Déploiement et configuration d'Access Point

Unified Access Gateway 2.8

vmware®

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

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

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 de VMware Access Point

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

Public visé

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

Préparation au déploiement d' Access Point

1

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

Ce chapitre aborde les rubriques suivantes :

Access Point en tant que passerelle sécurisée

Access Point est un dispositif de sécurité de couche 7 qui est normalement installé dans une zone démilitarisée (DMZ). Access Point est utilisé pour s'assurer que le trafic entrant dans le centre de données d'entreprise est effectué uniquement pour le compte d'un utilisateur distant à authentification élevée.

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

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

En général, les dispositifs Access Point résident dans une zone démilitarisée (DMZ) de réseau et agissent comme un hôte proxy pour les connexions à l'intérieur du réseau approuvé de votre entreprise. Cette conception offre une couche de sécurité supplémentaire en protégeant les postes de travail virtuels, les hôtes d'application et les serveurs vis-à-vis des sites Internet publics.

Access Point est un dispositif de sécurité renforcée conçu spécifiquement pour la zone DMZ. Les paramètres de renforcement suivants sont implémentés.

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

Utilisation d'Access Point à la place d'un réseau privé virtuel

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

Avantages d'Access Point par rapport aux solutions VPN génériques :

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

Configuration requise pour le système et le réseau Access Point

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

Versions de produit VMware prises en charge

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

Access Point 2.8 peut être utilisé en tant que passerelle sécurisée avec les offres VMware suivantes.

- Vmware AirWatch 8.4 et versions ultérieures
- VMware Identity Manager 2.7 et versions ultérieures
- VMware Horizon 6.2 et versions ultérieures
- VMware Horizon Air Hybrid Mode 1.0 et versions ultérieures
- VMware Horizon Air 15.3 et versions ultérieures

Exigences matérielles d'ESXi Server

Le dispositif Access Point doit être déployé sur une version de vSphere identique à celle prise en charge pour les produits et versions d'Horizon que vous utilisez.

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

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

Exigences du dispositif virtuel

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.

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

- Taille de téléchargement du dispositif virtuel : 2,5 Go
- Espace disque minimal requis à provisionnement fin : 2,5 Go
- Espace disque minimal requis à provisionnement statique : 20 Go

Les informations suivantes sont requises pour déployer le dispositif virtuel :

- Adresse IP statique
- Adresse IP du serveur DNS
- Mot de passe de l'utilisateur racine
- URL de l'instance de serveur de l'équilibrage de charge vers laquelle le dispositif Access Point pointe.

Configuration requise pour le réseau

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

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

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

Exigences de conservation des journaux

Les fichiers journaux sont configurés par défaut pour utiliser une certaine quantité d'espace qui est inférieure à la taille totale de disque dans l'agrégation. Les journaux pour Access Point sont alternés par défaut. Vous devez utiliser Syslog pour conserver ces entrées de journal. Reportez-vous à la section Collecte de journaux depuis le dispositif Access Point.

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.

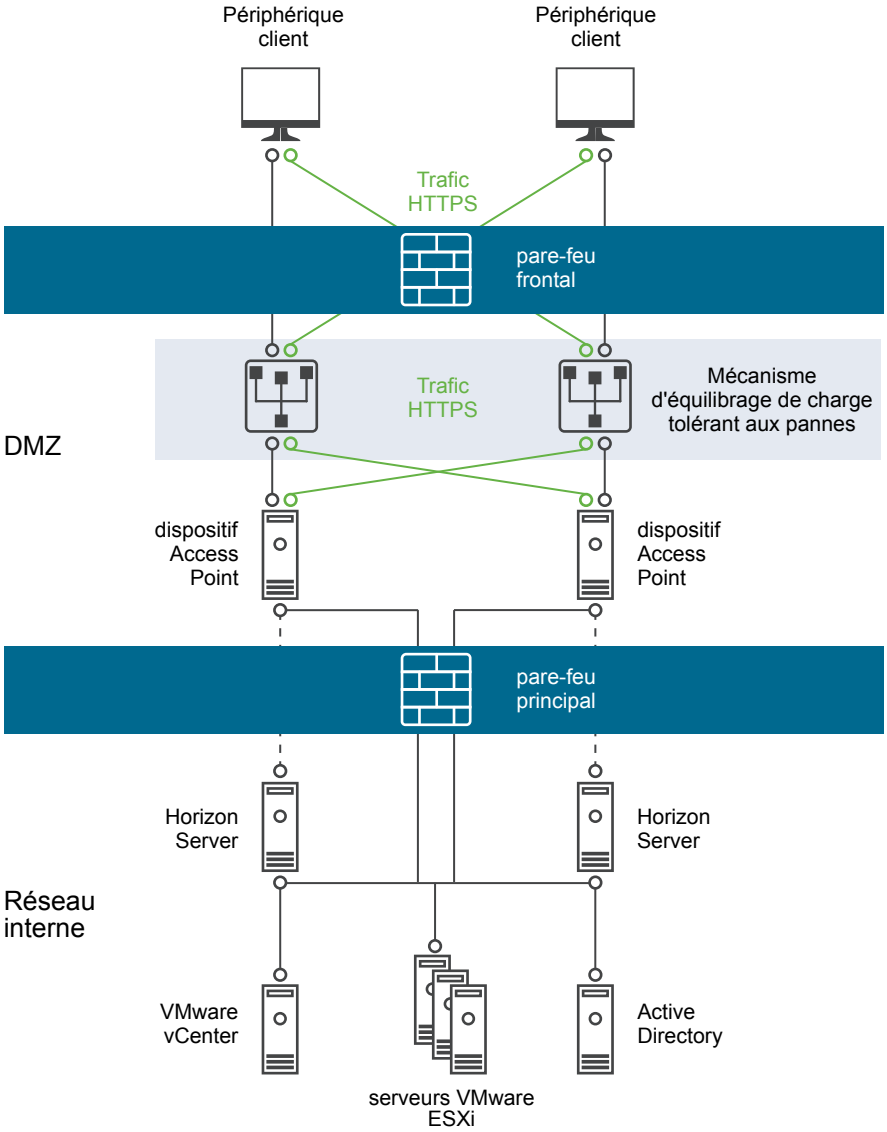
- Un pare-feu frontal externe en réseau est nécessaire pour protéger la zone DMZ et le réseau interne. Vous configurez ce pare-feu pour permettre au trafic réseau externe d'atteindre la zone DMZ.
- Un pare-feu principal, entre la zone DMZ et le réseau interne, est requis pour fournir un deuxième niveau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

La 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.

Pour autoriser des périphériques clients externes à se connecter à un dispositif Access Point dans la zone DMZ, le pare-feu frontal doit autoriser le trafic sur certains ports. Par défaut, les périphériques clients externes et les clients Web externes (HTML Access) se connectent à un dispositif Access Point dans la zone DMZ sur le port TCP 443. Si vous utilisez le protocole Blast, le port 443 doit être ouvert sur le pare-feu. Si vous utilisez le protocole PCOIP, le port 4172 doit être ouvert sur le pare-feu.

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

Figure 1-1. Topologie de double pare-feu



Topologies d'équilibrage de charge Access Point

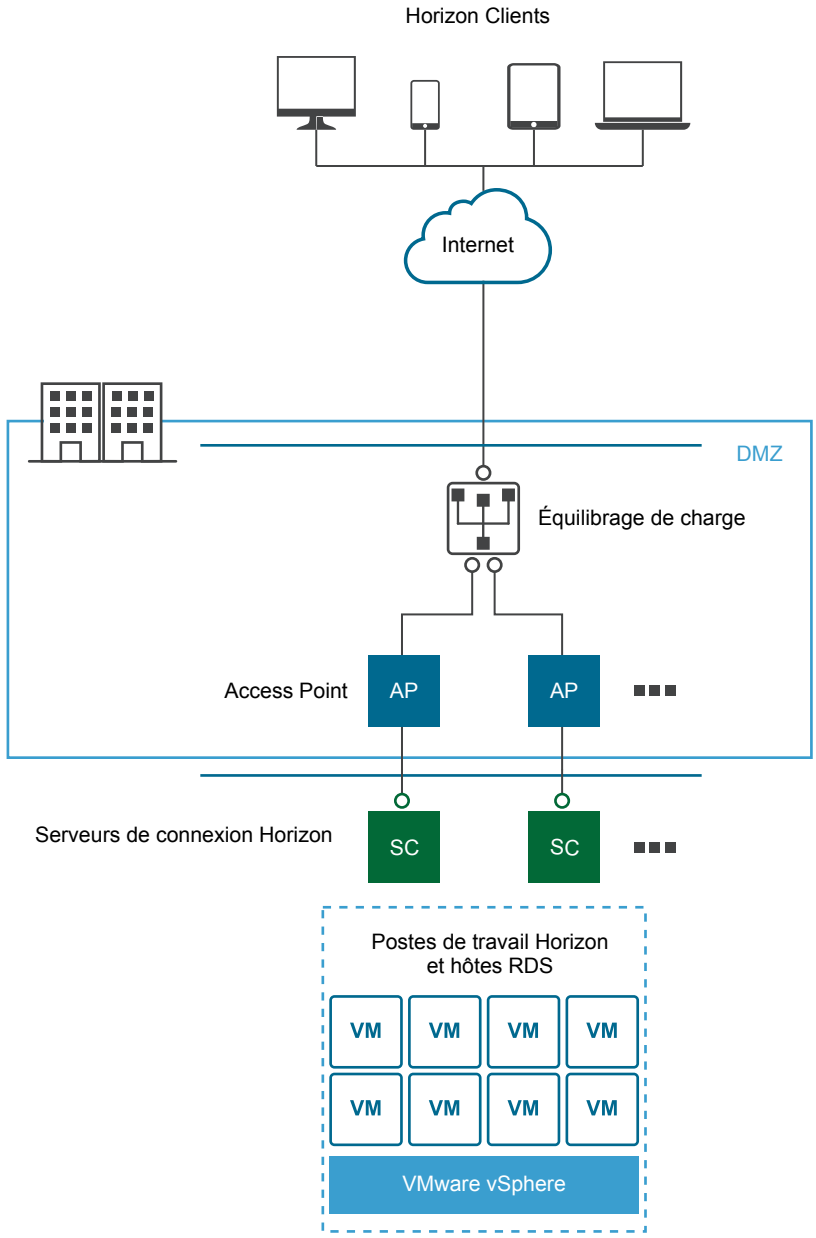
Vous pouvez implémenter plusieurs topologies différentes.

