphere ESXi avec un vCenter Server.
- 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/.
- Microsoft Hyper-V

  Note Pour plus d'informations, consultez la documentation de VMware Workspace ONE UEM.

- Microsoft Azure

  Note Pour plus d'informations, consultez la section Déploiement PowerShell du dispositif Unified Access Gateway sur Microsoft Azure .

- Amazon AWS EC2

  Note Pour plus d'informations, consultez la section Déploiement PowerShell du dispositif Unified Access Gateway sur Amazon Web Services .

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

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.

Important Avec un déploiement PowerShell, vous pouvez fournir tous les paramètres dans le fichier INI, et l'instance d'Unified Access Gateway sera prête pour la production dès qu'elle sera démarrée. Si vous ne souhaitez pas modifier les paramètres après le déploiement, vous ne devez pas fournir le mot de passe de l'interface utilisateur d'administration.

Cependant, l'interface utilisateur d'administration et l'API ne sont pas disponibles si le mot de passe de l'interface utilisateur d'administration n'est pas fourni lors du déploiement.

Note

- Si vous ne fournissez pas le mot de passe de l'interface utilisateur d'administration au moment du déploiement, vous ne pouvez pas ajouter ultérieurement un utilisateur pour permettre l'accès à l'interface utilisateur d'administration ou à l'API. Vous devez redéployer votre instance Unified Access Gateway avec un mot de passe valide si vous souhaitez ajouter un utilisateur de l'interface utilisateur d'administration.
- Unified Access Gateway 3.5 et versions ultérieures inclut une propriété INI `sshEnabled` facultative. Le paramètre `sshEnabled=true` dans la section `[General]` du fichier INI de PowerShell active automatiquement l'accès de `ssh` sur le dispositif déployé. VMware ne recommande généralement pas l'activation de `ssh` sur Unified Access Gateway, sauf dans certaines situations spécifiques et lorsque l'accès peut être limité. Cette capacité est principalement destinée aux déploiements d'Amazon AWS EC2 où l'accès à une console de remplacement n'est pas disponible.

  Note Pour plus d'informations sur Amazon AWS EC2, reportez-vous à la section Déploiement PowerShell du dispositif Unified Access Gateway sur Amazon Web Services.

  Si `sshEnabled=true` n'est pas spécifiée ou est défini sur `false`, `ssh` n'est pas activé.

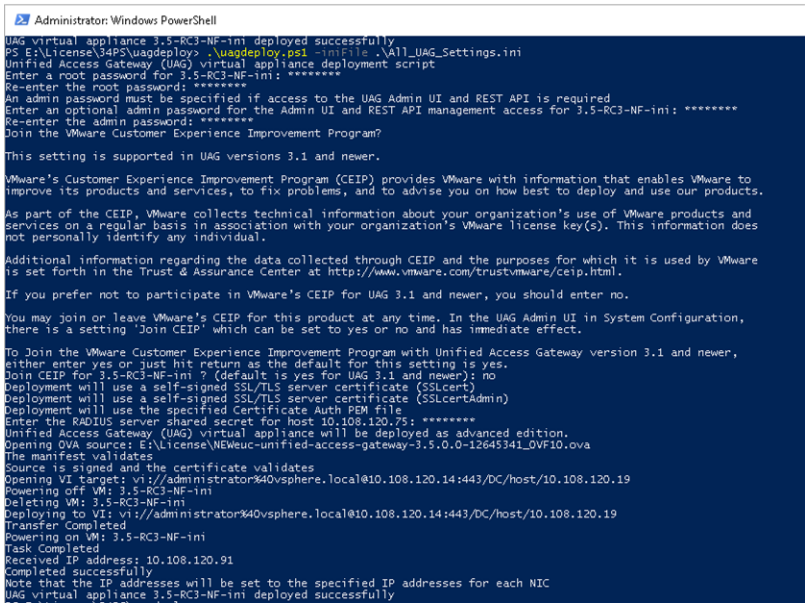
  L'activation de l'accès de `ssh` sur les déploiements d'Unified Access Gateway pour vSphere, de Hyper-V ou de Microsoft Azure n'est généralement pas requise, car l'accès à la console avec ces plates-formes peut être utilisé. Si l'accès à la console racine est requis pour le déploiement d'Amazon AWS EC2, définissez `sshEnabled=true`. Dans les cas où `ssh` est activé, l'accès 22 du port TCP doit être restreint dans les pare-feu ou les groupes de sécurité aux adresses IP sources des administrateurs individuels. EC2 prend en charge cette restriction dans le groupe de sécurité EC2 associée aux interfaces réseau d'Unified Access Gateway.

Conditions préalables

- Pour un déploiement Hyper-V, si vous mettez à niveau Unified Access Gateway avec une adresse IP statique, supprimez le dispositif antérieur avant de déployer l'instance d'Unified Access Gateway plus récente.
- 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



Procédure

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

   Les fichiers `ZIP` sont disponibles sur la page de téléchargement VMware pour Unified Access Gateway.
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 d'Unified Access Gateway.

Par exemple : déployez un nouveau dispositif Unified Access Gateway *UAG1*. Le fichier de configuration s'appelle *uag1.ini*. Ce fichier contient tous les paramètres de configuration pour UAG1. Vous pouvez utiliser les exemples de fichiers `.INI` dans le fichier `uagdeploy.ZIP` pour créer le fichier `INI` et modifier les paramètres en conséquence.

Note

- 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.

```
[General]
netManagementNetwork=
netInternet=
netBackendNetwork=
name=
dns = 192.0.2.1 192.0.2.2
dnsSearch = example1.com example2.com
ip0=10.108.120.119
diskMode=
source=
defaultGateway=10.108.120.125
target=
ds=
deploymentOption=onenic
authenticationTimeout=300000
fipsEnabled=false
uagName=UAG1
locale=en_US
ipModeforNIC3=DHCPV4_DHCPV6
tls12Enabled=true
ipMode=DHCPV4_DHCPV6
requestTimeoutMsec=10000
ipModeforNIC2=DHCPV4_DHCPV6
tls11Enabled=false
clientConnectionIdleTimeout=180
tls10Enabled=false
adminCertRolledBack=false
cookiesToBeCached=none
healthCheckUrl=/favicon.ico
quiesceMode=false
syslogUrl=10.108.120.108:514
isCiphersSetByUser=false
tlsPortSharingEnabled=true
ceipEnabled=true
bodyReceiveTimeoutMsec=15000
monitorInterval=60
```

```
cipherSuites=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TL
S_ECDHE_RSA_WITH_AES_128_CBC_SHA256
, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
adminPasswordExpirationDays=90
httpConnectionTimeout=120
isTLS11SetByUser=false
sessionTimeout=36000000
ssl30Enabled=false
snmpEnabled= TRUE | FALSE
ntpServers=ipOrHostname1 ipOrHostname2
fallBackNtpServers=ipOrHostname1 ipOrHostname2
sshEnabled=
sshPasswordAccessEnabled=
sshKeyAccessEnabled=
sshPublicKey1=
adminDisclaimerText=

[WebReverseProxy1]
proxyDestinationUrl=https://10.108.120.21
trustedCert1=
instanceId=view
healthCheckUrl=/favicon.ico
userNameHeader=AccessPoint-User-ID
proxyPattern=/(.*)
landingPagePath=/
hostEntry1=10.108.120.21 HZNView.uagqe.auto.com

[Horizon]
proxyDestinationUrl=https://enterViewConnectionServerUrl
trustedCert1=
gatewayLocation=external
disableHtmlAccess=false
healthCheckUrl=/favicon.ico
proxyDestinationIPSupport=IPV4
smartCardHintPrompt=false
queryBrokerInterval=300
proxyPattern=(/|/view-client(.*)|/portal(.*)|/appblast(.*))
matchWindowsUserName=false
windowsSSOEnabled=false

[Airwatch]
tunnelGatewayEnabled=true
tunnelProxyEnabled=true
pacFilePath=
pacFileURL=
credentialFilePath=
apiServerUsername=domain\apiusername
apiServerPassword=*****
proxyDestinationUrl=https://null
ntlmAuthentication=false
healthCheckUrl=/favicon.ico
organizationGroupCode=
apiServerUrl=https://null
airwatchOutboundProxy=false
outboundProxyHost=1.2.3.4
```

```
outboundProxyPort=3128
outboundProxyUsername=proxyuser
outboundProxyPassword=****
reinitializeGatewayProcess=false
airwatchServerHostname=tunnel.acme.com
trustedCert1=c:\temp\CA-Cert-A.pem
hostEntry1=1.3.5.7 backend.acme.com

[AirwatchSecureEmailGateway]
airwatchOutboundProxy=false
memConfigurationId=abc123
apiServerUsername=domain\apiusername
healthCheckUrl=/favicon.ico
apiServerUrl=https://null
outboundProxyHost=1.2.3.4
outboundProxyPort=3128
outboundProxyUsername=proxyuser
outboundProxyPassword=****
reinitializeGatewayProcess=false
airwatchServerHostname=serverNameForSNI
apiServerPassword=****
trustedCert1=c:\temp\CA-Cert-A.pem
pfxCerts=C:\Users\admin\My Certs\mycacerts.pfx
hostEntry1=1.3.5.7 exchange.acme.com

[AirWatchContentGateway]
cgConfigId=abc123
apiServerUrl=https://null
apiServerUsername=domain\apiusername
apiServerPassword=*****
outboundProxyHost=
outboundProxyPort=
outboundProxyUsername=proxyuser
outboundProxyPassword=*****
airwatchOutboundProxy=false
hostEntry1=192.168.1.1 cgbackend.acme.com
trustedCert1=c:\temp\CA-Cert-A.pem
ntlmAuthentication=false
reinitializeGatewayProcess=false
airwatchServerHostname=cg.acme.com

[SSLCert]
pemPrivKey=
pemCerts=
pfxCerts=
pfxCertAlias=

[SSLCertAdmin]
pemPrivKey=
pemCerts=
pfxCerts=
pfxCertAlias=

[JWTSettings1]
publicKey1=
```

```
publicKey2=
publicKey3=
name=JWT_1

[JWTSettings2]
publicKey1=
publicKey2=
name=JWT_2
```

5 Pour vérifier que l'exécution du script n'est pas restreinte, saisissez la commande PowerShell `set-executionpolicy`.

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

Vous n'avez besoin d'effectuer cette opération qu'une seule fois pour supprimer la restriction.

a (Facultatif) S'il existe un avertissement pour le script, exécutez la commande suivante pour débloquer l'avertissement : `unblock-file -path .\uagdeploy.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`.

```
.\uagdeploy.ps1 -iniFile uag1.ini
```

7 Entrez les informations d'identification lorsque vous y êtes invité et terminez le script.

Note 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.

Résultats

Pour plus d'informations sur les scripts PowerShell, consultez https://communities.vmware.com/docs/DOC-30835.

Étape suivante

Si vous souhaitez mettre à niveau Unified Access Gateway tout en conservant les paramètres existants, modifiez le fichier `.ini` pour utiliser la nouvelle version de la référence source, puis réexécutez le fichier `.ini` : `uagdeploy.ps1 uag1.ini`. Ce processus peut prendre jusqu'à 3 minutes.

```
[General]
name=UAG1
source=C:\temp\euc-unified-access-gateway-3.2.1-7766089_OVF10.ova
```

Si vous souhaitez procéder à la mise à niveau sans interruption de service, reportez-vous à la section Mettre à niveau sans interruption.

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, Horizon Cloud with On-Premises Infrastructure, Workspace ONE Access et Workspace ONE UEM.

Lisez les sections suivantes :

Déploiement avec Horizon et Horizon Cloud with On-Premises Infrastructure

Vous pouvez déployer Unified Access Gateway avec Horizon Cloud with On-Premises Infrastructure et l'infrastructure du Cloud Horizon Air.

Scénario de déploiement

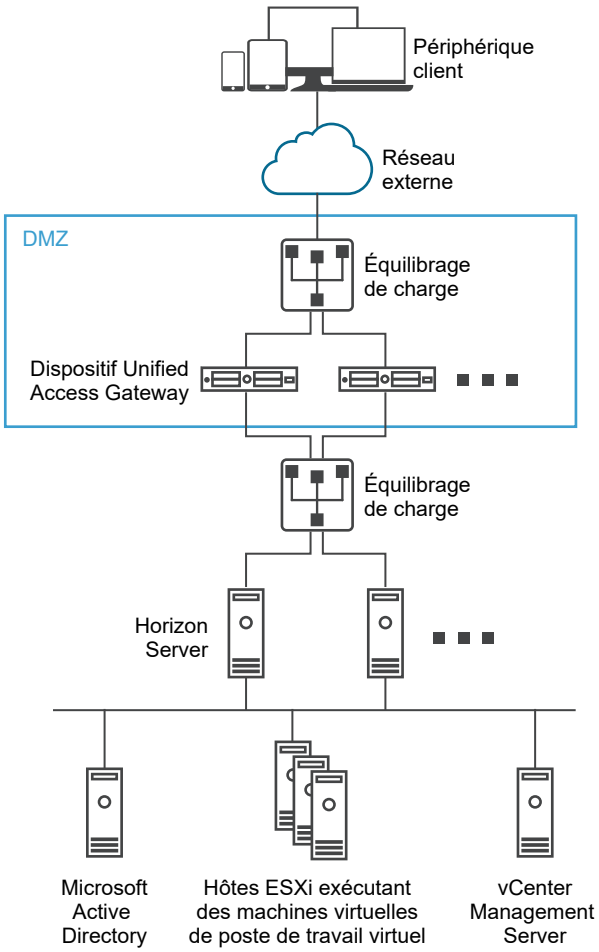
Unified Access Gateway fournit un accès distant sécurisé à des applications et à des postes de travail virtuels sur site dans un centre de données de client. Cela fonctionne avec un déploiement sur site d'Horizon ou d'Horizon Air pour une gestion unifiée.

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.

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

Figure 4-1. Unified Access Gateway dans la topologie de la zone DMZ



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.

- Par défaut, le port 8443 doit être disponible pour Blast TCP/UDP. Toutefois, le port 443 peut également être configuré pour Blast TCP/UDP.

  Note Si vous configurez Unified Access Gateway pour utiliser les modes IPv4 et IPv6, le protocole Blast TCP/UDP doit être défini sur le port 443. Reportez-vous à la section Unified Access Gateway Prise en charge du double mode IPv4 et IPv6 pour l'infrastructure Horizon .

- 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 les 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 du Serveur de connexion Horizon et activez ces passerelles sur les dispositifs Unified Access Gateway.

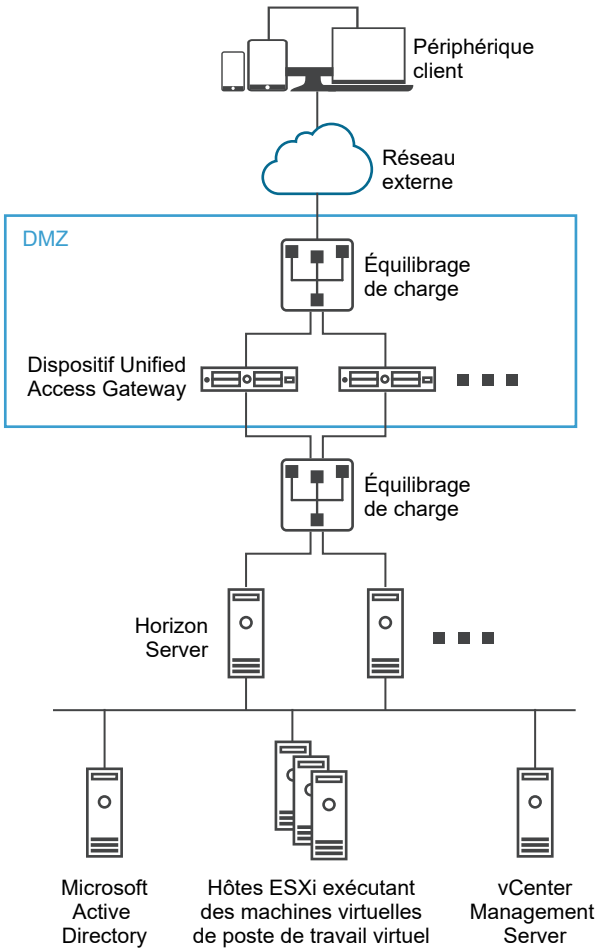
Il est recommandé que les utilisateurs déployant Horizon 7 utilisent le dispositif Unified Access Gateway plutôt que le serveur de sécurité Horizon.

Note Horizon Connection Server ne fonctionne pas avec un proxy inverse Web activé lorsqu'un chevauchement existe dans le modèle de proxy. Par conséquent, si Horizon et une instance du proxy inverse Web sont configurés et activés avec des modèles de proxy sur la même instance Unified Access Gateway, supprimez le modèle de proxy « / » des paramètres d'Horizon et conservez le modèle dans le proxy inverse Web afin d'empêcher le chevauchement. Conserver le modèle de proxy « / » dans l'instance du proxy inverse Web permet de garantir que lorsqu'un utilisateur clique sur l'URL d'Unified Access Gateway, la page appropriée du proxy inverse Web s'affiche. Si seuls les paramètres d'Horizon sont configurés, le changement ci-dessus n'est pas nécessaire.

Les différences entre le serveur de sécurité Horizon et le dispositif Unified Access Gateway sont les suivantes.

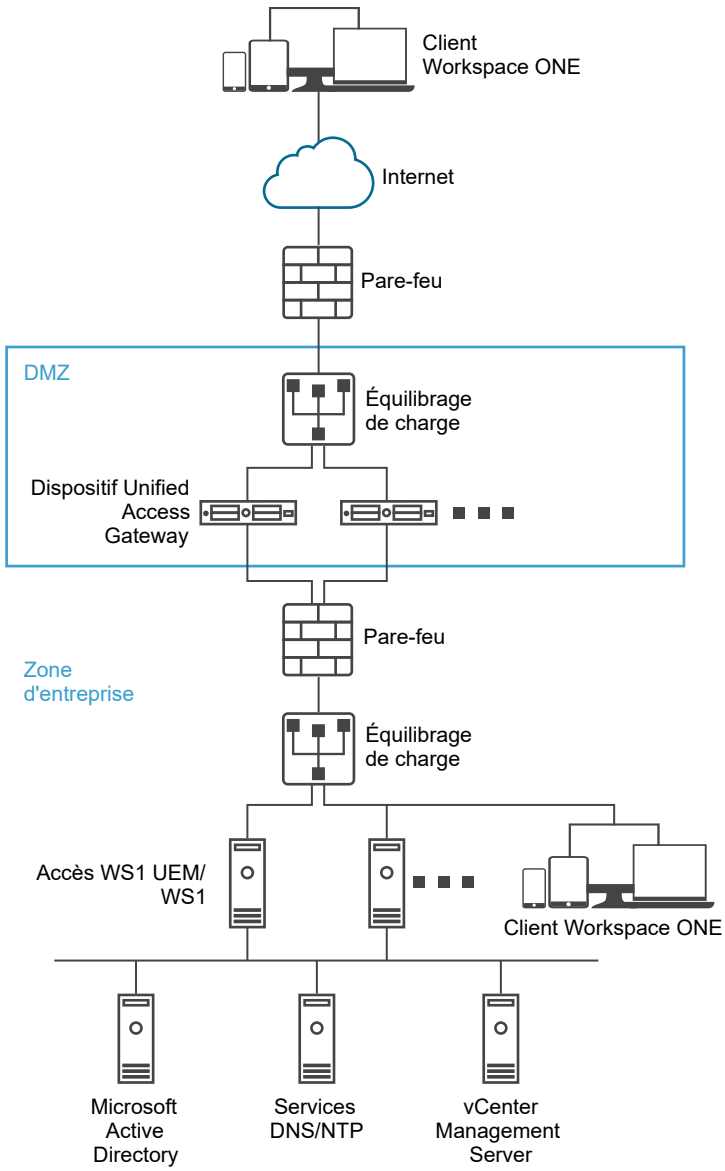
- Déploiement sécurisé. Unified Access Gateway est implémenté en tant que machine virtuelle basée sur Linux, préconfigurée, verrouillée et à sécurité renforcée.
- Évolutivité. Vous pouvez connecter Unified Access Gateway à un Serveur de connexion Horizon individuel ou via un équilibrage de charge devant plusieurs Serveurs de connexion Horizon, ce qui améliore la haute disponibilité. Il fait office de couche entre les clients Horizon Client et les Serveurs de connexion Horizon 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 4-2. 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 4-3. Dispositif Unified Access Gateway pointant vers une instance d'Horizon Server



Authentification

L'authentification utilisateur est semblable à celle du serveur de sécurité Horizon. 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 Horizon.
- Authentification à deux facteurs RSA SecurID, certifiée formellement par RSA pour SecurID.
- RADIUS via diverses solutions tierces de fournisseurs de sécurité à deux facteurs.
- Certificats utilisateur de carte à puce, CAC ou PIV X.509.

- SAML.

Ces méthodes d'authentification sont prises en charge avec Horizon Connection Server. Unified Access Gateway n'a pas besoin de communiquer directement avec Active Directory. Cette communication sert de proxy via le Horizon Connection Server, 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 Horizon Connection Server. 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.

Unified Access Gateway Prise en charge du double mode IPv4 et IPv6 pour l'infrastructure Horizon

Vous pouvez utiliser Unified Access Gateway en tant que pont pour que les clients Horizon puissent se connecter à un environnement Horizon Connection Server de serveur principal ou d'agent. Dans ce scénario, il est possible de configurer Horizon Client et le Horizon Connection Server avec différents modes IP : IPv4 ou IPv6 et inversement.

L'environnement du serveur principal Horizon peut être composé de Serveurs de connexion, de postes de travail d'agent ou d'une autre infrastructure côté serveur.

Combinaisons de mode IP pour l'infrastructure Horizon

Horizon Client et Horizon Connection Server peuvent disposer des modes IP suivants dans l'infrastructure Horizon :

Horizon Client	Horizon Connection Server	Pris en charge
IPv4	IPv4	Oui
IPv6	IPv4	Oui

Horizon Client	Horizon Connection Server	Pris en charge
IPv6	IPv6	Oui
IPv4	IPv6	Oui

Note Lorsque Horizon Client et Horizon Connection Server sont configurés avec différents modes IP (IPv4 ou IPv6 et inversement), le **mode IP du Serveur de connexion**, un paramètre dans l'interface utilisateur d'administration Unified Access Gateway peut comporter l'une des valeurs suivantes : même mode IP que le Horizon Connection Server ou le mode mixte `(IPv4+IPv6)`.

Par exemple : Horizon Client est configuré avec IPv4 et Horizon Connection Server est configuré avec IPv6, le **mode IP du Serveur de connexion** peut comporter les valeurs `IPv6` ou `IPv4+IPv6` (mode mixte).

Pour plus d'informations sur le paramètre du **mode IP du Serveur de connexion**, reportez-vous à Configuration des paramètres d'Horizon.

Lorsque le mode IP est ponté (IPv4 à IPv6 ou IPv6 à IPv4), Unified Access Gateway ne prend pas en charge les éléments suivants : Horizon Tunnel, PCoIP ou Blast UDP.

Note L'URL externe Blast doit être configurée pour utiliser le port TCP 443 ou 8443.

Paramètres avancés des services Edge

Unified Access Gateway utilise différentes variables pour différencier les services Edge, les proxys Web configurés et les URL de destination du proxy.

Modèle de proxy et modèle non sécurisé

Unified Access Gateway utilise un modèle de proxy pour transmettre les demandes HTTP entrantes au service Edge adéquat, tel que Horizon ou à l'une des instances du proxy inverse Web configurées telles que Workspace ONE Access. Par conséquent, il est utilisé en tant que filtre pour décider si un proxy inverse est nécessaire pour traiter le trafic entrant.

Si un proxy inverse est sélectionné, le proxy utilise un modèle non sécurisé spécifié afin de décider s'il faut autoriser ou non le trafic entrant à atteindre le serveur principal sans être authentifié.

L'utilisateur doit spécifier un modèle de proxy, en spécifiant qu'un modèle non sécurisé est facultatif. Le modèle non sécurisé est utilisé par des proxys inverses Web tels que Workspace ONE Access qui ont leur propre mécanisme de connexion et souhaitent que certaines URL telles que des chemins d'accès à des pages de connexion, des scripts JavaScript ou ressources d'image, soient transmises au serveur principal sans être authentifiées.

Note Un modèle non sécurisé est un sous-ensemble du modèle de proxy et, par conséquent, il est possible que certains chemins d'accès soient répétés entre les deux pour un proxy inverse.

Note Le modèle peut également être utilisé pour exclure certaines URL. Par exemple, pour autoriser toutes les URL mais bloquer /admin, vous pouvez utiliser l'expression suivante. `^/(?!admin(.*))(.*)`

Chaque service Edge peut avoir un modèle différent. Par exemple, le `Proxy Pattern` pour Horizon peut être configuré en tant que `(/|/view-client(.*)|/portal(.*)|/appblast(.*))` et le modèle pour Workspace ONE Access peut être configuré en tant que `(/|/SAAS(.*)|/hc(.*)|/web(.*)|/catalog-portal(.*))`.

Note Horizon Connection Server ne fonctionne pas avec un proxy inverse Web activé lorsqu'un chevauchement existe dans le modèle de proxy. Par conséquent, si Horizon et une instance du proxy inverse Web telle que Workspace ONE Access sont configurés et activés avec des modèles de proxy sur la même instance de Unified Access Gateway, supprimez le modèle de proxy « / » des paramètres Horizon et conservez le modèle dans Workspace ONE Access afin d'empêcher le chevauchement.

Conserver le modèle de proxy « / » dans l'instance du proxy inverse Web (Workspace ONE Access) permet de garantir que lorsqu'un utilisateur clique sur l'URL de Unified Access Gateway, la page Workspace ONE Access s'affiche.

Si seuls les paramètres Horizon sont configurés, le changement ci-dessus n'est pas nécessaire.

Modèle d'hôte de proxy

S'il existe plusieurs instances du proxy inverse Web configurées, et qu'un chevauchement est présent dans les modèles de proxy, Unified Access Gateway utilise le `Proxy Host Pattern` pour les différencier. Configurez `Proxy Host Pattern` en tant que nom de domaine complet du proxy inverse.

Par exemple, un modèle d'hôte pour SharePoint peut être configuré en tant que *sharepoint.myco.com* et un modèle pour JIRA peut être configuré en tant que *jira.myco.com*.

Entrées de l'hôte

Configurez cette zone de texte uniquement si Unified Access Gateway n'est pas en mesure d'accéder à l'application ou au serveur principal. Lorsque vous ajoutez l'adresse IP et le nom d'hôte de l'application principale aux entrées de l'hôte, cette information est ajoutée au fichier `/etc/hosts` de Unified Access Gateway. Ce champ est commun à l'ensemble des paramètres des services Edge.

URL de destination du proxy

Il s'agit de l'URL de l'application de serveur principale des paramètres des services Edge pour laquelle Unified Access Gateway est le proxy. Par exemple :

- Pour Horizon Connection Server, l'URL du serveur de connexion est l'URL de destination du proxy.
- Pour le proxy inverse Web, l'URL de l'application du proxy inverse Web configurée est l'URL de destination du proxy.

Configuration d'un proxy inverse unique

Lorsque Unified Access Gateway reçoit une demande entrante unique avec un URI, le modèle de proxy est utilisé pour déterminer si la demande doit être transférée ou déplacée.

Configuration de proxys inverses multiples

1. Lorsque Unified Access Gateway est configuré en tant que proxy inverse et que vous recevez une demande entrante avec un chemin d'accès d'URI, Unified Access Gateway utilise le modèle de proxy pour correspondre à l'instance du proxy inverse Web correct. S'il existe une correspondance, le modèle adéquat sera utilisé. S'il existe plusieurs correspondances, le processus de filtrage et de correspondance sera répété à l'étape 2. En cas de non-correspondance, la demande est abandonnée et une erreur HTTP 404 est renvoyée au client.
2. Le modèle d'hôte de proxy est utilisé pour filtrer la liste précédemment filtrée à l'étape 1. L'en-tête HOST est utilisé pour filtrer la demande et trouver l'instance du proxy inverse. S'il existe une correspondance, le modèle adéquat sera utilisé. S'il existe plusieurs correspondances, le processus de filtrage et de correspondance sera répété à l'étape 3.
3. Notez les points suivants :
   - La première correspondance dans la liste filtrée à l'étape 2 est utilisée. Il est possible que cette correspondance ne soit pas toujours l'instance de proxy inverse Web. Par conséquent, assurez-vous que la combinaison de modèle de proxy et de modèle d'hôte de proxy pour une instance du proxy inverse Web est unique s'il existe une configuration de proxys inverses multiples dans un Unified Access Gateway.
   - Le nom d'hôte de tous les proxys inverses configurés doit être résolu sur la même adresse IP que l'adresse externe de l'instance Unified Access Gateway.

Reportez-vous à la section Configurer le proxy inverse avec Workspace ONE Access pour obtenir plus d'informations et des instructions sur la configuration de proxy inverse.

Par exemple : deux proxys inverses configurés avec des modèles de proxys incompatibles, des modèles d'hôtes distincts

Supposez que le modèle du premier proxy inverse soit `/(.*)` avec le modèle d'hôte en tant que `host1.domain.com` et que le modèle du second proxy inverse soit `(/app2(.*)|/app3(.*)|/)` avec le modèle d'hôte en tant que `host2.domain.com`.

- Si une demande est effectuée avec le chemin d'accès défini sur `https://host1.domain.com/app1/index.html`, la demande est transmise au premier proxy inverse.
- Si une demande est effectuée avec le chemin d'accès défini sur `https://host2.domain.com/app2/index.html`, la demande est transmise au second proxy inverse.

Par exemple : deux proxys inverses avec des modèles de proxys s'excluant mutuellement

Supposez que le modèle du premier proxy inverse soit `/app1(.*)` et du second proxy inverse soit `(/app2(.*)|/app3(.*)|/)`.

- Si une demande est effectuée avec le chemin d'accès défini sur `https://<uag domain name>/app1/index.html`, la demande est transmise au premier proxy inverse.
- Si une demande est effectuée avec le chemin d'accès défini sur `https://<uag domain name>/app3/index.html` ou sur `https://<uag domain name>/`, la demande est transmise au second proxy inverse.

Configuration des paramètres d’Horizon

Vous pouvez déployer Unified Access Gateway avec Horizon Cloud with On-Premises Infrastructure et l'infrastructure du Cloud Horizon Air. Pour le déploiement d'Horizon, le dispositif Unified Access Gateway remplace le serveur de sécurité Horizon.

Conditions préalables

Si vous souhaitez que Horizon et une instance de proxy inverse Web telle que Workspace ONE Access soient tous deux configurés et activés sur la même instance d'Unified Access Gateway, reportez-vous à la section Paramètres avancés des services Edge.

Procédure

1. Dans la section **Configurer manuellement** de l'interface utilisateur d'administration, cliquez sur **Sélectionner**.
2. Dans **Paramètres généraux > Paramètres du service Edge**, cliquez sur **Afficher**.
3. Cliquez sur l'icône d'engrenage **Paramètres d’Horizon**.
4. Dans la page Paramètres d'Horizon, remplacez NON par **OUI** pour activer Horizon.

5 Configurez les ressources des paramètres du service Edge suivantes pour Horizon :

Option	Description
Identifiant	Définissez par défaut sur Horizon. Unified Access Gateway peut communiquer avec des serveurs qui utilisent le protocole Horizon XML, tels que le Serveur de connexion Horizon, Horizon Air 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`.
Empreinte numérique de l'URL du Serveur de connexion	Entrez la liste des empreintes numériques Horizon Server. Si vous ne fournissez pas de liste d'empreintes numériques, assurez-vous que les certificats de serveur sont 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.
Activer PCOIP	Remplacez NON par **OUI** pour spécifier si PCoIP Secure Gateway est activé.
Désactiver le certificat hérité PCOIP	Remplacez **NON** par **OUI** pour indiquer d'utiliser le certificat de serveur SSL téléchargé au lieu du certificat hérité. Les clients PCoIP hérités ne fonctionneront pas si ce paramètre est défini sur **OUI**.
URL externe PCOIP	URL utilisée par les clients Horizon pour établir la session PCoIP Horizon avec ce dispositif Unified Access Gateway. Cette URL doit contenir une adresse IPv4 et non un nom d'hôte. Par exemple, `10.1.2.3:4172`. La valeur par défaut est l'adresse IP d'Unified Access Gateway et le port 4172.
Activer Blast	Pour utiliser la passerelle sécurisée Blast, Remplacez NO par **YES**.
Mode IP du Serveur de connexion	Indique le mode IP d'un Horizon Connection Server Ce champ peut comporter les valeurs suivantes : `IPv4`, `IPv6` et `IPv4+IPv6`. La valeur par défaut est `IPv4`. ■ Si toutes les cartes réseau du dispositif Unified Access Gateway sont en mode IPv4 (et non en mode IPv6), ce champ peut comporter l'une des valeurs suivantes : `IPv4` ou `IPv4+IPv6` (mode mixte). ■ Si toutes les cartes réseau dans le dispositif Unified Access Gateway sont en mode IPv6 (et non pas en mode IPv4), ce champ peut comporter l'une des valeurs suivantes : `IPv6` ou `IPv4+IPv6` (mode mixte).
Réécrire l'en-tête d'origine	Si une demande entrante envoyée à Unified Access Gateway dispose de l'en-tête `Origin` et si le champ **Réécrire l'en-tête d'origine** est activé, Unified Access Gateway réécrit l'en-tête `Origin` avec l'**URL du Serveur de connexion**. Le champ **Réécrire l'en-tête d'origine** fonctionne avec la propriété CORS `checkOrigin` du Horizon Connection Server. Lorsque ce champ est activé, il n'est pas nécessaire que l'administrateur Horizon spécifie les adresses IP Unified Access Gateway dans le fichier `locked.properties`. Pour plus d'informations sur la vérification de l'origine, reportez-vous à la documentation *Sécurité d'Horizon 7*.

6 Pour configurer la règle de la méthode d'authentification et les 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 suivantes sont prises en charge : `SAML`, `SAML and Unauthenticated`, `RSA SecurID`, `SecurID and Unauthenticated`, `RADIUS`, `RADIUS and Unauthenticated` et `Device Certificate`. **Important** Si vous avez choisi l'une des méthodes `Unauthenticated` comme méthode d'authentification, veillez à configurer le **Niveau de ralentissement de la connexion** dans le Horizon Connection Server sur `Low`. Cette configuration est nécessaire pour éviter un long retard du délai de connexion pour les points de terminaison lors de l'accès à l'application ou au poste de travail distant. Pour plus d'informations sur la configuration du **Niveau de ralentissement de la connexion**, consultez la documentation de l' *Administration d'Horizon* sur VMware Docs.
Activer Windows SSO	Cette option être activée lorsque les méthodes d'authentification sont définies sur RADIUS et lorsque le code secret RADIUS est le même que le mot de passe du domaine Windows. Remplacez **NON** par **OUI** pour utiliser le nom d'utilisateur et le code secret RADIUS pour les informations d'identification de connexion au domaine Windows afin d'éviter de devoir inviter à nouveau l'utilisateur. Si Horizon est configuré sur un environnement à domaines multiples, si le nom d'utilisateur fourni ne contient pas de nom de domaine, le domaine ne sera pas envoyé à CS. Si le suffixe NameID est configuré et si le nom d'utilisateur fourni ne contient pas de nom de domaine, la valeur de configuration du suffixe NameID sera ajoutée au nom d'utilisateur. Par exemple, si un utilisateur a fourni jdoe comme nom d'utilisateur et que NameIDSuffix est défini sur `@north.int`, le nom d'utilisateur envoyé serait `jdoe@north.int`. Si le suffixe NameID est configuré et si le nom d'utilisateur fourni est au format UPN, le suffixe NameID sera ignoré. Par exemple, si un utilisateur a fourni `jdoe@north.int`, NameIDSuffix - `@south.int`, le nom d'utilisateur serait `jdoe@north.int` Si le nom d'utilisateur fourni est au format `<DomainName\username>`, par exemple `NORTH\jdoe`, Unified Access Gateway envoie le nom d'utilisateur et le nom de domaine séparément à CS.
Attributs de classe RADIUS	Cette option est activée lorsque les méthodes d'authentification doivent être définies sur RADIUS. Cliquez sur « + » pour ajouter une valeur pour l'attribut de classe. Entrez le nom de l'attribut de classe à utiliser pour l'authentification utilisateur. Cliquez sur « - » pour supprimer un attribut de classe. **Note** Si ce champ reste vide, l'autorisation supplémentaire n'est pas effectuée.
Texte d'exclusion de responsabilité	Texte du message de clause de non-responsabilité d'Horizon affiché que l'utilisateur doit accepter dans les cas où une **méthode d'authentification** est configurée.

