Configurer l'authentification AD (LDAP) et l'identité de l'utilisateur sur FTD géré par FDM pour les clients AnyConnect

Contenu

Introduction Conditions préalables **Conditions requises Components Used** Configuration Schéma et scénario du réseau **Configurations AD** Déterminer le DN de base LDAP Créer un compte FTD Créer des groupes AD et ajouter des utilisateurs aux groupes AD (facultatif) Copier la racine du certificat SSL LDAPS (obligatoire uniquement pour LDAPS ou STARTTLS) **Configurations FDM** Vérifier la licence Configurer la source d'identité AD Configurer AnyConnect pour l'authentification AD Activer la stratégie d'identité et configurer les stratégies de sécurité pour l'identité de l'utilisateur Vérification Configuration finale Connexion avec AnyConnect et vérification des règles de stratégie de contrôle d'accès Dépannage Déboguages Déboques LDAP de travail Impossible d'établir la connexion avec le serveur LDAP DN de connexion et/ou mot de passe de liaison incorrects Serveur LDAP introuvable Nom d'utilisateur Mot de passe incorrect pour le nom d'utilisateur **Test AAA** Captures de paquets Journaux de l'Observateur d'événements Windows Server

Introduction

L'objectif de ce document est de détailler comment configurer l'authentification Active Directory (AD) pour les clients AnyConnect qui se connectent à un système Cisco Firepower Threat Defense (FTD) géré par Firepower Device Management (FDM). L'identité de l'utilisateur sera utilisée dans les stratégies d'accès afin de restreindre les utilisateurs AnyConnect à des adresses IP et des ports spécifiques.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissance de base de la configuration VPN RA sur FDM
- Connaissance de base de la configuration du serveur LDAP sur FDM
- Connaissances de base en AD

Components Used

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

- Serveur Microsoft 2016
- FTDv exécutant 6.5.0

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

Schéma et scénario du réseau



Le serveur Windows est préconfiguré avec Internet Information Services (IIS) et Remote Desktop Protocol (RDP) afin de tester l'identité de l'utilisateur. Dans ce guide de configuration, trois comptes d'utilisateurs et deux groupes seront créés.

Comptes d'utilisateurs :

- Admin FTD : Ce compte sera utilisé comme compte de répertoire afin de permettre au FTD de se lier au serveur AD.
- Administrateur informatique : Compte administrateur de test utilisé pour démontrer l'identité de l'utilisateur.

• Utilisateur test : Compte utilisateur de test utilisé pour démontrer l'identité de l'utilisateur. Groupes :

 Administrateurs AnyConnect : Groupe de test auquel l'administrateur informatique sera ajouté afin de démontrer l'identité de l'utilisateur. Ce groupe ne disposera que d'un accès RDP au serveur Windows Utilisateurs AnyConnect : Groupe de tests auquel l'utilisateur de test sera ajouté afin de démontrer l'identité de l'utilisateur. Ce groupe ne disposera que d'un accès HTTP au serveur Windows

Configurations AD

Afin de configurer correctement l'authentification AD et l'identité de l'utilisateur sur FTD, quelques valeurs seront requises. Tous ces détails doivent être créés ou collectés sur Microsoft Server avant que la configuration puisse être effectuée sur FDM. Les principales valeurs sont les suivantes :

- le nom de domaine: Il s'agit du nom de domaine du serveur. Dans ce guide de configuration, exemple.com est le nom de domaine.
- Adresse IP/FQDN du serveur : Adresse IP ou nom de domaine complet utilisé pour atteindre le serveur Microsoft. Si un FQDN est utilisé, un serveur DNS doit être configuré dans FDM et FTD afin de résoudre le FQDN. Dans ce guide de configuration, ces valeurs sont win2016.example.com qui prend la résolution 192.168.1.1.
- Port du serveur : Port utilisé par le service LDAP. Par défaut, LDAP et STARTTLS utiliseront le port TCP 389 pour LDAP et LDAP sur SSL (LDAPS) utiliseront le port TCP 636.
- Autorité de certification racine : Si LDAPS ou STARTTLS est utilisé, l'autorité de certification racine utilisée pour signer le certificat SSL utilisé par LDAPS est requise.
- Nom d'utilisateur et mot de passe du répertoire : Il s'agit du compte utilisé par FDM et FTD pour établir une liaison avec le serveur LDAP, authentifier les utilisateurs et rechercher les utilisateurs et les groupes. Un compte nommé FTD Admin sera créé à cette fin.
- Nom distinctif de base (DN) : Le DN de base est le point de départ du FDM et le FTD indique à Active Directory de commencer à rechercher des utilisateurs. Dans ce guide de configuration, le domaine racine example.com sera utilisé comme DN de base ; cependant, dans un environnement de production, l'utilisation d'un DN de base plus loin dans la hiérarchie LDAP pourrait être préférable. Par exemple, prenez cette hiérarchie LDAP :



Si un administrateur souhaite que les utilisateurs de l'unité d'organisation Marketing puissent authentifier le DN de base peut être défini sur la racine (exemple.com), cela permettra également à l'utilisateur 1 de l'unité d'organisation Finance de se connecter également puisque la recherche de l'utilisateur commence à la racine et passe à Finance, Marketing et Recherche.

DN de base défini sur exemple.com.



Afin de limiter les connexions aux utilisateurs de l'unité d'organisation Marketing et des niveaux inférieurs, l'administrateur peut à la place définir le DN de base sur Marketing. À présent, seuls l'utilisateur 2 et l'utilisateur 3 pourront s'authentifier, car la recherche commencera à Marketing.

DN de base défini sur Marketing :



Notez que pour un contrôle plus précis au sein du FTD pour lequel les utilisateurs seront autorisés à se connecter ou à attribuer des autorisations différentes aux utilisateurs en fonction de leurs attributs AD, une carte d'autorisation LDAP devra être configurée.

Cette hiérarchie LDAP simplifiée est utilisée dans ce guide de configuration et le DN de l'exemple racine.com sera utilisé pour le DN de base.



Déterminer le DN de base LDAP

1. Ouvrez Utilisateurs et ordinateurs AD.

=	Best match						
ŵ	Active Directory Users and Computers Desktop app						
	Settings >						
	8 Edit local users and groups						
	陀 Change User Account Control settings						
	8 User Accounts						
	Select users who can use remote desktop						
۲							
	users						
-	ዶ 🗆 🤶 🚍 🤱 🖪						

2. Cliquez avec le bouton gauche sur le domaine racine (afin d'ouvrir le conteneur), cliquez avec le bouton droit sur le domaine racine, puis accédez à **Affichage** et cliquez sur **Fonctions avancées**.



3. Ceci active l'affichage des propriétés supplémentaires sous les objets AD. Par exemple, pour rechercher le DN du fichier exemple.com racine, cliquez avec le bouton droit de la souris sur **exemple.com** puis accédez à **Propriétés**.



4. Sous **Propriétés**, cliquez sur l'onglet **Éditeur d'attributs**. Recherchez **distinguéName** sous Attributs, puis cliquez sur **Affichage**.

example.	com Propertie	5				?	х
General	Managed By	Object	Security	Attribut	e Editor		
Attribute	18:						
Attribu	te	Valu	e				^
dc		exan	nple				
defaul	tLocalPolicyOb	j knot	set>				
descri	ption	knot	set>				
deskte	op Profile	knot	set>				
display	yName	knot	set>				
displa	vNamePrintable	e knot	set>	_			
disting	uishedName	DC=	example_D	C=com			
domai	nPolicyObject	<not< td=""><th>set></th><td></td><td></td><td></td><td></td></not<>	set>				
domai	nReplica	<not< td=""><th>set></th><td></td><td></td><td></td><td></td></not<>	set>				
dSAS	ignature	{ V1:	: Flags = Ox	0; Laten	cySecs :	= 0; DsaGuio	
dSCor	ePropagationD	0x0 :	=()				
eFSP	olicy	<not< td=""><th>set></th><td></td><td></td><td></td><td></td></not<>	set>				
extent	sionName	<not< td=""><th>set></th><td></td><td></td><td></td><td></td></not<>	set>				
flags		<not< td=""><th>set></th><td></td><td></td><td></td><td>~</td></not<>	set>				~
<						>	
W	ew					Filter	
	OK		Cancel		Apply	Hel	p

5. Cela ouvrira une nouvelle fenêtre dans laquelle le DN peut être copié et collé dans FDM ultérieurement. Dans cet exemple, le DN racine est DC=exemple, DC=com. Copiez la valeur. Cliquez sur **OK** afin de quitter la fenêtre Éditeur d'attributs de chaîne, puis cliquez à nouveau sur **OK** afin de quitter les Propriétés.

String Attribute Editor		×		
Attribute: distingu	ishedName			
Value: DC=example,DC=com Clear	ОК	Cancel	Undo Cut Copy	
			Paste Delete	
			Select All Right to left Reading order Show Unicode control characters Insert Unicode control character	>
example.com Properties General Managed By C Attributes:	bject Security Attribute Editor	? ×		
Attribute cn controlAccessRights creationTime dc defautLocalPolicyObj description desktopProfile displayName d	Value <pre> <pre> <pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre>	Daylight Tim		
OK	Cancel Apply	Help		

Cela peut être fait pour plusieurs objets dans AD. Par exemple, ces étapes sont utilisées pour rechercher le numéro de répertoire du conteneur utilisateur :



6. La vue Advanced Features (Fonctions avancées) peut être supprimée. Cliquez avec le bouton droit sur le DN racine, accédez à **Affichage** et cliquez une fois de plus sur **Fonctionnalités avancées**.



Créer un compte FTD

Ce compte d'utilisateur permettra à FDM et au FTD de se lier à l'AD afin de rechercher des utilisateurs et des groupes et de les authentifier. La création d'un compte FTD distinct a pour but d'empêcher tout accès non autorisé ailleurs dans le réseau si les informations d'identification utilisées pour la liaison sont compromises. Ce compte n'a pas besoin d'être compris dans la portée du DN de base.

1. Dans **Utilisateurs et ordinateurs Active Directory**, cliquez avec le bouton droit sur le conteneur/l'organisation auquel le compte FTD sera ajouté. Dans cette configuration, le compte FTD sera ajouté sous le conteneur Utilisateurs sous le nom d'utilisateur **ftd.admin@example.com**. Cliquez avec le bouton droit sur **Utilisateurs**, puis cliquez sur **Nouveau > Utilisateur**.

