Configuration et installation de connecteur de systèmes d'entreprise de VMware

VMware Identity Manager 2.9.1

vmware®

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

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

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

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

docfeedback@vmware.com

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

Installation et configuration de VMware Enterprise Systems Connector

Installation et configuration de VMware Enterprise Systems Connector fournit des informations sur la configuration du Connecteur de systèmes d'entreprise VMware™, qui offre aux entreprises la possibilité pour intégrer VMware AirWatch® et VMware Identity Manager™ à leurs systèmes d'entreprise back-end.

Ce document fournit des informations sur l'installation de deux composants de la VMware Enterprise Systems Connector, le AirWatch Cloud Connector et le VMware Identity Manager Connector.

Cette information est applicable pour les deux SaaS et sur les scénarios de déploiement de site. Vos remarques dans le texte indiquent les différences entre les environnements.

Public concerné

Ces informations sont destinées aux administrateurs système Windows expérimentés. Il est applicable pour les deux SaaS et sur les clients locaux.

Glossaire VMware Technical Publications

VMware Technical Publications fournit un glossaire des termes qui peuvent éventuellement ne pas vous être familiers. Pour consulter la définition des termes utilisés dans la documentation technique VMware, visitez le site Web http://www.vmware.com/support/pubs.

Aperçu de VMware Enterprise Systems Connector 1

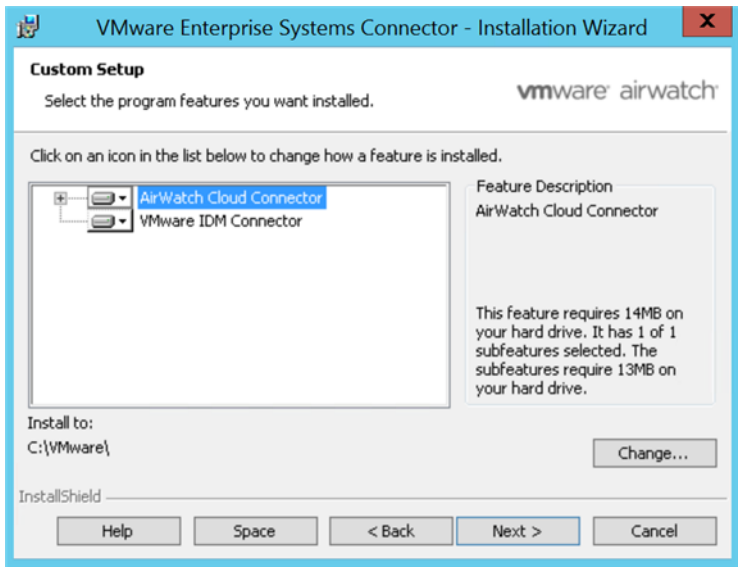
Avant d'installer le VMware Enterprise Systems Connector, passez en revue les informations sur la configuration requise, l'architecture et les modèles de déploiement.

Ce chapitre aborde les rubriques suivantes :

À propos de VMware Enterprise Systems Connector

Dans VMware AirWatch 9.1, AirWatch Cloud Connector (ACC) a été inclus en tant que composant dans un nouveau programme d'installation appelé le VMware Enterprise Systems Connector. Ce programme d'installation sert de package de connecteurs unifiés pour Workspace ONE, AirWatch et Identity. Il se compose de deux composants, ACC et le VMware Identity Manager Connector.

Pendant le processus d'installation, vous pouvez choisir les composants à installer.



Reportez-vous à la section « Déterminer les composants à installer », page 22 pour connaître les scénarios dans lesquels il est recommandé d'installer les deux composants.

Composant AirWatch Cloud Connector

AirWatch Cloud Connector (ACC) fournit aux organisations la possibilité d'intégrer AirWatch à leurs systèmes d'entreprise back-end.

L'ACC s'exécute sur le réseau interne, en servant de proxy qui transmet en toute sécurité les requêtes d'AirWatch aux composants d'infrastructure critiques de l'organisation. Cela permet aux organisations de tirer parti des avantages d'AirWatch Mobile Device Management (MDM), dans quelque configuration que ce soit, avec ceux de leurs LDAP, autorité de certification, messagerie électronique et autres systèmes internes existants. Reportez-vous également à la section Chapitre 2, « Présentation de l'architecture Enterprise Systems Connector », page 17.

L'ACC s'intègre aux composants internes suivants.

- Relais de messagerie (SMTP)
- Services d'annuaire (LDAP/AD)
- Gestion de messagerie Exchange 2010 (PowerShell)
- BlackBerry Enterprise Server (BES)
- Service Web Lotus Domino (HTTPS)
- Syslog (données du journal des événements)

Les composants suivants sont disponibles uniquement si vous avez acheté le composant complémentaire d'intégration de PKI, disponible séparément.

- Services de certificats Microsoft (PKI)
- Protocole d'inscription de certificats simples (SCEP PKI)
- Services de certificats tiers (sur site uniquement)

Composant VMware Identity Manager Connector

Le VMware Identity Manager Connector fournit l'intégration d'annuaire, l'authentification des utilisateurs et l'intégration à des ressources telles que Horizon View.

L'utilisation du composant VMware Identity Manager Connector fournit les fonctionnalités supplémentaires suivantes à votre déploiement.

- Les méthodes d'authentification VMware Identity Manager Connector, comme le mot de passe, RSA Adaptive Authentication, RSA SecurID et Radius
- Authentification Kerberos pour les utilisateurs internes
- Intégration avec les ressources suivantes :
  - Pools de postes de travail et d'applications Horizon View
  - Ressources publiées Citrix
  - VMware Horizon® Service cloud™ avec infrastructure hébergée et sur site

Démarrage

Remarque Concernant les déploiements sur site, avant de continuer avec ce guide, vous devez avoir lu et effectué les procédures indiquées dans le *Guide du service d'AirWatch Cloud Messaging (AWCM)*.

Si vous êtes un client local, assurez-vous qu'AWCM est correctement installé, qu'il est bien en cours d'exécution et qu'il communique sans erreurs avec AirWatch.

Configuration requise pour Enterprise Systems Connector

Pour déployer Enterprise Systems Connector, assurez-vous que votre système répond aux exigences nécessaires.

Configuration matérielle requise

Utilisez les exigences suivantes comme base pour la création de votre serveur Enterprise Systems Connector.

Si vous installez uniquement le composant ACC, utilisez les exigences suivantes.

Tableau 1-1. Exigences ACC

Nombre d'utilisateurs	Jusqu'à 10 000	De 10 000 à 50 000	De 50 000 à 100 000
Cœurs de CPU	2	2 serveurs à équilibrage de charge avec 2 cœurs de CPU	3 serveurs à équilibrage de charge avec 2 cœurs de CPU
RAM (Go) par serveur	4	4 chacun	8 chacun
Espace disque (Go)	50	50 chacun	50 chacun

Le composant VMware Identity Manager Connector a les exigences supplémentaires suivantes. Si vous installez les composants ACC et les composants VMware Identity Manager Connector, ajoutez ces exigences aux exigences ACC.

Tableau 1-2. Configuration requise pour VMware Identity Manager Connector

Nombre d'utilisateurs	Jusqu'à 1 000	De 1 000 à 10 000	De 10 000 à 25 000	De 25 000 à 50 000	De 50 000 à 100 000
CPU	2	2 serveurs à équilibrage de charge, chacun avec 4 CPU	2 serveurs à équilibrage de charge, chacun avec 4 CPU	2 serveurs à équilibrage de charge, chacun avec 8 CPU	2 serveurs à équilibrage de charge, chacun avec 8 CPU
RAM (Go) par serveur	6	8 chacun	16 chacun	32 chacun	64 chacun
Espace disque (Go)	100	100 chacun	100 chacun	150 chacun	200 chacun

Remarque

- Pour le composant ACC, l'équilibrage de charge du trafic est assuré automatiquement par le composant AWCM. Cela ne requiert pas d'équilibrage de charge distinct. Plusieurs instances ACC dans le même groupe d'organisation qui se connectent au même serveur AWCM pour haute disponibilité peuvent espérer recevoir le trafic (une configuration directe-directe). La manière dont le trafic est acheminé est déterminée par AWCM et dépend de la charge actuelle.
- Pour le composant VMware Identity Manager Connector, consultez « Configuration de la haute disponibilité pour le VMware Identity Manager Connector », page 51.
- Les cœurs de CPU doivent être chacun de 2,0 GHz ou plus. Un processeur Intel est requis.
- L'espace disque inclut obligatoirement : espace disque de 1 Go pour l'application Enterprise Systems Connector, système d'exploitation Windows et runtime .NET. L'espace disque supplémentaire est alloué pour la journalisation.

Configuration logicielle requise

Assurez-vous que votre serveur Enterprise Systems Connector respecte toutes les exigences de logiciel suivantes.

Liste de contrôle des états	Condition	Notes
	Windows Server 2008 R2 ou Windows Server 2012 ou Windows Server 2012 R2	Requis pour les deux composants
	Installer les PowerShell sur le serveur	Requis pour les deux composants **Remarque** (Composant AirWatch Cloud Connector) PowerShell version 3.0 et version ultérieure est requis si vous déployez le modèle direct PowerShell MEM pour la messagerie. Pour vérifier votre version, ouvrez PowerShell et exécutez la commande `$PSVersionTable`. **Remarque** (Composant VMware Identity Manager Connector) PowerShell version 4.0 est requis si vous effectuez l'installation sur Windows Server 2008 R2.
	Installez .NET Framework 4.6.2	Requis pour les deux composants **Remarque** (Composant AirWatch Cloud Connector) La fonctionnalité de mise à jour automatique AirWatch Cloud Connector ne fonctionnera pas correctement tant que votre serveur Enterprise Systems Connector n'est pas mis à jour à jour vers .NET Framework 4.6.2. La fonctionnalité de mise à jour automatique ne mettra pas automatiquement à jour .NET Framework. Installez .NET Framework 4.6.2 manuellement sur le serveur Enterprise Systems Connector avant d'effectuer une mise à niveau.

Conditions générales

Assurez-vous que votre serveur Enterprise Systems Connector est configuré avec les conditions générales suivantes pour garantir la réussite de l'installation.

Liste de contrôle des états	Condition	Notes
	Assurez-vous d'avoir accès à distance aux serveurs sur lequel est installé AirWatch.	VMware AirWatch recommande de configurer le Gestionnaire de connexion de postes de travail à distance pour la gestion de plusieurs serveurs. Vous pouvez télécharger le programme d'installation à partir de https://www.microsoft.com/en-us/download/details.aspx?id=44989. En général, les installations sont effectuées à distance via une réunion web ou un partage d'écran que fournit un consultant AirWatch. Certains clients fournissent également à AirWatch les informations d'identification VPN permettant d'accéder aussi directement à l'environnement.
	Installation de Notepad++ (recommandé)	VMware AirWatch vous recommande de configurer Notepad++.
	Comptes de services pour l'authentification aux systèmes backend	Valider la méthode de connectivité d'Active Directory à l'aide de l'outil LDP.exe (voir http://www.computerperformance.co.uk/ScriptsGuy/ldp.zip) LDAP, BES, PowerShell, etc.

Conditions requises pour le réseau

Pour configurer les ports répertoriés ci-dessous, l'ensemble du trafic est unidirectionnel (sortant) allant du composant source vers le composant de destination.

Un proxy sortant ou tout autre logiciel ou matériel de gestion de connexion ne doit pas se terminer ni rejeter la connexion sortante à partir du Enterprise Systems Connector. La connexion sortante requise pour une utilisation par Enterprise Systems Connector doit rester ouverte à tout moment.

Remarque Toutes les ressources, telles que les autorités de certification, que vous souhaitez atteindre avec ACC doivent être sur le même domaine.

Tableau 1-3. Conditions requises pour le port du composant AirWatch Cloud Connector (SaaS)

Liste de contrôle des états	Composant source	Composant de destination	Protocole	Port	Vérification
	Serveur Enterprise Systems Connector	AirWatch AWCM par exemple : (https://awcm274.awmdm. com)	HTTPS	443	En entrant le lien https://awcmXXX.awmdm.com/awcm/status, vérifiez et assurez-vous qu'il n'y a aucune erreur d'approbation de certificat. (Remplacez « XXX » avec le même nombre qui est utilisé dans l'URL de votre environnement, par exemple, 100 au lieu de cn100).
	Serveur Enterprise Systems Connector	AirWatch Console par exemple : (https://cn274.awmdm.com)	HTTP ou HTTPS	80 ou 443	En entrant le lien https://cnXXX.awmdm.com, vérifiez et assurez-vous qu'il n'y a aucune erreur d'approbation de certificat. (Remplacez « XXX » avec le même nombre qui est utilisé dans l'URL de votre environnement, par exemple, 100 au lieu de cn100). Si la mise à jour automatique est activée, ACC doit être capable d'interroger la Console AirWatch pour savoir s'il existe des mises à jour à l'aide du port 443.
	Serveur Enterprise Systems Connector	API AirWatch par exemple : (https://as274.awmdm.com)	HTTPS	443	En entrant le lien https://asXXX.awmdm.com/api/help, vérifiez et assurez-vous que vous êtes invité à entrer les informations d'identification. (Remplacez « XXX » avec le même nombre qui est utilisé dans l'URL de votre environnement, par exemple, 100 au lieu de cn100). L'accès ACC à API est requis pour le bon fonctionnement du service AirWatch Diagnostics.
	Serveur Enterprise Systems Connector	La liste de révocation des certificats : http://csc3-2010-crl.verisign.com/CSC3-2010.crl	HTTP	80	Pour que les différents services fonctionnent correctement
		Intégrations facultatives			
	Serveur Enterprise Systems Connector	SMTP interne	SMTP	25	
	Serveur Enterprise Systems Connector	LDAP interne	LDAP ou LDAPS	389, 636, 3268 ou 3269	

Tableau 1-3. Conditions requises pour le port du composant AirWatch Cloud Connector (SaaS) (suite)

Liste de contrôle des états	Composant source	Composant de destination	Protocole	Port	Vérification
	Serveur Enterprise Systems Connector	SCEP interne	HTTP ou HTTPS	80 ou 443	
	Serveur Enterprise Systems Connector	ADCS interne	DCOM	135, 1025-5000, 49152-65535	
	Serveur Enterprise Systems Connector	BES interne	HTTP ou HTTPS	80 ou 443	
	Serveur Enterprise Systems Connector	Interne Exchange 2010 ou version ultérieure	HTTP ou HTTPS	80 ou 443	

Tableau 1-4. Exigences pour le port du composant AirWatch Cloud Connector (sur site)

	Composant source	Composant de destination	Protocole	Port	Vérification
	Serveur Enterprise Systems Connector	Serveur de messagerie d'AirWatch Cloud	HTTPS	2001	Telnet à partir de Enterprise Systems Connector au serveur AWCM sur le port ou une fois installé. En entrant le lien **`https://<AWCM url="">:2001/awcm/état`**, vérifiez et assurez-vous qu'il n'y a aucune erreur d'approbation de certificat. Si la mise à jour automatique est activée, ACC doit être capable d'interroger la Console AirWatch pour savoir s'il existe des mises à jour à l'aide du port 443. Si vous utilisez ACC avec AWCM, que vous disposez de plusieurs serveurs AWCM et que vous souhaitez équilibrer leur charge, vous devez configurer la persistance. Pour plus d'informations sur la configuration des règles de persistance d'AWCM à l'aide de la touche F5, consultez l'article suivant de l'article de la base de connaissances : https://support.air-watch.com/articles/115001666028.
	Serveur Enterprise Systems Connector	Console AirWatch	HTTP ou HTTPS	80 ou 443	Telnet à partir de Enterprise Systems Connector vers la console sur le port ou une fois installé. En entrant le lien **`https://<URL de la console>`** , vérifiez et assurez-vous qu'il n'y a aucune erreur d'approbation de certificat. Si la mise à jour automatique est activée, ACC doit être capable d'interroger la Console AirWatch pour savoir s'il existe des mises à jour à l'aide du port 443.
	Serveur Enterprise Systems Connector	Serveur de l'API (ou là où est installé l'API)	HTTPS	443	Vérifiez en accédant à l'URL de votre serveur API. L'accès ACC à API est requis pour le bon fonctionnement du service AirWatch Diagnostics.
	Serveur Enterprise Systems Connector	La liste de révocation des certificats : http://csc3-2010-crl.verisign.com/CSC3-2010.crl	HTTP	80	Pour que les différents services fonctionnent correctement
			Intégrations facultatives		
	Serveur Enterprise Systems Connector	SMTP interne	SMTP	25	

Tableau 1-4. Exigences pour le port du composant AirWatch Cloud Connector (sur site) (suite)

	Composant source	Composant de destination	Protocole	Port	Vérification
	Serveur Enterprise Systems Connector	LDAP interne	LDAP ou LDAPS	389, 636, 3268 ou 3269	
	Serveur Enterprise Systems Connector	SCEP interne	HTTP ou HTTPS	80 ou 443	
	Serveur Enterprise Systems Connector	ADCS interne	DCOM	135, 1025-5000, 49152-65535	
	Serveur Enterprise Systems Connector	BES interne	HTTP ou HTTPS	80 ou 443	
	Serveur Enterprise Systems Connector	Interne Exchange 2010 ou version ultérieure	HTTP ou HTTPS	80 ou 443	

Tableau 1-5. Configurations requises pour le port du composant VMware Identity Manager Connector (SaaS ou sur site)

Liste de contrôle des états	Composant source	Composant de destination	Port	Protocole	Notes
	VMware Identity Manager Connector	Service VMware Identity Manager	443	HTTPS	Port par défaut. Ce port est configurable.
	Navigateurs	VMware Identity Manager Connector	8443	HTTPS	Port d'administration. Obligatoire
	Navigateurs	VMware Identity Manager Connector	80	HTTP	Obligatoire
	VMware Identity Manager Connector	Active Directory	389, 636, 3268, 3269		Ports par défaut. Ces ports sont configurables.
	VMware Identity Manager Connector	Serveur DNS	53	TCP/UDP	Chaque instance doit avoir accès au serveur DNS sur le port 53 et autoriser le trafic SSH entrant sur le port 22.
	VMware Identity Manager Connector	Contrôleur de domaine	88, 464, 135	TCP/UDP	
	VMware Identity Manager Connector	Système RSA SecurID	5500		Port par défaut. Ce port est configurable

Tableau 1-5. Configurations requises pour le port du composant VMware Identity Manager Connector (SaaS ou sur site) (suite)

Liste de contrôle des états	Composant source	Composant de destination	Port	Protocole	Notes
	VMware Identity Manager Connector	Serveur de connexion View	389, 443		Accès à des instances du serveur de connexion View pour des intégrations d'Horizon View
	VMware Identity Manager Connector	Integration Broker	80, 443		Accès à l'Integration Broker pour l'intégration à des ressources publiées Citrix. **Important** Si vous installez Integration Broker sur le même serveur Windows que le Enterprise Systems Connector, vous devez vous assurer que dans les liaisons de site de Site Web par défaut du serveur IIS, les ports de liaison HTTP et HTTPS ne sont pas en conflit avec les ports utilisés par le composant VMware Identity Manager Connector. Le VMware Identity Manager Connector utilise toujours le port 80. Il utilise également 443, sauf si un port différent est configuré pendant l'installation.

