Déploiement et configuration d'Access Point

Access Point 2.0
VMware Horizon 6

Ce document prend en charge la version de chacun des produits répertoriés, ainsi que toutes les versions publiées par la suite jusqu'au remplacement dudit document par une nouvelle édition. Pour rechercher des éditions plus récentes de ce document, rendez-vous sur : http://www.vmware.com/fr/support/pubs.

FR-001879-01

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

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

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

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

docfeedback@vmware.com

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

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

Table des matières

Déploiement et configuration d' Access Point

Déploiement et configuration d'un point d'accès fournit des informations sur la conception d'un déploiement View qui utilise Access Point pour un accès externe sécurisé à des serveurs et des postes de travail Horizon 6. Ce guide contient également des instructions sur le déploiement de dispositifs virtuels Access Point et sur la modification des paramètres de configuration après le déploiement, si nécessaire.

Public visé

Ces informations sont conçues pour toute personne souhaitant déployer et utiliser des dispositifs Access Point dans un environnement Horizon 6. Les informations sont rédigées pour des administrateurs système Linux expérimentés qui connaissent parfaitement la technologie des machines virtuelles et les opérations de datacenter.

Glossaire VMware Technical Publications

Les publications techniques VMware fournissent un glossaire de termes que vous ne connaissez peut-être pas. Pour obtenir la définition des termes tels qu'ils sont utilisés dans la documentation technique de VMware, visitez la page http://www.vmware.com/support/pubs.

Présentation de Access Point 1

Access Point fonctionne comme une passerelle sécurisée pour les utilisateurs qui veulent accéder à des postes de travail et des applications Horizon 6 depuis l'extérieur du pare-feu d'entreprise.

En général, les dispositifs Access Point résident dans une zone DMZ et agissent comme un hôte proxy pour les connexions à l'intérieur du réseau approuvé de votre entreprise. Cette conception offre une couche supplémentaire de sécurité en protégeant les postes de travail virtuels View, les hôtes d'application et les instances du Serveur de connexion View contre les sites Internet destinés au public.

Access Point dirige les demandes d'authentification au serveur approprié et ignore les demandes non authentifiées. Le seul trafic d'application et de poste de travail à distance qui peut entrer dans le centre de données de l'entreprise est le trafic au nom d'un utilisateur dont l'authentification est renforcée. Les utilisateurs ne peuvent accéder qu'aux ressources dont l'accès leur est autorisé.

Les dispositifs Access Point ont le même rôle que celui joué précédemment par les serveurs de sécurité View, mais Access Point apporte des avantages supplémentaires :

- Un dispositif Access Point peut être configuré pour pointer vers une instance du Serveur de connexion View ou vers un équilibrage de charge qui fait face à un groupe d'instances du Serveur de connexion View. Cette conception signifie que vous pouvez combiner le trafic distant et le trafic local.
- La configuration d'Access Point est indépendante des instances du Serveur de connexion View. Contrairement aux serveurs de sécurité, aucun mot de passe de couplage n'est requis pour coupler chaque serveur de sécurité avec une instance du Serveur de connexion View.
- Les dispositifs Access Point sont déployés en tant que dispositifs virtuels renforcés, qui sont basés sur un dispositif Linux qui a été personnalisé pour fournir un accès sécurisé. Les modules étrangers ont été supprimés pour réduire les accès dangereux potentiels.
- Access Point utilise un protocole HTTP(S) standard pour les communications avec le Serveur de connexion View. JMS, IPsec et AJP13 ne sont pas utilisés.

Les mécanismes d'authentification suivants sont disponibles et, pour tous ces mécanismes sauf l'authentification par carte à puce, l'authentification se fait en proxy sur le Serveur de connexion View :

- Informations d'identification Active Directory
- RSA SecurID
- RADIUS
- Cartes à puce (Notez que pour cette version, l'authentification par carte à puce est une fonctionnalité de la version d'évaluation technique.)
- SAML (Security Assertion Markup Language)

Ce chapitre aborde les rubriques suivantes :

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

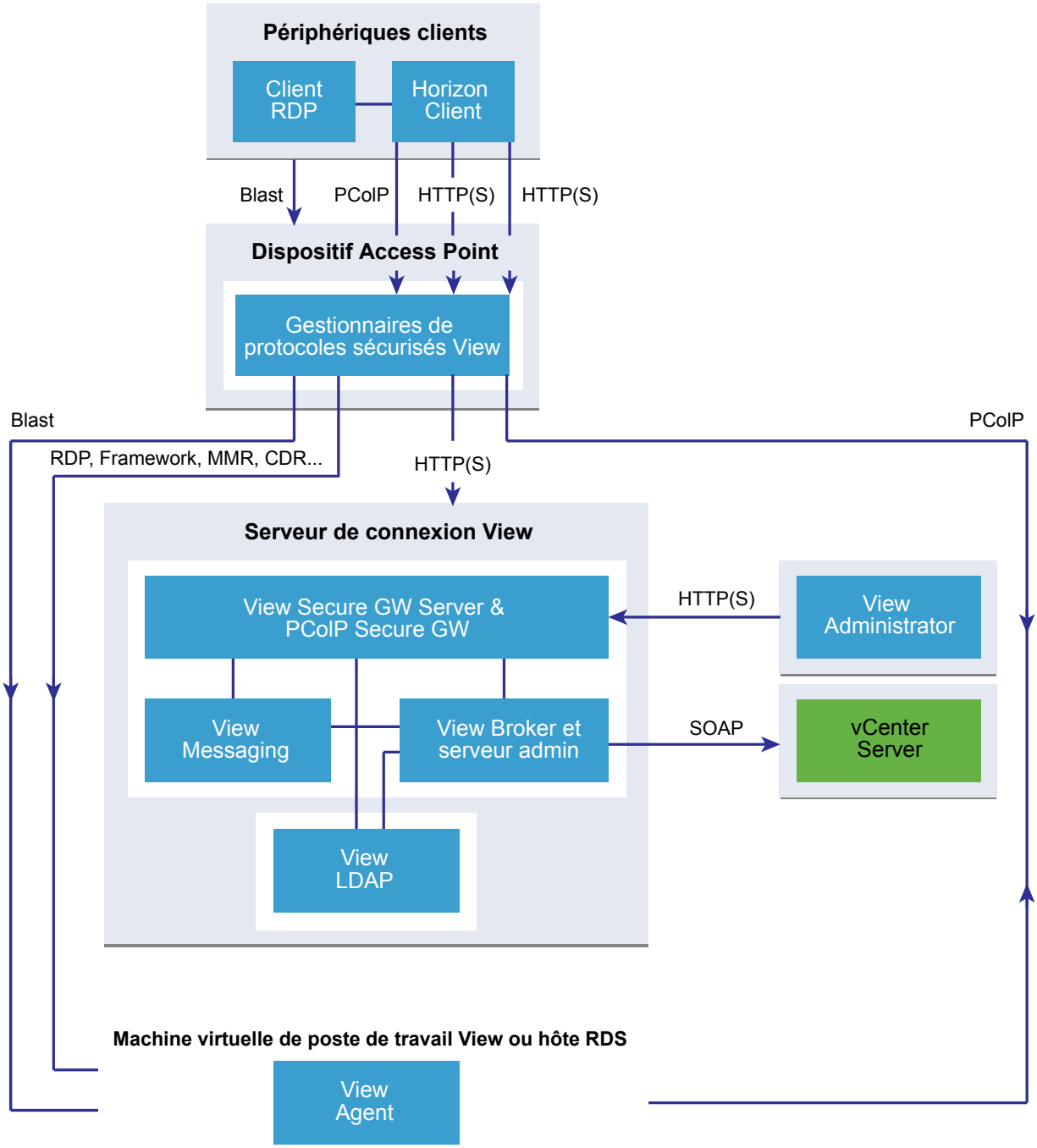
Les dispositifs Access Point basés sur une zone DMZ requièrent certaines règles de pare-feu sur les pare-feu frontaux et principaux. Lors de l'installation, les services Access Point sont configurés pour écouter sur certains ports réseau par défaut.

En général, un déploiement de dispositif Access Point 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 figure suivante indique les protocoles que chaque composant View utilise pour les communications. Cette configuration peut être utilisée dans un déploiment WAN classique.

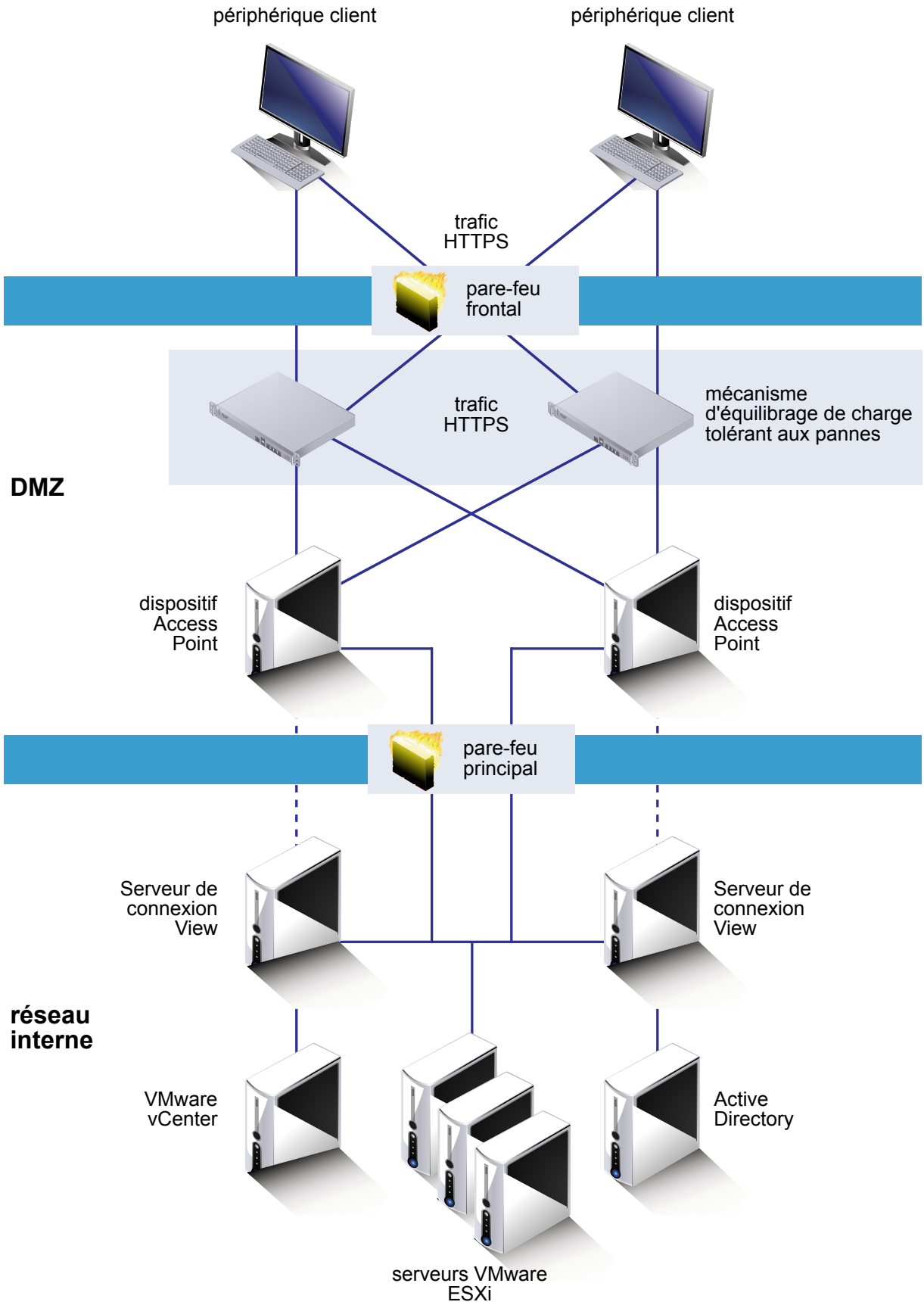
Figure 1-1. Composants View et protocoles avec Access Point



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

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

Figure 1-2. Topologie de double pare-feu



Règles de pare-feu frontal

Pour autoriser des périphériques client externes à se connecter à un dispositif Access Point dans la zone DMZ, le pare-feu frontal doit autoriser le trafic sur certains ports TCP et UDP.