Active Directory	Users and Comp	puters				-	×
File Action View	w Help						
🗢 🔿 🔁 📆	X 🗈 🗙 🛙	0 🔒 🛛	Þ	1 🗏 🐮 🛯	r 🗾 🔍		
Active Directory Users and Com Saved Queries Saved Queries Save		Name DefaultAcc Denied ROI DonsAdmins DonsUpdate Domain Ad Domain Co trol	o D s P i n	Type User Security Group Security Group Security Group Security Group Security Group Security Group	Description A user account manage. Members in this group of DNS Administrators Gro. DNS clients who are per. Designated administrato All workstations and ser. All domain controllers i All domain guests		^
	New All Tasks View Refresh Export List Properties	>	Computer Contact Group InetOrgPerson msDS-KeyCrede msDS-Resourcef msDS-ShadowP	ntial PropertyList incipalContainer			
< Creates a new item in	Help	WseAlertA WseAllow WseAllow		msImaging-PSP: MSMQ Queue Al Printer User Shared Folder	ias		~

2. Naviguez dans l'Assistant Nouvel objet - Utilisateur.

New Object - User		×
🤱 Create in:	example.com/Users	
Erst name:	FTD Initials:	
Last name:	Admin	
Full name:	FTD Admin	
User logon name:		
ftd.admin	@example.com ~	
User logon name (pre	<u>Wi</u> ndows 2000):	
EXAMPLE\	ftd.admin	
	< Back Next > Cancel	

New Object - User		×
🤱 Create in: exar	mple.com/Users	
Password:	•••••	
Confirm password:	•••••	
User must change passw	rord at next logon	
User cannot change pas	sword	
Password never expires		
Account is disabled		
	< Back Next >	Cancel
New Object - User		Х
New Object - User	mple.com/Users	×
New Object - User	mple.com/Users bliowing object will be created:	×
New Object - User Create in: example of the second	mple.com/Users ollowing object will be created:	×
New Object - User Create in: example When you click Finish, the for Full name: FTD Admin User logon name: ftd.admin	mple.com/Users ollowing object will be created: @example.com	×
New Object - User Create in: example of the second	mple.com/Users ollowing object will be created: @example.com s.	×
New Object - User Create in: example of the password never expires	mple.com/Users ollowing object will be created: @example.com 8.	×
New Object - User	mple.com/Users ollowing object will be created: @example.com s.	×
New Object - User Create in: example of the example	mple.com/Users ollowing object will be created: @example.com s.	×
New Object - User Create in: example of the example	mple.com/Users ollowing object will be created: @example.com s.	×
New Object - User Create in: exam When you click Finish, the for Full name: FTD Admin User logon name: ftd.admine The password never expires	mple.com/Users ollowing object will be created: @example.com s.	Cancel

3. Vérifiez que le compte FTD a été créé. En outre, deux comptes supplémentaires ont été créés, Administrateur informatique et Utilisateur de test.

Active Directory Users and Computers					×
File Action View Help					
🗢 🔿 🙍 📆 🔏 🗈 🗶 📴	a 🔒 🛛 🖬	1 % 🔌 🛍 🖷	r 🧕 🗽		
Active Directory Users and Com Saved Queries	Name	Type User	Description A user account manage		^
 Builtin Computers Domain Controllers ForeignSecurityPrincipal: Managed Service Accour Users 	Denied ROD DnsAdmins DnsUpdateP Domain Ad Domain Co Domain Con Domain Gue Domain Users	Security Group Security Group Security Group Security Group Security Group Security Group Security Group	Members in this group c DNS Administrators Gro DNS clients who are per Designated administrato All workstations and ser All domain controllers i All domain guests All domain users		
	Kenterprise A Enterprise K Enterprise R FTD Admin Group Polic	Security Group Security Group Security Group User Security Group User	Designated administrato Members of this group Members of this group Members in this group c Built-in account for gue		
< >>	LT Admin Key Admins Protected Us RAS and IAS Read-only D Schema Ad Test User	User Security Group Security Group Security Group Security Group User	Members of this group Members of this group Servers in this group can Members of this group Designated administrato		~

Créer des groupes AD et ajouter des utilisateurs aux groupes AD (facultatif)

Bien qu'ils ne soient pas requis pour l'authentification, les groupes peuvent être utilisés pour faciliter l'application des stratégies d'accès à plusieurs utilisateurs ainsi qu'à l'autorisation LDAP. Dans ce guide de configuration, les groupes seront utilisés pour appliquer ultérieurement les paramètres de stratégie de contrôle d'accès via l'identité de l'utilisateur dans FDM.

1. Dans Utilisateurs et ordinateurs Active Directory, cliquez avec le bouton droit sur le conteneur/l'organisation auquel le nouveau groupe sera ajouté. Dans cet exemple, le groupe AnyConnect Admins sera ajouté sous le conteneur Utilisateurs. Cliquez avec le bouton droit sur Utilisateurs, puis cliquez sur Nouveau > Groupe.

Active Directory Users and Com	puters			-	×
File Action View Help					
🗢 🔿 🙇 🚾 🔏 🖬 🗶	3 🙆 📑 🖬 🖬	e i 😤 📚 în 🤋	r 🗵 🐍		
Active Directory Users and Com Saved Queries Saved Queries Delegate Con Find	Name DefaultAcco Denied ROD DnsAdmins DnsUpdateP Domain Ad Domain Ad Domain Co ntrol	Type User Security Group Security Group Security Group Security Group Security Group Security Group Security Group	Description A user account manage Members in this group c DNS Administrators Gro DNS clients who are per Designated administrato All workstations and ser All domain controllers i All domain guests All domain users		~
All Tasks View Refresh	> > >	Computer Contact Group InetOrgPerson msDS-KeyCreder	ntial		
Export List Properties Help	Read-only	msDS-ResourcePropertyList msDS-ShadowPrincipalContainer msImaging-PSPs MSMQ Queue Alias			
< >> Creates a new item in this container.	Schema A	Printer User Shared Folder			~

2. Naviguez dans l'Assistant Nouvel objet - Groupe comme indiqué dans l'image.

New Object - Group	×
🥵 Create in: exam	nple.com/Users
Group name:	
AnyConnect Admins	
Group name (nre-Windows 20	100)-
AnyConnect Admins	
Group scope	Group type
O Domain local	Security
Global	ODistribution
OUniversal	
	OK Cancel

3. Vérifiez que le groupe a été créé. Le groupe Utilisateurs AnyConnect a également été créé.

Active Directory Users and Com	-	×			
File Action View Help					
🗢 🔿 🙍 📆 🖌 😫 🗉	3 🛛 🖬 🕲 🐜 🛍	🔻 🗾 🙇			
Active Directory Users and Com Saved Queries Saved Queries Sultin	Name AnyConnect Admins AnyConnect Users Calo Cert Publishers Cloneable Domain C Cloneable Domain C DefaultAccount Denied RODC Passw DisAdmins DisUpdateProxy Domain Admins Domain Computers Domain Computers Domain Controllers Domain Guests Domain Guests Domain Guests Comain Guests Enterprise Admins Enterprise Key Admins Enterprise Read-only FTD Admin Group Policy Creator Guest IT Admin Key Admins	Type Security Group Security Group User Security Group Security Group User User User Security Group	Description Built-in account for ad Members of this group A user account manage Members in this group c DNS Administrators Gro DNS clients who are per DNS clients who are per DNS clients who are per All workstations and ser All domain controllers i All domain guests All domain guests All domain users Designated administrato Members of this group Members of this group Built-in account for gue		~
	[[175] A		11 I V.I.		-

4. Cliquez avec le bouton droit sur le groupe auquel les utilisateurs seront ajoutés, puis sélectionnez **Propriétés**. Dans cette configuration, l'utilisateur **Administrateur informatique** sera ajouté au groupe **Administrateurs AnyConnect** et l'utilisateur **Test User** sera ajouté au groupe **Utilisateurs AnyConnect**.

Active Directory Users and Computer	iters			-	×
File Action View Help					
🗢 🔿 🙍 📰 🤞 🖾 🔀	@ 🔒 🛛 🖬 🖏	k 🛯 🔻 🧕 🕯	5		
Active Directory Users and Com	Name AnyConnect Admins	Type Security Group	Description		^
Builtin Computers Some Domain Controllers	AnyConnect Users calo	Security Group User Security Group	Add to a group Jser Buil Move ecurity Group Mer Send Mail All Tasks Jser A u: ecurity Group Mer Cut ecurity Group DNS Delete ecurity Group DNS Rename ecurity Group DNS Rename ecurity Group All C ecurity G ecurity G ecurity G ecurity G ecurity G ecurity G		
> ForeignSecurityPrincipal:	Cloneable Domain C Secu DefaultAccount User DefaultAccount User DefaultAccount Secu Domain Admins Secu Domain Admins Secu Domain Computers Secu Domain Controllers Secu Domain Guests Secu	Security Group User		>	
> 📫 Managed Service Accour		Security Group Security Group Security Group Security Group Security Group Security Group Security Group			
	Enterprise Admins Enterprise Key Admins Enterprise Read-only FTD Admin Group Policy Creator Guest IT Admin Key Admins	Security Group Security Group User Security Group User User Security Group	Designated administrato Members of this group Members of this group Members in this group c Built-in account for gue Members of this group		
Renames the current selection.	(h.s				Ŷ

5. Cliquez sur l'onglet Membres, puis sur Ajouter comme indiqué dans l'image.

AnyConnect Admins Properties	?	х
General Members Member Of Managed By		
Members:		
Name Active Directory Domain Services Folder		
Add Remove		
OK Cancel	Δορί	у

Entrez l'utilisateur dans le champ et cliquez sur le bouton Vérifier les noms afin de vérifier que l'utilisateur est trouvé. Une fois vérifié, cliquez sur OK.

Select Users, Contacts, Computers, Service Accounts, or	Groups X
Select this object type:	
Users, Service Accounts, Groups, or Other objects	Qbject Types
From this location:	
example.com	Locations
Enter the object names to select (examples):	
IT Admin (t.admin@example.com)	Qheck Names
Advanced	OK Cancel

Vérifiez que l'utilisateur correct est ajouté, puis cliquez sur le bouton **OK**. L'utilisateur Test User est également ajouté au groupe d'utilisateurs AnyConnect à l'aide des mêmes étapes.

AnyConn	ect Admin	s Properties	4		?	×
General	Members	Member Of	Managed By			
Membe	na:					_
Name & IT	Admin	Active Dir example.c	ectory Domain com/Users	Services Folder	,	
Ad	d	Remove				
			ОК	Cancel	Ар	ply

Copier la racine du certificat SSL LDAPS (obligatoire uniquement pour LDAPS ou STARTTLS)

1. Appuyez sur Win+R et tapez mmc.exe. Click OK.

🖅 Run		×
0	Type the name of a program, folder, docume resource, and Windows will open it for you.	nt, or Internet
<u>O</u> pen:	mmc.exe	~
	OK Cancel	<u>B</u> rowse

2. Accédez à Fichier > Ajouter/Supprimer un composant logiciel enfichable... comme le montre l'image.

ᡖ Cor	nsole1 - [Console Root]			-	o x
🚡 File	Action View Favorites	Window	Help		- 8 ×
4	New	Ctrl+N			
	Open	Ctrl+0		Actions	
	Save	Ctrl+S	There are no items to show in this view.	Console Root	
	Save As			More Actions	+
	Add/Remove Snap-in	Ctrl+M			
	Options				
	1 dnsmgmt				
	2 dsa				
	Exit				
Enables	you to add snap-ins to or rem	ove them fro	m the snap-in console.		