(Composant VMware Identity Manager Connector) Adresses IP VMware Identity Manager hébergées sur le Cloud

(Clients SaaS) Consultez l'article 2149884 de la base de connaissances pour obtenir la liste des adresses IP du service VMware Identity Manager auxquelles VMware Identity Manager Connector doit avoir accès.

(Composant VMware Identity Manager Connector) Conditions requises pour les enregistrements DNS et les adresses IP

Le connecteur doit disposer d'une entrée DNS et d'une adresse IP statique. Avant de commencer votre installation, demandez l'enregistrement DNS et les adresses IP pour utiliser et configurer les paramètres réseau du serveur Windows.

La configuration de la recherche inversée est facultative. Lorsque vous réalisez la recherche inversée, vous devez définir un enregistrement PTR sur le serveur DNS afin que le connecteur utilise la configuration réseau adéquate.

Vous pouvez utiliser la liste suivante d'exemples d'enregistrements DNS. Remplacez les informations de l'exemple par les informations de votre environnement. Cet exemple montre des enregistrements DNS et des adresses IP qui utilisent la résolution.

Tableau 1-6. Exemples d'enregistrements DNS et d'adresses IP qui utilisent la résolution

Nom de domaine	Type de ressource	Adresse IP
myidentitymanager.company.com	Aoû	10.28.128.3

Cet exemple montre des enregistrements DNS et des adresses IP qui utilisent la résolution inverse

Tableau 1-7. Exemples d'enregistrements DNS et d'adresses IP qui utilisent la résolution inverse

Adresse IP	Type de ressource	Nom d'hôte
10.28.128.3	PTR	myidentitymanager.company.com

Après avoir terminé la configuration DNS, vérifiez que la résolution DNS inverse est configurée correctement. Par exemple, la commande de dispositif virtuel `host IPaddress` doit être résolue en recherche de nom DNS.

Remarque Si vous disposez d'un équilibrage de charge avec une adresse IP virtuelle (VIP) devant les serveurs DNS, notez que VMware Identity Manager ne prend pas en charge l'utilisation d'une VIP. Vous pouvez spécifier plusieurs serveurs DNS séparés par une virgule.

Remarque Si vous utilisez un serveur DNS fonctionnant sur Unix ou sur Linux et que vous prévoyez de joindre le connecteur au domaine Active Directory, assurez-vous que les enregistrements de la ressource de service (SRV) appropriée sont créés pour chaque contrôleur de domaine Active Directory.

(Composant VMware Identity Manager Connector) Versions d'Active Directory prises en charge

VMware Identity Manager prend en charge Active Directory sous Windows Server 2008, Windows Server 2008 R2, Windows Server 2012 et Windows Server 2012 R2, avec un niveau fonctionnel Domaine et un niveau fonctionnel Forêt de Windows 2003 et versions ultérieures.

Un environnement Active Directory composé d'un seul domaine Active Directory, de plusieurs domaines dans une seule forêt Active Directory ou de plusieurs domaines dans plusieurs forêts Active Directory est pris en charge.

Présentation de l'architecture Enterprise Systems Connector 2

Enterprise Systems Connector contient deux services Windows qui peuvent être installés sur un serveur physique ou virtuel exécutant Windows 2008 R2, 2012 ou 2012 R2. Il fonctionne à partir de votre réseau interne et peut être configuré derrière des pare-feu web d'application existants ou des équilibreurs de charge.

En lançant une connexion sécurisée HTTPS de Enterprise Systems Connector à des services de messagerie intégrés dans AirWatch et VMware Identity Manager, Enterprise Systems Connector peut transmettre régulièrement les informations provenant de vos ressources internes comme AD, LDAP, etc. au produit sans modifications au niveau du pare-feu. Si vous prévoyez de vous servir d'un proxy pour un trafic via un proxy sortant, vous pouvez utiliser les paramètres dans la configuration du connecteur qui autorisent l'utilisation d'un proxy.

Configurations prises en charge

Utilisez Enterprise Systems Connector dans les configurations suivantes.

- Utilisation du transport HTTPS
- Prise en charge du trafic HTTP via un proxy sortant

Ce chapitre aborde les rubriques suivantes :

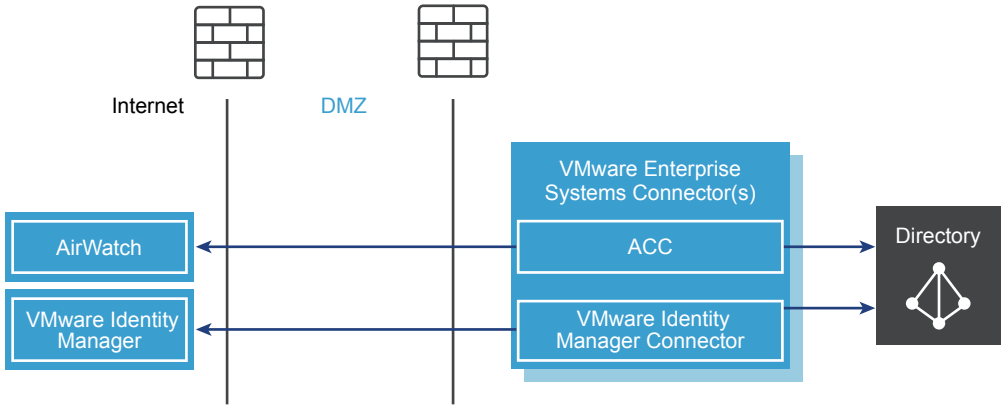
- « Modèle de déploiement SaaS Enterprise Systems Connector », page 17
- « Modèle de déploiement sur site Enterprise Systems Connector », page 18
- « Flux de travail d'intégration de certificat du composant ACC », page 20

Modèle de déploiement SaaS Enterprise Systems Connector

Dans un modèle de déploiement SaaS, le Enterprise Systems Connector se trouve dans votre réseau interne et s'intègre à vos systèmes internes, ce qui permet à AirWatch et à VMware Identity Manager de les exploiter pour diverses fonctions, comme les certificats et les services d'annuaire.

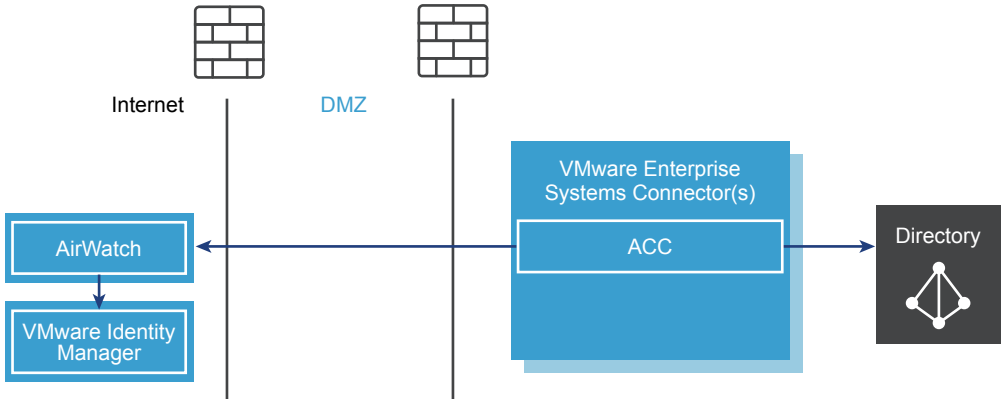
Le diagramme suivant présente le déploiement complet de l'Enterprise Systems Connector, avec, à la fois, ACC et des composants VMware Identity Manager Connector déployés.

Figure 2-1. Déploiement SaaS Enterprise Systems Connector



Le diagramme suivant présente le déploiement du composant ACC uniquement.

Figure 2-2. Déploiement SaaS Enterprise Systems Connector (ACC uniquement)

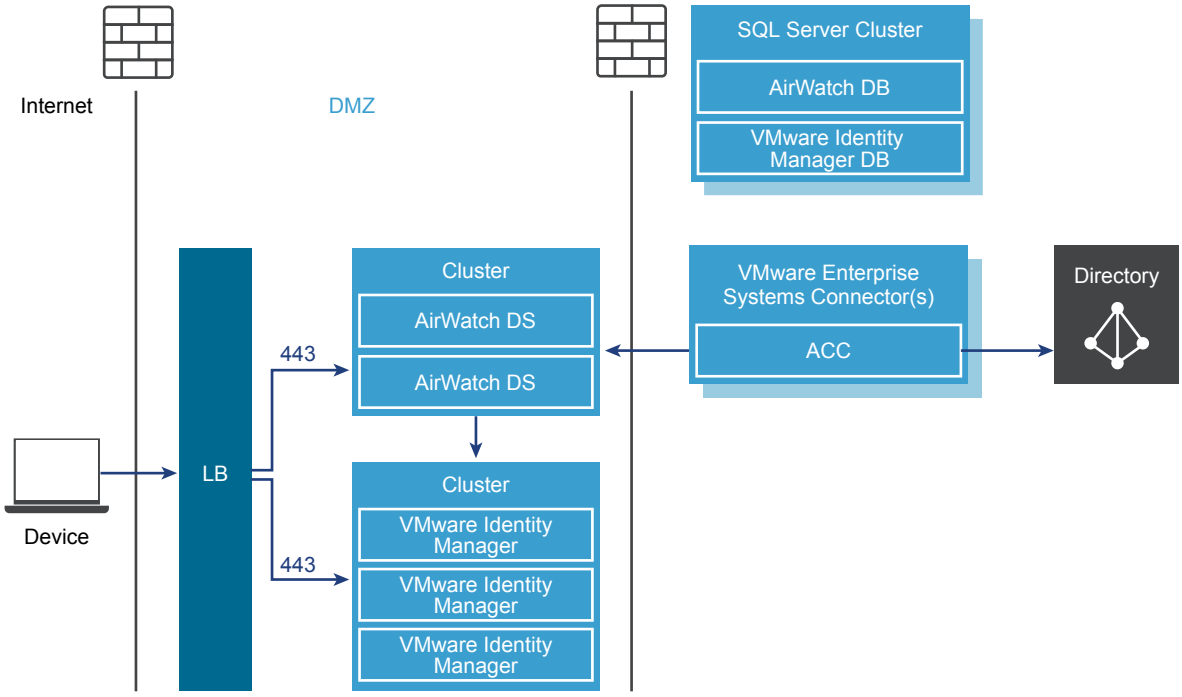


Modèle de déploiement sur site Enterprise Systems Connector

Dans un modèle de déploiement sur site, le Enterprise Systems Connector se trouve dans votre réseau interne et communique avec AWCM et le service VMware Identity Manager. AWCM est généralement installé sur le serveur de services de périphériques AirWatch.

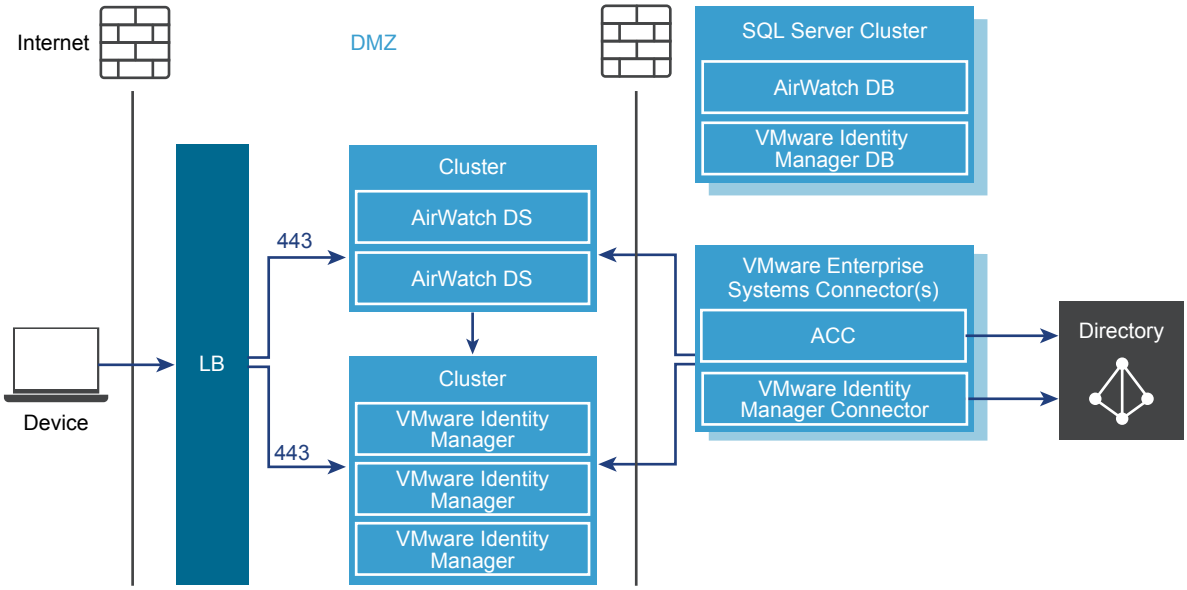
Le diagramme suivant présente le déploiement du composant ACC avec une disposition AirWatch classique sur site.

Figure 2-3. Déploiement sur site d' Enterprise Systems Connector (ACC uniquement)



Le diagramme suivant présente le déploiement sur site des composants ACC et VMware Identity Manager Connectoravec une disposition AirWatch classique.

Figure 2-4. Déploiement de site d' Enterprise Systems Connector (ACC et VMware Identity Manager Connector)



Flux de travail d'intégration de certificat du composant ACC

Les certificats sont utilisés pour authentifier la communication entre la Console AirWatch et AirWatch Cloud Connector (ACC).

Génération des certificats

- Vous activez l'ACC et générez ensuite des certificats pour AirWatch et ACC.
  - Les deux certificats sont uniques pour le groupe sélectionné dans la Console AirWatch et résident sur le serveur AirWatch.
  - Les deux certificats sont générés à partir d'une racine de confiance AirWatch.
- Installez ACC. Le certificat ACC que génère AirWatch est automatiquement groupé et installé avec ACC.

Acheminement des données dans des environnements sur site

- AirWatch envoie des demandes à AWCM. Les demandes sont chiffrées en SSL à l'aide de HTTPS.
- ACC interroge AWCM pour les demandes d'AirWatch. Les demandes sont chiffrées en SSL à l'aide de HTTPS.
- Toutes les données sont envoyées via AWCM.

La configuration ACC approuve seulement les messages signés à partir de l'environnement AirWatch. Cette approbation est unique pour chaque groupe.

Il est émis le même certificat unique ACC à tous les serveurs ACC supplémentaires définis dans le même groupe AirWatch dans le cadre d'une configuration haute disponibilité (HA). Pour plus d'informations sur la haute disponibilité, reportez-vous au Guide d'architecture recommandée VMware AirWatch, disponible sur les ressources d'AirWatch.

Sécurisation des données dans les environnements sur site

Le serveur AirWatch envoie chaque demande à l'AWCM sous forme de message crypté et signé.

- Les demandes sont chiffrées à l'aide de la clé publique unique de l'instance ACC. Seul ACC peut décrypter les demandes.
- Les demandes sont signées à l'aide de la clé privée de l'instance de serveur AirWatch qui est unique pour chaque groupe. Par conséquent, ACC approuve les demandes uniquement depuis le serveur configuré AirWatch.
- Les réponses d'ACC au serveur AirWatch sont chiffrées avec la même clé que la demande et signées avec la clé privée ACC

Processus d'installation du Enterprise Systems Connector 3

Vous devez effectuer plusieurs tâches pour configurer et installer le Enterprise Systems Connector dans votre réseau interne.

Procédure

1 « Déterminer les composants à installer », page 22 - Déterminez s'il faut installer uniquement le composant ACC, ou à la fois ACC et le VMware Identity Manager Connector.

2 « (Clients locaux uniquement) Installez le certificat de canal sécurisé sur AWCM », page 22 - Les clients locaux doivent installer un certificat de canal sécurisé pour établir la sécurité entre l'AWCM et les composants suivants : AirWatch Console, les services de périphérique, l'API et le Portail libre-service.

3 « Établir des Communications avec AWCM », page 23 - Les clients SaaS et sur site doivent établir des communications avec AWCM. Réaliser cette action vous permet de configurer une instance d'AirWatch pour utiliser un serveur AWCM particulier.

4 « Obtenir le programme d'installation VMware Enterprise Systems Connector », page 23 - Vous pouvez télécharger le programme d'installation du Enterprise Systems Connector à partir de la page Cloud Connector dans la console AirWatch comme décrit dans « Activer Enterprise Systems Connector depuis la Console AirWatch », page 24. Le programme d'installation est également disponible dans le cadre de l'assistant de démarrage de Workspace ONE.

5 « Activer Enterprise Systems Connector depuis la Console AirWatch », page 24 - Avant d'installer Enterprise Systems Connector, vous devez tout d'abord l'activer, générer des certificats et sélectionner les services d'entreprise et les services AirWatch à intégrer. Une fois cette étape terminée, vous pouvez installer Enterprise Systems Connector.

6 « Exécutez le programme d'installation Enterprise Systems Connector. », page 26 - Exécutez le programme d'installation Enterprise Systems Connector sur votre serveur configuré répondant à toutes les conditions préalables.

7 « Vérifier une Installation réussie Enterprise Systems Connector », page 32 - Une fois que vous avez installé Enterprise Systems Connector, vous pouvez vérifier la réussite de l'installation à partir de la console AirWatch.