Un dispositif Access Point dans la zone DMZ peut être configuré pour pointer vers un serveur ou vers un équilibrage de charge qui fait face à un groupe de serveurs. Les dispositifs 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 des serveurs, la sélection de l'instance du serveur est dynamique. Par exemple, l'équilibrage de charge peut faire une sélection en fonction de la disponibilité et de sa connaissance du nombre de sessions en cours sur chaque instance du serveur. En général, les instances du serveur dans le pare-feu d'entreprise contiennent un équilibrage de charge pour prendre en charge l'accès interne. Avec Access Point, vous pouvez pointer le dispositif Access Point vers ce même équilibrage de charge qui est souvent déjà en cours d'utilisation.

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

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



Protocoles Horizon

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

- Protocole Horizon principal

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

- Protocoles Horizon secondaires

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

  - Le tunnel HTTPS utilisé pour l'encapsulation des protocoles TCP tels que RDP, MMR/CDR et le canal de framework client. (TCP 443).
  - Le protocole d'affichage Blast Extreme (TCP 443 et UDP 443).
  - Le protocole d'affichage PCoIP (TCP 4172 et UDP 4172).

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

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

Access Point est un dispositif de sécurité de couche 7 qui est normalement installé dans une zone démilitarisée (DMZ). Access Point est utilisé pour s'assurer que le trafic entrant dans le centre de données d'entreprise est effectué uniquement pour le compte d'un utilisateur distant à authentification élevée.

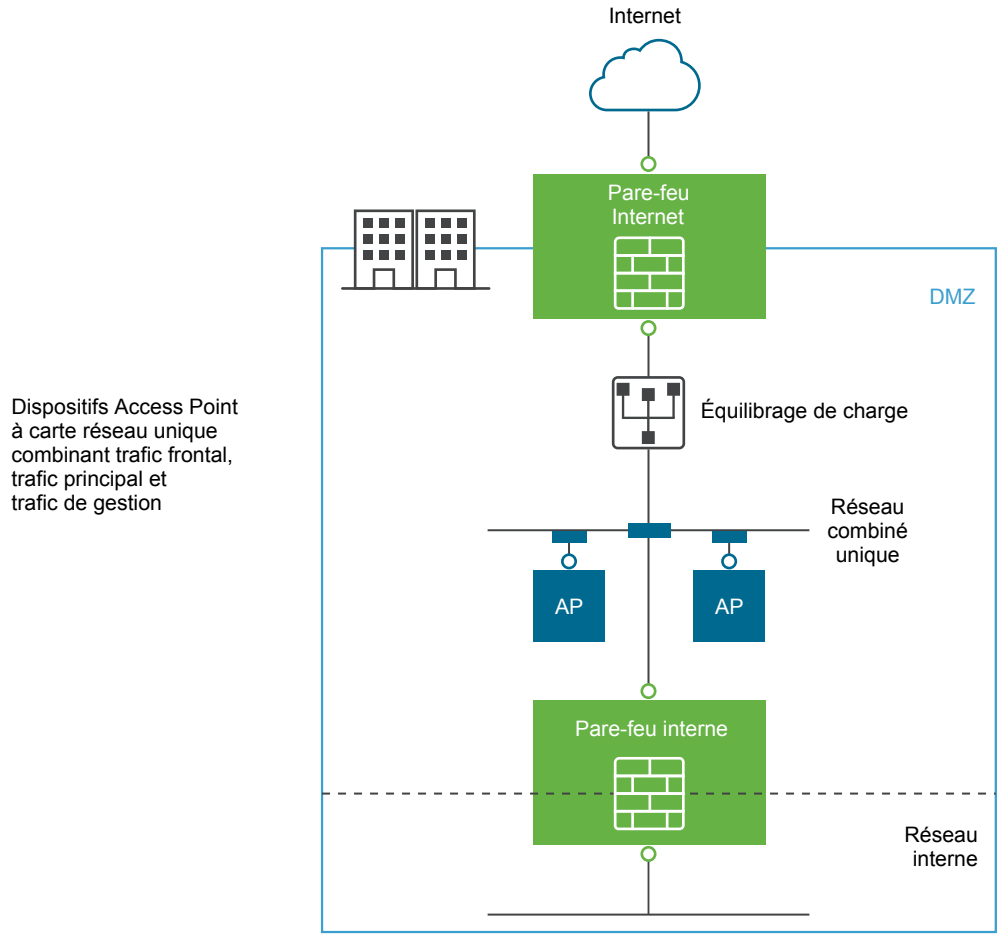
Un des paramètres de configuration pour Access Point est le nombre de cartes réseau à utiliser. Lorsque vous déployez Access Point, vous sélectionnez une configuration de déploiement pour votre réseau. Vous pouvez spécifier un, deux ou trois paramètres de carte réseau, appelés onenic, twonic ou threenic.

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

Déploiement DMZ typique avec une carte réseau unique

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

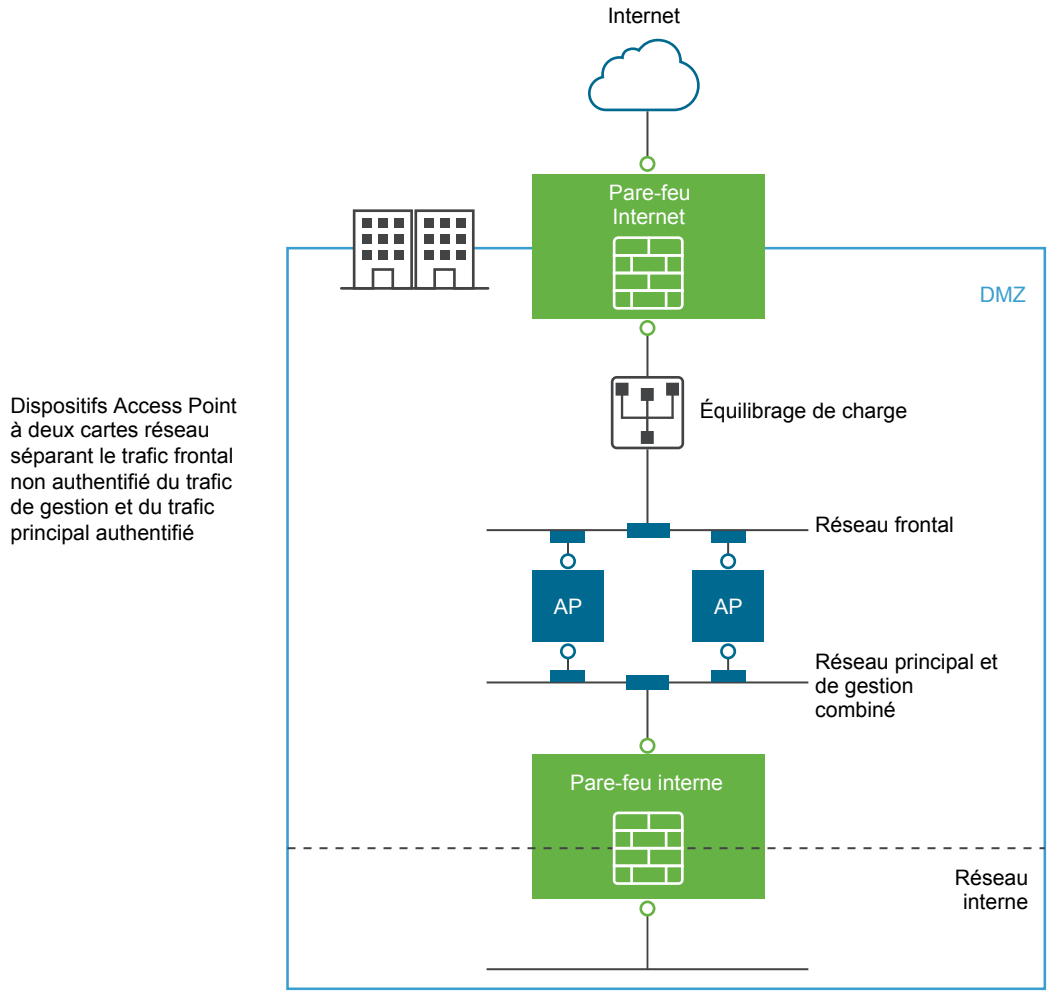
Figure 1-3. Option de carte réseau unique Access Point



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

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

Figure 1-4. Option de deux cartes réseau Access Point



Dans un déploiement à deux cartes réseau, le trafic en direction du réseau interne transitant par le pare-feu interne doit être autorisé par Access Point. Le trafic non autorisé ne se trouve pas sur ce réseau principal. Le trafic de gestion tel que REST API pour Access Point se trouve uniquement sur ce second réseau.