3. Sous les composants logiciels enfichables disponibles, cliquez sur Certificats, puis sur Ajouter.

Add or Remove Snap-ins				×			
You can select snap-ins for t extensible snap-ins, you can	You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.						
Available snap-ins:			Selected snap-ins:				
Snap-in	Vendor	^	Console Root Edit Ext	ensions			
Active Directory Do	Microsoft Cor		Re	move			
Active Directory Site	Microsoft Cor						
Active Directory Use	Microsoft Cor						
📹 ActiveX Control	Microsoft Cor	-	Mo	ve <u>U</u> p			
ADSI Edit	Microsoft Cor		Mour	a Down			
Authorization Manager	Microsoft Cor		Add >	Fouri			
Certificate Templates	Microsoft Cor						
Certificates	Microsoft Cor						
Certification Authority	Microsoft Cor						
Component Services	Microsoft Cor						
Computer Managem	Microsoft Cor						
Device Manager	Microsoft Cor						
Disk Management	Microsoft and	\checkmark	Ad <u>v</u> a	nced			
Description							
Description:							
The Certificates shap-in allo	ws you to browse	the	contents of the certificate stores for yourself, a service, or a compute	ar.			
			OK	Cancel			
			UN				

4. Sélectionnez Compte d'ordinateur, puis cliquez sur Suivant comme indiqué dans l'image.

Certificates snap-in	×
This snap-in will always manage certificates for: My user account Service account @Computer account	
< Back Next > Cancel	

Cliquez sur Finish.

Select Computer	×
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: Browse Another computer: Browse Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.	
< Back Finish Cancel	

5. Click OK.

Add or Remove Snap-ins					×	
You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.						
Available snap-ins: Selected snap-ins:						
Snap-in	Vendor	^		Console Root Edit Extensions		
Active Directory Do	Microsoft Cor Microsoft Cor			Certificates (Local Computer)		
Active Directory Use	Microsoft Cor Microsoft Cor			Move <u>U</u> p		
Authorization Manager	Microsoft Cor			Move <u>D</u> own		
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	5		Advanced		
Description:						
The Certificates snap-in allo	ws you to browse	the	contents of the	certificate stores for yourself, a service, or a computer.		
				OK Cancel		

6. Développez le dossier **Personnel**, puis cliquez sur **Certificats**. Le certificat utilisé par LDAPS doit être délivré au nom de domaine complet (FQDN) du serveur Windows. Sur ce serveur, 3 certificats sont répertoriés.

- Certificat CA délivré à et par exemple-WIN2016-CA.
- Certificat d'identité délivré au WIN2016 par exemple-WIN2016-CA.
- Certificat d'identité émis pour win2016.example.com par exemple-WIN2016-CA.

Dans ce guide de configuration, le nom de domaine complet est win2016.example.com et les 2 premiers certificats ne sont donc pas valides pour être utilisés comme certificat SSL LDAPS. Le certificat d'identité émis pour win2016.example.com est un certificat qui a été automatiquement émis par le service AC de Windows Server. Double-cliquez sur le certificat pour vérifier les détails.

Console1 - [Console Root\Certificates (Local Computer)\Personal\Certificates]					
🚟 File Action View Favorites	Window Help				- 8 ×
🗢 🏟 🖄 🚾 🗎 🔯 🗟					
Console Root Console Root Certificates (Local Computer) Personal Certificates Trusted Root Certification . Enterprise Trust Intermediate Certification . Trusted Publishers Untrusted Certificates Untrusted Certificates Untrusted People Client Authentication Issue Client Authentication Issue Preview Build Roots Client Authentication Issue Client Authentication Issue	Issued To Signexample-WIN2016-CA WIN2016 WIN2016	Issued By example-WIN2016-CA example-WIN2016-CA example-WIN2016-CA	Expiration Da 4/19/2060 4/27/2025 4/28/2021	Actions Certificates More Actions	•
 Smart Card Trusted Roots Trusted Devices Web Hosting 					
> 🔛 Windows Live ID Token Iss	<		>		
Personal store contains 3 certificates.					

7. Afin d'être utilisé comme certificat SSL LDAPS, le certificat doit satisfaire aux conditions suivantes :

• Le nom commun ou le nom secondaire de l'objet DNS correspond au nom de domaine complet de Windows Server.

• Le certificat possède l'authentification du serveur sous le champ Utilisation de clé améliorée.

Sous l'onglet Détails du certificat, sous **Subject** and **Subject Alternative Name**, le nom de domaine complet **win2016.example.com** est présent.

🙀 Certif	ficate				×
General	Details	Certification Pa	1th		
Show:	<al></al>		~		
Field			Value		^
<u>詞</u> Sut	bject		win2016.examp	le.com	
📋 Put	blic key		RSA (2048 Bits)		
Put	blic key pa	arameters	05 00		
Ce	rtificate T	emplate Name	DomainControlle	r	
Enf	hanced Ke	ey Usage	Client Authentic	ation (1.3.6.1	
() () () () () () () () () () () () () (IME Capa	Dilities	[1]SMIME Capat	olity: Object I	
	bject Key Iboritu Ka	Identifier	30 D7 20 He H8 0	27 fb 11 16	¥
CN = w	in2016.e:	<pre>kample.com</pre>			
		[Edit Properties	Copy to File	
				O	¢

🙀 Certil	ficate			×
General	Details	Certification Path		
Show:	<al></al>		\sim	
Field Sul Au Au Au Au Au	bject Key thority Ke L Distribu thority In	Identifier y Identifier tion Points formation Access	Value 30 b7 2b 4e 48 0f 2f 17 17 e6 KeyID=3d 9f 26 37 fb 11 1f 4 [1]CRL Distribution Point: Distr [1]Authority Info Access: Acc	^
Ke Th Th	y Usage umbprint : umborint	native Name	Other Name:DS Object Guid= Digital Signature, Key Encipher sha1 ca 8e 11 3d eb bc 0f 6e 4a 00	*
Other N DS 0 18 DNS Na	lame: Object Gu me=win2	id=04 10 90 99 a9 016.example.com	a2 38 24 65 47 84 74 64 26 cd c6 8	D
		Ed	It Properties Copy to File	
			0	¢

Sous Utilisation améliorée des clés, Authentification du serveur est présente.

🙀 Certi	ficate			×
General	Details	Certification Path		
Show:	<al></al>		\sim	
Field			Value	^
E Sul E Pul	bject blic key blic key pa	arameters	win2016.example.com RSA (2048 Bits) 05 00	
E SM E SM E SM	hanced Ko IME Capa bject Key thority Ke	blities Identifier	Clent Authentication (1.3.6.1 [1]SMIME Capability: Object I 30 b7 2b 4e 48 0f 2f 17 17 e6 KevID=3d 9f 26 37 fb 11 1f 4	~
Client / Server	Authenticz	tion (1.3.6.1.5.5.) ation (1.3.6.1.5.5.	7.3.2) 7.3.1) It Properties Copy to File	
			0	(

8. Une fois que cela a été confirmé, accédez à l'onglet **Chemin d'accès de la certification**. Cliquez sur le certificat supérieur qui doit être le certificat de l'autorité de certification racine, puis cliquez sur le bouton **Afficher le certificat**.

Certificate	×
General Details Certification Path	
Certification path	
example-WIN2016-CA	
View Certificate	
Certificate status:	
This certificate is OK.	
ок	

9. Ceci ouvrira les détails du certificat pour le certificat de l'autorité de certification racine.

Certificate	\times
General Details Certification Path	
Certificate Information	
This certificate is intended for the following purpose(s): • All issuance policies • All application policies	
Issued to: example-WIN2016-CA	-
Issued by: example-WIN2016-CA	
Valid from 4/27/2020 to 4/19/2060 Issuer Statemen	t
OK	

10. Ouvrez l'onglet **Détails**, puis cliquez sur **Copier dans un fichier...** comme le montre l'image.

Certificate		\times
General Details Certification Path		
Show: <all></all>	~	
Field	Value ^	
Version Serial number Signature algorithm Signature hash algorithm Valid from Valid from Valid to Subject	V3 13 86 46 e5 9d 70 4f a9 4e 35 sha256RSA sha256 example-WIN2016-CA Monday, April 27, 2020 10:50: Monday, April 19, 2060 10:50: example-WIN2016-CA	
E	dit Properties Copy to File]
	ОК	

11. Naviguez dans l'Assistant Exportation de certificat qui exportera l'autorité de certification racine au format PEM.

÷	F Certificate Export Wizard	×
	Welcome to the Certificate Export Wizard	
	This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.	
	A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.	
	To continue, dick Next.	
	Net	
	Cancer	

12. Sélectionnez Base-64 encoded X.509.

÷	🚰 Certificate Export Wizard	×
	Export File Format Certificates can be exported in a variety of file formats.	
	Select the format you want to use:	
	O DER encoded binary X.509 (.CER)	
	Base-64 encoded X.509 (.CER)	
	Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)	
	 Personal Information Exchange - PKCS #12 (.PFX) Include all certificates in the certification path if possible 	
	 Delete the private key if the export is successful 	
	Export all extended properties	
	Enable certificate privacy	
	 Microsoft Serialized Certificate Store (.SST) 	
	Next Cano	el

13. Sélectionnez le nom du fichier et l'emplacement vers lequel il sera exporté.

Erile to Export Specify the name of the file you want to export File name:	Browse	
	Next Cancel	
save As		×
← → ~ ↑ ■ > This PC > Desktop	∨ Ö Si	arch Desktop 🔎
Organize 🔻 New folder		III 🕶 😮
Image: Point of the second	Date modified Type No items match your search.	Size
File name: root		~
Save as type: Base64 Encoded X.509 (*.cer)		v
∧ Hide Folders	[Save Cancel

÷	🚰 Certificate Export Wizard	×
	File to Export Specify the name of the file you want to export	
	File name:	-
	C:\Users\admin\Desktop\root.cer Browse	
	Next Cancel	

14. Cliquez sur Finish.

÷	<i>Ş</i> ,	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\admin\Desktop\root.cer	
		Export Keys	No	
		Include all certificates in the certification path	No	
		File Format	Base64 Encoded X.509 (*.cer)	
			Finish Cano	cel

15. Maintenant, accédez à l'emplacement et ouvrez le certificat à l'aide d'un bloc-notes ou d'un autre éditeur de texte. Le certificat de format PEM s'affiche. Enregistrez ceci pour plus tard.