Ce chapitre aborde les rubriques suivantes :

- « Vérifier une Installation réussie Enterprise Systems Connector », page 32

Déterminer les composants à installer

Avant de commencer le processus d'installation et en fonction des besoins de votre entreprise, décidez d'installer uniquement le composant ACC, ou d'installer ACC et VMware Identity Manager Connector.

Pour la plupart des clients Workspace ONE, il est recommandé d'installer les deux composants du Enterprise Systems Connector. En plus des fonctionnalités ACC, l'installation complète prend en charge les fonctionnalités suivantes.

- Applications et postes de travail virtuels dans Workspace ONE
- Authentification RSA Secure ID
- authentification Windows intégrée
- Active Directory multiple, approuvé ou non-approuvé avec VMware Identity Manager
- VMware Identity Manager avec plusieurs configurations de groupe d'organisation de l'annuaire dans AirWatch
- Plate-forme pour les fonctionnalités d'intégration centrées sur l'identité

Si vous avez déjà déployé Workspace ONE avec ACC uniquement, ce modèle continue à être pris en charge, mais si vous prévoyez de tirer parti d'une de ces fonctionnalités, il est recommandé d'installer le connecteur de systèmes d'entreprise complet. Migration depuis ACC uniquement vers les VMware Identity Manager Connector disponibles dans le Enterprise Systems Connector est pris en charge. Voir Chapitre 6, « Migration d'un annuaire depuis ACC vers VMware Identity Manager Connector », page 61.

(Clients locaux uniquement) Installez le certificat de canal sécurisé sur AWCM

Les clients locaux doivent installer un certificat de canal sécurisé pour établir la sécurité entre l'AWCM et les composants suivants : AirWatch Console, les Services de périphérique, l'API et le Portail en libre-service.

Important Effectuez les étapes suivantes sur le serveur AWCM en cours d'exécution. Ne téléchargez pas le programme d'installation sur un autre ordinateur et copiez-le sur le serveur AWCM. Si le téléchargement échoue sur le serveur AWCM en cours d'exécution, contactez alors le Support de AirWatch pour des solutions potentielles.

Remarque Si vous apportez des modifications vers le certificat du canal sécurisé dans le magasin de clés AWCM après avoir téléchargé et installé AirWatch Tunnel ou Enterprise Systems Connector, vous devrez désinstaller, supprimez tous les dossiers, le télécharger et le réinstaller à nouveau.

Procédure

1. Accédez à **Groupes & paramètres > Tous les paramètres > Système > Avancés > Secure Channel certificat**.
2. Sélectionnez **Télécharger le programme d'installation AWCM Secure Channel** dans la section Messagerie d'AirWatch Cloud pour commencer l'installation du script d'installation de certificat de canal sécurisé.

   Le programme d'installation du canal sécurisé pour Linux est utilisé uniquement pour le Service de notification de Cloud. AWCM est uniquement pris en charge sur les serveurs Windows.
3. Copiez le script d'installation **Certificat de canal sécurisé** sur votre serveur AWCM local et faites un clic droit vers **Exécuter en tant qu'administrateur** pour exécuter et installer.

4 Entrez ou sélectionnez **Parcourir** pour trouver le chemin du magasin d'approbations et sélectionnez **OK**.

5 Sélectionnez **OK** lorsqu'une boîte de dialogue de Message vous informe que le certificat a été ajouté au magasin de clés.

6 Continuer avec les étapes pour Établir des communications avec AWCM.

7 Continuer avec les étapes d'installation pour Enterprise Systems Connector.

Établir des Communications avec AWCM

Les clients SaaS et sur site doivent établir des communications avec AWCM. Réaliser cette action vous permet de configurer une instance d'AirWatch pour utiliser un serveur AWCM particulier.

Procédure

1 Accédez aux Paramètres & groupes > Tous les paramètres > Système > Avancé > URL du Site pour afficher la section de messagerie AirWatch Cloud.

Remarque Si vous êtes un client SaaS et que vous ne voyez pas cette page dans les paramètres du système, ces paramètres ont déjà été configurés pour vous.

2 Configurez les paramètres suivants :

Paramètre	Description
Activer le serveur AirWatch	Cochez cette case pour autoriser la connexion entre la AirWatch Console et le serveur AWCM.
URL externe du serveur AirWatch	Ce champ vous permet d'entrer le nom du serveur utilisé par les composants externes et les périphériques (par ex., ACC) pour communiquer en toute sécurité (à l'aide de HTTPS) avec AWCM. Voici un exemple d'une URL ACC : Acme.com. N'ajoutez pas https:// car l'application le suppose et c'est ajouté automatiquement.
Port externe de AirWatch	C'est le port utilisé par le nom du serveur ci-dessus pour communiquer avec AWCM. Pour les communications externes sécurisées, utilisez le port 443. Si vous déchargez SSL par contournement, puis souhaitez utiliser un port interne de communication non sécurisé, qui est par défaut 2001 mais peut être modifié à d'autres numéros de port.
URL interne du serveur AWCM	Cette URL vous permet d'atteindre AWCM à partir de composants internes et de périphériques (par ex., Console d'administration, les Services de périphérique, etc.). Exemples d'URL AirWatch : https://Acme.com:2001/awcm ou http://AcmeInternal.Local/awcm. Si votre serveur AWCM et la AirWatch Console sont internes (sur le même réseau), et que vous souhaitez décharger SSL par contournement, une connexion sécurisée n'est pas nécessaire, vous pouvez alors utiliser http au lieu de https. Par exemple, http://AcmeInternal.Local:2001/awcm. Cet exemple montre que le serveur réside sur le réseau interne et communique sur le port 2001.

Obtenir le programme d'installation VMware Enterprise Systems Connector

Le programme d'installation VMware Enterprise Systems Connector est disponible à partir de plusieurs emplacements.

Le programme d'installation est disponible dans les Paramètres & groupes > Tous les paramètres > Système > Intégration d'entreprise > Page Cloud Connector dans la console AirWatch, comme décrit dans « Activer Enterprise Systems Connector depuis la Console AirWatch », page 24. Il est également disponible dans le cadre de l'assistant de démarrage Workspace ONE. Pour utiliser l'assistant de démarrage Workspace ONE, consultez le *Guide de Configuration rapide de VMware Workspace ONE*.

Activer Enterprise Systems Connector depuis la Console AirWatch

Avant d'installer Enterprise Systems Connector, vous devez tout d'abord l'activer, générer des certificats et sélectionnez les services d'entreprise et les services AirWatch à intégrer. Une fois cette étape terminée, vous pouvez installer Enterprise Systems Connector.

Remarque Effectuez les étapes suivantes sur le serveur qui exécutera Enterprise Systems Connector. Ne téléchargez pas le programme d'installation sur un autre ordinateur et copiez-le sur le serveur Enterprise Systems Connector .

Procédure

1 Accédez à **Paramètres & groupes > Tous les paramètres > Système > Intégration d'entreprise > Cloud Connector**.

2 Configurez les paramètres suivants sur l'onglet **Général**.

Paramètre	Description
Activer le connecteur de Cloud	Cochez cette case pour activer Enterprise Systems Connector et afficher l'onglet Général.
Activer la mise à jour automatique	Sélectionnez cette option pour activer Enterprise Systems Connector pour une mise à jour automatique lorsqu'une version plus récente est disponible. Pour plus d'informations concernant la mise à jour automatique, reportez-vous à l'option de mise à jour automatique de VMware Enterprise systèmes Connector.

3 Configurer les paramètres suivants dans l'onglet **Avancé**.

Paramètre	Description
Générer des certificats	Sélectionnez ce bouton pour générer un certificat pour le serveur Enterprise Systems Connector et le serveur AirWatch. Les certificats sont générés pour les deux et affichés sous certificats VMware Enterprise Systems Connector et les certificats AirWatch. Une fois que les certificats sont générés, le bouton change pour **Régénérer des certificats**. Pour plus d'informations sur la mise à jour des certificats, reportez-vous à la section « Régénérer des certificats », page 37.
Communication avec AWCM	Sélectionnez la manière dont le Enterprise Systems Connector communique avec AWCM sous la Communication avec AWCM. ■ **Utiliser les URL AWCM externe** – il s'agit de l'option par défaut qui s'appliquera à la plupart des déploiements. ■ **Utilisation interne AWCM URL** – Utilisez cette option si vos paramètres de sécurité restreignent votre serveur Enterprise Systems Connector de résoudre l'URL externe du AWCM. Par exemple, si Enterprise Systems Connector se trouve sur votre réseau interne et votre serveur AWCM se trouve dans une zone DMZ. Sélectionnez les boutons **Activé** ou **Désactivé** pour activer ou désactiver les Services d'entreprise. Les services que vous sélectionnez (activés) s'intégreront avec Enterprise Systems Connector. ■ SMTP (relais E-mail) AirWatch SaaS offre la livraison de messagerie via son propre SMTP, mais vous pouvez activer Enterprise Systems Connector pour utiliser un autre serveur SMTP ici. Entrez les paramètres des serveurs SMTP pour la messagerie dans **Groupes & paramètres > Tous les paramètres > Système > Intégration d'entreprise > E-mail (SMTP)**. ■ Services d'annuaire (LDAP/AD) ■ Échange PowerShell (pour certaines passerelles de messagerie sécurisée) ■ BES (BlackBerry utilisateur de synchronisation et informations sur les périphériques mobiles) ■ Syslog (Client/protocole de serveur utilisé pour intégrer les données du journal des événements AirWatch)

Paramètre	Description
Services d'entreprise	Les composants suivants sont disponibles uniquement si vous avez acheté le composant complémentaire d'intégration de PKI, disponible séparément. ■ Services de certificats Microsoft (PKI) ■ Protocole d'inscription de certificats simples (SCEP PKI) ■ OpenTrust CMS Mobile (services certificat tiers) ■ Confier PKI (services certificat tiers) ■ Symantec MPKI (services certificat tiers) Car il n'est pas nécessaire de recourir à Enterprise Systems Connector pour les services de certificats du Cloud, si vous souhaitez intégrer à des services de certificats (comme Symantec MPKI) en sélectionnant l'une des cases à cocher dans l'écran ci-dessous, le service que vous sélectionnez doit être sur site, pas dans le cloud (SaaS).
Services AirWatch	Sélectionnez **Activé** ou **Désactivé** pour activer ou désactiver les Services AirWatch. Les composants AirWatch que vous sélectionnez (activés) seront intégrés avec Enterprise Systems Connector. AirWatch vous recommande de laisser tous les services activés. ■ Services de périphérique (Console d'administration et tous les services qui lui sont demandés pour fonctionner, y compris les services Windows associés) ■ Gestion des périphériques (inscription, catalogue d'applications et services Windows associés) ■ Portail en libre-service automatique (y compris les services Windows associés) ■ Tous les autres composants (y compris les services Windows associés) **Remarque** (Les clients locaux) Si vous n'avez pas déjà effectué *Activer AWCM pour communiquer avec le connecteur de systèmes d'entreprise VMware*, vous pouvez sélectionner **Télécharger le programme d'installation AWCM Secure Channel** pour être redirigé vers la page de téléchargement. **Remarque** (Clients SaaS) Vous n'avez pas besoin de télécharger le programme d'installation du certificat de canal sécurisé.

4 Sélectionnez **Enregistrer** pour maintenir tous ces paramètres.

5 Accédez à l'onglet Général et sélectionnez **Télécharger un programme d'installation de connecteur de Cloud**.

Une page de téléchargement du programme d'installation connecteur Cloud s'affiche.

6 Entrez un mot de passe pour le certificat Enterprise Systems Connector dans les champs. Le mot de passe sera nécessaire ultérieurement lorsque vous exécutez le programme d'installation Enterprise Systems Connector et que vous avez besoin d'entrer le mot de passe du certificat.

7 Sélectionnez **Télécharger** et enregistrer le fichier .exe sur le serveur Enterprise Systems Connector pour une utilisation ultérieure.

Exécutez le programme d'installation Enterprise Systems Connector .

Exécutez le programme d'installation Enterprise Systems Connector sur un serveur Windows qui répond à toutes les exigences.

Le programme d'installation inclut les composants AirWatch Cloud Connector et VMware Identity Manager Connector. Vous pouvez installer un seul composant ou les deux. Après l'installation initiale, vous pouvez à nouveau exécuter le programme d'installation pour modifier des fonctionnalités ou mettre à jour votre installation.

Prérequis

Les conditions préalables suivantes s'appliquent au composant AirWatch Cloud Connector (ACC).

- Avant de commencer, les clients sur site doivent garantir que le serveur sur lequel Enterprise Systems Connector est installé peut atteindre AWCM en accédant à `https://{url}:port/awcm/status`où {url} correspond à l'URL de l'environnement AirWatch et où *port* correspond au port externe que vous avez configuré afin qu'AWCM puisse communiquer. L'état d'AWCM ne doit montrer aucune erreur SSL. S'il existe des erreurs, résolvez-les avant de poursuivre, sinon l'ACC ne fonctionnera pas correctement.
- Les clients SaaS doivent s'assurer que le serveur sur lequel vous installez Enterprise Systems Connector peut atteindre AWCM en accédant à https://awcm*XXX*.awmdm.com/awcm/status. Remplacez *XXX* par le même chiffre que celui utilisé dans votre URL d'environnement, par exemple, « 100 » à la place de cn100. L'état d'AWCM ne doit montrer aucune erreur SSL. S'il existe des erreurs, résolvez-les avant de continuer, sinon l'ACC ne fonctionnera pas correctement.

Les conditions préalables suivantes s'appliquent au composant VMware Identity Manager Connector .

- Les ports 80 et 8443 doivent être disponibles sur le serveur Windows. Si ces ports sont utilisés par d'autres services, vous ne pourrez pas installer le composant VMware Identity Manager Connector .
- Le serveur Windows doit être joint au domaine, et vous devez installer le composant VMware Identity Manager Connector en tant qu'utilisateur de domaine faisant partie du groupe d'administrateurs sur le serveur Windows, dans les cas suivants.
  - Si vous prévoyez de vous connecter à Active Directory (authentification Windows intégrée)
  - Si vous prévoyez d'utiliser l'authentification Kerberos
  - Si vous prévoyez d'intégrer Horizon View à VMware Identity Manager et que vous souhaitez utiliser les options Effectuer la synchronisation de l'annuaire ou Configuration du serveur de connexion 5.x.

  Dans ces cas-là, vous devez également choisir d'exécuter le service de connecteur IDM en tant qu'utilisateur de domaine pendant l'installation.
- Pour que le programme d'installation puisse parcourir et valider des domaines et des utilisateurs lors de l'installation, les exigences suivantes doivent être satisfaites.
  - Le système cible doit être joint au domaine.
  - Le service Navigateur de l'ordinateur doit être activé et en cours d'exécution.
  - Le pare-feu doit être configuré sauf pour le service Navigateur de l'ordinateur.
  - NetBIOS sur TCP/IP doit être activé sur le système cible.
  - Un système de navigateur principal doit être configuré sur le réseau.
  - Le trafic de diffusion doit être activé sur le réseau.

Procédure

1 Double-cliquez sur le programme d'installation.

2 Sur l'écran d'accueil, cliquez sur **Suivant**.

Le programme d'installation vérifie les conditions préalables sur le serveur. Si .NET Framework n'est pas installé, vous serez invité à installer ce logiciel et à redémarrer le serveur. Après le redémarrage, exécutez le programme d'installation Enterprise Systems Connector à nouveau pour reprendre le processus d'installation.

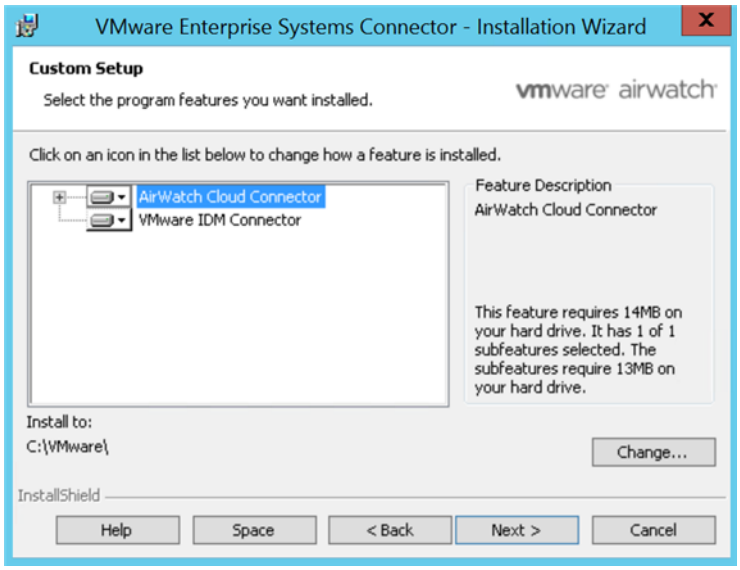
Si une version antérieure d'ACC est installée, le programme d'installation la détecte automatiquement et offre la possibilité de la mettre à jour vers la version la plus récente. Pour plus d'informations sur la mise à jour ACC, reportez-vous à la section Mises à jour ACC.

3 Acceptez le contrat de licence, puis cliquez sur **Suivant**.

4 Sur la page Installation personnalisée, sélectionnez les composants à installer.

Par défaut, AirWatch Cloud Connector et VMware Identity Manager Connector sont sélectionnés. Pour désélectionner un composant, cliquez sur la flèche de développement, puis sélectionnez **Cette fonction ne sera pas disponible**.

Pour plus d'informations sur les composants, reportez-vous à « Déterminer les composants à installer », page 22.

