Configurer la gestion des mots de passe à l'aide de LDAP pour RA VPN sur FTD géré par FMC

Table des matières

Introduction Conditions préalables **Exigences** Composants utilisés Configuration Diagramme et scénario du réseau Déterminer le DN de base LDAP et le DN de groupe Copier la racine du certificat SSL LDAPS En cas d'installation de plusieurs certificats dans le magasin de l'ordinateur local sur le serveur LDAP (facultatif) **Configurations FMC** Vérifier les licences Configurer le domaine Configurer AnyConnect pour la gestion des mots de passe **Déploiement Configuration finale Configuration AAA Configuration AnyConnect** Vérification Connexion à AnyConnect et vérification du processus de gestion des mots de passe pour la connexion utilisateur Dépannage Déboguages Débogages de gestion des mots de passe Erreurs courantes rencontrées lors de la gestion des mots de passe

Introduction

Ce document décrit la configuration de la gestion des mots de passe à l'aide de LDAP pour les clients AnyConnect se connectant à Cisco Firepower Threat Défense (FTD).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- · Connaissances de base de la configuration VPN d'accès à distance (VPN) sur FMC
- · Connaissances de base de la configuration du serveur LDAP sur FMC
- · Connaissances de base d'Active Directory

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Serveur Microsoft 2012 R2
- FMCv 7.3.0
- FTDv exécutant 7.3.0

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Configuration

Diagramme et scénario du réseau



Le serveur Windows est préconfiguré avec ADDS et ADCS afin de tester le processus de gestion des mots de passe utilisateur. Dans ce guide de configuration, ces comptes utilisateur sont créés.

Comptes utilisateurs:

- Administrateur : il est utilisé comme compte d'annuaire afin de permettre au FTD de se lier au serveur Active Directory.
- admin : compte d'administrateur de test utilisé pour démontrer l'identité de l'utilisateur.

Déterminer le DN de base LDAP et le DN de groupe

1. Open (ouvert) Active Directory Users and Computers via le tableau de bord du Gestionnaire de serveur.

Server Ma	nager • Dashboard		
I Local Server Local Server All Servers AD DS 과 AD DS 과 AD FS Comparison File and Storage Services 이 IIS 이 IIS 아 NAP	CUICK START CUICK START CUICK START C Add roles and features Add roles and features Add roles and features Add roles and features C Add roles	Active Directory Module for Windows PowerShell Active Directory Dises and Services Active Directory Users and Computers AD F5 Management AD5 Edit Certification Authority Component Services Computer Management Defragment and Optimize Drives DNS Event Viewer Group Policy Management Health Registration Authority Internet Information Services (IIS) Manager (ICS) Initiator Local Security Policy	
	Role: 7 Server group: 1 Servers total: 1 AD CS Manageability Events Services Performance BPA results 	1 AD FS 1 Image ability Image ability Events Events Services Services Performance BPA results	Network Policy Server OBC Data Sources (32-bit) ODBC Data Sources (32-bit) ODBC Data Sources (32-bit) ODBC Data Sources (32-bit) ODBC Data Sources (32-bit) Man Resource Monitor Even Services Servit Services Servit System Information BPA Task Scheduler Windows Firewall with Advanced Security Windows Memory Diagnostic Windows PowerShell
	IIS 1 • Manageability • Manageability Events • Manageability Services Performance BPA results BPA results	1 Imageability Imageability Imageability Events Services Performance BPA results BPA results	Windows PowerShell (k86) Windows PowerShell ISE Windows PowerShell ISE Windows Server Backup Windows Server Backup

2. Ouvrez le view Option sur le panneau supérieur et activez l'option Advanced Features, comme l'illustre l'image :

Active Directory	Users and Computers	_ 🗆 X
File Action View Help		
< i Add/Remove Columns		
Active Direc Large Icons	n	
Saved Q Small Icons	ntainer for up	
	ntainer for do	
Contacts, Groups, and Computers as containers	ntainer for sec	
Fore Advanced Features	ntainer for or ntainer for ma	
Lost Filter Options	ation for stor	
Prog Customize	tem settings	
> Image: Source of the second seco		
Displays items in a list.		

3. Cela permet d'afficher des propriétés supplémentaires sous les objets Active Directory. Par exemple, afin de trouver le DN pour la racine razor.local, clic droit razor.local, puis choisissez Properties, comme le montre cette image :



4. Sous Properties, sélectionnez la commande Attribute Editor s'affiche. Rechercher distinguishedName sous Attributs, puis cliquez sur View, comme l'illustre l'image.

Une nouvelle fenêtre s'ouvre, dans laquelle le nom distinctif (DN) peut être copié et collé dans FMC ultérieurement.

Dans cet exemple, le DN racine est DC=razor, DC=local. Copiez la valeur et enregistrez-la pour plus tard. Cliquer ok afin de quitter la fenêtre Éditeur d'attributs de chaîne et cliquez sur ok afin de quitter les Propriétés.

raz	zor.local Properties ?	x			
General Managed By Ob	oject Security Attribute Editor				
Attributes:					
Attribute	Value	~			
defaultLocalPolicyObj	<not set=""></not>				
description	<not set=""></not>				
desktopProfile	<not set=""></not>	=			
displayName	<not set=""></not>				
displayNamePrintable	<not set=""></not>				
distinguishedName	DC=razor,DC=local				
domainPolicyObject	<not set=""></not>				
domainReplica	<not set=""></not>				
dSASignature	{ V1: Flags = 0x0; LatencySecs = 0; DsaGuid				
dSCorePropagationD	0x0 = ()				
eFSPolicy	<not set=""></not>				
extensionName	<not set=""></not>				
flags	<not set=""></not>				
forceLogoff	(never)	~			
< 111	>				
View	Filter				
Stri	String Attribute Editor				
Attribute: distinguish	Attribute: distinguishedName				
Value:					
DC=razor,DC=local					
Clear	OK Cano	el			

Copier la racine du certificat SSL LDAPS

1. Presse Win+R et entrez mmc.exe, puis cliquez sur OK, comme le montre cette image.



2. Naviguez jusqu'à File > Add/Remove Snap-in..., comme le montre cette image :

🖥	Console1 - [Console Root]	_ D X
File Action View Favorites Window Help		_ 8 ×
New Ctrl+N		
Open Ctrl+O	Actions	
Save Ctrl+S	There are no items to show in this view. Console Roo	ot 🔺
Save As	More Actio	ons 🕨
Add/Remove Snap-in Ctrl+M		
1 C:\Windows\system32\dsa		
3 C:\Windows\system32\certmar		
4 C:\Windows\system32\certsrv		
Exit		
Enables you to add snap-ins to or remove them from the snap	p-in console.	