----BEGIN CERTIFICATE----

```
MIIDCDCCAfCgAwIBAgIQE4ZG5Z1wT6lONTjooEQyMTANBgkqhkiG9w0BAQsFADAd
MRswGQYDVQQDExjleGFtcGxlLVdJTjIwMTYtQ0EwIBcNMjAwNDI3MTQ1MDU5WhgP
MjA2MDA0MTkxNDUwNTlaMB0xGzAZBgNVBAMTEmV4YW1wbGUtV010MjAxNi1DQTCC
ASIwDQYJKoZIhvcNAQEBBQADqqEPADCCAQoCqqEBAI8qhT719NzSQpoQPh0YT67b
Ya+PngsxMyvkewP33QLTAWw1HW1Tb9Mk5BDW0ItTaVsgHwPBfd++M+bLn3AiZnHV
OO+k6dVVY/E5qVkEKSGoY+v940S2316lzdwReMOFhgbc2qMertIoficrRhihonuU
Cjyeub3CO+meJUuKom2R47C0D35TUvo/FEHGgXJFaJS1se2UrpN07KEMkfAlLPuM
aob4XE/OzxYQpPa18djsNnskfcFqD/HOTFQN4+SrOhHWlRnUIQBUaLdQaabhipD/
sVs5PneYJX8YKma821uYI6j90YuytmsHBtCieyC062a8BKqOL7N86HFPFkMA3u8C
\texttt{AwEAAaNCMEAwDgYDVR0PAQH/BAQDAgGGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0O}
BBYEFD2fjjf7ER9EM/HCxCVFN5QzqEdvMA0GCSqGSIb3DQEBCwUAA4IBAQB31ZJo
vzwVD3c5Q1nrNP+6Mq62OFpYH91k4Ch9S5g/CEOemhcwg8MDIoxW2dTsjenAEt7r
phFIHZoCoSyjBjMgK3xybmoSeg8vBjCXseYNGEmOc9KW1oFmTOvdNVIb7Xpl1IVa
6tALTt3ANRNgREtxPA6yQbthKGavW0Anfsojk9IcDr2vp0MTjlBCxsTscbubRl+D
dLEFKQqmMeYvkVf+a7a64mqPZsG3Uxo0rd6cZxAPkq/ylcdwNSJFfQV3DqZq+R96
9WLCR3Obig6xyo9Zu+lixcWpdrbADO6zMhbEYEhkhOOjBrUEBBI6Cy83iTZ9ejsk
KgwBJXEu33PplW6E
```

----END CERTIFICATE----

Configurations FDM

Vérifier la licence

Pour configurer AnyConnect sur FDM, le FTD devra être enregistré auprès du serveur de licences Smart et une licence Plus, Apex ou VPN Only valide doit être appliquée au périphérique.

1. Accédez à **Device > Smart License** comme indiqué dans l'image.



2. Vérifiez que le FTD est enregistré sur le serveur de licences Smart et que la licence AnyConnect Plux, Apex ou VPN Only est activée.

CISCO. Firepower Device Manager Monitoring Policies Objects	Device: FTD-3		
Device Summary Smart License Converse Last sync: 15 Apr 2020 08:27 AM	Contra Chard Services A ve		
SUFFICIENT LICENSE Next sync: 16 Apr 2020 08:37 AM			
SUBSCRIPTION LICENSES INCLUDED			
Threat ENABLE Disabled by user	Malware ENABLE		
This License allows you to perform intrusion detection and prevention and file control. You must have this license to apply intrusion policies in access rules. You also must have this license to apply file policies that control files based on file type.	This License allows you to perform Cisco Advanced Malware Protection (AMP) with AMP for Firepower and AMP Throat Grid. You must have this license to apply file policies that detect and block malware in files transmitted over your network. Includes: C File Policy		
Includes: 🎭 Intrusion Policy			
URL License DISABLE	RA VPN License Type PLUS V DISABLE		
C Enabled	C Enabled		
This license allows you to control web access based on URL categories and reputations, rather than by individual URL alone. You must have this license to deploy access rules that filter web traffic based on category and reputation.	Please select the license type that you purchased to enable remote access VPN. Note that Firepower Device Manager does not support any of the advanced features covered by the Apex license.		
Includes: URL Reputation	Includes: RA-VPN		

Configurer la source d'identité AD

1. Accédez à Objets > Sources d'identité, puis cliquez sur le symbole + et sélectionnez AD comme

indiqué dans l'image.

cisco. Firepower Devi	ce Manager Monitoring	Policies Objects Device: FTD-3	S 🚑 🐵 ? :	admin Administrator
Object Types 🔶 ^	Identity Sources			
C Networks	1 object		Q Search	+ ~
와 Ports	* NAME	пи	VALUE	RADIUS Server
🔒 Security Zones	1 LocalIdentitySource	LOCAL		RADIUS Server Group
🐔 Application Filters				AD
Ø URLS				Identity Services Engine
Geolocations				
🚦 Syslog Servers				
🔏 IKE Policies				
🐴 IPSec Proposals				
🔒 AnyConnect Client				
E Identity Sources				
1 Users				
A Certificates				
🔒 Secret Keys				
DNS Groups				
Vert List Filters				

2. Complétez les paramètres appropriés pour le serveur Active Directory avec les informations collectées précédemment. Si un nom d'hôte (FQDN) est utilisé pour le serveur Microsoft au lieu d'une adresse IP, assurez-vous de créer un groupe DNS approprié sous Objets > Groupe DNS. Appliquez ensuite ce groupe DNS au FTD en naviguant vers Device > System Settings > DNS Server, en appliquant le groupe DNS sous l'interface de gestion et l'interface de données, puis spécifiez l'interface de sortie appropriée pour les requêtes DNS. Cliquez sur le bouton Test afin de vérifier une configuration et une accessibilité réussies à partir de l'interface de gestion de FTD. Puisque ces tests sont initiés à partir de l'interface de gestion du FTD et non par l'une des interfaces routables configurées sur le FTD (telles que interne, externe, dmz), une connexion réussie (ou échouée) ne garantit pas le même résultat pour l'authentification AnyConnect puisque les demandes d'authentification LDAP AnyConnect seront lancées à partir de l'une des interfaces routables du FTD. Pour plus d'informations sur le test des connexions LDAP à partir du FTD, consultez les sections Test AAA et Packet Capture dans la zone Dépannage.

Add Identity Realm

Ŀ.

Identity Realm is used for Identity Policies and Remote Access VPN. Any changes impact all features that use this realm.

Name	Туре
LAB-AD	Active Directory (AD)
Directory Username	Directory Password
ftd.admin@example.com	••••••
e.g. user@example.com	
Base DN	AD Primary Domain
DC=example,DC=com	example.com
e.g. ou=user, dc=example, dc=com	e.g. example.com
Directory Server Configuration	
win2016.example.com:389	▲
Hostname / IP Address	Port
Hostname / IP Address win2016.example.com	389
Hostname / IP Address win2016.example.com e.g. ad.example.com	Port 389
Hostname / IP Address win2016.example.com e.g. ad.example.com Encryption	Port 389 Trusted CA certificate
Hostname / IP Address win2016.example.com e.g. ad.example.com Encryption NONE	Port 389 Trusted CA certificate Please select a certificate
Hostname / IP Address win2016.example.com e.g. ad.example.com Encryption NONE ✓ TEST ✓ Connection to realm is successful	Port 389 Trusted CA certificate Please select a certificate
Hostname / IP Address win2016.example.com e.g. ad.example.com Encryption NONE ~ TEST Connection to realm is successful Add another configuration	Port 389 Trusted CA certificate Please select a certificate
Hostname / IP Address win2016.example.com e.g. ad.example.com Encryption NONE ✓ TEST ✓ Connection to realm is successful Add another configuration	Port 389 Trusted CA certificate Please select a certificate

Si LDAPS ou STARTTLS est utilisé, sélectionnez le chiffrement approprié, puis sélectionnez le certificat de CA de confiance. Si l'autorité de certification racine n'est pas déjà ajoutée, cliquez sur **Créer un nouveau certificat d'autorité de certification de confiance**. Indiquez un nom pour le certificat de l'autorité de certification racine, puis collez le certificat de l'autorité de certification racine au format PEM collecté précédemment.

Add Trusted CA Certificate

	Name LDAPS_ROOT			
	Paste certificate, or choose file: UPLOAD CERTIFICATE The supported formats are: PEM, DER.			
BEGIN CERTIFICATE MIIDCDCCAfCgAwIBAgIQE4ZG5Z1wT6IONTjooEQyMTANBgkqhkiG9w0BAQsFADAd MRswGQYDVQQDExJleGFtcGxILVdJTjlwMTYtQ0EwIBcNMjAwNDI3MTQ1MDU5WhgP MjA2MDA0MTkxNDUwNTlaMB0xGzAZBgNVBAMTEmV4YW1wbGUtV0IOMjAxNi1DQTCC AShwDOX_IKoZlbwcNAOEBBOADggEPADCCAOoCggEBAl8gbT719NzSOggODb0YT67b				
		CANCEL	ок	
	Directory Server Configuration			
	win2016.example.com:636			

8 X

Hostname / IP Address	Port
win2016.example.com	636
e.g. ad.example.com	
Encryption	Trusted CA certificate
LDAPS ~	LDAPS_ROOT V
TEST ✓ Connection to realm is succe	ssful

Dans cette configuration, ces valeurs ont été utilisées :

- Name : LAB-AD
- Nom d'utilisateur du répertoire : ftd.admin@example.com
- DN de base : DC=exemple, DC=com
- Domaine principal AD : example.com
- Nom d'hôte/Adresse IP : win2016.example.com
- Port : 389
- 3. Cliquez sur le bouton Modifications en attente en haut à droite, comme illustré dans l'image.

cisco. Firepower De	vice Manager Monitoring Policies	Objects Device: FTD-3) * admin * Administrator ~
Object Types 🛛 🗧	Identity Sources		
C Networks	2 objects	Q. Search	+ ~
S Ports	H NAME	THRE VALUE	ACTIONS
Security Zones	1 LocalIdentitySource	LOCAL	
Application Filters	2 LAB-AD	AD win2016.example.com	

4. Cliquez sur le bouton Déployer maintenant.

Pe	ending Changes	0	×
0	Last Deployment Completed Successfully 01 May 2020 12:54 PM. See Deployment History		
	Deployed Version (01 May 2020 12:54 PM)	Pending Version CLEGEND Removed Added Er	dited
0	Active Directory Realm Added: LAB-AD		^
	- - - - - - - -	<pre>dirPassword.masked: false dirPassword.encryptedString: *** directoryConfigurations[0].port: 389 directoryConfigurations[0].hostname: win2016.example.com directoryConfigurations[0].encryptionProtocol: NONE adPrimaryDomain: example.com dirUsername: ftd.admin@example.com baseDN: DC=example,DC=com enabled: true realmId: 9 name: LAB-AD</pre>	v
M	ORE ACTIONS Y	CANCEL DEPLOY NOW	~

Configurer AnyConnect pour l'authentification AD

Pour utiliser la source d'identité AD configurée, elle doit être appliquée à la configuration AnyConnect.

1. Accédez à **Device > Remote Access VPN** comme indiqué dans l'image.

CISCO. Firepower Device Manager	Monitoring Policies Objects	Device: FTD-3	admin
	<u>av</u>		
Interfaces Connected Enabled 3 of 4 View All Interfaces	Routing 2 routes View Configuration	Updates Geolocation, Rule, VDB, System Upgrade, Security Intelligence Feeds View Configuration	System Settings Management Access Logging Settings DHCP Server
Smart License Registered	Backup and Restore	Troubleshoot No files created yet REQUEST FILE TO BE CREATED	Management Interface Hostname NTP Cloud Services Reboot/Shutdown
Site-to-Site VPN	Remote Access VPN	Advanced Configuration	URL Filtering Preferences Device Administration
There are no connections yet View Configuration	Configured 1 connection 2 Group Policies View Configuration	Includes: FlexConfig. Smart CLI View Configuration	Audit Events, Deployment History, Download Configuration View Configuration

2. Cliquez sur le symbole + ou sur le bouton **Créer un profil de connexion** comme indiqué dans l'image.



3. Dans la section Connection and Client Configuration, sélectionnez la source d'identité AD créée précédemment. Configurez les valeurs appropriées pour les autres sections, notamment le nom du profil de connexion et l'affectation du pool d'adresses client. Cliquez sur **Soumettre la requête** lorsque vous avez terminé.