Tableau 1-1. Règles de pare-feu frontal

Source	Port par défaut	Protocole	Destination	Port de destination	Remarques
Horizon Client	Tout port TCP	HTTP	Dispositif Access Point	TCP 80	(Facultatif) Des périphériques client externes se connectent à un dispositif Access Point dans la zone DMZ sur le port TCP 80 et sont automatiquement dirigés vers HTTPS. Pour plus d'informations sur les aspects de la sécurité liés au fait de laisser les utilisateurs se connecter avec HTTP plutôt qu'avec HTTPS, reportez-vous au guide *Sécurité de View*.
Horizon Client	Tout port TCP	HTTPS	Dispositif Access Point	TCP 443	Des périphériques client externes se connectent à un dispositif Access Point dans la zone DMZ sur le port TCP 443.
Horizon Client	Tout port TCP Tout port UDP	PCoIP	Dispositif Access Point	TCP 4172 UDP 4172	Des périphériques client externes se connectent à un dispositif Access Point dans la zone DMZ sur le port TCP 4172 et sur le port UDP 4172 pour communiquer avec une application ou un poste de travail distant sur PCoIP.
Dispositif Access Point	UDP 4172	PCoIP	Horizon Client	Tout port UDP	Des dispositifs Access Point renvoient des données PCoIP à un périphérique client externe à partir du port UDP 4172. Le port UDP de destination est le port source des paquets UDP reçus. Comme ces paquets contiennent des données de réponse, il est normalement inutile d'ajouter une règle de pare-feu explicite pour ce trafic.
Navigateur Web client	Tout port TCP	HTTPS ou Blast	Dispositif Access Point	TCP 8443	Si vous utilisez HTML Access, le Web Client externe se connecte à un dispositif Access Point dans la zone DMZ sur le port HTTPS 8443 pour communiquer avec les postes de travail distants.

Règles de pare-feu principal

Pour autoriser un dispositif Access Point à communiquer avec une instance du Serveur de connexion View ou un équilibrage de charge qui réside sur le réseau interne, le pare-feu principal doit autoriser le trafic entrant sur certains ports TCP. Derrière le pare-feu principal, les pare-feu internes doivent être configurés de la même manière pour autoriser les applications et postes de travail distants et les instances du Serveur de connexion View à communiquer entre eux.

Tableau 1-2. Règles de pare-feu principal

Port source	Port par défaut	Protocole	Destination	Port de destination	Remarques
Dispositif Access Point	Tout port TCP	HTTPS	Serveur de connexion View ou équilibrage de charge	TCP 443	Des dispositifs Access Point se connectent sur le port TCP 443 pour communiquer avec une instance du Serveur de connexion View ou un équilibrage de charge devant plusieurs instances du Serveur de connexion View.
Dispositif Access Point	Tout port TCP	RDP	Poste de travail distant	TCP 3389	Des dispositifs Access Point se connectent à des postes de travail distants sur le port TCP 3389 pour échanger du trafic RDP.

Tableau 1-2. Règles de pare-feu principal (suite)

Port source	Port par défaut	Protocole	Destination	Port de destination	Remarques
Dispositif Access Point	Tout port TCP	MMR ou CDR	Poste de travail distant	TCP 9427	Des dispositifs Access Point se connectent à des postes de travail distants sur le port TCP 9427 pour recevoir le trafic MMR (redirection multimédia) ou CDR (redirection de lecteur client).
Dispositif Access Point	Tout port TCP Tout port UDP	PCoIP	Application ou poste de travail distant	TCP 4172 UDP 4172	Des dispositifs Access Point se connectent aux applications et postes de travail distants sur le port TCP 4172 et le port UDP 4172 pour échanger du trafic PCoIP.
Application ou poste de travail distant	UDP 4172	PCoIP	Dispositif Access Point	Tout port UDP	Des applications et des postes de travail distants renvoient des données PCoIP à un dispositif Access Point à partir du port UDP 4172. Le port UDP de destination sera le port source des paquets UDP reçus. Comme ces paquets sont des données de réponse, il est normalement inutile d'ajouter une règle de pare-feu explicite pour cela.
Dispositif Access Point	Tout port TCP	USB-R	Poste de travail distant	TCP 32111	Des dispositifs Access Point se connectent à des postes de travail distants sur le port TCP 32111 pour échanger le trafic de redirection USB entre un périphérique client externe et le poste de travail distant.
Dispositif Access Point	Tout port TCP	HTTPS	Poste de travail distant	TCP 22443	Si vous utilisez HTML Access, des dispositifs Access Point se connectent à des postes de travail distants sur le port HTTPS 22443 pour communiquer avec l'agent Blast.

Remarque Access Point peut éventuellement écouter sur le port TCP 9443 le trafic de l'API REST d'administrateur et envoyer les événements Syslog sur le port UDP 514 par défaut. Si un pare-feu est en place pour cette communication, ces ports ne doivent pas être bloqués.

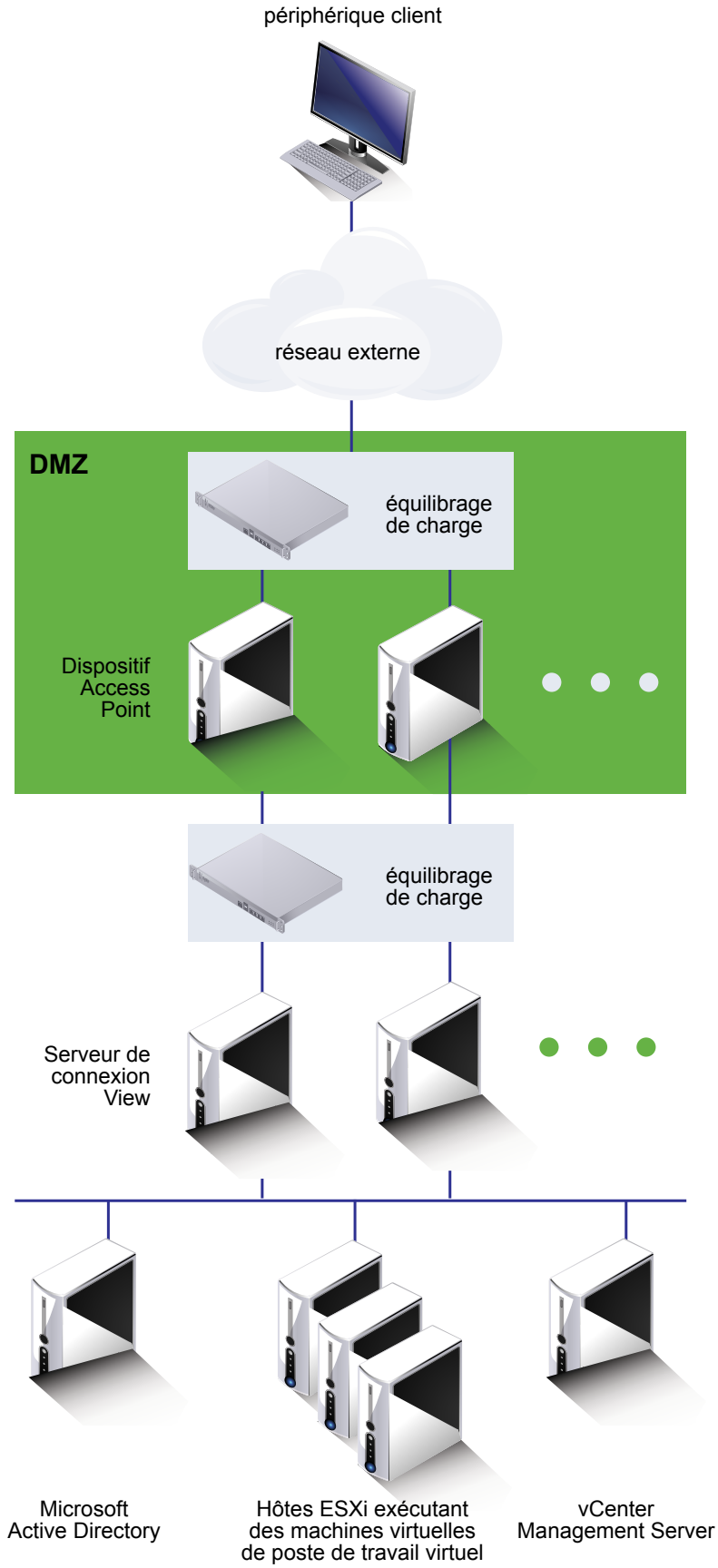
Topologies d' Access Point

Vous pouvez implémenter plusieurs topologies différentes.

Un dispositif Access Point dans la DMZ peut être configuré pour pointer vers une instance du Serveur de connexion View ou vers un équilibrage de charge qui fait face à un groupe d'instances du Serveur de connexion View. Les dispositifs Access Point fonctionnent avec des solutions d'équilibrage de charge tierces standard qui sont configurées pour HTTPS.

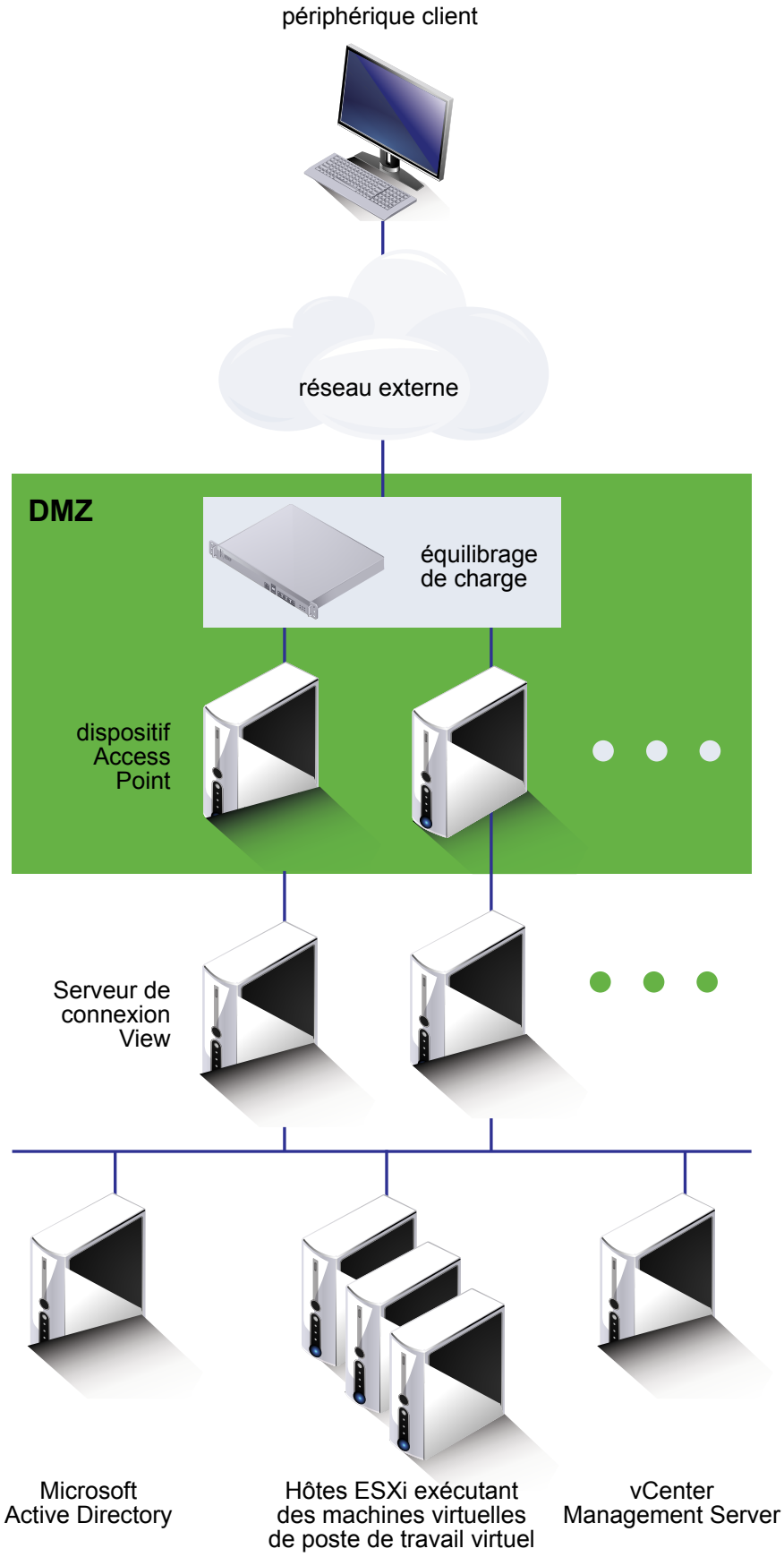
Si le dispositif Access Point pointe vers un équilibrage de charge devant les instances du Serveur de connexion View, la sélection de l'instance du Serveur de connexion View est dynamique. Par exemple, l'équilibrage de charge peut faire une sélection en fonction de la disponibilité et de sa connaissance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

Figure 1-3. Dispositif Access Point pointant vers un équilibrage de charge



Vous pouvez également régler un ou plusieurs dispositifs Access Point pour qu'ils pointent vers une instance du Serveur de connexion View individuelle, comme c'était le cas avec les serveurs de sécurité View. Avec les deux approches, utilisez un équilibrage de charge devant deux dispositifs Access Point ou plus dans la zone DMZ.