Si un périphérique sur le réseau frontal non authentifié a été compromis, comme l'équilibrage de charge, il n'est pas possible de reconfigurer ce périphérique pour contourner Access Point dans ce déploiement à deux cartes réseau. Il associe des règles de pare-feu de couche 4 à une sécurité Access Point de couche 7. De la même façon, si le pare-feu Internet n'a pas été correctement configuré pour autoriser le

port TCP 9443, cela n'expose toujours pas la REST API de gestion d'Access Point pour les utilisateurs Internet. Un principe de défense en profondeur fait appel à plusieurs niveaux de protection, comme le fait de savoir qu'une simple erreur de configuration ou attaque du système n'entraîne pas nécessairement une vulnérabilité générale.

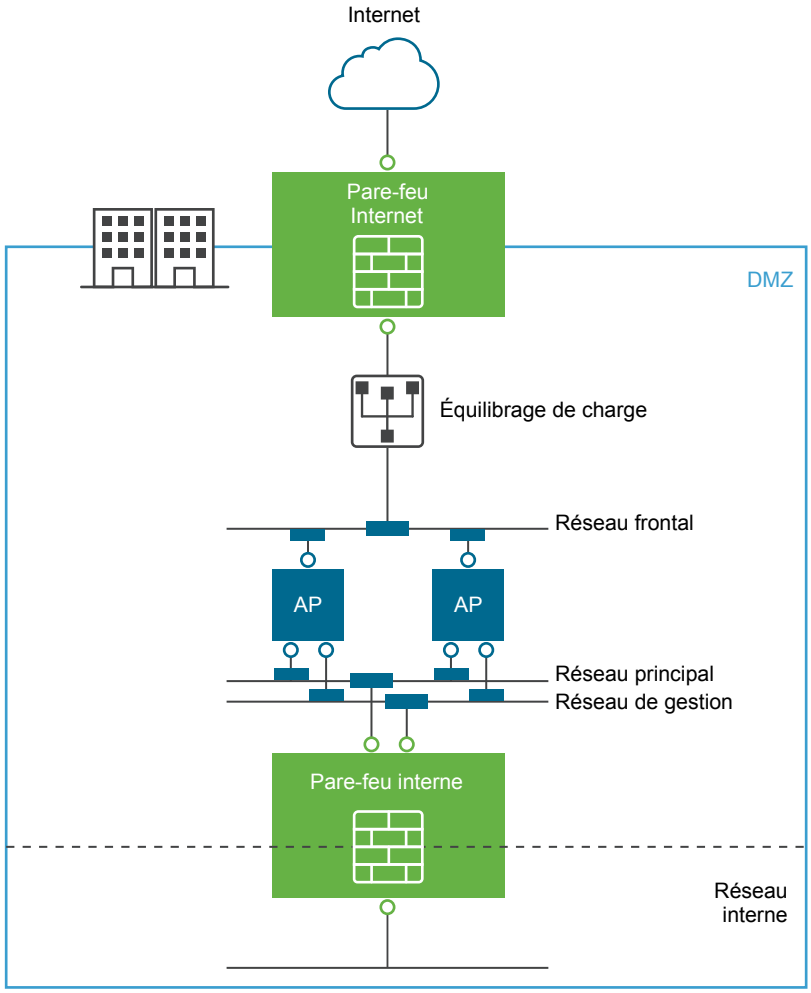
Dans un déploiement à deux cartes réseau, il est courant d'introduire des systèmes d'infrastructure supplémentaires, tels que des serveurs DNS, des serveurs RSA SecurID Authentication Manager sur le réseau principal au sein de la DMZ de façon que ces serveurs ne soient pas visibles sur le réseau Internet.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

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

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

Figure 1-5. Option de trois cartes réseau Access Point

Dispositifs Access Point à trois cartes réseau fournissant une séparation complète entre le trafic frontal non authentifié, le trafic principal authentifié et le trafic de gestion



Déploiement du dispositif Access Point 2

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

Deux méthodes principales peuvent être utilisées pour installer le dispositif Access Point.

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

Ce chapitre aborde les rubriques suivantes :

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

Utilisation de l'assistant de modèle OVF pour déployer Access Point

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

Une fois qu' Access Point est déployé, accédez à l'interface utilisateur (IU) d'administration pour configurer l'environnement Access Point, les ressources de poste de travail et d'application et les méthodes d'authentification à utiliser dans la zone DMZ.

Propriétés du déploiement d'Access Point

Lorsque vous déployez OVF, vous configurez le nombre d'interfaces réseau nécessaires, et vous définissez l'adresse IP et le mot de passe de l'administrateur. Les autres propriétés de déploiement peuvent être définies à partir des pages d'administration d'Access Point.

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

Propriété de déploiement	Description
Configuration du déploiement	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)	(Obligatoire) Spécifie l'adresse IPv4 ou IPv6 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 ou IPv6 Internet. Valeur par défaut : aucune.
Adresse IP du réseau de gestion	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	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 acheminé vers les autres interfaces réseau. Valeur par défaut : aucune.
Adresses de serveur DNS	(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	(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	(Obligatoire) Si vous ne définissez pas ce mot de passe, vous ne pourrez pas accéder à la console d'administration et 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.

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

Propriété de déploiement	Description
Paramètre régional à utiliser pour les messages localisés	(Obligatoire) Spécifie le paramètre régional à utiliser pour générer les messages d'erreur. ■ **en_US** pour l'anglais ■ **ja_JP** pour le japonais ■ **fr_FR** pour le français ■ **de_DE** pour l'allemand ■ **zh_CN** pour le chinois simplifié ■ **zh_TW** pour le chinois traditionnel ■ **ko_KR** pour le coréen Valeur par défaut : en_US.
URL du serveur Syslog	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.

Déploiement d' Access Point au moyen de l'assistant de modèle OVF

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

Remarque Si vous utilisez vSphere Web Client pour déployer OVF, vous pouvez également spécifier les adresses du serveur DNS, de la passerelle et du masque réseau pour chaque réseau. Si vous utilisez vSphere Client natif, vérifiez que vous avez affecté un pool IP à chaque réseau. Pour ajouter un pool IP dans vCenter Server au moyen du vSphere Client natif, accédez à l'onglet Pools IP du centre de données. Si vous utilisez vSphere Web Client, vous pouvez également créer un profil de protocole réseau. Accédez à l'onglet Gérer du centre de données et sélectionnez l'onglet Profils de protocole réseau.

Prérequis

- Familiarisez-vous avec les options de déploiement disponibles dans l'assistant. Reportez-vous à la section Configuration requise pour le système et le réseau Access Point.
- Déterminez le nombre d'interfaces réseau et d'adresses IP statiques à configurer pour le dispositif Access Point. Reportez-vous à la section Configuration requise pour le réseau.
- Téléchargez le fichier de programme d'installation `.ova` pour le 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-`*`Y.Y`*`.0.0-`*`xxxxxxx`*`_OVF10.ova`), où *Y.Y* est le numéro de version et *xxxxxxx* le numéro de build.

Procédure

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

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

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

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

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

Une page d'informations détaillées s'affiche. Examinez les détails du produit, la version et les exigences de taille.

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

Option	Description
Sélectionner une configuration de déploiement	Pour un réseau IPv4, vous pouvez utiliser une, deux ou trois interfaces réseau (cartes réseau). Pour un réseau IPv6, utilisez trois cartes réseau. Access Point requiert une adresse IP statique séparée pour chaque carte réseau. De nombreuses implémentations de zone DMZ utilisent des réseaux distincts pour sécuriser les différents types de trafic. Configurez Access Point en fonction de la conception de réseau de la zone DMZ dans laquelle il est déployé.
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.

Option	Description
Configuration des réseaux/Mappage réseau	Si vous utilisez vSphere Web Client, la page Configuration des réseaux vous permet de mapper chaque carte réseau vers un réseau et de spécifier des paramètres de protocole. a Sélectionnez IPv4 ou IPv6 dans la liste déroulante **Protocole IP**. b Sélectionnez la première ligne du tableau **Internet** et cliquez sur la flèche vers le bas pour sélectionner le réseau de destination. Si vous sélectionnez IPv6 comme protocole IP, vous devez sélectionner le réseau avec des capacités IPv6. Après avoir sélectionné la ligne, vous pouvez également entrer des adresses IP pour le serveur DNS, la passerelle et le masque de réseau dans la partie inférieure de la fenêtre. c Si vous utilisez plusieurs cartes réseau, sélectionnez la ligne suivante **ManagementNetwork**, sélectionnez le réseau de destination ; vous pouvez ensuite entrer les adresses IP pour le serveur DNS, la passerelle et le masque de réseau pour ce réseau. Si vous n'utilisez qu'une seule carte réseau, toutes les lignes sont mappées vers le même réseau. d Si vous avez une troisième carte réseau, sélectionnez également la troisième ligne et remplissez les paramètres. Si vous n'utilisez que deux cartes réseau, pour cette troisième ligne **BackendNetwork**, sélectionnez le réseau que vous avez utilisé pour **ManagementNetwork**. Avec vSphere Web Client, s'il n'existe pas encore de profil de protocole réseau, il est automatiquement créé lorsque l'assistant est terminé. Si vous utilisez le vSphere Client natif (plutôt que Web Client), la page Mappage réseau vous permet de mapper chaque carte réseau vers un réseau, mais il n'y a pas de champ pour spécifier les adresses du serveur DNS, de la passerelle et du masque de réseau. Comme décrit dans les conditions préalables, vous devez déjà avoir attribué un pool IP à chaque réseau ou avoir créé un profil de protocole réseau.
Personnaliser le modèle Propriétés	Les cases sur la page Propriétés sont spécifiques à Access Point et il est probable qu'elles ne soient pas requises pour d'autres types de dispositifs virtuels. Le texte sur la page de l'assistant explique chaque paramètre. Si le texte est tronqué sur le côté droit de l'assistant, redimensionnez la fenêtre en faisant glisser le curseur à partir de l'angle inférieur droit. Vous devez entrer des valeurs dans les cases suivantes : ■ **IPMode:STATICV4/STATICV6**. Si vous entrez STATICV4, vous devez entrer l'adresse IPv4 de la carte réseau. Si vous entrez STATICV6, vous devez entrer l'adresse IPv6 de la carte réseau. ■ **Liste de règles de transfert séparées par une virgule au format {tcp| udp}/listening-port-number/destination-ip-address:destination-port-nu** ■ **Adresse IPv4 de la carte réseau 1 (ETH0)**. Entrez l'adresse IPv4 de la carte réseau si vous avez entré STATICV4 pour le mode de carte réseau. ■ **Liste d'itinéraires personnalisés IPv4 séparée par une virgule pour la carte réseau 1 (eth0) au format ipv4-network-address/bits.ipv4-gateway-address** ■ **Adresse IPv6**. Entrez l'adresse IPv6 de la carte réseau si vous avez entré STATICV6 pour le mode de carte réseau. ■ **Adresses de serveur DNS**. Entrez les adresses IPv4 ou IPv6 séparées par des espaces des serveurs de nom de domaine de la VM.