Connection and Client Configuration

inside network.							
Connection Profile Name This name is configured as a connection allas, it can	n be used to connect to the VPN gateway						
General							
Group Alias	Group URL						
General							
Add Group Alias	Add.Group.URL						
Primary Identity Source							
Authentication Type							
AAA Only Client Certificate Only AAA and Client Certificate							
Primary Identity Source for User Authenticat	ion Fallback Local Identity Source 🔥						
Filter	✓ Please Select Local Identity Source ✓						
11 LocalIdentitySource	^						
11 LAB-AD	0						
11 Special-Identities-Realm	\sim						
Create new 🜱							

Client Address Pool Assignment

IPv4 Address Pool Endpoints are provided an address from this pool	IPv6 Address Pool Endpoints are provided an address from this pool			
C AnyConnect-Pool				
+ DHCP Servers				
CANCEL	SUBMIT QUERY			

4. Dans la section Expérience utilisateur à distance, sélectionnez la stratégie de groupe appropriée. Par défaut, la **DfltGrpPolicy** sera utilisée ; cependant, il est possible d'en créer une autre.

```
View Group Policy
```

DfltGrpPolicy

Policy Group Brief Details

None
None
Unlimited / 1 Minutes
30 / 1 Minutes
3
Allow all traffic over tunnel
Allow all traffic over tunnel
None

5. Dans la section Global Settings, spécifiez au minimum le certificat SSL, l'interface externe et les packages AnyConnect. Si aucun certificat n'a été créé précédemment, un certificat auto-signé par défaut (DefaultInternalCertificate) peut être sélectionné, mais un message de certificat de serveur non approuvé s'affiche. La stratégie de contrôle d'accès de contournement pour le trafic déchiffré (sysopt permit-vpn) doit être désactivée afin que les règles de stratégie d'accès aux identités des utilisateurs prennent effet ultérieurement. NAT Exempt peut également être configuré ici. Dans cette configuration, tout le trafic ipv4 provenant de l'interface interne qui se rend aux adresses IP du client AnyConnect est différent de la NAT. Pour les configurations plus complexes telles que l'épinglage externe à externe, des règles NAT supplémentaires devront être créées dans le cadre de la stratégie NAT. Les packages AnyConnect sont disponibles sur le site d'assistance Cisco : https://software.cisco.com/download/home. Une licence Plus ou Apex valide est requise pour télécharger le package AnyConnect.

Global Settings

These settings control the basic functioning of the connection. Changes to any of these options apply to all connection profiles; you cannot configure different settings in different profiles.

Certificate of Device Identity	Outside Interface
FTD-3-Manual ~	outside (GigabitEthernet0/0)
Fully-qualified Domain Name for the Outside Inter	iace
ftd3.example.com	
e.g. ravpn.example.com	
Access Control for VPN Traffic Decrypted VPN traffic is subjected to access control policy policy for decrypted traffic option bypasses the access con and the authorization ACL downloaded from the AAA server Bypass Access Control policy for decrypted to	r inspection by default. Enabling the Bypass Access Control ntrol policy, but for remote access VPN, the VPN Filter ACL er are still applied to VPN traffic raffic (sysopt permit-vpn)
NAT Exempt	
Inside Interfaces The interfaces through which remote access VPN users can connect to the internal networks	Inside Networks The internal networks remote access VPN users are allowed to use. The IP versions of the internal networks and address pools must match, either IPv4, IPv6, or both.
inside (GigabitEthernet0/1)	+
	الَّتِ any-ipv4
AnyConnect Package	
If a user does not already have the right AnyConnect packa installer when the client authenticates for the first time. The	ge installed, the system will launch the AnyConnect user can then install the package from the system.
You can download AnyConnect packages from software.cls You must have the necessary AnyConnect software license	ico.com.
Packages	



6. Dans la section Résumé, vérifiez que AnyConnect est configuré correctement, puis cliquez sur Envoyer la requête.

Summary

Review the summary of the Remote Access VPN configuration.

General		
STEP 1: CONNECTION AND CLIENT CONFIGURATION	DN	
Primary Identity Source	-	
Authentication Type	AAA Only	
Primary Identity Source	北 LAB-AD	
Fallback Local Identity Source	-	
Strip Identity Source server from username	No	
Strip Group from Username	No	
Secondary Identity Source		
Secondary Identity Source for User Authentication	ı –	
Fallback Local Identity Source	-	
O Advanced		
Authorization Server		
Accounting Server		
Client Address Pool Assignment		

7. Cliquez sur le bouton Modifications en attente en haut à droite, comme illustré dans l'image.

cisco. Firepower Dev	ice Manager Monitoring Polici	ies Objects Device: FTD-3	> 🛃 @ ?	* admin * Administrator
RA VPN +	Device Summary Remote Access VPN Conn	ection Profiles		
Connection Profiles	1 object		Q. Search	+
	# NAME	***	GROUP POLICY	ACTIONS
	1 General	Authentication: AAA Only Authorization: None Accounting: None	DftGrpPolicy	

8. Cliquez sur Déployer maintenant.



Activer la stratégie d'identité et configurer les stratégies de sécurité pour l'identité de l'utilisateur

Àce stade, les utilisateurs d'AnyConnect doivent être en mesure de se connecter correctement, mais peuvent ne pas pouvoir accéder à des ressources spécifiques. Cette étape active l'identité de l'utilisateur afin que seuls les utilisateurs des administrateurs AnyConnect puissent se connecter aux ressources internes à l'aide du protocole RDP et que seuls les utilisateurs du groupe Utilisateurs AnyConnect puissent se connecter aux ressources internes à l'aide du protocole HTTP.

1. Accédez à Politiques > Identité et cliquez sur Activer la stratégie d'identité.



Pour cette configuration, aucune autre configuration n'est nécessaire et l'action par défaut est suffisante.

cisco. Firepo	wer Device Manage	f Mor	itoring Policies	譜王 Objects	Device: FTD-3	(D 🔒 🛛) (?) :	admin Administrator	/
🛷 Security F	olicies									
	SL Decryption $ ightarrow$	Identity \Rightarrow	O Security Intellige	nce 🔶 📀 NA	T $ ightarrow$ 🕗 Acce	ess Control \Rightarrow 🛛 🗞 la	trusion			
Identity Policy	D					Q Search			¢2 +	F
			SOURCE			DESTINATION				
H NAME	AUTHENTICATION	AUTH, TYPE	ZONES	NETWORKS	PORTS	ZONES	NETWORKS	PORTS/PROT	D ACTIONS	
				There are no k	lentity rules yet.					
				Start by creating th	he first identity rule.					
				CREATE ID	ENTITY RULE					
Default Action	Passive Auth Any	Identity Source	~ 0							

2. Accédez à **Policies > NAT** et assurez-vous que NAT est configuré correctement. Si l'exception NAT configurée dans les paramètres AnyConnect est suffisante, aucune configuration supplémentaire ne sera nécessaire ici.

cisco. Firepow	er Device	Manager	Monitori	ng Policies	i‡⊞ Objects	Device: FTD-3		۵ 🔮	0?	admin Admini	strator
🛷 Security Po	licies										
□ → ○ sst	Decryption	-> 🕑 Id	entity \rightarrow ()	Security Intelligen	ce 🔶 🕑 NA	T -> 📀 Acci	ess Control \rightarrow	S Intrusion			
1 rule								Q Search			+
			OFFISINAL PACKET				TRANSLATED PACK	£Τ			
a NAME	TYPE	INTERFACES	SOUNCE AD	DESTINATIO	SOURCE PORT	DESTINATIO	SOURCE AD	DESTINATIO	SOUNCE PORT	DESTINATIO	ACTIONS
Auto NAT Rules											
> # Internet_PAT	DYNAMIC	U ANY outside	any-ipv4	ARC	ANY	ANY	Interface	ANY	ANY	ANY	

3. Accédez à **Politiques > Contrôle d'accès**. Dans cette section, l'action par défaut est définie sur Bloquer et aucune règle d'accès n'a été créée. Ainsi, une fois qu'un utilisateur AnyConnect se connecte, il ne pourra plus accéder à quoi que ce soit. Cliquez sur le symbole + ou sur Créer une règle d'accès pour ajouter une nouvelle règle.

cisco. Firepo	ower Device Manager	题 Monitoring	Ø Policies	前面 Objects	Device: FTD-3		6.	0?	adi Ad	min v ministrator
Ø Security Policies										
	🖽 -> 🔿 SSL Decryption -> 📀 Identity -> 🔿 Security Intelligence -> 📀 NAT -> 💽 Access Control -> 🗞 Intrusion									
						Q Search				@. +
	sounce			DESTINATION						
* NAME	ACTION ZONES	NETWORKS	PORTS	20NE3	NETWORKS	PORTS/PROTO	APPLICATIONS	URLS	USERS	ACTIONS
				There are no a	access rules yet.					
				Start by creating I	the first access rule.					
	CREATE ACCESS RULE									
Default Action	Access Control 😑 Block	9. E. V								

4. Remplissez les champs avec les valeurs appropriées. Dans cette configuration, les utilisateurs du groupe Admins AnyConnect doivent disposer d'un accès RDP au serveur Windows du réseau interne. Pour la source, la zone est configurée comme zone_externe, qui est l'interface externe à laquelle les utilisateurs d'AnyConnect se connecteront et le réseau est configuré en tant qu'objet AnyConnect. Pour l'identité de l'utilisateur dans FDM, la source doit être la zone et le réseau à partir desquels l'utilisateur initiera la connexion. Pour la destination, la zone est configurée en tant qu'objet Inside_Net qui est l'interface interne de Windows Server, le réseau est configuré en tant qu'objet Server et les ports/protocoles sont définis sur deux objets de port personnalisés pour permettre l'accès RDP sur TCP 3389 et UDP 3389.

Edit Access	Rul	e										×
Order Title Action 1 AC RDP Access Image: Allow mark Source/Destination Applications URLs Users Intrusion Policy File policy Logging												
SOURCE						DESTINATION						
Zones	+	Networks	÷	Ports +		Zones	÷	Networks	+	Ports/Protocols		+
outside_zone		C AnyConnect-Pool		ANY		inside_zone		Dinside_Net				
Show Diagram	\supset	Not hit yet							CA	WCEL	ок	

Dans la section Utilisateurs, le groupe Admins AnyConnect sera ajouté afin que les utilisateurs autres que ce groupe puissent accéder au RDP sur Windows Server. Cliquez sur le symbole +, sur l'onglet Groupes, sur le groupe approprié, puis sur **OK**. Notez que les utilisateurs individuels et la source d'identité peuvent également être sélectionnés.