Figure 1-4. Dispositif Access Point pointant vers une instance du Serveur de connexion View



Configuration système requise et déploiement

2

Vous déployez un dispositif Access Point à peu près comme vous déployez d'autres dispositifs virtuels VMware.

Ce chapitre aborde les rubriques suivantes :

Configuration système pour Access Point

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

Exigences logicielles

Access Point 2.0 est conçu pour s'intégrer à Horizon 6 version 6.2.

- Serveurs Horizon 6 : lors d'une mise à niveau de ces composants, assurez-vous que les instances du Serveur de connexion View sont mises à niveau vers la version 6.2 avant d'utiliser des dispositifs Access Point. Access Point n'est pas conçu pour interagir avec des versions antérieures du Serveur de connexion.
- Hôtes ESX/ESXi vSphere et vCenter Server : les dispositifs Access Point doivent être déployés sur une version de vSphere qui est la même qu'une version prise en charge pour Horizon 6.2.

  Pour plus d'informations sur les versions d'View compatibles avec les versions de vCenter Server et d'ESXi, consultez la matrice d'interopérabilité des produits VMware à l'adresse http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.
- Horizon Client : même si VMware vous recommande d'effectuer la mise à niveau vers la dernière version des clients pour obtenir de nouvelles fonctionnalités et améliorer les performances, Access Point 2.0 est conçu pour fonctionner avec toutes les versions de client prises en charge avec Serveur de connexion View 6.2 et View Agent 6.2.

Configuration matérielle requise

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

Exigences requises pour la mise en réseau

Vous pouvez utiliser une, deux ou trois interfaces réseau, et Access Point requiert une adresse IP statique séparée pour chacune d'entre elles.

- 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.

Préparation du Serveur de connexion View pour l'utiliser avec Access Point

Les administrateurs doivent effectuer des tâches spécifiques pour s'assurer que le Serveur de connexion View fonctionne correctement avec Access Point.

- Si vous prévoyez d'utiliser une connexion par tunnel sécurisé pour les périphériques client, désactivez le tunnel sécurisé pour le Serveur de connexion View. Dans View Administrator, accédez à la boîte de dialogue Modifier les paramètres du Serveur de connexion View et décochez la case nommée **Utiliser une connexion par tunnel sécurisé à la machine**. Par défaut, le tunnel sécurisé est activé sur le dispositif Access Point.
- Désactivez PCoIP Secure Gateway pour le Serveur de connexion View. Dans View Administrator, accédez à la boîte de dialogue Modifier les paramètres du Serveur de connexion View et décochez la case nommée **Utiliser PCoIP Secure Gateway pour les connexions PCoIP à la machine**. Par défaut, PCoIP Secure Gateway est activé sur le dispositif Access Point.
- Désactivez Blast Secure Gateway pour le Serveur de connexion View. Dans View Administrator, accédez à la boîte de dialogue Modifier les paramètres du Serveur de connexion View et décochez la case nommée **Utiliser Blast Secure Gateway pour un HTML Access à la machine**. Par défaut, Blast Secure Gateway est activé sur le dispositif Access Point.
- Pour pouvoir utiliser une authentification à deux facteurs, telle que l'authentification RSA SecurID ou RADIUS, avec Horizon Client, vous devez activer cette fonctionnalité sur le Serveur de connexion View. Consultez les rubriques concernant l'authentification à deux facteurs dans le document *Administration de View*.

Déployer le dispositif Access Point

La façon la plus simple de déployer le dispositif Access Point consiste à ouvrir une session sur vCenter Server et à utiliser l'assistant Déployer le modèle OVF. L'ouverture de session directement sur un hôte ESXi pour utiliser l'assistant de déploiement n'est pas prise en charge.

Si vous préférez utiliser l'outil VMware OVF Tool de ligne de commande pour déployer le dispositif, reportez-vous à la section « Utilisation de VMware OVF Tool pour déployer le dispositif Access Point », page 21. Avec cet outil, vous pouvez définir des propriétés avancées qui ne sont pas disponibles dans l'assistant de déploiement.

Remarque Pour les environnements de production, VMware vous recommande d'utiliser VMware OVF Tool plutôt que l'assistant de déploiement pour assurer une installation répétable via des scripts. Cette méthode permet également de définir des paramètres avancés, tels que la configuration des URL externes et le certificat de serveur TLS/SSL à appliquer au moment du déploiement. L'assistant de déploiement interactif n'inclut pas ces paramètres avancés.

Prérequis

- Familiarisez-vous avec les options de déploiement disponibles dans l'assistant. Reportez-vous à

  « Propriétés du déploiement d'Access Point », page 23. Les options suivantes sont requises : adresse IP statique du dispositif Access Point, adresse IP du serveur DNS, mot de passe de l'utilisateur racine et URL de l'instance du Serveur de connexion View ou de l'équilibrage de charge vers lequel pointera ce dispositif Access Point.

- Déterminez combien d'interfaces réseau et d'adresses IP statiques configurer pour le dispositif Access Point. Reportez-vous à la section « Exigences requises pour la mise en réseau », page 18.

  Si vous utilisez vSphere Web Client, vous devez également spécifier les adresses du serveur DNS, de la passerelle et du masque réseau pour chaque réseau. Si vous utilisez le vSphere Client natif, vérifiez que vous avez affecté un pool IP à chaque réseau. Pour ajouter un pool IP, dans vCenter Server, allez dans l'onglet **Pools IP** du centre de données.

- Vérifiez que vous pouvez ouvrir une session sur vSphere Client ou vSphere Web Client en tant qu'utilisateur avec des privilèges d'**administrateur système**. Par exemple, vous pouvez ouvrir une session en tant que l'utilisateur administrator@vsphere.local.

  Si vous utilisez vSphere Web Client, utilisez un navigateur pris en charge. Consultez la rubrique « Configuration logicielle requise pour le plug-in d'intégration du client » dans le centre de documentation vSphere pour votre version de vSphere.

- Vérifiez que la banque de données que vous prévoyez d'utiliser pour le dispositif a un espace disque libre suffisant et qu'elle répond aux autres spécifications système. La taille de téléchargement du dispositif virtuel est de 1,4 Go. Par défaut, pour un disque à provisionnement fin, le dispositif requiert 2,5 Go et un disque à provisionnement statique requiert 20 Go. Reportez-vous également à la section « Configuration système pour Access Point », page 17.

- Téléchargez le fichier du programme d'installation `.ova` du dispositif Access Point 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-2.0.0.0-xxxxxxx_OVF10.ova`).

- Si vous prévoyez d'utiliser vSphere Web Client, vérifiez que le plug-in d'intégration du client est installé. Pour plus d'informations, voir la documentation vSphere. Par exemple, pour vSphere 6, voir Installer le plug-in d'intégration du client. Si vous n'installez pas ce plug-in avant de démarrer l'assistant de déploiement, l'assistant vous invite à installer le plug-in, ce qui implique la fermeture de votre navigateur et de l'assistant.

Procédure

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

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 **Actions > Déployer le modèle OVF**.

3 Sur la page Sélectionner la source de l'assistant, accédez à l'emplacement du fichier `.ova` que vous avez téléchargé ou entrez une URL et cliquez sur **Suivant**.

Une page de détails apparaît qui indique l'espace disque dont le dispositif a besoin.

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

Option	Description
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.
Stratégie de stockage VM	(vSphere Web Client uniquement) Cette option est disponible si des stratégies de stockage sont activées sur la ressource de destination.
Informations d'identification d'administrateur pour l'API REST	Même si ce paramètre n'est pas strictement requis, pour les environnements de production, VMware recommande fortement de définir des informations d'identification d'administrateur.
(Autres options)	Le texte sur chaque page de l'assistant explique chaque contrôle. Dans certains cas, le texte change de façon dynamique à mesure que vous sélectionnez diverses options. 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. Si vous utilisez vSphere Web Client, pour vous aider, vous pouvez également cliquer sur le bouton d'aide contextuelle, qui est une icône de point d'interrogation (**?**) dans le coin supérieur droit de l'assistant.

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

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

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

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

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

Si le déploiement réussit, le portail Web d'Horizon apparaît. 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.

7 Pour vérifier que les informations d'identification d'administrateur pour accéder à l'API REST ont été correctement définies, ouvrez un navigateur, entrez l'URL suivante et entrez les informations d'identification de l'utilisateur administrateur.

   `https://FQDN-of-AP-appliance:9443/rest/swagger.yaml`

   Une page contenant la spécification de l'API REST Access Point apparaît. Si vous obtenez un message d'erreur, vous pouvez déployer de nouveau le dispositif et veiller à suivre les exigences du mot de passe ou vous pouvez ouvrir une session sur la machine virtuelle Access Point et définir le mot de passe administrateur à l'aide de l'API REST.

Le dispositif Access Point est déployé et démarre automatiquement.

Suivant

Configurez des certificats de sécurité pour Access Point. Si vous n'avez pas défini les informations d'identification d'administrateur correctement pour l'API REST, vous pouvez les définir à l'aide de la procédure « Réinitialiser le mot de passe administrateur pour l'API REST Access Point », page 28.

Important Configurez l'horloge (UTC) sur le dispositif Access Point pour qu'il soit à l'heure exacte. Par exemple, vérifiez que l'heure de l'hôte ESXi est synchronisée avec un serveur NTP, et vérifiez que VMware Tools, qui est exécuté dans la machine virtuelle de dispositif, synchronise l'heure sur la machine virtuelle avec l'heure sur l'hôte ESXi.

Utilisation de VMware OVF Tool pour déployer le dispositif Access Point

Comme alternative à l'utilisation de l'assistant de déploiement, vous pouvez utiliser cet outil de ligne de commande pour déployer Access Point. L'utilisation de cet outil vous permet de définir des options de configuration qui ne sont pas disponibles dans l'assistant de déploiement.

Vous pouvez télécharger VMware OVF Tool et sa documentation à l'adresse https://www.vmware.com/support/developer/ovf/. En plus des commandes standard décrites dans la documentation d'OVF Tool, vous pouvez utiliser des options spécifiques d'Access Point. Pour consulter une liste des propriétés et options disponibles, reportez-vous à la section « Propriétés du déploiement d'Access Point », page 23.