Option	Description
	■ **Adresse IP du réseau de gestion** si vous avez spécifié 2 cartes réseau et **Adresse IP du réseau principal** si vous avez spécifié 3 cartes réseau ■ **Options de mot de passe**. Entrez le mot de passe de l'utilisateur racine de cette VM et le mot de passe de l'administrateur qui accède à la console d'administration et qui active l'accès à REST API. Tous les autres paramètres sont facultatifs ou ont déjà un paramètre par défaut. Notez les exigences de mot de passe répertoriées sur la page de l'assistant. Pour voir une description de toutes les propriétés de déploiement, reportez-vous à la section Propriétés du déploiement d'Access Point.

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

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

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

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

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

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

Le dispositif Access Point est déployé et démarre automatiquement.

Suivant

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

Configuration d' Access Point à partir des pages de configuration d'administration

Après avoir déployé l'OVF et que le dispositif Access Point est mis sous tension, connectez-vous à l'interface utilisateur d'administration d'Access Point afin de configurer les paramètres suivants.

- Configuration système d'Access Point et certificat du serveur SSL.

- Paramètres du service Edge pour Horizon, proxy inverse, tunnel par application et paramètres proxy pour AirWatch.
- Paramètres d'authentification pour RSA SecurID, RADIUS, certificat X.509 et RSA Adaptive Authentication.
- Paramètres du fournisseur d'identité SAML et du fournisseur de services.

Les options suivantes sont accessibles à partir des pages de configuration.

- Téléchargez les fichiers zip de journaux d'Access Point.
- Exportez les paramètres d' Access Point pour extraire les paramètres de configuration.
- Importez les paramètres d' Access Point pour créer et mettre à jour une configuration Access Point complète.

Configuration des paramètres système Access Point

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

L'URL de l'interface utilisateur d'administration d'Access Point est au format `https://<mycoAccessPointappliance.com>:9443/admin/index.html`. Pour vous connecter, entrez le nom d'utilisateur et le mot de passe de l'administrateur que vous avez configurés lorsque vous avez déployé le fichier OVF.

Prérequis

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

Procédure

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

3 Modifiez les valeurs suivantes de configuration du dispositif Access Point.

Option	Valeur par défaut et description
Paramètre régional	Spécifie le paramètre régional à utiliser pour générer les messages d'erreur. ■ **`en_US`** pour l'anglais ■ **`ja_JP`** pour le japonais ■ **`fr_FR`** pour le français ■ **`de_DE`** pour l'allemand ■ **`zh_CN`** pour le chinois simplifié ■ **`zh_TW`** pour le chinois traditionnel ■ **`ko_KR`** pour le coréen
Mot de passe Admin	Ce mot de passe a été défini lorsque vous avez déployé le dispositif. Vous pouvez le réinitialiser. Les mots de passe doivent contenir au moins 8 caractères, au moins une majuscule et une minuscule, un chiffre et un caractère spécial, qui inclut ! @ # $ % * ( ).
Suites de chiffrement	Dans la plupart des cas, les paramètres par défaut ne doivent pas être modifiés. Il s'agit des algorithmes cryptographiques qui sont utilisés pour chiffrer les communications entre les clients et le dispositif Access Point. Les paramètres de chiffement permettent d'activer différents protocoles de sécurité.
Respecter l'ordre de chiffrement	La valeur par défaut est NO. Sélectionnez **YES** pour activer le contrôle d'ordre de liste de chiffrement TLS.
SSL 3.0 activé	La valeur par défaut est NO. Sélectionnez **YES** pour activer le protocole de sécurité SSL 3.0.
TLS 1.0 activé	La valeur par défaut est NO. Sélectionnez **YES** pour activer le protocole de sécurité TLS 1.0.
TLS 1.1 activé	La valeur par défaut est YES. Le protocole de sécurité TLS 1.1 est activé.
TLS 1.2 activé	La valeur par défaut est YES. Le protocole de sécurité TLS 1.2 est activé.
URL Syslog	Entrez l'URL du serveur Syslog qui est utilisée pour la journalisation des événements Access Point. Cette valeur peut être une URL, un nom d'hôte ou une adresse IP. Si vous ne définissez pas l'URL du serveur Syslog, aucun événement n'est journalisé. Utilisez le format `syslog://server.example.com:514`.
URL de contrôle de santé	Entrez une URL à laquelle l'équilibrage de charge se connecte et vérifie la santé d'Access Point.
Cookies à mettre en cache	Ensemble de cookies mis en cache par Access Point. La valeur par défaut est aucun.
Mode IP	Sélectionnez le mode IP statique : STATICV4 ou STATICV6.
Délai d'expiration de session	La valeur par défaut est de **36 000 000** millisecondes.
Mode de mise au repos	Choisissez **YES** pour mettre en pause le dispositif Access Point afin d'obtenir un état cohérent permettant d'effectuer les tâches de maintenance.
Surveiller l'intervalle	La valeur par défaut est **60**.

4 Cliquez sur **Enregistrer**.

Suivant

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

Mise à jour des certificats signés du serveur SSL

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

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

Prérequis

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

Procédure

1. Dans la console d'administration, cliquez sur **Sélectionner**.
2. Dans la section Paramètres avancés, cliquez sur l'icône en forme d'engrenage Paramètres de certificat du serveur SSL.
3. Dans la ligne Clé privée, cliquez sur **Sélectionner** et accédez au fichier de clé privée.
4. Cliquez sur **Ouvrir** pour télécharger le fichier.
5. Dans la ligne Chaîne de certificat, cliquez sur Sélectionner et accédez au fichier de chaîne de certificat.
6. Cliquez sur **Ouvrir** pour télécharger le fichier.
7. Cliquez sur **Enregistrer**.

Suivant

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

Utilisation de PowerShell pour déployer Access Point

3

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

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

Ce chapitre aborde les rubriques suivantes :

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

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

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

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

  La machine peut également être un serveur vCenter Server exécuté sur Windows ou une machine Windows séparée.
- La commande VMware OVF Tool doit être installée sur la machine Windows exécutant le script.

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

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

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

Utilisation de PowerShell pour déployer le dispositif Access Point

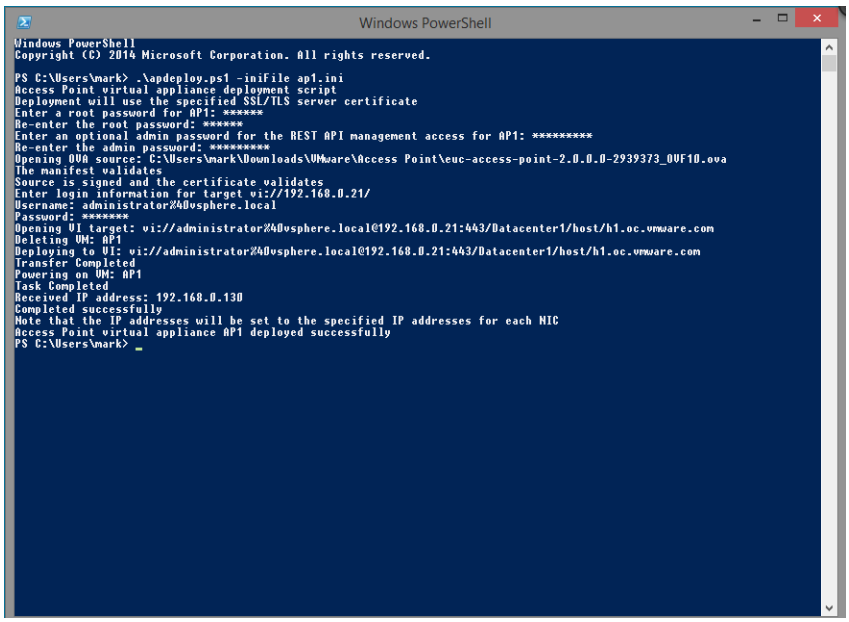
Les scripts PowerShell préparent votre environnement avec tous les paramètres de configuration. Lorsque vous exécutez le script PowerShell pour déployer Access Point, la solution est prête pour la production lors du premier démarrage système.