Option	Description
Invite de conseil de carte à puce	Remplacez NON par **OUI** pour activer l'indication de mot de passe pour l'authentification par certificat.
Chemin d'accès à l'URI de contrôle de santé	Chemin d'accès à l'URI du serveur de connexion auquel se connecte Unified Access Gateway pour contrôler l'état de santé.
URL externe Blast	URL utilisée par les clients Horizon pour établir la session Horizon Blast ou BEAT avec ce dispositif Unified Access Gateway. Par exemple, `https://uag1.myco.com` ou `https://uag1.myco.com:443`. Si le numéro de port TCP n'est pas spécifié, le port TCP par défaut est 8443. Si le numéro de port UDP n'est pas spécifié, le port UDP par défaut est également 8443.
Activer le serveur UDP	Les connexions sont établies via le serveur de tunnel UDP si la bande passante est faible.
Certificat de proxy Blast	Certificat de proxy pour Blast. Cliquez sur **Sélectionner** pour télécharger un certificat au format PEM et l'ajouter au magasin des approbations BLAST. Cliquez sur **Modifier** pour remplacer le certificat existant. Si l'utilisateur télécharge manuellement le même certificat pour Unified Access Gateway dans l'équilibrage de charge et qu'il doit utiliser un certificat différent pour Unified Access Gateway et pour Blast Gateway, l'établissement d'une session de poste de travail Blast échoue, car l'empreinte numérique entre le client et Unified Access Gateway ne correspond pas. L'entrée de l'empreinte numérique personnalisée dans Unified Access Gateway ou dans Blast Gateway résout le problème en relayant l'empreinte numérique afin d'établir la session client.
Activer le tunnel	Si le tunnel sécurisé Horizon est utilisé, remplacez NON par **OUI**. Le client utilise l'URL externe pour les connexions par tunnel via Horizon Secure Gateway. Le tunnel est utilisé pour le trafic RDP, USB et de redirection multimédia (MMR).
URL externe de tunnel	URL utilisée par les clients Horizon pour établir la session Horizon Tunnel avec ce dispositif Unified Access Gateway. Par exemple, `https://uag1.myco.com` ou `https://uag1.myco.com:443`. Si le numéro de port TCP n'est pas spécifié, le port TCP par défaut est 443.
Certificat du proxy de tunnel	Certificat du proxy pour Horizon Tunnel. Cliquez sur **Sélectionner** pour télécharger un certificat au format PEM et l'ajouter au magasin des approbations Tunnel. Cliquez sur **Modifier** pour remplacer le certificat existant. Si l'utilisateur télécharge manuellement le même certificat pour Unified Access Gateway dans l'équilibrage de charge et qu'il doit utiliser un certificat différent pour Unified Access Gateway et pour Horizon Tunnel, l'établissement d'une session Tunnel échoue, car l'empreinte numérique entre le client et Unified Access Gateway ne correspond pas. L'entrée de l'empreinte numérique personnalisée dans Unified Access Gateway ou dans Horizon Tunnel résout le problème en relayant l'empreinte numérique afin d'établir la session client.
Fournisseur de vérification de la conformité du point de terminaison	Sélectionnez le fournisseur de vérification de la conformité du point de terminaison. La valeur par défaut est OPSWAT.

Option	Description
Modèle de proxy	Entrez l'expression régulière qui correspond aux URI liés à l'URL d'Horizon Server (proxyDestinationUrl). Sa valeur par défaut est `(/|/view-client(.*)|/portal(.*)|/appblast(.*))`. **Note** Le modèle peut également être utilisé pour exclure certaines URL. Par exemple, pour autoriser toutes les URL mais bloquer /admin, vous pouvez utiliser l'expression suivante.`^/(?!admin(.*))(.*)`
SP SAML	Entrez le nom du fournisseur de services SAML pour le broker Horizon XMLAPI. Ce nom doit correspondre à celui des métadonnées du fournisseur de services configuré ou à la valeur spéciale DEMO.
Déconnexion lors de la suppression du certificat	**Note** Cette option est disponible lorsque l'une des méthodes d'authentification par carte à puce est sélectionnée comme **méthode d'authentification**. Si cette option est définie sur `YES` et si la carte à puce est supprimée, l'utilisateur final est obligé de se déconnecter d'une session Unified Access Gateway.
Étiquette du nom d'utilisateur pour RADIUS	Entrez du texte pour personnaliser l'étiquette du nom d'utilisateur dans Horizon Client. Par exemple, `Domain Username` La méthode d'authentification RADIUS doit être activée. Pour activer RADIUS, reportez-vous à la section Configuration de l'authentification RADIUS. Le nom d'étiquette par défaut est `Username`. Le nom de l'étiquette ne doit pas dépasser 20 caractères.
Étiquette de code secret pour RADIUS	Entrez un nom pour personnaliser l'étiquette du code secret dans Horizon Client. Par exemple, `Password` La méthode d'authentification RADIUS doit être activée. Pour activer RADIUS, reportez-vous à la section Configuration de l'authentification RADIUS. Le nom d'étiquette par défaut est `Passcode`. Le nom de l'étiquette ne doit pas dépasser 20 caractères.

Option	Description
Correspondre au nom d'utilisateur Windows	Remplacez **NON** par **OUI** pour faire correspondre RSA SecurID et le nom d'utilisateur Windows. Lorsqu'il est défini sur **OUI**, *securID-auth* est défini sur true et la correspondance de *securID* et du nom d'utilisateur Windows est appliquée. Si Horizon est configuré sur un environnement à domaines multiples, si le nom d'utilisateur fourni ne contient pas de nom de domaine, le domaine ne sera pas envoyé à CS. Si le suffixe NameID est configuré et si le nom d'utilisateur fourni ne contient pas de nom de domaine, la valeur de configuration du suffixe NameID sera ajoutée au nom d'utilisateur. Par exemple, si un utilisateur a fourni jdoe comme nom d'utilisateur et que NameIDSuffix est défini sur `@north.int`, le nom d'utilisateur envoyé serait `jdoe@north.int`. Si le suffixe NameID est configuré et si le nom d'utilisateur fourni est au format UPN, le suffixe NameID sera ignoré. Par exemple, si un utilisateur a fourni `jdoe@north.int`, NameIDSuffix - `@south.int`, le nom d'utilisateur serait `jdoe@north.int` Si le nom d'utilisateur fourni est au format `<DomainName\username>`, par exemple `NORTH\jdoe`, Unified Access Gateway envoie le nom d'utilisateur et le nom de domaine séparément à CS. **Note** Dans Horizon 7, si vous activez les paramètres **Masquer les informations de serveur dans l'interface utilisateur client** et **Masquer la liste de domaines dans l'interface utilisateur client** et que vous sélectionnez l'authentification à deux facteurs (RSA SecureID ou RADIUS) pour l'instance du Serveur de connexion, n'appliquez pas la correspondance des noms d'utilisateur Windows. L'application de la correspondance des noms d'utilisateur Windows empêche les utilisateurs d'entrer des informations de domaine dans la zone de texte Nom d'utilisateur, et la connexion échoue toujours. Pour plus d'informations, reportez-vous aux rubriques concernant l'authentification à deux facteurs dans le document Administration d'Horizon 7.
Emplacement de la passerelle	Emplacement d'origine de la demande de connexion. Le serveur de sécurité et Unified Access Gateway définissent l'emplacement de la passerelle. L'emplacement peut être `External` ou `Internal`. **Important** L'emplacement doit être défini sur `Internal` lorsque l'une des méthodes d'authentification suivantes est sélectionnée : `SAML and Unauthenticated`, `SecurID and Unauthenticated` ou `RADIUS and Unauthenticated`.
Paramètres JWT	**Note** Pour la validation de l'artefact SAML du jeton JWT de Workspace ONE Access, assurez-vous que le champ **Nom** est configuré dans la section **Paramètres JWT** de **Paramètres avancés**. Sélectionnez le nom de l'un des **paramètres JWT** configurés.
Publics JWT	Liste facultative des destinataires prévus du JWT utilisé pour la validation de l'artefact SAML de Workspace ONE Access Horizon. Pour que la validation JWT réussisse, au moins un des destinataires de cette liste doit correspondre à l'un des publics spécifiés dans la configuration de Workspace ONE Access Horizon. Si aucun public JWT n'est spécifié, la validation JWT ne tient pas compte des publics.

Option	Description
Certificats approuvés	Ajoutez un certificat approuvé à ce service Edge. Cliquez sur le signe « + » pour sélectionner un certificat au format PEM et l'ajouter au magasin des approbations. Cliquez sur le signe «- » pour supprimer un certificat du magasin d'approbations. Par défaut, le nom d'alias est le nom de fichier du certificat PEM. Modifiez la zone de texte de l'alias afin de fournir un nom différent à l'alias.
En-têtes de sécurité de réponse	Cliquez sur « + » pour ajouter un en-tête. Entrez le nom de l'en-tête de sécurité. Entrez la valeur. Cliquez sur « - » pour supprimer un en-tête. Modifiez un en-tête de sécurité existant pour mettre à jour le nom et la valeur de l'en-tête. **Important** Les noms et valeurs d'en-têtes ne sont enregistrés qu'après avoir cliqué sur **Enregistrer**. Certains en-têtes de sécurité standard sont présents par défaut. Les en-têtes configurés sont ajoutés à la réponse d'Unified Access Gateway au client uniquement si les en-têtes correspondants sont absents dans la réponse du serveur principal configuré. **Note** Modifiez les en-têtes de réponse de sécurité avec précaution. La modification de ces paramètres risque d'affecter le fonctionnement sécurisé d'Unified Access Gateway.
Mappages de redirection d'hôte	Pour plus d'informations sur la prise en charge de la capacité de redirection d'hôte HTTP par UAG et certaines considérations requises pour l'utilisation de cette capacité, reportez-vous à la section Prise en charge par Unified Access Gateway de la redirection d'hôte HTTP. ■ **Hôte source** Entrez le nom d'hôte de la source (équilibrage de charge). ■ **Hôte de redirection** Entrez le nom d'hôte du dispositif UAG (Unified Access Gateway) dont l'affinité doit être maintenue avec Horizon Client.
Entrées de l'hôte	Entrez les détails qui doivent être ajoutés 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`**. pour ajouter plusieurs entrées de l'hôte, cliquez sur le signe « + ». **Important** Les entrées de l'hôte sont enregistrées uniquement après avoir cliqué sur **Enregistrer**.
Publics SAML	Assurez-vous que la méthode d'authentification SAML, ou SAML et relais, est choisie. Entrez l'URL du public. **Note** Si la zone de texte reste vide, les publics ne sont pas restreints. Pour comprendre comment UAG prend en charge les publics SAML, consultez la section Publics SAML.

Option	Description
Attribut de nom d'utilisateur non authentifié SAML	Entrer le nom de l'attribut personnalisé **Note** Ce champ n'est disponible que lorsque la valeur des **Méthodes d'authentification** est `SAML and Unauthenticated`. Lorsqu'UAG valide l'assertion SAML, si le nom d'attribut spécifié dans ce champ est présent dans l'assertion, UAG fournit l'accès non authentifié au nom d'utilisateur configuré pour l'attribut dans le fournisseur d'identité. Pour plus d'informations sur la méthode `SAML and Unauthenticated`, consultez la section Méthodes d'authentification pour l'intégration d'Unified Access Gateway et du fournisseur d'identité tiers.
Nom d'utilisateur non authentifié par défaut	Entrer le nom d'utilisateur par défaut qui doit être utilisé pour l'accès non authentifié Ce champ est disponible dans l'interface utilisateur d'administration lorsque l'une des **Méthodes d'authentification** suivantes est sélectionnée : `SAML and Unauthenticated`, `SecurID and Unauthenticated` et `RADIUS and Unauthenticated`. **Note** Pour la méthode d'authentification `SAML and Unauthenticated`, le nom d'utilisateur par défaut pour l'accès non authentifié n'est utilisé que lorsque le champ **Attribut de nom d'utilisateur non authentifié SAML** est vide ou que le nom d'attribut spécifié dans ce champ est manquant dans l'assertion SAML.
Désactiver HTML Access	Si l'option est définie sur OUI, désactive l'accès Web à Horizon. Reportez-vous à la section Configurer les paramètres du fournisseur de vérification de la conformité du point de terminaison pour Horizon pour plus d'informations.

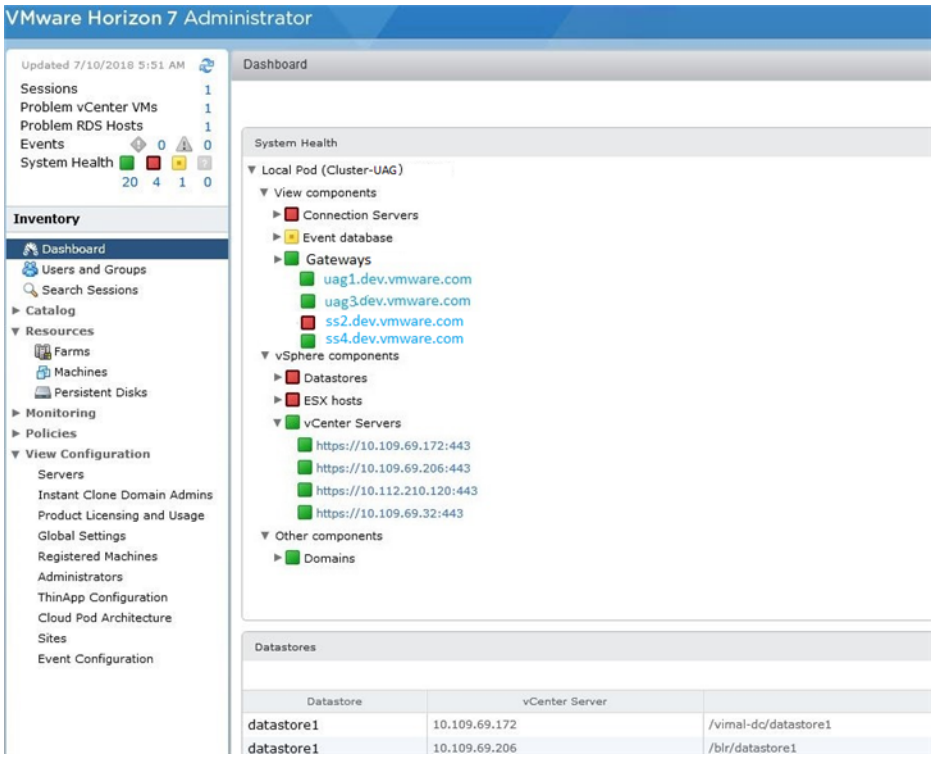
7 Cliquez sur **Enregistrer**.

Surveillance d'Unified Access Gateway dans Horizon Console

L'intégration d'Unified Access Gateway à la console d'administration Horizon fournit la visibilité sur les informations d'état, de statistiques et de sessions dans l'interface utilisateur d'administration d'Horizon. Vous pouvez surveiller la santé du système d'Unified Access Gateway.

Le nouvel onglet **Passerelle** dans la console d'administration Horizon fournit une fonctionnalité d'enregistrement et d'annulation de l'enregistrement d'Unified Access Gateway.

Figure 4-4. Tableau de bord



L'écran Tableau de bord affiche les détails de l'instance d'Unified Access Gateway enregistrée pour la version 3.4 ou version ultérieure, les composants vSphere, les domaines, les postes de travail et l'utilisation de la banque de données.

Prise en charge par Unified Access Gateway de la redirection d'hôte HTTP

Vous pouvez utiliser la capacité de redirection d'hôte HTTP pour simplifier les exigences d'affinité d'équilibrage de charge Horizon dans certains environnements à plusieurs adresses IP virtuelles. Pour utiliser la capacité de redirection d'hôte HTTP, les administrateurs UAG doivent configurer la zone de texte **Mappages de redirection d'hôte** dans les paramètres d'Horizon.

Lorsqu'une demande HTTP atteint UAG avec le nom d'hôte d'un équilibrage de charge, UAG répond par une redirection HTTP 307 et remplace le nom d'hôte de l'équilibrage de charge par le propre nom d'hôte configuré d'UAG. Pour les demandes suivantes, Horizon Client se reconnecte directement avec UAG. Cela permet de s'assurer que les demandes ultérieures ne sont pas acheminées via l'équilibrage de charge. La capacité de redirection évite les problèmes de contrôle d'affinité sur les équilibrages de charge où les demandes pouvaient être acheminées vers le l'instance appropriée d'UAG.

Par exemple, prenez un environnement avec un équilibrage de charge et deux dispositifs UAG, UAG1 et UAG2. Si une demande atteint UAG1 avec le nom d'hôte de l'équilibrage de charge comme `load-balancer.example.com`, UAG1 répond par une redirection `HTTP 307` et remplace le nom d'hôte de l'équilibrage de charge par le propre nom d'hôte configuré d'UAG, `uag1.example.com`. Pour les demandes suivantes, Horizon Client se reconnecte directement avec UAG1.

Éléments à prendre en compte lors de l'utilisation de la redirection d'hôte HTTP

Vous devez tenir compte des éléments suivants lors de l'utilisation de la fonctionnalité de redirection d'hôte HTTP :

- L'adresse IP virtuelle `N + 1` est requise, où

  `N` : nombre de dispositifs UAG déployés dans l'environnement

  `1` : adresse IP virtuelle de l'équilibrage de charge

- Vous ne pouvez pas utiliser des équilibrages de charge qui fonctionnent à la couche 7.

Pour configurer les paramètres dans Horizon, reportez-vous à la section Configuration des paramètres d'Horizon

Publics SAML

Publics SAML est une fonctionnalité prise en charge par UAG (Unified Access Gateway) pour les services Edge, tel qu'Horizon et le proxy inverse Web. Grâce à la fonctionnalité Publics SAML, les administrateurs UAG peuvent limiter l'accès des publics aux clients Horizon et aux applications principales.

Dans le service Horizon Edge, les méthodes d'authentification SAML, et SAML et relais prennent en charge les publics SAML. Dans le service Edge du proxy inverse Web, la méthode d'authentification SAML prend en charge les publics SAML uniquement lorsque le pontage d'identité est activé.

Si l'option **Publics SAML** est configurée avec des valeurs, UAG valide cette liste de valeurs dans les publics reçus dans l'assertion SAML. S'il existe au moins une correspondance, l'assertion SAML est acceptée. Sinon, UAG rejette l'assertion SAML. Si l'option Publics SAML n'est pas configurée, UAG ne valide pas les publics dans l'assertion SAML.

Pour restreindre les publics du service Horizon Edge, consultez la section Configuration des paramètres d'Horizon. Pour restreindre les publics du service Edge du proxy inverse Web, consultez la section Configurer un proxy inverse Web pour le pontage d'identité (SAML sur Kerberos).

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:xxxx/?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.

Vérifications de la conformité du point de terminaison pour Horizon

La fonctionnalité Vérifications de la conformité du point de terminaison sur UAG (Unified Access Gateway) fournit une couche supplémentaire de sécurité pour accéder à des postes de travail Horizon, en plus des autres services d'authentification utilisateur disponibles sur UAG.

Vous pouvez utiliser la fonctionnalité Vérifications de la conformité du point de terminaison pour garantir la conformité à différentes stratégies, telles qu'une stratégie antivirus ou une stratégie de chiffrement sur des points de terminaison. La conformité du point de terminaison est vérifiée lorsqu'un utilisateur tente de lancer une application ou un poste de travail à distance à partir des droits répertoriés.

La stratégie de conformité du point de terminaison est définie sur un service exécuté dans le Cloud ou sur site. Dans le cas d'OPSWAT, la vérification de la conformité du point de terminaison est effectuée par l'OPSWAT MetaAccess persistent agent ou l'OPSWAT MetaAccess on-demand agent sur Horizon Client. Les agents OPSWAT communiquent l'état de conformité à une instance d'OPSWAT qui s'exécute dans le Cloud ou sur site.

Les Vérifications de la conformité du point de terminaison sont des paramètres avancés, qui peuvent être configurés sur la page **Paramètres du fournisseur de vérification de la conformité du point de terminaison**. Sur cette page, vous pouvez configurer les informations du fournisseur de vérification de la conformité, les intervalles de vérification de la conformité, les codes d'état, etc.

La page **Paramètres du fournisseur de vérification de la conformité du point de terminaison** comprend également des paramètres qui offrent la possibilité de configurer Unified Access Gateway pour l'hébergement de l'on-demand agent. Cette configuration permet à Horizon Client de télécharger l'on-demand agent à partir d'Unified Access Gateway lorsque cela est nécessaire.

Configurer les paramètres du fournisseur de vérification de la conformité du point de terminaison pour Horizon

Pour le service Edge Horizon, vous pouvez configurer les paramètres du fournisseur de vérification de la conformité du point de terminaison dans l'interface utilisateur d'administration d'Unified Access Gateway.

Si les paramètres **Fournisseur de vérification de la conformité du point de terminaison** sont configurés sur la page **Paramètres d'Horizon**, Unified Access Gateway effectue une vérification du périphérique de point de terminaison Horizon Client avec le fournisseur de vérification de conformité. Cette vérification est effectuée de façon à ce que les utilisateurs dont les points de terminaison ne sont pas conformes se voient refuser l'accès aux applications et aux postes de travail Horizon.

Conditions préalables

Le fournisseur de vérification de la conformité du point de terminaison actuellement pris en charge sur Unified Access Gateway est OPSWAT. Pour ce fournisseur, vous devez effectuer les tâches suivantes avant de configurer les paramètres sur l'interface utilisateur d'administration d'Unified Access Gateway :

1. Créez un compte OPSWAT et enregistrez vos applications sur le site OPSWAT. Reportez-vous à la section https://go.opswat.com/communityRegistration.
2. Notez la clé du client et la clé secrète du client. Vous avez besoin des clés pour configurer OPSWAT dans Unified Access Gateway.
3. Connectez-vous au site OPSWAT et configurez les stratégies de conformité pour vos points de terminaison.

   Consultez la documentation OPSWAT appropriée.

Procédure

1. Connectez-vous à l'interface utilisateur d'administration et accédez à **Paramètres avancés > Paramètres du fournisseur de vérification de la conformité du point de terminaison**.

2 Cliquez sur **Ajouter**.

Les zones de texte **Fournisseur de vérification de la conformité du point de terminaison** et **Nom d'hôte** sont déjà renseignées.

3 Entrez **Clé du client** et **Secret du client**.

4 Entrez la valeur souhaitée pour **Intervalle de vérification de la conformité (minutes)**.

- Valeurs valides (en minutes) : entre `5` et `1440`
- Valeur par défaut : `0`

  `0` indique que l'option **Intervalle de vérification de la conformité (minutes)** est désactivée.

Pour plus d'informations sur les vérifications de conformité périodiques et l'option **Intervalle de vérification de la conformité (minutes)**, reportez-vous à la section Intervalle de vérification périodique de conformité du point de terminaison.

5 Entrez la valeur souhaitée pour **Intervalle rapide de vérification de la conformité (minutes)**.

Important Pour configurer l'option **Intervalle rapide de vérification de la conformité (minutes)**, vérifiez que l'option **Intervalle de vérification de la conformité (minutes)** est configurée et qu'elle n'est pas définie sur `0`.

- Valeurs valides (en minutes) : entre `1` et `1440`
- Valeur par défaut : `0`

  `0` indique que l'option **Intervalle rapide de vérification de la conformité (minutes)** est désactivée.

Pour plus d'informations sur les vérifications de conformité périodiques et l'option **Intervalle rapide de vérification de vérification de la conformité (minute)**, reportez-vous à la section Intervalle de vérification périodique de conformité du point de terminaison.

6 Pour modifier la valeur par défaut des états et autoriser le lancement des points de terminaison, cliquez sur **Afficher les codes d'état autorisés**.

Les codes d'état suivants sont pris en charge : `In compliance`, `Not in compliance`, `Out of license usage`, `Assessment pending`, `Endpoint unknown` et `Others`.

7 Pour le **Code d'état** souhaité, cliquez pour passer de **DENY** à **ALLOW**.

La valeur par défaut du code d'état **Conforme** est `ALLOW`. Seul le lancement des points de terminaison conformes est autorisé.

La valeur par défaut de tous les autres codes d'état est `DENY`.

8 Pour charger le fichier exécutable d'OPSWAT MetaAccess on-demand agent pour Windows et macOS sur Unified Access Gateway, cliquez sur **Afficher les paramètres de l'agent OPSWAT à la demande** et configurez les paramètres requis.

Reportez-vous à la section Charger le logiciel de l'OPSWAT MetaAccess on-demand agent sur Unified Access Gateway.

9 Cliquez sur **Enregistrer**.

Étape suivante

1 Accédez aux paramètres d'Horizon, localisez la zone de texte **Fournisseur de vérification de la conformité du point de terminaison**, puis sélectionnez `OPSWAT` dans le menu déroulant.

2 Cliquez sur **Enregistrer**.

Charger le logiciel de l'OPSWAT MetaAccess on-demand agent sur Unified Access Gateway

Les administrateurs peuvent charger le fichier exécutable de l'on-demand agent sur Unified Access Gateway. Cela permet éventuellement à Horizon Client de télécharger et d'exécuter automatiquement l'on-demand agent une fois que l'utilisateur s'est authentifié avec succès.

Pour en savoir plus sur l'on-demand agent, reportez-vous à la section À propos d'OPSWAT MetaAccess on-demand agent.

Conditions préalables

Localisez le fichier exécutable de l'on-demand agent sur le site Web OPSWAT approprié et téléchargez le fichier sur votre système.

Vous pouvez également placer le fichier exécutable sur un serveur de fichiers et spécifier l'URL d'emplacement du serveur de fichiers correspondante lors de la configuration des paramètres sur l'interface utilisateur d'administration. Avec cette référence d'URL, Unified Access Gateway peut télécharger le fichier à partir de l'URL configurée.

Important Pour que Unified Access Gateway télécharge correctement le fichier, le serveur de fichiers doit disposer de l'en-tête `Content-Disposition` avec le nom de fichier de l'agent à la demande en tant que valeur dans la réponse HTTP.

Procédure

- Pour la plate-forme Windows, suivez les étapes décrites ci-dessous.
  a Sélectionnez le **Type de chargement de fichier**.
    - Si vous ne souhaitez charger aucun fichier, sélectionnez `None`.
    - `None` est la valeur par défaut.
  b En fonction du type de chargement de fichier sélectionné, entrez les informations requises pour le chargement de l'on-demand agent sur Unified Access Gateway.

Option	Procédure
Local	1 Localisez et sélectionnez le fichier exécutable d'on-demand agent que vous avez téléchargé à partir d'OPSWAT. 2 Entrez les informations supplémentaires suivantes pour l'on-demand agent : **Nom** et **Paramètres**.
Référence d'URL	1 Dans **URL du fichier d'agent**, entrez l'URL de l'emplacement du serveur de fichiers à partir duquel Unified Access Gateway peut télécharger le fichier exécutable de l'on-demand agent. 2 Entrez les informations supplémentaires suivantes pour l'agent : **Nom**, **Paramètres**, **Empreintes numériques de l'URL de l'agent**, **Certificats approuvés** et **Intervalle d'actualisation du fichier d'agent (secondes)**

Les informations suivantes ont pour but de vous aider à comprendre les paramètres fournis pour le chargement de l'on-demand agent sur Unified Access Gateway :

Nom

Nom du fichier exécutable de l'on-demand agent.

Paramètres

Paramètres de ligne de commande utilisés par Horizon Client pour exécuter l'on-demand agent sur le point de terminaison.

Pour les paramètres de ligne de commande qui peuvent être utilisés dans la zone de texte **Paramètres**, reportez-vous à la documentation d'OPSWAT appropriée.

Empreintes numériques de l'URL de l'agent

Entrez la liste des empreintes numériques de l'URL de l'agent. Si vous ne fournissez pas de liste d'empreintes numériques, assurez-vous que les certificats de serveur sont 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.

Certificats approuvés

Si le certificat du serveur de l'URL de l'agent n'est pas émis par une autorité de certification publique approuvée, vous pouvez spécifier ce certificat (au format PEM) pour qu'il soit approuvé par Unified Access Gateway lors de la communication avec l'URL de l'agent pour le téléchargement de l'agent OPSWAT. Il s'agit d'une alternative aux empreintes numériques de l'URL de l'agent.

Pour sélectionner un certificat au format PEM et l'ajouter au magasin d'approbations, cliquez sur le signe **+**. Pour supprimer un certificat du magasin d'approbations, cliquez sur le signe **-**. Par défaut, le nom d'alias est le nom de fichier du certificat PEM. Pour fournir un nom différent, modifiez la zone de texte de l'alias.

Intervalle d'actualisation du fichier d'agent (secondes)

Intervalle, en secondes, auquel le fichier exécutable de l'on-demand agent est extrait de l'URL spécifiée dans la zone de texte **URL du fichier d'agent**.

c Cliquez sur **Enregistrer**.

- Pour la plate-forme macOS, suivez les étapes décrites ci-dessous.
  a Sélectionnez le **Type de chargement de fichier**.

    Si vous ne souhaitez charger aucun fichier, sélectionnez `None`.

  b En fonction du type de chargement de fichier sélectionné, entrez les informations requises pour le chargement de l'on-demand agent sur Unified Access Gateway.

Option	Procédure
Local	1 Sélectionnez le fichier exécutable de l'on-demand agent que vous avez téléchargé à partir d'OPSWAT. 2 Entrez les informations supplémentaires suivantes pour l'on-demand agent : **Nom** et **Paramètres**. 3 Dans la zone de texte **Chemin d'accès à l'exécutable**, entrez l'emplacement du fichier exécutable de l'on-demand agent.
Référence d'URL	1 Dans **URL du fichier d'agent**, entrez l'URL de l'emplacement du serveur de fichiers à partir duquel Unified Access Gateway peut télécharger l'on-demand agent. 2 Entrez les informations supplémentaires suivantes pour l'agent : **Nom**, **Paramètres**, **Empreintes numériques de l'URL de l'agent**, **Certificats approuvés** et **Intervalle d'actualisation du fichier d'agent (secondes)** 3 Dans la zone de texte **Chemin d'accès à l'exécutable**, entrez l'emplacement du fichier exécutable de l'on-demand agent.

  Les informations suivantes ont pour but de vous aider à comprendre les paramètres fournis pour le chargement de l'on-demand agent sur Unified Access Gateway :

Nom

Nom du fichier exécutable de l'on-demand agent.

Paramètres

Paramètres de ligne de commande utilisés par Horizon Client pour exécuter l'on-demand agent sur le point de terminaison.

Pour les paramètres de ligne de commande qui peuvent être utilisés dans la zone de texte **Paramètres**, reportez-vous à la documentation d'OPSWAT appropriée.

Empreintes numériques de l'URL de l'agent

Entrez la liste des empreintes numériques de l'URL de l'agent. Si vous ne fournissez pas de liste d'empreintes numériques, assurez-vous que les certificats de serveur sont 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.

Certificats approuvés

Si le certificat du serveur de l'URL de l'agent n'est pas émis par une autorité de certification publique approuvée, vous pouvez spécifier ce certificat (au format PEM) pour qu'il soit approuvé par Unified Access Gateway lors de la communication avec l'URL de l'agent pour le téléchargement de l'agent OPSWAT. Il s'agit d'une alternative aux empreintes numériques de l'URL de l'agent.

Pour sélectionner un certificat au format PEM et l'ajouter au magasin d'approbations, cliquez sur le signe **+**. Pour supprimer un certificat du magasin d'approbations, cliquez sur le signe **-**. Par défaut, le nom d'alias est le nom de fichier du certificat PEM. Pour fournir un nom différent, modifiez la zone de texte de l'alias.

Intervalle d'actualisation du fichier d'agent

Intervalle, en secondes, auquel le fichier exécutable de l'on-demand agent est extrait de l'URL spécifiée dans la zone de texte **URL du fichier d'agent**.

Chemin d'accès à l'exécutable

Emplacement du fichier exécutable de l'on-demand agent.

Pour les points de terminaison macOS, le fichier de l'on-demand agent est compressé dans un fichier zip. Le fichier exécutable se trouve dans le fichier zip. Horizon Client décompresse le fichier et exécute ce fichier exécutable sur le point de terminaison à partir de l'emplacement indiqué dans cette zone de texte.

c Cliquez sur **Enregistrer**.

Étape suivante

Pour terminer l'ensemble de tâches suivant, reportez-vous à la section Configurer les paramètres du fournisseur de vérification de la conformité du point de terminaison pour Horizon.

À propos d'OPSWAT MetaAccess on-demand agent

OPSWAT MetaAccess on-demand agent est un client OPSWAT. Cet agent peut être utilisé plutôt que d'exécuter OPSWAT MetaAccess persistent agent, qui s'exécute en continu sur un point de terminaison lorsqu'il est installé sur celui-ci. Par conséquent, on-demand agent offre la possibilité d'exécuter l'agent uniquement lorsque cela est nécessaire.

OPSWAT MetaAccess dispose de deux types de clients : on-demand agent et persistent agent.

persistent agent est installé par l'utilisateur sur chaque point de terminaison et s'exécute en continu sur celui-ci après l'installation.

Quant à on-demand agent, suite à l'authentification réussie de l'utilisateur, il est automatiquement téléchargé depuis Unified Access Gateway et exécuté par Horizon Client.

Note Le téléchargement se produit uniquement si Horizon Client ne dispose pas de la même version d'on-demand agent que celle qui se trouve sur Unified Access Gateway.

Les administrateurs peuvent charger les fichiers exécutables d'on-demand agent pour Windows et macOS sur Unified Access Gateway.

Pour charger l'agent sur Unified Access Gateway, reportez-vous à la section Charger le logiciel de l'OPSWAT MetaAccess on-demand agent sur Unified Access Gateway.

Pour plus d'informations sur persistent agent et lon-demand agent, consultez la documentation pertinente relative à OPSWAT.

Intervalle de vérification périodique de conformité du point de terminaison

Les administrateurs peuvent configurer des intervalles de vérification périodique de la conformité d'un point de terminaison au cours d'une session utilisateur authentifiée. La vérification périodique de la conformité garantit que le périphérique reste conforme pendant toute la session. Les intervalles peuvent être configurés sur la page **Paramètres du fournisseur de vérification de la conformité du point de terminaison**.

Unified Access Gateway effectue des vérifications de conformité sur un point de terminaison lorsqu'un utilisateur tente de lancer une session d'application ou de poste de travail distant à l'aide de Horizon Client sur ce point de terminaison. Si les intervalles sont configurés, la conformité des points de terminaison est vérifiée régulièrement, à ces intervalles.

