# Configurer l'identité d'utilisateur et l'authentification d'AD (LDAP) sur FTD géré par FMC pour les clients AnyConnect

## Table des matières

Introduction Conditions préalables **Exigences** Composants utilisés Informations générales Configurer Diagramme et scénario du réseau **Configurations Active Directory** Déterminer le DN de base LDAP et le DN de groupe Créer un compte FTD Créer des groupes AD et ajouter des utilisateurs à des groupes AD (facultatif) Copier la racine du certificat SSL LDAPS (obligatoire uniquement pour LDAPS ou STARTTLS) **Configurations FMC** Vérifier les licences Configurer le domaine Configurer AnyConnect pour l'authentification AD Activer la stratégie d'identité et configurer les stratégies de sécurité pour l'identité utilisateur Configurer l'exemption NAT **Déploiement** Vérifier **Configuration finale Configuration AAA Configuration AnyConnect** Connexion à AnyConnect et vérification des règles de stratégie de contrôle d'accès Vérifier avec les événements de connexion FMC Dépannage Déboguages Débogages LDAP en cours Impossible d'établir une connexion avec le serveur LDAP DN et/ou mot de passe de connexion incorrects Le serveur LDAP ne trouve pas le 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

Ce document décrit comment configurer l'authentification AD pour les clients AnyConnect qui se connectent à Cisco Firepower Threat Defense (FTD).

## Conditions préalables

### Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissances de base de la configuration VPN RA sur FMC
- Connaissances de base de la configuration du serveur LDAP sur FMC
- Connaissances de base d'Active Directory (AD)

#### Composants utilisés

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

- Microsoft 2016 Server
- FMCv version 6.5.0
- FTDv 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.

#### Informations générales

Ce document décrit comment configurer l'authentification Active Directory (AD) pour les clients AnyConnect qui se connectent à Cisco Firepower Threat Defense (FTD), géré par Firepower Management Center (FMC).

L'identité de l'utilisateur est utilisée dans les politiques d'accès pour limiter les utilisateurs d'AnyConnect à des adresses IP et des ports spécifiques.

## Configurer

#### Diagramme et scénario du réseau





inside

outside

Windows Server

AnyConnect Client

Le serveur Windows est préconfiguré avec IIS et RDP afin de tester l'identité des utilisateurs. Dans ce guide de configuration, trois comptes d'utilisateurs et deux groupes sont créés.

Comptes utilisateurs:

- FTD Admin : il s'agit du compte d'annuaire permettant au FTD de se lier au serveur Active Directory.
- IT Admin : compte d'administrateur de test utilisé pour démontrer l'identité de l'utilisateur.

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

- AnyConnect Admins : groupe de test ajouté par l'administrateur informatique pour démontrer l'identité de l'utilisateur. Ce groupe dispose uniquement d'un accès RDP au serveur Windows.
- AnyConnect Users : groupe de test ajouté par l'utilisateur test pour démontrer l'identité de l'utilisateur. Ce groupe dispose uniquement d'un accès HTTP au serveur Windows.

### **Configurations Active Directory**

Afin de configurer correctement l'authentification AD et l'identité de l'utilisateur sur FTD, quelques valeurs sont requises.

Tous ces détails doivent être créés ou collectés sur le serveur Microsoft avant que la configuration puisse être effectuée sur FMC. Les principales valeurs sont les suivantes :

#### · le nom de domaine:

Il s'agit du nom de domaine du serveur. Dans ce guide de configuration, example.com est le nom de domaine.

#### Adresse IP/FQDN du serveur :

Adresse IP ou nom de domaine complet (FQDN) utilisé pour atteindre le serveur Microsoft. Si un nom de domaine complet est utilisé, un serveur DNS doit être configuré dans FMC et FTD pour résoudre le nom de domaine complet.

Dans ce guide de configuration, cette valeur est win2016.example.com (qui correspond à 192.168.1.1).

#### • Port du serveur :

Port utilisé par le service LDAP. Par défaut, LDAP et STARTTLS utilisent le port TCP 389 pour LDAP, et LDAP sur SSL (LDAPS) utilise 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 FMC et FTD pour établir une liaison avec le serveur LDAP, authentifier les utilisateurs et rechercher des utilisateurs et des groupes.