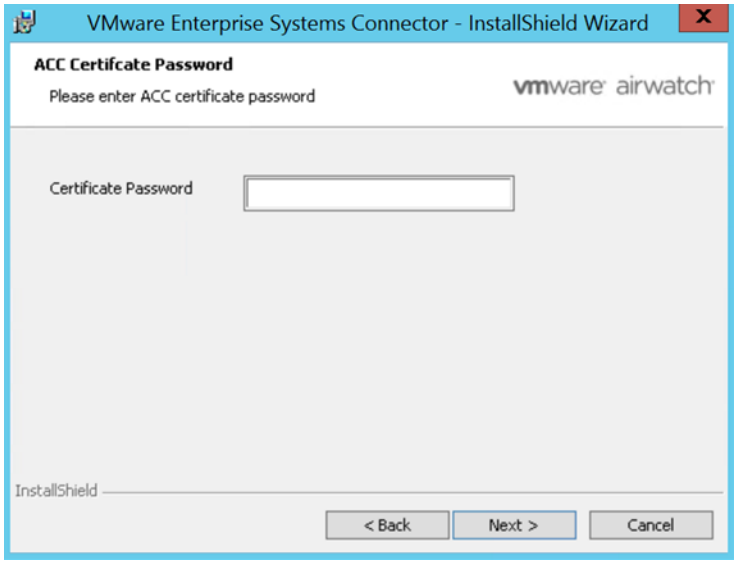


5 Sélectionnez **Modifier...** pour modifier le répertoire d'installation si nécessaire, puis cliquez sur **Suivant**.

Le composant VMware Identity Manager Connector exige Java Runtime Environment (JRE™). Si JRE n'est pas installé sur le serveur Windows, ou si la version installée est inférieure à celle fournie avec le programme d'installation, vous êtes invité à installer ce logiciel. Notez que les versions existantes de JRE ne sont pas supprimées lorsque la version requise est installée.

6 Vérifiez le dossier de destination, puis cliquez sur **Suivant**.

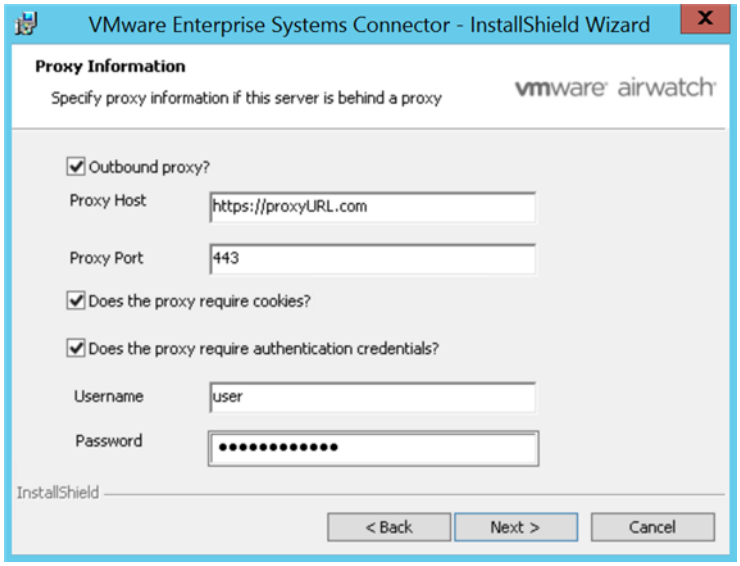
7 Entrez le mot de passe de certificat ACC que vous avez fourni sur la page Paramètres système dans AirWatch, puis cliquez sur **Suivant**.



8 Si vous prévoyez de vous servir d'un proxy pour le trafic ACC via un proxy sortant, cochez la case et fournissez les informations sur le serveur proxy.

Si nécessaire, entrez le nom d'utilisateur et le mot de passe.

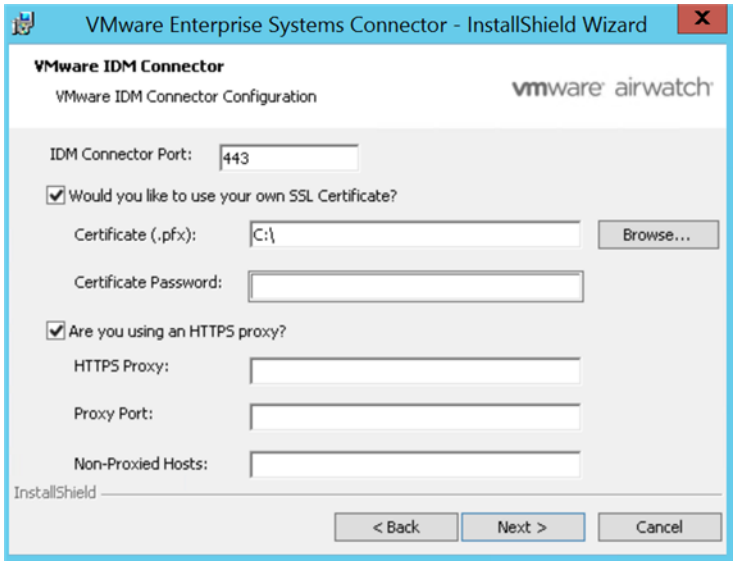
Remarque Les paramètres indiqués sur cette page s'appliquent uniquement à ACC. Les informations du serveur proxy pour le VMware Identity Manager Connector sont entrées séparément par la suite.



9 Cliquez sur **Suivant**.

10 (VMware Identity Manager Connector uniquement) Sur la page Configuration du connecteur IDM, entrez les informations suivantes, puis cliquez sur **Suivant**.

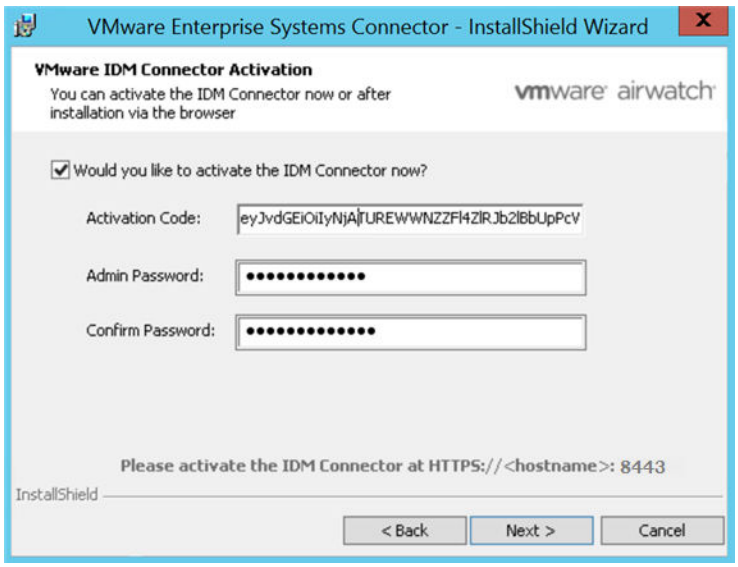
Option	Description
Port du connecteur IDM	Entrez un numéro de port si vous voulez que le VMware Identity Manager Connector s'exécute sur un port autre que 443.
Voulez-vous utiliser votre propre certificat SSL ?	Par défaut, un certificat auto-signé est généré pour le VMware Identity Manager Connector pendant le processus d'installation. Vous pouvez installer ultérieurement un certificat signé en vous connectant aux pages d'administrateur du connecteur sur la page https://*vidmConnectorHostname*:8443/cfg/login et en accédant à la page Installer un certificat. Si vous disposez déjà d'un certificat et que vous souhaitez l'installer maintenant, cochez la case, puis sélectionnez le certificat et entrez le mot de passe du certificat. Le certificat doit être au format PFX.
Vous utilisez un proxy HTTPS ?	Sélectionnez cette option pour configurer un serveur proxy HTTPS pour les communications sortantes, si nécessaire. **Proxy HTTPS** : l'URL du serveur proxy. Les serveurs proxy qui requièrent l'authentification ne sont pas pris en charge. **Port proxy** : port du serveur proxy HTTPS. **Hôtes non-proxy** : hôtes accessibles par le VMware Identity Manager Connector sans passer par le serveur proxy. Par exemple, localhost ou les hôtes sur le même sous-réseau.



11 (VMware Identity Manager Connector uniquement) Sur la page Activation du connecteur VMware IDM, cochez la case si vous souhaitez activer le connecteur maintenant.

Option	Description
Code d'activation	Si VMware Identity Manager est configuré dans le groupe d'organisation AirWatch à partir duquel vous avez téléchargé le programme d'installation, ce champ est prérempli avec le code d'activation. Si le champ n'est pas déjà pré-renseigné, générez un code d'activation dans la console d'administration de VMware Identity Manager, puis copiez/collez-le ici. Voir « Générer un code d'activation pour un connecteur VMware Identity Manager Connector », page 41 pour plus d'informations.
Mot de passe de l'administrateur	Créez un mot de passe pour les pages d'administrateur du connecteur. Vous pouvez accéder à ces pages pour recueillir des bundles de fichiers journaux et télécharger des certificats.
Confirmer le mot de passe	Entrez à nouveau le mot de passe.

Si vous n'activez pas le VMware Identity Manager Connector maintenant, vous pouvez l'activer ultérieurement à partir de https://*vidmConnectorHostname*: 8443. Par exemple, https://myconnector.example.com:8443.

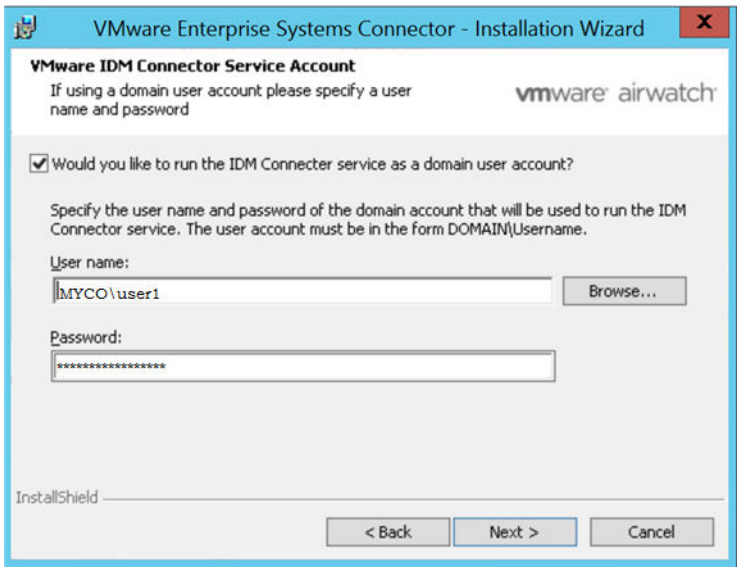


12 Cliquez sur **Suivant**.

13 (VMware Identity Manager Connector uniquement) Sur la page du compte de service du connecteur IDM, cochez la case si vous voulez exécuter le service du connecteur IDM en tant qu'utilisateur de domaine Windows.

Vous devez exécuter le service en tant qu'utilisateur de domaine dans les cas suivants.

- Si vous prévoyez de vous connecter à Active Directory (authentification Windows intégrée)
- Si vous prévoyez d'utiliser l'authentification Kerberos
- Si vous prévoyez d'intégrer Horizon View à VMware Identity Manager et que vous souhaitez utiliser les options Effectuer la synchronisation de l'annuaire ou Configuration du serveur de connexion 5.x



Remarque Pour effectuer des sélections sur cette page, vous devez exécuter le programme d'installation en tant qu'utilisateur de domaine faisant partie du groupe d'administrateurs sur le serveur Windows.

Remarque Si vous ne parvenez pas à localiser les domaines ou les utilisateurs lorsque vous cliquez sur **Parcourir**, vérifiez que vous respectez les conditions préalables.

14 Cliquez sur **Suivant**.

15 Cliquez sur **Installer** pour commencer l'installation.

Le programme d'installation affiche une case à cocher pour les mises à jour automatiques d'ACC. Pour plus d'informations sur la mise à jour automatique, reportez-vous à l' Option de mise à jour automatique ACC.

16 Cliquez sur **Terminer**.

Vérifier une Installation réussie Enterprise Systems Connector

Après avoir installé le Enterprise Systems Connector, vous pouvez vérifier la réussite de l'installation à partir de la console AirWatch.

Remarque L'option Tester la connexion s'applique uniquement au composant ACC de la Enterprise Systems Connector. Elle ne s'applique pas au composant VMware Identity Manager Connector.

Procédure

1 Accédez à **Paramètres & groupes > Tous les paramètres > Système > Intégration d'entreprise > Cloud Connector**.

2 Sélectionnez **Tester la connexion** en bas de l'écran et le message suivant s'affiche.

3 S'il y a migration, déterminer quelles fonctionnalités sont nouvelles et testez la nouvelle fonctionnalité pour vérifier que la migration a réussi.

Suivant

Maintenant que vous avez correctement installé le Enterprise Systems Connector, vous pouvez l'utiliser pour l'intégrer à votre infrastructure de service d'annuaire.

Gestion ACC 4

Cette section contient des informations sur la mise à jour du composant ACC et la régénération de certificats.

Ce chapitre aborde les rubriques suivantes :

Mises à jour ACC

Mettez à niveau AirWatch Cloud Connector (ACC) depuis la console AirWatch pour tirer parti des derniers correctifs de bogues et des dernières améliorations. Ce processus peut être automatisé à l'aide de l'option de mise à jour automatique ACC ou être effectué manuellement pour les situations où le contrôle d'administration est une priorité.

Remarque Pour plus d'informations sur la mise à niveau du composant VMware Identity Manager Connector reportez-vous à « Mise à niveau de VMware Identity Manager Connector », page 60.

Mise à jour automatique d'ACC

Lorsque vous installez ACC, la case de mise à jour automatique est sélectionnée par défaut. La mise à jour automatique permet la mise à niveau automatique d'ACC vers la version la plus récente sans intervention de l'utilisateur en interrogeant AirWatch pour les nouvelles versions d'ACC. AirWatch recommande que vous autorisiez des mises à jour automatiques (ne désactivez pas la case à cocher), mais AirWatch a rendu cela facultatif pour les environnements et situations dans lesquels les mises à niveau manuelles sont préférables.

Remarque L'option de mise à jour automatique s'applique uniquement au composant ACC du Enterprise Systems Connector. Elle ne s'applique pas au composant VMware Identity Manager Connector.

Avantages de la mise à jour automatique

- Il n'est pas nécessaire de le déterminer manuellement si vous devez effectuer la mise à niveau et que vous devez ensuite rechercher la dernière version ACC : le logiciel le fait pour vous.
- Vous disposez toujours des dernières fonctionnalités, améliorations et corrections.
- Plus important encore, vous disposez de la sécurité la plus récente.

Processus de mise à jour

La mise à jour automatique d'ACC est effectuée à l'aide des dossiers Banque1 et Banque2 à l'intérieur du dossier Cloud Connector. AirWatch détecte lequel de ces dossiers est vide et diffuse les fichiers ACC appropriés en continu, en plus de vider le contenu de l'autre dossier. Pour la mise à jour ultérieure, AirWatch réitère le processus à l'exception de l'autre dossier. Ce processus se répète chaque fois qu'une nouvelle version est mise à jour automatiquement. Ce processus est illustré dans la figure Flux de processus de mise à jour.

Important Ne supprimez pas les dossiers Banque1 ou Banque2. Les dossiers Banque1 et Banque2 sont essentiels pour le processus de mise à jour automatique ACC.

Figure 4-1. Flux de processus de mise à jour

Sécurité de la mise à jour automatique

Les mises à jour automatiques d'ACC sont exécutées en toute sécurité. Chaque mise à jour est signée par la AirWatch Console et vérifiée par ACC, afin qu'il se mette à jour seulement avec une mise à niveau de confiance. Le processus de mise à niveau est également transparent pour l'administrateur AirWatch. Lorsqu'une version plus récente est disponible, ACC le sait en interrogeant la AirWatch Console sur le port 443, puis une mise à niveau a lieu ensuite.

ACC étant indisponible pendant sa mise à niveau vers la dernière version, il se produit une courte perte de service (c'est-à-dire environ 1 minute). Lorsque plusieurs serveurs ACC sont installés, pour garantir que tous les services ACC ne sont pas en panne en même temps, AirWatch incorpore un minuteur aléatoire au processus de mise à niveau afin que les pannes ACC aient lieu à des moments différents sur de courtes périodes.

Si ACC effectue une mise à jour automatique, la version sous Ajouter ou Supprimer des programmes ne change pas : la version d'origine est toujours répertoriée. La version sous Ajouter ou Supprimer des programmes change uniquement lorsque vous exécutez le programme d'installation complet d'ACC. La meilleure manière de vérifier si la mise à jour automatique a abouti consiste à rechercher quelle version est en cours d'exécution dans les journaux ACC.

Effets de la désactivation de mise à jour automatique

Si vous choisissez de désactiver cette fonctionnalité alors qu'ACC n'est pas mis à niveau, ACC reste opérationnel jusqu'à ce que l'une des actions suivantes se produise.

- ACC est éteint, puis rallumé (intentionnellement ou à cause d'une panne de courant).
- ACC doit être réinstallé.
- AirWatch Console est mis à niveau vers une version ultérieure.
- Les certificats AirWatch, AWCM ou ACC sont régénérés. Lorsque les certificats sont régénérés, la dernière version d'ACC doit être installée et redémarrée pour reconnaître les nouveaux certificats.

Effectuez une mise à jour manuelle ACC

AirWatch recommande de ne pas effectuer une mise à jour manuelle ACC, mais cette méthode est disponible en option si celle-ci répond mieux aux besoins de votre environnement. Pour plus d'informations sur l'autre solution, reportez-vous à la section des mises à jour automatiques ACC.

Procédure

1 Assurez-vous que la mise à jour automatique est désactivée dans la AirWatch Console. Cette action enregistrera les derniers fichiers .zip ACC sur votre serveur ACC lorsque la console est mise à niveau et créera des entrées dans votre fichier de journal ACC vous informant que ACC doit être mis à niveau.

2 Arrêtez le service AirWatch Cloud Connector.

3 Exécutez l'une des tâches suivantes.

   a La première approche consiste à décompresser manuellement les fichiers .zip ACC dans le dossier de banque mentionné dans le fichier journal. Soit vous écrasez les fichiers existants dans ce dossier, soit vous supprimez tous les fichiers. Lors du redémarrage du service Cloud Connector, la version ACC obtiendra des mises à jour.

   b La deuxième approche consiste à utiliser un des dossiers de la banque. Dans ce cas, laissez soit le fichier .config ou. config.old disponible dans l'autre dossier de banque pour que le fichier .config stock puisse être réparé vers des valeurs personnalisées. Décompressez les fichiers, puis redémarrez le service Cloud Connector, qui fonctionnera avec la version récemment mis à niveau.