Après la vérification de conformité initiale, au cours de la session, un point de terminaison peut devenir non conforme pour plusieurs raisons, par exemple en raison de la modification d'une stratégie par les administrateurs. Dans certains cas, les points de terminaison peuvent nécessiter un accès pour lancer une session, bien que l'évaluation de leur conformité soit en attente. Pour s'assurer que seuls les points de terminaison conformes accèdent à l'application ou au poste de travail distant au cours d'une session, les administrateurs peuvent configurer les intervalles de vérification de la conformité via deux options : **Intervalle de vérification de la conformité (minutes)** et **Intervalle rapide de vérification de la conformité (minutes)**.

Lorsque l'**Intervalle rapide de vérification de la conformité (minutes)** est également configuré, Unified Access Gateway exécute d'abord l'**Intervalle rapide de vérification de la conformité (minutes)**. Lorsque le point de terminaison devient conforme, Unified Access Gateway exécute ensuite l'**Intervalle de vérification de conformité (minutes)**.

Lors de la vérification périodique de la conformité, si un point de terminaison n'est pas conforme, Horizon Client met fin à la session utilisateur sur ce périphérique.

Intervalle de vérification de la conformité (minutes)

Cette zone de texte vous permet de configurer un intervalle périodique auquel Horizon Client envoie des demandes de vérification de conformité à Unified Access Gateway au cours d'une session.

Intervalle rapide de vérification de la conformité (minutes)

Cette zone de texte vous permet de configurer un intervalle périodique plus fréquent auquel Horizon Client envoie des demandes de vérification de conformité à Unified Access Gateway au cours d'une session pour un point de terminaison se trouvant dans des états spécifiques, autres que `In compliance`. Les états sont `Device not found`, `Assessment pending` et `Endpoint unknown`. Ils doivent tous être configurés avec `ALLOW`.

Par exemple, lorsque l'on-demand agent évalue un point de terminaison et que l'état du périphérique est `Assessment pending` ou `Endpoint unknown`, vous pouvez définir l'intervalle sur `1 minute` afin que les vérifications de conformité soient plus fréquentes au début d'une session.

Important L'option **Intervalle rapide de vérification de vérification de la conformité (minutes)** peut être uniquement configurée lorsque l'option **Intervalle de vérification de la conformité (minutes)** l'est également et qu'elle n'est pas définie sur `0`.

Pour configurer les intervalles, reportez-vous à la section Configurer les paramètres du fournisseur de vérification de la conformité du point de terminaison pour Horizon.

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 zone DMZ.

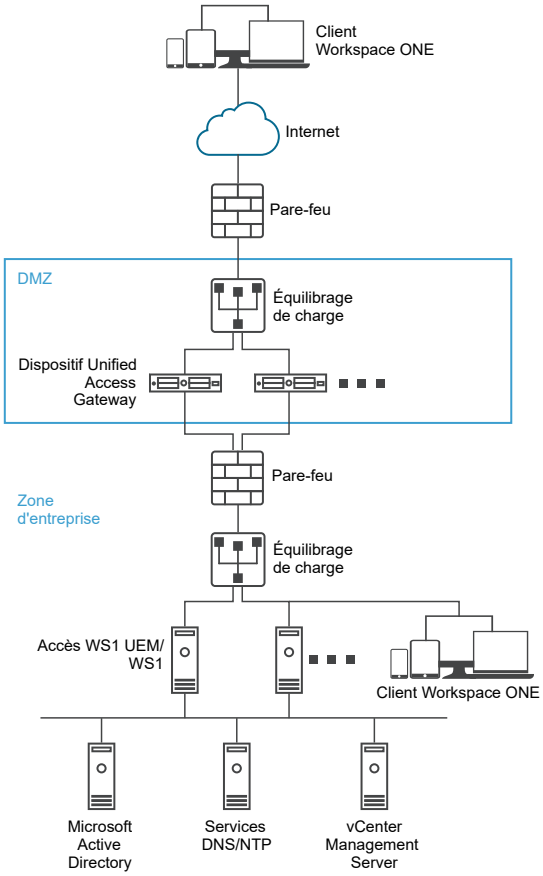
Scénario de déploiement

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

Note Une seule instance de Unified Access Gateway peut gérer jusqu'à 15 000 connexions TCP simultanées. Si la charge attendue est supérieure à 15 000, plusieurs instances de Unified Access Gateway doivent être configurées derrière l'équilibrage de charge.

Reportez-vous à la section Paramètres avancés des services Edge pour plus d'informations sur les paramètres utilisés lors de la configuration du proxy inverse.

Figure 4-5. Dispositif Unified Access Gateway pointant vers VMware Identity Manager



Comprendre le proxy inverse

Unified Access Gateway fournit aux utilisateurs distants un accès au portail d'applications pour leur permettre de s'authentifier et d'accéder à leurs ressources. Le portail d'applications est une application principale comme SharePoint, JIRA ou VIDM, pour lequel Unified Access Gateway agit en tant que proxy inverse.

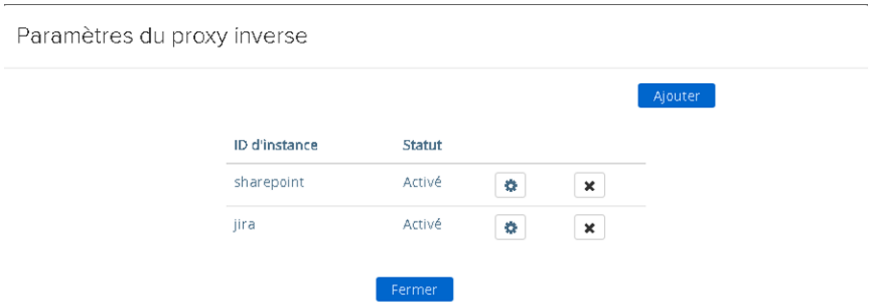
Note Horizon Connection Server ne fonctionne pas avec un proxy inverse Web activé lorsqu'un chevauchement existe dans le modèle de proxy. Par conséquent, si Horizon et une instance du proxy inverse Web sont configurés et activés avec des modèles de proxy sur la même instance Unified Access Gateway, supprimez le modèle de proxy « / » des paramètres d'Horizon et conservez le modèle dans le proxy inverse Web afin d'empêcher le chevauchement. Conserver le modèle de proxy « / » dans l'instance du proxy inverse Web permet de garantir que lorsqu'un utilisateur clique sur l'URL d'Unified Access Gateway, la page appropriée du proxy inverse Web s'affiche. Si seuls les paramètres d'Horizon sont configurés, le changement ci-dessus n'est pas nécessaire.

Tenez compte des points suivants lors de l'activation et de la configuration du proxy inverse :

- Vous devez activer l'authentification du proxy inverse sur un gestionnaire des services Edge. Actuellement, les méthodes d'authentification RSA SecurID et RADIUS sont prises en charge.

- Vous devez générer les métadonnées de fournisseur d'identité (métadonnées IDP) avant d'activer l'authentification sur le proxy inverse Web.
- Unified Access Gateway fournit un accès distant à Workspace ONE Access et aux applications Web avec ou sans authentification à partir d'un client basé sur un navigateur, puis lance un poste de travail Horizon.
- Vous pouvez configurer plusieurs instances du proxy inverse, chacune d'elles peut en outre être supprimée.
- Les modèles de proxy simples sont sensibles à la casse. Les liens de page et les modèles de proxy doivent correspondre.

Figure 4-6. Plusieurs proxys inverses configurés



Configurer le proxy inverse avec Workspace ONE Access

Vous pouvez configurer le service de proxy inverse Web pour utiliser Unified Access Gateway avec Workspace ONE Access.

Conditions préalables

Notez les exigences suivantes pour le déploiement avec Workspace ONE Access :

- DNS fractionné. En externe, le nom d'hôte doit être résolu sur l'adresse IP d'Unified Access Gateway. En interne, sur Unified Access Gateway, le même nom d'hôte doit être résolu sur le serveur Web réel par le biais d'un mappage DNS interne ou d'une entrée de nom d'hôte sur Unified Access Gateway.

  Note Si vous déployez uniquement avec le proxy inverse Web, il n'est pas nécessaire de configurer le pontage d'identité.

- Le service Workspace ONE Access 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.
- La combinaison de modèle de proxy et de modèle d'hôte de proxy pour une instance du proxy inverse Web doit être unique s'il existe une configuration de proxys inverses multiples dans une instance de Unified Access Gateway.

- Les noms d'hôte de tous les proxys inverses configurés doivent être résolus sur la même adresse IP de l'instance de Unified Access Gateway.
- Reportez-vous à la section Paramètres avancés des services Edge pour plus d'informations sur les paramètres avancés des services Edge.

Procédure

1. Dans la section Configuration manuelle de l'interface utilisateur d'administration, cliquez sur **Sélectionner**.
2. Dans **Paramètres généraux > Paramètres des services 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, qui est généralement l'URL du serveur principal. Par exemple, pour Workspace ONE Access, ajoutez l'adresse IP, le nom d'hôte Workspace ONE Access et le DNS externe sur la machine cliente. Dans l'interface utilisateur d'administration, ajoutez l'adresse IP, le nom d'hôte Workspace ONE Access et le DNS interne.
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 spécifiez *****, n'importe quel certificat sera accepté. 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 **`(/|/SAAS(.*)|/hc(.*)|/web(.*)|/catalog-portal(.*))`**. **Note** 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. Les méthodes d'authentification par certificat de périphérique, RSA SecurID et RADIUS sont prises en charge.
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	Requis lorsque vous configurez Unified Access Gateway en tant que proxy inverse authentifié pour Workspace ONE Access. 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.
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 `https://<host:port>`.
Modèle non sécurisé	Entrez le modèle de redirection Workspace ONE Access connu. Par exemple : `(/|/catalog-portal(.*)|/|/SAAS/|/SAAS|/SAAS/API/1.0/GET/image(.*)|/SAAS/horizon/css(.*)|/SAAS/horizon/angular(.*)|/SAAS/horizon/js(.*)|/SAAS/horizon/js-lib(.*)|/SAAS/auth/login(.*)|/SAAS/jersey/manager/api/branding|/SAAS/horizon/images/(.*)|/SAAS/jersey/manager/api/images/(.*)|/hc/(.*)/authenticate/(.*)|/hc/static/(.*)|/SAAS/auth/saml/response|/SAAS/auth/authenticatedUserDispatcher|/web(.*)|/SAAS/apps/|/SAAS/horizon/portal/(.*)|/SAAS/horizon/fonts(.*)|/SAAS/API/1.0/POST/sso(.*)|/SAAS/API/1.0/REST/system/info(.*)|/SAAS/API/1.0/REST/auth/cert(.*)|/SAAS/API/1.0/REST/oauth2/activate(.*)|/SAAS/API/1.0/GET/user/devices/register(.*)|/SAAS/API/1.0/oauth2/token(.*)|/SAAS/API/1.0/REST/oauth2/session(.*)|/SAAS/API/1.0/REST/user/resources(.*)|/hc/t/(.*)/(.*)/authenticate(.*)|/SAAS/API/1.0/REST/auth/logout(.*)|/SAAS/auth/saml/response(.*)|/SAAS/(.*)/(.*)auth/login(.*)|/SAAS/API/1.0/GET/apps/launch(.*)|/SAAS/API/1.0/REST/user/applications(.*)|/SAAS/auth/federation/sso(.*)|/SAAS/auth/oauth2/authorize(.*)|/hc/prepareSaml/failure(.*)|/SAAS/auth/oauthtoken(.*)|/SAAS/API/1.0/GET/metadata/idp.xml|/SAAS/auth/saml/artifact/resolve(.*)|/hc/(.*)/authAdapter(.*)|/hc/authenticate/(.*)|/SAAS/auth/logout|/SAAS/common.js|/SAAS/auth/launchInput(.*)|/SAAS/launchUsersApplication.do(.*)|/hc/API/1.0/REST/thinapp/download(.*)|/hc/t/(.*)/(.*)/logout(.*)|/SAAS/auth/wsfed/services(.*)|/SAAS/auth/wsfed/active/logon(.*))`
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**

Option	Description
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.
Certificats approuvés	Ajoutez un certificat approuvé à ce service Edge. Cliquez sur le signe « + » pour sélectionner un certificat au format PEM et l'ajouter au magasin des approbations. Cliquez sur '-' pour supprimer un certificat du magasin de confiance. Par défaut, le nom d'alias est le nom de fichier du certificat PEM. Modifiez la zone de texte de l'alias afin de donner un nom différent à l'alias.
En-têtes de sécurité de réponse	Cliquez sur « + » pour ajouter un en-tête. Entrez le nom de l'en-tête de sécurité. Entrez la valeur. Cliquez sur « - » pour supprimer un en-tête. Modifiez un en-tête de sécurité existant pour mettre à jour le nom et la valeur de l'en-tête. **Important** Les noms et valeurs d'en-têtes ne sont enregistrés qu'après avoir cliqué sur **Enregistrer**. Certains en-têtes de sécurité standard sont présents par défaut. Les en-têtes configurés sont ajoutés à la réponse d'Unified Access Gateway au client uniquement si les en-têtes correspondants sont absents dans la réponse du serveur principal configuré. **Note** Modifiez les en-têtes de réponse de sécurité avec précaution. La modification de ces paramètres risque d'affecter le fonctionnement sécurisé d'Unified Access Gateway.
Entrées de l'hôte	Entrez les détails qui doivent être ajoutés 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`**. pour ajouter plusieurs entrées de l'hôte, cliquez sur le signe « + ». **Important** Les entrées de l'hôte sont enregistrées uniquement après avoir cliqué sur **Enregistrer**.

Note Les options `UnSecure Pattern`, `Auth Cookie` et `Login Redirect URL` sont applicables uniquement avec Workspace ONE Access. Les valeurs fournies ici s'appliquent également à Access Point 2.8 et Unified Access Gateway 2.9.

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

8 Cliquez sur **Enregistrer**.

Étape suivante

Pour activer le pontage d'identité, consultez Configuration des paramètres du pontage d'identité.

Configurer le proxy inverse avec l'API VMware Workspace ONE UEM

Lors de l'utilisation d'installations sur site de Workspace ONE UEM, le serveur API est généralement installé derrière un pare-feu sans accès Internet entrant. Pour utiliser de manière

sécurisée les capacités d'automatisation de Workspace ONE Intelligence, vous pouvez configurer un service Edge de proxy inverse Web dans le dispositif Unified Access Gateway pour autoriser l'accès uniquement au service d'API, afin que des actions puissent être effectuées au niveau des périphériques, des utilisateurs et d'autres ressources.

Conditions préalables

- Le service API UEM doit avoir un nom de domaine complet (FQDN) comme nom d'hôte.
- Unified Access Gateway doit utiliser le DNS interne. Cela signifie que l'URL de destination du proxy doit utiliser un FQDN.
- La combinaison de modèle de proxy et de modèle d'hôte de proxy pour une instance du proxy inverse Web doit être unique s'il existe une configuration de proxys inverses multiples dans une instance d'Unified Access Gateway.
- Les noms d'hôte de tous les proxys inverses configurés doivent être résolus sur la même adresse IP de l'instance d'Unified Access Gateway.
- Pour plus d'informations sur les paramètres avancés des services Edge, consultez la section Paramètres avancés des services Edge.

Procédure

1. Dans la section Configuration manuelle de l'interface utilisateur d'administration, cliquez sur **Sélectionner**.
2. Dans **Paramètres généraux > 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, qui est généralement l'URL du serveur principal. Par exemple, pour le serveur API Workspace ONE UEM, il peut s'agir d'une URL ou d'une adresse IP différente de votre connexion à la console. Vous pouvez le vérifier en consultant les pages des paramètres UEM sous **Paramètres > Système > Avancé > API > REST API > URL de REST API** .

Option	Description
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 spécifiez *****, n'importe quel certificat sera accepté. 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. Pour l'API Workspace ONE UEM, utilisez : `(/API(.*)|/api(.*)|/Api(.*)|).` **Note** 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. Les méthodes d'authentification par certificat de périphérique, RSA SecurID et RADIUS sont prises en charge.
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 `https://<host:port>`. **Note** Lors de l'utilisation d'Unified Access Gateway derrière un équilibrage de charge, entrez l'URL de l'équilibrage de charge dans ce champ.
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.

Option	Description
Certificats approuvés	Ajoutez un certificat approuvé à ce service Edge. Cliquez sur le signe « + » pour sélectionner un certificat au format PEM et l'ajouter au magasin des approbations. Cliquez sur '-' pour supprimer un certificat du magasin de confiance. Par défaut, le nom d'alias est le nom de fichier du certificat PEM. Modifiez la zone de texte de l'alias afin de fournir un nom différent à l'alias.
Entrées de l'hôte	Entrez les détails qui doivent être ajoutés 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`**. pour ajouter plusieurs entrées de l'hôte, cliquez sur le signe « + ». **Important** Les entrées de l'hôte sont enregistrées uniquement après avoir cliqué sur **Enregistrer**.

8 Cliquez sur **Enregistrer**.

Étape suivante

Pour configurer Workspace UEM API Connector à utiliser avec Workspace ONE Intelligence, reportez-vous à la rubrique *Démarrage avec des automatisations* de la documentation de *Workspace ONE Intelligence*. Utilisez l'URL externe configurée pour votre instance d'Unified Access Gateway au lieu de l'URL du serveur UEM REST API interne.

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

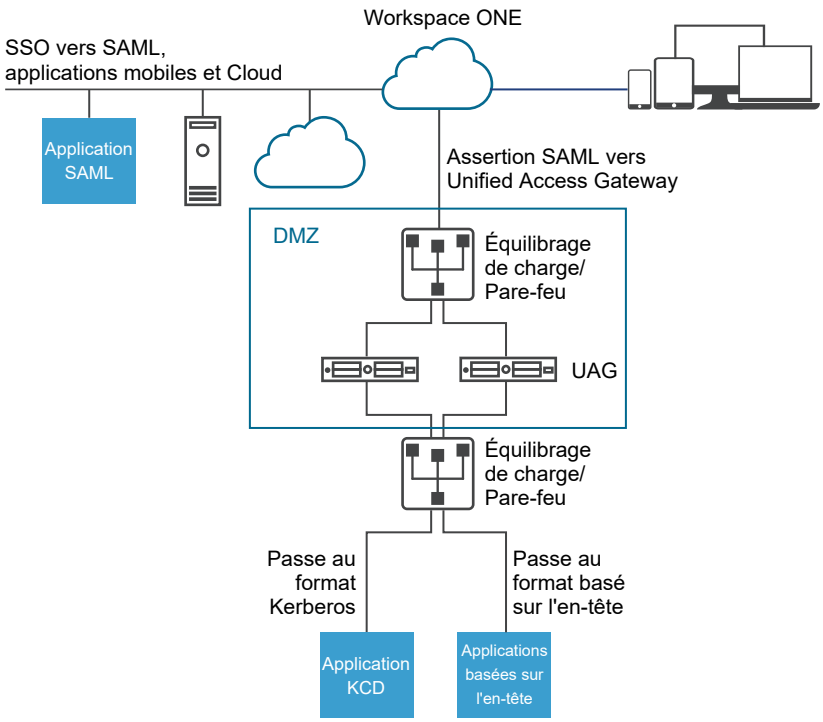
La fonctionnalité de pontage d'identité d'Unified Access Gateway peut être configurée pour fournir l'authentification unique (SSO) à des applications Web héritées qui utilisent la délégation Kerberos contrainte (KCD) ou l'authentification basée sur l'en-tête.

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. Workspace ONE Access 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, Workspace ONE Access 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.

Note Horizon Connection Server ne fonctionne pas avec un proxy inverse Web activé lorsqu'un chevauchement existe dans le modèle de proxy. Par conséquent, si Horizon et une instance du proxy inverse Web sont configurés et activés avec des modèles de proxy sur la même instance Unified Access Gateway, supprimez le modèle de proxy « / » des paramètres d'Horizon et conservez le modèle dans le proxy inverse Web afin d'empêcher le chevauchement. Conserver le modèle de proxy « / » dans l'instance du proxy inverse Web permet de garantir que lorsqu'un utilisateur clique sur l'URL d'Unified Access Gateway, la page appropriée du proxy inverse Web s'affiche. Si seuls les paramètres d'Horizon sont configurés, le changement ci-dessus n'est pas nécessaire.

Figure 4-7. 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.

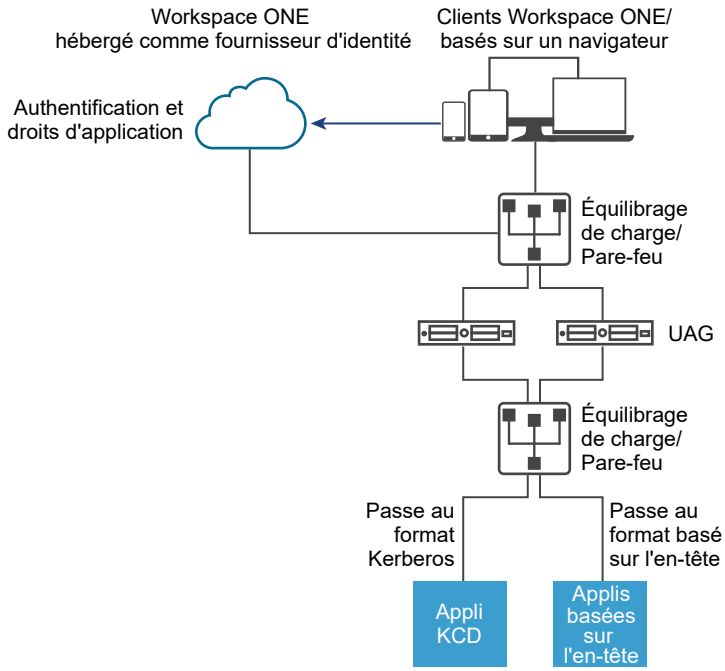
Si l'utilisateur est validé, le fournisseur d'identité crée un jeton SAML et l'envoie à l'utilisateur. L'utilisateur transmet le jeton SAML à Unified Access Gateway dans la zone DMZ. Unified Access Gateway valide le jeton SAML et récupère le nom principal de l'utilisateur à partir du jeton.

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 4-8. 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.

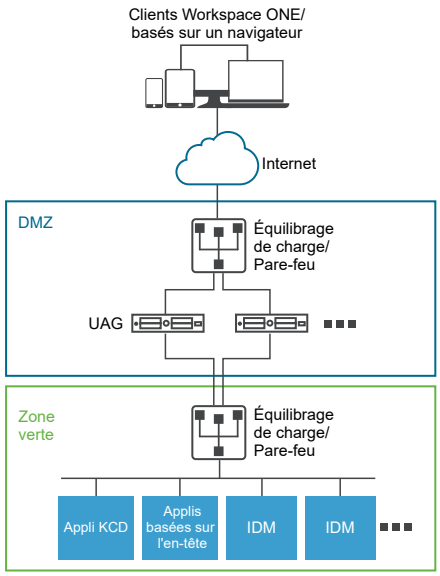
L'utilisateur transmet le jeton SAML à Unified Access Gateway. Unified Access Gateway valide le jeton SAML et récupère le nom principal de l'utilisateur à partir du jeton.

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 4-9. Pontage d'identité d'Unified Access Gateway sur site



Utilisation du pontage d'identité avec Certificat sur Kerberos

Vous pouvez configurer le pontage d'identité pour fournir l'authentification unique aux applications non-SAML héritées sur site à l'aide de la validation du certificat. Reportez-vous à la section Configurer un proxy inverse Web pour le pontage d'identité (certificat sur Kerberos).

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, téléchargez les métadonnées du fournisseur d'identité, ainsi que le fichier keytab et configurez les paramètres de domaine KCD.

Note Cette version de pontage d'identité prend en charge la fonction inter-domaines avec une configuration de domaine unique. Ainsi, l'utilisateur et le compte SPN peuvent utiliser différents domaines.

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.
- Assurez-vous que les ports suivants sont ouverts :
  - Le port 443 pour les demandes HTTP entrantes
  - Le port TCP/UDP 88 pour la communication Kerberos avec Active Directory
  - Unified Access Gateway utilise TCP pour communiquer avec les applications principales. Le port approprié sur lequel le serveur principal est à l'écoute, par exemple, le port TCP 8080.

Note

- La configuration du pontage d'identité pour SAML et Certificat sur Kerberos pour deux instances différentes de proxys inverses sur la même instance d'Unified Access Gateway n'est pas prise en charge.
- Les instances de proxys inverses Web avec autorité de certification et sans authentification basée sur le certificat, dont le pontage d'identité n'est pas activé sur le même dispositif, ne sont pas prises en charge.

Authentification basée sur l'en-tête à l'aide de SAML

Les réponses SAML du fournisseur d'identité au fournisseur de services (en cas de pontage d'identité, Unified Access Gateway) contiennent des assertions SAML, qui comprennent des

attributs SAML. Les attributs SAML sont configurables dans le fournisseur d'identité pour pointer vers différents paramètres, tels que le nom d'utilisateur, l'e-mail, etc.

Dans l'authentification basée sur l'en-tête à l'aide de SAML, la valeur d'un attribut SAML peut être envoyée en tant qu'en-tête HTTP vers la destination par proxy du serveur principal. Le nom d'attribut SAML défini dans Unified Access Gateway est le même que celui dans le fournisseur d'identité. Par exemple, si l'attribut d'un fournisseur d'identité est défini en tant que `Name: userNameValue: idmadmin`, le nom d'attribut SAML dans Unified Access Gateway doit être défini en tant que `"userName"`.

L'attribut SAML qui ne correspond pas à l'attribut défini dans le fournisseur d'identité est ignoré. Unified Access Gateway prend en charge à la fois plusieurs attributs SAML et des attributs SAML à plusieurs valeurs. Les exemples d'extraits de l'assertion SAML prévue d'un fournisseur d'identité sont mentionnés dans les propositions suivantes pour chaque cas. Par exemple,

1. Réponse SAML prévue du fournisseur d'identité pour plusieurs attributs SAML

```
<saml:AttributeStatement>
      <saml:Attribute Name="userName" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:basic">
                   <saml:AttributeValue xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xsd:string">idmadmin</
saml:AttributeValue>
      </saml:Attribute>
      <saml:Attribute Name="userEmail" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:basic">
                  <saml:AttributeValue xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xsd:string">63ecfabf-
a577-46c3-b4fa-caf7ae49a6a3</saml:AttributeValue>
      </saml:Attribute>
</saml:AttributeStatement>
```

Dans l'exemple précédent, une assertion contient deux attributs, `"userName"` et `"userEmail"`. Si l'authentification basée sur l'en-tête est configurée uniquement pour `"userName"`, avec le nom d'en-tête étant `"HTTP_USER_NAME"`, l'en-tête est envoyé en tant que : `"HTTP_USER_NAME: idmadmin"`. Étant donné que `"userEmail"` n'est pas configuré sur Unified Access Gateway pour l'authentification basée sur l'en-tête, il n'est pas envoyé en tant qu'en-tête.

2. Réponse SAML prévue du fournisseur d'identité pour l'attribut SAML à plusieurs valeurs

```
<saml:AttributeStatement>
      <saml:Attribute Name="group" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:basic">
             <saml:AttributeValue xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xsd:string">All Employees</
saml:AttributeValue>
             <saml:AttributeValue xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xsd:string">All Contractors</
saml:AttributeValue>
             <saml:AttributeValue xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xsd:string">All Executives</
saml:AttributeValue>
```

```
            <saml:AttributeValue xmlns:xsd="http://www.w3.org/2001/
XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xsd:string">All</
saml:AttributeValue>
     </saml:Attribute>
</saml:AttributeStatement>
```

Dans l'exemple précédent, un attribut `"group"` contient quatre valeurs, à savoir `"All Employees"`, `"All Contractors"`, `"All Executives"` et `"All"`. Si l'authentification basée sur l'en-tête est configurée uniquement pour `"group"`, avec le nom d'en-tête étant `"HTTP_GROUP"`, l'en-tête est envoyé en tant que `"HTTP_GROUP: All Employees, All Contractors, All Executives, All"` avec une liste séparée par des virgules de toutes les valeurs d'attributs en tant que valeur d'en-tête.

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 de Unified Access Gateway version 3.0, vous pouvez supprimer les domaines définis auparavant.

Important En cas de configuration entre domaines, ajoutez les détails de tous les domaines en incluant les sous-domaines principal et secondaire et les informations du KDC associé. Assurez-vous que le niveau de confiance est activé entre les domaines.

Conditions préalables

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**.

4 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.

5 Cliquez sur **Enregistrer**.

Étape suivante

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.

Note 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.

Vous pouvez également générer le fichier keytab à l'aide de la ligne de commande. Par exemple :

```
ktpass /princ HOST/nom_utilisateur@domaine.com /ptype KRB5_NT_PRINCIPAL /pass * /out
C:\Temp\kerberos.keytab /mapuser uagkerberos /crypto All
```

Consultez la documentation de Microsoft pour obtenir des informations détaillées sur la commande `ktpass`.

Conditions préalables

Vous devez avoir accès au fichier keytab Kerberos pour le 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

1. Dans la section Modèles de configuration du dispositif de gestion, cliquez sur **Ajouter**.
2. Dans la section Pramètres de pontage d'identité, cliquez sur **Configurer**.
3. Sur la page Paramètres du fichier KeyTab Kerberos, cliquez sur Ajouter **Nouveau fichier KeyTab**.
4. Entrez un nom unique comme identifiant.
5. (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.

   Assurez-vous 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 de keytab échoue.
6. Dans la zone de texte **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.
7. Cliquez sur **Enregistrer**.

Configuration d'un proxy inverse Web pour le pontage d'identité (SAML sur Kerberos)

Pour configurer un proxy inverse Web pour le pontage d'identité (SAML sur Kerberos), vous devez avoir enregistré le fichier de métadonnées du fournisseur d'identité dans Unified Access Gateway.

Vous pouvez ensuite activer le pontage d'identité sur la console d'administration et configurer le nom d'hôte externe pour le service.

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.

Conditions préalables

Le fichier XML de métadonnées SAML doit être enregistré sur un ordinateur auquel vous avez accès.

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

Procédure

1. Dans la console d'administration, cliquez sur **Sélectionner** sous **Configurer manuellement**.
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**.

Étape suivante

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 un proxy inverse Web pour le pontage d'identité (SAML sur Kerberos)

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 Workspace ONE Access.

Conditions préalables

Vous devez avoir configuré les paramètres du pontage d'identité suivants sur la console d'administration d'Unified Access Gateway. Vous trouvez ces paramètres dans la section **Paramètres avancés**.

- 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.

Assurez-vous que le port TCP/UDP 88 est ouvert car Unified Access Gateway l'utilise pour la communication Kerberos avec Active Directory.

Procédure

1. Dans la section **Configurer manuellement** de l'interface utilisateur d'administration, cliquez sur **Sélectionner**.

2 Dans la ligne **Paramètres généraux > 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 Définissez **Activer les paramètres du proxy inverse** sur OUI et configurez les paramètres suivants du service Edge.

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	Entrez les chemins d'URI correspondants qui assurent la transmission à l'URL de destination. Par exemple, entrez **`(/|/SAAS(.*)|/hc(.*)|/web(.*)|/catalog-portal(.*))`**. Remarque : lorsque vous configurez plusieurs proxys inverses, fournissez le nom d'hôte dans le modèle d'hôte de proxy.

6 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. Les méthodes d'authentification par certificat de périphérique, RSA SecurID et RADIUS sont prises en charge.
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	Requis lorsque vous configurez Unified Access Gateway en tant que proxy inverse authentifié pour Workspace ONE Access. 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.
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 `https://<host:port>`.

Option	Description
Modèle non sécurisé	Entrez le modèle de redirection Workspace ONE Access connu. Par exemple : `(/|/catalog-portal(.*)|/|/SAAS/|/SAAS|/SAAS/API/1.0/GET/image(.*)|/SAAS/horizon/css(.*)|/SAAS/horizon/angular(.*)|/SAAS/horizon/js(.*)|/SAAS/horizon/js-lib(.*)|/SAAS/auth/login(.*)|/SAAS/jersey/manager/api/branding|/SAAS/horizon/images/(.*)|/SAAS/jersey/manager/api/images/(.*)|/hc/(.*)/authenticate/(.*)|/hc/static/(.*)|/SAAS/auth/saml/response|/SAAS/auth/authenticatedUserDispatcher|/web(.*)|/SAAS/apps/|/SAAS/horizon/portal/(.*)|/SAAS/horizon/fonts(.*)|/SAAS/API/1.0/POST/sso(.*)|/SAAS/API/1.0/REST/system/info(.*)|/SAAS/API/1.0/REST/auth/cert(.*)|/SAAS/API/1.0/REST/oauth2/activate(.*)|/SAAS/API/1.0/GET/user/devices/register(.*)|/SAAS/API/1.0/oauth2/token(.*)|/SAAS/API/1.0/REST/oauth2/session(.*)|/SAAS/API/1.0/REST/user/resources(.*)|/hc/t/(.*)/(.*)/authenticate(.*)|/SAAS/API/1.0/REST/auth/logout(.*)|/SAAS/auth/saml/response(.*)|/SAAS/(.*)/(.*)auth/login(.*)|/SAAS/API/1.0/GET/apps/launch(.*)|/SAAS/API/1.0/REST/user/applications(.*)|/SAAS/auth/federation/sso(.*)|/SAAS/auth/oauth2/authorize(.*)|/hc/prepareSaml/failure(.*)|/SAAS/auth/oauthtoken(.*)|/SAAS/API/1.0/GET/metadata/idp.xml|/SAAS/auth/saml/artifact/resolve(.*)|/hc/(.*)/authAdapter(.*)|/hc/authenticate/(.*)|/SAAS/auth/logout|/SAAS/common.js|/SAAS/auth/launchInput(.*)|/SAAS/launchUsersApplication.do(.*)|/hc/API/1.0/REST/thinapp/download(.*)|/hc/t/(.*)/(.*)/logout(.*)|/SAAS/auth/wsfed/services(.*)|/SAAS/auth/wsfed/active/logon(.*))`
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.
Certificats approuvés	Ajoutez un certificat approuvé à ce service Edge. Cliquez sur le signe « + » pour sélectionner un certificat au format PEM et l'ajouter au magasin des approbations. Cliquez sur '-' pour supprimer un certificat du magasin de confiance. Par défaut, le nom d'alias est le nom de fichier du certificat PEM. Modifiez la zone de texte de l'alias afin de donner un nom différent à l'alias.

Option	Description
En-têtes de sécurité de réponse	Cliquez sur « + » pour ajouter un en-tête. Entrez le nom de l'en-tête de sécurité. Entrez la valeur. Cliquez sur « - » pour supprimer un en-tête. Modifiez un en-tête de sécurité existant pour mettre à jour le nom et la valeur de l'en-tête. **Important** Les noms et valeurs d'en-têtes ne sont enregistrés qu'après avoir cliqué sur **Enregistrer**. Certains en-têtes de sécurité standard sont présents par défaut. Les en-têtes configurés sont ajoutés à la réponse d'Unified Access Gateway au client uniquement si les en-têtes correspondants sont absents dans la réponse du serveur principal configuré. **Note** Modifiez les en-têtes de réponse de sécurité avec précaution. La modification de ces paramètres risque d'affecter le fonctionnement sécurisé d'Unified Access Gateway.
Entrées de l'hôte	Entrez les détails qui doivent être ajoutés 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`**. pour ajouter plusieurs entrées de l'hôte, cliquez sur le signe « + ». **Important** Les entrées de l'hôte sont enregistrées uniquement après avoir cliqué sur **Enregistrer**.