3. Sous Composants logiciels enfichables disponibles, sélectionnez Certificates puis cliquez sur Add, comme le montre cette image :

nap-in	Vendor	^	Co	nsole Root	Edit Extensions
Active Directory Do	Microsoft Cor				Remove
Active Directory Site	Microsoft Cor				Demove
Active Directory Use	Microsoft Cor				
ActiveX Control	Microsoft Cor				Move Up
ADSI Edit	Microsoft Cor				Move Down
Authorization Manager	Microsoft Cor		Add >		Linke Fouri
Certificate Templates	Microsoft Cor				
Certificates	Microsoft Cor				
Certification Authority	Microsoft Cor				
Component Services	Microsoft Cor				
Computer Managem	Microsoft Cor				
Device Manager	Microsoft Cor				
PDisk Management	Microsoft and				A discound of

4. Choisir Computer account puis cliquez sur Next, comme le montre cette image :

Certificates snap-in	\times
This snap-in will always manage certificates for: <u>Service account</u> <u>Service account</u>	
< <u>B</u> ack <u>N</u> ext > Cancel	

Comme indiqué ici, cliquez sur Finish.

Select Computer	Х
Select the computer you want this snap-in to manage. This snap-in will always manage: Local computer: (the computer this console is running on) Another computer:	
< Back Finish Cancel	

5. Maintenant, cliquez sur ${\rm o}\kappa,$ comme le montre cette image.

nap-in	Vendor	^		Console Root	Edit Extensions
Active Directory Do	Microsoft Cor			up Certificates (Local Computer,	Bemove
Active Directory Site	Microsoft Cor				
Active Directory Use	Microsoft Cor				Maualla
ACTIVEX CONTROL	Microsoft Cor				Hove Go
AUSI Euro Authorization Manage	Microsoft Cor				Move Down
Certificate Templates	Microsoft Cor		<u>A</u> dd >		
Certificates	Microsoft Cor				
Certification Authority	Microsoft Cor				
Component Services	Microsoft Cor				
Computer Managem	Microsoft Cor				
Device Manager	Microsoft Cor				
Disk Management	Microsoft and	~			Advanced

- 6. Développez le Personal, puis cliquez sur Certificates. Le certificat utilisé par les LDAP doit être délivré au nom de domaine complet (FQDN) du serveur Windows. Sur ce serveur, trois certificats sont répertoriés :
- Un certificat CA a été délivré à et par razor-WIN-E3SKFJQD6J7-CA.
- Un certificat CA délivré à et par supinfo-WIN-FNJVP9QUEH9-CA.
- Un certificat d'identité a été délivré à WIN-E3SKFJQD6J7.razor.local par razor-WIN-E3SKFJQD6J7-CA.

Dans ce guide de configuration, le nom de domaine complet est WIN-E3SKFJQD6J7.razor.local Les deux premiers certificats ne sont donc pas valides pour être utilisés comme certificat SSL LDAP. Le certificat d'identité délivré à WIN-E3SKFJQD6J7.razor.local est un certificat qui a été émis automatiquement par le service AC de Windows Server. Double-cliquez sur le certificat afin de vérifier les détails.



- 7. Pour être utilisé comme certificat SSL LDAP, le certificat doit répondre aux exigences suivantes :
- Le nom commun ou le nom secondaire de l'objet DNS correspond au nom de domaine complet de Windows Server.
- Le certificat dispose de l'authentification serveur dans le champ Enhanced Key Usage.

Sous la Details pour le certificat, sélectionnez Subject Alternative Name, où le nom de domaine complet WIN-E3SKFJQD6J7.razor.local est présent.

Cer	tificate	x		
General Details Certification Path				
Show: <all></all>	~			
Field	Value			
Enhanced Key Usage	Client Authentication (1.3.6.1			
Application Policies	[1]Application Certificate Polic			
Subject Key Identifier	1b 34 75 f8 c4 3e ef 58 fb 43			
Authority Key Identifier	KeyID=cf 83 92 a4 14 00 e7 5	_		
CRL Distribution Points	[1]CRL Distribution Point: Distr	_		
Authority Information Access	[1]Authority Info Access: Acc	=		
🙀 Key Usage	Digital Signature, Key Encipher			
Subject Alternative Name	DNS Name=WIN-E3SKFJQD6J	~		
DNS Name=WIN-E3SKFJQD6J7.raz	or.local			
DNS Name=razor.local DNS Name=RAZOR				
J		- 1		
E	dit Properties Copy to File			
Learn more about certificate dotaile				
Learn more about <u>ceruncate details</u>				
	OK			

Sous Enhanced Key Usage, Server Authentication est présent.