Régénérer des certificats

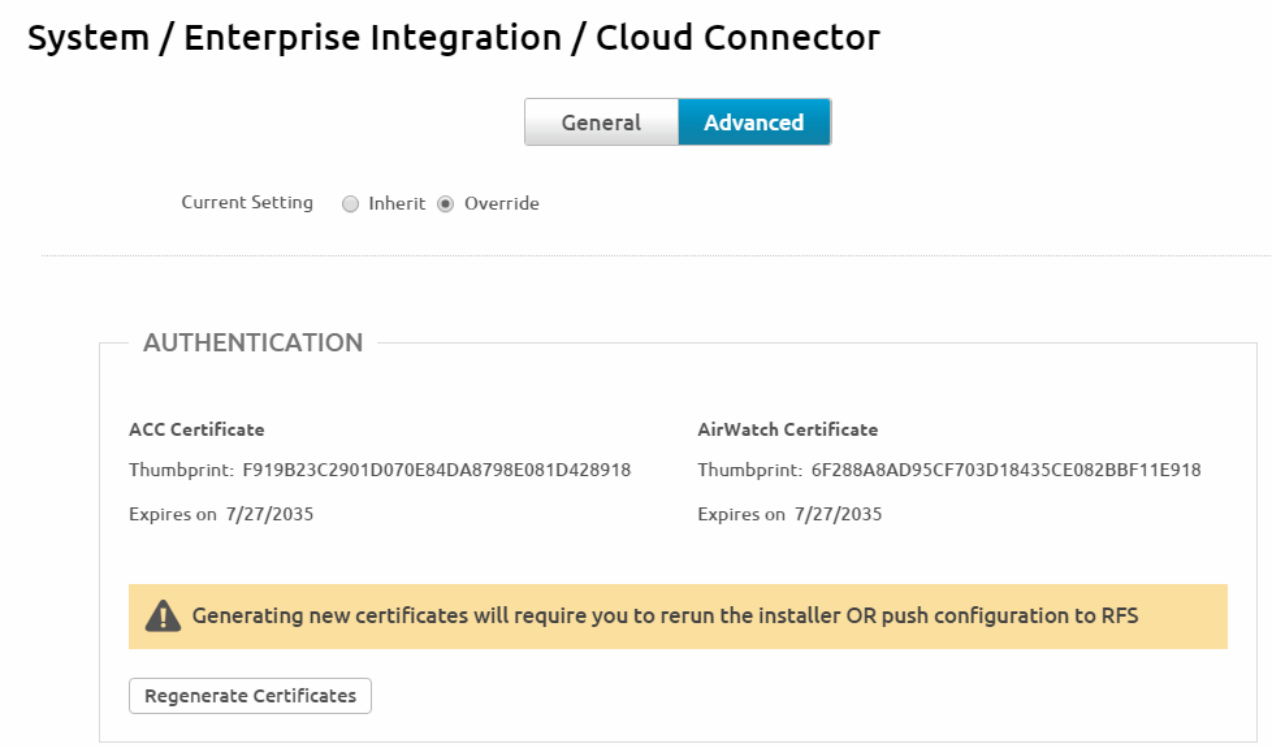
Vous estimerez nécessaire de régénérer les certificats utilisés pour les serveurs AirWatch et AirWatch Cloud Connector (ACC), par exemple s'ils expirent ou si votre organisation l'exige à intervalles réguliers. Le processus est simple et est effectué à partir de la AirWatch Console, mais il vous oblige à télécharger et exécuter le programme d'installation ACC à nouveau.

Les certificats contiennent une empreinte et la date expiration. Les deux peuvent être effacés et régénérés en même temps en sélectionnant le bouton Régénérer les certificats et en suivant les indications. Si vous régénérez des certificats, ACC ne sera plus en mesure de communiquer avec AirWatch et vous devrez effectuer la procédure d'installation à nouveau pour permettre aux deux serveurs de reconnaître les nouveaux certificats.

Procédure

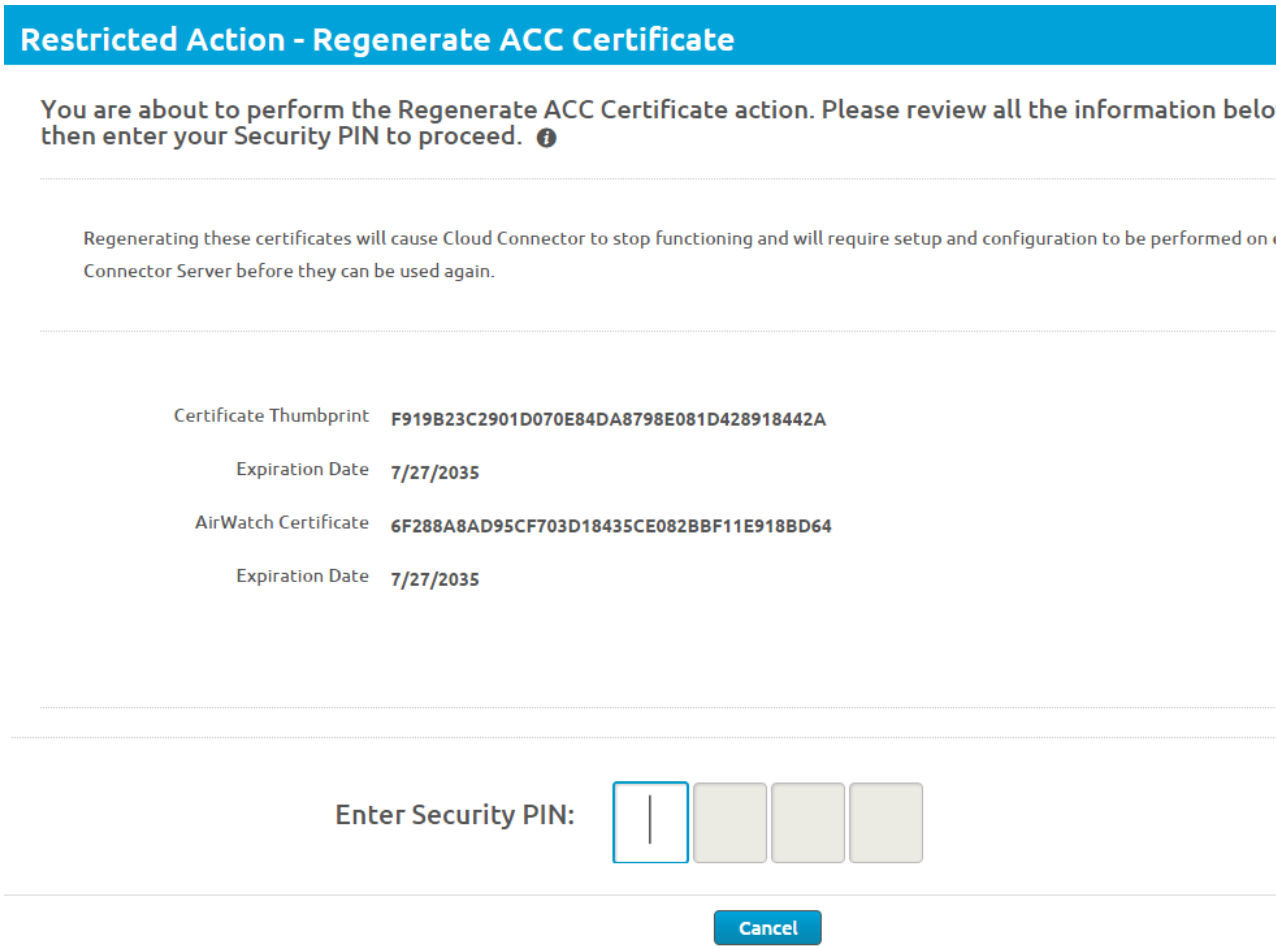
1 Accédez à **Paramètres & groupes > Tous les paramètres > Système > Intégration d'entreprise > Cloud Connector**. Les certificats, leurs empreintes et les dates d'expiration sont affichés sur l'onglet Avancé.

2 Sélectionnez **Régénérer les certificats** pour générer un nouveau certificat pour les serveurs ACC et AirWatch.



3 Si nécessaire, entrez votre code PIN pour confirmer l'action et reconnaître le message d'avertissement de sécurité. Les anciens certificats sont supprimés et les nouveaux certificats, les empreintes, et les dates d'expiration sont régénérés.

Figure 4-2.



Lorsque vous entrez votre code PIN pour confirmation, ACC ne peut plus communiquer avec le serveur AirWatch. Pour restaurer les communications entre ACC et le serveur AirWatch, revenez à ACC installation et exécutez de nouveau toutes les étapes. Cela permet aux deux serveurs de reconnaître le dernier certificat et rétablir des communications.

Configuration de VMware Identity Manager Connector 5

Cette section contient des informations sur la configuration de VMware Identity Manager Connector et la gestion des paramètres d'administration. Il comprend également des informations de configuration avancée.

Ce chapitre aborde les rubriques suivantes :

Configuration du VMware Identity Manager Connector

Après avoir installé le composant VMware Identity Manager Connector , vous devez le configurer.

La configuration du VMware Identity Manager Connector implique les tâches suivantes.

1 Si vous ne l'avez pas fait pendant l'installation, générez un code d'activation et activez le connecteur.

2 Configurez un répertoire.

3 Activez des adaptateurs d'authentification sur le connecteur.

4 Activez le mode de sortie pour le connecteur.

Générer un code d'activation pour un connecteur VMware Identity Manager Connector

Connectez-vous à la console d'administration VMware Identity Manager et générer un code d'activation pour le VMware Identity Manager Connector. Ce code d'activation est utilisé pour établir une connexion entre votre locataire et votre instance de connecteur.

Remarque Si VMware Identity Manager est configuré dans le groupe d'organisation AirWatch à partir duquel vous avez téléchargé le programme d'installation, vous n'avez pas besoin de générer le code d'activation. Si vous activez le connecteur depuis le programme d'installation, le code d'activation est prérempli dans le champ **Code d'activation**. Continuer avec le programme d'installation.

Prérequis

(Environnements SaaS) Vous avez votre URL de locataire VMware Identity Manager , par exemple, *mycompany.vmwareidentity.com*. Lorsque vous recevez votre confirmation, accédez à l'URL de votre locataire et connectez-vous à l'aide des informations d'identification d'administrateur local que vous avez reçues. Cet administrateur est un utilisateur local.

Procédure

1 Connectez-vous à la console d'administration.

2 Cliquez sur **Accepter** pour accepter les conditions générales de l'accord.

3 Cliquez sur l'onglet **Identité et gestion de l'accès**.

4 Cliquez sur **Configuration**

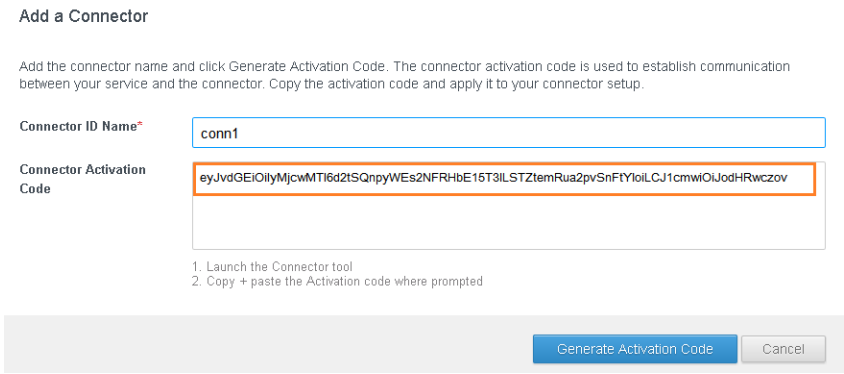
5 Sur la page Connecteurs, cliquez sur **Ajouter un connecteur**.

6 Entrez un nom pour le connecteur.

7 Cliquez sur **Générer un code d'activation**.

Le code d'activation s'affiche sur la page.

8 Copiez le code d'activation et enregistrez-le.



Suivant

Si vous activez le composant du connecteur VMware Identity Manager lors de l'exécution du programme d'installation Enterprise Systems Connector, copiez et collez le code du connecteur dans la page d'Activation du connecteur IDM VMware du programme d'installation.

Si vous activez le composant de connecteur VMware Identity Manager plus tard, après l'installation, reportez-vous à la section « Activer le VMware Identity Manager Connector », page 42.

Activer le VMware Identity Manager Connector

Si vous n'avez pas activé le VMware Identity Manager Connector depuis le programme d'installation Enterprise Systems Connector pendant l'installation, vous pouvez l'activer ultérieurement en accédant à l'URL https://*vidmConnectorHostname*: 8443.

Prérequis

Vous disposez d'un code d'activation pour le connecteur.

Procédure

1 Accédez à l'URL https://*vidmConnectorHostname*:8443.

Spécifiez *vidmConnectorHostname* comme nom de domaine complet. Par exemple, https://myconnector.example.com:8443.

2 Sur la page d'accueil, cliquez sur **Continuer**.

3 Sur la page Définir les mots de passe, créez un mot de passe pour les pages de l'administrateur du connecteur, puis cliquez sur **Continuer**.

Vous pouvez accéder à ces pages pour recueillir des bundles de fichiers journaux et télécharger des certificats.

4 Sur la page Activer le connecteur, entrez le code d'activation, puis cliquez sur **Continuer**.

Le message « Le programme d'installation est terminé » s'affiche lorsque le connecteur est correctement activé.

Configurer un répertoire

Après avoir installé et activé le VMware Identity Manager Connector, configurez un répertoire dans la console d'administration VMware Identity Manager et établissez la connexion à votre annuaire d'entreprise pour synchroniser les utilisateurs et les groupes au service.

VMware Identity Manager prend en charge l'intégration des types de répertoire suivants.

- Active Directory via LDAP
- Active Directory (authentification Windows intégrée)
- répertoire LDAP

Consultez le guide *Intégration d'annuaire avec VMware Identity Manager* pour plus d'informations avant de configurer le répertoire. Les tâches de haut niveau sont répertoriées ici.

Prérequis

Les conditions requises varient selon le type d'annuaire que vous intégrez. Consultez le guide *Intégration d'annuaire avec VMware Identity Manager* pour plus d'informations.

Procédure

1 Connectez-vous à la console d'administration de VMware Identity Manager.

Conseil Vous pouvez également accéder à la console d'administration en cliquant sur le lien **Connexion à la console d'administration** dans la page Configuration terminée qui s'affiche une fois que vous avez activé le connecteur.

2 Sélectionnez les attributs utilisateur à synchroniser avec l'annuaire.

a Cliquez sur l'onglet **Gestion des identités et des accès** et cliquez sur **Configuration**.

b Dans l'onglet **Attributs utilisateur**, sélectionnez les attributs requis et ajoutez des attributs supplémentaires si nécessaire.

Si un attribut est marqué comme requis, seuls les utilisateurs avec cet attribut sont synchronisés avec le service.

Important Tenez compte des limitations suivantes :

- Après la création du répertoire, vous ne pouvez pas modifier un attribut de facultatif à requis. Vous devez faire cette sélection maintenant.
- Les paramètres sur la page Attributs utilisateur s'appliquent à tous les annuaires dans le service. Lorsque vous marquez un attribut comme requis, tenez compte de l'effet sur les autres annuaires.
- Si vous prévoyez de synchroniser des ressources XenApp avec VMware Identity Manager, vous devez faire de **distinguishedName** un attribut requis.

---

3 Cliquez sur **Ajouter un répertoire** et sélectionnez le type de répertoire que vous voulez ajouter.

4 Suivez l'assistant pour entrer les informations de configuration du répertoire, sélectionnez des groupes et des utilisateurs à synchroniser et synchronisez les utilisateurs avec le service VMware Identity Manager.

Pour plus d'informations, reportez-vous à la section « Configuration d'Active Directory connexion pour le Service » du guide *Intégration d'annuaire à VMware Identity Manager*.

Suivant

Cliquez sur l'onglet **Utilisateurs et groupes** et vérifiez que les utilisateurs ont été synchronisés.

VMware Identity Manager Connector Activer des adaptateurs d'authentification sur le connecteur

Plusieurs adaptateurs d'authentification sont disponibles pour le VMware Identity Manager Connector en mode de sortie, notamment PasswordIdpAdapter, RSAAIdpAdapter, SecurIDAdapter et RadiusAuthAdapter. Configurez et activez les adaptateurs que vous prévoyez d'utiliser.

Lorsque vous avez créé le répertoire, la méthode d'authentification de mot de passe a été automatiquement activée pour lui. Le PasswordIdpAdapter a été configuré avec les informations que vous avez fournies pour le répertoire.

Procédure

1 Dans la console d'administration de VMware Identity Manager, cliquez sur l'onglet **Identité et gestion de l'accès**.

2 Cliquez sur **Configuration**, puis sur l'onglet **Connecteurs**.

Le connecteur que vous avez déployé est répertorié.

3 Cliquez sur le lien dans la colonne **Travailleur**.

4 Cliquez sur l'onglet **Adaptateurs d'authentification**.

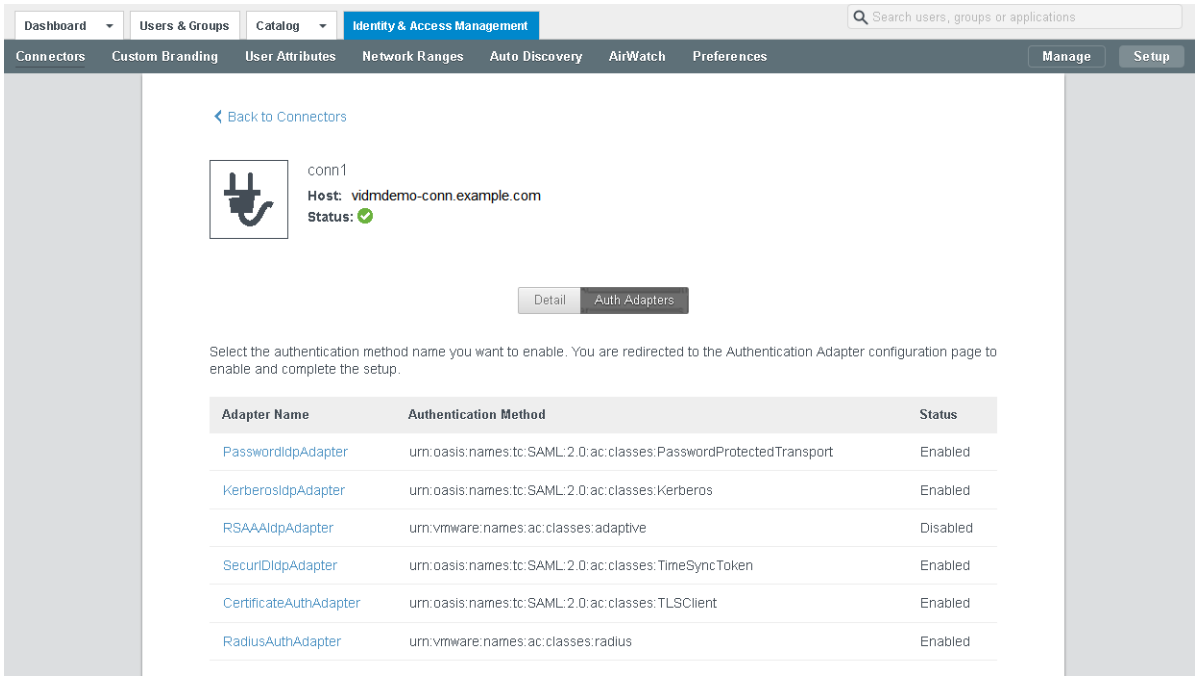
Tous les adaptateurs d'authentification disponibles pour le connecteur sont répertoriés.