Exemple d'utilisation de propriétés de déploiement d' Access Point

Voici un exemple de commande pour déployer un dispositif Access Point à l'aide d'OVF Tool sur une machine cliente Windows :

```
ovftool --X:enableHiddenProperties --powerOffTarget --powerOn --overwrite --vmFolder=folder1 ^
     --net:Internet="VM Network" --net:ManagementNetwork="VM Network" --net:BackendNetwork="VM
Network" ^
     -ds=PERFORMANCE-X --name=name1 --ipAllocationPolicy=fixedPolicy ^
     --deploymentOption=onenic --prop:ip0=10.20.30.41 --prop:DNS=192.0.2.1 ^
     --prop:adminPassword=P@ssw0rd --prop:rootPassword=vmware ^
     --prop:viewDestinationURL=https://192.0.2.2 --prop:viewDestinationURLThumbprints="sha1=b6
77 dc 9c 19 94 2e f1 78 f0 ad 4b ec 85 d1 7a f8 8b dc 34" ^
      euc-access-point-2.0.0.0-xxxxxxx_OVF10.ova ^
     vi://root:password@vc.example.com/ExampleDC/host/ap
```

Remarque Les carets à la fin des lignes sont des caractères d'échappement pour la continuation de ligne sous Windows. Vous pouvez également saisir simplement toute la commande sur une seule ligne.

Voici un exemple de commande pour déployer un dispositif Access Point à l'aide d'OVF Tool sur une machine cliente Linux :

```
ovftool --X:enableHiddenProperties --powerOffTarget --powerOn --overwrite --vmFolder=folder1 \
     --net:Internet="VM Network" --net:ManagementNetwork="VM Network" --net:BackendNetwork="VM
Network" \
     -ds=PERFORMANCE-X --name=name1 --ipAllocationPolicy=fixedPolicy \
     --deploymentOption=onenic --prop:ip0=10.20.30.41 --prop:DNS=192.0.2.1 \
     --prop:adminPassword=P@ssw0rd --prop:rootPassword=vmware \
     --prop:viewDestinationURL=https://192.0.2.2 --prop:viewDestinationURLThumbprints="sha1=b6
77 dc 9c 19 94 2e f1 78 f0 ad 4b ec 85 d1 7a f8 8b dc 34" \
      euc-access-point-2.0.0.0-xxxxxxx_OVF10.ova \
     vi://root:password@vc.example.com/ExampleDC/host/ap
```

Remarque Les barres obliques inversées à la fin des lignes sont des caractères d'échappement pour la continuation de ligne sous Linux. Vous pouvez également saisir simplement toute la commande sur une seule ligne.

Si vous utilisez cette commande, vous pouvez utiliser l'API REST d'administrateur Access Point pour configurer des paramètres supplémentaires, tels que le certificat de sécurité et les passerelles sécurisées. Vous pouvez également utiliser la propriété `settingsJSON` pour configurer ces paramètres au moment du déploiement.

Exemple d'utilisation de la propriété settings.JSON

En plus des propriétés de déploiement indiquées dans l'exemple précédent, vous pouvez utiliser la propriété `settingsJSON` pour transmettre une chaîne JSON directement à la ressource `SettingsResource` dans l'API REST d'administrateur d'Access Point. De cette manière, vous pouvez utiliser OVF Tool pour définir des propriétés de configuration au cours du déploiement qui doivent sinon être définies à l'aide de l'API REST après le déploiement.

L'exemple suivant montre comment utiliser la propriété `settingsJSON` pour définir les URL externes pour les passerelles sécurisées. Cet exemple utilise des caractères d'échappement pour exécuter la commande sur une machine cliente Windows.

```
ovftool --X:enableHiddenProperties --powerOffTarget --powerOn --overwrite --vmFolder=folder1 ^
     --net:Internet="VM Network" --net:ManagementNetwork="VM Network" --net:BackendNetwork="VM
Network" ^
     --deploymentOption=onenic --prop:ip0=10.20.30.41   --prop:DNS=192.0.2.1 ^
     -ds="PERFORMANCE-X" --name=name1 --ipAllocationPolicy=fixedPolicy ^
     --prop:adminPassword=P@ssw0rd --prop:rootPassword=vmware ^
     --prop:settingsJSON="{\"edgeServiceSettingsList\": { \"edgeServiceSettingsList\": ^
    [ { \"identifier\": \"VIEW\", \"enabled\":
true, \"proxyDestinationUrl\": \"https://192.0.2.2\", ^
     \"proxyDestinationUrlThumbprints\": \"sha1=b6 77 dc 9c 19 94 2e f1 78 f0 ad 4b ec 85 d1 7a
f8 8b dc 34\", ^
     \"pcoipEnabled\": true, \"pcoipExternalUrl\": \"10.20.30.40:4172\", ^
     \"blastEnabled\": true, \"blastExternalUrl\": \"https://ap1.example.com:8443\", ^
     \"tunnelEnabled\": true, \"tunnelExternalUrl\": \"https://ap1.example.com:443\" ^
     \"proxyPattern\":\"/\" } ] }}" ^
      euc-access-point-2.0.0.0-xxxxxxx_OVF10.ova ^
     vi://root:password@vc.example.com/ExampleDC/host/ap
```

L'exemple suivant montre comment utiliser la propriété `settingsJSON` pour définir les URL externes pour les passerelles sécurisées. Cet exemple utilise des caractères d'échappement pour exécuter la commande sur une machine cliente Linux.

```
ovftool --X:enableHiddenProperties --powerOffTarget --powerOn --overwrite --vmFolder=folder1 \
     --net:Internet="VM Network" --net:ManagementNetwork="VM Network" --net:BackendNetwork="VM
Network"  \
     --deploymentOption=onenic --prop:ip0=10.20.30.41 --prop:DNS=192.0.2.1  \
     -ds=PERFORMANCE-X --name=name1 --ipAllocationPolicy=fixedPolicy  \
     --prop:adminPassword=P@ssw0rd --prop:rootPassword=vmware \
     --prop:settingsJSON='{"edgeServiceSettingsList": { "edgeServiceSettingsList": \
    [ { "identifier": "VIEW", "enabled": true, "proxyDestinationUrl": "https://192.0.2.2", \
     "proxyDestinationUrlThumbprints": "sha1=b6 77 dc 9c 19 94 2e f1 78 f0 ad 4b ec 85 d1 7a f8
8b dc 34", \
     "pcoipEnabled": true, "pcoipExternalUrl": "10.20.30.40:4172", \
     "blastEnabled": true, "blastExternalUrl": "https://ap1.example.com:8443", \
     "tunnelEnabled": true, "tunnelExternalUrl": "https://ap1.example.com:443", \
     "proxyPattern":"/"  } ] }}' \
      euc-access-point-2.0.0.0-xxxxxxx_OVF10.ova  \
     vi://root:password@vc.example.com/ExampleDC/host/ap
```

Important Vous devez configurer les URL externes pour le tunnel sécurisé, PCoIP Secure Gateway et Blast Secure Gateway au moment du déploiement. Vous pouvez effectuer cette configuration à l'aide d'OVF Tool ou via l'API REST. Cette étape de configuration doit être réalisée pour que vous puissiez utiliser Access Point pour le trafic View. Pour plus d'informations sur ces URL, reportez-vous à la section « Configuration des passerelles sécurisées », page 36.

Pour consulter une liste des propriétés de l'API REST pour configurer Access Point, reportez-vous à la section « Propriétés de l'API REST pour Access Point », page 29.

Propriétés du déploiement d'Access Point

Pour vous faciliter la tâche, la plupart des propriétés de déploiement peuvent être définies à l'aide de l'assistant de déploiement ou de l'interface de ligne de commande OVF Tool.

Pour plus d'informations sur la spécification de ces propriétés à l'aide de l'assistant de déploiement, reportez-vous à la section « Déployer le dispositif Access Point », page 19. Pour spécifier les propriétés à l'aide de l'interface de ligne de commande OVF Tool, reportez-vous à la section « Utilisation de VMware OVF Tool pour déployer le dispositif Access Point », page 21.

Tableau 2-1. Options de déploiement d' Access Point

Propriété de déploiement	Option d'OVF Tool	Description
Configuration du déploiement	`--deploymentOption {onenic|twonic|threenic}`	Spécifie le nombre d'interfaces réseau disponibles dans la machine virtuelle Access Point. Par défaut, cette propriété n'est pas définie, ce qui signifie qu'une seule carte réseau est utilisée.
Adresse IP externe (accessible sur Internet)	`--prop:ip0=`*external-ip-address*	(Obligatoire) Spécifie l'adresse IPv4 publique utilisée pour accéder à cette machine virtuelle sur Internet. **Remarque** Le nom d'ordinateur est défini via une requête DNS de cette adresse IPv4 Internet. Valeur par défaut : aucune.

Tableau 2-1. Options de déploiement d' Access Point (suite)

Propriété de déploiement	Option d'OVF Tool	Description
Adresse IP du réseau de gestion	`--prop:ip1=`*management-ip-address*	Spécifie l'adresse IP de l'interface connectée au réseau de gestion. Si elle n'est pas configurée, le serveur d'administration écoute sur l'interface accessible sur Internet. Valeur par défaut : aucune.
Adresse IP du réseau principal	`--prop:ip2=`*backend-ip-address*	Spécifie l'adresse IP de l'interface connectée au réseau principal. Si elle n'est pas configurée, le trafic réseau envoyé aux systèmes principaux est dirigé vers les autres interfaces réseau. Valeur par défaut : aucune.
Adresses de serveur DNS	`--prop:DNS=`*ip-of-name-server1*[*ip-of-name-server2* ...]	(Obligatoire) Spécifie une ou plusieurs adresses IPv4 séparées par un espace des serveurs de nom de domaine pour cette machine virtuelle (exemple : 192.0.2.1 192.0.2.2). Vous pouvez spécifier jusqu'à trois serveurs. Par défaut, cette propriété n'est pas définie, ce qui signifie que le système utilise le serveur DNS associé à la carte réseau accessible sur Internet. **Avertissement** Si vous laissez cette option vide et qu'aucun serveur DNS n'est associé à la carte réseau accessible sur Internet, le dispositif ne sera pas déployé correctement.
Mot de passe de l'utilisateur racine	`--prop:rootPassword=` *password*	(Obligatoire) Spécifie le mot de passe de l'utilisateur racine de cette machine virtuelle. Le mot de passe doit être un mot de passe Linux valide. Valeur par défaut : aucune.
Mot de passe de l'utilisateur administrateur	`--prop:adminPassword=` *password*	Si vous ne définissez pas ce mot de passe, vous ne pourrez pas accéder à l'API REST sur le dispositif Access Point. 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 ! @ # $ % * ( ). Valeur par défaut : aucune.
Paramètre régional à utiliser pour les messages localisés	`--prop:locale=`*locale-code*	(Obligatoire) Spécifie le paramètre régional à utiliser pour générer les messages d'erreur. ■ **`us_EN`** pour l'anglais ■ **`ja_JP`** pour le japonais ■ **`fr_FR`** pour le français ■ **`de_DE`** pour l'allemand ■ **`zh_CN`** pour le chinois simplifié ■ **`zh_TW`** pour le chinois traditionnel ■ **`ko_KR`** pour le coréen Valeur par défaut : en_US.

Tableau 2-1. Options de déploiement d' Access Point (suite)

Propriété de déploiement	Option d'OVF Tool	Description
URL du serveur Syslog	`--prop:syslogUrl=`*url-of-syslog-server*	Spécifie le serveur Syslog utilisé pour journaliser les événements Access Point. Cette valeur peut être une URL, un nom d'hôte ou une adresse IP. Le schéma et le numéro de port sont facultatifs (exemple : syslog://server.example.com:514). Par défaut, cette propriété n'est pas définie, ce qui signifie qu'aucun événement n'est journalisé sur un serveur Syslog.
URL du serveur Horizon	`--prop:viewDestinationURL=`*URL*	(Obligatoire) Spécifie l'URL de destination de l'équilibrage de charge ou du Serveur de connexion View vers laquelle le dispositif Access Point dirige le trafic. L'URL de destination doit contenir le protocole, le nom d'hôte ou l'adresse IP et le numéro de port (exemple : https://load-balancer.example.com:443) Valeur par défaut : aucune.
Empreintes numériques du Serveur de connexion Horizon	`--prop:viewDestinationURLThumbprints=` *thumbprint-list*	Si vous ne fournissez pas une liste d'empreintes numériques séparées par une virgule, les certificats de serveur doivent être émis par une autorité de certification approuvée. Le format inclut l'algorithme (sha1 ou md5) et les chiffres d'empreinte numérique hexadécimaux (exemple : sha1=b6 77 dc 9c 19 94 2e f1 78 f0 ad 4b ec 85 d1 7a f8 8b dc 34). Pour trouver ces propriétés, accédez au Serveur de connexion View, cliquez sur l'icône de verrouillage dans la barre d'adresses et affichez les détails du certificat. Valeur par défaut : aucune.