Add Access Rule	• ×
Order Title 1 Y AC RDP Access	Action Allow
Source/Destination Applications URLs Users	Intrusion Policy File policy Logging
▼ Filter Identity Sources Groups Users	If you configure identity policies to establish user identity based on source IP address, you can control access based on user name or user group membership. By controlling access based on user identity, you can apply the appropriate access controls whether the user changes workstations or obtains a different address through DHCP. If you base rules on group membership, user
北 LAB-AD \ Account Operators 北 LAB-AD \ Administrators	 network access changes as users change roles in your organization, moving from one group to another.
LAB-AD \ Allowed RODC Password Replication Group LAB-AD \ AnyConnect Admins LAB-AD \ AnyConnect Users	Ĵ
Create new Identity Realm CANCEL OK	
Show Diagram	CANCEL OK

Une fois les options appropriées sélectionnées, cliquez sur OK.

Add Access Rule		o ×
Order Title 1 AC RDP Access Source/Destination Applications URLs U	Action Allow File policy Logging	
AVAILABLE USERS	CONTROLLING ACCESS FOR USERS AND U If you configure identity policies to establi address, you can control access based or membership. By controlling access based appropriate access controls whether the different address through DHCP. If you ba network access changes as users change from one group to another.	ISER GROUPS sh user identity based on source IP n user name or user group I on user identity, you can apply the user changes workstations or obtains a se rules on group membership, user roles in your organization, moving
Show Diagram		CANCEL OK

5. Créez davantage de règles d'accès si nécessaire. Dans cette configuration, une autre règle

d'accès est créée pour autoriser les utilisateurs du groupe AnyConnect Users à accéder au serveur Windows via HTTP.

Edit Access Rule Ø ×												
Order Title				Action								
2 🗸 AC HT	TTP A	ccess		Allow 🚿	1							
Source/Destination	Ap	plications URLs	Use	ers Intrusion Policy	F	ile policy ⁹ Logging						
SOURCE						DESTINATION						
Zones	+	Networks	+	Ports +		Zones +	Networks		+	Ports/Prot	ocols	+
outside_zone		AnyConnect-Pool		ANY		inside_zone	Dinside_	Net		🖕 нтт	>	
Show Diagram	Show Diagram O CANCEL OK											
Edit Access I	Rule	9									0	×
Order Title				Action								
2 V ACHI	TP A	ccess		Allow S								
Source/Destination	Ap	plications URLs	Use	ers Intrusion Policy	F	ile policy ⁹ Logging						
AVAILABLE USERS				+		1 CONTROLLING ACCESS	FOR USERS AN	D USER G	ROUPS			
LAB-AD \ AnyConn	ect Us	iers				If you configure identity p address, you can control i membership. By controllir appropriate access contro different address through network access changes from one group to anothe	olicies to esta access based ng access base pls whether th DHCP. If you as users chan r.	blish use on user ed on us e user c base rul ge roles	er identi r name o ser iden thanges les on g i in your	ty based o r user grou tity, you ca workstatio roup memt organizatio	n source IF up in apply thins or obtai bership, us bership, us on, moving	e ins a er
Show Diagram	\supset	e Not hit yet							CA	NCEL	ок	

6. Vérifiez la configuration de la règle d'accès, puis cliquez sur le bouton Modifications en attente

en haut à droite, comme illustré dans l'image.

ului cisc	Image: Second state Image: Second st												
øs	🕫 Security Policies												
Ð	$\Box \rightarrow \bigcirc$ SSL Decryption $\rightarrow \oslash$ Identity $\rightarrow \bigcirc$ Security Intelligence $\rightarrow \oslash$ NAT $\rightarrow \bigtriangledown$ Access Control $\rightarrow $ \clubsuit Intrusion												
2 rules								Q Search				0	+
			SOURCE			DESTINATION	3						
	NAME	ACTION	ZONES	NETWORKS	PORTS	ZONES	NETWORKS	PORTS/PROTO_	APPLICATIONS	UNLS	USERS		ACTIONS
> 1	AC RDP Access	Allow	outside_zone	AnyConnect-Pool	ANY	inside_zone	Inside_Not	RDP-TCP RDP-UDP	ANY	ANY	AnyConne	Ф.С.	
> 2	AC HTTP Access	Allow	outside_zone	AnyConnect-Pool	ANY	inside_zone	Inside_Net	HTTP	ANY	ANY	AnyConne	9 C	
Defau	Default Action Access Control 😄 Block 🖏 📴 🗸												

7. Vérifiez les modifications, puis cliquez sur Déployer maintenant.

Pe	Pending Changes 🛛 💿 🗙								
♥ 1 2	Last Deployment Completed Successfully 28 Apr 2020 01:35 PM. See Deployment History								
	Deployed Version (28 Apr 2020 01:35 PM)	Pending Version C LEG	END Removed Added	Edited					
0	Access Rule Added: AC HTTP Access								
		users[0].name: AnyConnect Users logFiles: false eventLogAction: LOG_NONE ruleId: 268435467 name: AC HITP Access							
	sourceZones:								
	- destinationZones:	outside_zone							
	-	inside_zone							
	sourceNetworks:								
	-	AnyConnect-Pool							
	destinationNetworks:								
	-	Inside_Net							
	destinationPorts:								
	-	HTTP							
	users[0].identitySource:								
	-	LAS-AD							
0	Access Rule Added: AC RDP Access			~					
MO	DRE ACTIONS Y	CANCEL	DEPLOY NOW	~					

Vérification

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Configuration finale

Configuration AAA

show running-configuration aaa-server aaa-server LAB-AD protocol ldap realm-id 7 aaa-server LAB-AD host win2016.example.com serverport 389 ldap-base-dn DC=example,DC=com ldap-scope subtree ldap-login-password ***** ldap-logindn ftd.admin@example.com server-type auto-detect

Configurer AnyConnect

```
> show running-config webvpn
webvpn
enable outside
http-headers
 hsts-server
  enable
  max-age 31536000
  include-sub-domains
  no preload
 hsts-client
  enable
 x-content-type-options
 x-xss-protection
 content-security-policy
anyconnect image disk0:/anyconnpkgs/anyconnect-linux64-4.7.03052-webdeploy-k9.pkg 1
anyconnect image disk0:/anyconnpkgs/anyconnect-win-4.7.03052-webdeploy-k9.pkg 2
anyconnect enable
tunnel-group-list enable
 cache
 disable
error-recovery disable
> show running-config tunnel-group
tunnel-group General type remote-access
tunnel-group General general-attributes
address-pool AnyConnect-Pool
authentication-server-group LAB-AD
tunnel-group General webvpn-attributes
group-alias General enable
> show running-config group-policy
group-policy DfltGrpPolicy attributes
vpn-tunnel-protocol ssl-client
split-tunnel-policy tunnelspecified
split-tunnel-network-list value DfltGrpPolicy|splitAcl
webvpn
 anyconnect ssl dtls none
> show running-config ssl
```

ssl trust-point FTD-3-Manual outside

Connexion avec AnyConnect et vérification des règles de stratégie de contrôle d'accès

Cisco AnyConnect Se	g ftd3.example.com.						
	Cisco AnyConnect ftd3.example.com Group: General Username: it.admin Password: ********						
	OK Cancel						
🚳 Cisco AnyConnect Se	cure Mobility Client — 🗆 🗙						
VPN: Connected to ftd3.example.com. ftd3.example.com ftd3.example.com							
00:00:14	IPv4						
Q (i)							

L'administrateur informatique de l'utilisateur fait partie du groupe Admins AnyConnect qui dispose d'un accès RDP à Windows Server, mais n'a pas accès au protocole HTTP. L'ouverture d'une session RDP et Firefox sur ce serveur vérifie que cet utilisateur ne peut accéder au serveur que via RDP.



Si vous êtes connecté à un utilisateur de test qui fait partie du groupe Utilisateurs AnyConnect disposant d'un accès HTTP mais non RDP, vous pouvez vérifier que les règles de stratégie de contrôle d'accès prennent effet.



Dépannage

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Déboguages

Ce débogage peut être exécuté dans l'interface CLI de diagnostic afin de dépanner les problèmes liés à l'authentification LDAP : **debug Idap 255**.

Afin de dépanner les problèmes de stratégie de contrôle d'accès d'identité utilisateur, le **système prend en charge firewall-engine-debug** peut être exécuté en clish afin de déterminer pourquoi le trafic est autorisé ou bloqué de manière inattendue.

Débogues LDAP de travail

```
[53] Session Start
[53] New request Session, context 0x00002bldl3f4bbf0, reqType = Authentication
[53] Fiber started
[53] Creating LDAP context with uri=ldap://192.168.1.1:389
[53] Connect to LDAP server: ldap://192.168.1.1:389, status = Successful
[53] supportedLDAPVersion: value = 3
[53] supportedLDAPVersion: value = 2
[53] LDAP server 192.168.1.1 is Active directory
[53] Binding as ftd.admin@example.com
[53] Performing Simple authentication for ftd.admin@example.com to 192.168.1.1
[53] LDAP Search:
Base DN = [DC=example,DC=com]
Filter = [sAMAccountName=it.admin]
```

```
Scope
              = [SUBTREE]
[53] User DN = [CN=IT Admin, CN=Users, DC=example, DC=com]
[53] Talking to Active Directory server 192.168.1.1
[53] Reading password policy for it.admin, dn:CN=IT Admin,CN=Users,DC=example,DC=com
[53] Read bad password count 6
[53] Binding as it.admin
[53] Performing Simple authentication for it.admin to 192.168.1.1
[53] Processing LDAP response for user it.admin
[53] Message (it.admin):
[53] Authentication successful for it.admin to 192.168.1.1
[53] Retrieved User Attributes:
[53]
      objectClass: value = top
       objectClass: value = person
[53]
[53]
       objectClass: value = organizationalPerson
[53]
      objectClass: value = user
      cn: value = IT Admin
[53]
[53]
      sn: value = Admin
[53]
      givenName: value = IT
[53]
      distinguishedName: value = CN=IT Admin, CN=Users, DC=example, DC=com
      instanceType: value = 4
[53]
       whenCreated: value = 20200421025811.0Z
[53]
       whenChanged: value = 20200421204622.0Z
[53]
[53]
       displayName: value = IT Admin
      uSNCreated: value = 25896
[53]
[53]
      memberOf: value = CN=AnyConnect Admins,CN=Users,DC=example,DC=com
      uSNChanged: value = 26119
[53]
      name: value = IT Admin
[53]
       objectGUID: value = &...J..O..2w...c
[53]
[53]
       userAccountControl: value = 512
[53]
      badPwdCount: value = 6
      codePage: value = 0
[53]
[53]
      countryCode: value = 0
      badPasswordTime: value = 132320354378176394
[53]
[53]
      lastLogoff: value = 0
[53]
      lastLogon: value = 0
[53]
       pwdLastSet: value = 132319114917186142
      primaryGroupID: value = 513
[53]
      objectSid: value = .....{I...;....j...
[53]
[53]
      accountExpires: value = 9223372036854775807
[53]
      logonCount: value = 0
[53]
      sAMAccountName: value = it.admin
      sAMAccountType: value = 805306368
[53]
[53]
       userPrincipalName: value = it.admin@example.com
[53]
       objectCategory: value = CN=Person, CN=Schema, CN=Configuration, DC=example, DC=com
[53]
       dSCorePropagationData: value = 16010101000000.0Z
       lastLogonTimestamp: value = 132319755825875876
[53]
[53] Fiber exit Tx=515 bytes Rx=2659 bytes, status=1
[53] Session End
```