Un compte nommé FTD Admin est créé à cette fin.

#### • Nom distinctif (DN) de base et de groupe :

Le DN de base est le point de départ du FMC et le FTD indique à Active Directory de commencer la recherche et l'authentification des utilisateurs.

De même, le nom de domaine du groupe est le point de départ où FMC indique à Active Directory où commencer la recherche de groupes pour l'identité de l'utilisateur.

Dans ce guide de configuration, le domaine racine example.com est utilisé comme DN de base et DN de groupe.

Cependant, pour un environnement de production, il est préférable d'utiliser un **DN de base** et un **DN de groupe** plus loin dans la hiérarchie LDAP.

Par exemple, cette hiérarchie LDAP :



Si un administrateur souhaite que les utilisateurs au sein de l'unité d'organisation **Marketing** puissent authentifier le DN de base, il peut être défini sur la racine (example.com).

Cependant, cela permet également à l'utilisateur1 sous 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 **Research**.

DN de base défini sur example.com



Afin de limiter les connexions au seul utilisateur dans l'unité d'organisation **Marketing** et en dessous, l'administrateur peut à la place définir le DN de base sur **Marketing**.

Désormais, seuls User2 et User3 peuvent s'authentifier, car la recherche commence par **Marketing**.

DN de base défini sur Marketing



Notez que pour un contrôle plus granulaire au sein du FTD pour lequel les utilisateurs sont autorisés à se connecter ou à attribuer aux utilisateurs des autorisations différentes en fonction de leurs attributs AD, un mappage d'autorisation LDAP doit être configuré.

Pour plus d'informations à ce sujet, cliquez ici : <u>Configurez le mappage LDAP AnyConnect sur</u> <u>Firepower Threat Defense (FTD)</u>.

Cette hiérarchie LDAP simplifiée est utilisée dans ce guide de configuration et le DN de la racine example.com est utilisé pour le DN de base et le DN de groupe.



Déterminer le DN de base LDAP et le DN de groupe

1. Ouvrez Utilisateurs et ordinateurs Active Directory.

=	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** (pour ouvrir le conteneur), cliquez avec le bouton droit sur le **domaine racine**, puis sous **Affichage**, cliquez sur **Fonctionnalités avancées**.



3. Cela permet d'afficher des propriétés supplémentaires sous les objets AD. Par exemple, pour trouver le DN de la racine example.com, cliquez avec le bouton droit sur example.com, puis choisissez **Propriétés**.



4. Sous **Propriétés**, sélectionnez l'onglet **Éditeur d'attributs**. Recherchez **nomDistinct** sous **Attributs**, puis cliquez sur **Afficher**.

example.	com Propertie	5				?	×
General	Managed By	Object	Security	Attribut	te Editor		
Attribute	88:						
Attribu	te	Valu	e				^
dc		exan	nple				
defau	tLocalPolicyOb	j knot	set>				
descri	ption	<not< td=""><th>set&gt;</th><td></td><td></td><td></td><td></td></not<>	set>				
deskt	op Profile	knot	set>				
displa	yName	knot	set>				
displa	vNamePrintable	e knot	set>	_			
disting	uishedName	DC=	example_D	C=com			
domai	nPolicyObject	<not< td=""><th>set&gt;</th><td></td><td></td><td></td><td></td></not<>	set>				
domai	nReplica	<not< td=""><th>set&gt;</th><td></td><td></td><td></td><td></td></not<>	set>				
dSAS	ignature	{ V1	: Flags = O	0; Later	icySecs :	= 0; DsaGu	JiC
dSCo	rePropagationD	0x0	=()				
eFSP	olicy	<not< td=""><th>set&gt;</th><td></td><td></td><td></td><td></td></not<>	set>				
exten	sionName	<not< td=""><th>set&gt;</th><td></td><td></td><td></td><td></td></not<>	set>				
flags		<not< td=""><th>set&gt;</th><td></td><td></td><td></td><td>~</td></not<>	set>				~
<						3	>
V	ew					Filter	,
	OK		Cancel		Apply	Н	elp

5. Une nouvelle fenêtre s'ouvre, dans laquelle le numéro de répertoire peut être copié et collé dans FMC ultérieurement. Dans cet exemple, le DN racine est DC=example,DC=com.