Vous pouvez également utiliser la propriété `settingsJSON` pour spécifier d'autres paramètres de configuration d'API REST à l'aide d'OVF Tool, comme pour configurer les URL externes des passerelles sécurisées. Pour plus d'informations, reportez-vous à la section « Exemple d'utilisation de la propriété settings.JSON », page 22.

Configuration d' Access Point 3

Vous utilisez l'API REST Access Point pour configurer Access Point.

IMPORTANT Après le déploiement, la première tâche de configuration consiste à configurer l'horloge (UTC) sur le dispositif Access Point pour qu'il soit à l'heure exacte. Par exemple, vérifiez que l'heure de l'hôte ESXi est synchronisée avec un serveur NTP, et vérifiez que VMware Tools, qui est exécuté dans la machine virtuelle de dispositif, synchronise l'heure sur la machine virtuelle avec l'heure sur l'hôte ESXi. Utilisez vCenter Server, au lieu de l'API REST, pour cette tâche de configuration.

Ce chapitre aborde les rubriques suivantes :

Utilisation de l'API REST Access Point

Même si vous pouvez configurer plusieurs paramètres lors du déploiement du dispositif, après avoir déployé le dispositif Access Point, vous devez utiliser l'API REST Access Point pour modifier ou ajouter des paramètres de configuration.

La spécification de l'API REST Access Point est disponible à l'adresse suivante sur la machine virtuelle sur laquelle Access Point est installé : `https://access-point-appliance.example.com:9443/rest/swagger.yaml`.

Vous pouvez utiliser n'importe quelle application cliente REST, telle que `curl` ou `postman`. Par exemple, la commande suivante utilise un client `curl` pour récupérer la configuration d'Access Point :

```
curl -k -u 'admin:P@ssw0rd' https://access-point-appliance.example.com:
9443/rest/v1/config/settings
```

Dans cet exemple, *P@ssw0rd* est le mot de passe de l'utilisateur administrateur et *access-point-appliance.example.com* est le nom de domaine complet du dispositif Access Point. Il est préférable, pour des raisons de sécurité, d'omettre le mot de passe pour l'utilisateur administrateur de tous les scripts. Lorsque le mot de passe est omis, la commande `curl` vous invite à le fournir et s'assure qu'aucun mot de passe n'est stocké par mégarde dans les fichiers de script.

Utilisez également des demandes JSON pour appeler l'API REST Access Point et apporter des modifications de configuration. L'exemple suivant indique une demande JSON de configuration pour le service Edge de View :

```
{
  "identifier": "VIEW",
  "enabled": true,
  "proxyDestinationUrl": "https://192.0.2.1",
```

```
  "proxyDestinationUrlThumbprints": "sha1=b6 77 dc 9c 19 94 2e f1 78 f0 ad 4b ec 85 d1 7a f8 8b
dc 34",
  "pcoipEnabled": true,
  "pcoipExternalUrl": "https://10.20.30.40:4172",
  "blastEnabled": true,
  "blastExternalUrl": "https://ap1.example.com:8443",
  "tunnelEnabled": true,
  "tunnelExternalUrl": "https://ap1.example.com:443"
  "proxyPattern": "/"
}
```

Cet exemple indique l'adresse du Serveur de connexion View (`proxyDestinationUrl`), active les passerelles sécurisées, spécifie l'empreinte numérique du Serveur de connexion View et fournit les URL externes de PCoIP Secure Gateway, de Blast Secure Gateway et de la passerelle par tunnel sécurisé. Les propriétés indiquées dans cet exemple sont décrites plus en détail dans la section « Propriétés de l'API REST pour Access Point », page 29.

Remarque Lorsque vous créez une demande JSON, fournissez le jeu complet de propriétés de cette ressource. Un paramètre non spécifié dans l'appel JSON est réinitialisé sur la valeur par défaut. Vous pouvez également commencer par récupérer les paramètres, puis modifier la chaîne JSON sur les nouvelles valeurs.

Réinitialiser le mot de passe administrateur pour l'API REST Access Point

Si le mot de passe de l'utilisateur administrateur est inconnu, ou si des problèmes vous empêchent d'ouvrir une session sur l'API REST pour réinitialiser le mot de passe, vous pouvez utiliser cette procédure pour réinitialiser le mot de passe.

Prérequis

Vous devez posséder le mot de passe pour ouvrir une session sur la machine virtuelle en tant qu'utilisateur racine.

Procédure

1 Ouvrez une session sur le système d'exploitation du dispositif Access Point en tant qu'utilisateur racine.

2 Entrez les commandes suivantes :

```
echo 'adminPassword=P@ssw0rd' > /opt/vmware/gateway/conf/firstboot.properties
chown gateway /opt/vmware/gateway/conf/firstboot.properties
supervisorctl restart admin
```

Dans cet exemple, **`P@ssw0rd`** est un mot de passe qui contient au moins 8 caractères : une majuscule et une minuscule, un chiffre et un caractère spécial, notamment ! @ # $ % * ( ).

Lorsque le serveur administrateur redémarre, il génère le message suivant dans le fichier `/opt/vmware/gateway/logs/admin.log` : `Successfully set initial settings from firstboot.properties` (Définition réussie des paramètres initiaux à partir de firstboot.properties).

Suivant

Vous pouvez maintenant ouvrir une session sur l'interface d'administration REST à l'aide du nom d'utilisateur admin et du mot de passe que vous venez de définir (par exemple, P@ssw0rd).

Propriétés de l'API REST pour Access Point

Utilisez les propriétés API REST Access Point pour configurer quels certificats de sécurité, protocoles et suites de chiffrement sont utilisés, pour configurer l'authentification par carte à puce, pour spécifier quelle instance du Serveur de connexion View utiliser, etc.

Vous pouvez utiliser les propriétés dans les tableaux suivants pour apporter des modifications de configuration après le déploiement du dispositif Access Point, ou bien utiliser la propriété `--X:enableHiddenProperties=settingsJSON` d'OVF Tool avec certaines de ces propriétés pour configurer le dispositif au moment du déploiement. Pour plus d'informations sur l'utilisation d'Access Point avec OVF Tool, reportez-vous à la section « Propriétés du déploiement d'Access Point », page 23.

Réglages système

Ces paramètres sont inclus dans la ressource SystemSettings. L'URL est

```
https://access-point-appliance.example.com:9443/rest/v1/config/system
```

Dans cette URL, *access-point-appliance.example.com* est le nom de domaine complet du dispositif Access Point.

Tableau 3-1. Propriétés de l'API REST pour la ressource SystemSettings

Propriété de l'API REST	Description et exemple	Valeur par défaut
`adminPassword`	Spécifie le mot de passe administrateur pour accéder à l'API REST. 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 ! @ # $ % * ( ).	(Non défini sauf si défini par l'assistant de déploiement ou OVF Tool.)
`cipherList`	Configure la liste de chiffrements pour limiter l'utilisation de certains algorithmes cryptographiques avant l'établissement d'une connexion TLS/SSL cryptée. Ce paramètre est utilisé avec les paramètres pour activer divers protocoles de sécurité.	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA, TLS_RSA_WITH_AES_128_CBC_SHA, SSL_RSA_WITH_RC4_128_SHA (La même valeur par défaut que pour Serveur de connexion View 6.2.)
`ssl30Enabled`	Spécifie si le protocole de sécurité SSLv3.0 est activé.	FAUX
`tls10Enabled`	Spécifie si le protocole de sécurité TLSv1.0 est activé.	VRAI
`tls11Enabled`	Spécifie si le protocole de sécurité TLSv1.1 est activé.	VRAI
`tls12Enabled`	Spécifie si le protocole de sécurité TLSv1.2 est activé.	VRAI
`locale`	Spécifie le paramètre régional à utiliser pour les messages localisés. ■ **`us_EN`** pour l'anglais ■ **`ja_JP`** pour le japonais ■ **`fr_FR`** pour le français ■ **`de_DE`** pour l'allemand ■ **`zh_CN`** pour le chinois simplifié ■ **`zh_TW`** pour le chinois traditionnel ■ **`ko_KR`** pour le coréen	en_US
`syslogUrl`	Spécifie le serveur Syslog utilisé pour journaliser des événements Access Point. Cette valeur peut être une URL, un nom d'hôte ou une adresse IP. Le schéma et le numéro de port sont facultatifs (exemple : syslog://server.example.com: 514).	(Non défini sauf si défini par l'assistant de déploiement ou OVF Tool.)

Certificat du serveur

Ces paramètres sont inclus dans la ressource ServerCertificate. L'URL est

```
https://access-point-appliance.example.com:9443/rest/v1/config/certs/ssl
```

Dans cette URL, *access-point-appliance.example.com* est le nom de domaine complet du dispositif Access Point.

Tableau 3-2. Propriétés de l'API REST pour la ressource ServerCertificate

Propriété de l'API REST	Description et exemple	Valeur par défaut
`privateKeyPem`	Spécifie la clé privée pour le certificat au format PEM.	(Générée par le système)
`certChainPem`	Spécifie la chaîne de certificats au format PEM.	(Générée par le système)

Paramètres du service Edge pour View

Ces paramètres sont inclus dans la ressource EdgeServiceSettings. L'URL est

```
https://access-point-appliance.example.com:9443/rest//v1/config/edgeservice/view
```

Dans cette URL, *access-point-appliance.example.com* est le nom de domaine complet du dispositif Access Point.

Tableau 3-3. Propriétés de l'API REST pour la ressource EdgeServiceSettings pour View

Propriété de l'API REST	Description et exemple	Valeur par défaut
`proxyDestinationUrl`	Spécifie l'URL du serveur Horizon (équilibrage de charge ou Serveur de connexion View) vers lequel le dispositif Access Point dirige le trafic. Cette URL doit contenir le protocole, le nom d'hôte ou l'adresse IP et le numéro de port (exemple : https://load-balancer.example.com:443).	Aucune
`proxyDestinationUrlThumbprints`	Spécifie une liste d'empreintes numériques du Serveur de connexion Horizon. Si vous ne fournissez pas une liste d'empreintes numériques séparées par une virgule, les certificats de serveur doivent être émis par une autorité de certification approuvée. Le format inclut l'algorithme (sha1 ou md5) et les chiffres d'empreinte numérique hexadécimaux (exemple : sha1=b6 77 dc 9c 19 94 2e f1 78 f0 ad 4b ec 85 d1 7a f8 8b dc 34). Pour trouver ces propriétés, accédez au Serveur de connexion View, cliquez sur l'icône de verrouillage dans la barre d'adresses et affichez les détails du certificat.	Aucune
`tunnelEnabled`	Spécifie si le tunnel sécurisé View est activé.	FAUX **Remarque** Si vous utilisez VMware OVF Tool pour spécifier une valeur pour la propriété `proxyDestinationUrl`, `tunnelEnabled` est défini sur TRUE.