Impossible d'établir la connexion avec le serveur LDAP

```
[-2147483611] Session Start
[-2147483611] New request Session, context 0x00007f9e65ccdc40, reqType = Authentication
[-2147483611] Fiber started
[-2147483611] Creating LDAP context with uri=ldap://171.16.1.1:389
[-2147483611] Connect to LDAP server: ldap://172.16.1.1:389, status = Failed
[-2147483611] Unable to read rootDSE. Can't contact LDAP server.
[-2147483611] Fiber exit Tx=0 bytes Rx=0 bytes, status=-2
[-2147483611] Session End
```

Solutions potentielles :

- Vérifiez le routage et assurez-vous que le serveur LDAP reçoit une réponse du FTD.
- Si LDAPS ou STARTTLS est utilisé, assurez-vous que le certificat d'autorité de certification racine correct est approuvé afin que la connexion SSL puisse s'effectuer correctement.
- Vérifiez que l'adresse IP et le port corrects sont utilisés. Si un nom d'hôte est utilisé, vérifiez que DNS est en mesure de le résoudre à l'adresse IP correcte

DN de connexion et/ou mot de passe de liaison incorrects

```
[-2147483615] Session Start
[-2147483615] New request Session, context 0x00007f9e65ccdc40, reqType = Authentication
[-2147483615] Fiber started
[-2147483615] Creating LDAP context with uri=ldap://192.168.1.1:389
[-2147483615] Connect to LDAP server: ldap://192.168.1.1:389, status = Successful
[-2147483615] defaultNamingContext: value = DC=example,DC=com
[-2147483615] supportedLDAPVersion: value = 3
[-2147483615] supportedLDAPVersion: value = 2
[-2147483615] LDAP server 192.168.1.1 is Active directory
[-2147483615] supportedSASLMechanisms: value = GSSAPI
[-2147483615] supportedSASLMechanisms: value = GSS-SPNEGO
[-2147483615] supportedSASLMechanisms: value = EXTERNAL
[-2147483615] supportedSASLMechanisms: value = DIGEST-MD5
[-2147483615] Binding as ftd.admin@example.com
[-2147483615] Performing Simple authentication for ftd.admin@example.com to 192.168.1.1
[-2147483615] Simple authentication for ftd.admin@example.com returned code (49) Invalid
credentials
[-2147483615] Failed to bind as administrator returned code (-1) Can't contact LDAP server
[-2147483615] Fiber exit Tx=186 bytes Rx=744 bytes, status=-2
[-2147483615] Session End
```

Solution potentielle : Vérifiez que le DN de connexion et le mot de passe de connexion sont configurés correctement. Ceci peut être vérifié sur le serveur AD avec **Idp.exe**. Afin de vérifier qu'un compte peut se lier correctement à l'utilisation de Idp, naviguez à travers ces étapes :

1. Sur le serveur AD, appuyez sur Win+R et recherchez ldp.exe.

💷 Run	×
	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
<u>O</u> pen:	ldp.exe ~
	OK Cancel <u>B</u> rowse

2. Cliquez sur **Connexion > Connexion...** comme le montre l'image.

🔝 Ldp	_		×
Connection Browse View Options Utilities Help			
Connect			
Bind Ctrl+B			
Disconnect			
New Ctrl+N			
Save			
Exit			
		NUM	

3. Spécifiez localhost pour le serveur et le port approprié, puis cliquez sur OK.

Connect		×
<u>S</u> erver:	localhost	
Port:	389	Co <u>n</u> nectionless
<u>0</u> K		Cancel

4. La colonne de droite affiche le texte qui indique une connexion réussie. Cliquez sur Connexion
> Lier... comme le montre l'image.

🔝 Idap://w	/in2016.ex	ample.co	om/DC	= example, DC	=com		_		\times
Connection	Browse	View	Optio	ns Utilities	Help				
Conne Bind Discon New Save Save A Exit	ct nect	Ctrl+B		Id = Idap_op Established Retrieving b Getting 1 en Dn: (RootD configu CN= current Tim defaultM dnsHos domainf dsServi Set Firs Nan con forestFo highest(isGlobal isSynch	en ("localho connection ase DSA in tries: SE) rationNamin =Configurati Time: 5/1/20 e; VamingConte tName: win ControllerFu Functionality iceName: CP tings,CN=W st-Site- me,CN=Sites n; unctionality: CommittedU ICatalogRea pronized: TF viceName: C	st", 389); <u>to localhost.</u> formation gContext: ion,DC=examp 20 4:16:55 PM ext: DC=exam 2016.example inctionality: 7 = /: 7 = (WIN201 N=NTDS IN2016,CN=Se s,CN=Configur : 7 = (WIN2010 SN: 13410; idy: TRUE; RUE; example.com:	le,DC=c 1 Easter ple,DC=c .com; = (WIN2 16); ervers,C ation,DC 6); win2016	om; n Daylight com; 016); N=Default- 2=example,	DC=

5. Sélectionnez **Liaison simple**, puis spécifiez le nom d'utilisateur et le mot de passe du compte d'annuaire. Click OK.

Bind	×				
User:	ftd.admin@example.com				
<u>D</u> omain:					
Bind type Bind as <u>c</u> ur Bind with c Simple bind <u>A</u> dvanced	rently logged on user redentials (DIGEST) affic after bind Cancel OK				

Avec une liaison réussie, ldp affiche Authenticated en tant que DOMAIN\username.

Map://win2016.example.com/DC=example,DC=com								\times		
Connection	Browse	View	Options	Utilities	Help					
				1.2. 1.2. 1.2. supporte Max Max Max Max Max Max Max Max	840.113550 840.113550 840.113550 edLDAPPol PercentDir ReceiveBut Connection BatchRetut DirSyncDut ResultSetS ResultSetS ValRange; edLDAPVe edSASLMe IEGO; EXTE	5.1.4.2255; 6.1.4.2256; 6.1.4.2309; icies (20): Mi SyncReques iffer; InitRecuns; MaxConn rnMessages ration; MaxT Size; MinResu PerConn; Max MaxValRang Limit; Syster rsion (2): 3; 2 chanisms (4 RNAL; DIGE _s(Id, 'ftd.ad	axPoolThr sts; MaxDa vTimeout; IdleTime; I ; MaxQuel empTable: ultSets; axNotificat geTransitiv mMemoryL 2;): GSSAPI ST-MD5; min@exar min'.	eads; atagramR MaxPage ryDuratio Size; tionPerCo ve; .imitPerce I; GSS-	lecv; Size; m; onn; ent;	
Ready										:

Si vous tentez une liaison avec un nom d'utilisateur ou un mot de passe non valide, cela entraînera un échec comme celui-ci.

🔝 Idap://w	in2016.exa	mple.co	om/DC=ex	ample,DC:	=com		_		×
Connection	Browse	View	Options	Utilities	Help				
				Max Max Max Thre supporte supporte SPN es = Idap_s unavailable unavailable unavailable suthenticate	ResultSetS ResultSets ValRange; eadMemory edLDAPVe edSASLMe IEGO; EXTE imple_bind >; // v.3 ed as: 'EXA	Size; MinResu PerConn; Ma MaxValRang (Limit; Syster rsion (2): 3; 2 chanisms (4 RNAL; DIGE _s(Id, 'ftd.ad MPLE\ftd.adr _s(Id, 'wrong	ultSets; axNotificat geTransition MemoryL 2;): GSSAP ST-MD5; min@exan min'. g@examp	tionPerConr ve; .imitPercent I; GSS- mple.com',	;
			< E S C E ir	unavailable rror <49>: I server error comment: Ac rror 0x8009 ivalid	>); // v.3 Idap_simple :: 80090308 cceptSecur 90308 The	e_bind_s() fa 3: LdapErr: D rityContext e token supplie	ailed: Inval SID-0C09 rror, data ed to the f	id Credentia 042A, 52e, v3839 unction is	ils ∀
Ready									

Serveur LDAP introuvable Nom d'utilisateur

```
[-2147483612] Session Start
[-2147483612] New request Session, context 0x00007f9e65ccdc40, reqType = Authentication
[-2147483612] Fiber started
[-2147483612] Creating LDAP context with uri=ldap://192.168.1.1:389
[-2147483612] Connect to LDAP server: ldap://192.168.1.1:389, status = Successful
[-2147483612] supportedLDAPVersion: value = 3
[-2147483612] supportedLDAPVersion: value = 2
[-2147483612] LDAP server 192.168.1.1 is Active directory
[-2147483612] Binding as ftd.admin@example.com
[-2147483612] Performing Simple authentication for ftd.admin@example.com to 192.168.1.1
[-2147483612] LDAP Search:
       Base DN = [dc=example,dc=com]
       Filter = [samaccountname=it.admi]
       Scope
              = [SUBTREE]
[-2147483612] Search result parsing returned failure status
[-2147483612] Talking to Active Directory server 192.168.1.1
[-2147483612] Reading password policy for it.admi, dn:
[-2147483612] Binding as ftd.admin@example.com
[-2147483612] Performing Simple authentication for ftd.admin@example.com to 192.168.1.1
[-2147483612] Fiber exit Tx=456 bytes Rx=1082 bytes, status=-1
[-2147483612] Session End
```

Solution potentielle : Vérifiez qu'AD peut trouver l'utilisateur avec la recherche effectuée par le FTD. Cela peut également être fait avec ldp.exe.

1. Une fois la liaison établie, accédez à Affichage > Arborescence comme indiqué dans l'image.

🔝 Idap://w	🔝 Idap://win2016.example.com/DC=example,DC=com — 🗆 🗙							×		
Connection	Browse	View	/ Option	s Utilities	Help					
		~	Tree Enterprise Status Ba Set Font	e Configurat r	ion	Ctrl+T	AaxPoo sts; Ma svTime nktleTin s; Max	v; re;		
		MaxDirSyncDuration; MaxTempTableSize; MaxResultSetSize; MinResultSets; MaxResultSetsPerConn; MaxNotificationPerConn MaxValRange; MaxValRangeTransitive; ThreadMemoryLimit; SystemMemoryLimitPercent supportedLDAPVersion (2): 3; 2; supportedSASLMechanisms (4): GSSAPI; GSS- SPNEGO; EXTERNAL; DIGEST-MD5;							erConn Percent; S-	;
				res = ldap_s <unavailable Authenticate</unavailable 	imple_bii >>); // v.3 ed as: 'E>	nd_s(ld, 'ftd KAMPLE\ftd	l.admin@ .admin'.	example.	.com',	~