Prérequis

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

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

  Figure 3-1. Exemple de script PowerShell



Procédure

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

   Les fichiers compressés sont disponibles à l'adresse https://communities.vmware.com/docs/DOC-30835.
3. Ouvrez un script PowerShell et modifiez le répertoire vers l'emplacement de votre script.

4 Créez un fichier de configuration .INI pour le dispositif virtuel Access Point.

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

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

Exemple de fichier .INI à modifier.

```
name=AP1
source=C:\APs\euc-access-point-2.8.0.0-000000000_OVF10.ova
target=vi://administrator@vsphere.local:PASSWORD@192.168.0.21/Datacenter1/host/esx1.myco.int
ds=Local Disk 1
netInternet=VM Network
netManagementNetwork=VM Network
netBackendNetwork=VM Network

[Horizon/WebReverseProxy/AirwatchTunnel]
proxyDestinationUrl=https://192.168.0.209

# For IPv4, proxydestinationURL=https://192.168.0.209
# For IPv6, proxyDEstinationUrl=[fc00:10:112:54::220]
```

5 Pour vérifier la réussite de l'exécution du script, tapez la commande PowerShell set-executionpolicy.

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

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

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

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

6 Exécutez la commande pour démarrer le déploiement. Si vous ne spécifiez pas le fichier .INI, le script est défini par défaut sur ap.ini.

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

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

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

Le dispositif Access Point est déployé et disponible pour la production.

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

Cas d'utilisation pour le déploiement

4

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

Vous pouvez déployer Access Point avec Horizon View, Horizon Air Hybrid-Mode, VMware Identity Manager et VMware AirWatch.

Ce chapitre aborde les rubriques suivantes :

Déploiement d'Access Point avec Horizon View et Horizon Air Hybrid-Mode

Vous pouvez déployer Access Point avec Horizon View et Horizon Air Hybrid-Mode. Pour le composant View de VMware Horizon, les dispositifs Access Point jouent le même rôle que celui précédemment joué par les serveurs de sécurité View.

Scénario de déploiement

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

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

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

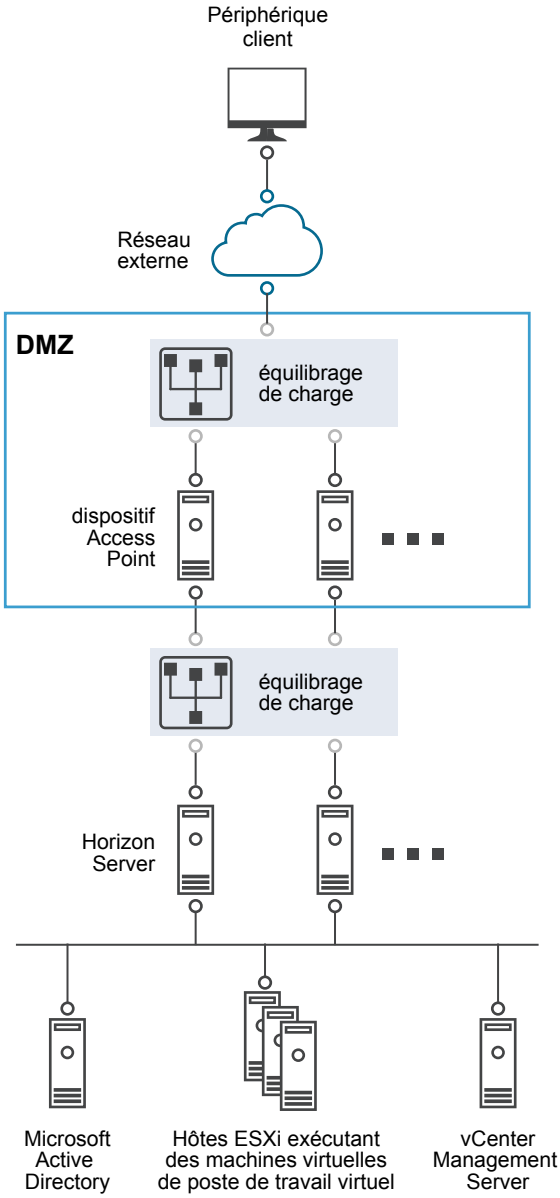
Vous devez vérifier les exigences pour un déploiement transparent d'Access Point avec Horizon.

- Si le dispositif Access Point pointe vers un équilibrage de charge devant les serveurs Horizon Server, la sélection de l'instance du serveur est dynamique.
- Access Point remplace le serveur de sécurité Horizon.
- Le port 443 doit être disponible pour Blast TCP/UDP.
- Blast Secure Gateway et PCoIP Secure Gateway doivent être activés lorsqu'Access Point est déployé avec Horizon. Cela garantit que les protocoles d'affichage peuvent servir de proxy automatiquement via Access Point. Les paramètres BlastExternalURL et pcoipExternalURL spécifient des adresses de connexion utilisées par les instances d'Horizon Client pour acheminer ces connexions de protocole d'affichage via les passerelles appropriées sur Access Point. Cela améliore la sécurité, car ces passerelles garantissent que le trafic du protocole d'affichage est contrôlé pour le compte d'un utilisateur authentifié. Le trafic de protocole d'affichage non autorisé est ignoré par Access Point.
- Désactivez les passerelles sécurisées sur les instances de Serveur de connexion View et activez-les sur les dispositifs Access Point.

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

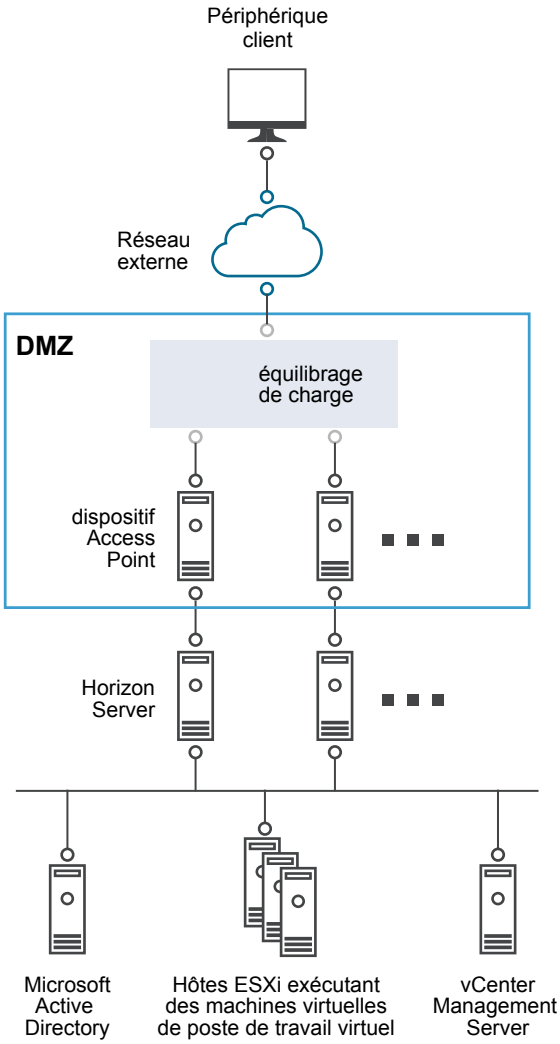
- Déploiement sécurisé. Access Point est implémenté en tant que machine virtuelle basée sur Linux, préconfigurée, verrouillée et à sécurité renforcée.
- Évolutivité. Vous pouvez connecter Access Point à un Serveur de connexion View individuel ou vous pouvez le connecter via un équilibrage de charge devant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

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



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

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



Authentification

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

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

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

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

Configuration des paramètres Horizon

Vous pouvez déployer Access Point à partir d'Horizon View et Horizon Air Hybrid-Mode. Pour le composant View de VMware Horizon, le dispositif Access Point joue le même rôle que celui précédemment joué par le serveur de sécurité View.