Tableau 3-3. Propriétés de l'API REST pour la ressource EdgeServiceSettings pour View (suite)

Propriété de l'API REST	Description et exemple	Valeur par défaut
`tunnelExternalUrl`	Spécifie une URL externe du dispositif Access Point, que les clients utiliseront pour les connexions par tunnel via View Secure Gateway. Ce tunnel est utilisé pour le trafic RDP, USB et de redirection multimédia (MMR).	https://*appliance*:443 (*appliance* est le nom de domaine complet du dispositif Access Point.)
`pcoipEnabled`	Spécifie si PCoIP Secure Gateway est activé.	FAUX **Remarque** Si vous utilisez VMware OVF Tool pour spécifier une valeur pour la propriété `proxyDestinationUrl`, `pcoipEnabled` est défini sur TRUE.
`pcoipExternalUrl`	Spécifie une URL externe du dispositif Access Point, que les clients utiliseront pour les connexions sécurisées via PCoIP Secure Gateway. Cette connexion est utilisée pour le trafic PCoIP.	https://*applianceIP*:4172 (*applianceIP* est l'adresse IPv4 du dispositif Access Point.)
`blastEnabled`	Spécifie si Blast Secure Gateway est activé.	FAUX **Remarque** Si vous utilisez VMware OVF Tool pour spécifier une valeur pour la propriété `proxyDestinationUrl`, `blastEnabled` est défini sur TRUE.
`blastExternalUrl`	Spécifie une URL externe du dispositif Access Point, qui permet aux utilisateurs finaux d'établir des connexions sécurisées à partir de leurs navigateurs Web via Blast Secure Gateway. Cette connexion est utilisée pour la fonctionnalité HTML Access.	https://*appliance*:8443 (*appliance* est le nom de domaine complet du dispositif Access Point.)
`proxyPattern`	Spécifie l'expression régulière qui correspond aux URI devant être transmis à l'URL du serveur Horizon (proxyDestinationUrl). Pour le Serveur de connexion View, une barre oblique (/) est une valeur classique pour la redirection vers le client Web HTML Access lorsque vous utilisez le dispositif Access Point.	Aucune
`authMethods`	Spécifie le type d'authentification à utiliser. Définissez cette propriété sur `certificate-auth` pour modifier la méthode d'authentification sur carte à puce.	Par défaut, l'authentification est transmise au Serveur de connexion View, qui peut être configuré pour le mot de passe AD, RSA SecurID, RADIUS ou SAML.

Configuration de certificats TLS/SSL pour les dispositifs Access Point

TLS/SSL est requis pour les connexions client à des dispositifs Access Point. Les dispositifs face au client Access Point 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 Access Point. 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 Access Point. 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 Access Point a besoin d'un certificat.

Lorsque vous soumettez une demande de signature de certificat à une autorité de certification, vous fournissez le nom de serveur qui sera associé au certificat. Vérifiez que le dispositif Access Point 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 Access Point 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 sera valide, car il correspondra au nom d'hôte spécifié par le client.

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 Access Point ont besoin de certificats TLS/SSL, vous pouvez utiliser un certificat de caractère générique pour ces serveurs. Toutefois, si vous utilisez un certificat de caractère générique partagé avec d'autres services, la sécurité du produit VMware Horizon dépend également de la sécurité de ces autres services.

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

Les certificats que vous importez dans le dispositif Access Point doivent être approuvés par des machines clientes et doivent également être applicables à toutes les instances d'Access Point 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 Access Point afin de configurer des paramètres de certificat, 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'Access Point, 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 Access Point.
- 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 Access Point.

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 Access Point.

Prérequis

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

Procédure

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

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

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

   Par exemple, si le nom du certificat est `sslservercerts.p12`, utilisez les commandes suivantes pour convertir le certificat :

```
openssl pkcs12 -in sslservercerts.p12 -nokeys -out sslservercerts.pem
openssl pkcs12 -in sslservercerts.p12 -nodes -nocerts -out sslservercertskey.pem
```

3 Utilisez la commande UNIX suivante pour convertir chaque fichier `.pem` en une valeur pouvant être transmise dans une chaîne JSON à l'API REST Access Point :

```
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 nouveau format place toutes les informations de certificat sur une seule ligne avec des caractères de saut de ligne intégrés.

Vous pouvez maintenant créer et utiliser une demande JSON pour configurer le certificat.

Suivant

Si vous avez converti un certificat de serveur TLS/SSL, reportez-vous à la section « Remplacer le certificat de serveur TLS/SSL par défaut pour Access Point », page 34. Pour les certificats de carte à puce, reportez-vous à la section Chapitre 5, « Configuration de l'authentification par carte à puce », page 41.

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

Pour stocker un certificat de serveur TLS/SSL signé par une autorité de certification approuvée sur le dispositif Access Point, vous devez convertir le certificat au bon format et utiliser l'API REST Access Point pour configurer le certificat.

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

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

Prérequis

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

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

- Convertissez le certificat en fichiers au format PEM et convertissez les fichiers `.pem` au format sur une seule ligne. Reportez-vous à la section « Convertir des fichiers de certificat au format PEM sur une ligne », page 33.

- Familiarisez-vous avec l'API REST Access Point. La spécification de cette API est disponible à l'adresse suivante sur la machine virtuelle sur laquelle Access Point est installé : `https://`*`access-point-appliance.example.com`*`:9443/rest/swagger.yaml`.

Procédure

1 Créez une demande JSON pour soumettre le certificat au dispositif Access Point.

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

Dans cet exemple, les valeurs *string* sont les valeurs PEM sur une seule ligne JSON que vous avez créées comme décrit dans les conditions préalables.

2 Utilisez un client REST, tel que `curl` ou `postman`, pour utiliser la demande JSON afin d'appeler l'API REST Access Point et stocker le certificat et la clé sur le dispositif Access Point.

L'exemple suivant utilise une commande `curl`. Dans l'exemple, *access-point-appliance.example.com* est le nom de domaine complet du dispositif Access Point et *cert*.json est la demande JSON que vous avez créée à l'étape précédente.

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

Suivant

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

Modifier les protocoles de sécurité et les suites de chiffrement utilisés pour la communication TLS/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 crypter les communications entre les clients et le dispositif Access Point.

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 v1.0, TLS v1.1 et TLS v1.2 sont activés. (SSL v3.0 et SSL v2.0 sont désactivés.)

Prérequis

- Familiarisez-vous avec l'API REST Access Point. La spécification de cette API est disponible à l'adresse suivante sur la machine virtuelle sur laquelle Access Point est installé : `https://access-point-appliance.example.com:9443/rest/swagger.yaml`.
- Familiarisez-vous avec les propriétés spécifiques relatives à la configuration des suites de chiffrement et des protocoles : `cipherSuites`, `ssl30Enabled`, `tls10Enabled`, `tls11Enabled` et `tls12Enabled`. Reportez-vous à la section « Propriétés de l'API REST pour Access Point », page 29.

Procédure

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

L'exemple suivant a les paramètres par défaut.

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

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

   L'exemple suivant utilise une commande `curl`. Dans l'exemple, *access-point-appliance.example.com* est le nom de domaine complet du dispositif Access Point et *ciphers*.json est la demande JSON que vous avez créée à l'étape précédente.

```
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
```

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

Configuration des passerelles sécurisées

Par défaut, le tunnel sécurisé, PCoIP Secure Gateway et Blast Secure Gateway sont tous activés sur le dispositif Access Point. Les URL externes doivent être définies sur des valeurs pouvant être utilisées par des clients Horizon distants pour se connecter au dispositif Access Point pour la connexion par tunnel, la connexion PCoIP et la connexion Blast, respectivement.

Tableau 3-4. Exemples de paramètres de passerelle sécurisée

Type de passerelle sécurisée	Nom de propriété	Exemple de paramètre
Tunnel sécurisé	`tunnelExternalUrl`	`https://ap1.example.com:443`
PCoIP Secure Gateway	`pcoipExternalUrl`	`https://10.20.30.40:4172`
Blast Secure Gateway	`blastExternalUrl`	`https://ap1.example.com:8443`

Ces propriétés sont décrites plus en détail dans la section « Paramètres du service Edge pour View », page 30.

L'URL externe PCoIP doit utiliser une adresse IPv4. Les autres URL peuvent utiliser une adresse IP ou un nom d'hôte pouvant être résolu par le client sur le réseau externe, qui est généralement Internet. Ces adresses externes sont utilisées uniquement par les clients. La connexion depuis le client pour les trois URL doit se diriger vers le dispositif Access Point spécifique et elle ne doit pas être à équilibrage de charge. Dans un environnement NAT, les adresses doivent être les adresses externes et non les adresses NAT internes.

L'exemple suivant indique une demande JSON de configuration qui comporte ces propriétés.:

```
{
  "identifier": "VIEW",
  "enabled": true,
  "proxyDestinationUrl": "https://192.0.2.1",
  "proxyDestinationUrlThumbprints": "sha1=b6 77 dc 9c 19 94 2e f1 78 f0 ad 4b ec 85 d1 7a f8 8b
dc 34",
  "pcoipEnabled": true,
  "pcoipExternalUrl": "https://10.20.30.40:4172",
  "blastEnabled": true,
  "blastExternalUrl": "https://ap1.example.com:8443",
  "tunnelEnabled": true,
  "tunnelExternalUrl": "https://ap1.example.com:443",
  "proxyPattern": "/"
}
```

Ces paramètres sont inclus dans la ressource EdgeServiceSettings. L'URL est

```
https://access-point-appliance.example.com:9443/rest//v1/config/edgeservice/view
```

Dans cette URL, *access-point-appliance.example.com* est le nom de domaine complet du dispositif Access Point.

VMware vous recommande de configurer ces paramètres au moment du déploiement, à l'aide de VMware OVF Tool. Pour voir un exemple, reportez-vous à la section « Utilisation de VMware OVF Tool pour déployer le dispositif Access Point », page 21.

Collecte de journaux depuis le dispositif Access Point

4

Vous pouvez entrer une URL dans un navigateur afin d'obtenir un fichier ZIP qui contient des journaux depuis votre dispositif Access Point.

Utilisez l'URL suivante pour collecter des journaux depuis votre dispositif Access Point.

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

Dans cet exemple, *access-point-appliance.example.com* est le nom de domaine complet du dispositif Access Point.

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 4-1. Fichiers qui contiennent des informations système pour faciliter le dépannage

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

Tableau 4-2. Fichiers journaux d' Access Point

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

Tableau 4-2. Fichiers journaux d' Access Point (suite)

Nom de fichier	Description
`bsg.log`	Contient des messages de journal de Blast Security Gateway.
`SecurityGateway_*.log`	Contient des messages de journal de PCoIP Security Gateway.

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

Configuration de l'authentification par carte à puce

5

Par défaut, Access Point utilise l'authentification directe pour que les utilisateurs puissent entrer leurs informations d'identification Active Directory, et ces informations d'identification sont envoyées via un système principal pour authentification. Toutefois, vous pouvez configurer le dispositif Access Point pour effectuer l'authentification par carte à puce.

Avec l'authentification par carte à puce, un utilisateur ou un administrateur insère une carte à puce dans un lecteur de carte à puce connecté à l'ordinateur client et entre un code PIN. L'authentification par carte à puce fournit une authentification à deux facteurs en vérifiant à la fois ce que la personne a (la carte à puce) et ce qu'elle sait (le code PIN). Les utilisateurs finaux peuvent utiliser des cartes à puce pour ouvrir une session sur un système d'exploitation de poste de travail View distant et pour les applications compatibles pour une carte 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.

Remarque L'authentification par carte à puce est une fonctionnalité de la version d'évaluation technique de la version Access Point 2.0, ce qui signifie qu'elle est disponible à l'essai, mais elle n'est pas recommandée pour une utilisation en production et aucun support n'est fourni.

Avec cette fonctionnalité, l'authentification de certificat par carte à puce est effectuée avec Access Point et Access Point communique des informations sur le certificat X.509 de l'utilisateur final et le code PIN de carte à puce au Serveur de connexion View à l'aide d'une assertion SAML.

Ce chapitre aborde les rubriques suivantes :

Copier des métadonnées SAML Access Point sur le Serveur de connexion View

Vous devez générer des métadonnées SAML sur le dispositif Access Point et échanger des métadonnées avec le Serveur de connexion View 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 cette procédure, vous générez des métadonnées SAML Access Point à l'aide de l'API REST Access Point. Vous copiez ces métadonnées et utilisez l'utilitaire ADSI Edit sur l'hôte du Serveur de connexion View pour modifier View LDAP et le coller dans les métadonnées. De cette façon, vous créez manuellement un authentificateur SAML Access Point sur l'instance du Serveur de connexion View.

Prérequis

- Configurez l'horloge (UTC) sur le dispositif Access Point pour qu'il soit à l'heure exacte. Par exemple, vérifiez que l'heure de l'hôte ESXi est synchronisée avec un serveur NTP, et vérifiez que VMware Tools, qui est exécuté dans la machine virtuelle de dispositif, synchronise l'heure sur la machine virtuelle avec l'heure sur l'hôte ESXi.

  Important Si l'heure sur le dispositif Access Point ne correspond pas à l'heure sur l'hôte du Serveur de connexion View, il est possible que l'authentification par carte à puce ne fonctionne pas.

- Pour plus d'informations sur l'utilisation de l'utilitaire ADSI Edit sur votre version du système d'exploitation Windows, consultez le site Web Microsoft TechNet.
- Obtenez un certificat de signature SAML que vous pouvez utiliser pour signer les métadonnées Access Point.

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

- Si vous ne l'avez pas déjà fait, convertissez le certificat de signature SAML en fichiers au format PEM et convertissez les fichiers `.pem` au format sur une seule ligne. Reportez-vous à la section « Convertir des fichiers de certificat au format PEM sur une ligne », page 33.

Procédure

1. Créez une demande JSON pour générer les métadonnées SAML pour le dispositif Access Point.
   - Si vous ne disposez pas d'un certificat de signature SAML pour le dispositif Access Point, le corps de la demande JSON est représenté par des accolades vides :

     ```
     {}
     ```

   - Si vous disposez d'un certificat de signature SAML, utilisez la syntaxe suivante :

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

     Dans cet exemple, les valeurs *string* sont les valeurs PEM sur une seule ligne JSON que vous avez créées comme décrit dans les conditions préalables.

2. Utilisez un client REST, tel que `curl` ou `postman`, pour utiliser la demande JSON afin d'appeler l'API REST Access Point et générer les métadonnées Access Point.

   L'exemple suivant utilise une commande `curl`. Dans l'exemple, *access-point-appliance.example.com* est le nom de domaine complet du dispositif Access Point et *ap-metadata*.json est la demande JSON que vous avez créée à l'étape précédente.

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

3 Utilisez un client REST pour obtenir les métadonnées générées, puis copiez les métadonnées.