2. Spécifiez le DN de base configuré sur le FTD, puis cliquez sur OK.

Tree View	×
BaseDN: DC=example,DC=com	~
Cancel	OK

3. Cliquez avec le bouton droit sur le DN de base, puis cliquez sur Rechercher comme indiqué dans l'image.

🔝 Idap://wi	n2016.exa	mple.co	om/DC=ex	ample,DC	=com	_		×
Connection	Browse	View	Options	Utilities	Help			
<mark>. DC=exam</mark>	iple,DC=c	om	Search Virtual L Delete Modify Modify Add chil Compar Advance Copy DN Copy Select al Clear ou	ist View DN Id e ed N	Ctrl+S Ctrl+D Ctrl+M Ctrl+R Ctrl+A ; Ctrl+A	cipals,DC=examp 11D2B9AA00C0 =example,DC=co E11D297C400C0 example,DC=co 11D1ADED00C0 =example,DC=co 11D1ADED00C0 ple,DC=com; 11D1AA4B00C0 s,DC=example,DC 11D1ADED00C0 ample,DC=com; 311D1ADED00C0 e,DC=com; 0 3:43:59 PM East	ole,DC=com 4F79F805:C m; 4FD8D5CD: m; 4FD8D5CD: m; 4FD8D5CD: 4FD8D5CD: 4FD8D5CD: 4FD8D5CD: 04FD8D5CD: 04FD8D5CD stern Daylig tern Dayligh	C C C C C C C C C C C C C C C C C C C
			-					>
Create a new o	locument							

4. Spécifiez les mêmes valeurs de base DB, de filtre et d'étendue que celles indiquées dans les débogages. Dans cet exemple, voici :

- DN de base : dc=exemple,dc=com
- Filtre : samaccountname=it.admi
- Champ d'application : SOUS-ARBRE

🟠 Idap://w	n2016.example.com/DC=example,DC=com	– 🗆 ×
Connection	Browse View Options Utilities Help	
Search	>	C=example,DC=com; S8811D1ADED00C04FD8D5CD:C
Base DN:	DC=example,DC=com	58811D1ADED00C04FD8D5CD:C
Filter:	sAMAccountName=it.admi ~	ample,DC=com; D211D1AA4B00C04FD7D83A:O
Scope Base	One Level Subtree	lers,DC=example,DC=com; 58811D1ADED00C04FD8D5CD:C example,DC=com;
Attributes:	objectClass;name;description;canonicalName ~	68811D1ADED00C04FD8D5CD:C mple,DC=com; :020 3:43:59 PM Eastern Daylight
Options	Run Close)20 2:41:57 PM Eastern Daylight
	***Searching Idap_search_s(Id, "DC "sAMAccountName=it. Getting 0 entries:	=example,DC=com", 2, admi", attrList, 0, &msg) ∀
Ready		

ldp trouve 0 entrée car il n'y a pas de compte utilisateur avec **samaccountname=it.admi** sous le DN de base dc=example,dc=com.

Une nouvelle tentative avec le **nom_compte=it.admin** correct montre un résultat différent. Idp trouve 1 entrée sous le DN de base dc=exemple, dc=com et imprime le DN de cet utilisateur.

Idap://win2016.example.com/DC=exam	ple,DC	=com		– 🗆 ×
Connection Browse View Options U	tilities	Help		
Search			×	58811D1ADED00C04FD8D5CD:C DC=example,DC=com; 58811D1ADED00C04FD8D5CD:C
Base DN: DC=example,DC=com			\sim	ample,DC=com;
Filter: sAMAccountName=it.admin			\sim	lers,DC=example,DC=com;
Scope O <u>B</u> ase O <u>O</u> ne Level <u>Subtree</u>				58811D1ADED00C04FD8D5CD:C example,DC=com; 68811D1ADED00C04FD8D5CD:C mple,DC=com;
Attributes: objectClass;name;description;ca	nonicali	Name	\sim	020 3:43:59 PM Eastern Daylight
O <u>p</u> tions <u>R</u> un		<u>C</u> lose)20 2:41:57 PM Eastern Daylight
***Se Idap "sAM Getti Dn:	earching search Accou ing 1 en CN=IT A canonic name: IT objectCl use	g n_s(ld, " ntName tries: Admin, alName Admin; ass (4): r;	DC=e =it.ad CN=U : exar ; : top;	example,DC=com", 2, Imin", attrList, 0, &msg) Jsers,DC=example,DC=com mple.com/Users/IT Admin; person; organizationalPerson;
Ready				

Mot de passe incorrect pour le nom d'utilisateur

```
[-2147483613] Session Start
[-2147483613] New request Session, context 0x00007f9e65ccdc40, reqType = Authentication
[-2147483613] Fiber started
[-2147483613] Creating LDAP context with uri=ldap://192.168.1.1:389
[-2147483613] Connect to LDAP server: ldap://192.168.1.1:389, status = Successful
[-2147483613] supportedLDAPVersion: value = 3
[-2147483613] supportedLDAPVersion: value = 2
[-2147483613] LDAP server 192.168.1.1 is Active directory
[-2147483613] Binding as ftd.admin@example.com
[-2147483613] Performing Simple authentication for ftd.admin@example.com to 192.168.1.1
[-2147483613] LDAP Search:
        Base DN = [dc=example,dc=com]
        Filter = [samaccountname=it.admin]
               = [SUBTREE]
        Scope
[-2147483613] User DN = [CN=IT Admin, CN=Users, DC=example, DC=com]
[-2147483613] Talking to Active Directory server 192.168.1.1
[-2147483613] Reading password policy for it.admin, dn:CN=IT Admin,CN=Users,DC=example,DC=com
[-2147483613] Read bad password count 0
[-2147483613] Binding as it.admin
[-2147483613] Performing Simple authentication for it.admin to 192.168.1.1
```

```
[-2147483613] Simple authentication for it.admin returned code (49) Invalid credentials
[-2147483613] Message (it.admin): 80090308: LdapErr: DSID-0C09042A, comment:
AcceptSecurityContext error, data 52e, v3839
[-2147483613] Invalid password for it.admin
[-2147483613] Fiber exit Tx=514 bytes Rx=2764 bytes, status=-1
[-2147483613] Session End
```

Solution potentielle : Vérifiez que le mot de passe de l'utilisateur est configuré correctement et qu'il n'a pas expiré. Tout comme le DN de connexion, le FTD établit une liaison avec AD avec les informations d'identification de l'utilisateur. Cette liaison peut également être effectuée dans ldp afin de vérifier que la distance administrative est capable de reconnaître les mêmes informations d'identification de nom d'utilisateur et de mot de passe. Les étapes de ldp sont affichées dans la section Liaison du nom de connexion et/ou du mot de passe incorrect. En outre, les journaux de l'Observateur d'événements du serveur Microsoft peuvent être examinés pour une raison potentielle.

Test AAA

La commande test aaa-server peut être utilisée afin de simuler une tentative d'authentification du FTD avec un nom d'utilisateur et un mot de passe spécifiques. Ceci peut être utilisé pour tester les échecs de connexion ou d'authentification. La commande est **test aaa-server authentication [AAA-server] host [AD IP/hostname]**.

```
> show running-configuration aaa-server
aaa-server LAB-AD protocol ldap
realm-id 7
aaa-server LAB-AD host win2016.example.com
server-port 389
ldap-base-dn DC=example,DC=com
ldap-scope subtree
ldap-login-password *****
ldap-login-dn ftd.admin@example.com
server-type auto-detect
> test aaa-server authentication LAB-AD host win2016.example.com
Username: it.admin
Password: *******
INFO: Attempting Authentication test to IP address (192.168.1.1) (timeout: 12 seconds)
INFO: Authentication Successful
```

Captures de paquets

Les captures de paquets peuvent être utilisées pour vérifier l'accessibilité au serveur AD. Si les paquets LDAP quittent le FTD, mais qu'il n'y a pas de réponse, cela peut indiquer un problème de routage.

Voici une capture qui montre le trafic LDAP bidirectionnel :

```
> show route 192.168.1.1
Routing entry for 192.168.1.0 255.255.255.0
Known via "connected", distance 0, metric 0 (connected, via interface)
Routing Descriptor Blocks:
 * directly connected, via inside
     Route metric is 0, traffic share count is 1
```

```
> capture AD interface inside match tcp any host 192.168.1.1 eq 389
> show capture
capture AD type raw-data interface inside [Capturing - 0 bytes]
 match tcp any host 192.168.1.1 eq ldap
> test aaa-server authentication LAB-AD host win2016.example.com username it.admin password
*****
INFO: Attempting Authentication test to IP address (192.168.1.1) (timeout: 12 seconds)
INFO: Authentication Successful
> show capture
capture AD type raw-data interface inside [Capturing - 10905 bytes]
 match tcp any host 192.168.1.1 eq ldap
> show capture AD
54 packets captured
  1: 23:02:16.770712
                          192.168.1.17.61960 > 192.168.1.1.389: S 3681912834:3681912834(0) win
32768 <mss 1460,nop,nop,timestamp 1061373057 0>
   2: 23:02:16.772009
                      192.168.1.1.389 > 192.168.1.17.61960: S 491521506:491521506(0) ack
3681912835 win 8192 <mss 1460,nop,nop,timestamp 762393884 1061373057>
   3: 23:02:16.772039
                          192.168.1.17.61960 > 192.168.1.1.389: . ack 491521507 win 32768
<nop,nop,timestamp 1061373058 762393884>
   4: 23:02:16.772482
                          192.168.1.17.61960 > 192.168.1.1.389: P 3681912835:3681912980(145)
ack 491521507 win 32768 <nop,nop,timestamp 1061373059 0>
                          192.168.1.1.389 > 192.168.1.17.61960: P 491521507:491522141(634) ack
   5: 23:02:16.772924
3681912980 win 65160 <nop,nop,timestamp 762393885 1061373059>
   6: 23:02:16.772955
                          192.168.1.17.61960 > 192.168.1.1.389: . ack 491522141 win 32768
<nop,nop,timestamp 1061373059 762393885>
  7: 23:02:16.773428
                          192.168.1.17.61960 > 192.168.1.1.389: P 3681912980:3681913024(44)
ack 491522141 win 32768 <nop,nop,timestamp 1061373060 0>
  8: 23:02:16.775030
                         192.168.1.1.389 > 192.168.1.17.61960: P 491522141:491522163(22) ack
3681913024 win 65116 <nop,nop,timestamp 762393887 1061373060>
                      192.168.1.17.61960 > 192.168.1.1.389: . ack 491522163 win 32768
   9: 23:02:16.775075
<nop,nop,timestamp 1061373061 762393887>
[...]
54 packets shown
```

Journaux de l'Observateur d'événements Windows Server

Les journaux de l'Observateur d'événements sur la van du serveur AD fournissent des informations plus détaillées sur les raisons d'une défaillance.

1. Recherchez et ouvrez Observateur d'événements.

=	Best match
ŵ	Event Viewer Desktop app
	Settings >
	Wiew event logs
٢	
	event
	ዶ 🖬 🧀 🔒 🛽

2. Développez **Journaux Windows** et cliquez sur **Sécurité**. Recherchez **Échec de l'audit** avec le nom de compte de l'utilisateur et vérifiez les informations d'échec comme indiqué dans l'image.



An account failed to log on.

Subject: Security ID:SYSTEM Account Name:WIN2016\$ Account Domain:EXAMPLE Logon ID:0x3E7

Logon Type:3

Account For Which Logon Failed: Security ID:NULL SID Account Name:it.admin Account Domain:EXAMPLE

Failure Information:

Failure Reason: The specified user account has expired. Status: 0xC0000193 Sub Status: 0x0

Process Information: Caller Process ID:0x25c Caller Process Name:C:\Windows\System32\lsass.exe

Network Information: Workstation Name:WIN2016 Source Network Address:192.168.1.17 Source Port:56321