Procédure

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

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

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

Option	Description
Méthodes d'authentification	Sélectionnez les méthodes d'authentification à utiliser. La méthode par défaut est l'utilisation d'une authentification directe du nom d'utilisateur et du mot de passe. Les méthodes d'authentification que vous avez configurées dans Access Point figurent dans les menus déroulants. Pour configurer l'authentification qui inclut l'application d'une seconde méthode d'authentification si la première tentative échoue : a Sélectionnez une méthode d'authentification dans le premier menu déroulant. b Cliquez sur **+** et sélectionnez ET ou OU. c Sélectionnez la seconde méthode d'authentification dans le troisième menu déroulant. Pour obliger les utilisateurs à s'authentifier par le biais de deux méthodes d'authentification, remplacez OU par ET dans la liste déroulante.
URL de contrôle de santé	Si l'équilibrage de charge est configuré, entrez l'URL que l'équilibrage de charge utilise pour se connecter et contrôler la santé du dispositif Access Point.
SP SAML	Entrez le nom du fournisseur de services SAML pour le Broker View XMLAPI. Ce nom doit correspondre à celui des métadonnées du fournisseur de services configuré ou à la valeur spéciale DEMO.
PCOIP activé	Remplacez NO par **YES** pour spécifier si la passerelle sécurisée PCoIP est activée.
URL externe du proxy	Entrez l'URL externe du dispositif Access Point. Les clients utilisent cette URL pour des connexions sécurisées via la passerelle sécurisée PCoIP. Cette connexion est utilisée pour le trafic PCoIP. La valeur par défaut est l'adresse IP d'Access Point et le port 4172.
Invite de conseil de carte à puce	Remplacez NO par **YES** pour permettre au dispositif Access Point de prendre en charge la fonctionnalité des conseils de nom d'utilisateur pour la carte à puce. Avec la fonctionnalité de conseils de nom d'utilisateur de carte à puce, le certificat de carte à puce d'un utilisateur peut effectuer un mappage vers plusieurs comptes d'utilisateur de domaine Active Directory.
Blast activé	Pour utiliser la passerelle sécurisée Blast, Remplacez NO par **YES**.
URL externe Blast	Entrez l'URL du nom de domaine complet du dispositif Access Point que les utilisateurs emploient pour établir une connexion sécurisée à partir des navigateurs Web via la passerelle sécurisée Blast. Entrez-la sous la forme https://exampleappliance:443
Tunnel activé	Si le tunnel sécurisé View est utilisé, Remplacez NO par **YES**. Le client utilise l'URL externe pour les connexions de tunnel via la passerelle sécurisée View. Le tunnel est utilisé pour le trafic RDP, USB et de redirection multimédia (MMR).
URL externe de tunnel	Entrez l'URL externe du dispositif Access Point. La valeur Access Point par défaut est utilisée le cas échéant.
Faire correspondre au nom d'utilisateur Windows	Remplacez NO par **YES** pour faire correspondre le RSA SecurID et le nom d'utilisateur Windows. Lorsqu'il est défini sur YES, securID-auth est défini sur true et la correspondance de securID et du nom d'utilisateur Windows est appliquée.

Option	Description
Emplacement de la passerelle	Remplacez NO par **YES** pour activer l'emplacement à partir duquel sont issues les demandes. Le serveur de sécurité et Access Point définissent l'emplacement de la passerelle. L'emplacement peut être externe ou interne.
Windows SSO activé	Remplacez NO par **YES** pour activer l'authentification RADIUS. La connexion Windows utilise les informations d'identification utilisées dans la première demande d'accès RADIUS réussie.

7 Cliquez sur **Enregistrer**.

Déploiement d'Access Point comme proxy inverse

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

Scénario de déploiement

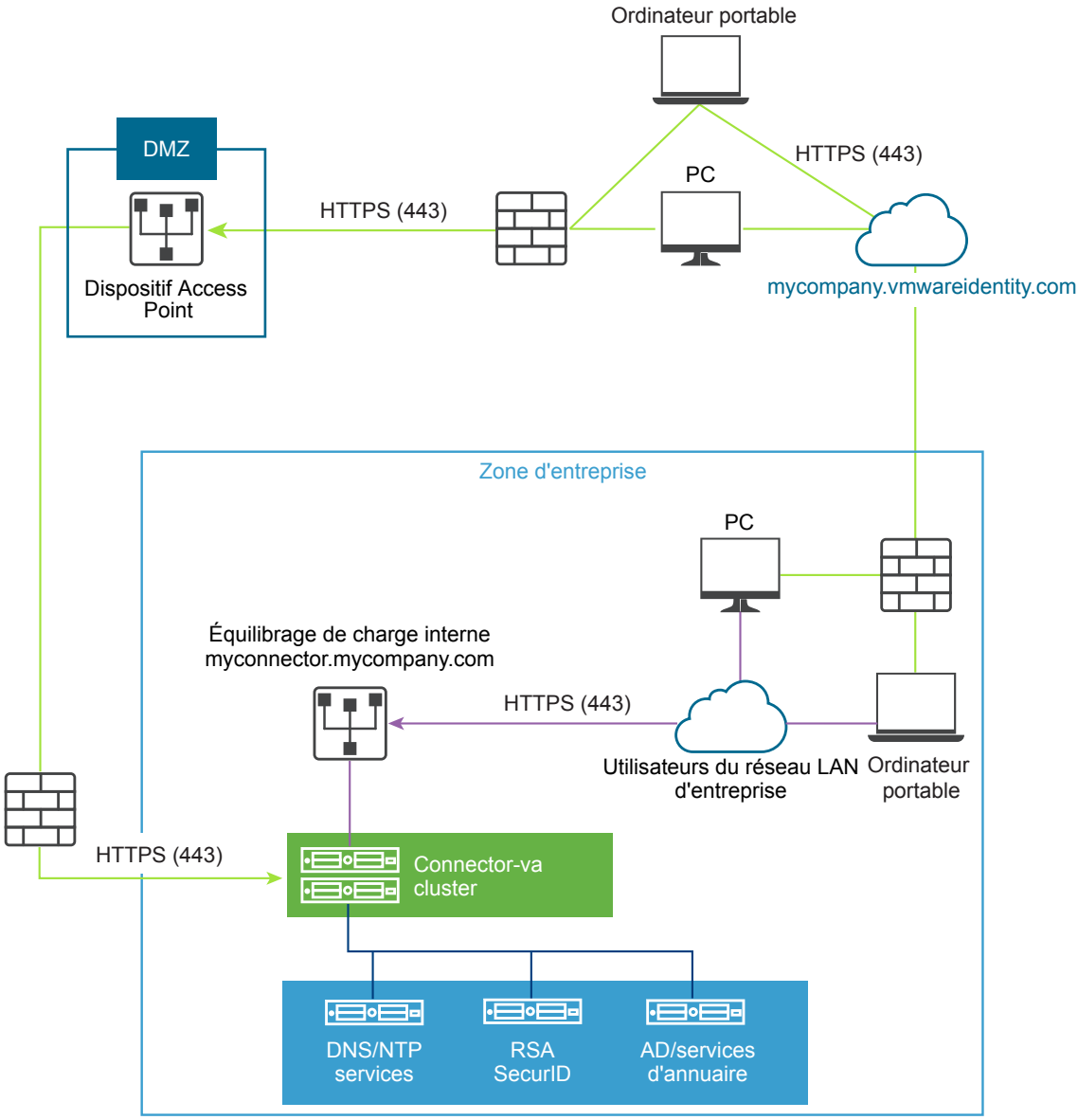
Access Point fournit un accès distant sécurisé pour un déploiement sur site de VMware Identity Manager. En général, les dispositifs Access Point sont déployés dans une zone démilitarisée (DMZ) de réseau. Avec VMware Identity Manager, le dispositif Access Point agit en tant que proxy inverse Web entre le navigateur d'un utilisateur et le service VMware Identity Manager dans le centre de données. Access Point autorise également les accès distants au catalogue VMware Identity Manager pour le lancement d'applications Horizon.

Exigences du déploiement d'Access Point avec VMware Identity Manager

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

- Access Point doit utiliser le DNS interne. Cela signifie que proxyDestinationURL doit utiliser un FQDN.

Figure 4-3. Dispositif Access Point pointant vers le connecteur



Comprendre le proxy inverse

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

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

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

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

La prise en charge du proxy inverse est limitée avec Access Point 2.8 à VMware Identity Manager et aux ressources Web internes, telles que confluence et WIKI. À l'avenir, la liste de ressources sera allongée.

Remarque Les propriétés `authCookie` et `unSecurePattern` ne sont pas valides pour Authn Reverse Proxy. Vous devez utiliser la propriété `authMethods` pour définir la méthode d'authentification.

Configuration du proxy inverse pour VMware Identity Manager

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

Prérequis

Configuration requise pour un déploiement d'Access Point avec VMware Identity Manager.

- DNS fractionné
- Le service VMware Identity Manager doit avoir un nom de domaine complet (FQDN) comme nom d'hôte.
- Access Point doit utiliser le DNS interne. Cela signifie que l'URL proxyDestination doit utiliser un FQDN.

Procédure

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

Option	Description
Identifiant	L'identifiant du service Edge est défini sur WEB_REVERSE_PROXY.
URL de destination du proxy	Entrez l'adresse du serveur VMware Identity Manager. Par exemple, entrez `https://vmwareidentitymgr.example.com`.

Option	Description
Empreintes numériques de l'URL de destination du proxy	Entrez une liste des empreintes numériques de certificat serveur SSL acceptables pour l'URL proxyDestination. Si vous incluez le caractère générique *, n'importe quel certificat est autorisé. Une empreinte numérique est au format [alg=]xx:xx, où alg peut correspondre à sha1, la valeur par défaut, ou md5. Les « xx » correspondent à des chiffres hexadécimaux. Par exemple, sha=C3 89 A2 19 DC 7A 48 2B 85 1C 81 EC 5E 8F 6A 3C 33 F2 95 C3 Si vous ne configurez pas les empreintes numériques, les certificats de serveur doivent être émis par une autorité de certification approuvée.
Modèle de proxy	Entrez les chemins d'URI correspondants qui assurent la transmission à l'URL de destination. Par exemple, entrez **`(/|/SAAS(.*)|/hc(.*)|/web(.*)|/catalog-portal(.*))`**.

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

Option	Description
Méthodes d'authentification	La méthode par défaut est l'utilisation d'une authentification directe du nom d'utilisateur et du mot de passe. Les méthodes d'authentification que vous avez configurées dans Access Point figurent dans les menus déroulants. Les méthodes d'authentification que vous avez configurées dans Access Point figurent dans le menu déroulant.
URL de contrôle de santé	Si l'équilibrage de charge est configuré, entrez l'URL que l'équilibrage de charge utilise pour se connecter et contrôler la santé du dispositif Access Point.
SP SAML	Entrez le nom du fournisseur de services SAML pour le broker API XML View. Ce nom doit correspondre à celui des métadonnées du fournisseur de services configuré ou à la valeur spéciale **`DEMO`**.
Code d'activation	Entrez le code d'activation généré par le service VMware Identity Manager et importé dans Access Point pour établir la confiance entre VMware Identity Manager et Access Point.
URL externe	La valeur par défaut est l'URL de l'hôte Access Point, le port 443. Vous pouvez entrer une autre URL externe. Utilisez le format `https://<host:port>`.