7 Dans la section Activer le pontage d'identité, remplacez **NON** par **OUI**.

8 Configurez les paramètres de pontage d'identité suivants.

Option	Description
Types d'authentification	Sélectionnez SAML.
Attributs SAML	Liste d'attributs SAML qui est transmise en tant qu'en-têtes de demandes. Cette option n'est visible que lorsque l'option **Activer le pontage d'identité** est définie sur **Oui** et que l'option **Types d'authentification** est définie sur **SAML**. Cliquez sur « + » en regard d'un attribut SAML dans le cadre de l'en-tête.
Publics SAML	Assurez-vous que le type d'authentification SAML est choisi. Entrez l'URL du public. **Note** Si la zone de texte reste vide, les publics ne sont pas restreints. Pour comprendre comment UAG prend en charge les publics SAML, consultez la section Publics SAML.
Fournisseur d'identité	Dans le menu déroulant, sélectionnez le fournisseur d'identité.
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.

Option	Description
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.

9 Dans la section Télécharger des métadonnées SP, cliquez sur **Télécharger**.

Enregistrez le fichier de métadonnées de fournisseur de services.

10 Cliquez sur **Enregistrer**.

Étape suivante

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 Workspace ONE Access.

Ajouter le fichier de métadonnées au service VMware Workspace ONE Access

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

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

Conditions préalables

Vous devez avoir enregistré le fichier de métadonnées de fournisseur de services d'Unified Access Gateway sur l'ordinateur.

Procédure

1 Connectez-vous à la console d'administration de Workspace ONE Access.

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**.

Étape suivante

Attribuez cette application à des utilisateurs et des groupes.

Note 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.

Configuration d'un proxy inverse Web pour le pontage d'identité (certificat sur Kerberos)

Configurez la console Workspace ONE UEM pour extraire et utiliser des certificats d'autorité de certification avant de configurer la fonctionnalité de pontage Unified Access Gateway afin de fournir l'authentification unique (SSO) aux applications non-SAML héritées sur site à l'aide de la validation du certificat.

Autoriser la console Workspace ONE UEM à extraire et utiliser des certificats d'autorité de certification

Vous pouvez ajouter un modèle utilisateur dans le serveur d'autorité de certification et configurer les paramètres de Workspace ONE UEM Console pour permettre à Workspace ONE UEM d'extraire et d'utiliser les certificats de l'autorité de certification.

Procédure

1 Ajouter un modèle utilisateur

Ajoutez un modèle utilisateur dans le serveur d'autorité de certification comme première étape pour permettre à Workspace ONE UEM d'extraire des certificats.

2 Ajouter une autorité de certification dans la console

Ajouter une autorité de certification (CA) dans la console Workspace ONE UEM.

3 Ajouter un modèle de demande d'autorité de certification

Ajoutez un modèle de demande d'autorité de certification après avoir ajouté une autorité de certification dans la console Workspace ONE UEM.

4 Mettre à jour des stratégies de sécurité pour utiliser le certificat d'autorité de certification extrait

Mettez à jour les stratégies de sécurité dans la console Workspace ONE UEM pour utiliser le certificat d'autorité de certification extrait.

Ajouter un modèle utilisateur

Ajoutez un modèle utilisateur dans le serveur d'autorité de certification comme première étape pour permettre à Workspace ONE UEM d'extraire des certificats.

Procédure

1 Connectez-vous au serveur sur lequel l'autorité de certification est configurée.

2 Cliquez sur **Démarrer** et tapez **`mmc.exe`**.

3 Dans la fenêtre **MMC**, accédez à **Fichier > Ajouter/Supprimer un composant logiciel enfichable**.

4 Dans la fenêtre **Ajouter ou supprimer des composants logiciels enfichables**, sélectionnez **Modèles de certificat** et cliquez sur **Ajouter**.

5 Cliquez sur **OK**.

6 Dans la fenêtre **Modèles de certificat**, faites défiler vers le bas et sélectionnez **Utilisateur > Dupliquer le modèle**.

7 Dans la fenêtre **Propriétés du nouveau modèle**, sélectionnez l'onglet **Général** et fournissez un nom pour le **Nom complet du modèle**.

Le **Nom du modèle** est automatiquement renseigné avec ce nom, sans espace.

8 Sélectionnez l'onglet **Nom de l'objet** et sélectionnez **Fournir dans la demande**.

9 Cliquez sur **Appliquer**, puis sur **OK**.

10 Dans la fenêtre **MMC**, accédez à **Fichier > Ajouter/Supprimer un composant logiciel enfichable**.

11 Dans la fenêtre **Ajouter ou supprimer des composants logiciels enfichables**, sélectionnez **Autorité de certification** et cliquez sur **Ajouter**.

12 Dans la fenêtre **MMC**, sélectionnez **Autorité de certification > Modèle de certificat**.

13 Cliquez avec le bouton droit sur **Autorité de certification** et sélectionnez **Nouveau > Modèle de certificat à délivrer**.

14 Sélectionnez le modèle que vous avez créé à l'étape 6.

Étape suivante

Vérifiez que le modèle que vous avez ajouté s'affiche dans la liste.

Connectez-vous à la console Workspace ONE UEM et ajoutez une autorité de certification.

Ajouter une autorité de certification dans la console

Ajouter une autorité de certification (CA) dans la console Workspace ONE UEM.

Conditions préalables

- Vous devez avoir ajouté un modèle d'utilisateur dans le serveur d'autorité de certification.
- Vous devez disposer du nom de l'émetteur d'autorité de certification. Connectez-vous au serveur Active Directory (AD) et exécutez la commande `certutil` depuis l'invite de commande pour obtenir le nom d'émetteur de l'autorité de certification.
- Spécifiez le *Nom d'utilisateur* de l'autorité de certification qui doit être de type *compte de service*.

Procédure

1. Connectez-vous à la console Workspace ONE UEM et sélectionnez le groupe d'organisation approprié.
2. Accédez à **Tous les paramètres** et cliquez sur **Intégration d'entreprise > Autorités de certification** dans le menu déroulant.
3. Cliquez sur l'onglet **Autorités de certification** et cliquez sur **Ajouter**.
4. Entrez les informations suivantes pour l'autorité de certification :

Option	Description
Nom	Nom valide de l'autorité de certification
Type d'autorité	Microsoft ADCS
Protocole	ADCS
Nom d'hôte du serveur	Nom d'hôte du serveur AD
Nom de l'autorité	Nom d'émetteur de l'autorité de certification
Authentification	Compte de service
Nom d'utilisateur	Nom d'utilisateur avec un compte de service au format *domaine**nomutilisateur*.
Mot de passe	Mot de passe correspondant au nom d'utilisateur.
Options supplémentaires	aucune

5. Cliquez sur **Enregistrer**.

Ajouter un modèle de demande d'autorité de certification

Ajoutez un modèle de demande d'autorité de certification après avoir ajouté une autorité de certification dans la console Workspace ONE UEM.

Conditions préalables

1. Vous devez avoir ajouté un modèle d'utilisateur dans le serveur d'autorité de certification.
2. Vous devez avoir ajouté une autorité de certification dans la console Workspace ONE UEM.

Procédure

1 Connectez-vous à la console Workspace ONE UEM, accédez à **Tous les paramètres** et cliquez sur **Intégration d'entreprise > Autorités de certification** dans la liste déroulante.

2 Cliquez sur l'onglet **Modèles de demande** et cliquez sur **Ajouter**.

3 Entrez les informations suivantes pour le modèle :

Option	Description
Nom	Nom valide du modèle de certificat
Description (facultative)	Description du modèle
Autorité de certification	Autorité de certification ajoutée précédemment
Modèle d'émission	Nom du modèle utilisateur créé dans le serveur d'autorité de certification
Nom du sujet	Pour ajouter le nom du sujet, maintenez le curseur sur le champ de valeur (après la valeur par défaut « CN= »), cliquez sur le bouton « + » et sélectionnez l'adresse e-mail appropriée
Longueur de clé privée	2 048
Type de clé privée	Sélectionnez *Signature*
Type de réseau de stockage	Cliquez sur **Ajouter** et choisissez *Nom principal de l'utilisateur*
Renouvellement automatique du certificat (facultatif)	
Activer la révocation de certificat (facultatif)	
Publier la clé privée (facultatif)	

4 Cliquez sur **Enregistrer**.

Mettre à jour des stratégies de sécurité pour utiliser le certificat d'autorité de certification extrait

Mettez à jour les stratégies de sécurité dans la console Workspace ONE UEM pour utiliser le certificat d'autorité de certification extrait.

Conditions préalables

Procédure

1 Connectez-vous à la console Workspace ONE UEM, accédez à **Tous les paramètres** et cliquez sur **Applications > Sécurité et stratégies > Stratégies de sécurité** dans le menu déroulant.

2 Sélectionnez **Remplacer** pour Paramètres actuels.

3 Activez **Authentification intégrée**.

   a Sélectionnez **Utiliser le certificat**.

   b Définissez la **Source des informations d'identification** sur **Autorité de certification**.

   c Spécifiez l'**Autorité de certification** et le **Modèle de certificat** définis précédemment.

4 Définissez **Sites autorisés** sur *.

5 Cliquez sur **Enregistrer**.

Configurer un proxy inverse Web pour le pontage d'identité (certificat sur Kerberos)

Configurez la fonctionnalité de pontage Unified Access Gateway pour fournir l'authentification unique aux applications non-SAML héritées sur site à l'aide de la validation du certificat.

Conditions préalables

Avant de commencer le processus de configuration, vérifiez que vous disposez des fichiers et certificats suivants :

- Fichier keytab d'une application principale, comme Sharepoint ou JIRA
- Certificat d'autorité de certification racine ou chaîne de certificats complète avec le certificat intermédiaire pour l'utilisateur
- Vous devez avoir ajouté et téléchargé un certificat dans la console Workspace ONE UEM. Reportez-vous à la section Autoriser la console Workspace ONE UEM à extraire et utiliser des certificats d'autorité de certification.

Reportez-vous à la documentation produit pertinente pour générer les certificats racine et utilisateur, ainsi que le fichier keytab pour les applications non-SAML.

Assurez-vous que le port TCP/UDP 88 est ouvert car Unified Access Gateway s'en sert pour les communications Kerberos avec Active Directory.

Procédure

1 À partir de **Paramètres d'authentification > Certificat X509**, accédez à :

   a Dans **Certificat d'autorité de certification intermédiaire et racine**, cliquez sur **Sélectionner** et téléchargez toute la chaîne de certificats.

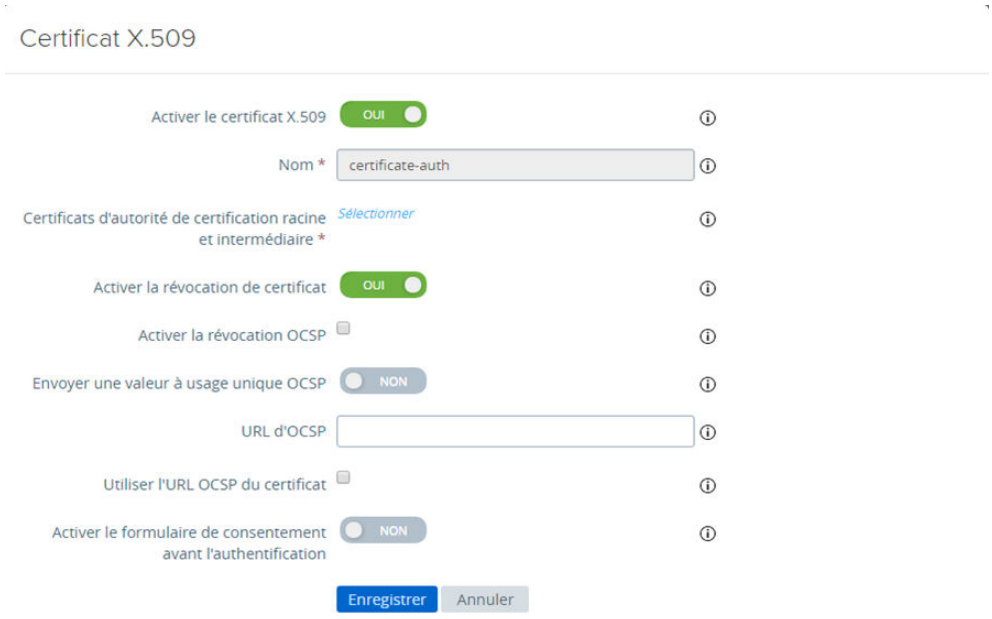
   b Dans **Activer la révocation de certificat**, définissez la bascule sur **Oui**.

   c Cochez la case **Activer la révocation OCSP**.

d Dans la zone de texte **URL d'OCSP**, entrez l'URL du répondeur OCSP.

Unified Access Gateway envoie la demande OCSP à l'URL spécifiée et reçoit une réponse qui contient des informations indiquant si le certificat est révoqué ou non.

e Cochez la case **Utiliser l'URL OCSP du certificat** uniquement s'il existe un cas d'utilisation pour envoyer la demande OCSP à l'URL d'OCSP dans le certificat client. Si cette option n'est pas activée, elle est définie par défaut sur la valeur de la zone de texte URL d'OCSP.



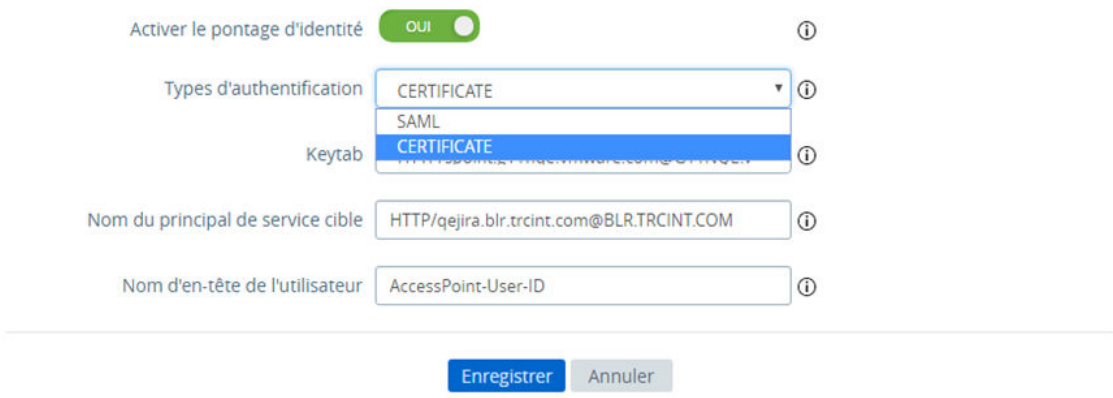
2 Dans **Paramètres avancés > Paramètres du pontage d'identité > Paramètres OSCP**, cliquez sur **Ajouter**.

a Cliquez sur **Sélectionner** et téléchargez le certificat de signature OCSP.

3 Cliquez sur l'icône d'engrenage **Paramètres du domaine** et configurez les paramètres du domaine comme décrit dans la section Configurer des paramètres de domaine.

4 Dans **Paramètres généraux > Paramètres du service Edge**, cliquez sur l'icône d'engrenage **Paramètres du proxy inverse**.

5 Définissez **Activer les paramètres du pontage d'identité** sur **OUI**, configurez les paramètres de pontage d'identité suivants, puis cliquez sur **Enregistrer**.



Option	Description
Types d'authentification	Sélectionnez CERTIFICAT dans le menu déroulant.
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.
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 ou utilisez la valeur par défaut, AccessPoint-User-ID.

Étape suivante

Lorsque vous utilisez Workspace ONE Web pour accéder au site Web cible, ce dernier agit comme le proxy inverse. Unified Access Gateway valide le certificat présenté. Si le certificat est valide, le navigateur affiche la page d'interface utilisateur de l'application principale.

Pour prendre connaissance des messages d'erreur spécifiques et des informations de dépannage, reportez-vous à la section Dépannage des erreurs : pontage d'identité.

Configuration d'Horizon pour l'intégration d'Unified Access Gateway et du fournisseur d'identité tiers

Si vous utilisez un fournisseur d'identité SAML 2.0, vous pouvez directement intégrer le fournisseur d'identité à UAG (Unified Access Gateway) pour prendre en charge l'authentification utilisateur d'Horizon Client. Pour utiliser l'intégration tierce de SAML à UAG, vous devez utiliser le Serveur de connexion Horizon 7.11 ou des versions ultérieures.

La séquence d'authentification peut être SAML et relais pour l'authentification SAML et l'authentification par mot de passe AD ou uniquement SAML lorsqu'elle est utilisée avec l'authentification unique réelle Horizon.

Unified Access Gateway prend en charge l'accès non authentifié à un utilisateur d'Horizon Client se connectant à Unified Access Gateway lorsqu'il est intégré à un fournisseur d'identité SAML. Après l'authentification initiale auprès d'Unified Access Gateway, l'utilisateur peut recevoir des droits pour les applications publiées sans authentification supplémentaire. La méthode SAML et non authentifiée prend en charge cette fonctionnalité.

Avec la prise en charge de l'intégration d'UAG et du fournisseur d'identité SAML tiers, l'installation de Workspace ONE Access n'est pas utilisée.

Pour intégrer UAG au fournisseur d'identité, vous devez configurer le fournisseur d'identité avec les informations de celui-ci (UAG), télécharger le fichier de métadonnées du fournisseur d'identité sur UAG et configurer les paramètres d'Horizon sur la console de l'interface utilisateur d'administration d'UAG.

Pour plus d'informations sur l'authentification des utilisateurs à Horizon Client sans être invités à fournir des informations d'identification Active Directory, consultez la section *Authentification des utilisateurs sans demander les informations d'identification* et les informations associées dans le *Guide d'administration d'Horizon* sur VMware Docs.

Configurer le fournisseur d'identité avec les informations d'Unified Access Gateway

Pour intégrer UAG (fournisseur de services) au fournisseur d'identité, vous devez configurer le fournisseur d'identité avec les informations du fournisseur de services, telles que l'ID d'entité et l'URL de point de terminaison du service clients d'assertion. Dans ce cas précis, UAG est le fournisseur de services.

Procédure

1. Connectez-vous à la console d'administration du fournisseur d'identité.
2. Pour créer une application SAML, suivez les étapes appropriées dans la console d'administration du fournisseur d'identité.

   Si celui-ci comprend une fonctionnalité de chiffrement d'assertion, assurez-vous que la fonctionnalité est désactivée dans les paramètres SAML de l'application que vous créez dans le fournisseur d'identité.

3 Configurez le fournisseur d'identité avec les informations d'UAG de l'une des manières suivantes :

Option	Description
Téléchargez les métadonnées du fournisseur de services SAML à partir d'UAG.	Pour importer les métadonnées SAML dans le fournisseur d'identité, assurez-vous que le fournisseur d'identité prend en charge la fonctionnalité d'importation. a Dans la section **Configurer manuellement** de l'interface utilisateur d'administration d'UAG, cliquez sur **Sélectionner**. b Dans la section **Paramètres généraux**, pour **Paramètres du service Edge**, cliquez sur **Afficher**. c Cliquez sur l'icône d'engrenage **Paramètres d'Horizon**. d Sur la page **Paramètres d'Horizon**, cliquez sur **Plus**. e Sélectionnez les **Méthodes d'authentification**. Les **Méthodes d'authentification** peuvent être `SAML`, `SAML and Passthrough` ou `SAML and Unauthenticated`. **Note** Si vous choisissez `SAML and Unauthenticated`, veillez à configurer le paramètre Horizon Connection Server, comme indiqué pour cette **Méthode d'authentification** dans Configurer les paramètres d'Horizon sur Unified Access Gateway pour l'intégration SAML. f Cliquez sur **Télécharger les métadonnées du fournisseur de services SAML**. g Dans la fenêtre **Télécharger les métadonnées du fournisseur de services SAML**, entrez le nom d'hôte externe. h Cliquez sur **Télécharger**. i Enregistrez le fichier de métadonnées `.xml` dans un emplacement de votre ordinateur auquel vous avez accès. j Connectez-vous à la console d'administration du fournisseur d'identité. k Importez le fichier de métadonnées téléchargé dans le fournisseur d'identité.
Configurez les paramètres SAML suivants dans la console d'administration du fournisseur d'identité.	a Configurez l'ID d'entité sous `https://<uagIP/domain>/portal` b Configurez l'URL de point de terminaison du service clients d'assertion sous `https://<uagIP/domain>/portal/samlsso`.

Pour plus d'informations sur les méthodes d'authentification pour Unified Access Gateway et l'intégration d'un fournisseur d'identité tiers, consultez la section Méthodes d'authentification pour l'intégration d'Unified Access Gateway et du fournisseur d'identité tiers.

4 (Facultatif) Configurez l'attribut personnalisé avec un nom d'utilisateur.

Dans l'interface utilisateur d'administration d'Unified Access Gateway, lorsque `SAML and Unauthenticated` est sélectionné comme méthode d'authentification, si l'option **Attribut de nom d'utilisateur non authentifié SAML** est configurée avec le même nom d'attribut que celui spécifié ici et lorsque l'assertion SAML est validée, Unified Access Gateway fournit l'accès non authentifié au nom d'utilisateur configuré pour cet attribut personnalisé.

Pour comprendre comment Unified Access Gateway fournit l'accès non authentifié à ce nom d'utilisateur, consultez la section Méthodes d'authentification pour l'intégration d'Unified Access Gateway et du fournisseur d'identité tiers.

Étape suivante

Téléchargez le fichier XML de métadonnées SAML du fournisseur d'identité vers UAG.

Télécharger les métadonnées SAML du fournisseur d'identité vers Unified Access Gateway

Pour configurer des méthodes d'authentification SAML, et SAML et relais dans Horizon, vous devez télécharger le fichier XML de métadonnées de certificat SAML du fournisseur d'identité vers UAG (Unified Access Gateway). Le téléchargement permet à UAG de faire confiance au fournisseur d'identité en vérifiant la signature d'une assertion à l'aide de la clé publique du fournisseur d'identité.

Conditions préalables

Vous devez avoir téléchargé le fichier XML de métadonnées SAML à partir du fournisseur d'identité et enregistré ce fichier sur un ordinateur auquel vous pouvez accéder.

Procédure

1. Dans la section **Configurer manuellement** de la console l'administration d'UAG, 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 à l'emplacement d'enregistrement du fichier de métadonnées.
5. Cliquez sur **Ouvrir**.
6. Cliquez sur **Enregistrer**.

   Le message suivant s'affiche : `La configuration est enregistrée.`

Étape suivante

Configurez les paramètres d'Horizon sur UAG pour sélectionner la méthode d'authentification et choisir le fournisseur d'identité requis.

Configurer les paramètres d'Horizon sur Unified Access Gateway pour l'intégration SAML

Vous devez sélectionner la méthode d'authentification SAML appropriée et choisir le fournisseur d'identité (IDP) pris en charge par votre organisation sur la page Paramètres d'Horizon sur UAG (Unified Access Gateway). La méthode d'authentification détermine le flux de connexion de l'utilisateur lors de l'utilisation d'Horizon Client avec UAG.

Pour plus d'informations sur les méthodes d'authentification, reportez-vous à la section Méthodes d'authentification pour l'intégration d'Unified Access Gateway et du fournisseur d'identité tiers

Conditions préalables

- Veillez à utiliser le Serveur de connexion Horizon 7.11 ou des versions ultérieures.
- Vous devez avoir déjà téléchargé les métadonnées du fournisseur d'identité sur UAG.

  Reportez-vous à la section Télécharger les métadonnées SAML du fournisseur d'identité vers Unified Access Gateway.

Procédure

1. Dans la section **Configurer manuellement** de l'interface utilisateur d'administration d'UAG, cliquez sur **Sélectionner**.
2. Dans la section **Paramètres généraux**, pour **Paramètres du service Edge**, cliquez sur **Afficher**.
3. Cliquez sur l'icône d'engrenage **Paramètres d'Horizon**.
4. Sur la page **Paramètres d'Horizon**, cliquez sur **Plus** pour configurer les paramètres suivants :

Option	Description
Méthodes d'authentification	Sélectionnez `SAML`, `SAML and Passthrough` ou `SAML and Unauthenticated` **Note** Si TrueSSO est activé sur le Serveur de connexion Horizon, vous devez utiliser la méthode d'authentification SAML. **Important** Si vous choisissez `SAML and Unauthenticated`, veillez à configurer le **Niveau de ralentissement de la connexion** dans le Horizon Connection Server sur `Low`. Cette configuration est nécessaire pour éviter un long retard du délai de connexion pour le point de terminaison lors de l'accès à l'application ou au poste de travail distant. Pour plus d'informations sur la configuration du **Niveau de ralentissement de la connexion**, consultez la documentation de l' *Administration d'Horizon* sur VMware Docs.
Fournisseur d'identité	Sélectionnez le fournisseur d'identité qui doit être intégré à UAG. **Note** Un fournisseur d'identité est disponible pour la sélection uniquement si les métadonnées du fournisseur d'identité sont téléchargées vers UAG.

Pour configurer les autres paramètres d'Horizon, reportez-vous à la section Configuration des paramètres d'Horizon.

Méthodes d'authentification pour l'intégration d'Unified Access Gateway et du fournisseur d'identité tiers

SAML, SAML et relais, ainsi que SAML et Non authentifié sont les méthodes d'authentification prises en charge pour intégrer UAG (Unified Access Gateway) à un fournisseur d'identité tiers pour contrôler l'accès aux postes de travail et aux applications Horizon. La méthode d'authentification détermine la façon dont l'utilisateur d'Horizon est authentifié.

Lors de la configuration des paramètres d'Horizon dans UAG, vous devez sélectionner l'une des méthodes d'authentification.

SAML

Dans la méthode d'authentification SAML, UAG valide d'abord l'assertion SAML. Si l'assertion SAML est valide, UAG transmet l'assertion SAML au Horizon Connection Server. Pour que le Horizon Connection Server accepte l'assertion, il doit être configuré avec les métadonnées du fournisseur d'identité. Lorsqu'un utilisateur accède à Horizon Client, il reçoit des droits sans être invité à fournir les informations d'identification Active Directory.

Note Si le paramètre TrueSSO est activé sur le Horizon Connection Server, vous devez utiliser la méthode d'authentification SAML.

SAML et relais

Dans la méthode d'authentification SAML et relais, UAG valide l'assertion SAML. Si celle-ci est valide, l'utilisateur est invité à fournir les informations d'identification d'authentification Active Directory lors de l'accès à Horizon Client. Dans cette méthode d'authentification, UAG ne transmet pas l'assertion SAML au Horizon Connection Server.

SAML et Non authentifié

Dans la méthode SAML et Non authentifié, Unified Access Gateway combine l'authentification de l'utilisateur SAML avec la fonctionnalité d'accès non authentifié d'Horizon. Si l'assertion SAML est valide, l'utilisateur peut accéder aux applications hébergées RDS sans aucune autre authentification requise. Dans la fonctionnalité d'accès non authentifié d'Horizon, un alias d'utilisateur basé sur les rôles est utilisé avec Horizon pour déterminer les droits des applications. L'alias d'utilisateur peut être utilisé comme alias par défaut par Horizon. Cet alias peut également être spécifié par défaut dans la configuration d'Unified Access Gateway (**Nom d'utilisateur non authentifié par défaut**) ou il peut s'agir de la valeur d'un attribut SAML nommé présenté comme une réclamation dans l'assertion SAML envoyée par le fournisseur d'identité.

L' interface utilisateur d'administration d'Unified Access Gateway comporte deux zones de texte, **Attribut de nom d'utilisateur non authentifié SAML** et **Nom d'utilisateur non authentifié par défaut**, qui peuvent être utilisées pour spécifier l'alias d'utilisateur. Ces zones de texte sont disponibles dans l'interface utilisateur d'administration lorsque la méthode d'authentification est SAML et Non authentifié.

Si la zone de texte **Attribut de nom d'utilisateur non authentifié SAML** est définie dans l'interface utilisateur d'administration, lorsque Unified Access Gateway valide l'assertion SAML et si le nom est présent dans l'assertion SAML, Unified Access Gateway utilise cette valeur comme alias d'utilisateur d'accès non authentifié d'Horizon.

Lorsque la zone de texte **Attribut de nom d'utilisateur non authentifié SAML** est vide ou que le nom d'attribut qui y est spécifié est manquant dans l'assertion SAML, Unified Access Gateway utilise le nom d'utilisateur par défaut configuré dans la zone de texte **Nom d'utilisateur non authentifié par défaut** en tant qu'alias d'utilisateur d'accès non authentifié d'Horizon.

Si **Attribut de nom d'utilisateur non authentifié SAML** n'est pas utilisé et que la zone de texte **Nom d'utilisateur non authentifié par défaut** est vide, Unified Access Gateway utilise l'alias d'utilisateur par défaut configuré dans Horizon.

Pour plus d'informations sur la configuration des utilisateurs d'accès non authentifié, reportez-vous à la section *Fourniture d'un accès non authentifié pour des applications publiées* et aux informations associées dans le guide *Administration d'Horizon* sur le site VMware docs.

Pour plus d'informations sur la fourniture de droits (applications publiées) aux utilisateurs d'accès non authentifié, reportez-vous à la section *Autoriser les utilisateurs d'accès non authentifié à accéder à des applications publiées* et aux informations associées dans le guide *Administration d'Horizon* sur le site VMware Docs.

Composants de Workspace ONE UEM sur Unified Access Gateway

Vous pouvez déployer VMware Tunnel à l'aide du dispositif Unified Access Gateway. Unified Access Gateway prend en charge le déploiement sur les environnements ESXi ou Microsoft Hyper-V. VMware Tunnel fournit une méthode sécurisée et efficace pour que les applications individuelles accèdent aux ressources d'entreprise. Content Gateway (CG) est un composant de la solution de gestion de contenu de Workspace ONE UEM qui permet d'accéder en toute sécurité au contenu du référentiel sur site sur des terminaux mobiles.

Configuration requise de DNS pour VMware Tunnel et Content Gateway

Lorsque les services VMware Tunnel et Content Gateway sont activés sur le même dispositif, et que le partage de port TLS est activé, les noms DNS doivent être uniques pour chaque service. Lorsque TLS n'est pas activé, seul un nom DNS peut être utilisé pour les deux services, car le port différenciera le trafic entrant.

Déploiement d'VMware Tunnel sur Unified Access Gateway

Le déploiement de VMware Tunnel 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 sur les environnements ESXi ou Microsoft Hyper-V.

VMware Tunnel comprend deux composants indépendants : le proxy tunnel et le tunnel par application. Vous déployez VMware Tunnel à l'aide de modèles d'architecture réseau à niveau unique ou multiniveau.

Les modèles de déploiement du proxy tunnel et du tunnel par application peuvent tous deux être utilisés pour un réseau multiniveau sur le dispositif Unified Access Gateway. 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 Tunnel Proxy sécurise le trafic réseau entre un terminal d'utilisateur final et un site Web via Workspace ONE Web ou n'importe quelle application activée pour Workspace ONE SDK, déployée à partir de Workspace ONE UEM. 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 Workspace ONE UEM. En général, ce composant doit être utilisé lorsque plusieurs périphériques non gérés nécessitent un accès sécurisé aux ressources internes.

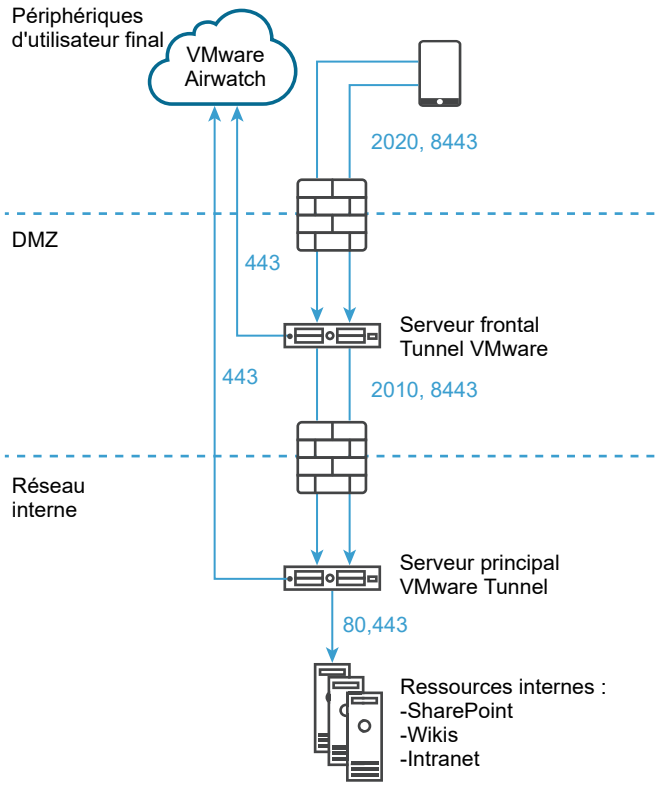
Pour les terminaux entièrement inscrits, le composant Tunnel par application permet aux terminaux de se connecter aux ressources internes sans avoir besoin de Workspace ONE SDK. Ce composant utilise les capacités natives de VPN par application des systèmes d'exploitation iOS, Android, Windows 10 et macOS.

Pour plus d'informations sur ces plateformes et les capacités du composant VMware Tunnel, consultez la dernière documentation de Tunnel sur la page de documentation de Workspace ONE UEM.

Le déploiement de VMware Tunnel pour votre environnement Workspace ONE UEM implique les étapes suivantes :

1. Configurez les informations de port et de nom d'hôte VMware Tunnel dans la console Workspace ONE UEM. Reportez-vous à la section Règles de pare-feu pour les dispositifs Unified Access Gateway basés sur une zone DMZ.
2. Téléchargez et déployez le modèle OVF Unified Access Gateway.
3. Configurez manuellement VMware Tunnel.

Figure 4-10. Déploiement multiniveau du VMware Tunnel : tunnel proxy et tunnel par application



AirWatch v9.1 et versions ultérieures prend en charge le mode cascade en tant que modèle de déploiement multiniveau pour VMware Tunnel. 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 Workspace ONE UEM et AWCM. Le mode **cascade** de VMware Tunnel prend en charge l'architecture multiniveau pour le composant Tunnel par application.

Pour les considérations relatives à l'équilibrage de charge pour Content Gateway et le proxy Tunnel, reportez-vous à la section Topologies d'équilibrage de charge Unified Access Gateway.

Accédez à la page de documentation de VMware Workspace ONE UEM pour obtenir une liste complète des guides et des notes de mise à jour de Workspace ONE UEM.

Configurer le proxy VMware Tunnel

Configurez le proxy VMware Tunnel à l'aide de l'assistant de configuration. Les options configurées dans l'assistant sont modularisées dans le programme d'installation, que vous pouvez télécharger depuis Workspace ONE UEM Console et déplacer vers vos serveurs de tunnel.

Configurez le proxy VMware Tunnel dans UEM Console sous **Groupes et paramètres > Tous les paramètres > Système > Intégration d'entreprise > VMware Tunnel > Proxy**. L'assistant vous guide pas à pas à travers la configuration du programme d'installation. Les options configurées dans l'assistant sont modularisées dans le programme d'installation, que vous pouvez télécharger depuis Workspace ONE UEM Console et déplacer vers vos serveurs de tunnel. La modification des détails de cet assistant nécessite généralement une réinstallation de VMware Tunnel avec la nouvelle configuration.