Si vous avez déjà configuré un répertoire, PasswordIdpAdapter est déjà configuré et activé, avec les informations de configuration que vous avez spécifiées lors de la création du répertoire.

5 Configurez et activez les adaptateurs d'authentification que vous voulez utiliser en cliquant sur leurs liens et en entrant les informations de configuration. Vous devez activer au moins un adaptateur d'authentification.

Pour plus d'informations sur la configuration d'adaptateurs d'authentification spécifiques, consultez le *Guide d'administration de VMware Identity Manager*.

Par exemple :



Activer le mode de sortie pour le connecteur VMware Identity Manager Connector

Pour activer le mode de connexion sortie seule pour le connecteur VMware Identity Manager Connector, associez-le avec le fournisseur d'identité intégré.

Le fournisseur d'identité intégré est disponible par défaut dans le service VMware Identity Manager et fournit des méthodes d'authentification intégrée supplémentaires, telles que VMware Verify. Pour plus d'informations sur le fournisseur d'identité intégré, consultez le *Guide d'administration de VMware Identity Manager*.

Remarque Le connecteur peut être utilisé en mode normal et en mode sortant de manière simultanée. Même si vous activez le mode sortant, vous pouvez configurer l'authentification Kerberos pour les utilisateurs internes à l'aide de stratégies et méthodes d'authentification.

Procédure

1 Dans l'onglet **Identité et gestion de l'accès** de la console d'administration, cliquez sur **Gérer**.

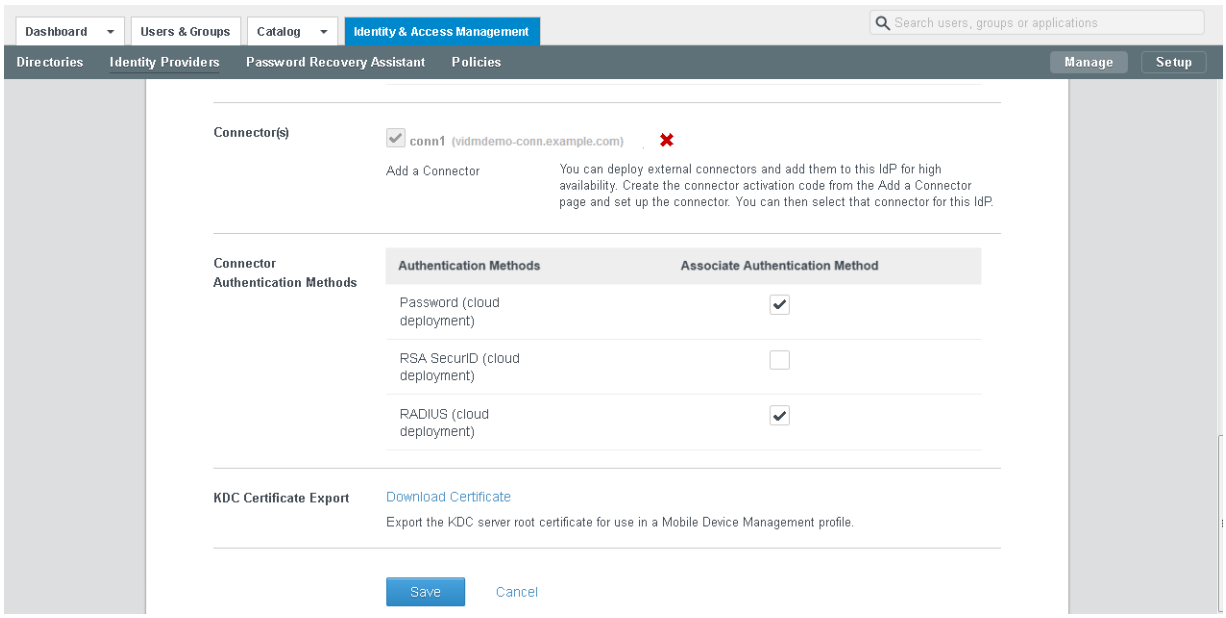
2 Cliquez sur l'onglet **Fournisseurs d'identité**.

3 Cliquez sur le lien **Intégré**.

4 Entrez les informations suivantes.

Option	Description
Utilisateurs	Sélectionnez le répertoire ou les domaines qui utiliseront le fournisseur d'identité intégré.
Réseau	Sélectionnez les plages réseau qui utiliseront le fournisseur d'identité intégré.
Connecteur(s)	Sélectionnez le connecteur que vous avez configuré. **Remarque** Ensuite, lorsque vous ajoutez des connecteurs supplémentaires pour la haute disponibilité, sélectionnez et ajoutez-les tous ici pour les associer au fournisseur d'identité intégré. VMware Identity Manager distribue automatiquement le trafic sur tous les connecteurs associés au fournisseur d'identité intégré. Aucun équilibrage de charge n'est nécessaire.
Méthodes d'authentification du connecteur	Les méthodes de déploiement que vous avez activées pour le connecteur sont répertoriées. Sélectionnez les méthodes d'authentification que vous voulez utiliser. PasswordIdpAdapter, qui a été automatiquement configuré et activé lorsque vous avez créé un répertoire, est affiché sur cette page sous la forme **Mot de passe (déploiement de cloud)**, ce qui indique qu'il est utilisé avec le connecteur en mode de sortie.

Par exemple :



5 Cliquez sur **Enregistrer** pour enregistrer la configuration du fournisseur d'identité intégré.

6 Modifiez les stratégies pour utiliser les méthodes d'authentification que vous avez activées.

a Dans l'onglet **Identité et gestion de l'accès**, cliquez sur **Gérer**.

b Cliquez sur l'onglet **Stratégies** et cliquez sur la stratégie que vous voulez modifier.

c Sous **Règles de stratégie**, pour la règle que vous voulez modifier, cliquez sur le lien dans la colonne **Méthode d'authentification**.

d Sur la page Modifier la règle de stratégie, sélectionnez la méthode d'authentification que vous voulez utiliser pour cette règle.

e Cliquez sur **OK**.

f Cliquez sur **Enregistrer**.

Pour plus d'informations sur la configuration de stratégies, consultez le *Guide d'administration de VMware Identity Manager*.

Le mode de sortie du connecteur est maintenant activé. Lorsqu'un utilisateur se connecte à l'aide de l'une des méthodes d'authentification que vous avez activées pour le connecteur sur la page du fournisseur d'identité intégré, une redirection HTTP vers le connecteur n'est pas requise.

Gestion des paramètres d'administration VMware Identity Manager Connector

Après la configuration initiale de VMware Identity Manager Connector , vous pouvez accéder aux pages de l'administrateur du connecteur à tout moment pour installer des certificats, gérer des mots de passe et télécharger des fichiers journaux.

Les pages d'administration VMware Identity Manager Connector sont disponibles sur la page https://*connectorFQDN*: 8443/cfg/login, par exemple, https://myconnector.example.com:8443/cfg/login. Ouvrez une session en tant que l'utilisateur Admin de connecteur avec le mot de passe admin que vous avez créé lorsque vous avez installé le connecteur.

Tableau 5-1. Paramètres du connecteur

Option	Description
Installer le certificat	Vous pouvez installer un certificat auto-signé ou personnalisé pour le connecteur. Si le connecteur est configuré avec un équilibrage de charge, vous pouvez installer le certificat racine d'équilibrage de charge. L'emplacement du certificat CA du connecteur racine est également affiché sur cette page, dans l'onglet **Interrompre SSL sur un équilibrage de charge**.
Changer le mot de passe	Sur cette page, vous pouvez changer le mot de passe de l'administrateur du connecteur.
Emplacements des fichiers journaux	Vous pouvez accéder aux fichiers de journaux du connecteur directement sur l'ordinateur hôte ou rassembler les fichiers journaux du connecteur dans un fichier zip à télécharger.

Utilisation des certificats SSL

Lorsque le dispositif VMware Identity Manager Connector est installé, un certificat de serveur SSL par défaut est généré automatiquement. Vous pouvez utiliser ce certificat auto-signé pour effectuer un test général de l'installation. VMware vous recommande vivement de générer et d'installer des certificats SSL commerciaux dans votre environnement de production.

Une autorité de certification est une entité approuvée qui garantit l'identité du certificat et de son créateur. Lorsqu'un certificat est signé par une autorité de certification de confiance, les utilisateurs ne reçoivent plus les messages leur demandant de vérifier le certificat.

Si vous déployez le SSL VMware Identity Manager Connector avec le certificat SSL auto-signé, le certificat de l'autorité de certification racine doit être disponible en tant qu'autorité de certification de confiance pour les clients qui accèdent au connecteur. Les clients peuvent inclure les machines des utilisateurs finaux, les équilibreurs de charge, les proxys, etc. Vous pouvez télécharger l'autorité de certification racine à l'adresse *https://myconnector.domain.com/horizon_workspace_rootca.pem*.

Installez un certificat signé par une autorité de certification pour le VMware Identity Manager Connector

Lorsque VMware Identity Manager Connector est installé, un certificat de serveur SSL par défaut est généré. Vous devez générer et installer des certificats SSL commerciaux pour l'environnement de votre connecteur.

Remarque Si le connecteur pointe vers un équilibrage de charge, le certificat SSL est appliqué à celui-ci.

Prérequis

Générez une demande de signature de certificat (CSR) pour obtenir un certificat valide et signé d'une autorité de certification. Si votre entreprise fournit des certificats SSL signés par une autorité de certification, vous pouvez les utiliser. Le certificat doit être au format PEM.

Procédure

1 Connectez-vous aux pages d'administration VMware Identity Manager Connector sur https://*connectorFQDN*: 8443/cfg/login en tant qu'utilisateur Admin.

2 Cliquez sur **Installer le certificat**.

3 Dans l'onglet Interrompre SSL sur Identity Manager Appliance, pour l'option **Certificat SSL** , sélectionnez **Un certificat personnalisé**.

4 Dans la zone de texte **Chaîne de certificat SSL**, collez les certificats hôte, intermédiaire et racine, dans cet ordre.

Le certificat SSL ne fonctionne que si vous incluez toute la chaîne de certificat dans le bon ordre. Pour chaque certificat, copiez tout ce qui se trouve entre les lignes -----BEGIN CERTIFICATE----- et -----END CERTIFICATE----, en incluant celles-ci.

Vérifiez que le certificat inclut le nom d'hôte FQDN.

5 Collez la clé privée dans la zone de texte **Clé privée**. Copiez tout ce qui se trouve entre les lignes ---- BEGIN RSA PRIVATE KEY et ---END RSA PRIVATE KEY.

6 Cliquez sur **Enregistrer.**

Exemple : Exemples de certificat

Exemple de chaîne de certificat
-----BEGIN CERTIFICATE-----
jlQvt9WdR9Vpg3WQT5+C3HU17bUOwvhp/r0+ ... ... W53+O05j5xsxzDJfWr1lqBlFF/OkIYCPcyK1
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
WdR9Vpg3WQT5+C3HU17bUOwvhp/rjlQvt90+ ... ... O05j5xsxzDJfWr1lqBlFF/OkIYCPW53+cyK1
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----

Exemple de chaîne de certificat
dR9Vpg3WQTjlQvt9W5+C3HU17bUOwvhp/r0+ ... ... 5j5xsxzDJfWr1lqW53+O0BlFF/OkIYCPcyK1
-----END CERTIFICATE-----

Exemple de clé privée
-----BEGIN RSA PRIVATE KEY-----
jlQvtg3WQT5+C3HU17bU9WdR9VpOwvhp/r0+ ... ... 1lqBlFFW53+O05j5xsxzDJfWr/OkIYCPcyK1
-----END RSA PRIVATE KEY-----

Gestion de vos mots de passe VMware Identity Manager Connector

Lorsque vous avez installé le VMware Identity Manager Connector, vous avez créé un mot de passe pour l'utilisateur Admin. Vous pouvez modifier ce mot de passe dans les pages d'administration du connecteur.

Important Assurez-vous de créer des mots de passe forts. Les mots de passe forts doivent contenir au moins huit caractères, des majuscules et des minuscules et au moins un chiffre ou caractère spécial.

Procédure

1. Connectez-vous aux pages d'administration VMware Identity Manager Connector sur https://*connectorFQDN*: 8443/cfg/login en tant qu'utilisateur Admin.
2. Cliquez sur **Modifier le mot de passe**.
3. Entrez les anciens et nouveaux mots de passe.

   Important Le mot de passe de l'utilisateur Admin doit contenir au moins 6 caractères.

4. Cliquez sur **Enregistrer**.

Affichage des fichiers journaux

Les fichiers journaux VMware Identity Manager Connector peuvent vous aider à effectuer un débogage ou un dépannage. Les fichiers journaux peuvent être trouvés dans le répertoire `\IDMConnector\opt\vmware\horizon\workspace\logs` *`InstallDirectory`*.

Les fichiers journaux les plus pertinents sont les suivants.

Tableau 5-2. Fichiers journaux

Composant	Emplacement du fichier journal sous Windows	Description
Journaux du Programme de configuration	*InstallDirectory*\IDMConnector\opt\vmware\horizon\workspace\logs\configurator.log	Requêtes que le programme de configuration reçoit du client REST et de l'interface Web.
Journaux Connector	*InstallDirectory*\IDMConnector\opt\vmware\horizon\workspace\logs\connector.log	Enregistrement de chaque demande reçue de l'interface Web. Chaque entrée de journal inclut également l'URL, l'horodatage et les exceptions de la requête. Aucune action de synchronisation n'est enregistrée.
Journaux Apache Tomcat	*InstallDirectory*\IDMConnector\opt\vmware\horizon\workspace\logs\catalina.log	Apache Tomcat enregistre les messages qui ne sont pas enregistrés dans d'autres fichiers journaux.

Vous pouvez également télécharger un bundle de fichier journal à partir des pages d'administration VMware Identity Manager Connector .

Télécharger un bundle de journaux

Vous pouvez télécharger un bundle de fichiers journaux pour le VMware Identity Manager Connector à partir des pages d'administration du connecteur. Les fichiers journaux peuvent vous aider à effectuer un débogage ou un dépannage.

Pour collecter les journaux à partir de chaque instance du connecteur dans votre environnement, connectez-vous aux pages d'administration pour chaque instance.

Procédure

1 Connectez-vous aux pages d'administration VMware Identity Manager Connector sur https://*connectorFQDN*: 8443/cfg/login en tant qu'utilisateur Admin.

2 Cliquez sur **Emplacements des fichiers journaux** et cliquez sur **Préparer le bundle de journaux**.

Les informations sont collectées dans un fichier .zip à télécharger.

3 Téléchargez le bundle de journaux

Activation des paramètres de proxy après l'installation

Si vous n'avez pas configuré les paramètres de proxy HTTPS pour le composant VMware Identity Manager Connector pendant l'installation, vous pouvez les configurer ultérieurement en modifiant le fichier `C:\INSTALL_DIR\opt\vmware\horizon\workspace\conf\wrapper.conf`.

Procédure

1 Connectez-vous au serveur Windows.

2 Ouvrez le fichier suivant dans un éditeur de texte

`C:\INSTALL_DIR\opt\vmware\horizon\workspace\conf\wrapper.conf`

3 Après la dernière entrée `wrapper.java.additional`, ajoutez les entrées suivantes :

```
wrapper.java.additional.32="-Dhttps.proxyHost=proxyServer"
wrapper.java.additional.33="-Dhttps.proxyPort=proxyServerPort"
```

où *proxyServer* est le serveur proxy HTTPS, *proxyServerPort* est le port du serveur proxy HTTPS, et le nombre correspond au nombre d'entrées `wrapper.java.additional`. Par exemple, si le fichier a déjà 31 entrées `wrapper.java.additional`, utilisez 32 et 33 pour les nouvelles entrées comme indiqué dans l'exemple.

4 Si vous exécutez le service IDM Connector en tant qu'utilisateur de domaine, ajoutez également les lignes suivantes :

```
wrapper.ntservice.account=DOMAINE/nom d'utilisateur
wrapper.ntservice.password=******
```

Par exemple :

```
wrapper.ntservice.account=example/userA
wrapper.ntservice.password=******
```

5 À partir de la ligne de commande, exécutez les commandes suivantes en tant qu'administrateur :

a `C:\INSTALL_DIR\usr\local\horizon\scripts\horizonService.bat reinstall`

La commande doit renvoyer la sortie suivante :

```
Derived instance name: workspace
Reinstalling instance at
C:\VMware\IDMConnector\opt\vmware\horizon\workspace
wrapper | Service is running. Stopping it...
wrapper | Waiting to stop...
wrapper | VMware IDM Connector stopped.
wrapper | VMware IDM Connector removed.
wrapper | VMware IDM Connector installed.
```

b `C:\VMware\IDMConnector\usr\local\horizon\scripts\horizonService.bat start`

La commande doit renvoyer la sortie suivante :

```
Derived instance name: workspace
Starting instance at C:\VMware\IDMConnector\opt\vmware\horizon\workspace
wrapper | Starting the VMware IDM Connector service...
wrapper | VMware IDM Connector started.
```

Configuration de la haute disponibilité pour le VMware Identity Manager Connector

Vous pouvez configurer le VMware Identity Manager Connector pour la haute disponibilité et le basculement du connecteur en ajoutant plusieurs instances de connecteur dans un cluster. Si l'un des dispositifs virtuels devient indisponible pour une raison quelconque, d'autres instances seront toujours disponibles.