```
curl –k –u 'admin' https://access-point-appliance.example.com:9443/rest/v1/config/idp-metadata
```

Après avoir copié les métadonnées SAML Access Point, vous pouvez les coller dans View LDAP pour créer un authentificateur SAML sur le Serveur de connexion View.

4 Démarrez l'utilitaire ADSI Edit sur votre hôte du Serveur de connexion View et connectez-vous à View LDAP.

   a Dans l'arborescence de la console, sélectionnez **Se connecter à**.

   b Dans la zone de texte **Sélectionnez ou entrez un nom unique ou un contexte d'attribution de noms**, tapez le nom unique **`DC=vdi, DC=vmware, DC=int`**.

   c Dans le volet Ordinateur, sélectionnez ou tapez **`localhost:389`** ou le nom de domaine complet du Serveur de connexion View, suivi du port 389.

   Par exemple : **`localhost:389`** ou **`mycomputer.example.com:389`**

5 Développez l'arborescence d'ADSI Edit, développez **OU=Properties**, cliquez avec le bouton droit sur **OU=Authenticator** et sélectionnez **Nouveau > Objet**.

6 Dans l'assistant Créer un objet, sélectionnez **pae-SAMLAuthenticator** et cliquez sur **Suivant**.

7 Dans la zone de texte **Valeur**, entrez un nom, comme **`ap`** pour Access Point, cliquez sur **Suivant**, puis sur **Terminer**.

L'objet apparaît dans le volet de droite. Pour cet exemple, le nom de l'objet est **CN=ap**.

8 Double-cliquez sur l'objet **CN=*name*** et modifiez les attributs suivants.

Attribut	Description
pae-SAMLLabel	Donnez un nom à l'authentificateur SAML. Cette étiquette apparaîtra dans le Serveur de connexion View, dans les paramètres d'authentification du Serveur de connexion View.
pae-SAMLMetaDataXml	Collez les métadonnées SAML que vous avez générées sur le dispositif Access Point. Assurez-vous que les métadonnées ne contiennent pas de caractères d'échappement avant les guillemets doubles. Par exemple, le format correct est **`<?xml version="1.0"`**, pas **`<?xml version=\"1.0\"`**.
pae-SAMLMetaDataUrl	(Facultatif) Si vous spécifiez une URL dans cet attribut (par exemple, **`https://access-point.example.com`**), l'URL sera affichée dans la boîte de dialogue Gérer des authentificateurs dans View Administrator.

Dans le Serveur de connexion View, le nouveau paramètre s'applique immédiatement. Vous n'avez pas à redémarrer le service Serveur de connexion View ou l'ordinateur client.

Modifier la période d’expiration des métadonnées du fournisseur de service

Si vous ne modifiez pas la période d'expiration, le Serveur de connexion View cessera d'accepter les assertions SAML de l'authentificateur SAML, tel qu'Access Point ou un fournisseur d'identité tiers, après 24 heures, et l'échange de métadonnées doit être répété.

Suivez cette procédure pour indiquer le délai en jours après lequel le Serveur de connexion View arrête d'accepter les assertions SAML du fournisseur d'identité. Cette valeur est utilisée à la fin de la période d'expiration actuelle. Par exemple, si la période d'expiration actuelle est d'un jour et que vous indiquez 90 jours, lorsque le délai d'un jour est écoulé, le Serveur de connexion View génère des métadonnées avec une période d'expiration de 90 jours.

Prérequis

Pour plus d'informations sur l'utilisation de l'utilitaire ADSI Edit sur votre version du système d'exploitation Windows, consultez le site Web Microsoft TechNet.

Procédure

1 Démarrez l'utilitaire ADSI Edit sur votre hôte du Serveur de connexion View.

2 Dans l'arborescence de la console, sélectionnez **Se connecter à**.

3 Dans la zone de texte **Sélectionnez ou entrez un nom unique ou un contexte d'attribution de noms**, tapez le nom unique **`DC=vdi, DC=vmware, DC=int`**.

4 Dans le volet Ordinateur, sélectionnez ou tapez **`localhost:389`** ou le nom de domaine complet du Serveur de connexion View, suivi du port 389.

   Par exemple : **`localhost:389`** ou **`mycomputer.example.com:389`**

5 Développez l'arborescence d'ADSI Edit, développez **OU=Properties**, sélectionnez **OU=Global** et double-cliquez sur **OU=Common** dans le volet de droite.

6 Dans la boîte de dialogue Propriétés, modifiez l'attribut **pae-NameValuePair** pour ajouter les valeurs suivantes

   ```
   cs-samlencryptionkeyvaliditydays=number-of-days
   cs-samlsigningkeyvaliditydays=number-of-days
   ```

   Dans cet exemple, *number-of-days* est le nombre de jours pouvant s'écouler avant qu'un Serveur de connexion View distant cesse d'accepter des assertions SAML. Après cette période de temps, le processus d'échange des métadonnées SAML doit être répété.

Copier des métadonnées SAML du Serveur de connexion View sur Access Point

Après avoir activé l'authentificateur SAML Access Point dans View Administrator, vous pouvez générer des métadonnées du Serveur de connexion View et utiliser ces métadonnées pour créer un fournisseur de service sur le dispositif Access Point.

Prérequis

- Vérifiez que vous pouvez ouvrir une session sur View Administrator en tant qu'administrateur.
- Vérifiez que vous avez créé un authentificateur SAML Access Point en copiant les métadonnées SAML Access Point dans View LDAP. Reportez-vous à la section « Copier des métadonnées SAML Access Point sur le Serveur de connexion View », page 41.
- Vérifiez que la période d'expiration des métadonnées est définie pour le nombre correct de jours. La valeur par défaut est un jour. Reportez-vous à la section « Modifier la période d'expiration des métadonnées du fournisseur de service », page 43.

Procédure

1 Ouvrez une session sur View Administrator, accédez à **Configuration de View > Serveurs** et cliquez sur l'onglet **Serveurs de connexion**.

2 Sélectionnez l'instance de View Connection Server et cliquez sur **Edit (Modifier)**.

3 Cliquez sur l'onglet **Authentification** puis, dans la liste déroulante **Délégation de l'authentification à VMware Horizon (authentificateur SAML 2.0)**, sélectionnez **Autorisé** ou **Requis**, le cas échéant.

4 Dans la liste **Authentificateur SAML**, sélectionnez le nom de l'authentificateur Access Point que vous avez créé et cliquez sur **OK**.

5 Dans la section Intégrité du système du tableau de bord de View Administrator, sélectionnez **Autres composants > Authentificateurs SAML 2.0**, sélectionnez l'authentificateur SAML que vous avez ajouté, puis vérifiez les détails.

   Si la configuration est réussie, la santé de l'authentificateur peut être verte ou rouge. La santé de l'authentificateur peut également s'afficher en rouge si le certificat n'est pas approuvé, si Access Point n'est pas disponible ou si l'URL des métadonnées n'est pas valide. Si l'indicateur de santé est rouge, il n'est pas nécessaire de cliquer sur **Vérifier** pour valider et accepter le certificat. Il est nécessaire de cliquer sur **Vérifier** uniquement pour les authentificateurs SAML dynamiques. L'authentificateur SAML Access Point est un authentificateur SAML statique.

6 Ouvrez un nouvel onglet dans le navigateur et entrez l'URL pour obtenir les métadonnées SAML du Serveur de connexion View.

   https://*connection-server.example.com*/SAML/metadata/sp.xml

   Dans cet exemple, *connection-server.example.com* est le nom de domaine complet de l'hôte du Serveur de connexion View.

   Cette page affiche les métadonnées SAML du Serveur de connexion View.

7 Utilisez une commande **Enregistrer sous** pour enregistrer la page Web en tant que fichier XML.

   Par exemple, vous pouvez enregistrer la page sous forme d'un fichier avec le nom `connection-server-metadata.xml`. Le contenu de ce fichier commence par le texte suivant :

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

8 Utilisez un client REST, tel que `curl` ou `postman`, pour appeler l'API REST Access Point et stocker les métadonnées sur le dispositif Access Point.

   L'exemple suivant utilise une commande `curl`. Dans l'exemple, *access-point-appliance.example.com* est le nom de domaine complet du dispositif Access Point, *service-provider-name* est le nom à utiliser comme fournisseur de service du Serveur de connexion View et *connection-server-metadata.xml* est le fichier de métadonnées que vous avez créé à l'étape précédente.

   ```
   curl -k -d @- -u 'admin' -H "Content-Type: text/xml" -X POST https://access-point-appliance.example.com:9443/rest/v1/config/sp-metadata/service-provider-name < connection-server-metadata.xml
   ```

Access Point et le Serveur de connexion View peuvent maintenant échanger des informations d'authentification et d'autorisation.

Suivant

Pour vérifier que la commande POST a fonctionné, vous pouvez utiliser une commande GET avec la même URL.

Pour vérifier que l'authentificateur SAML Access Point a bien été configuré après sa sélection dans View Administrator, ouvrez l'utilitaire ADSI Edit sur l'hôte du Serveur de connexion View, connectez-vous à View LDAP (**DC=vdi, DC=vmware, DC=int**) et, dans l'arborescence d'ADSI Edit, sous **OU=Properties**, sélectionnez **OU=Server** et double-cliquez sur l'élément **CN=*name*** dans le volet de droite. L'attribut **pae-SAMLConfigDN** sera rempli avec le nom unique.

Obtenir des certificats d'autorités de certification

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

Si vous ne disposez pas du certificat racine ou intermédiaire de l'autorité de certification qui a signé les certificats sur les cartes à puce présentées par vos utilisateurs et administrateurs, vous pouvez exporter les certificats à partir des certificats d'utilisateurs signés par une autorité de certification ou d'une carte à puce qui en contient un. Reportez-vous à la section « Obtenir le certificat d'une autorité de certification de Windows », page 46.

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.

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 sera utilisé dans Étape 4.

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.

Configurer des paramètres de carte à puce sur le dispositif Access Point

Sur le dispositif Access Point, vous devez activer l'authentification par carte à puce, copier le certificat et modifier le type d'authentification sur authentification par carte à puce.

Remarque L'authentification par carte à puce est une fonctionnalité de la version d'évaluation technique de la version Access Point 2.0.

Prérequis

- Obtenez le certificat de l'émetteur d'autorité de certification approuvée qui a été utilisé pour signer les certificats X.509 pour les cartes à puce. Reportez-vous à

  « Obtenir des certificats d'autorités de certification », page 46. pour le certificat qui sera placé sur la carte à puce
- Convertissez le certificat en fichier PEM qui contient la chaîne de certificats. Reportez-vous à la section « Convertir des fichiers de certificat au format PEM sur une ligne », page 33.
- Vérifiez que vous avez copié les métadonnées SAML d'Access Point sur le Serveur de connexion View et copié les métadonnées SAML du Serveur de connexion View sur le dispositif Access Point. Reportez-vous aux sections « Copier des métadonnées SAML Access Point sur le Serveur de connexion View », page 41 et « Copier des métadonnées SAML du Serveur de connexion View sur Access Point », page 44.
- Familiarisez-vous avec les propriétés du certificat de carte à puce et déterminez quels paramètres utiliser. Reportez-vous à la section « Propriétés du certificat de carte à puce pour les options avancées », page 49.
- Si vous utilisez un équilibrage de charge entre Access Point et des instances du Serveur de connexion View, vérifiez que l'arrêt TLS/SSL n'est pas effectué sur l'équilibrage de charge. L'équilibrage de charge doit être configuré pour transmettre l'authentification au Serveur de connexion View.

Procédure

1 Utilisez un client REST, tel que `curl` ou `postman`, pour appeler l'API REST Access Point et obtenir les paramètres de certificat par défaut.

  L'exemple suivant utilise une commande `curl`. Dans l'exemple, *access-point-appliance.example.com* est le nom de domaine complet du dispositif Access Point.