Pour configurer le proxy VMware Tunnel, il vous faut les détails du serveur sur lequel vous prévoyez d'effectuer l'installation. Avant la configuration, déterminez le modèle de déploiement, les noms d'hôte et les ports, ainsi que les fonctionnalités de VMware Tunnel à implémenter. Vous pouvez envisager de modifier l'intégration du journal d'accès, le déchargement SSL, l'intégration de l'autorité de certification d'entreprise, etc.

Note L'assistant affiche dynamiquement les options appropriées selon vos sélections. Les écrans de configuration peuvent afficher des zones de texte et des options différentes.

Procédure

1. Accédez à **Groupes et paramètres > Tous les paramètres > Système > Intégration d'entreprise > VMware Tunnel > Proxy**.
   - S'il s'agit d'une première configuration de VMware Tunnel, sélectionnez **Configurer** et suivez les écrans de l'assistant de configuration.
   - Si vous configurez VMwareTunnel pour la première fois, sélectionnez **Remplacer**, puis le bouton bascule **VMware Tunnel Activé** et enfin **Configurer**.

     Note Le remplacement des paramètres de proxy de VMware Tunnel ne remplace pas les paramètres de configuration de VMware Tunnel.
2. Dans l'écran **Type de déploiement**, sélectionnez le bouton bascule **Activer le proxy (Windows et Linux)**, puis sélectionnez les composants à configurer à l'aide du menu déroulant **Type de configuration du proxy**.
3. Dans les menus déroulants qui s'affichent, indiquez si vous configurez un **Point de terminaison relais** ou le déploiement du **Type de configuration du proxy**. Pour afficher un exemple du type sélectionné, sélectionnez l'icône d'informations.
4. Sélectionnez **Suivant**.

5 Dans l'écran **Détails**, configurez les paramètres suivants. Les options affichées dans l'écran **Détails** dépendent du type de configuration que vous avez sélectionné dans le menu déroulant **Type de configuration du proxy**.

- **Type de configuration du proxy de base**, entrez les informations suivantes :

Paramètre	Description
Nom d'hôte	Entrez le nom de domaine complet du nom d'hôte public pour le serveur de tunnel, par exemple, tunnel.acmemdm.com. Ce nom d'hôte doit être disponible publiquement, car il s'agit du DNS auquel les terminaux se connectent depuis Internet.
Port de relais	Le service de proxy est installé sur ce port. Les terminaux se connectent à <relayhostname>:<port> pour utiliser la fonctionnalité du proxy VMware Tunnel. La valeur par défaut est 2020.
Nom d'hôte relais	(Point de terminaison relais uniquement). Entrez le nom de domaine complet du nom d'hôte public du serveur relais de tunnel, par exemple, tunnel.acmemdm.com. Ce nom d'hôte doit être disponible publiquement, car il s'agit du DNS auquel les terminaux se connectent depuis Internet.
Activer le déchargement SSL	Cochez cette case pour utiliser le déchargement SSL afin d'alléger la charge de chiffrement et de déchiffrement du trafic à partir du serveur VMware Tunnel.
Utiliser le proxy Kerberos	Pour autoriser l'accès à l'authentification Kerberos pour vos services Web principaux de la cible, sélectionnez la prise en charge du proxy Kerberos. Cette fonctionnalité ne prend actuellement pas en charge la délégation contrainte de Kerberos (KCD, Kerberos Constrained Delegation). Pour plus d'informations, consultez la section Configurer les paramètres du proxy Kerberos. Le serveur de point de terminaison doit se trouver sur le même domaine que le centre de distribution de clés (KDC, Key Distribution Center) pour que le proxy Kerberos communique avec le KDC.

- Si vous choisissez **Type de configuration du proxy** du **point de terminaison relais**, entrez les informations suivantes :

Paramètre	Description
Nom d'hôte relais	(Point de terminaison relais uniquement). Entrez le nom de domaine complet du nom d'hôte public du serveur relais de tunnel, par exemple, tunnel.acmemdm.com. Ce nom d'hôte doit être disponible publiquement, car il s'agit du DNS auquel les terminaux se connectent depuis Internet.
Nom d'hôte du point de terminaison	DNS interne du serveur de point de terminaison du tunnel. Cette valeur est le nom d'hôte auquel le serveur de relais se connecte sur le port du point de terminaison relais. Si vous prévoyez d'installer VMware Tunnel sur un serveur déchargé SSL, entrez le nom de ce serveur à la place du **nom d'hôte**. Lorsque vous entrez le **nom d'hôte**, n'incluez pas un protocole, tel que http://, https://, etc.
Port de relais	Le service de proxy est installé sur ce port. Les terminaux se connectent à <relayhostname>:<port> pour utiliser la fonctionnalité du proxy VMware Tunnel. La valeur par défaut est 2020.

Paramètre	Description
Port de point de terminaison	(Point de terminaison relais uniquement). Cette valeur est le port utilisé pour la communication entre le relais VMware Tunnel et le point de terminaison VMware Tunnel. La valeur par défaut est 2010. Si vous utilisez une combinaison de proxy et de tunnel par application, le point de terminaison relais s'installe dans le cadre du serveur frontal pour le mode cascade. Les ports doivent utiliser des valeurs différentes.
Activer le déchargement SSL	Cochez cette case pour utiliser le déchargement SSL afin d'alléger la charge de chiffrement et de déchiffrement du trafic à partir du serveur VMware Tunnel.
Utiliser le proxy Kerberos	Pour autoriser l'accès à l'authentification Kerberos pour vos services Web principaux de la cible, sélectionnez la prise en charge du proxy Kerberos. Cette fonctionnalité ne prend actuellement pas en charge la délégation contrainte de Kerberos (KCD, Kerberos Constrained Delegation). Pour plus d'informations, consultez la section Configurer les paramètres du proxy Kerberos. Le serveur de point de terminaison doit se trouver sur le même domaine que le centre de distribution de clés (KDC, Key Distribution Center) pour que le proxy Kerberos communique avec le KDC. Dans la zone de texte **Domaine**, entrez le domaine du serveur KDC.

6 Sélectionnez **Suivant**.

7 Dans l'écran **SSL**, vous pouvez configurer le certificat SSL public qui sécurise la communication client-serveur de l'application activée sur un périphérique vers VMware Tunnel. Par défaut, cette configuration utilise un certificat AirWatch pour une communication serveur-client sécurisée.

   a Sélectionnez l'option **Utiliser le certificat SSL public** si vous préférez utiliser un certificat SSL tiers pour le chiffrement entre Workspace ONE Web ou des applications activées pour le SDK et le serveur VMware Tunnel.

   b Sélectionnez **Télécharger** pour télécharger un fichier de certificat .PFX ou .P12 et entrez le mot de passe. Ce fichier doit contenir votre paire de clés publique et privée. Les fichiers CER et CRT ne sont pas pris en charge.

8 Sélectionnez **Suivant**.

9 Dans l'écran **Authentification**, configurez les paramètres suivants pour sélectionner les certificats que les terminaux utilisent pour s'authentifier auprès de VMware Tunnel.

Par défaut, tous les composants utilisent des certificats émis par AirWatch. Pour utiliser des certificats d'autorité de certification d'entreprise pour l'authentification client-serveur, sélectionnez l'option **Autorité de certification d'entreprise**.

a Sélectionnez **Par défaut** pour utiliser les certificats émis par AirWatch. Le certificat client émis par AirWatch par défaut n'est pas renouvelé automatiquement. Pour renouveler ces certificats, republiez le profil de VPN sur les périphériques dont le certificat client arrive à expiration ou est expiré. Affichez l'état du certificat d'un terminal en accédant à **Terminaux > Détails du terminal > Plus > Certificats**.

b Sélectionnez **Autorité de certification d'entreprise** à la place des certificats émis par AirWatch pour l'authentification entre Workspace ONE Web, les applications activées pour le tunnel par application ou les applications activées pour le SDK. VMware Tunnel exige qu'une autorité de certification et qu'un modèle de certificat soient configurés dans votre environnement Workspace ONE UEM avant de configurer VMware Tunnel.

c Sélectionnez les options **Autorité de certification** et **Modèle de certificat** qui permettent de demander un certificat auprès de l'autorité de certification.

d Sélectionnez **Télécharger** pour télécharger la chaîne complète de la clé de publique de votre autorité de certification vers l'assistant de configuration.

Le modèle d'autorité de certification doit contenir CN=UDID dans le nom du sujet. Les autorités de certification prises en charge sont ADCS, RSA et SCEP.

Renouvellement automatique des certificats en fonction des paramètres de votre modèle d'autorité de certification.

10 Cliquez sur **Ajouter** pour ajouter un certificat intermédiaire.

11 Sélectionnez **Suivant**.

12 Dans l'écran **Divers**, vous pouvez utiliser les journaux d'accès pour les composants Proxy ou Tunnel par application. Activez le bouton bascule **Journaux d'accès** pour configurer la fonctionnalité.

Si vous prévoyez d'utiliser cette fonctionnalité, vous devez la définir maintenant dans le cadre de la configuration, car vous ne pourrez pas l'activer ultérieurement sans reconfigurer le tunnel et réexécuter le programme d'installation. Pour plus d'informations sur ces paramètres, consultez les journaux d'accès et l'intégration Syslog, puis configurez les paramètres avancés de VMware Tunnel.

a Entrez l'URL de votre hôte Syslog dans le champ **Nom d'hôte Syslog**. Ce paramètre s'affiche après l'activation des journaux d'accès.

b Entrez le port sur lequel vous voulez communiquer avec l'hôte Syslog dans le champ **Port UDP**.

13 Sélectionnez **Suivant**, examinez le résumé de votre configuration, confirmez que tous les noms d'hôte, les ports et les paramètres sont corrects et sélectionnez **Enregistrer**.

   Le programme d'installation est désormais téléchargeable dans l'écran VMware Tunnel **Configuration**.

14 Dans l'écran **Configuration**, sélectionnez l'onglet **Général**. L'onglet **Général** permet d'effectuer les opérations suivantes :

   a Vous pouvez sélectionner **Tester la connexion** pour vérifier la connectivité.

   b Vous pouvez sélectionner **Télécharger le fichier XML de configuration** pour récupérer la configuration de l'instance existante de VMware Tunnel en tant que fichier XML.

   c Vous pouvez sélectionner le lien hypertexte **Télécharger Unified Access Gateway**. Ce bouton télécharge le fichier OVA non-FIPS. Le fichier de téléchargement comprend également le script PowerShell et le fichier de modèle .ini pour la méthode de déploiement PowerShell. Vous devez télécharger le fichier OVA VHDX ou FIPS depuis My Workspace ONE.

   d Pour les méthodes d'installation héritées, vous pouvez sélectionner **Télécharger Windows Installer**.

      Ce bouton télécharge un fichier BIN unique utilisé pour le déploiement du serveur VMware Tunnel. Vous pouvez télécharger le fichier XML de configuration requis pour l'installation depuis Workspace ONE UEM Console après avoir confirmé le mot de passe du certificat.

15 Sélectionnez **Enregistrer**.

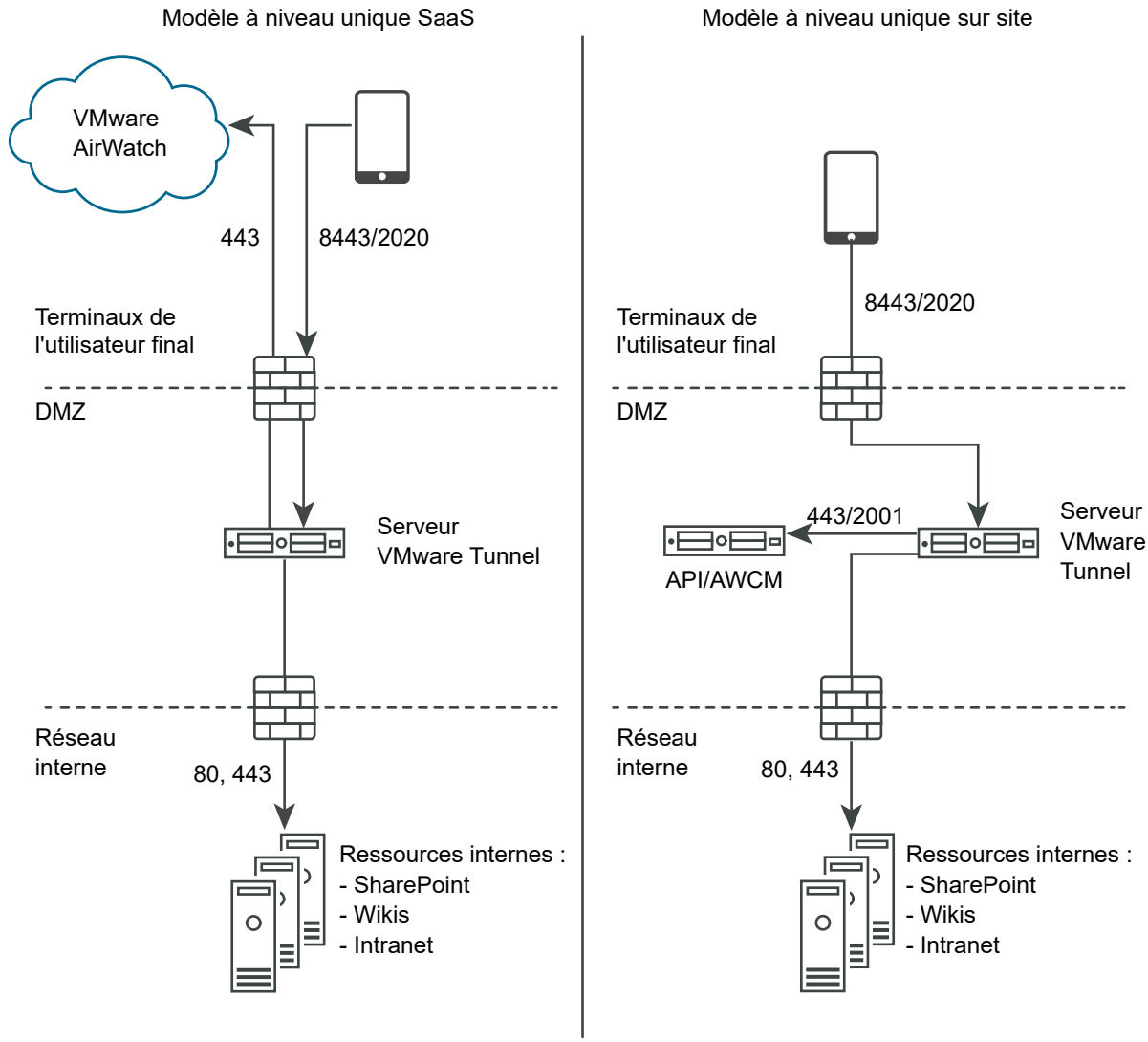
Modèle de déploiement à niveau unique

Si vous utilisez le modèle de déploiement à niveau unique, utilisez le mode de point de terminaison de base. Le modèle de déploiement de point de terminaison de base de VMware Tunnel est une instance unique du produit installé sur un serveur avec un DNS disponible publiquement.

VMware Tunnel de base est généralement installé sur le réseau interne derrière un équilibrage de charge dans la zone DMZ qui transfère le trafic sur les ports configurés vers VMware Tunnel, qui se connecte ensuite directement à vos applications Web internes. Toutes les configurations de déploiement prennent en charge l'équilibrage de charge et le proxy inverse.

Le serveur de tunnel de point de terminaison de base communique avec l'API et AWCM pour recevoir une liste blanche de clients autorisés à accéder à VMware Tunnel. Les composants Proxy et Tunnel par application prennent en charge l'utilisation d'un proxy sortant pour communiquer avec l'API/AWCM dans ce modèle de déploiement. Lorsqu'un terminal se connecte à VMware Tunnel, il est authentifié selon les certificats X.509 uniques émis par Workspace ONE UEM. Une fois qu'un terminal est authentifié, VMware Tunnel (point de terminaison de base) transmet la demande au réseau interne.

Si le point de terminaison de base est installé dans la zone DMZ, les modifications réseau appropriées doivent être effectuées pour permettre à VMware Tunnel d'accéder à diverses ressources internes sur les ports nécessaires. L'installation de ce composant derrière un équilibrage de charge dans la zone DMZ minimise le nombre de modifications réseau pour implémenter VMware Tunnel et fournit une couche de sécurité, car le DNS public n'est pas pointé directement vers le serveur qui héberge VMware Tunnel.


Modèle à niveau unique SaaS
VMware
AirWatch
443
8443/2020
Terminaux de
l'utilisateur final
DMZ
Serveur
VMware Tunnel
Réseau
interne
80, 443
Ressources internes :
- SharePoint
- Wikis
- Intranet
Modèle à niveau unique sur site
8443/2020
Terminaux de
l'utilisateur final
DMZ
443/2001
API/AWCM
Serveur
VMware
Tunnel
Réseau
interne
80, 443
Ressources internes :
- SharePoint
- Wikis
- Intranet

Déploiement en mode cascade

L'architecture de modèle de déploiement en cascade comprend deux instances de VMware Tunnel avec des rôles distincts. En mode cascade, le serveur frontal se trouve dans la zone DMZ et communique avec le serveur principal sur votre réseau interne.

Seul le composant Tunnel par application prend en charge le modèle de déploiement en cascade. Si vous utilisez uniquement le composant Proxy, vous devez utiliser le modèle de point de terminaison relais. Pour plus d'informations, consultez la section Déploiement de point de terminaison relais.

Les terminaux accèdent au serveur frontal pour le mode cascade à l'aide d'un nom d'hôte configuré sur les ports configurés. Le port par défaut pour l'accès au serveur frontal est le port 8443. Le serveur principal pour le mode cascade est installé sur le réseau interne hébergeant vos sites intranet et vos applications Web. Ce modèle de déploiement sépare le serveur frontal disponible publiquement du serveur principal qui se connecte directement à des ressources internes, ce qui fournit une couche supplémentaire de sécurité.

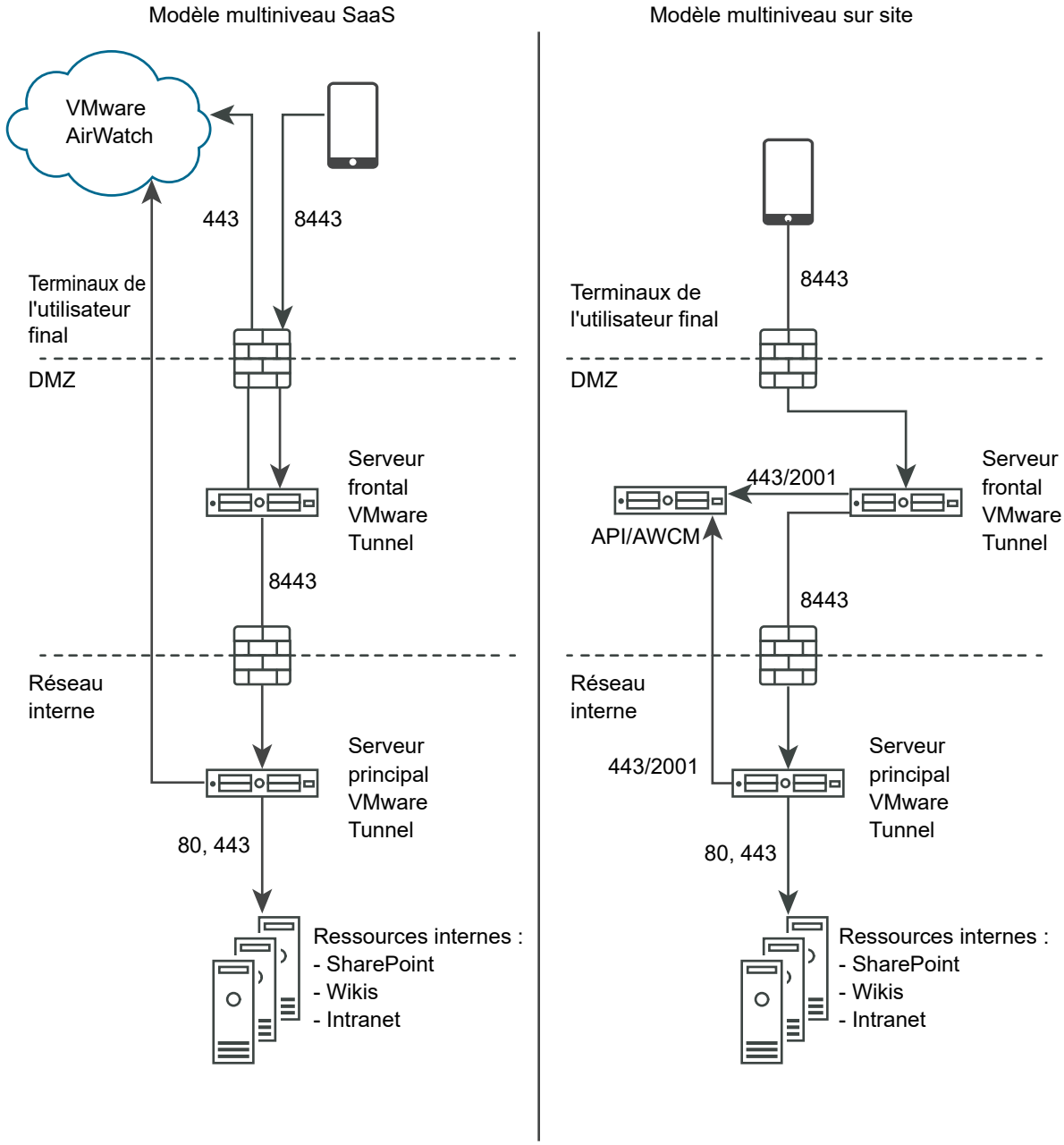
Le serveur frontal facilite l'authentification des terminaux en se connectant à AWCM lorsque des demandes sont faites à VMware Tunnel. Lorsqu'un périphérique fait une demande à VMware Tunnel, le serveur frontal détermine si le terminal est autorisé à accéder au service. Une fois authentifiée, la demande est transférée en toute sécurité à l'aide de TLS sur un port unique au serveur principal.

Le serveur principal se connecte au DNS interne ou à l'adresse IP demandée par le terminal.

Le mode cascade communique à l'aide de la connexion TLS (ou une connexion DTLS facultative). Vous pouvez héberger autant de serveurs frontaux et principaux que vous le souhaitez. Chaque serveur frontal agit de manière indépendante lors de la recherche d'un serveur principal actif pour connecter des terminaux au réseau interne. Vous pouvez configurer plusieurs entrées de DNS dans une table de recherche DNS pour permettre l'équilibrage de charge.

Les serveurs frontaux et principaux communiquent avec le serveur API Workspace ONE UEM et AWCM. Le serveur API fournit la configuration VMware Tunnel et AWCM fournit l'authentification des terminaux, les listes blanches et les règles de trafic. Le serveur frontal et principal communique avec l'API/AWCM via des connexions TLS directes, sauf si vous activez les appels de proxy sortants. Utilisez cette connexion si le serveur frontal ne peut pas accéder aux serveurs API/AWCM. Si activés, les serveurs frontaux se connectent via le serveur principal aux serveurs API/AWCM. Ce trafic, ainsi que celui du serveur principal, est acheminé à l'aide des règles de trafic côté serveur. Pour plus d'informations, consultez la section Règles de trafic réseau pour le tunnel par application

Le diagramme suivant illustre le déploiement multiniveau pour le composant Tunnel par application en mode cascade :



Déploiement de point de terminaison relais

Si vous utilisez un modèle de déploiement multiniveau et le composant Proxy de VMware Tunnel, utilisez le mode de déploiement de point de terminaison relais. L'architecture de mode de

déploiement de point de terminaison relais comprend deux instances de VMware Tunnel avec des rôles distincts. Le serveur de relais VMware Tunnel réside dans la zone DMZ et est accessible depuis le DNS public sur les ports configurés.

Si vous utilisez uniquement le composant Tunnel par application, pensez à utiliser un déploiement en mode cascade. Pour plus d'informations, consultez la section Déploiement en mode cascade.

Les ports d'accès au DNS public sont par défaut le port 8443 pour le tunnel par application et le port 2020 pour le proxy. Le serveur de point de terminaison VMware Tunnel est installé sur le réseau interne qui héberge des sites intranet et des applications Web. Ce serveur doit disposer d'un enregistrement DNS interne résolu par le serveur de relais. Ce modèle de déploiement sépare le serveur disponible publiquement du serveur qui se connecte directement à des ressources internes, fournissant ainsi une couche supplémentaire de sécurité.

Le rôle du serveur de relais inclut la communication avec les composants API et AWCM et l'authentification des terminaux lorsque des demandes sont faites à VMware Tunnel. Dans ce modèle de déploiement, la communication à l'API et AWCM à partir du serveur de relais peut être acheminée vers le proxy sortant via le serveur de point de terminaison. Le service Tunnel par application doit communiquer avec l'API et AWCM directement. Lorsqu'un périphérique fait une demande à VMware Tunnel, le serveur de relais détermine si le terminal est autorisé à accéder au service. Une fois authentifiée, la demande est transférée en toute sécurité à l'aide de HTTPS sur un port unique (le port par défaut est 2010) au serveur de point de terminaison VMware Tunnel.

Le rôle du serveur de point de terminaison consiste à se connecter au DNS interne ou à l'adresse IP demandée par le terminal. Le serveur de point de terminaison ne communique pas avec l'API ou AWCM, sauf si l'option **Activer les appels sortants API et AWCM via proxy** est définie sur **Activé** dans les paramètres de VMware Tunnel dans Workspace ONE UEM Console. Le serveur de relais exécute des contrôles de la santé à intervalles réguliers pour s'assurer que le point de terminaison est actif et disponible.

Ces composants peuvent être installés sur des serveurs partagés ou dédiés. Installez VMware Tunnel sur des serveurs Linux dédiés pour vous assurer que les performances ne sont pas affectées par d'autres applications exécutées sur le même serveur. Pour un déploiement de point de terminaison de relais, les composants Proxy et Tunnel par application sont installés sur le même serveur de relais.

Figure 4-11. Configuration sur site pour les déploiements de point de terminaison relais

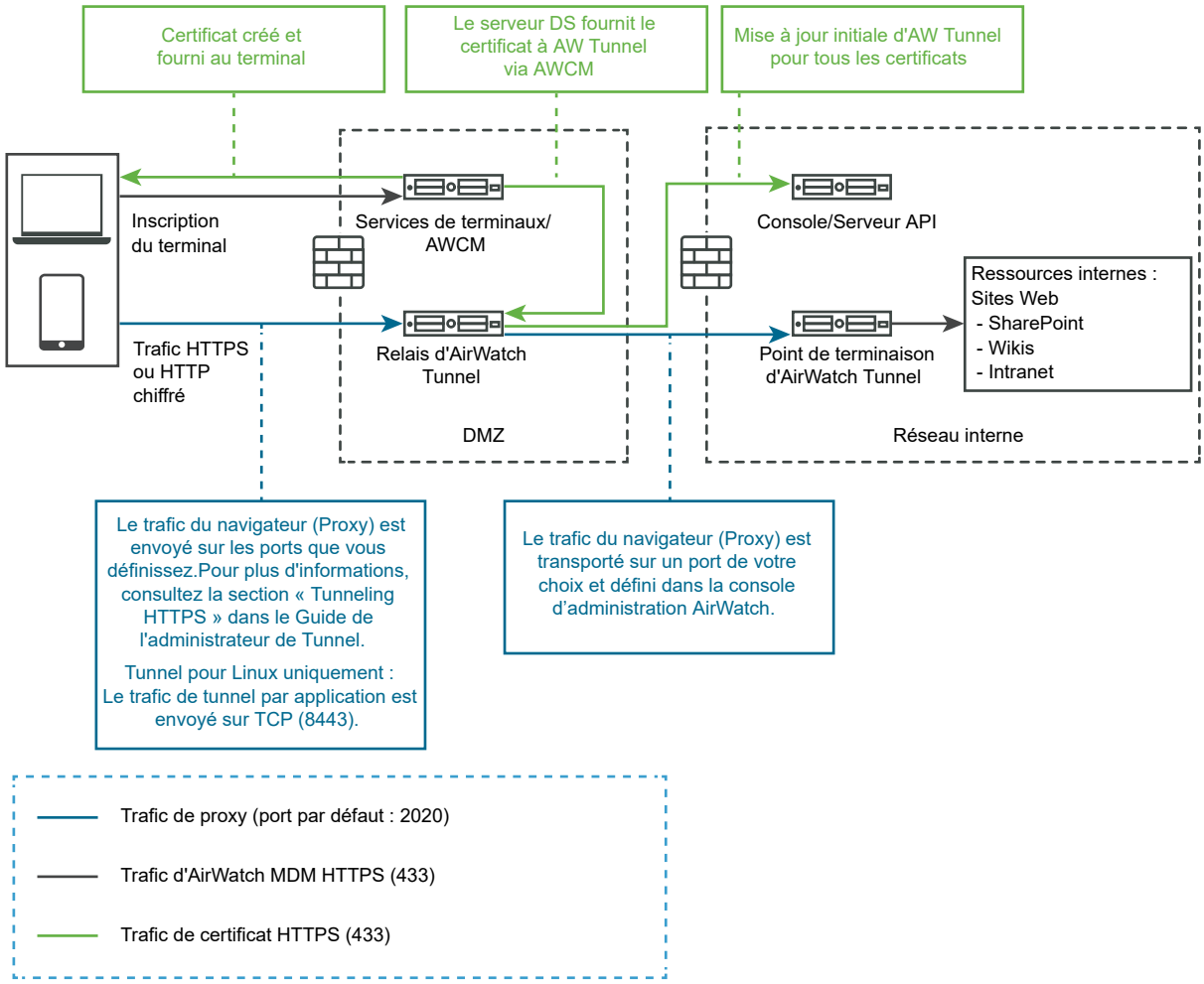
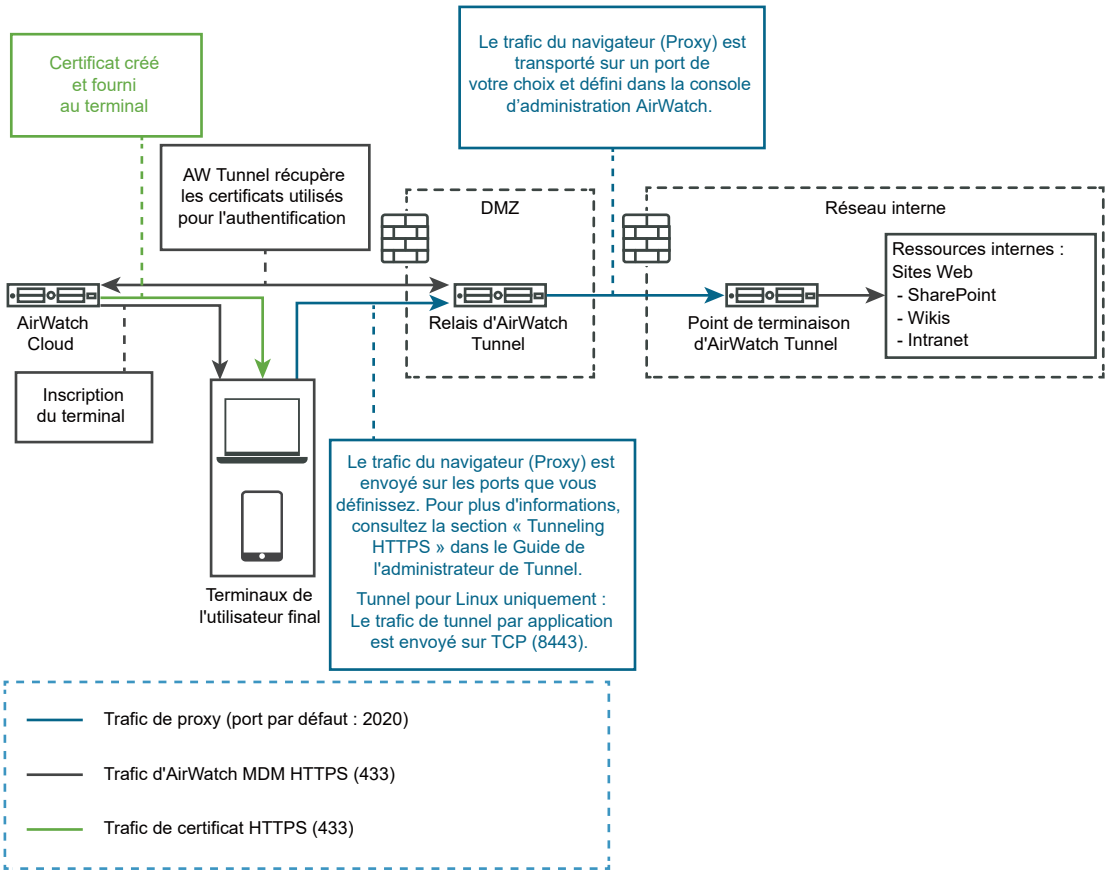


Figure 4-12. Configuration SaaS pour les déploiements de point de terminaison relais



Configurer les paramètres de VMware Tunnel pour Workspace ONE UEM

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

Procédure

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

2 Accédez à **Paramètres généraux > Paramètres du service Edge** et 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 API Workspace ONE UEM. Par exemple, entrez-la sous la forme *https://example.com:<port>*.
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 de groupe de l'organisation	Entrez l'organisation de l'utilisateur.
Nom d'hôte du serveur du tunnel	Entrez le nom d'hôte externe de VMware Tunnel configuré dans la console Workspace ONE UEM.

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. **Note** 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 NON par **OUI** 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 depuis la console Workspace ONE UEM.

Option	Description
Entrées de l'hôte	Entrez les détails qui doivent être ajoutés 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`**. Pour ajouter plusieurs entrées de l'hôte, cliquez sur le signe « + ». **Important** Les entrées de l'hôte sont enregistrées uniquement après avoir cliqué sur **Enregistrer**.
Certificats approuvés	Sélectionnez les fichiers de certificat approuvés (au format PEM) à ajouter au magasin d'approbations. Par défaut, le nom d'alias est le nom de fichier du certificat PEM. Modifiez la zone de texte de l'alias afin de donner un nom différent à l'alias.

7 Cliquez sur **Enregistrer**.

Déploiement de VMware Tunnel pour Workspace ONE UEM à l'aide de PowerShell

Vous pouvez utiliser PowerShell pour déployer VMware Tunnel pour Workspace ONE UEM.

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

(Déploiement de VMware Tunnel avec PowerShell)

À propos du partage de port TLS

Le partage de port TLS est activé par défaut sur Unified Access Gateway chaque fois que plusieurs services Edge sont configurés pour utiliser le port TCP 443. Les services Edge pris en charge sont VMware Tunnel (VPN par application), Content Gateway, Secure Email Gateway et proxy inverse Web.

Note Si vous souhaitez que le port TCP 443 soit partagé, veillez à ce que chaque service Edge configuré possède un nom d'hôte externe unique pointant vers Unified Access Gateway.

Content Gateway sur Unified Access Gateway

Content Gateway (CG) est un composant de la solution de gestion de contenu de Workspace ONE UEM qui permet d'accéder en toute sécurité au contenu du référentiel sur site sur des terminaux mobiles.

Conditions préalables

Vous devez configurer le nœud Content Gateway à l'aide de la console Workspace ONE UEM avant de pouvoir configurer Content Gateway sur Unified Access Gateway. Après avoir configuré le nœud, notez la valeur *GUID de configuration de Content Gateway*, qui est générée automatiquement.

Note L'acronyme CG est également utilisé pour faire référence à Content Gateway.

Procédure

1 Accédez à **Paramètres généraux > Paramètres du service Edge > Paramètres Content Gateway** et cliquez sur l'icône d'engrenage.