Cer	tificate	x		
General Details Certification Path				
Show: <all></all>	~			
Field	Value	~		
Certificate Template Inform	Template=LDAPoverSSL(1.3.6			
🐻 Enhanced Key Usage	Client Authentication (1.3.6.1			
Application Policies	[1]Application Certificate Polic			
🛐 Subject Key Identifier	1b 34 75 f8 c4 3e ef 58 fb 43			
Authority Key Identifier	KeyID=cf 83 92 a4 14 00 e7 5	=		
CRL Distribution Points	[1]CRL Distribution Point: Distr			
Authority Information Access	[1]Authority Info Access: Acc			
Key Usage	Digital Signature, Key Encipher	~		
Client Authentication (1.3.6.1.5.5.7.3.2) Server Authentication (1.3.6.1.5.5.7.3.1) Smart Card Logon (1.3.6.1.4.1.311.20.2.2) KDC Authentication (1.3.6.1.5.2.3.5)				
Edit Properties Copy to File Learn more about certificate details				
	OK			

8. Une fois que cela est confirmé, sous la rubrique Certification Path , choisissez le certificat de niveau supérieur qui est le certificat d'autorité de certification racine, puis cliquez sur view Certificate. Les détails du certificat pour le certificat de l'autorité de certification racine s'ouvrent comme indiqué dans l'image :

Certificate	x	Certificate X
General Details Certification Path Certification path area razor-WIN-E3SKFJQD6J7-CA WIN-E3SKFJQD6J7.razor.local		General Details Certification Path Image: Certificate Information This certificate is intended for the following purpose(s): • All issuance policies • All application policies
View Certificate		Issued to: razor-WIN-E3SKFJQD6J7-CA Issued by: razor-WIN-E3SKFJQD6J7-CA
Certificate status: This certificate is OK.		Valid from 3/22/2021 to 3/22/2026
Learn more about <u>certification paths</u>		Issuer Statement
ОК		OK

9. Sous la Details du certificat CA racine, cliquez sur Copy to File et naviguez à travers leCertificate Export Wizard qui exporte la CA racine au format PEM.

Choisir Base-64 encoded X.509 comme format de fichier.

e 🦻	Certificate Export Wizard		
	Completing the Certificate Exp	oort Wizard	
	You have successfully completed the Certificate	Export wizard.	
	You have specified the following settings:		
	File Name	C:\Users\Administrator\Downloads\roo	
	Export Keys	No	
	Include all certificates in the certification path	No	
	File Format	Base64 Encoded X.509 (*.cer)	
	< 111	>	
		Finish C	ancel

10. Ouvrez le certificat d'autorité de certification racine stocké à l'emplacement sélectionné sur la machine à l'aide d'un bloc-notes ou d'un autre éditeur de texte.

Affiche le certificat de format PEM. Enregistrez ceci pour plus tard.

----BEGIN CERTIFICATE-----

MIIDfTCCAmWgAwIBAgIQV4ymxtI3BJ9JHnDL+luYazANBgkqhkiG9w0BAQUFADBRMRUwEwYKCZImiZPyLGQBGRYFbG9jYWwxFTATBgovcjEhMB8GA1UEAxMYcmF6b3ItV010LUUzU0tGS1FENko3LUNBMB4XDTIxMDMyMjE0MzMxNVoXDTI2MDMyMjE0NDMxNVowUTEVMBMGCguBWxvY2FsMRUwEwYKCZImiZPyLGQBGRYFcmF6b3IxITAfBgNVBAMTGHJhem9yLVdJTi1FM1NLRkpRRDZKNy1DQTCCASIwDQYJKoZIhvcGCAQoCggEBAL803nQ6xPpazjj+HBZYc+8fV++RXCG+cUnb1xwtX0B2G4UxZ3LRrWznjXaS02Rc3qVw41n0AziGs4ZMNM1X8UWeKuwi8W9dkncZaGtQ1cPmqcnCWunfTsaENKbgoKi4eXjpwwUSbEYwU30aiiI/tp422ydy3Kg17Iqt1s4XqpZmTezykWra7dUyXfkuESk61E0AVCCSkTQTRXYryy8dJrWjAF/n6A3VnS/17Uhuj1x4CD20BkfQy6p5HpGxdc4GMTTnDzUL46ot6imeBXPHF0IJehh+tZk3bxpoxTDXECAwEDAgGGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR00BBYEFM+DkqQUA0dY379NnViaMIJAVTZ1MBAGCSsGAQQBgjcVAQQDAgEAMA0GCSqGSIAA41BAQCiSm5U7U6Y7zXdx+d1eJd0QmGgKayAAuYAD+MWNwC4NzFD8Yr7Bn06f/VnF6VGYPXa+Dvs7VLZewMNkp3i+VQpkBCKdhAV6q4sMZffbVrG1Rz7twW36J5G5vhNUhzZ1N20Lw6wtHg2S08X1vpTS5fAnyCZgSK3VPKfXnn1HLp7UH5/SWN2JbPL15r+wCW84b8nry1bGuDsepY7/u2uWfy/vpTJigeok2DH6HFf0ET3sE+7rsIAY+of0kWW5gNwQ4h0wv4Goqj+YQRAXXi2OZy1tHR1dfUUbwVENSFQtDnFA7X

En cas d'installation de plusieurs certificats dans le magasin de l'ordinateur local sur le serveur LDAP (facultatif)

1. Dans une situation de certificats d'identité multiples qui peuvent être utilisés par LDAPS et lorsqu'il y a une incertitude quant à savoir lequel est utilisé, ou lorsqu'il n'y a pas d'accès au serveur LDAPS, il est toujours possible d'extraire l'autorité de certification racine d'une capture de paquets effectuée sur le FTD.

2. Dans le cas où vous avez plusieurs certificats valides pour l'authentification du serveur dans le magasin de certificats de l'ordinateur local du serveur LDAP (tel que le contrôleur de domaine AD DS), il peut être remarqué qu'un certificat différent est utilisé pour les communications LDAP. La meilleure solution à ce problème consiste à supprimer tous les certificats inutiles du magasin de certificats de l'ordinateur local et à n'avoir qu'un seul certificat valide pour l'authentification du serveur.

Toutefois, s'il existe une raison légitime pour laquelle vous avez besoin de deux certificats ou plus et que vous disposez au moins d'un serveur LDAP Windows Server 2008, le magasin de certificats des services de domaine Active Directory (NTDS\Personal) peut être utilisé pour les communications LDAP.

Ces étapes montrent comment exporter un certificat compatible LDAPS d'un magasin de certificats d'ordinateur local de contrôleur de domaine vers le magasin de certificats de service des services de domaine Active Directory (NTDS\Personal).