  ```
  curl -k -u 'admin' https://access-point-appliance.example.com:
  9443/rest/v1/config/authmethod/certificate-auth
  ```

2 Transmettez ces informations dans une demande JSON pour activer l'authentification par carte à puce et coller le certificat.

  Les deux propriétés suivantes sont les propriétés devant être configurées. Vous pouvez également modifier les valeurs par défaut des autres propriétés.

  ```
  {
  "enabled": "true",
  "caCertificates": "-----BEGIN CERTIFICATE------ ... -----END CERTIFICATE------"
  }
  ```

  Dans cet exemple, les points de suspension (...) indiquent le contenu central du texte du certificat. Le texte du certificat doit tenir sur une seule ligne pouvant être transmise dans une chaîne JSON à l'API REST Access Point, comme décrit dans les conditions préalables.

Pour `caCertificates`, vous pouvez spécifier plusieurs certificats en utilisant des espaces comme séparateurs. Lorsqu'un utilisateur initie une connexion avec le dispositif Access Point, Access Point envoie une liste d'autorités de certification approuvées au système client. Le système client compare cette liste aux certificats utilisateur disponibles, sélectionne un certificat approprié et invite l'utilisateur à entrer un code PIN de carte à puce. Si plusieurs certificats utilisateur sont valides, le système client invite l'utilisateur à sélectionner un certificat.

3 Utilisez un client REST, tel que `curl` ou `postman`, pour utiliser la demande JSON afin d'appeler l'API REST Access Point, stocker le certificat sur le dispositif Access Point et activer l'authentification par carte à puce.

   L'exemple suivant utilise une commande `curl`. Dans l'exemple, *access-point-appliance.example.com* est le nom de domaine complet du dispositif Access Point et *smartcard*.json est la demande JSON que vous avez créée à l'étape précédente.

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

4 Utilisez un client REST pour obtenir les paramètres du service Edge par défaut pour le Serveur de connexion View.

   ```
   curl -k -u 'admin' https://access-point-appliance.example.com:
   9443/rest/v1/config/edgeservice/VIEW
   ```

5 Collez ces informations dans une demande JSON pour activer l'authentification par carte à puce pour le serveur View Server et ajoutez les propriétés `authMethods` et `samlSP`.

   ```
   {
     "identifier": "VIEW",
     "enabled": true,
     "proxyDestinationUrl": "https://connection-server.example.com",
     "proxyDestinationUrlThumbprints": "sha1=40 e6 98 9e a9 d1 bc 6f 86 8c c0 ad b1 ea ff f7 4a
   3b 12 8c",
     "pcoipEnabled": true,
     "blastEnabled": true,
     "tunnelEnabled": true,
     "proxyPattern": "/",
     "authMethods": "certificate-auth",
     "samlSP": "connection-server-sp"
   }
   ```

   Dans cet exemple, *connection-server.example.com* est le nom de domaine complet de l'hôte du Serveur de connexion View. Vous avez spécifié ce nom lorsque vous avez déployé le dispositif Access Point. Également dans cet exemple, *connection-server-sp* est le nom du fournisseur de service que vous avez spécifié lorsque vous avez copié les métadonnées du Serveur de connexion View sur le dispositif Access Point. Le texte `proxyDestinationUrlThumbprints` n'est qu'un exemple. Remplacez ce texte par l'empreinte numérique de votre serveur de destination.

6 Utilisez un client REST pour envoyer la demande JSON à l'API Access Point et configurez le service Edge pour qu'il utilise l'authentification par carte à puce.

   Dans l'exemple suivant, *smartauth*.json est la demande JSON que vous avez créée à l'étape précédente.

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

Les utilisateurs finaux peuvent désormais utiliser des cartes à puce lorsqu'ils ouvrent une session sur Access Point.

Propriétés du certificat de carte à puce pour les options avancées

Les propriétés de l'authentification par carte à puce fournissent des fonctionnalités pour la révocation de certificat, les formulaires de consentement et la configuration de l'autre nom de l'objet.

Vous pouvez empêcher les utilisateurs avec des certificats utilisateur révoqués de s'authentifier avec des cartes à puce en configurant la vérification de la révocation des certificats. Les certificats sont souvent révoqués lorsqu'un utilisateur quitte une entreprise, perd une carte à puce ou passe d'un service à un autre.

Access Point prend en charge la vérification de la révocation des certificats avec des listes de révocation de certificats (CRL) et avec le protocole OCSP (Online Certificate Status Protocol). 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 de certificat utilisé pour obtenir l'état de révocation d'un certificat X.509.

Lorsque vous configurez les deux types de vérification de la révocation des certificats, Access Point tente d'utiliser d'abord OCSP et peut être configuré pour revenir à la CRL si OCSP échoue. Access Point ne revient pas à OCSP si la CRL échoue. L'autorité de certification doit être accessible à partir de l'hôte Access Point.

Lorsque vous utilisez l'API REST pour obtenir les données de configuration pour l'authentification par carte à puce, vous voyez une liste des éléments que vous pouvez configurer. Par exemple, vous pouvez utiliser une demande GET avec l'URL suivante :

```
https://access-point-appliance.example.com:9443/rest/v1/config/authmethod/certificate-auth
```

Si vous n'avez modifié aucun paramètre de configuration, les paramètres par défaut suivants sont renvoyés.


```
"enableOCSP": null,
"ocspSigningCert": null,
"caCertificates": null,
"displayName": "CertificateAuthAdapter",
"versionNum": null,
"enableAlternateUPN": "",
"className": "com.vmware.horizon.adapters.certificateAdapter.CertificateAuthAdapter",
"sendOCSPNonce": null,
"enabled": "false",
"enableCertCRL": "true",
"enableOCSPCRLFailover": "true",
"enableConsentForm": null,
"ocspURL": null,
"jarFile": "/opt/vmware/gateway/data/authbroker/certificate-auth-adapter-0.1.jar",
"enableCertRevocation": "",
"name": "certificate-auth",
"certificatePolicies": null,
"consentForm": null,
"authMethod": "urn:oasis:names:tc:SAML:2.0:ac:classes:TLSClient",
"crlLocation": null,
"enableEmail": "",
"crlCacheSize": "100"
```

Tableau 5-1. Propriétés du certificat de carte à puce que vous pouvez configurer

Nom de propriété	Description	Valeurs valides
enableOCSP	Spécifie si vous voulez utiliser le protocole OCSP (Online Certificate Status Protocol) pour la vérification de la révocation des certificats. Lorsque ce paramètre est activé, Access Point envoie une demande à un répondeur OCSP afin de déterminer l'état de révocation d'un certificat utilisateur spécifique. La valeur par défaut est true.	true ou false
ocspSigningCert	Spécifie le chemin d'accès au certificat du répondeur OCSP, s'il est connu.	Chemin d'accès au fichier sur l'hôte du répondeur OCSP (par exemple, `/path/to/file.cer`).
caCertificates	(Obligatoire) Spécifie un ou plusieurs certificats d'autorité de certification approuvée au format PEM.	Le texte de chaque certificat a le format `"-----BEGIN CERTIFICATE------ ... -----END CERTIFICATE------"` où les points de suspension (...) indiquent le contenu central du texte du certificat. Séparez les certificats par des espaces.
enableAlternateUPN	Spécifie si vous voulez utiliser d'autres champs dans l'autre nom de l'objet. Les connexions par carte à puce utilisent le nom principal de l'utilisateur (UPN) d'Active Directory pour valider les comptes d'utilisateur. Si le domaine sur lequel réside un utilisateur de carte à puce est différent du domaine à partir duquel est émis votre certificat racine, vous devez définir l'UPN de l'utilisateur sur l'autre nom de l'objet (SAN) contenu dans le certificat racine de l'autorité de certification approuvée.	true ou false
sendOCSPNonce	Spécifie si vous voulez inclure une valeur à usage unique dans la demande OCSP et si vous voulez qu'elle soit incluse dans la réponse. Une valeur à usage unique est un nombre arbitraire utilisé une seule fois dans une communication cryptographique.	true ou false
activé	(Obligatoire) Spécifie si vous voulez utiliser l'authentification de certificat par carte à puce. Vous pouvez passer ce paramètre sur true. La valeur par défaut est false.	true ou false
enableCertCRL	Spécifie si vous voulez utiliser l'extension de points de distribution des listes de révocation de certificats du certificat.	true ou false
enableOCSPCRLFailover	Spécifie si vous voulez utiliser une liste de révocation de certificats si OCSP échoue. La valeur par défaut est true.	true ou false
enableConsentForm	Spécifie si vous voulez présenter aux utilisateurs une fenêtre de formulaire de consentement avant qu'ils ouvrent une session à l'aide de l'authentification de certificat.	true ou false
ocspURL	Spécifie l'URL du répondeur OCSP à utiliser pour la vérification de la révocation (par exemple, http://ocspurl.com).	Une URL qui commence par http ou https.
enableCertRevocation	Spécifie si vous voulez utiliser la vérification de la révocation des certificats.	true ou false

Tableau 5-1. Propriétés du certificat de carte à puce que vous pouvez configurer (suite)

Nom de propriété	Description	Valeurs valides
certificatePolicies	Spécifie la liste d'identificateur d'objet (OID) acceptée dans l'extension des stratégies de certificats.	Un OID.
consentForm	Spécifie le contenu du formulaire de consentement à afficher aux utilisateurs.	Du texte.
crlLocation	Spécifie l'emplacement de la liste de révocation de certificats à utiliser pour la vérification de la révocation.	URL ou chemin d'accès au fichier (par exemple, `http://crlurl.crl` ou `file:///crlFile.crl`). **Remarque** N'utilisez pas d'URL `ldap:`.
enableEmail	Spécifie si vous voulez utiliser le champ RFC822 dans l'autre nom de l'objet si aucun UPN (nom principal de l'utilisateur) n'est trouvé dans le certificat.	true ou false

Index