2 Sélectionnez **OUI** pour activer les paramètres Content Gateway.

3 Configurer les paramètres suivants

Option	Description
Identifiant	Indique que ce service est activé.
URL du serveur API	URL du serveur API Workspace ONE UEM `[http[s]://]hostname[:port]` L'URL de destination doit contenir le protocole, le nom d'hôte ou l'adresse IP et le numéro de port. Par exemple : `https://load-balancer.example.com:8443` Unified Access Gateway extrait la configuration de Content Gateway du serveur API.
Nom d'utilisateur du serveur API	Nom d'utilisateur pour se connecter au serveur API. **Note** Il est nécessaire que le compte d'administrateur dispose, au minimum, d'autorisations associées au rôle Content Gateway
Mot de passe du serveur API	Mot de passe pour se connecter au serveur API.
Nom d'hôte CG	Nom d'hôte utilisé pour configurer des paramètres Edge.
GUID de configuration CG	ID de configuration de Workspace ONE UEM Content Gateway. Cet ID est généré automatiquement lorsque Content Gateway est configuré sur la console Workspace ONE UEM. Le GUID de configuration s'affiche sur la page Content Gateway dans UEM Console sous **Paramètres > Contenu > Content Gateway**.
Hôte de proxy sortant	Hôte sur lequel le proxy sortant est installé. Unified Access Gateway établit une connexion au serveur API via un proxy sortant si configuré.
Port de proxy sortant	Port du proxy sortant.
Nom d'utilisateur de proxy sortant	Nom d'utilisateur pour se connecter au proxy sortant.
Mot de passe de proxy sortant	Mot de passe pour se connecter au proxy sortant.
Authentification NTLM	Spécifiez si le proxy sortant requiert l'authentification NTLM.

Option	Description
Certificats approuvés	Ajoutez un certificat approuvé à ce service Edge. Cliquez sur le signe « + » pour sélectionner un certificat au format PEM et l'ajouter au magasin des approbations. Cliquez sur '-' pour supprimer un certificat du magasin de confiance. Par défaut, le nom d'alias est le nom de fichier du certificat PEM. Modifiez la zone de texte de l'alias afin de donner un nom différent à l'alias.
Entrées de l'hôte	Entrez les détails qui doivent être ajoutés 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`**. Cliquez sur le signe « + » pour ajouter plusieurs entrées de l'hôte. **Important** Les entrées de l'hôte sont enregistrées uniquement après avoir cliqué sur **Enregistrer**.

Note Le trafic HTTP n'est pas autorisé pour Content Gateway sur le port 80 sur Unified Access Gateway, car le port TCP 80 est utilisé par Edge Service Manager.

4 Cliquez sur **Enregistrer**.

Configuration de Content Gateway

Configurez les paramètres Content Gateway dans Workspace ONE UEM Console pour établir un nœud et préconfigurez les paramètres intégrés dans le fichier de configuration. Cela évite de configurer manuellement les paramètres après l'installation sur le serveur.

La configuration comprend la sélection de la plate-forme, du modèle de configuration, des ports associés, et si nécessaire, le téléchargement d'un certificat SSL.

À partir de Workspace ONE UEM Console version 9.6 et version ultérieure, Unified Access Gateway (UAG) est le type d'installation recommandé lors de la configuration du nœud de Content Gateway. Cette option permet de configurer une nouvelle instance de Content Gateway sur Unified Access Gateway ou de migrer votre instance existante de Content Gateway vers Unified Access Gateway.

Pour plus d'informations sur la configuration de Content Gateway sur Unified Access Gateway, reportez-vous aux composants de Workspace ONE UEM sur Unified Access Gateway dans la documentation d'UAG. Pour plus d'informations sur la migration, reportez-vous à la documentation Migration de Content Gateway vers Unified Access Gateway.

Pour plus d'informations sur les valeurs personnalisées de Content Gateway, reportez-vous à la documentation de *Content Gateway* dans le cadre de la *Documentation de Workspace ONE UEM* dans VMware Docs.

Procédure

1 Accédez à **Groupes et paramètres > Tous les paramètres > Système > Intégration d'entreprise > Content Gateway** dans le groupe d'organisation de votre choix.

2 Définissez **Activer Content Gateway** sur **Activé**.

Vous devrez peut-être sélectionner **Remplacer** pour déverrouiller les paramètres Content Gateway.

3 Cliquez sur **Ajouter**.

4 Remplissez les champs qui s'affichent pour configurer une instance de Content Gateway.

a Configurez le **type d'installation**.

Paramètre	Description
Type d'installation	Sélectionnez le système d'exploitation du serveur Content Gateway.

b Configurez les paramètres de **Configuration de Content**.

Paramètre	Description
Type de configuration	■ **De base** : configuration du point de terminaison sans composant de relais. ■ **Relais** : configuration du point de terminaison avec un composant de relais.
Nom	Indiquez un nom unique utilisé pour sélectionner cette instance de Content Gateway lors de son attachement à un référentiel de Content, un modèle de référentiel ou un nœud RFS.
Adresse de relais Content Gateway	Si vous implémentez une configuration de relais, entrez l'URL permettant d'accéder au relais Content Gateway à partir d'Internet.
Port de relais Content Gateway	Si vous implémentez une configuration de relais, entrez le port du serveur de relais.
Adresse de point de terminaison Content Gateway	Entrez le nom d'hôte du point de terminaison Content Gateway. Le certificat SSL public lié au port configuré doit être valide pour cette entrée.
Port de point de terminaison Content Gateway	Entrez le port du serveur de point de terminaison.

c Configurez les paramètres du **Certificat SSL de Content**.

Paramètre	Description
Certificat SSL public (requis pour les exigences Linux)	Si nécessaire, téléchargez un fichier de certificat PKCS12 (.pfx) avec une chaîne complète du programme d'installation de Content Gateway à lier au port. La chaîne complète comprend un mot de passe, un certificat de serveur, des certificats intermédiaires, un certificat racine et une clé privée. **Note** Pour vérifier que votre fichier PFX contient la chaîne de certificats entière, vous pouvez exécuter des commandes, telles que `certutil -dump myCertificate.pfx` ou `openssl pkcs12 -in myCertificate.pfx -nokeys` à l'aide d'outils de ligne de commande, tels que Certutil ou OpenSSL. Ces commandes affichent les informations complètes du certificat. Les exigences varient selon la plate-forme et la configuration SSL.
Ignorer les erreurs SSL (non recommandé)	Si vous utilisez un certificat auto-signé, pensez à activer cette fonctionnalité. Si vous l'activez, Content Gateway ignore les erreurs d'approbation de certificat et les conflits de noms de certificat.

Les configurations du proxy ICAP ne sont pas prises en charge depuis Workspace ONE UEM Console version 9.7. Vous pouvez, cependant, modifier les configurations existantes. Pour plus d'informations sur la configuration du proxy ICAP, reportez-vous à https://support.workspaceone.com/articles/115001675368.

5 Sélectionnez **Ajouter**.

6 Sélectionnez **Enregistrer**.

Étape suivante

Lors de la configuration, vous spécifiez le modèle de plate-forme et de configuration pour Content Gateway. Après avoir configuré les paramètres dans UEM Console, téléchargez le programme d'installation, configurez les nœuds supplémentaires ou gérez les nœuds configurés.

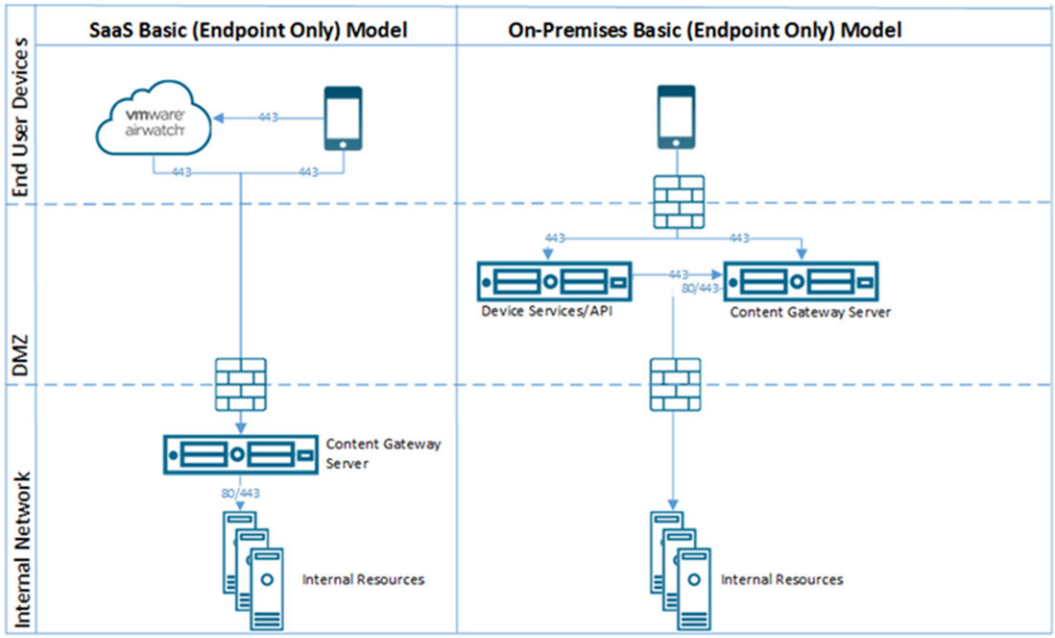
Modèle de déploiement (point de terminaison uniquement) de base pour Content Gateway

Le modèle de déploiement de point de terminaison de base de VMware Content Gateway est une instance unique du produit installé sur un serveur avec un DNS disponible publiquement.

Dans le modèle de déploiement de base, VMware Content Gateway est généralement installé sur le réseau interne derrière un équilibrage de charge dans la zone DMZ qui transfère le trafic sur les ports configurés vers VMware Content Gateway. VMware Content Gateway se connecte ensuite directement à vos référentiels de Content internes. Toutes les configurations de déploiement prennent en charge l'équilibrage de charge et le proxy inverse.

Le serveur Content Gateway de point de terminaison de base communique avec les services de terminaux. Ceux-ci connectent le terminal de l'utilisateur final à l'instance appropriée de Content Gateway.

Si le point de terminaison de base est installé dans la zone DMZ, les modifications réseau appropriées doivent être effectuées pour que VMware Content Gateway accède à diverses ressources internes sur les ports nécessaires. L'installation de ce composant derrière un équilibrage de charge dans la zone DMZ minimise le nombre de modifications réseau pour implémenter VMware Content Gateway. Il fournit une couche de sécurité, car le DNS public n'est pas pointé directement vers le serveur qui héberge VMware Content Gateway.



Modèle de déploiement de point de terminaison relais pour Content Gateway

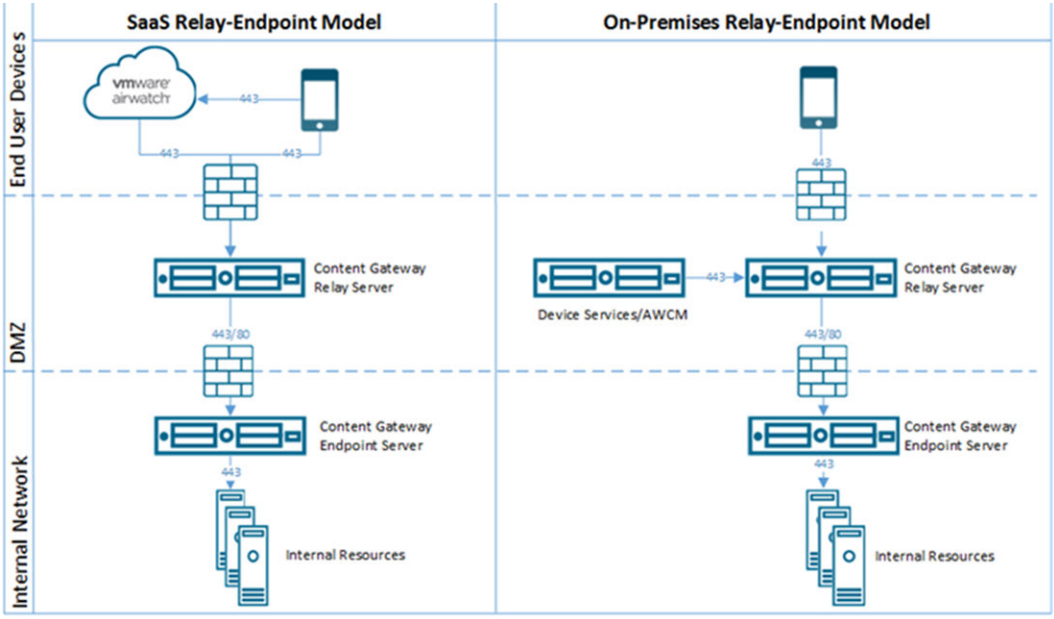
L'architecture de modèle de déploiement de point de terminaison relais comprend deux instances de VMware Content Gateway avec des rôles distincts.

Le serveur de relais VMware Content Gateway réside dans la zone DMZ et est accessible depuis le DNS public sur les ports configurés.

Par défaut, 443 est le port d'accès à Content Gateway. Le serveur de point de terminaison VMware Content Gateway est installé sur le réseau interne hébergeant les ressources internes. Ce serveur doit disposer d'un enregistrement DNS interne que le serveur de relais peut résoudre. Ce modèle de déploiement sépare le serveur disponible publiquement du serveur qui se connecte directement à des ressources internes, fournissant ainsi une couche supplémentaire de sécurité.

Le rôle du serveur de point de terminaison consiste à se connecter au contenu ou au référentiel interne demandé par le terminal. Le serveur de relais exécute des contrôles de la santé à intervalles réguliers pour s'assurer que le point de terminaison est actif et disponible.

Ces composants peuvent être installés sur des serveurs partagés ou dédiés. Pour vous assurer que les autres applications exécutées sur le même serveur n'affectent pas les performances, installez VMware Content Gateway sur des serveurs dédiés.



Secure Email Gateway sur Unified Access Gateway

Secure Email Gateway est un composant de Workspace ONE UEM qui aide à protéger votre infrastructure de messagerie et active la fonctionnalité de gestion des e-mails mobiles (MEM, Mobile Email Management).

Conditions préalables

Vous devez configurer Secure Email Gateway à l'aide de Workspace ONE UEM Console avant de pouvoir configurer Secure Email Gateway sur Unified Access Gateway. Après avoir configuré le nœud, notez le GUID de configuration de Secure Email Gateway, qui est généré automatiquement. Pour plus d'informations, consultez la documentation de Secure Email Gateway.

Note L'acronyme SEG est également utilisé pour faire référence à Secure Email Gateway.

Note

- Secure Email Gateway est pris en charge par toutes les versions d'Unified Endpoint Management (UEM).
- Secure email Gateway est configuré pour suivre les configurations Syslog configurées dans le cadre des paramètres système du dispositif Unified Access Gateway. Par défaut, seul le contenu du fichier app.log dans Secure email Gateway sera déclenché en tant qu'événements Syslog. Pour plus d'informations, consultez la section Paramètres système d'Unified Access Gateway.

Procédure

1 Accédez à **Paramètres généraux >Paramètres du service Edge > Paramètres de Secure Email Gateway** et cliquez sur l'icône en forme d'engrenage.

2 Sélectionnez **OUI** pour activer les paramètres de Secure Email Gateway.

3 Configurez les paramètres suivants.

Option	Valeur par défaut et description
URL du serveur API	URL du serveur API Workspace ONE UEM `[http[s]://]hostname[:port]` L'URL de destination doit contenir le protocole, le nom d'hôte ou l'adresse IP et le numéro de port. Par exemple : `https://load-balancer.example.com:8443` Unified Access Gateway récupère la configuration de Secure Email Gateway depuis le serveur API.
Nom d'utilisateur du serveur API	Nom d'utilisateur pour se connecter au serveur API. **Note** Il est nécessaire que le compte d'administrateur dispose, au minimum, d'autorisations associées au rôle Secure Email Gateway.
Mot de passe du serveur API	Mot de passe pour se connecter au serveur API.
Nom d'hôte du serveur Secure Email Gateway	Nom d'hôte utilisé pour configurer des paramètres Edge.
GUID de configuration MEM	ID de configuration de gestion des e-mails mobiles de Workspace ONE UEM. Cet ID est généré automatiquement lorsque la gestion des e-mails mobiles est configurée sur la console Workspace ONE UEM Console. Le GUID de configuration est affiché sur la page de configuration de la gestion des e-mails mobiles sur la console UEM.
Ajouter un certificat SSL	Basculez pour ajouter un certificat SSL si l'option de chargement local du certificat SSL est activée sous Paramètres d'e-mail dans UEM Console.
Certificat SSL	Cliquez sur Sélectionner pour télécharger un fichier de certificat .PFX ou .P12. **Note** Vous pouvez également charger le certificat SSL dans Workspace ONE UEM Console. Lorsque le certificat est téléchargé localement, l'empreinte numérique du certificat s'affiche sur l'interface utilisateur graphique d'administration.
Mot de passe	Entrez le mot de passe du certificat SSL.
Hôte de proxy sortant	Hôte sur lequel le proxy sortant est installé. Unified Access Gateway établit une connexion au serveur API via un proxy sortant si configuré.
Port de proxy sortant	Port du proxy sortant.
Nom d'utilisateur de proxy sortant	Nom d'utilisateur pour se connecter au proxy sortant.
Mot de passe de proxy sortant	Mot de passe pour se connecter au proxy sortant.

Option	Valeur par défaut et description
Certificats approuvés	Ajoutez un certificat approuvé à ce service Edge. Cliquez sur le signe « + » pour sélectionner un certificat au format PEM et l'ajouter au magasin des approbations. Cliquez sur '-' pour supprimer un certificat du magasin de confiance. Par défaut, le nom d'alias est le nom de fichier du certificat PEM. Modifiez la zone de texte de l'alias afin de donner un nom différent à l'alias.
Entrées de l'hôte	Entrez les détails qui doivent être ajoutés 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. Cliquez sur le signe « + » pour ajouter plusieurs entrées de l'hôte. **Note** Les entrées de l'hôte sont enregistrées uniquement après avoir cliqué sur **Enregistrer**.

4 Cliquez sur **Enregistrer**.

Modification des niveaux de journalisation pour Secure Email Gateway sur Unified Access Gateway

Vous pouvez modifier les niveaux de journal pour Secure Email Gateway dans Unified Access Gateway.

Conditions préalables

Activez SSH sur la machine virtuelle Linux, si ce n'est pas déjà fait.

Procédure

1 Connectez-vous à la machine Secure Email Gateway dans Unified Access Gateway à l'aide de Secure Shell.

2 Modifiez le fichier de configuration du journal pour SEG à l'aide de la commande.

```
vi /opt/vmware/docker/seg/container/config/logback.xml
```

3 Recherchez une journalisation appropriée pour laquelle vous souhaitez modifier le niveau de journalisation. Par exemple, `logger name="com.airwatch" groupKey="app.logger" level="error"`

4 Remplacez la valeur de l'attribut `level` de `error` par n'importe quel niveau, tel que `warn`, `Info`, `Debug`.

5 Enregistrez le fichier.

Résultats

La modification du niveau de journalisation est reflétée dans les journaux.

Activer le proxy EWS sur SEG

SEG fournit une autorisation et une conformité pour le trafic Exchange Web Services (EWS) utilisé par VMware Email Notification Service (ENS).

La procédure suivante décrit les étapes pour activer le proxy EWS sur Secure email Gateway.

Procédure

1. Connectez-vous à la machine Secure Email Gateway dans Unified Access Gateway à l'aide de Secure Shell.
2. Modifiez le fichier de propriétés à l'aide de la commande suivante

   ```
   vi /opt/vmware/docker/seg/container/config/override/application-override.properties
   ```

3. Ajoutez l'entrée dans le fichier `application-override.properties`.

   ```
   enable.boxer.ens.ews.proxy=true
   ```

4. Enregistrez le fichier.
5. Enregistrez à nouveau la configuration de SEG sur l'interface utilisateur d'administration d'Unified Access Gateway.

Cas d'utilisation pour un déploiement supplémentaire

Vous pouvez déployer Unified Access Gateway avec plusieurs services Edge sur le même dispositif, comme avec Horizon et un proxy inverse Web et Unified Access Gateway avec VMware Tunnel, Content Gateway et un proxy inverse Web.

Éléments à prendre en compte pour le déploiement de Unified Access Gateway avec plusieurs services

Notez les points importants suivants avant de déployer les services edge ensemble.

- Comprenez et respectez les exigences de mise en réseau - reportez-vous à la section Règles de pare-feu pour les dispositifs Unified Access Gateway basés sur une zone DMZ.
- Suivez les instructions de dimensionnement - voir la section sur les options de dimensionnement dans la rubrique Déploiement d'Unified Access Gateway au moyen de l'assistant de modèle OVF.
- Horizon Connection Server ne fonctionne pas avec un proxy inverse Web activé lorsqu'un chevauchement existe dans le modèle de proxy. Ainsi, si Horizon et une instance de serveur inverse Web sont configurés et activés avec des modèles de proxy sur la même instance Unified Access Gateway, supprimez le modèle de proxy « / » des paramètres d'Horizon et conservez le modèle dans le proxy inverse Web afin d'empêcher le chevauchement. Conserver le modèle de proxy « / » dans l'instance du proxy inverse Web permet de garantir que lorsqu'un utilisateur clique sur l'URL d'Unified Access Gateway, la page appropriée du proxy inverse Web s'affiche. Si seuls les paramètres Horizon sont configurés, le changement ci-dessus n'est pas nécessaire.

- Lorsque vous déployez Unified Access Gateway avec les services combinés de VMware Tunnel, Content Gateway, Secure Email Gateway et un proxy inverse Web, si vous utilisez le même port 443 pour tous les services, chaque service doit avoir un nom d'hôte externe unique. Reportez-vous à la section À propos du partage de port TLS.
- Les différents services Edge peuvent être configurés indépendamment à l'aide de l'interface utilisateur d'administration et vous pouvez importer les paramètres précédents si vous le souhaitez. Lorsque vous effectuez le déploiement avec PowerShell, le fichier INI rend le déploiement prêt pour la production.
- Si Horizon Blast et VMware Tunnel sont activés sur le même dispositif Unified Access Gateway, vous devez configurer VMware Tunnel pour utiliser un autre numéro de port autre que 443 ou 8443. Si vous souhaitez utiliser le port 443 ou 8443 pour VMware Tunnel, vous devez déployer le service Horizon Blast sur un dispositif Unified Access Gateway distinct.

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.

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

Lisez les sections suivantes :

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

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.

Note 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.

Conditions préalables

- 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. Pour afficher le format de la liste de chiffrements, vous pouvez rechercher « openssl cipher string » dans un navigateur Web.
- 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` (certificat et clé) en une valeur pouvant être transmise dans une chaîne JSON à la REST API 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

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.

Résultats

Vous pouvez désormais 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 Unified Access Gateway » (Utilisation de PowerShell pour déployer VMware Unified 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.

Étape suivante

Vous pouvez remplacer le certificat auto-signé par défaut par un certificat signé par une autorité de certification. Reportez-vous à la section Mise à jour des certificats signés du serveur SSL. 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.

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 v1.2 est activé. TLS v1.0, TLS v1.1 et SSL v3.0 sont désactivés.

Conditions préalables

- 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`, `ssl30Disabled`, `tls10Enabled`, `tls11Disabled` 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_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_RSA_
   WITH_AES_128_CBC_SHA256
   , TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384",
     "ssl30Enabled": "false",
     "tls10Enabled": "false",
     "tls11Enabled": "false",
     "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.

Résultats

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.

Note Seule l'une des méthodes d'authentification à deux facteurs de l'utilisateur peut être spécifiée pour un Service Edge. Cela peut être l'authentification par certificat/carte à puce, l'authentification RADIUS ou RSA adaptive Authentication.

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

Lisez les sections suivantes :

- Configuration de l'authentification par certificat ou carte à puce sur le dispositif Unified Access Gateway
- Configurer l'authentification RSA SecurID dans Unified Access Gateway
- Configuration de RADIUS pour Unified Access Gateway
- Configuration de RSA Adaptive Authentication dans Unified Access Gateway
- Générer des métadonnées SAML Unified Access Gateway

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 Horizon 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 l'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.

Note Le contrôle de la révocation ne revient pas à OCSP en cas d'échec de la CRL.

Note Pour Workspace ONE Access, l'authentification est toujours transmise via Unified Access Gateway au service Workspace ONE Access. 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.

Conditions préalables

- 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.

- 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 l'interface utilisateur d'administration d'Unified Access Gateway, accédez à la section **Configurer manuellement**, puis cliquez sur **Sélectionner**.

2 Sous **Paramètres généraux > Paramètres d'authentification**, cliquez sur **Afficher**.

3 Cliquez sur l'icône en forme d'engrenage 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.
* **Certificats d'autorité de certification racine et intermédiaire**	Pour charger les fichiers du certificat, cliquez sur **Sélectionner**. Il est possible de sélectionner plusieurs certificats d'autorité de certification racine et intermédiaire qui utilisent l'encodage DER ou PEM. **Note** Si plusieurs certificats avec le même nom de domaine sont chargés, le dernier certificat chargé remplace le certificat existant. Par conséquent, plusieurs certificats portant le même nom de domaine ne peuvent pas coexister dans Unified Access Gateway.
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.

Option	Description
URL d'OCSP	Si vous avez activé la révocation OCSP, entrez l'adresse de serveur OCSP pour le contrôle de la révocation.
Utiliser l'URL OCSP du certificat	Cochez cette case pour utiliser l'URL OCSP.
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.

5 Cliquez sur **Enregistrer**.

Étape suivante

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'e l'équilibrage de charge 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. 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.

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.

Étape suivante

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.

Étape suivante

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.

Conditions préalables

- 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. **Note** 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.

Option	Action
*Nom d'HÔTE interne	Entrez la valeur attribuée à l'invite **Adresse IP** sur le serveur RSA SecurID.
*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 `sdconf.rec`.
*Suffixe d'ID de nom	Entrez le nameId tel que *@somedomain.com*. Est utilisé pour envoyer du contenu supplémentaire comme le nom de domaine pour le serveur RADIUS ou le serveur RSA SecurID. Par exemple, si un utilisateur ouvre une session en tant que *user1*, *user1@somedomain.com* est envoyé au serveur.

Configuration de RADIUS pour Unified Access Gateway

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

La prise en charge de RADIUS offre une large gamme d'options d'authentification à deux facteurs de tiers. Pour utiliser l'authentification RADIUS dans Unified Access Gateway, vous devez disposer d'un serveur RADIUS configuré accessible sur le réseau depuis Unified Access Gateway.

Lorsque les utilisateurs se connectent et que l'authentification RADIUS est activée, les utilisateurs entrent leur nom d'utilisateur et code secret de l'authentification RADIUS dans la boîte de dialogue de connexion. Si le serveur RADIUS génère un challenge d'accès RADIUS, Unified Access Gateway affiche une seconde boîte de dialogue et invite l'utilisateur à saisir le texte Stimulation/Réponse. Cela peut être un code communiqué à l'utilisateur via un texte SMS ou un autre mécanisme hors bande. La prise en charge de la saisie du code secret RADIUS et de la saisie de Stimulation/Réponse est uniquement limitée à la saisie basée sur le texte. La saisie du texte Stimulation/Réponse correct termine l'authentification.

Si le serveur RADIUS requiert que l'utilisateur entre son mot de passe Active Directory comme code secret RADIUS, pour utiliser Horizon, l'administrateur peut activer la fonctionnalité Single Sign-On Windows d'Horizon dans Unified Access Gateway. De cette façon, une fois que l'authentification est terminée, l'utilisateur n'est pas invité à entrer à nouveau le même mot de passe du domaine Active Directory.

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.

Conditions préalables

- 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.

Option	Action
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 tel que *@somedomain.com*. Est utilisé pour envoyer du contenu supplémentaire comme le nom de domaine pour le serveur RADIUS ou le serveur RSA SecurID. Par exemple, si un utilisateur ouvre une session en tant que *user1*, *user1@somedomain.com* est envoyé au serveur.
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 la validation MS-CHAPv2 de base	Remplacez NO par **YES** pour activer la validation de base de MS-CHAPv2. Si cette option est définie sur **YES**, la validation supplémentaire de la réponse du serveur RADIUS est ignorée. Par défaut, la validation complète sera effectuée.
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.

Note 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.

Conditions préalables

- 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.

Note 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.

Option	Description
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.
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.

Conditions préalables

- 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.

  Note 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.

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 SAML**.
3. Cliquez sur la section **Paramètres du fournisseur d'identité SAML**.
4. Sélectionnez **Fournir un certificat**.
5. Pour ajouter le fichier de clé privée, cliquez sur **Sélectionner** et accédez au fichier de clé privée du certificat.
6. Pour ajouter le fichier de chaîne de certificat, cliquez sur **Sélectionner** et accédez au fichier de chaîne de certificat.
7. Cliquez sur **Enregistrer**.
8. 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 Air, 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 Horizon Connection Server.

Conditions préalables

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 différents fournisseurs de services ont des procédures distinctes. 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**.

Résultats

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.

Lisez les sections suivantes :

Surveillance des statistiques de session de service Edge

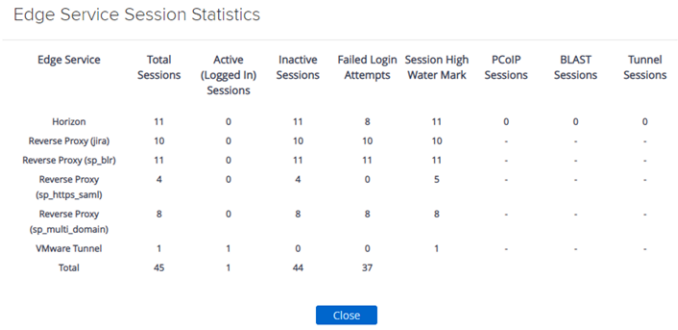
Unified Access Gateway fournit des informations sur les sessions actives de chaque service Edge. Vous pouvez voir rapidement que les services que vous avez déployés sont configurés, actifs et en cours d'exécution à partir de l'interface utilisateur d'administration du service Edge.

Procédure

1 Accédez à **Paramètres de prise en charge** > **Statistiques de session de service Edge**.

2 Dans la section **Paramètres de prise en charge**, cliquez sur l'icône en forme d'engrenage **Statistiques de session de service Edge**.

Figure 7-1. Statistiques de session de service Edge



- Le **Service Edge** répertorie le service Edge spécifique pour lequel les statistiques de la session s'affichent.
- Le **Nombre total de sessions** indique la somme des sessions actives et inactives.
- Les **Sessions actives(Sessions connectées)** indiquent le nombre de sessions authentifiées en cours.
- Les **Sessions inactives** indiquent le nombre de sessions non authentifiées.
- Les **Tentatives de connexion échouées** indiquent le nombre de tentatives de connexion échouées.
- Le **Seuil supérieur de sessions** indique le nombre maximal de sessions simultanées à un moment précis donné.
- Les **Sessions PCoIP** indiquent le nombre de sessions établies à l'aide de PCoIP.
- Les **Sessions BLAST** indiquent le nombre de sessions établies à l'aide de Blast.
- Les **Sessions de tunnel** indiquent le nombre de sessions établies à l'aide d'Horizon Tunnel.

Tableau 7-1. Exemple de statistiques de session de service Edge

Service Edge	Nombre total de sessions	Sessions (connectées) actives	Sessions inactives	Tentatives de connexion échouées	Seuil supérieur de sessions	Sessions PCoIP	Sessions BLAST	Sessions de tunnel
Horizon	11	0	11	8	11	0	0	0
Proxy inverse (jira)	10	0	10	10	10	-	-	-
Proxy inverse (sp_blr)	11	0	11	11	11	-	-	-
Proxy inverse (sp_https_saml)	4	0	4	0	5	-	-	-
Proxy inverse (sp_multi_domain)	8	0	8	8	8	-	-	-
VMware Tunnel	1	1	0	0	1	-	-	-
Total	45	1	44	37		-	-	-

Surveiller l'API de statistiques de session

Les paramètres répertoriés ici décrivent les statistiques de session capturées lors du dernier intervalle de surveillance.

Appel d'URL : `https://<UAGIP>:9443/rest/v1/monitor/stats`

Tableau 7-2. Horizon View

Attribut	Description
`totalSessions`	Indique la somme des sessions actives et inactives. Interface utilisateur d'administration : **Total de Sessions** .
`highWaterMarkOfSessions`	Indique le nombre maximal de sessions simultanées à un moment donné. Interface utilisateur d'administration : **Seuil supérieur de sessions**.
`authenticatedSessions`	Indique le nombre de sessions authentifiées en cours (sessions connectées). Interface utilisateur d'administration : **Sessions actives (connectées)**.
`unauthenticatedSessions`	Indique le nombre de sessions non authentifiées. Interface utilisateur d'administration : **Sessions inactives**.
`failedLoginAttempts`	Indique le nombre de tentatives de connexion infructueuses. Interface utilisateur d'administration : **Tentatives infructueuses de connexion**

Tableau 7-2. Horizon View (suite)

Attribut	Description
`userCount`	Indique le nombre d'utilisateurs uniques actuellement authentifiés.
BLAST	
`sessions`	Indique le nombre de sessions BLAST actives.
`maxSessions`	Indique le nombre de sessions BLAST autorisées.
PCoIP	
`sessions`	Indique le nombre de sessions PCoIP actives créées pendant le démarrage d'une application ou d'un poste de travail.
`maxSessions`	Indique le nombre maximal de sessions PCoIP simultanées à un moment donné.
VMware Tunnel	
`sessions`	Indique le nombre de sessions VMware Tunnel actives créées à l'authentification via View Client.
`maxSessions`	Indique le nombre maximal de sessions VMware Tunnel simultanées à un moment donné.

Tableau 7-3. Proxy inverse Web

Attribut	Description
`totalSessions`	Indique la somme des sessions actives et inactives. Interface utilisateur d'administration : **Total de Sessions** .
`highWaterMarkOfSessions`	Indique le nombre maximal de sessions simultanées à un moment donné. Interface utilisateur d'administration : **Seuil supérieur de sessions**.
`authenticatedSessions`	Indique le nombre de sessions authentifiées en cours (sessions connectées). Interface utilisateur d'administration : **Sessions actives (connectées)**.
`unauthenticatedSessions`	Indique le nombre de sessions non authentifiées. Interface utilisateur d'administration : **Sessions inactives**.
`failedLoginAttempts`	Indique le nombre de tentatives de connexion infructueuses. Interface utilisateur d'administration : **Échec des tentatives de connexion** .
`userCount`	Indique le nombre d'utilisateurs uniques actuellement authentifiés.
backendStatus	
`status`	Indique si l'application principale est accessible. (En cours d'exécution, non accessible)
`reason`	Indique et explique l'état avec la raison. (Accessible, détails de l'erreur)
kcdStatus	
`status`	Indique si le serveur de kcd est accessible. (En cours d'exécution, non accessible)
`reason`	Indique et explique l'état avec la raison. (Accessible, détails de l'erreur)

Tableau 7-4. VMware Tunnel

Attribut	Description
`identifier`	Indique que le service VMware Tunnel est activé.
`status`	État du service VMware Tunnel (service `vpnd`).
`reason`	Indique et explique l'état et la raison pour le service VMware Tunnel. Les étiquettes Actif ou Inactif indiquent l'état du service. Par exemple, il est accessible lorsque le service est actif et en cours d'exécution, le serveur VMware Tunnel n'est pas accessible lorsque le service est inactif.
`totalSessions`	Indique le nombre de sessions VMware Tunnel actives créées à l'authentification via le client VMware Tunnel.
`connections`	Indique le nombre de connexions sortantes actives depuis le serveur VMware Tunnel.
`upTime`	Indique la durée active (d'exécution) du service VMware Tunnel.
`apiConnectivity`	Connectivité du serveur VMware Tunnel à l'API. Par exemple, True ou False.
`awcmConnectivity`	Connectivité du serveur VMware Tunnel à AWCM. Par exemple, True ou False.
`cascadeMode`	Fournit des informations en cascade. Par exemple, Désactivé pour le mode de base et frontal ou principal pour une configuration en cascade.