- Accédez à la console MMC sur le serveur Active Directory, sélectionnez Fichier, puis cliquez sur Add/Remove Snap-in.
- Cliquer Certificates puis cliquez sur Add.
- Dans la Certificates snap-in, choisissez Computer account puis cliquez sur Next.
- Dans Select Computer, choisissez Local Computer, cliquez sur OK, puis cliquez sur Finish. Dans Add or Remove Snap-ins, cliquez sur OK.
- Dans la console des certificats d'un ordinateur qui contient un certificat utilisé pour l'authentification du serveur, cliquez avec le bouton droit sur le certificate, cliquez sur All Tasks, puis cliquez sur Export.

E	nsole1 - [Console Root\Certificates (Local C	omputer)\Personal\Certificates]	_ D X
🚟 File Action View Favorites Windo	Help		_ 8 ×
🗢 🄿 🖄 📰 🐇 🖬 😹 🖬			
Console Root	Issued To Issued By	Expiration Date	Actions
△ 💭 Certificates (Local Computer)	arazor-WIN-E3SKFJQD6J7-CA razor-WIN-E3SK	JQD6J7-CA 3/22/2026	Certificates
Certificates	supinto-WIN-FNJVP9QUEH9-CA supinto-WIN-FN	JVP9QUEH9-CA 2/23/2025	More Actions
Trusted Root Certification Autho		Open	WIN-E3SKEIOD617 razor local
Enterprise Trust Intermediate Certification Author		All Tasks Op	en 🕨
Trusted Publishers		Cut Re	quest Certificate with New Key
Untrusted Certificates		Copy Re	new Certificate with New Key
Third-Party Root Certification Au		Delete Ma	anage Private Keys
Client Authentication Issuer		Properties Ad	vanced Operations
Client Authentication issuers Other People			· · · · ·
Remote Desktop		Help	port
Certificate Enrollment Requests			
Smart Card Trusted Roots			
Trusted Devices			
Web Hosting			
	III	>	
Export a certificate			

• Exporter le certificat dans le pfx dans les sections suivantes. Référez-vous à cet article pour savoir comment exporter un certificat dans le pfx format à partir de MMC :

https://www.cisco.com/c/en/us/support/docs/security/web-security-appliance/118339-technote-wsa-00.html.

- Une fois l'exportation du certificat terminée, accédez à Add/Remove Snap-in activé MMC console. Cliquer Certificates puis cliquez sur Add.
- Choisir Service account puis cliquez sur Next.

Certificates snap-in	X
This snap-in will always manage certificates for:	
Service account O Computer account	

- Dans la Select Computer, choisissez Local Computer et cliquez sur Next.
- Choisir Active Directory Domain Services puis Cliquez sur Finish.

Certificates	s snap-in
Select a service account to manage on the local co	omputer.
Active Directory Certificate Services Active Directory Domain Services Active Directory Web Services AD FS Windows Service Application Experience Application Host Helper Service Application Identity Application Information Application Layer Gateway Service Application Management ASP.NET State Service Background Intelligent Transfer Service Background Tasks Infrastructure Service Base Filtering Engine	
	< Back Finish Cancel

- Sur la page Add/Remove Snap-ins , cliquez sur OK.
- Accroissement Certificates Services (Active Directory Domain Services) puis cliquez sur NTDS\Personal.
- Cliquer avec le bouton droit NTDS\Personal, cliquez sur All Tasks, puis cliquez sur Import.

Console1 - [Console Roo	ot\Certificates - Service (Active Directory Domain Services) on Local Compu	ter\NTDS\Personal]
🚟 File Action View Favorites Window H	Help	_ & ×
🗢 🌳 🗖 📰 📋 🖻 📑		
Console Root OI	bject Type	Actions
Certificates (Local Computer)	Certificates	NTDS\Personal
Certificates - Service (Active Directory D		More Actions
▶ 🔂 NT Find Certificates		
▶ 🗂 NT All Tasks	Find Certificates	
NT View	Import	
New Window from Here	Advanced Operations	
New Taskpad View		
NT Refresh		
Export List		
Help		
< III >]
Add a certificate to a store		

- Sur la page Certificate Import Wizard écran de bienvenue, cliquez sur Next.
- Dans l'écran Fichier à importer, cliquez sur Browseet localisez le fichier de certificat que vous avez exporté précédemment.
- Dans l'écran Ouvrir, vérifiez que l'échange d'informations personnelles (*pfx,*.p12) est sélectionné comme type de fichier, puis parcourez le système de fichiers pour localiser le certificat que vous avez exporté précédemment. Cliquez ensuite sur ce certificat.

	Oper	n			x			
€ 🕘 ▼ ↑ 📑 ኑ Lib	raries > Documents		✓ ♂ Search Documents					
Organize 👻 New folder				•== •				
🔆 Favorites	Name	Date modified	Туре	Size				
Desktop	🦻 Idapcert	4/25/2022 12:01	Personal Informati	5 KB				
i Downloads 🗿 Recent places								
詞 Libraries								
Documents								
J Music								
Pictures								
Computer								
🙀 Network								
File na	me: Idapcert		✓ Persona	Information Exc	hange 🗸			
			Op	en Ca	ancel			

- Cliquer Open puis cliquez sur Next.
- Dans l'écran Mot de passe, entrez le mot de passe que vous avez défini pour le fichier, puis cliquez sur Next.
- Sur la page Magasin de certificats, assurez-vous que l'option Placer tous les certificats est sélectionnée et lisez Magasin de certificats : NTDS\Personal puis cliquez sur Next.