Pour créer un cluster, vous installez les nouvelles instances de connecteur et vous les configurez exactement de la même manière que vous configurez le premier connecteur.

Vous associez ensuite toutes les instances de connecteur au fournisseur d'identité intégré. Le service VMware Identity Manager distribue automatiquement le trafic sur tous les connecteurs associés au fournisseur d'identité intégré. Aucun équilibrage de charge n'est nécessaire. Si l'un des connecteurs devient non disponible en raison d'un problème de réseau, le service ne dirige pas le trafic vers celui-ci. Lorsque la connectivité est restaurée, le service reprend l'envoi du trafic au connecteur.

Après la configuration du cluster de connecteur, les méthodes d'authentification que vous avez activées sur le connecteur sont hautement disponibles. Si l'une des instances de connecteur n'est pas disponible, l'authentification est toujours disponible. Toutefois, pour la synchronisation d'annuaire, en cas d'échec de l'instance de connecteur, vous devez sélectionner manuellement une autre instance de connecteur comme connecteur de synchronisation. Cela est dû au fait que la synchronisation de répertoire ne peut être activée que sur un seul connecteur à la fois.

Remarque Cette section ne s'applique pas à la haute disponibilité de l'authentification Kerberos. Voir « Ajout d'une méthode d'authentification Kerberos à votre déploiement de connecteur VMware Identity Manager Connector », page 54.

Installer des instances VMware Identity Manager Connector supplémentaires

Après avoir installé et configuré la première instance de VMware Identity Manager Connector, vous pouvez ajouter des connecteurs supplémentaires pour une haute disponibilité en installant de nouvelles instances de connecteur et en les configurant exactement de la même façon que la première instance de connecteur.

Important Les nouvelles instances de connecteur doivent être activées sur le même service VMware Identity Manager que la première instance de connecteur.

Prérequis

Vous avez installé et configuré la première instance de connecteur, comme décrit dans « Exécutez le programme d'installation Enterprise Systems Connector. », page 26.

Procédure

1 Installez et configurez une nouvelle instance de connecteur VMware Identity Manager Connector en suivant ces instructions.

- « Exécutez le programme d'installation Enterprise Systems Connector. », page 26
- « Configuration du VMware Identity Manager Connector », page 41

Important Vous devez activer la nouvelle instance de connecteur par rapport au même service VMware Identity Manager que le premier connecteur.

2 Associez le nouveau connecteur VMware Identity Manager Connector au `WorkspaceIDP` de la première instance de connecteur.

a Dans la console d'administration VMware Identity Manager, sélectionnez l'onglet **Gestion des identités et des accès**, puis l'onglet **Fournisseurs d'identité**.

b Sur la page Fournisseurs d'identité, recherchez le `WorkspaceIDP` de la première instance de connecteur et cliquez sur le lien.

c Dans le champ **Connecteur(s)**, sélectionnez le nouveau connecteur.

d Entrez le mot de passe de nom unique de liaison et cliquez sur **Ajouter un connecteur**.

e Cliquez sur **Enregistrer**.

3 Configurez et activez des adaptateurs d'authentification sur le nouveau connecteur.

Important Les adaptateurs d'authentification sur tous les connecteurs de votre cluster doivent être configurés de la même manière. Les mêmes méthodes d'authentification doivent être activées sur tous les connecteurs.

a Dans l'onglet **Identité et gestion de l'accès**, cliquez sur **Configuration**, puis sur l'onglet **Connecteurs**.

b Cliquez sur le lien dans la colonne **Travailleur** du nouveau connecteur.

c Cliquez sur l'onglet **Adaptateurs d'authentification**.

Tous les adaptateurs d'authentification disponibles pour le connecteur sont répertoriés.

PasswordIdpAdapter est déjà configuré et activé, car vous avez associé le nouveau connecteur au répertoire associé au premier connecteur.

d Configurez et activez les autres adaptateurs d'authentification de la même façon que le premier connecteur. Vérifiez que les informations de configuration sont identiques.

Pour plus d'informations sur la configuration des adaptateurs d'authentification, consultez le *Guide d'administration de VMware Identity Manager*.

Suivant

« Ajouter de nouvelles instances VMware Identity Manager Connector au fournisseur d'identité intégré », page 53

Ajouter de nouvelles instances VMware Identity Manager Connector au fournisseur d'identité intégré

Une fois que vous avez déployé et configuré les nouvelles instances de connecteur VMware Identity Manager Connector, ajoutez-les au fournisseur d'identité intégré et activez les mêmes méthodes d'authentification que celles activées sur la première instance de connecteur. VMware Identity Manager distribue automatiquement le trafic sur tous les connecteurs associés au fournisseur d'identité intégré.

Procédure

1 Dans l'onglet **Gestion des identités et des accès** de la console d'administration VMware Identity Manager, cliquez sur **Gérer**.

2 Cliquez sur l'onglet **Fournisseurs d'identité**.

3 Cliquez sur le lien **Intégré**.

4 Dans le champ **Connecteur(s)**, sélectionnez le nouveau connecteur dans la liste déroulante et cliquez sur **Ajouter un connecteur**.

5 Dans la section **Méthodes d'authentification de connecteur**, activez les mêmes méthodes d'authentification que celles que vous avez sélectionnées pour le premier connecteur.

La méthode d'authentification Mot de passe (déploiement de Cloud) est automatiquement configurée et activée. Vous devez activer les autres méthodes d'authentification.

Important Les adaptateurs d'authentification sur tous les connecteurs de votre cluster doivent être configurés de la même manière. Les mêmes méthodes d'authentification doivent être activées sur tous les connecteurs.

Pour plus d'informations sur la configuration d'adaptateurs d'authentification spécifiques, consultez le *Guide d'administration de VMware Identity Manager*.

6 Cliquez sur **Enregistrer** pour enregistrer la configuration du fournisseur d'identité intégré.

Activation de la synchronisation de répertoire sur un autre connecteur en cas d'échec

En cas d'échec de l'instance de connecteur, l'authentification est gérée automatiquement par une autre instance de connecteur. Toutefois, pour la synchronisation de répertoire, vous devez modifier les paramètres de répertoire dans le service VMware Identity Manager afin d'utiliser une autre instance de connecteur plutôt que l'instance de connecteur d'origine. La synchronisation de répertoire ne peut être activée que sur un seul connecteur à la fois.

Procédure

1 Connectez-vous à la console d'administration de VMware Identity Manager.

2 Cliquez sur l'onglet **Identité et gestion de l'accès** et cliquez sur **Répertoires**.

3 Cliquez sur le répertoire qui était associé à l'instance du connecteur d'origine.

Conseil Vous pouvez voir ces informations sur la page **Configuration > Connecteurs**.

4 Dans la section **Synchronisation et authentification du répertoire** de la page du répertoire, dans la liste déroulante **Connecteur de synchronisation**, sélectionnez une autre instance de connecteur.

5 Dans la zone de texte **Mot de passe du nom unique de liaison**, entrez votre mot de passe de compte Bind Active Directory.

6 Cliquez sur **Enregistrer**.

Ajout d'une méthode d'authentification Kerberos à votre déploiement de connecteur VMware Identity Manager Connector

Vous pouvez ajouter à votre déploiement l'authentification Kerberos pour les utilisateurs internes (ce qui nécessite le mode de connexion entrant) en fonction des connecteurs en mode de connexion sortant uniquement. Les mêmes connecteurs peuvent être configurés pour utiliser l'authentification Kerberos pour les utilisateurs provenant du réseau interne et une autre méthode d'authentification pour les utilisateurs de l'extérieur. Cela peut être obtenu en définissant des stratégies d'authentification basées sur plages réseau.

Remarque Pour configurer la haute disponibilité pour l'authentification Kerberos, un équilibrage de charge est requis.

Configuration et activation de l'adaptateur d'authentification Kerberos

Configurez et activez KerberosIdpAdapter sur le connecteur VMware Identity Manager Connector. Si vous avez déployé un cluster pour la haute disponibilité, configurez et activez l'adaptateur sur tous les connecteurs dans votre cluster.

Important Les adaptateurs d'authentification sur tous les connecteurs de votre cluster doivent être configurés de la même manière. Les mêmes méthodes d'authentification doivent être configurées sur tous les connecteurs.

Lorsque vous configurez l'adaptateur d'authentification Kerberos, le connecteur VMware Identity Manager tente d'initialiser Kerberos automatiquement. Si le service VMware IDM Connector n'est pas exécuté avec des privilèges suffisants pour initialiser Kerberos, un message d'erreur s'affiche. Dans ce cas, suivez les instructions dans http://kb.vmware.com/kb/2149753 pour exécuter un script afin d'initialiser Kerberos.

Pour plus d'informations sur la configuration de l'authentification Kerberos, consultez le *Guide d'administration de VMware Identity Manager*.

Prérequis

- La machine Windows sur laquelle est installé le connecteur VMware Identity Manager doit être jointe au domaine.
- Vous devez avoir installé le composant VMware Identity Manager Connector en tant qu'utilisateur de domaine faisant partie du groupe d'administrateurs sur la machine Windows, et vous devez exécuter le service VMware IDM Connector en tant qu'utilisateur de domaine Windows.

Procédure

1 Dans la console d'administration de VMware Identity Manager, cliquez sur l'onglet **Identité et gestion de l'accès**.

2 Cliquez sur **Configuration**, puis sur l'onglet **Connecteurs**.

Tous les connecteurs que vous avez déployés sont répertoriés.

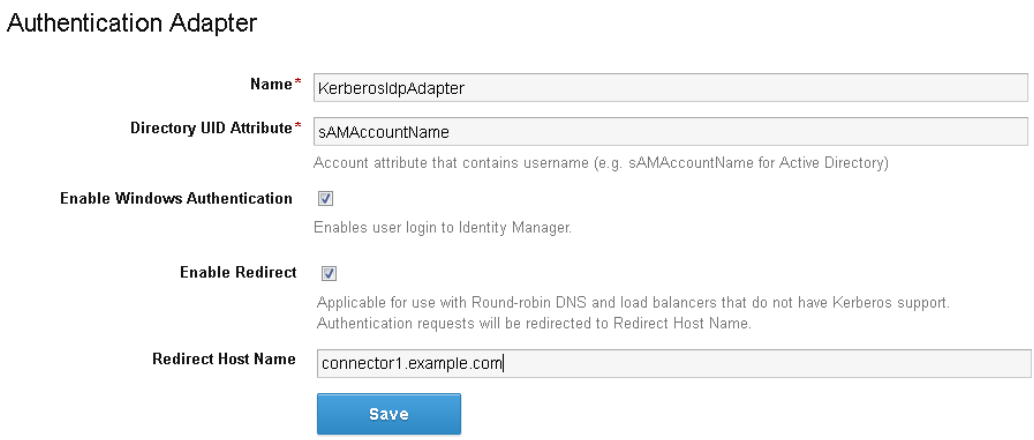
3 Cliquez sur le lien dans la colonne **Travailleur** de l'un des connecteurs.

4 Cliquez sur l'onglet **Adaptateurs d'authentification**.

5 Cliquez sur le lien KerberosIdpAdapter, puis configurez et activez l'adaptateur.

Option	Description
Nom	Le nom par défaut de l'adaptateur est KerberosIdpAdapter. Vous pouvez modifier ce nom.
Attribut UID du répertoire	Attribut de compte qui contient le nom d'utilisateur.
Activer l'authentification Windows	Sélectionnez cette option.
Activer la redirection	Si vous disposez de plusieurs connecteurs dans un cluster et que vous prévoyez de configurer la haute disponibilité Kerberos en utilisant un équilibrage de charge, sélectionnez cette option et spécifiez une valeur pour **Nom d'hôte de redirection**. Si votre déploiement ne contient qu'un seul connecteur, vous n'avez pas besoin d'utiliser les options **Activer la redirection** et **Nom d'hôte de redirection**.
Nom d'hôte de redirection	Une valeur est requise si l'option **Activer la redirection** est sélectionnée. Entrez le nom d'hôte du connecteur. Par exemple, si le nom d'hôte du connecteur est connector1.example.com, entrez **`connector1.example.com`** dans la zone de texte.

Par exemple :



Pour plus d'informations sur la configuration de KerberosIdPAdapter, consultez le *Guide d'administration de VMware Identity Manager*.

6 Cliquez sur **Enregistrer**.

Remarque Si vous obtenez une erreur indiquant que l'initialisation de Kerberos a échoué, exécutez le script d'initialisation Kerberos manuellement en suivant les instructions dans http://kb.vmware.com/kb/2149753, puis revenez à cette page et configurer l'adaptateur.

7 Si vous avez déployé un cluster, configurez KerberosIdPAdapter sur tous les connecteurs de votre cluster.

Assurez-vous de configurer l'adaptateur de la même manière sur tous les connecteurs.

Suivant

Configurez la haute disponibilité pour l'authentification Kerberos, si nécessaire. L'authentification Kerberos n'est pas hautement disponible sans équilibrage de charge.

Configuration de la haute disponibilité pour l'authentification Kerberos

Pour configurer la haute disponibilité pour l'authentification Kerberos, installez un équilibrage de charge sur votre réseau interne dans le pare-feu et ajoutez-lui les instances VMware Identity Manager Connector.

Vous devez également configurer certains paramètres sur l'équilibrage de charge, établir l'approbation SSL entre l'équilibrage de charge et le connecteur et modifier l'URL d'authentification du connecteur pour utiliser le nom d'hôte de l'équilibrage de charge.

Configurer des paramètres d'équilibrage de charge

Vous devez configurer certains paramètres sur l'équilibrage de charge, tels que l'activation des en-têtes X-Forwarded-For, la définition correcte du délai d'expiration de l'équilibrage de charge et l'activation des sessions rémanentes.

Configurez ces paramètres.

- En-têtes X-Forwarded-For

  Vous devez activer les en-têtes X-Forwarded-For sur votre équilibrage de charge. Cela détermine la méthode d'authentification. Pour plus d'informations, consultez la documentation de l'équilibrage de charge.

- Délai d'expiration de l'équilibreur de charge

  Pour un bon fonctionnement de VMware Identity Manager Connector, vous pouvez avoir besoin d'augmenter la valeur par défaut du délai d'expiration des demandes d'équilibrage de charge. Cette valeur est définie en minutes. Si le paramètre du délai d'expiration est trop bas, l'erreur suivante peut se produire.

  ```
  Erreur 502 : Le service est actuellement indisponible
  ```

- Activer les sessions rémanentes

  Vous devez activer le paramètre de session rémanente sur l'équilibrage de charge si votre déploiement dispose de plusieurs instances de connecteur. L'équilibrage de charge établit ensuite une liaison entre la session d'un utilisateur et une instance de connecteur spécifique.

Appliquer le certificat racine de VMware Identity Manager Connector à l'équilibrage de charge

Lorsque le VMware Identity Manager Connector est configuré derrière un équilibrage de charge, vous devez établir la relation d'approbation entre l'équilibrage de charge et le connecteur. Le certificat racine du connecteur doit être copié dans l'équilibrage de charge en tant que certificat racine approuvé.

Le certificat du VMware Identity Manager Connector peut être téléchargé depuis les pages d'administration de connecteur sur https://*connectorFQDN*: 8443/cfg/ssl.

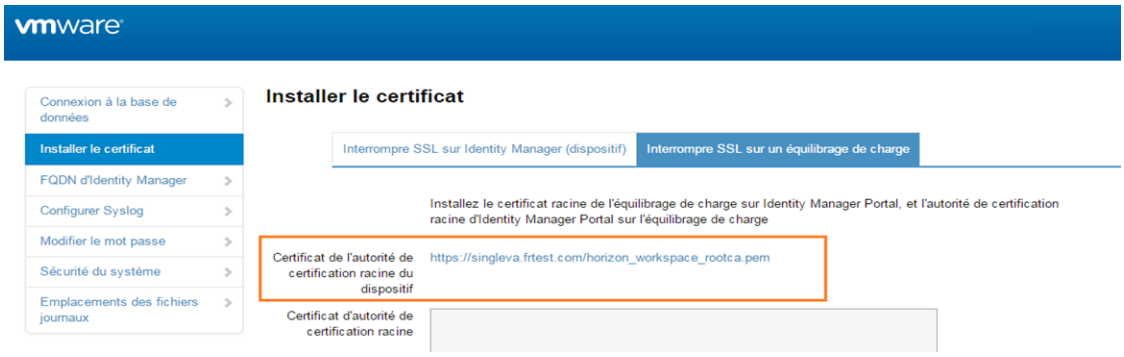
Si le nom de domaine du connecteur pointe vers un équilibrage de charge, le certificat SSL peut uniquement être appliqué à cet équilibrage de charge.

Procédure

1 Accédez aux pages d'administration du connecteur sur https://*connectorFQDN*: 8443/cfg/login et connectez-vous comme utilisateur Admin.

2 Sélectionnez **Installer le certificat**.

3 Sélectionnez l'onglet **Interrompre SSL sur un équilibrage de charge** et, dans le champ **Certificat de l'autorité de certification racine du dispositif**, cliquez sur le lien `https://hostname/horizon_workspace_rootca.pem`.



4 Copiez tout ce qui se trouve entre les lignes -----BEGIN CERTIFICATE----- et -----END CERTIFICATE----, en incluant celles-ci, et collez le certificat racine à l'emplacement adéquat sur chacun de vos équilibrages de charge. Reportez-vous à la documentation relative à l'équilibrage de charge.

Suivant

Copiez-collez le certificat racine de l'équilibrage de charge sur le dispositif du VMware Identity Manager Connector.

Appliquer le certificat racine d'équilibrage de charge au VMware Identity Manager Connector

Lorsque le VMware Identity Manager Connector est configuré derrière un équilibrage de charge, vous devez établir la relation d'approbation entre l'équilibrage de charge et le connecteur. En plus de copier le certificat racine du connecteur sur l'équilibrage de charge, vous devez copier le certificat racine de l'équilibrage de charge sur le connecteur.