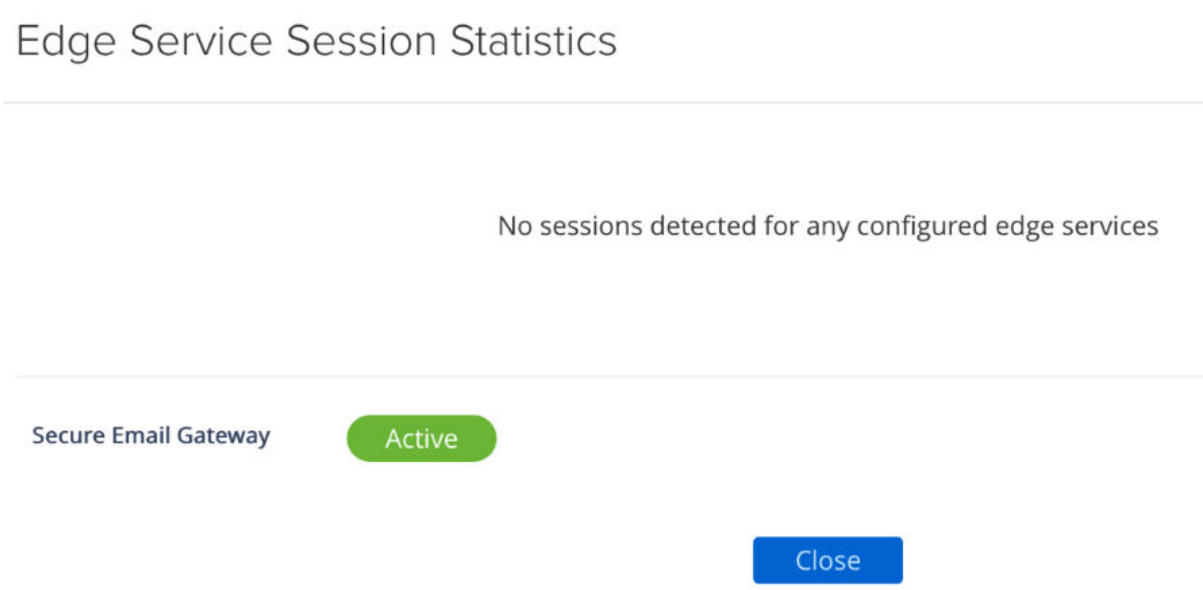
Surveillance de la santé et des diagnostics de SEG

Vous pouvez utiliser la page d'administration de SEG V2 pour surveiller la santé et les diagnostics de SEG.

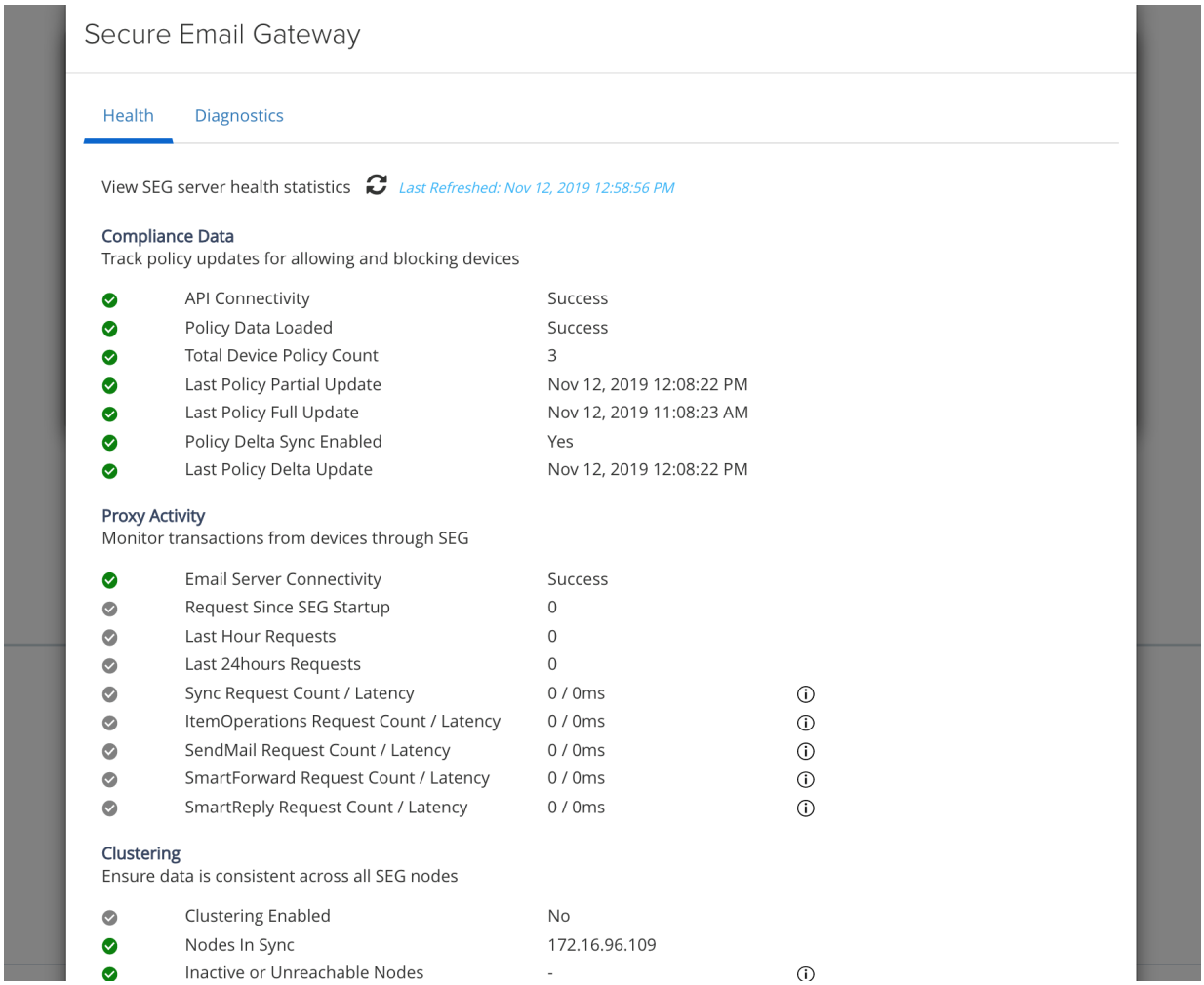
La procédure suivante décrit les étapes à suivre pour afficher les informations de santé et de diagnostics de SEG.

1 Accédez à **Paramètres de prise en charge > Statistiques de session de service Edge**.

2 Cliquez sur l'icône d'engrenage **Statistiques de session de service Edge**, dans la section **Paramètres de prise en charge**. Si SEG est activé, l'écran suivant s'affiche.



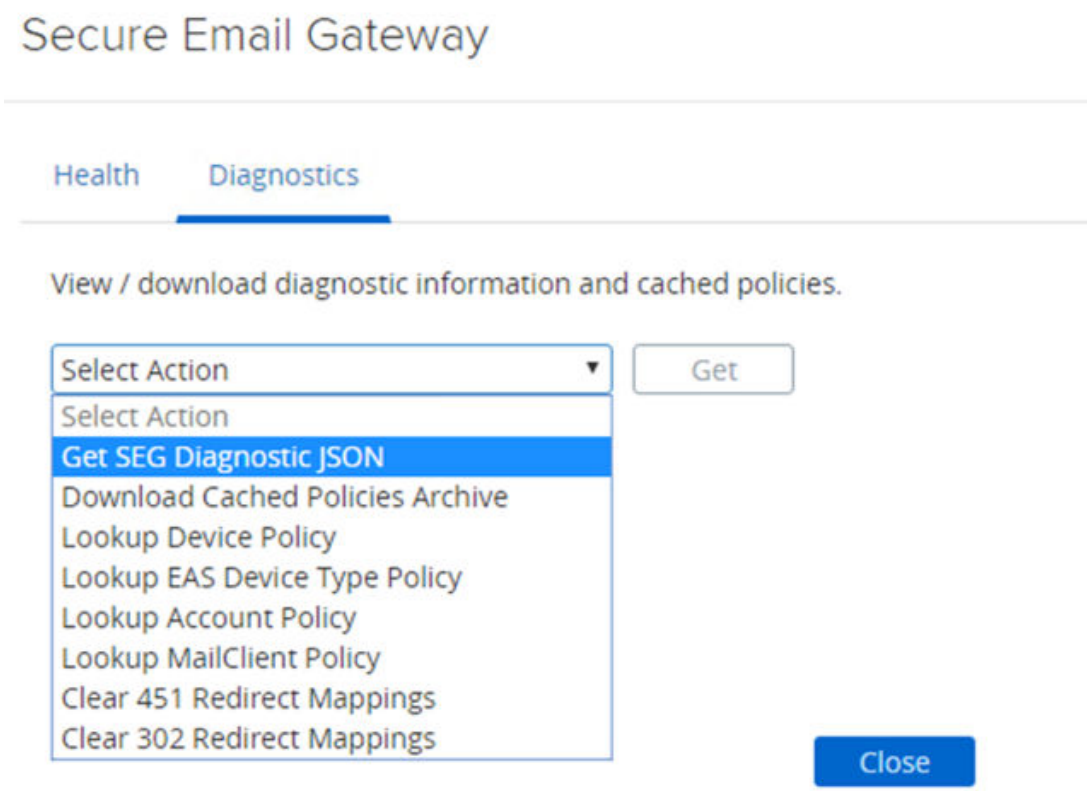
3 Cliquez sur **Actif** pour ouvrir l'écran de surveillance de la santé et des diagnostics de SEG. L'écran suivant s'affiche.



L'écran Diagnostics de SEG fournit les options suivantes à l'utilisateur :

- Affichez ou téléchargez le fichier JSON de diagnostics de SEG.
- Recherchez la stratégie spécifique à partir du cache de SEG.
- Archivez et téléchargez les stratégies mises en cache de SEG, les mappages de redirection et les informations de diagnostics.
- Effacez les mappages de redirection du cache de SEG.

L'image suivante montre l'écran Diagnostics pour SEG.



API de diagnostics de SEG

Le tableau suivant décrit le chemin d'accès de l'API et les paramètres d'accès aux informations de diagnostics de SEG.

URL de diagnostics de SEG : GET https://<UAGIP>:9443/rest/v1/monitor/seg/diagnostics/<apiPath>.

Chemin d'accès à l'API	Description
Diagnostic	Affichez le fichier JSON de diagnostics de SEG.
`policy/device/<easDeviceId>`	Recherchez la stratégie d'un ID de périphérique EAS spécifique.
`policy/account/<accountId>`	Recherchez la stratégie d'un utilisateur ou d'un groupe spécifique à l'aide de l'ID de compte.

Chemin d'accès à l'API	Description
policy/easdevicetype/<easdevicetype>	Recherchez la stratégie d'un type de périphérique EAS donné.
policy/mailclient/<mailclientname>	Recherchez la stratégie d'un client de messagerie donné.
cache/archive	Archivez et téléchargez les stratégies mises en cache de SEG, les mappages de redirection et les informations de diagnostics.
policy/account/<accountId>	Recherchez la stratégie d'un ID de périphérique EAS spécifique.

Le tableau suivant répertorie les API permettant d'effacer les mappages de redirection du cache de SEG.

URL d'effacement des mappages de cache de redirection : DELETE https://<UAGIP>:9443/rest/v1/monitor/seg/cache/<parameter>

Paramètre	Description
451	Effacez les mappages de redirection 451 du cache de SEG.
302	Effacez les mappages de redirection 302 du cache de SEG.

API de santé de SEG

Le tableau suivant décrit les attributs de réponse aux statistiques de santé de SEG.

URL de santé de SEG : GET https://<UAGIP>:9443/rest/v1/monitor/seg/healthStats

Attribut de réponse	Description
diagnosticExportTime	Spécifiez l'heure de génération des statistiques, en millisecondes, depuis l'époque d'UNIX.
apiConnectivity	État de la connectivité entre SEG et le serveur API. La valeur d'état peut être **Réussite** ou **Échec**.
policyDataLoaded	État du chargement des données de la stratégie dans le cache de SEG. La valeur d'état peut être **Réussite**, **En cours** ou **Échec**.
totalDevicePolicyCount	Spécifiez le nombre de stratégies de périphérique chargées dans le cache de SEG.
lastPolicyPartialUpdate	Spécifiez l'heure de la dernière exécution de la mise à jour de la stratégie partielle réussie, en millisecondes, depuis l'époque d'UNIX.
lastPolicyFullUpdate	Spécifiez l'heure de la dernière exécution de la mise à jour de la stratégie réussie, en millisecondes, depuis l'époque d'UNIX.

Attribut de réponse	Description
lastPolicyDeltaUpdate	Spécifiez l'heure de la dernière exécution de la mise à jour de la stratégie delta, en millisecondes, depuis l'époque d'UNIX.
policyDeltaSyncEnabled	Indicateur permettant de spécifier si la synchronisation delta de la stratégie est activée.
emailServerConnectivity	État de la connectivité entre SEG et le serveur API. Les valeurs d'attributs peuvent être **Réussite** ou **Échec**.
requestsSinceSEGstartup	Nombre de demandes ActiveSync depuis le lancement du serveur SEG.
lastHourRequests	Nombre de demandes ActiveSync au cours de la dernière heure.
last24hourRequests	Nombre de demandes ActiveSync au cours des dernières 24 heures.
syncStat ■ count ■ latency	Spécifiez les statistiques correspondantes aux demandes de **synchronisation**. ■ Nombre de demandes au cours de la dernière heure. ■ Latence moyenne au cours des dernières 24 heures.
itemOperationsStat ■ count ■ latency	Spécifiez les statistiques correspondantes aux demandes d'**itemOperations**. ■ Nombre de demandes au cours de la dernière heure. ■ Latence moyenne au cours des dernières 24 heures.
sendMailStat ■ count ■ latency	Spécifiez les statistiques correspondantes aux demandes de **sendMail**. ■ Nombre de demandes au cours de la dernière heure. ■ Latence moyenne au cours des dernières 24 heures.
smartForwardStat ■ count ■ latency	Spécifiez les statistiques correspondantes aux demandes de **smartForward**. ■ Nombre de demandes au cours de la dernière heure. ■ Latence moyenne au cours des dernières 24 heures.
smartReplyStat ■ count ■ latency	Spécifiez les statistiques correspondantes aux demandes de **smartReply**. ■ Nombre de demandes au cours de la dernière heure. ■ Latence moyenne au cours des dernières 24 heures.
clusteringEnabled	Indicateur permettant de spécifier si le clustering est activé.
nodesOnline	Liste des nœuds actifs dans le cluster.
nodesOffline	Liste de nœuds répertoriés dans la configuration MEM, mais qui sont inactifs dans le cluster.
nodesSynchronized	Indicateur permettant de spécifier si tous les nœuds du cluster sont synchronisés.

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 7-2. Contrôle de santé

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

- Cercle vide : le paramètre n'est pas configuré.
- Cercle rouge : le service est arrêté.
- Cercle orange : le service est exécuté partiellement.
- Cercle vert : 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 .\uagdeploy.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, netInternet, netManagementNetwork et netBackendNetwork.

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.

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 Server. 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.

Message d'erreur : Impossible de récupérer le certificat client à partir de la session sessionId

- Vérifiez que le certificat d'utilisateur est correctement installé dans le navigateur.
- Vérifiez que la version 1.2 du protocole TLS par défaut est activée sur le navigateur et sur Unified Access Gateway.

Impossible de déployer le fichier ova d'Unified Access Gateway à l'aide de VMware vSphere Web Client lancé sur le navigateur Chrome

Vous devez installer le plug-in d'intégration de client sur le navigateur que vous utilisez pour déployer un fichier ova sur vSphere Web Client. Après avoir installé le plug-in sur le navigateur Chrome, un message d'erreur s'affiche pour indiquer que le navigateur n'est pas installé et ne vous permettra pas d'entrer l'URL du fichier ova dans l'emplacement source. Il s'agit d'un problème du navigateur Chrome qui n'est pas lié au fichier ova d'Unified Access Gateway. Il est recommandé d'utiliser un autre navigateur pour déployer le fichier ova d'Unified Access Gateway.

Impossible de déployer le fichier ova d'Unified Access Gateway à l'aide de VMware vSphere HTML4/5 Web Client

Vous pouvez rencontrer des erreurs telles que celle-ci : `Valeur non valide spécifiée pour la propriété`. Ce problème n'est pas lié au fichier ova d'Unified Access Gateway. Il est recommandé d'utiliser le client FLEX vSphere à la place pour déployer le fichier ova.

Impossible de déployer le fichier ova d'Unified Access Gateway à l'aide de VMware vSphere 6.7 HTML5 Web Client

Vous pouvez trouver des champs manquants sur la page **Propriétés de déploiement** dans VMware vSphere 6.7 HTML5 Web Client. Ce problème n'est pas lié au fichier ova d'Unified Access Gateway. Il est recommandé d'utiliser le client FLEX vSphere à la place pour déployer le fichier ova.

Impossible de lancer XenApp dans Chrome à partir de Workspace ONE Access

Après avoir déployé Unified Access Gateway en tant que proxy inverse Web depuis Workspace ONE Access, vous ne pouvez pas lancer XenApp à partir du navigateur Chrome.

Suivez les étapes ci-dessous pour résoudre ce problème.

1 Utilisez la REST API suivante pour désactiver l'indicateur de fonctionnalité `orgUseNonNPAPIForCitrixLaunch` à partir du service Workspace ONE Access.

```
PUT https://fqdn/SAAS/jersey/manager/api/tenants/settings?tenantId=tenantname
{ "items":[ {"name":"orgUseNonNPAPIForCitrixLaunch","value": "false"} ] }
with the following two headers:
Content-Type application/vnd.vmware.horizon.manager.tenants.tenant.config.list+json
Authorization HZN value_of_HZN_cookie_for_admin_user
```

2 Attendez 24 heures pour que la modification prenne effet ou redémarrez le service Workspace ONE Access.

   - Pour redémarrer le service sous Linux, connectez-vous au dispositif virtuel et exécutez la commande suivante : `service horizon-workspace restart`.

- Pour redémarrer le service sous Windows, exécutez le script suivant : `install_dir\usr\local\horizon\scripts\horizonService.bat restart .`

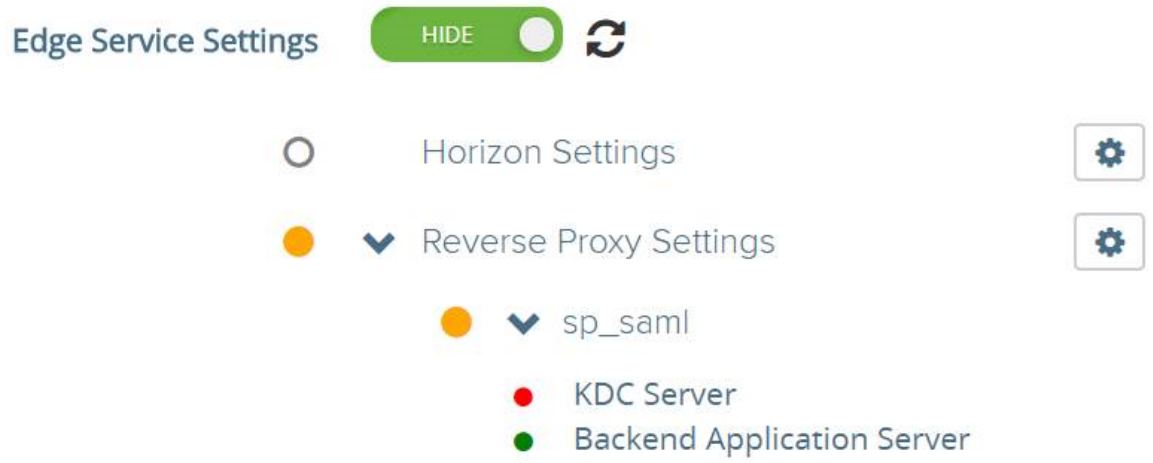
Dépannage des erreurs : pontage d'identité

Des problèmes peuvent se produire lorsque vous configurez Certificat sur-Kerberos ou SAML sur Kerberos dans votre environnement. Vous pouvez utiliser diverses procédures pour diagnostiquer et corriger ces problèmes.

Surveillance de la santé du serveur KDC et du serveur d'applications principal.

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 des paramètres Edge.

Figure 7-3. Contrôle de santé : paramètres de proxy inverse



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

- Cercle rouge : si l'état est rouge, cela peut impliquer un des problèmes suivants.
  - Problèmes de connectivité entre Unified Access Gateway et Active Directory
  - Problèmes de blocage de ports entre Unified Access Gateway et Active Directory.

    Note Assurez-vous que le port 88 TCP et UDP est ouvert dans la machine exécutant Active Directory.

  - Il est possible que le nom et les informations d'identification du serveur principal soient incorrectes dans le fichier keytab téléchargé.
- Cercle vert : si l'état est vert, cela implique qu'Unified Access Gateway peut se connecter à Active Directory avec les informations d'identification fournies dans le fichier keytab.

Erreur lors de la création du contexte Kerberos : variation d'horloge trop importante

Ce message d'erreur :

```
ERROR:"wsportal.WsPortalEdgeService[createKerberosLoginContext: 119][39071f3d-9363-4e22-
a8d9-5e288ac800fe]: Error creating kerberos context.
Identity bridging may not work
javax.security.auth.login.LoginException: Clock skew too great"
```

s'affiche lorsque l'heure d'Unified Access Gateway et l'heure du serveur AD sont considérablement désynchronisées. Réinitialisez l'heure sur le serveur AD pour qu'elle corresponde à l'heure UTC exacte d'Unified Access Gateway.

Erreur lors de la création du contexte Kerberos : nom ou service inconnu

Ce message d'erreur :

```
wsportal.WsPortalEdgeService[createKerberosLoginContext: 133][]: Error creating kerberos
context.
Identity bridging may not work
javax.security.auth.login.LoginException: Name or service not known
```

s'affiche lorsque Unified Access Gateway ne peut pas joindre le domaine configuré ou ne peut pas se connecter à KDC avec les détails utilisateur dans le fichier keytab. Vérifiez ce qui suit :

- le fichier keytab est généré avec le mot de passe correct du compte utilisateur SPN et téléchargé sur Unified Access Gateway
- le nom d'hôte et l'adresse IP de l'application principale sont ajoutés correctement dans les entrées de l'hôte.

Erreur lors de la réception du jeton Kerberos pour l'utilisateur : user@domain.com, erreur : erreur de délégation Kerberos : nom de la méthode : gss_acquire_cred_impersonate_name : échec GSS non spécifié. Un code mineur peut fournir plus d'informations

```
"Kerberos Delegation Error: Method name: gss_acquire_cred_impersonate_name: Server not
found in Kerberos database"
```

Si ce message s'affiche, vérifiez si :

- La relation de confiance entre les domaines fonctionne.
- Le nom SPN cible est configuré correctement.

Dépannage des erreurs : Cert-to-Kerberos

Vous pouvez rencontrer des difficultés lorsque vous configurez Cert-to-Kerberos dans votre environnement. Vous pouvez utiliser diverses procédures pour diagnostiquer et corriger ces problèmes.

Message d'erreur : Erreur interne. Contactez l'administrateur

Recherchez le message dans le fichier `/opt/vmware/gateway/logs/authbroker.log`

```
"OSCP validation of CN=clientCert, OU=EUC, O=<org name>, ST=<state name>, C=IN failed with "Could not send OCSP request to responder: Connection refused (Connection refused) , will attempt CRL validation"
```

Cela indique que l'URL d'OCSP configurée dans « Certificat X.509 » n'est pas accessible ou incorrecte.

Erreur lorsque le certificat OCSP n'est pas valide

```
"revocation.RevocationCheck: OSCP validation of CN=clientCert failed with "Could not verify signing certificate for OCSP responder:http://asdkad01/ocsp". will attempt CRL validation."
```

s'affiche lorsqu'un certificat non valide pour OCSP est téléchargé ou si le certificat OCSP est révoqué.

Erreur lorsque la vérification de la réponse OCSP échoue

```
"WARN ocsp.BouncyCastleOCSPHandler: Failed to verify OCSP response: CN=asdkAD01.Asdk.ADrevocation.RevocationCheck: 08/23 14:25:49,975" [tomcat-http--26] WARN revocation.RevocationCheck: OSCP validation of CN=clientCert failed with "Could not verify signing certificate for OCSP responder: http://asdkad01/ocsp". will attempt CRL validation."
```

s'affiche parfois lorsque la vérification de la réponse OCSP échoue.

Message d'erreur : impossible de récupérer le certificat client à partir de la session : <sessionId>

Si ce message s'affiche :

- Vérifiez les paramètres de certificat X.509 et déterminez s'ils sont configurés
- Si les paramètres du certificat X.509 sont configurés : vérifiez le certificat client installé sur le navigateur côté client pour voir s'il est émis par la même autorité de certification téléchargée dans le champ « Certificats d'autorité de certification racine et intermédiaire » dans les paramètres du certificat X.509.

Dépannage de la conformité du point de terminaison

Vous pouvez rencontrer des difficultés lorsque vous déployez le fournisseur de vérification de la conformité du point de terminaison dans votre environnement. Vous pouvez utiliser diverses procédures pour diagnostiquer et corriger des problèmes avec votre déploiement.

Note `Esmanager.log` journalise des informations sur l'adresse MAC du périphérique utilisé pour la vérification de la conformité. Cela est utile pour identifier l'adresse MAC utilisée pour la vérification de la conformité du point de terminaison, si le périphérique dispose de plusieurs cartes réseau ou commutateurs vers des réseaux différents.

Unified Access Gateway affiche « Informations d'identification du client incorrectes »

Unified Access Gateway effectue l'appel API OPSWAT pour valider la clé du client et la phrase secrète du client fournies. Si les informations d'identification ne sont pas correctes, les paramètres ne sont pas enregistrés, ce qui entraîne une erreur

```
Informations d'identification du client incorrectes
```

.

Vérifiez que la clé du client et la phrase secrète du client correctes se trouvent dans les champs Nom d'utilisateur et Mot de passe.

Pour générer des informations d'identification du client, enregistrez votre application ici https://gears.opswat.com/o/app/register.

Unified Access Gateway affiche « DNS ne peut pas résoudre l'hôte `https://gears.opswat.com` »

Utilisez la commande ping pour découvrir l'adresse IP de `gears.opswat.com` pour votre région.

Ensuite, utilisez l'adresse IP de la commande ping pour créer une entrée `/etc/hosts` pour `https://gears.opswat.com`. Accédez aux paramètres d'Horizon depuis l'interface utilisateur d'administration et fournissez la valeur dans **Entrées de l'hôte** pour le service View Edge.

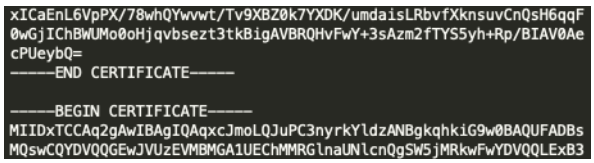
Unified Access Gateway affiche « La demande a expiré lors de la connexion à l'hôte `https://gears.opswat.com` »

Cela peut se produire si l'entrée d'hôte `gears.opswat.com` est mal configurée dans UAG ou si `https://gears.opswat.com` n'accepte pas la demande de connexion.

Dépannage de la validation du certificat dans l'interface utilisateur d'administration

Si vous rencontrez des erreurs lors de la validation du format PEM d'un certificat, recherchez le message d'erreur ici pour plus d'informations.

Voici une liste de scénarios possibles dans lesquels des erreurs sont générées.

Erreur	Problème
Format PEM non valide. Peut être dû à un format BEGIN incorrect. Consultez le journal pour plus de détails.	Le certificat BEGIN PrivateKey n'est pas valide.
Format PEM non valide. Message d'exception : -----END RSA PRIVATE KEY not found. Consultez le journal pour plus de détails.	Le certificat END PrivateKey n'est pas valide.
Format PEM non valide. Message d'exception : problem creating RSA private key: java.lang.IllegalArgumentException: failed to construct sequence from byte[]: corrupted stream - out of bounds length found. Consultez le journal pour plus de détails.	PrivateKey dans le certificat est endommagé.
Impossible d'analyser les certificats de chaîne PEM. Consultez le journal pour plus de détails.	Le certificat BEGIN PublicKey n'est pas valide.
Données PEM incorrectes trouvées. Consultez le journal pour plus de détails.	Le certificat END PublicKey n'est pas valide.
Données PEM incorrectes trouvées. Consultez le journal pour plus de détails.	PublicKey dans le certificat est endommagé.
Il n'y a aucun certificat cible/de fin pour créer le chaînage.	Il n'existe aucun certificat cible ou de fin.
Impossible de générer le chemin d'accès de la chaîne de certificats, tous les certificats cibles ne sont pas valides. Il peut manquer des certificats intermédiaires/racine.	Il n'existe aucune chaîne de certificats à créer.
Erreur ambiguë : plusieurs chaînes de certificats trouvées, incertitude sur celle à renvoyer	Il existe plusieurs chaînes de certificats.
Impossible de créer le chemin d'accès de la chaîne de certificats, CertificateExpiredException : le certificat a expiré le *20171206054737GMT + 00:00*. Consultez le journal pour plus de détails.	Le certificat a expiré.
Message d'erreur « Données inattendues détectées dans le flux » lors du téléchargement du certificat au format PEM.	Ligne vide manquante ou attributs supplémentaires entre le certificat feuille et intermédiaire dans le certificat de chaîne. L'ajout d'une ligne vide entre le certificat feuille et intermédiaire résoudrait le problème. Figure 7-4. Exemple 

Dépannage des problèmes de connexion et de pare-feu

Vous pouvez surveiller, tester et résoudre les problèmes de réseau tels que les problèmes de connexion et de pare-feu à partir de votre instance de Unified Access Gateway avec différents outils et commandes comme `tcpdump` et `curl`.

Installer et exécuter `tcpdump`

`tcpdump` est un outil de ligne de commande que vous pouvez utiliser pour analyser les paquets TCP pour le dépannage et à des fins de test.

Si vous n'avez pas installé `tcpdump` sur votre instance de Unified Access Gateway, exécutez la commande suivante à partir de la ligne de commande pour installer `tcpdump` :

```
/etc/vmware/gss-support/install.sh
```

Les exemples suivants illustrent l'utilisation de `tcpdump` :

- Exécutez les commandes suivantes pour contrôler le trafic sur des ports spécifiques.

  Note Si vous spécifiez le port 8443, assurez-vous que UDP 8443 n'est pas bloqué par un pare-feu externe.

  a `tcpdump -i eth0 -n -v udp port 8443`

  b `tcpdump -i eth0 -n -v tcp port 8443`

  c `tcpdump -i any -n -v port 22443`

- Exécutez les commandes suivantes pour suivre les paquets qui arrivent vers et depuis le serveur RADIUS sur Unified Access Gateway :

  ```
  nslookup <radius-server-hostname>
  tracepath <radius-server-hostname>
  tcpdump -i any -n -v port 1812
  ```

- Exécutez les commandes suivantes pour suivre les paquets qui arrivent vers et depuis le serveur RSA SecurID sur Unified Access Gateway.

  ```
  nslookup <rsa-auth-server-hostname>
  tracepath <rsa-auth-server-hostname>
  ```

Utilisation de la commande `curl`

Vous pouvez également utiliser la commande `curl` pour récupérer des informations sur les connexions réseau.

- Exécutez la commande suivante pour tester la connexion à un serveur de connexion principal ou un serveur Web :

  `curl -v -k https://<hostname-or-ip-address>:443/`

Vous pouvez afficher les problèmes de connexion du serveur principal dans le fichier `esmanager.log` :

```
07/14 07:29:03,882[nioEventLoopGroup-7-1]ERROR
view.ViewEdgeService[onFailure: 165][]: Failed to resolve hostname
address in proxyDestinationUrl:xref:mbxxx-cs.xyz.in
```

- Vous ne pouvez pas tester les connexions aux postes de travail virtuels du serveur principal comme PCoIP 4172 et Blast 22443 à l'aide de `tcpdump`, car les postes de travail n'écoutent pas sur ces numéros de port avant qu'une session soit prête. Consultez les journaux pour rechercher d'éventuels échecs de connexion sur ces ports.
  - Exécutez la commande suivante pour la connexion à Horizon Framework Channel TCP :

    `curl -v telnet://<virtualdesktop-ip-address>:32111`
  - Exécutez la commande suivante pour la connexion à Horizon MMR/CDR TCP :

    `curl -v telnet://<virtualdesktop-ip-address>:9427`
  - Exécutez la commande suivante pour tester la connectivité de port entre Unified Access Gateway et le poste de travail virtuel. Avant d'exécuter cette commande, assurez-vous que la session avec le poste de travail virtuel est activée.

    `curl -v telnet://<virtualdesktop-ip-address>:22443`

Commandes PowerShell

Exécutez les commandes suivantes à partir de la ligne de commande PowerShell pour contrôler la connectivité pour des ports spécifiques :

1. `Test-NetConnection <uag-hostname-or-ip-address> -port 443`
2. `Test-NetConnection <uag-hostname-or-ip-address> -port 8443`
3. `Test-NetConnection <uag-hostname-or-ip-address> -port 4172`

Dépannage des problèmes de connexion racine

Si vous vous connectez en tant que racine à la console d'Unified Access Gateway avec les nom d'utilisateur et mot de passe corrects et que vous obtenez l'erreur « Connexion incorrecte », recherchez les problèmes de mappage de clavier et réinitialisez le mot de passe racine.

Une erreur de connexion a plusieurs raisons :

- Le clavier utilisé ne mappe pas certains caractères du mot de passe correctement en fonction de la définition de clavier d'Unified Access Gateway
- Le mot de passe a expiré. Le mot de passe racine expire 365 jours après le déploiement du fichier OVA.
- Le mot de passe n'a pas été défini correctement lorsque le dispositif a été déployé. Il s'agit d'un problème connu avec les versions antérieures d'Unified Access Gateway.

- Le mot de passe a été oublié.

Pour vérifier que le clavier mappe les caractères correctement, essayez d'entrer le mot de passe en réponse à l'invite du nom d'utilisateur « Connexion : ». Cela vous permet de voir tous les caractères du mot de passe et d'identifier où les caractères sont mal interprétés.

Pour toutes les autres causes, réinitialisez le mot de passe racine du dispositif.