€	🕖 Certificate Import Wizard								
	Certificate Store								
	Certificate stores are system areas where certificates are kept.								
	Windows can automatically select a certificate store, or you can specify a location for the certificate.								
	\bigcirc Automatically select the certificate store based on the type of certificate								
	Iace all certificates in the following store								
	Certificate store:								
	NTDS\Personal Browse								
	Learn more about <u>certificate stores</u>								
	Next Cancel								

х

• Sur la page Certificate Import Wizard écran de fin, cliquez sur Finish. Un message s'affiche pour indiquer que l'importation a réussi. Cliquer OK. Le certificat a été importé sous le magasin de certificats : NTDS\Personal.

Console1 - [Console Root\Certific	ates - Service (Active Directory	Domain Services) on Local C	Computer\NTDS\Pe	ersonal\Certificates]	_ 🗆 X
藩 File Action View Favorites Window	/ Help				_ & ×
🗢 🤿 🖄 📰 🔏 🖏 🔀 🖬 🖉					
Console Root	Issued To 📩	Issued By	Expiration Date	Actions	
Certificates (Local Computer)	razor-WIN-E3SKFJQD6J7-CA	razor-WIN-E3SKFJQD6J7-CA	3/22/2026	Certificates	
Certificates - Service (Active Directory D Image: A Image: Active Directory D Image: A Image: Active Directory D Image: Active D Image: Actined D Image: Active D Image: Active D Image: Active D	WIN-E3SKFJQD6J7.razor.local	razor-WIN-E3SKFJQD6J7-CA	4/25/2023	More Actions	•
Certificates				WIN-E3SKFJQD6J7.r	azor.local 🔺
NIDS\Trusted Koot Certification Au MTDS\Enterprise Trust MTDS\Intermediate Certification Au MTDS\Intermediate Certificates MTDS\Untrusted Publishers MTDS\Third-Party Root Certification MTDS\Trusted People MTDS\Client Authentication Issuers				More Actions	,
< <u> </u>	< III		>		
NTDS\Personal store contains 2 certificates.					

Configurations FMC

Vérifier les licences

Pour déployer la configuration AnyConnect, le FTD doit être enregistré auprès du serveur de licences Smart et une licence Plus, Apex ou VPN Only valide doit être appliquée au périphérique.

Configurer le domaine

1. Naviguez jusqu'à System > Integration. Naviguez jusqu'à Realms, puis cliquez sur Add Realm, comme le montre cette image :

Overview Analy	ysis Policies D	Devices Objects	AMP Intelligence									%	Deploy Sy	stem Help 🔻	admin 🔻
						Configuration	Users	Domains	Integration	Updates	Licenses v	Logging v	Health •	¹ Monitoring •	Tools •
	3								2						
Cloud Services	Realms	Identity Sources	High Availability	eStreamer	Host Input Client	Smart Software Man	ager On-I	Prem							
Realms	Realm Sequences	s Sync Results													4
													Compa	re Realms	id Realm
Name -	Description	-				AD Delevery Demail	-		Base DN				Charles		

2. Remplissez les champs affichés en fonction des informations collectées à partir du serveur Microsoft pour les LDAP. Avant cela, importez le certificat d'autorité de certification racine qui a signé le certificat de service LDAP sur le serveur Windows sous Objects > PKI > Trusted CAs > Add Trusted CA, car il est référencé dans la sectionDirectory Server Configuration du royaume. Une fois terminé, cliquez sur ok.

Firepower Manag Objects / Object Manage	ement Center Overview Analy	sis Policies Devices Objects AMP Intelligence		Deploy Q 🚱 🔅 (admin 🔹
AAA Server Access List Address Pools Application Elitere	Trusted CAs Trusted certificate authority (CA) object	represents a CA public key certificate belonging to a trusted CA. You can use e	xternal CA objects in	Add Trusted CA Q. Filter SSL policy, realm configurations and ISE/ISE-PIC connection	on.
AS Path Cipher Suite List Community List	Name ISRG-Root-X1 Izence.com			Value CN=ISRG Root X1, ORG=Internet Security Research G CN=Izenoe.com, ORG=IZENPE S.A., C=ES	11
DNS Server Group External Attributes Eile List	LDAPS-ROOT-CERT Microsec-e-Szigno-Root-CA-2009	Edit Trusted Certificate Authority	0	CN=razor-WIN-E3SKFJQD6J7-CA CN=Microsec e-Szigno Root CA 2009, ORG=Microse	11
FlexConfig Geolocation Interface	NetLock-Arany-Class-Gold-FAtanAosAtv OISTE-WISeKey-Global-Root-GA-CA	Name: LDAPS-ROOT-CERT		CN=NetLock Arany (Class Gold) FA tanA2sÅtvÅjny, CN=OISTE WISeKey Global Root GA CA, ORG=WISeK	/1
Key Chain Network V PKI	OISTE-WISeKey-Global-Root-GB-CA OISTE-WISeKey-Global-Root-GC-CA	Subject: Common Name: razor-WIN-E3SKFJQD6J7-CA Organization:		CN=OISTE WISeKey Global Root GB CA, ORG=WISeK CN=OISTE WISeKey Global Root GC CA, ORG=WISeK	/1
Cert Enrollment External Cert Groups External Certs	QuoVadis-Root-CA-1-G3 QuoVadis-Root-CA-2	Organization Unit: Issuer: Common Name: razor-WIN-E3SKFJQD6J7-CA		CN=QuoVadis Root CA 1 G3, ORG=QuoVadis Limited, CN=QuoVadis Root CA 2, ORG=QuoVadis Limited, C=	/1
Internal CA Groups Internal CAs Internal Cert Groups	QuoVadis-Root-CA-3 QuoVadis-Root-CA-3-G3	Organization: Organization Unit: Not Valid Before:		CN=QuoVadis Root CA 3, ORG=QuoVadis Limited, C= CN=QuoVadis Root CA 3 G3, ORG=QuoVadis Limited,	11
Internal Certs Trusted CA Groups Trusted CAs	QuoVadis-Root-Certification-Authority Secure-Global-CA	Mar 22 14:33:15 2021 GMT Not Valid After: Mar 22 14:43:15 2026 GMT		CN=QueVadis Root Certification Authority, ORG=QueV CN=Secure Global CA, ORG=SecureTrust Corporation	11
Policy List Port	SecureTrust-CA	Install Certificate Cance	el Save	CN*SecureTrust CA, ORG*SecureTrust Corporation, Displaying 81 - 100 of 125 rows < < Page 5	/ ⊒ 017 > > C