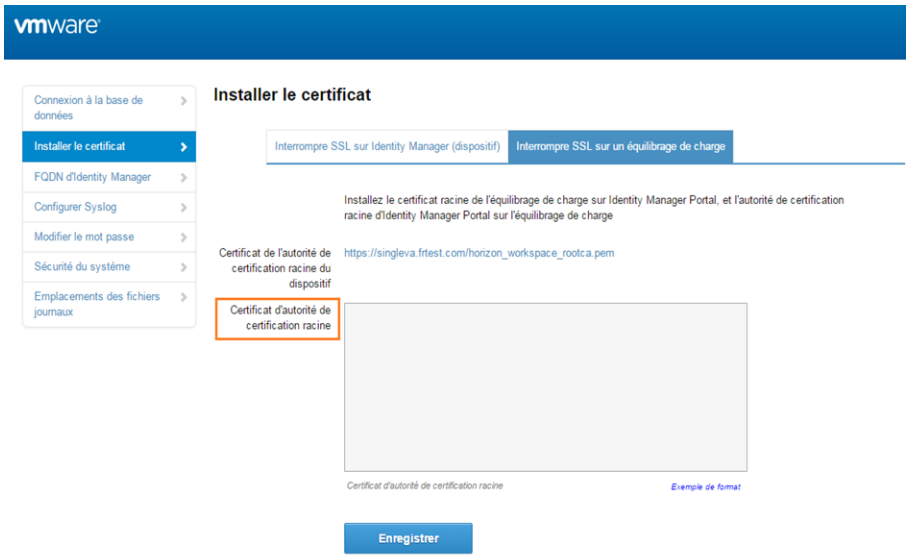
Procédure

1 Obtenez le certificat racine de l'équilibrage de charge.

2 Accédez aux pages d'administration VMware Identity Manager Connector sur https://*connectorFQDN*:8443/cfg/login et connectez-vous en tant qu'utilisateur Admin.

3 Sur la page **Installer le certificat**, sélectionnez l'onglet **Interrompre SSL sur un équilibrage de charge**.

4 Copiez le texte du certificat de l'équilibrage de charge dans le champ **Certificat d'autorité de certification racine**.



5 Cliquez sur **Enregistrer**.

Remplacer le nom d'hôte IdP de connecteur par le nom d'hôte d'équilibrage de charge

Une fois que vous avez ajouté les instances VMware Identity Manager Connector à l'équilibrage de charge, vous devez remplacer le nom d'hôte IdP sur l'IdP Workspace de chaque connecteur par le nom d'hôte d'équilibrage de charge.

Prérequis

Les instances de connecteur sont configurées derrière un équilibrage de charge. Assurez-vous que le port de l'équilibrage de charge est le port 443. N'utilisez pas 8443, car ce numéro de port est le port administratif.

Procédure

1 Connectez-vous à la console d'administration de VMware Identity Manager.

2 Cliquez sur l'onglet **Identité et gestion de l'accès**.

3 Cliquez sur l'onglet **Fournisseurs d'identité**.

4 Sur la page Fournisseurs d’identité, cliquez sur le lien IdP Workspace de votre instance de connecteur.

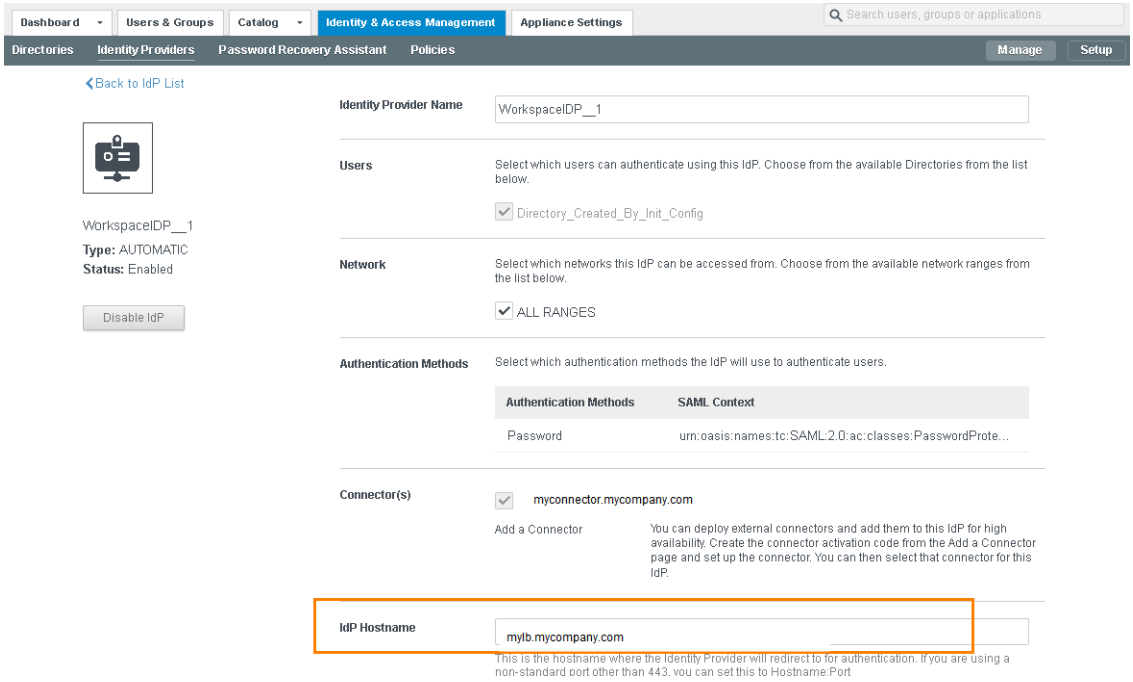
5 Dans la zone de texte **Nom d’hôte IdP**, remplacez le nom d’hôte du nom d’hôte du connecteur par le nom d’hôte d’équilibrage de charge.

Par exemple, si le nom d’hôte de votre connecteur est `myconnector` et que le nom d’hôte de votre équilibrage de charge est `mylb`, remplacez l’URL

`myconnector.mycompany.com:`*`port`*

par ce qui suit :

`mylb.mycompany.com:`*`port`*



Suppression d'une instance de VMware Identity Manager Connector

Vous pouvez supprimer une instance de VMware Identity Manager Connector depuis le service VMware Identity Manager. Une instance de connecteur ne peut pas être supprimée si elle est associée à un répertoire.

Par exemple, vous pouvez supprimer une instance de connecteur lorsque vous voulez utiliser le même nom d’hôte pour une nouvelle instance de connecteur.

Procédure

1 Connectez-vous à la console d'administration de VMware Identity Manager.

2 Sélectionnez l'onglet **Identité et gestion de l'accès** et cliquez sur **Configuration**.

3 Si un répertoire est associé à l’instance de connecteur que vous voulez supprimer, supprimez le répertoire d’abord.

a Cliquez sur le nom du répertoire dans la colonne **Répertoire associé**.

b Cliquez sur **Supprimer le répertoire**.

4 Sur la page **Configuration > Connecteurs**, cliquez sur l'icône **Supprimer** à côté de l'instance de connecteur que vous voulez supprimer et cliquez sur **Confirmer** dans la boîte de dialogue de confirmation.

   L'instance de connecteur est supprimée du service VMware Identity Manager.

5 Désinstallez le composant VMware Identity Manager Connector à partir du serveur Windows sur lequel il est installé.

Mise à niveau de VMware Identity Manager Connector

Pour mettre à niveau le composant VMware Identity Manager Connectord'Enterprise Systems Connector, téléchargez le programme d'installation à partir de la nouvelle version de la console AirWatch et exécutez-le.

Après la mise à niveau, il est inutile de générer un nouveau code d'activation ou de réactiver VMware Identity Manager Connector. Votre configuration existante s'applique au connecteur mis à niveau.

Procédure

1 Connectez-vous à la nouvelle version de la console AirWatch.

2 Accédez à **Groupes et paramètres > Tous les paramètres > Système > Intégration d'entreprise > VMware Enterprise Systems Connector**.

3 Dans l'onglet **Général**, cliquez sur **Télécharger le programme d'installation de VMware Enterprise Systems Connector**.

   La page de téléchargement du programme d'installation de VMware Enterprise Systems Connector s'affiche.

4 Créez un mot de passe pour le certificat et cliquez sur **Télécharger**.

   Vous avez besoin de ce mot de passe lorsque vous installez le composant ACC.

5 Enregistrez le fichier du programme d'installation sur le serveur Windows où la précédente version du connecteur est installée.

6 Exécutez le programme d'installation et suivez les instructions à l'écran pour effectuer la mise à niveau.

Migration d'un annuaire depuis ACC vers VMware Identity Manager Connector

6

Les clients de l'espace de travail ONE ayant déployé la synchronisation Active Directory avec VMware Identity Manager en utilisant uniquement leurs connecteurs ACC existant doivent suivre une procédure de migration s'ils souhaitent tirer parti des fonctionnalités supplémentaires incluses avec le composant VMware Identity Manager Connector du Enterprise Systems Connector. Cette procédure à usage unique convertit le répertoire ACC de type Autre en un répertoire de type Active Directory via LDAP ou Active Directory (authentification Windows intégrée), qui sont associés au VMware Identity Manager Connector. Cette procédure ne supprime pas le répertoire existant ou tous les droits d'accès qui lui sont associés.

Remarque Le modèle unique ACC de synchronisation d'annuaire et authentification avec VMware Identity Manager est toujours disponible et pris en charge en mettant simplement à jour l'ACC par la suite. La procédure de migration est uniquement nécessaire si vous souhaitez bénéficier des nouvelles fonctionnalités.

La conversion de l'autre annuaire comprend les tâches suivantes.

1 Convertissez l'autre annuaire Active Directory sur LDAP ou Active Directory (authentification Windows intégrée).

2 Configurez si nécessaire les méthodes d'authentification supplémentaires de connecteur VMware Identity Manager pour le répertoire. La méthode d'authentification de mot de passe est disponible par défaut.

3 Modifier la stratégie par défaut et les stratégies personnalisées pour utiliser le mot de passe ou une autre méthode d'authentification de connecteur VMware Identity Manager au lieu de Mot de passe (AirWatch Connector).

4 Arrêtez la synchronisation des utilisateurs et des groupes à partir d'AirWatch vers le répertoire VMware Identity Manager.

Ce chapitre aborde les rubriques suivantes :

Convertir un autre répertoire vers Active Directory sur LDAP ou Active Directory (authentification Windows intégrée)

Vous pouvez convertir un répertoire de type Autre, qui stocke les utilisateurs et groupes synchronisés à partir d'AirWatch, dans un répertoire de type Active Directory via LDAP ou Active Directory (authentification Windows intégrée), qui sont associés avec le connecteur VMware Identity Manager. Après la conversion du répertoire, le connecteur VMware Identity Manager est utilisé au lieu d'ACC afin de synchroniser les utilisateurs et groupes à partir de votre annuaire d'entreprise à VMware Identity Manager.

Prérequis

- Installez et activez le composant VMware Identity Manager Connector du VMware Enterprise Systems Connector sur un serveur Windows.

  Pour utiliser certaines fonctionnalités, le serveur Windows doit être joint au domaine, vous devez installer le composant VMware Identity Manager Connector en tant qu'utilisateur de domaine faisant partie du groupe d'administrateurs sur le serveur Windows, et vous devez choisir d'exécuter le service IDM Connector en tant qu'utilisateur de domaine Windows.

  Cette exigence s'applique aux cas suivants.

  - Si vous prévoyez de convertir le répertoire Autre en Active Directory (authentification Windows intégrée)
  - Si vous prévoyez d'utiliser l'authentification Kerberos
  - Si vous prévoyez d'intégrer Horizon View à VMware Identity Manager et que vous souhaitez utiliser les options Effectuer la synchronisation de l'annuaire ou Configuration du serveur de connexion 5.x.
- Les informations d'Active Directory ci-dessous sont requises :
  - Si vous convertissez vers Active Directory via LDAP, le nom unique de base, le nom unique de liaison et le mot de passe de nom unique de liaison sont requis. Il est recommandé d'utiliser un compte d'utilisateur de nom unique de liaison avec un mot de passe sans date d'expiration.
  - Si vous convertissez vers Active Directory (Authentification Windows intégrée), l'adresse UPN de l'utilisateur Bind et le mot de passe du domaine sont requis. Il est recommandé d'utiliser un compte d'utilisateur de nom unique de liaison avec un mot de passe sans date d'expiration.
  - Si Active Directory requiert un accès via SSL ou STARTTLS, le certificat d'autorité de certification racine du contrôleur de domaine Active Directory est requis.
  - Pour Active Directory (authentification Windows intégrée), lorsque vous avez configuré un annuaire Active Directory à forêts multiples et que le groupe local du domaine contient des membres de domaines provenant de différentes forêts, assurez-vous que l'utilisateur Bind est ajouté au groupe Administrateurs du domaine dans lequel se trouve le groupe local du domaine. Sinon, ces membres ne seront pas présents dans le groupe local du domaine.

Procédure

1. Dans la console d'administration VMware Identity Manager, cliquez sur l'onglet **Gestion des identités et des accès**, puis sur l'onglet **Répertoires**.
2. Cliquez sur le nom du journal que vous souhaitez personnaliser.
3. Dans la page répertoire, cliquez sur le bouton **Convertir** .
4. Dans la page Ajouter un annuaire, modifiez le nom du répertoire si nécessaire et sélectionnez le type d'annuaire vers lequel vous souhaitez convertir l'autre annuaire **Active Directory via LDAP** ou **Active Directory (authentification Windows intégrée)**.

5 Entrez les informations de connexion Active Directory et continuez avec l'assistant pour configurer le répertoire.

Pour plus d'informations, reportez-vous à la section « Configuration de la connexion au service d'Active Directory » du guide *Intégration d'annuaire avec VMware Identity Manager*.

Suivez ces instructions.

- Dans le champ **Connecteur de synchronisation**, sélectionnez le connecteur VMware Identity Manager que vous avez installé.
- Dans la section **Synchronisation d'annuaire et authentification**, sélectionnez **Oui** pour l' **Authentification**, sauf si vous prévoyez d'utiliser un fournisseur d'identité tiers au lieu du connecteur pour l'authentification.
- Assurez-vous de configurer le répertoire converti comme l'annuaire AirWatch afin qu'il ait la même structure de répertoires. Sélectionnez les mêmes domaines. Lorsque vous spécifiez les utilisateurs et les groupes à synchroniser, effectuez les mêmes sélections que le répertoire AirWatch afin que les mêmes utilisateurs et groupes soient synchronisés avec l'annuaire convertie.

6 Sur la dernière page de l'Assistant, cliquez sur **Synchroniser l'annuaire**.

Le répertoire est converti et configuré pour utiliser le connecteur VMware Identity Manager. Un fournisseur d'identité de Workspace est créé, si une n'existe pas déjà, et le répertoire lui est associé automatiquement. La méthode d'authentification de mot de passe est déjà activée pour le répertoire.

7 (Facultatif) Pour activer les autres méthodes d'authentification pour le répertoire, procédez comme suit.

a Dans l'onglet **Identité et gestion de l'accès**, cliquez sur **Configuration**.

b Sur la page connecteurs, localisez le connecteur et le travailleur auquel le répertoire converti est associé et cliquez sur le lien dans la colonne **Travailleur**.

c Dans la page travailleur, cliquez sur l'onglet **Adaptateurs d'authentification** .

d Configurez et activez les adaptateurs d'authentification que vous voulez utiliser en cliquant sur leurs liens et en entrant les informations de configuration.

Pour plus d'informations sur la configuration des adaptateurs d'authentification, reportez-vous à la section *Administration de VMware Identity Manager*.

8 Modifier la default_access_policy_set et toute stratégie personnalisée pour sélectionner les méthodes d'authentification de connecteur VMware Identity Manager au lieu de Mot de passe (AirWatch Connector).

a Dans l'onglet **Identité et gestion de l'accès**, cliquez sur l'onglet **Répertoires**.

b Cliquez sur **Modifier la stratégie par défaut**.

c Sous **Règles de stratégie**, modifiez la colonne **Méthodes d'authentification** pour chaque règle et remplacez le **mot de passe (AirWatch Connector)** avec le **mot de passe**, qui est une méthode d'authentification de connecteur VMware Identity Manager.

d Cliquez de nouveau sur l'onglet **Stratégies** et modifiez les stratégies personnalisées, le cas échéant, à utiliser le mot de passe ou tout autre VMware Identity Manager méthode d'authentification de connecteur que vous avez configuré.

Important Si vous ne changez pas le mot de passe (Airwatch Connector) au mot de passe ou une autre méthode d'authentification basée sur le connecteur VMware Identity Manager , les utilisateurs du répertoire converti ne seront pas en mesure de se connecter.

Suivant

Arrêtez la synchronisation d'annuaire à partir d'AirWatch vers le répertoire converti.

Arrêtez la synchronisation d'annuaire à partir d'AirWatch à VMware Identity Manager

Une fois que vous convertissez l'autre annuaire vers Active Directory via LDAP ou Active Directory (authentification Windows intégrée) et l'associez à un connecteur VMware Identity Manager, le connecteur VMware Identity Manager est utilisé pour synchroniser les utilisateurs et les groupes à partir de votre annuaire d'entreprise dans le répertoire converti. Vous devez arrêter la synchronisation d'utilisateur et de groupe à partir d'AirWatch vers l'annuaire VMware Identity Manager.

Procédure

1 Dans la console AirWatch, accédez à votre groupe d'organisation.

2 Accédez à la page **Paramètres & groupes > Tous les paramètres > Système > Intégration d'entreprise > VMware Identity Manager**.

3 Cliquez sur le bouton **Supprimer** en bas de la page.

La conversion du répertoire est terminée. Les utilisateurs et groupes sont désormais synchronisés à partir de votre annuaire d'entreprise pour le service VMware Identity Manager par le connecteur VMware Identity Manager. Les utilisateurs peuvent continuer à se connecter et accéder à leurs applications.

Remarque Après la conversion du répertoire, si le nom de domaine est différent du nom de domaine NETBIOS, le nom de domaine affiché sur la page de connexion peut être différent. Avec la synchronisation AirWatch, le nom de domaine NETBIOS s'affiche. Avec la synchronisation du connecteur VMware Identity Manager, le nom de domaine s'affiche.

Index

R

S

V