7 Cliquez sur **Enregistrer**.

Déploiement d'Access Point avec AirWatch Tunnel

Le dispositif Access Point est déployé sur la zone DMZ. Le déploiement implique l'installation des composants Access Point et des composants AirWatch, tels que les services d'agent et de proxy tunnel

Le déploiement d'AirWatch Tunnel pour votre environnement AirWatch implique la configuration du matériel initial, la configuration des informations sur le serveur et des paramètres d'application dans la console d'administration AirWatch, le téléchargement d'un fichier de programme d'installation et l'exécution du programme d'installation sur votre serveur AirWatch Tunnel.

Vous pouvez configurer manuellement chacun des services Edge lorsque l'installation d'OVF est terminée et que les valeurs sont modifiées.

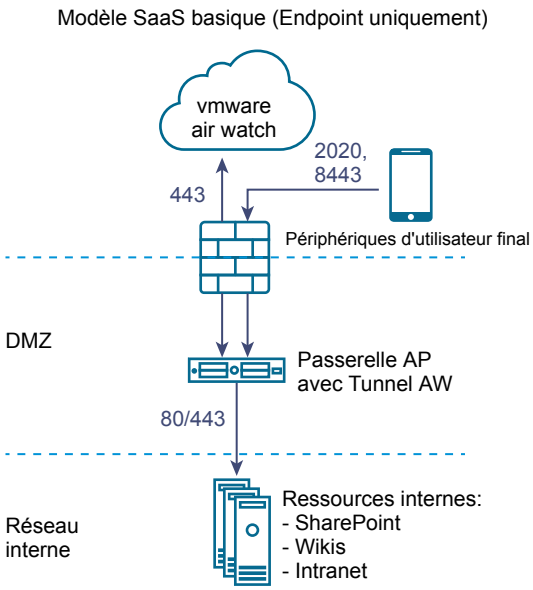
Pour plus d'informations sur le déploiement d'Access Point avec AirWatch, consultez https://resources.air-watch.com/view/vb7zp7wwhpw756m2pfxy .

Déploiement de proxy tunnel pour AirWatch

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

L'application mobile crée une connexion HTTPS sécurisée avec le serveur Tunnel Proxy et protège les données sensibles. Pour utiliser une application interne avec le proxy AirWatch Tunnel, vérifiez que le SDK AirWatch est intégré dans votre application qui vous offre des capacités de tunneling avec ce composant.

Figure 4-4. Déploiement de proxy tunnel

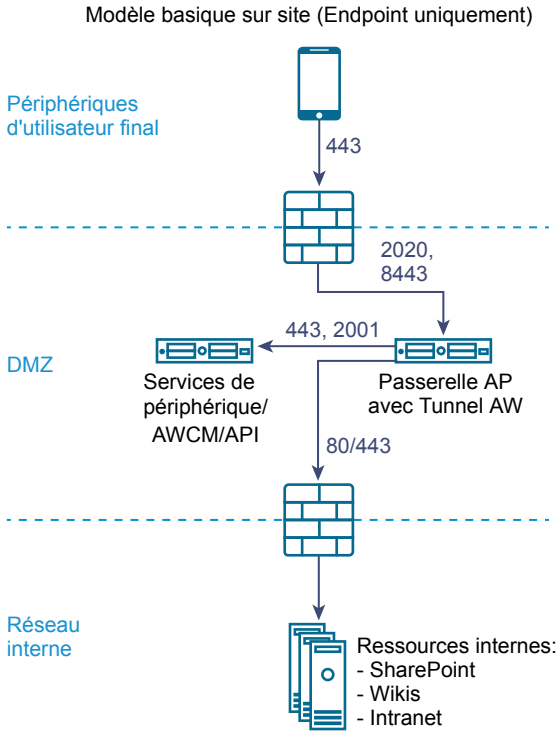


Déploiement de tunnel par application avec AirWatch

Le déploiement de tunnel par application permet aux applications internes et publiques d'accéder en toute sécurité à des ressources d'entreprise qui résident sur votre réseau interne sécurisé.

Il utilise les capacités par application offertes par les systèmes d'exploitation ; tels qu'iOS 7+ ou Android 5.0+. Ces systèmes d'exploitation permettent à des applications spécifiques approuvées par les administrateurs de mobilité d'accéder à des ressources internes application par application. L'avantage de cette solution est qu'aucun changement de code n'est requis pour les applications mobiles. La prise en charge du système d'exploitation offre une expérience utilisateur transparente et une meilleure sécurité que les autres solutions personnalisées.

Figure 4-5. Déploiement de tunnel par application



Configuration du tunnel par application et des paramètres de proxy pour AirWatch

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

Procédure

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

Option	Description
Identifiant	Définissez par défaut sur View. Access Point peut communiquer avec des serveurs qui utilisent le protocole View XML, tels que le Serveur de connexion View, Horizon Air et Horizon Air Hybrid-mode.
URL du serveur API	Entrez l'URL du serveur d'API AirWatch. Par exemple, entrez-la sous la forme https://example.com:<port>.
Nom d'utilisateur du serveur API	Entrez le nom d'utilisateur pour vous connecter au serveur API.
Mot de passe du serveur API	Entrez le mot de passe pour vous connecter au serveur API.

Option	Description
Code du groupe d'organisation	Entrez l'organisation de l'utilisateur.
Nom d'hôte du serveur AirWatch	Entrez le nom d'hôte du serveur AirWatch.

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

Option	Description
Proxy sortant AirWatch	Remplacez NO par **YES** pour initialiser le service de proxy tunnel.
HÔTE de proxy sortant	Entrez le nom d'hôte sur lequel le proxy sortant est installé. **Remarque** Il ne s'agit pas de Tunnel Proxy.
PORT de proxy sortant	Entrez le numéro de port du proxy sortant.
Nom d'utilisateur du proxy sortant	Entrez le nom d'utilisateur pour vous connecter au proxy sortant.
Mot de passe de proxy sortant	Entrez le mot de passe pour vous connecter au proxy sortant.
Authentification NTLM	Remplacez NO par **YES** pour spécifier que la demande de proxy sortant nécessite une authentification NTLM.
Utiliser pour le proxy AirWatch Tunnel	Remplacez NO par **YES** pour utiliser ce proxy en tant que proxy sortant pour AirWatch Tunnel. S'il n'est pas activé, Access Point utilise ce proxy pour l'appel API initial afin d'obtenir la configuration à partir de la console d'administration AirWatch.

7 Cliquez sur **Enregistrer**.

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

5

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

Remarque La configuration des certificats TLS/SSL pour le dispositif Access Points'applique à Horizon View, Horizon Air Hybrid-Mode et Web Reverse Proxy uniquement.

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, ou pour utiliser les scripts PowerShell, vous devez convertir le certificat en fichiers au format PEM pour la chaîne de certificats et la clé privée, et vous devez ensuite convertir les fichiers `.pem` en un format sur une seule ligne qui inclut des caractères de saut de ligne intégrés.

Lors de la configuration d'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 `mycaservercert.pfx`, utilisez les commandes suivantes pour convertir le certificat :

   ```
   openssl pkcs12 -in mycaservercert.pfx -nokeys -out mycaservercert.pem
   openssl pkcs12 -in mycaservercert.pfx -nodes -nocerts -out mycaservercert.pem
   openssl rsa -in mycaservercertkey.pem -check -out mycaservercertkeyrsa.pem
   ```

3. Modifiez `mycaservercert.pem` et supprimez les entrées inutiles du certificat. Il doit contenir le certificat de serveur SSL, ainsi que les certificats d'autorité de certification intermédiaires et racine nécessaires.

4 Utilisez la commande UNIX suivante pour convertir chaque fichier `.pem` en une valeur pouvant être transmise dans une chaîne JSON à l'API REST 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. Si vous disposez d'un certificat intermédiaire, convertissez ce certificat en format sur une seule ligne et ajoutez-le au premier certificat pour que les deux se trouvent sur la même ligne.

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

Suivant

Si vous avez converti un certificat de serveur TLS/SSL, reportez-vous à la section Remplacer le certificat de serveur TLS/SSL par défaut pour Access Point. Pour les certificats de carte à puce, reportez-vous à la section Configuration de l'authentification par certificat ou carte à puce sur le dispositif Access Point.

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 des scripts PowerShell ou 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.

Cette procédure décrit comment utiliser l'API REST pour remplacer le certificat. Une méthode plus facile consiste à utiliser les scripts PowerShell joints à l'article de blog « Using PowerShell to Deploy VMware Access Point » (Utilisation de PowerShell pour déployer VMware Access Point) disponible sur la page https://communities.vmware.com/docs/DOC-30835. Si vous avez déjà déployé le dispositif Access Point nommé, exécuter de nouveau le script mettra le dispositif hors tension, le supprimera et le redéploiera avec les paramètres actuels que vous spécifiez.

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.
- 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 ou SSL

Même si, dans quasiment tous les cas, les paramètres par défaut n'ont pas à être modifiés, vous pouvez configurer les protocoles de sécurité et les algorithmes cryptographiques qui sont utilisés pour chiffrer les communications entre les clients et le dispositif 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 v1.1 et TLS v1.2 sont activés. TLS v1.0 et SSL v3.0 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`.