Add New Realm

Name*	Description				
LDAP-Server					
Туре					
LDAP					
Directory Username*	Directory Password*				
Administrator@razor.local					
E.g. user@domain.com					
Base DN*	Group DN*				
DC=razor,DC=local	DC=razor,DC=local				
E.g. ou=group,dc=cisco,dc=com	E.g. ou=group,dc=cisco,dc=com				
Directory Server Configuration					
 WIN-E3SKFJQD6J7.razor.local:636 					
Hostname/IP Address*	Port*				
WIN-E3SKFJQD6J7.razor.local	636				
Encryption	CA Certificate*				
LDAPS	LDAPS-ROOT-CERT V +				
Interface used to connect to Directory server (i)					
Resolve via route lookup					
Choose an interface					
Default: Management/Diagnostic Interface	\sim				
Test					
Add another directory					

0 X

3. Cliquer Test afin de s'assurer que FMC peut se lier correctement avec le nom d'utilisateur et le mot de passe du répertoire fournis à l'étape précédente. Puisque ces tests sont initiés à partir du FMC et non par l'intermédiaire d'une des interfaces routables configurées sur le FTD (comme l'intérieur, l'extérieur, dmz), une connexion réussie (ou échouée) ne garantit pas le même résultat pour l'authentification AnyConnect puisque les demandes d'authentification LDAP AnyConnect sont initiées à partir de l'une des interfaces routables FTD.

Add Directory	@ ×
Hostname/IP Address* WIN-E3SKFJQD6J7.razor.loc	Port* 636
Encryption	CA Certificate*
LDAPS	LDAPS-ROOT-CERT V +
Interface used to connect to Dire Resolve via route lookup Choose an interface Default: Management/Diag Test Test	ctory server i
	Cancel OK

4. Activez le nouveau domaine.

Quere de								•	Dealers	11-1	- 41
Overview Anal	iysis Policies Devices Ob	jects AMP Intelligence						10	Deploy Syst	tem Help +	admin *
				Configuration User	Domains	Integration	Updates Lie	censes • Logging •	Health *	Monitoring *	Tools •
Cloud Service	Realms Identity So	rces High Availability eSt	treamer Host Input Client	Smart Software Manager O	n-Prem						
Realms	Realm Sequences Sync R	esults									
									Compar	e Realms Ad	d Realm
Name +	Description	Туре	Domain	AD Primary Domain		Base DN			State		
AC-Local		LOCAL	Global						C Enable	sd 🕂	/ B 🗑
LDAP		AD	Global	cisco01.com		OU=Users,OU	J=CISCO,DC=cis	sco01,DC=com	C Enable	sd 🛨	/ fa 🗑
LDAP-Server		AD	Global	razor.local		DC=razor,DC	=local		C Enable	sd 🛨 /	/ ¶a 🗑

Configurer AnyConnect pour la gestion des mots de passe

1. Choisissez le profil de connexion existant ou créez-en un nouveau, s'il s'agit d'une configuration initiale d'AnyConnect. Ici, un profil de connexion existant nommé «

AnyConnect-AD » mappé avec l'authentification locale est utilisé.

Overview Analysis Policies Devices Objects AMP Intel	lligence		🎙 Deploy System Help 🔻 admin 🔻
Device Management Device Upgrade NAT VPN > Remote Acce	QoS Platform Settings FlexConfig Certificates		
AnyConnect Enter Description			Save Save
			Policy Assignments (1)
		Local Realm: asa	Dynamic Access Policy: Hostscan
Connection Profile Access Interfaces Advanced			
			0
Name	ААА	Group Policy	
DefaultWEBVPNGroup	Authentication: Mone Authorization: Mone Accounting: Mone	DftGrpPolicy	/ 0
AnyConnect	Authentication: Radius (RADIUS) Authorization: Radius (RADIUS) Accounting: Assoc	DftGrpPolicy	/ 6
AnyConnect-AD	Authentication: LOCAL Authorization: Mone Accounting: Mone	AnyConnect-Group	/ 9

2. Modifiez le profil Connection et mappez le nouveau serveur LDAP configuré aux étapes précédentes, sous les paramètres AAA du profil Connection. Une fois terminé, cliquez sur save dans l'angle supérieur droit.

Firepower Management Center Devices / VPN / Edit Connection Profile	Analysis Policies Devices Objects AMP Intelligence	Deploy 🔍 💕 🌣 🔞 admin 🔻
AnyConnect		Save Cancel
Enter Description		Policy Assignments (1)
Connection Profile Access Interfaces Advanced	Edit Connection Profile	Local Realm: None Dynamic Access Policy: Hostscan
	Connection Profile:* AnyConnect-AD	
	Group Policy:* AnyConnect-Group +	+
Name	Edit Group Policy Client Address Assignment AAA Aliases	
DefaultWEBVPNGroup	Authentication	/1
AnyConnect	Authentication Method: AAA Only v	/1
AnvConnect-AD	Authentication Server: LDAP-Server (AD)	11
	Fallback to LOCAL Authentication	
	Use secondary authentication	
	Authorization	
	Authorization Server: Use same authentication server 🔻	
	Allow connection only if user exists in authorization database Configure LDAP Attribute Map	
	Accounting	
	Accounting Server:	
	 Advanced Settings 	
	Strip Realm from username	
	Cancel Save	