Note Pour réinitialiser le mot de passe racine, vous devez :

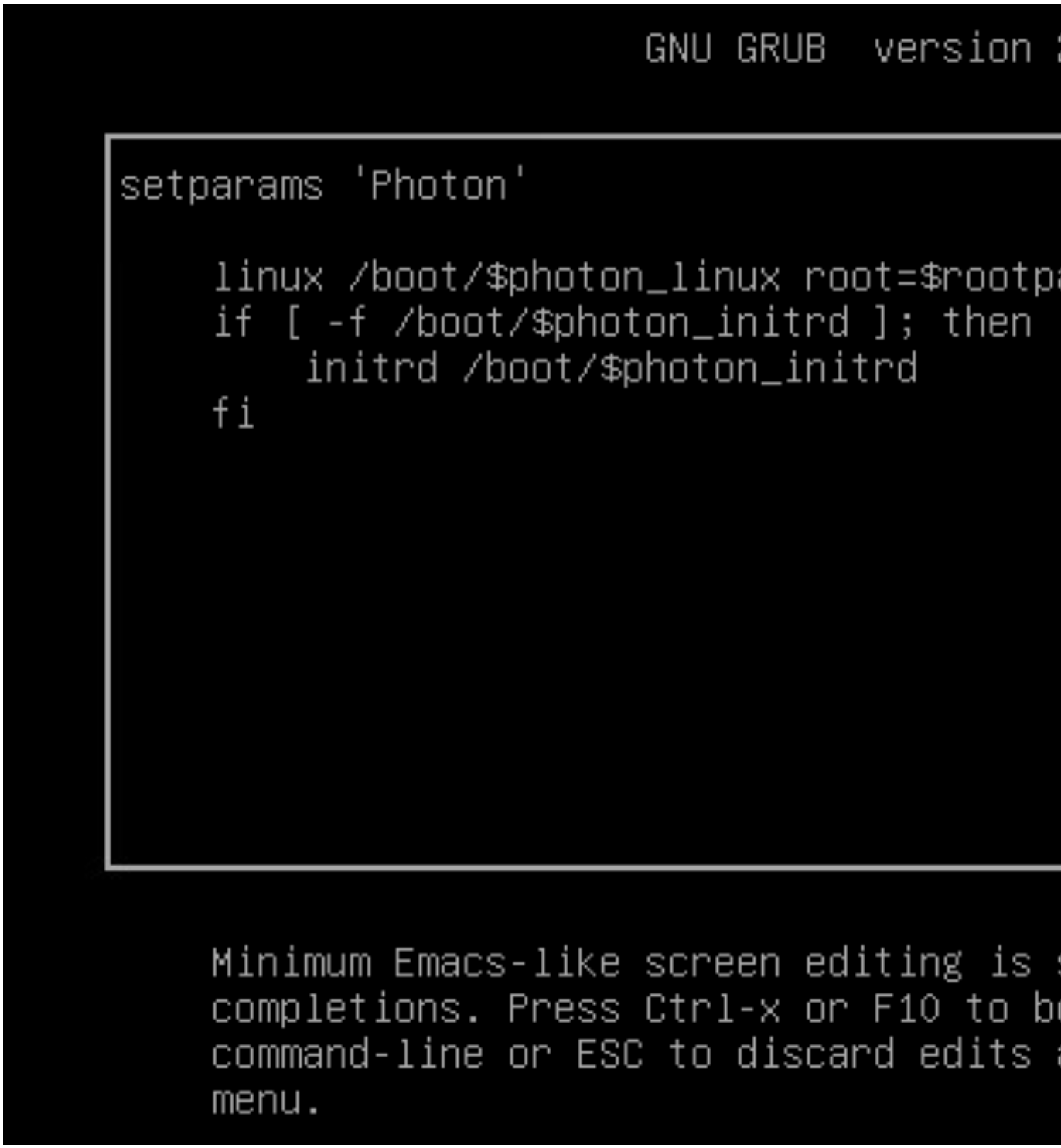
- disposer d'un accès de connexion à vCenter
- connaître le mot de passe de connexion de vCenter
- être autorisé à accéder à la console du dispositif

Si vous avez configuré un mot de passe de menu de chargeur de démarrage Grub2 pour le dispositif, vous devrez l'entrer dans le cadre de cette procédure.

Procédure

1. Redémarrez le dispositif à partir de vCenter et connectez-vous immédiatement à la console.
2. Dès que l'écran de démarrage Photon OS s'affiche, appuyer sur la touche e pour entrer dans le menu d'édition GNU GRUB

3 Dans le menu d'édition GNU GRUB, accédez à la fin de la ligne qui commence par `linux`, ajoutez un espace et tapez `/boot/$photon_linux root=$rootpartition rw init=/bin/bash`. Après l'ajout de ces valeurs, le menu d'édition GNU GRUB doit être exactement semblable à celui-ci :



Note Pour un dispositif FIPS, la ligne doit être `linux /boot/$photon_linux root=$rootpartition rw init=/bin/bash fips=1`

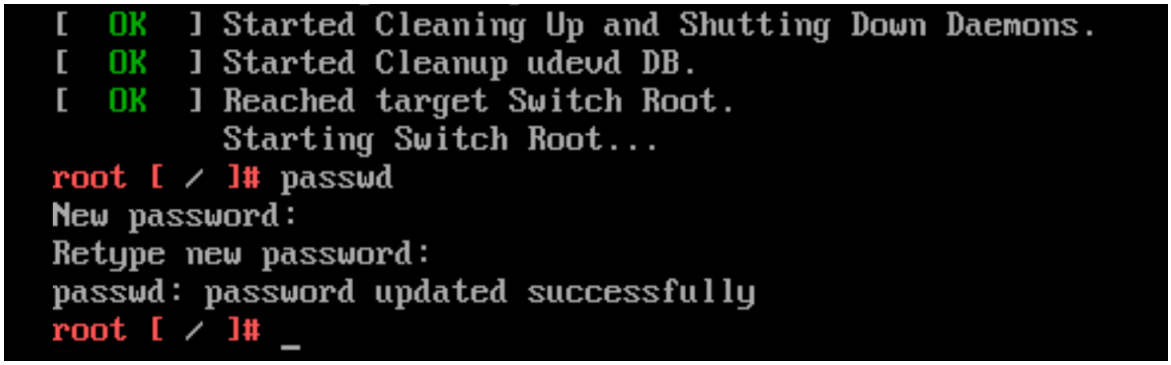
4 Appuyez sur la touche F10 et à l'invite de commande bash, entrez **passwd** pour modifier le mot de passe.

```
passwd

New password:

Retype new password:

passwd: password updated successfully
```



5 Redémarrer le dispositif `reboot -f`

- Une fois le dispositif démarré, connectez-vous en tant qu'utilisateur racine avec le mot de passe que vous venez de définir.

À propos du mot de passe Grub2

Vous pouvez utiliser le mot de passe Grub2 pour votre connexion racine.

À partir d'Unified Access Gateway 3.1, le mot de passe de modification Grub2 sera défini par défaut.

Le nom d'utilisateur est root et le mot de passe est le même que le mot de passe racine que vous avez configuré lors du déploiement d'Unified Access Gateway. Ce mot de passe ne sera jamais réinitialisé, sauf si vous le réinitialisez explicitement en vous connectant à la machine.

Note Modifier manuellement le mot de passe racine en vous connectant à la machine à l'aide de n'importe quelle commande ne réinitialisera pas le mot de passe Grub2. Ils s'excluent mutuellement. Ce n'est que lors du déploiement que le même mot de passe sera défini pour les deux (avec UAG 3.1 et versions ultérieures).

Collecte de journaux depuis le dispositif Unified Access Gateway

Téléchargez le fichier `UAG-log-archive.zip` dans la section Paramètres de prise en charge de 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 7-5. 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	Désigne les événements généralement susceptibles d'être utiles pour déboguer les problèmes, pour afficher ou modifier l'état interne du dispositif et pour 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 7-6. Fichiers qui contiennent des informations système pour faciliter le dépannage

Filename	Description	Commande Linux (le cas échéant)
`version.info`	Contient les versions du système d'exploitation, du noyau, du GCC et du dispositif Unified Access Gateway.	
`ipv4-forwardrules`	Règles de transfert IPv4 configurées sur le dispositif.	
`df.log`	Contient des informations sur l'utilisation de l'espace disque sur le dispositif.	`df -a -h --total`

Tableau 7-6. Fichiers qui contiennent des informations système pour faciliter le dépannage (suite)

Filename	Description	Commande Linux (le cas échéant)
netstat.log	Contient des informations sur les ports ouverts et les connexions TCP existantes.	netstat -anop
netstat-s.log	Statistiques réseau (octets envoyés/reçus, etc.) depuis l'heure de création du dispositif.	netstat -s
netstat-r.log	Itinéraires statiques créés sur le dispositif.	netstat -r
uag_config.json, uag_config.ini, uagstats.json	Configuration complète du dispositif Unified Access Gateway, affichant tous les paramètres sous forme d'un fichier JSON et d'un fichier INI.	
ps.log	Inclut les processus en cours d'exécution au moment du téléchargement des journaux.	ps -elf --width 300
ifconfig.log	Configuration de l'interface réseau du dispositif.	ifconfig -a
free.log	Disponibilité de la RAM au moment du téléchargement des journaux.	free
top.log	Liste triée de processus par utilisation de la mémoire au moment du téléchargement des journaux.	top -b -o %MEM -n 1
iptables.log	Tables d'adresses IP pour IPv4.	iptables-save
ip6tables.log	Tables d'adresses IP pour IPv6.	ip6tables-save
w.log	Informations sur le temps d'activité, les utilisateurs actuellement sur la machine, ainsi que leurs processus.	w
systemctl.log	Liste des services en cours d'exécution sur le dispositif	systemctl
resolv.conf	Pour la connexion directe des clients locaux à tous les serveurs DNS connus	
hastats.csv	Contient les statistiques par nœud et les informations de statistiques totales pour chaque type de serveur principal (Edge Service Manager, VMware Tunnel, Content Gateway)	
system_logs_archive	Le répertoire contient les fichiers journaux suivants : cpu.info, mem.info, sysctl. log et journalctl_archive.	
cpu.info	Contient les informations de CPU de la machine virtuelle collectées dans /proc/cpuinfo.	
mem.info	Contient des informations sur la mémoire de la machine virtuelle, telles que la mémoire totale disponible, la quantité de mémoire disponible, etc. collectées dans /proc/meminfo.	
sysctl.log	Contient des informations sur tous les paramètres de noyau de la machine virtuelle.	sysctl -a

Tableau 7-6. Fichiers qui contiennent des informations système pour faciliter le dépannage (suite)

Filename	Description	Commande Linux (le cas échéant)
journalctl_archive	Les fichiers contiennent des informations de journal journalctl qui s'étendent sur 7 jours jusqu'à ce que l'archive soit téléchargée. Par exemple, si un administrateur télécharge l'archive des journaux à partir de l'interface utilisateur d'administration d'Unified Access Gateway à 9 h aujourd'hui, l'archive contient des informations pour les 7 derniers jours, notamment jusqu'à 9 h 00. Si la taille des journaux collectés est inférieure ou égale à 25 MB, un seul fichier, journalctl.log, est généré. Si la taille des journaux collectés est supérieure à 25 MB, le dossier journalctl_archive est créé avec plusieurs fichiers journalctl. log .	journalctl -x --since '1 week ago'
journald.conf	Contient des informations sur la configuration des journaux journalctl.	
system-logs-collection-status.log	Contient des informations qui indiquent si les fichiers journaux suivants ont été collectés : cpu.info, mem.info, sysctl. log et journalctl_archive.	
hôtes	Contient les entrées /etc/hosts.	
firstboot	Contient des informations qui sont générées lorsque Unified Access Gateway est démarré pour la première fois.	
subsequentboot	Contient des informations qui sont générées lors des redémarrages suivants d'Unified Access Gateway.	
vami-ovf.log	Contient des informations relatives à la configuration, telles que les propriétés d'OVF, le réseau, etc. du dispositif Unified Access Gateway pendant le déploiement.	

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

Filename	Description	Commande Linux (le cas échéant)
supervisord.log	Journal Supervisor (gestionnaire pour Edge Service Manager, l'administrateur et un AuthBroker).	
esmanager-x.log, esmanager-std-out.log	Un ou plusieurs journaux d'Edge Service Manager, indiquant les processus principaux exécutés sur le dispositif.	
audit.log	Journal d'audit de toutes les opérations d'administrateur.	
authbroker.log	Contient des messages de journal du processus AuthBroker, qui gère l'authentification Radius et RSA SecurID.	

Tableau 7-7. Fichiers journaux d'Unified Access Gateway (suite)

Filename	Description	Commande Linux (le cas échéant)
admin.log, admin-std-out.log	Journaux de l'interface utilisateur d'administration. Contient des messages de journal du processus qui fournit l'API REST Unified Access Gateway sur le port 9443.	
bsg.log	Contient des messages de journal de Blast Secure Gateway.	
SecurityGateway_xxx.log	Contient des messages de journal de PCoIP Secure Gateway.	
utserver.log	Contient des messages de journal du serveur de tunnel UDP.	
activeSessions.csv	Liste des sessions Horizon ou WRP actives.	
haproxy.conf	Contient des paramètres de configuration de proxy HA pour le partage de port TLS.	
vami.log	Contient des messages de journal des commandes vami en cours d'exécution pour définir des interfaces réseau pendant le déploiement.	
content-gateway.log, content-gateway-wrapper.log, 0.content-gateway-YYYY-mm.dd.log.zip	Contient des messages de journal de Content Gateway.	
admin-zookeeper.log	Contient des messages de journal liés à la couche de données utilisée pour stocker la configuration d'Unified Access Gateway.	
tunnel.log	Contient des messages de journal du processus de tunnel utilisé dans le cadre du traitement API XML. Pour afficher ce journal, le tunnel doit être activé dans les paramètres d'Horizon.	
tunnel_snap.log	Contient des informations qui indiquent si les journaux du proxy et du serveur VMware Tunnel ont été collectés.	
tunnel-snap.tar.gz	Tarball contenant les journaux du proxy et du serveur VMware Tunnel.	
appliance-agent.log	Journaux de l'agent du dispositif (pour le démarrage des services Workspace ONE UEM).	
config.yml	Contient les détails de niveau de journal et de configuration de Content Gateway.	
smb.conf	Contient la configuration du client SMB.	
smb-connector.conf	Contient les détails de niveau de journal et de protocole SMB.	

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.

Tableau 7-8. Informations de rotation des journaux relatives aux fichiers journaux d'Unified Access Gateway

Nom du fichier journal	Emplacement	Propriété
admin-zookeeper.log	/opt/vmware/gateway/conf/log4j-admin.properties	log4j.appender.zookeeper.MaxFileSize=10MB log4j.appender.zookeeper.MaxBackupIndex=5
admin.log	/opt/vmware/gateway/conf/log4j-admin.properties	log4j.appender.default.MaxFileSize=10MB log4j.appender.default.MaxBackupIndex=5
audit.log	/opt/vmware/gateway/conf/log4j-admin.properties	log4j.appender.adminAudit.MaxFileSize=10MB log4j.appender.adminAudit.MaxBackupIndex=5
authbroker.log	/opt/vmware/gateway/conf/log4j-authbroker.properties	appender.rollingFile.policies.size.size=10MB appender.rollingFile.strategy.max=5
bsg.log	/opt/vmware/gateway/lib/bsg/absg.properties	logFilesize=8*1024*1024 logBackupCount=5
esmanager.log	/opt/vmware/gateway/conf/log4j-esmanager.properties	log4j.appender.default.MaxFileSize=25MB log4j.appender.default.MaxBackupIndex=10
tunnel.log	/opt/vmware/gateway/conf/log4j-tunnel.properties	log4j.appender.default.MaxFileSize=25MB log4j.appender.default.MaxBackupIndex=5
Fichiers présents dans /var/log/journal	/etc/systemd/journald.conf	SystemMaxUse=1G
keepalived.log	/etc/logrotate.d/keepalived	rotate 5 size 5M
haproxy.log	/etc/logrotate.d/haproxy	rotate 5 size 25M
/var/log/messages /var/log/cron	/etc/logrotate.d/messages_and_cron	rotate 20 size 50M maxage 30

Événements Syslog

Le serveur Syslog consigne les événements qui se produisent sur le dispositif Unified Access Gateway. Cette rubrique vous aide à comprendre les informations capturées lorsque ces événements sont consignés.

Événements d'audit Syslog

Le tableau suivant décrit les événements d'audit avec des exemples :

Description de l'événement	Exemple d'événement
Les événements sont consignés lorsqu'un administrateur se connecte à l'interface utilisateur d'administration d'Unified Access Gateway, effectue des modifications de configuration dans l'interface utilisateur d'administration ou se déconnecte de l'interface utilisateur d'administration.	■ `06-09-2020 16:56:03 User.Info` *`Syslog_Server_IP_Address`* `UAG-AUDIT:[qtp332498651-46]INFO utils.SyslogAuditManager[logAuditLog: 382] - LOGIN_SUCCESS: SOURCE_IP_ADDR=`*`Client_Machine_IP_Address`*`: USERNAME=admin"` ■ `06-09-2020 16:57:25 User.Info` *`Syslog_Server_IP_Address`* `UAG-AUDIT:[qtp332498651-44]INFO utils.SyslogAuditManager[logAuditLog: 382] - CONFIG_CHANGE: SOURCE_IP_ADDR=`*`Client_Machine_IP_Address`*`: USERNAME=admin: CHANGE=tlsSyslogServerSettings:(null->[]) - dns:(null->) - monitorInterval:(20->60) - sshPublicKeys:(null->[]) - ntpServers: (null->) - dnsSearch:(null->) - fallBackNtpServers:(null->) -` ■ `06-09-2020 16:55:57 User.Info` *`Syslog_Server_IP_Address`* `UAG-AUDIT:[qtp332498651-22]INFO utils.SyslogAuditManager[logAuditLog: 382] - LOGOUT_SUCCESS: SOURCE_IP_ADDR=`*`Client_Machine_IP_Address`*`: USERNAME=admin`

Événements Syslog

Le tableau suivant décrit les événements système avec des exemples :

Description de l'événement	Exemple d'événement
Un événement est consigné lorsque les services Edge configurés dans Unified Access Gateway sont démarrés et arrêtés en conséquence.	Dans les exemples d'événements suivants, *UAG Name* représente l'option qui est configurée dans le cadre de la **Configuration système** d'Unified Access Gateway dans l'interface utilisateur d'administration : ■ `06-09-2020 16:57:26 Local2.Info` *`Syslog_Server_IP_Address`* `Jun 9 11:25:59` *`UAG Name`* `UAG-ESMANAGER: [Curator-QueueBuilder-0]INFO utils.SyslogManager[stop: 993][] - EDGE_SERVICE_MANAGER:STOPPED:Stopped Edge Service Manager` ■ `06-09-2020 16:57:26 Local2.Info` *`Syslog_Server_IP_Address`* `Jun 9 11:25:59` *`UAG Name`* `UAG-ESMANAGER: [Curator-QueueBuilder-0]INFO utils.SyslogManager[start: 321][] - EDGE_SERVICE_MANAGER:STARTED:Started EdgeServiceManager.`
Les événements sont consignés en cas d'accès à Unified Access Gateway à l'aide du schéma HTTP et de redirection vers HTTPS.	■ `06-09-2020 16:57:28 Local2.Info` *`Syslog_Server_IP_Address`* `Jun 9 11:26:01` *`UAG Name`* `UAG-ESMANAGER: [main-EventThread]INFO utils.SyslogManager[startAndStopHttpAndHttpsServer: 768][] - HTTP_REDIRECTION_SERVER:STARTED:Started HTTP redirection server listening on port 8080` ■ `06-09-2020 16:57:26 Local2.Info` *`Syslog_Server_IP_Address`* `Jun 9 11:25:59` *`UAG Name`* `UAG-ESMANAGER: [Curator-QueueBuilder-0]INFO utils.SyslogManager[stop: 977][] - HTTP_REDIRECTION_SERVER:STOPPED:Stopped HTTP redirection serverlistening on port 8080`
Les événements sont consignés lorsque les paramètres du proxy inverse Web sont activés ou désactivés dans l'interface utilisateur d'administration d'Unified Access Gateway.	■ `06-10-2020 11:11:06 Local2.Info` *`Syslog_Server_IP_Address`* `Jun 10 05:39:39` *`UAG Name`* `UAG-ESMANAGER: [main-EventThread]INFO utils.SyslogManager[startService: 207][] - WS_PORTAL_SERVICE:STARTED:Started WS Portal Edge Service` ■ `06-10-2020 11:10:32 Local2.Info` *`Syslog_Server_IP_Address`* `Jun 10 05:39:04` *`UAG Name`* `UAG-ESMANAGER: [main-EventThread]INFO utils.SyslogManager[stopService: 274][] - WS_PORTAL_SERVICE:STOPPED:Stopped WS Portal Edge Service`

Description de l'événement	Exemple d'événement
Les événements sont consignés lorsque les paramètres du service Edge Horizon sont activés ou désactivés dans l'interface utilisateur d'administration d'Unified Access Gateway.	■ 06-10-2020 11:03:10 Local2.Info *Syslog_Server_IP_Address* Jun 10 05:31:43 *UAG Name* UAG-ESMANAGER: [main-EventThread]INFO utils.SyslogManager[stopService: 689][] - HORIZON_SERVICE:STOPPED:Horizon View Edge Service ■ 06-10-2020 11:04:40 Local2.Info *Syslog_Server_IP_Address* Jun 10 05:33:13 *UAG Name* UAG-ESMANAGER: [main-EventThread]INFO utils.SyslogManager[startService: 332][] - HORIZON_SERVICE:STARTED:Started Horizon Edge Service
Les événements sont consignés lorsqu'une session Horizon est établie, ce qui constitue la connexion utilisateur, l'authentification utilisateur et l'arrêt de la session.	Lorsque plusieurs événements sont consignés via le flux, les exemples d'événements incluent les scénarios de connexion, les scénarios de réussite et d'échec de l'authentification utilisateur et le délai d'expiration de l'authentification. Dans l'un des exemples, Horizon a été configuré grâce à la méthode d'authentification RADIUS : ■ Sample Event -06-10-2020 10:46:09 Local2.Info *Syslog_Server_IP_Address* Jun 10 05:14:42 *UAG Name* UAG-ESMANAGER: [nioEventLoopGroup-6-4]INFO utils.SyslogManager[processXmlString: 189] [3df5-***-41f6] - Authentication attempt - LOGIN initiated ■ 06-10-2020 10:46:09 Local2.Info *Syslog_Server_IP_Address* Jun 10 05:14:42 *UAG Name* UAG-ESMANAGER: [nioEventLoopGroup-6-4]INFO utils.SyslogManager[processDocument: 110] [3df5-***-41f6] - Authentication attempt response - ok ■ 06-11-2020 14:52:47 Local2.Info *Syslog_Server_IP_Address* Jun 11 09:21:20 *UAG Name* UAG-ESMANAGER: [nioEventLoopGroup-16-2]INFO utils.SyslogManager[processDocument: 110] [1e85-***-1f8d] - Authentication attempt response - partial ■ 06-11-2020 15:02:28 Local2.Info *Syslog_Server_IP_Address* Jun 11 09:31:01 *UAG Name* UAG-ESMANAGER: [jersey-client-async-executor-1]INFO utils.SyslogManager[logMessage: 188][f7ba-***-7a21] - AUTH SUCCESS for user radius. Auth type: RADIUS-AUTH, Sub type: passcode ■ 06-11-2020 14:52:47 Local2.Warning *Syslog_Server_IP_Address* Jun 11 09:21:20 *UAG Name* UAG-ESMANAGER:

Description de l'événement	Exemple d'événement
	[nioEventLoopGroup-16-2]WARN utils.SyslogManager[persistFailedLoginAttempt: 386][1e85-***-1f8d] - Authentication attempt - FAILED ■ 06-11-2020 14:58:22 Local2.Info *Syslog_Server_IP_Address* Jun 11 09:26:55 *UAG Name* UAG-ESMANAGER: [jersey-client-async-executor-0]INFO utils.SyslogManager[logMessage: 188][f22c-***-162d] - AUTH FAILED for user radius with error Received timeout from RADIUS server for user radius. Auth type: RADIUS-AUTH, Sub type: passcode ■ 06-10-2020 10:47:03 Local2.Info *Syslog_Server_IP_Address* Jun 10 05:15:36 *UAG Name* UAG-ESMANAGER: [nioEventLoopGroup-6-4]INFO utils.SyslogManager[terminateSession: 450][3df5-***-41f6] - HORIZON_SESSION:TERMINATED:Horizon Session terminated - Session count:2, Authenticated sessions: 1

Secure Email Gateway

Secure Email Gateway est configuré pour suivre les configurations Syslog configurées dans le cadre des paramètres système d'Unified Access Gateway. Par défaut, seul le contenu du fichier `app.log` dans Secure Email Gateway est déclenché en tant qu'événements Syslog.

Pour plus d'informations sur les configurations Syslog, consultez la section Configurer les paramètres système d'Unified Access Gateway.

VMware Tunnel

Pour plus d'informations, consultez les sections *Journaux d'accès et intégration Syslog* et *Configurer VMware Tunnel* dans la *Documentation du produit VMware Workspace ONE UEM* de VMware Docs.

Exporter les paramètres d'Unified Access Gateway

Exportez les paramètres de configuration d'Unified Access Gateway aux formats JSON et INI à partir de l'interface utilisateur d'administration.

Vous pouvez exporter tous les paramètres de configuration d'Unified Access Gateway et les enregistrer au format JSON ou INI. Vous pouvez utiliser le fichier INI exporté pour déployer Unified Access Gateway à l'aide de scripts Powershell.

Procédure

1 Accédez à **Paramètres de prise en charge > Exporter les paramètres d'**Unified Access Gateway.

2 Cliquez sur **JSON** ou **INI** pour exporter les paramètres d'Unified Access Gateway au format de votre choix. Pour enregistrer les paramètres dans les deux formats, cliquez sur le bouton **Archive de journal**.

   Les fichiers sont enregistrés par défaut dans votre dossier Téléchargements.

Importer les paramètres d'Unified Access Gateway

L'interface utilisateur d'administration d'Unified Access Gateway offre la possibilité d'exporter les paramètres de configuration au format JSON. Après avoir exporté les paramètres de configuration au format JSON, vous pouvez utiliser le fichier JSON exporté pour configurer une version récemment déployée du dispositif Unified Access Gateway.

Procédure

1 Accédez à **Paramètres de prise en charge>Exporter les paramètres d'Unified Access Gateway.**

2 Cliquez sur JSON pour exporter les paramètres d'Unified Access Gateway au format JSON.

   Le fichier est enregistré par défaut dans votre dossier Téléchargements.

3 Supprimez l'ancien dispositif Unified Access Gateway ou mettez-le en mode de mise au repos pour le supprimer ultérieurement.

4 Déployez la nouvelle version du dispositif Unified Access Gateway.

5 Importez le fichier JSON que vous avez précédemment exporté.

Dépannage des erreurs : Content Gateway

Vous pouvez rencontrer des difficultés lorsque vous configurez Content Gateway dans votre environnement. Vous pouvez utiliser la procédure pour diagnostiquer et corriger le problème.

Problème avec la synchronisation, le téléchargement et l’importation des utilisateurs à l'aide de partages hébergés sur des serveurs NetApp.

1 Connectez-vous à Workspace ONE UEM Console.

2 Accédez à la page **Configuration de Content Gateway**.

3 Dans la section **Paramètres de passerelle personnalisés**, cliquez sur **Ajouter une ligne**.

4 Dans le tableau affiché, entrez les valeurs suivantes :

   - **Clé** = `aw.fileshare.jcifs.active`

- **Type**=`Boolean`
- **Valeur**=`true`

  La valeur par défaut est `false`.

5 Cliquez sur **Enregistrer**.

6 Dans l'interface utilisateur d'administration d'Unified Access Gateway, accédez à la page **Paramètres Content Gateway**.

7 Cliquez sur **Enregistrer**.

Note Lorsque les paramètres de l'interface utilisateur d'administration d'Unified Access Gateway sont enregistrés, la configuration de Content Gateway est extraite de Workspace ONE UEM Console et le service Content Gateway est redémarré.

Pour que les modifications de la configuration de Content Gateway prennent effet, vous devez mettre à jour la **Valeur** dans Workspace ONE UEM Console, puis enregistrer les paramètres de Content Gateway dans l'interface utilisateur d'administration d'Unified Access Gateway.

Dépannage de la haute disponibilité

Vous pouvez rencontrer des difficultés lorsque vous configurez Haute disponibilité dans votre environnement. Vous pouvez utiliser diverses procédures pour diagnostiquer et corriger ces problèmes.

1 Connectez-vous à la console Unified Access Gateway.

2 Exécutez la commande `ip addr` pour vérifier si l'adresse IP virtuelle configurée est attribuée à l'interface eth0.

3 Assurez-vous que l'adresse IP virtuelle est attribuée dans le même sous-réseau que l'interface eth0. Vérifiez qu'elle est accessible à partir de la machine client. En cas de problèmes de connectivité, cela pourrait être dû à l'adresse IP virtuelle non unique et déjà attribuée à une machine physique ou virtuelle.

4 Dans le fichier `haproxy.conf` du bundle de journaux, la configuration associée au cluster actuel est disponible. Par exemple,

```
server uag1 127.0.0.1:XXXX .....
server uag2 <IP of machine 2>:XXXX ....
server uag3 <IP of machine 3>:XXXX ....
```

La configuration back-end est basée sur les paramètres configurés dans Unified Access Gateway

- `lb_esmanageris` pour les cas d'utilisation d'Horizon et de proxy inverse Web.
- `lb_cg_server` s'applique aux cas d'utilisation de Content Gateway.
- `lb_tunnel_server` s'applique aux cas d'utilisation de Tunnel.

5 Dans le fichier `haproxy.conf` du bundle de journaux, vous trouverez plus d'informations sur la source de la connexion client, la connexion envoyée correspondante et le serveur Unified Access Gateway qui gère les connexions. Par exemple,

```
2018-11-27T07:21:09+00:00 ipv6-localhost haproxy[15909]:
                incoming:::ffff:<IP of Client:xxxx> backend:lb_esmanager
                connecting-server:uag2/<IP of uag2> connecting-through:<IP of master
                node:xxxx> wait-time:1 connect-time:0 total-incoming:1 total-outgoing:1
                total-to-server:1
```

6 Pour afficher les statistiques, reportez-vous à la section Collecte des journaux à partir du dispositif Unified Access Gateway .

Tableau 7-9. Exemple de fichier CSV

Nom de la colonne	Description
scur	Indique le nombre actuel de connexions simultanées gérées par ce serveur.
smax	Limite supérieure de connexions simultanées gérées par ce serveur durant le temps d'activité en cours.
stot	Indique le nombre total de connexions gérées par ce serveur durant le temps d'activité en cours.
bin	Indique le nombre total d'octets envoyés à ce serveur.
bout	Indique le nombre total d'octets reçus à partir de ce serveur.
status	Indique l'état du serveur. Par exemple, si l'état est Actif ou Inactif. Il est basé sur le dernier contrôle de santé effectué sur ce serveur.

7 Plusieurs problèmes de choix du nœud master peuvent être observés dans les cas suivants,

- Adresse IP virtuelle ou ID de groupe différent configuré sur les nœuds censés former le cluster.
- Adresse IP virtuelle et eth0 dans un sous-réseau différent.
- Plusieurs cartes réseau dans Unified Access Gateway configurées dans le même sous-réseau.

Résolution des problèmes de sécurité : Meilleures pratiques

Lorsque le service détecte un périphérique d'équilibrage de charge dans vos serveurs Web, ces informations supplémentaires relatives à votre réseau sont une vulnérabilité. Vous pouvez utiliser diverses procédures pour diagnostiquer et corriger ces problèmes.

Différentes techniques sont utilisées pour détecter la présence d'un périphérique d'équilibrage de charge, y compris l'analyse des en-têtes HTTP et l'analyse des valeurs de durée de vie (TTL) des adresses IP, des valeurs d'identification (ID) des adresses IP et des numéros de séquence initiale (ISN) de TCP. Le nombre exact de serveurs Web derrière un équilibrage de charge est difficile de déterminer, le nombre indiqué peut donc être incorrect.

En outre, Netscape Enterprise Server Version 3.6 est connu pour afficher un champ de `"Date:"` erronée dans l'en-tête HTTP lorsque le serveur reçoit plusieurs demandes. Cela rend difficile pour le service de déterminer si un périphérique d'équilibrage de charge est présent en analysant les en-têtes HTTP.

En outre, le résultat donné par l'analyse des identifiants des adresses IP et des valeurs ISN de TCP peut varier en raison de conditions de réseau différentes lorsque l'analyse a été effectuée. En exploitant cette vulnérabilité, un intrus pourrait utiliser ces informations en conjonction avec d'autres éléments d'information pour élaborer des attaques sophistiquées à l'encontre de votre réseau.

Note Si les serveurs Web derrière l'équilibrage de charge ne sont pas identiques, les résultats d'analyse pour les vulnérabilités HTTP peuvent varier d'une analyse à une autre.

- Unified Access Gateway est un dispositif qui est normalement installé dans une zone démilitarisée (DMZ). Les étapes ci-dessous vous permettent de protéger Unified Access Gateway contre les analyseurs de vulnérabilité qui détectent ce problème.
  - Pour empêcher la détection de la présence d'un périphérique d'équilibrage de charge basé sur l'analyse des en-têtes HTTP, vous devez utiliser le protocole NTP pour synchroniser les horloges sur tous vos hôtes (au moins ceux de la zone DMZ).
  - Pour empêcher la détection en analysant les valeurs TTL des adresses IP, les valeurs ID des adresses IP et les valeurs ISN de TCP, vous pouvez utiliser des hôtes avec une implémentation TCP/IP qui génère des nombres aléatoires pour ces valeurs. Cependant, la plupart des systèmes d'exploitation disponibles aujourd'hui ne sont pas fournis avec une mise en œuvre de TCP/IP.

Sessions utilisateur impactées par les modifications des paramètres de l'interface utilisateur d'administration d'Unified Access Gateway

En cas de modification de certains paramètres de l'interface utilisateur d'administration d'Unified Access Gateway, il se peut que les sessions XMLAPI existantes (sessions Unified Access Gateway) soient interrompues et que les utilisateurs finaux ne puissent donc pas accéder aux postes de travail et aux applications lancés. Les paramètres modifiés sont susceptibles d'affecter uniquement les postes de travail et les applications lancés, les sessions XMLAPI et de poste de travail ou les sessions d'application.

Vous devez prévoir la modification des paramètres d'interface utilisateur d'administration d'Unified Access Gateway au cours d'une fenêtre de maintenance.

Paramètres de l'interface utilisateur d'administration		Affecte la session d'Unified Access Gateway existante	Affecte les applications et les postes de travail lancés
Importer les paramètres Vous pouvez utiliser cette section de l'interface utilisateur d'administration pour importer le fichier `JSON` précédemment exporté (à partir du déploiement précédent) afin de configurer une version récemment déployée du dispositif Unified Access Gateway.	`Yes`		`Yes`
Paramètres d'Horizon			
Activer PCOIP		`No`	`Yes`
Activer Blast		`No`	`Yes`
Activer l'UDP du serveur Tunnel		`No`	`Yes`
Activer le tunnel		`Yes`	`Yes`
Désactiver le service Horizon Edge		`Yes`	`Yes`
Paramètres d'authentification			
Certificat X.509		`Yes`	`Yes`
Configuration système			
Paramètre régional		`Yes`	`Yes`
Suites de chiffrement		`Yes`	`Yes`
Activer TLS 1.0		`Yes`	`Yes`
Activer TLS 1.1		`Yes`	`Yes`
Activer TLS 1.2		`Yes`	`Yes`
Activer TLS 1.3		`Yes`	`Yes`
URL Syslog		`Yes`	`Yes`
URL d'audit de Syslog		`Yes`	`Yes`
Cookies à mettre en cache		`Yes`	`Yes`
Surveiller l'intervalle		`Yes`	`Yes`
Paramètres réseau	`Yes`		`Yes`
Paramètres de haute disponibilité	`Yes`		`Yes`
Paramètres du certificat de serveur TLS (interface Internet uniquement)	`Yes`		`Yes`