Procédure

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

   L'exemple suivant a les paramètres par défaut.

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

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

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

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

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

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

Configuration de l'authentification dans la zone DMZ

6

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

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

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

Ce chapitre aborde les rubriques suivantes :

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

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

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

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

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

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

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

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

Configuration de l'authentification par certificat dans Access Point

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

Prérequis

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

Procédure

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

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

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

5. Cliquez sur **Enregistrer**.

Suivant

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

Obtenir des certificats d'autorités de certification

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

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

Procédure

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

Obtenir le certificat d'une autorité de certification de Windows

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

Procédure

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

   Si le certificat utilisateur n'apparaît pas dans votre magasin personnel, utilisez le logiciel du lecteur pour exporter le certificat utilisateur vers un fichier. Ce fichier est utilisé à l'étape 4 de cette procédure.
2. Dans Internet Explorer, sélectionnez **Outils > Options Internet**.
3. Sous l'onglet **Contenu**, cliquez sur **Certificats**.

4 Sous l'onglet **Personnel**, sélectionnez le certificat que vous voulez utiliser et cliquez sur **Affichage**.

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

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

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

6 Sous l'onglet **Détails**, cliquez sur **Copier dans un fichier**.

   L'assistant **Certificate Export (Exportation de certificat)** apparaît.

7 Cliquez sur **Suivant > Suivant**, puis tapez un nom et un emplacement pour le fichier à exporter.

8 Cliquez sur **Suivant** pour enregistrer le fichier comme certificat racine dans l'emplacement spécifié.

Configuration de RSA SecurID Authentication dans Access Point

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

Prérequis

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

Procédure

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

2 Dans Paramètres généraux, section Paramètres d'authentification, cliquez sur **Afficher**.

3 Cliquez sur l'engrenage dans la ligne RSA SecurID.

4 Configurez la page RSA SecurID.

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

Option	Action
Activer RSA SecurID	Remplacez NO par **YES** pour activer l'authentification SecurID.
*Nom	Le nom est securid-auth.
*Nombre d'itérations	Entrez le nombre de tentatives d'authentification autorisées. Il s'agit du nombre maximal d'échecs de tentatives de connexion à l'aide du jeton RSA SecurID. La valeur par défaut est de 5 tentatives. **Remarque** Lorsque plusieurs annuaires sont configurés et que vous implémentez l'authentification RSA SecurID avec des annuaires supplémentaires, configurez **Nombre de tentatives d'authentification autorisées** avec la même valeur pour chaque configuration RSA SecurID. Si la valeur est différente, l'authentification SecurID échoue.
*Nom d'HÔTE externe	Entrez l'adresse IP de l'instance Access Point. La valeur que vous entrez doit correspondre à celle que vous avez utilisée lorsque vous avez ajouté le dispositif Access Point en tant qu'agent d'authentification au serveur RSA SecurID.
*Nom d'HÔTE interne	Entrez la valeur attribuée à l'invite **Adresse IP** sur le serveur RSA SecurID.
*Configuration du serveur	Cliquez sur Modifier pour télécharger le fichier de configuration du serveur RSA SecurID. Vous devez d'abord télécharger le fichier compressé auprès du serveur RSA SecurID, puis extraire le fichier de configuration du serveur qui est appelé par défaut `sdconf.rec`.
*Suffixe d'ID de nom	Entrez le nameId qui permet à View d'offrir une expérience TrueSSO.

Configuration de RADIUS pour Access Point

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

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

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

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

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

Configuration de l'authentification RADIUS

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

Prérequis

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

Les informations de serveur RADIUS suivantes sont requises.

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

Procédure

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

Option	Action
Activer RADIUS	Remplacez NO par **YES** pour activer l'authentification RADIUS.
Nom*	Le nom est radius-auth
Type d'authentification*	Entrez le protocole d'authentification pris en charge par le serveur RADIUS. PAP, CHAP, MSCHAP1 ou MSCHAP2.
Secret partagé*	Entrez le secret partagé RADIUS.
Nombre de tentatives d'authentification autorisées*	Entrez le nombre maximal de tentatives de connexion échouées lorsque vous utilisez RADIUS pour vous connecter. La valeur par défaut est de trois tentatives.

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

4 Cliquez sur **Enregistrer**.

Configuration de RSA Adaptive Authentication dans Access Point

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

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

Méthodes d'authentification prises en charge de RSA Adaptive Authentication

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

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

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

Inscription d'utilisateurs avec le serveur RSA Adaptive Authentication

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

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

Configuration de RSA Adaptive Authentication dans Access Point

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

Prérequis

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

- Informations de configuration Active Directory et certificat SSL Active Directory disponibles.

Procédure

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

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

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

Option	Description
Nom unique de liaison*	Entrez le compte pouvant rechercher des utilisateurs. Par exemple : CN=binduser,OU=myUnit,DC=myCorp,DC=com.
Mot de passe de liaison	Entrez le mot de passe du compte ND Bind.
Attribut de recherche	Entrez l'attribut du compte contenant le nom d'utilisateur.
Certificat de l'annuaire	Pour établir des connexions SSL sécurisées, ajoutez le certificat du serveur d'annuaire dans la zone de texte. S'il existe plusieurs serveurs, ajoutez le certificat racine de l'autorité de certification.
Utiliser STARTTLS	Remplacez NO par **YES** pour utiliser STARTTLS.

5 Cliquez sur **Enregistrer**.

Générer des métadonnées SAML Access Point

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

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

Prérequis

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

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

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

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

Procédure

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

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

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

Pour un serveur Horizon Air Hybrid-mode, consultez la documentation du produit pour obtenir des instructions spécifiques.

Copier les métadonnées SAML du fournisseur de services sur Access Point

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

Prérequis

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

Procédure

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

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

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

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

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

2. Dans la section Configuration manuelle de l'interface utilisateur d'administration d'Access Point, cliquez sur **Sélectionner**.
3. Dans la section Paramètres avancés, cliquez sur l'icône en forme d'engrenage **Paramètres du fournisseur de serveur SAML** .
4. Entrez le nom du fournisseur de services dans la zone de texte correspondante.
5. Dans la zone de texte Métadonnées XML, collez le fichier de métadonnées que vous avez créé à l'étape 1.
6. Cliquez sur **Enregistrer**.

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

Dépannage du déploiement d'Access Point 7

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

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

Ce chapitre aborde les rubriques suivantes :

Dépannage des erreurs de déploiement

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

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

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

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

Commande ovftool introuvable

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

Réseau non valide dans la propriété netmask1

- Le message peut indiquer netmask0, netmask1 ou netmask2. Vérifiez qu'une valeur a été définie dans le fichier .INI pour chacun des trois réseaux, par exemple netInternet, netManagementNetwork et netBackendNetwork.

- Vérifiez qu'un profil de protocole de réseau vSphere a été associé à chaque nom de réseau référencé. Cela spécifie des paramètres réseau tels que le masque de sous-réseau IPv4, la passerelle, etc. Vérifiez que le profil de protocole réseau associé dispose des valeurs correctes pour chaque paramètre.

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

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

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

Configurer Access Point pour l'authentification RSA SecureID

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

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

Ajoutez une section en bas de votre fichier .INI.

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

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

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

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

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

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

```
target=vi://administrator@vsphere.local:PASSWORD@192.168.0.21/Datacenter1/
target=vi://administrator@vsphere.local:PASSWORD@192.168.0.21/Datacenter1/host
target=vi://administrator@vsphere.local:PASSWORD@192.168.0.21/Datacenter1/host/Cluster1/
or
target=vi://administrator@vsphere.local:PASSWORD@192.168.0.21/Datacenter1/host/esxhost1
```

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

Collecte de journaux depuis le dispositif Access Point

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 7-1. 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 7-2. 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.

Tableau 7-2. Fichiers journaux d' Access Point (suite)

Nom de fichier	Description
`tunnel.log`	Contient des messages de journal du processus de tunnel utilisé dans le cadre du traitement API XML.
`bsg.log`	Contient des messages de journal de Blast Secure Gateway.
`SecurityGateway_*.log`	Contient des messages de journal de PCoIP Secure Gateway.

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

Fichiers journaux d'Access Point pour AirWatch

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

  Les fichiers tunnel-init.log et tunnel.log sont capturés à partir de ce répertoire.

- `/var/log.airwatch/proxy`

  Le fichier proxy.log est capturé à partir de ce répertoire.

- `/var/log/airwatch/appliance–agent`

  Le fichier appliance-agent.log est capturé à partir de ce répertoire.

Activation du mode de débogage

Vous pouvez activer le mode de débogage pour un dispositif Access Point afin d'afficher ou de modifier l'état interne du dispositif. Le mode de débogage vous permet de tester le scénario de déploiement dans votre environnement.

Prérequis

- Vérifiez que le dispositif Access Point n'est pas utilisé.

  Remarque Il est utile de collecter des informations de journalisation sur un dispositif Access Point qui ne fonctionne pas. Les journaux peuvent être obtenus de façon classique.

Procédure

1. Connectez-vous à la machine Access Point.
2. Entrez la commande suivante dans l'interface de ligne de commande.

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

3. Affichez le fichier de propriétés de journal.

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

4. Recherchez la ligne suivante dans le fichier de propriétés et modifiez-la. Remplacez info par debug.

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

5 Entrez la commande pour modifier la configuration de journalisation depuis n'importe quel chemin.

```
supervisorctl restart esmanager
```