3. Activez la gestion des mots de passe sous AAA > Advanced Settings et enregistrez la configuration.

Overview Analysis Policies Devices Objects AMP Intell Device Management Device Upgrade NAT VPN > Remote Acces	s QoS Platform Settings FlexConfig Certificates	🇛 Deploy System Help + admin +
AnyConnect		Save 🚺 Cancel
samaa sekse genoen		Policy Assignments (1) Local Realm: asa Dynamic Access Policy: <u>Hostscan</u>
Connection Profile Access Interfaces Advanced	Edit Connection Profile ? ×	
Name	Connection Profile:* AnyConnect-AD Group Policy:* AnyConnect-Group Edit Group Policy	0
DefaultWEBVPNGroup	Client Address Assignment AAA Aliases	/ 9
AnyConnect	LDAP-Server (AD)	×8
AnyConnect-AD	Use secondary authentication	/8
	Authorization Authorization Server: Use same authentication server ¥	
sjobs	Allow connection only if user exists in authorization database Configure LDAP Attribute Map	/ 5
	Configure LDAP Attribute Map Accounting Accounting Server: Advanced Settings Strip Group from username Strip Group from username Enable Password Management enable Vase: 1 days prior to password expiration Notify user on the day of password expiration Save Cancel	

Déploiement

1. Une fois la configuration terminée, cliquez sur le boutonDeploy en haut à droite.

Overview	Analysis	Policies	Devices	Objects	AMP	Intelligence

2. Cochez la case en regard de la configuration FTD qui lui est appliquée, puis cliquez sur Deploy, comme le montre cette image :

n Deploy System Help v admin v

Overview	Analysis Policies	Devices Objects	AMP Intelligence						9 Deploy System	Help + admin +
									Deployment	Deployment History
T Q	Search using device	name, user name, type,	group or status						1 device Deploy time:	Estimate Deploy
•	Device		Modified by	Inspect Interruption	Туре	Group	Last Deploy Time	Preview	Status	
> 🛛	10.197.224.190_FT	D1	admin		FTD		May 30, 2022 7:34 AM	₿.	Pending	

Configuration finale

Il s'agit de la configuration affichée dans l'interface de ligne de commande du FTD après le déploiement réussi.

Configuration AAA

<#root>

```
> show running-config aaa-server
```

Configuration AnyConnect

<#root>

```
> show running-config webvpn
```

webvpn

enable Outside

anyconnect image disk0:/csm/anyconnect-win-4.10.01075-webdeploy-k9.pkg 1 regex "Windows"

anyconnect profiles FTD-Client-Prof disk0:/csm/ftd.xml

anyconnect enable

tunnel-group-list enable

cache

no disable

error-recovery disable

```
> show running-config tunnel-group
```

```
tunnel-group AnyConnect-AD type remote-access
tunnel-group AnyConnect-AD general-attributes
address-pool Pool-1
```

authentication-server-group LDAP-Server

default-group-policy AnyConnect-Group

password-management password-expire-in-days 1

tunnel-group AnyConnect-AD webvpn-attributes

group-alias Dev enable

> show running-config group-policy AnyConnect-Group

group-policy

AnyConnect-Group

internal

<----- Group-Policy configuration that is mapped once the user is authenticated</pre>

group-policy AnyConnect-Group attributes

vpn-simultaneous-logins 3

vpn-idle-timeout 35791394

vpn-idle-timeout alert-interval 1

vpn-session-timeout none

vpn-session-timeout alert-interval 1

vpn-filter none

vpn-tunnel-protocol ikev2 ssl-client

<----- LDAPs Serve

<---- Password-management

split-tunnel-network-list value Remote-Access-Allow default-domain none split-dns none split-tunnel-all-dns disable client-bypass-protocol disable vlan none address-pools none webvpn anyconnect ssl dtls enable anyconnect mtu 1406 anyconnect firewall-rule client-interface public none anyconnect firewall-rule client-interface private none anyconnect ssl keepalive 20 anyconnect ssl rekey time none anyconnect ssl rekey method none anyconnect dpd-interval client 30 anyconnect dpd-interval gateway 30 anyconnect ssl compression none anyconnect dtls compression none anyconnect modules value none anyconnect profiles value FTD-Client-Prof type user anyconnect ask none default anyconnect anyconnect ssl df-bit-ignore disable

> show running-config ssl

ssl trust-point ID-New-Cert Outside

<----- FTD ID-cert trustpoint name mapped to the outside interface on which AnyConnect Connections

Vérification

Connexion à AnyConnect et vérification du processus de gestion des mots de passe pour la connexion utilisateur

1. Établissez une connexion au profil de connexion concerné. Une fois qu'il a été déterminé lors de la connexion initiale que le mot de passe doit être modifié puisque le mot de passe précédent a été rejeté par le serveur Microsoft au moment de son expiration, l'utilisateur est invité à modifier le mot de passe.

S Cisco AnyConnect FTD-Hostname		
Group: Dev v Username: edmn Password: [OK Cancel	Cisco AnyConnect Secure Mobility Client - X VPR Contacting FTD-Hosthame. FTD-Hosthame Connect	
Continue	a new strue. © Cisco AnyConnect Secure Mobility Client – × VPIE Contacting FTD-Hostname. FTD-Hostname Continue	
	Care and a second	

2. Une fois que l'utilisateur a entré le nouveau mot de passe de connexion, la connexion est établie avec succès.

🚳 Cisco AnyC	onnect Secure Mobility Client		_		×
	VPN: Connected to FTD-Hostname. FTD-Hostname	~		Disconnec	t
00:02:43					IPv4
\$ (i)					diala cisco

3. Vérifiez la connexion utilisateur sur l'interface de ligne de commande FTD :

```
<#root>
```

FTD_2# sh vpn-sessiondb anyconnect

Session Type: AnyConnect

 Username
 : admin

 Index
 : 7

 <------ Username, IP address assigned information of the client</td>

 Assigned IP
 : 10.1.x.x

 Public IP
 : 10.106.xx.xx

 Protocol
 :

 AnyConnect-Furth SSL-Tunnel

 License
 : AnyConnect-Furth (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES-GCM-256

Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA384

Bytes Tx	:	16316	Bytes Rx	:	2109
Group Policy	:	AnyConnect-Group	Tunnel Group	:	AnyConnect-AD
Login Time	:	13:22:24 UTC Mon Apr 2	5 2022		
Duration	:	Oh:00m:51s			
Inactivity	:	Oh:00m:00s			
VLAN Mapping	:	N/A	VLAN	:	none
Audt Sess ID	:	0ac5e0fa000070006266a09	90		
Security Grp	:	none	Tunnel Zone	:	0

Dépannage

Déboguages

Ce débogage peut être exécuté dans la CLI de diagnostic afin de dépanner les problèmes liés à la gestion des mots de passe : debug ldap 255.

Débogages de gestion des mots de passe

```
<#root>
[24] Session Start
[24] New request Session, context 0x0000148f3c271830, reqType = Authentication
[24] Fiber started
[24] Creating LDAP context with uri=ldaps://10.106.71.234:636
[24] Connect to LDAP server: ldaps://10.106.71.234:636, status = Successful
[24] supportedLDAPVersion: value = 3
[24] supportedLDAPVersion: value = 2
[24] Binding as *****@razor.local
[24] Performing Simple authentication for *****@razor.local to 10.106.71.234
[24] LDAP Search:
```

Base DN = [DC=razor,DC=local]

Filter = [sAMAccountName=admin]

Scope = [SUBTREE]

[24] User DN = [CN=admin,CN=Users,DC=razor,DC=local]

[24] Talking to Active Directory server 10.106.71.234

[24] Reading password policy for admin, dn:CN=admin,CN=Users,DC=razor,DC=local

[24] Read bad password count 3

[24] Binding as admin

[24] Performing Simple authentication for admin to 10.106.71.234

[24] Simple authentication for admin returned code (49) Invalid credentials

[24] Message (admin): 80090308: LdapErr: DSID-0C0903C5, comment: AcceptSecurityContext error, data 773,

[24] Checking password policy

[24] New password is required for admin

[24] Fiber exit Tx=622 bytes Rx=2771 bytes, status=-1

[24] Session End

[25] Session Start

[25] New request Session, context 0x0000148f3c271830, reqType = Modify Password

[25] Fiber started

[25] Creating LDAP context with uri=ldaps://10.106.71.234:636

[25] Connect to LDAP server: ldaps://10.106.71.234:636, status = Successful

- [25] supportedLDAPVersion: value = 3
- [25] supportedLDAPVersion: value = 2
- [25] Binding as *****@razor.local
- [25] Performing Simple authentication for *****@razor.local to 10.106.71.234
- [25] LDAP Search:

Base DN = [DC=razor, DC=local]

Filter = [sAMAccountName=admin]

Scope = [SUBTREE]

- [25] User DN = [CN=admin,CN=Users,DC=razor,DC=local]
- [25] Talking to Active Directory server 10.106.71.234
- [25] Reading password policy for admin, dn:CN=admin,CN=Users,DC=razor,DC=local

[25] Read bad password count 3

[25] Change Password for admin successfully converted old password to unicode

[25] Change Password for admin successfully converted new password to unicode

[25] Password for admin successfully changed

[25] Retrieved User Attributes:

- [25] objectClass: value = top
- [25] objectClass: value = person
- [25] objectClass: value = organizationalPerson
- [25] objectClass: value = user
- [25] cn: value = admin
- [25] givenName: value = admin
- [25] distinguishedName: value = CN=admin,CN=Users,DC=razor,DC=local
- [25] instanceType: value = 4
- [25] whenCreated: value = 20201029053516.0Z

[25]	whenChanged: value = 20220426032127.0Z
[25]	displayName: value = admin
[25]	uSNCreated: value = 16710
[25]	uSNChanged: value = 98431
[25]	name: value = admin
[25]	objectGUID: value =0.].LH9.4
[25]	userAccountControl: value = 512
[25]	<pre>badPwdCount: value = 3</pre>
[25]	codePage: value = 0
[25]	countryCode: value = 0
[25]	badPasswordTime: value = 132610388348662803
[25]	lastLogoff: value = 0
[25]	lastLogon: value = 132484577284881837
[25]	<pre>pwdLastSet: value = 0</pre>
[25]	primaryGroupID: value = 513
[25]	objectSid: value =7Z RQ
[25]	accountExpires: value = 9223372036854775807
[25]	logonCount: value = 0
[25]	sAMAccountName: value = admin
[25]	sAMAccountType: value = 805306368
[25]	userPrincipalName: value = *****@razor.local
[25]	<pre>objectCategory: value = CN=Person,CN=Schema,CN=Configuration,DC=razor,DC=local</pre>
[25]	dSCorePropagationData: value = 20220425125800.0Z
[25]	dSCorePropagationData: value = 20201029053516.0Z
[25]	dSCorePropagationData: value = 16010101000000.0Z
[25]	lastLogonTimestamp: value = 132953506361126701
[25]	<pre>msDS-SupportedEncryptionTypes: value = 0</pre>
[25]	uid: value = *****@razor.local
[25] F	Fiber exit Tx=714 bytes Rx=2683 bytes, status=1

[25] Session End

Erreurs courantes rencontrées lors de la gestion des mots de passe

En général, si la stratégie de mot de passe définie par Microsoft Server n'est pas respectée pendant que l'utilisateur fournit le nouveau mot de passe, la connexion se termine avec l'erreur « Le mot de passe ne répond pas aux exigences de la stratégie de mot de passe ». Par conséquent, assurez-vous que le nouveau mot de passe respecte la stratégie définie par Microsoft Server pour les LDAP.

S Cisco AnyCon	nect FTD-Hostname X		
Cannot or password complexit	omplete password change because the password does not meet the policy requirements. Check the minimum password length, password y, and password history requirements.		
Group:	Dev 🗸	😚 Cisco AnyConnect Secure Mobility Client — 🗆 🗙	
Username	e: admin		
Password	k	Cannot complete password change because the password	
	OK Cancel	FTD-Hostname Connect	
		Cisco AnyConnect X	
		Cannot complete password change because the password does not meet the password policy requirements. Check the minimum password length, password complexity, and password history requirements.	
		ОК	

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.