Copiez la valeur et enregistrez-la pour plus tard. Cliquez sur OK pour quitter la fenêtre Éditeur d'attributs de chaîne et cliquez à nouveau sur OK pour quitter les Propriétés.

the second				
nbute: distingui:	neoname			
lue:				
C-example, DC-com			Undo	
Clear	OK	Cancel	Cut	
		_	Copy	
			Paste	
			Delete	
			Venue	
			Select All	
			Right to left Reading order	
			Show Unicode control characters	
			Insert Unicode control character	
ample.com Properties	ſ	×		
ample.com Properties	f	×		
eneral Managed By O	r bject Security Attribute Editor	×		
eneral   Managed By   O Attributes:	pject Security Attribute Editor	×		
ample.com Properties eneral Managed By O Attributes: Attribute	r bject Security Attribute Editor	×		
eneral Managed By O Attributes: Attribute cn	r bject Security Attribute Editor Value <not set=""></not>	^		
eneral Managed By O Attributes: Attribute cn controlAccessRights	r bject Security Attribute Editor Value <not set=""> <not set=""></not></not>	^		
emple.com Properties eneral Managed By O Attributes: Attribute cn controlAccessRights creation Time	Value <pre> value <pre> cnot set&gt; 4/29/2020 2:43:49 PM Eastern Dayligh </pre></pre>	nt Tim		
eneral Managed By O Attributes: Attribute cn controlAccessRights creationTime dc	f bject Security Attribute Editor Value <not set=""> <not set=""> 4/29/2020 2:43:49 PM Eastern Dayligh example</not></not>	nt Tim		
eneral Managed By O Attributes: Attribute cn controlAccessRights creationTime dc defaultLocalPolicyObj desortetion	yect Security Attribute Editor Value <not set=""> <not set=""> 4/29/2020 2:43:49 PM Eastern Dayligh example <not set=""></not></not></not>	nt Tim		
eneral Managed By O Attributes: Attribute cn controlAccessRights creationTime dc defaultLocalPolicyObj description desktooPmfile	Value <pre> value <pre> cnot set&gt; 4/29/2020 2:43:49 PM Eastern Dayligh example <pre> cnot set&gt; cnot set&gt; <pre> cnot set&gt; cnot set&gt; </pre></pre></pre></pre>	nt Tim		
emple.com Properties eneral Managed By O Attributes: Attribute cn controlAccessRights creationTime dc defaultLocalPolicyObj description desktopProfile displayName	Value (not set> (not set> 4/29/2020 2:43:49 PM Eastern Daylight example (not set> (not set>) (not set> (not set> (not set>) (not set> (not set>) (not set> (not set>) (not set> (not set>) (not set> (not set>) (not set> (not set> (not set>) (not set>) (not set>) (not set> (not set>) (not s	nt Tim		
eneral Managed By O Attributes: Attribute cn controlAccessRights creation Time dc defaultLocalPolicyObj description desktopProfile displayName displayName	f bject Security Attribute Editor Value <not set=""> <not set=""> 4/29/2020 2:43:49 PM Eastern Dayligh example <not set=""> <not set=""> &lt;</not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not>	nt Tim		
eneral Managed By O Attributes: Attribute cn controlAccessRights creationTime dc defaultLocalPolicyObj description desktopProfile displayName displayName distinguishedName	Value (not set) 4/29/2020 2:43:49 PM Eastern Dayligh example (not set) (not set) (	nt Tim		
eneral Managed By O Attributes: Attributes: Attribute cn controlAccessRights creationTime dc defaultLocalPolicyObj description desktopProfile displayName displayName displayName displayName displayName displayName	Value (not set> (not set> 4/29/2020 2:43:49 PM Eastern Daylight example (not set> (not set>) (not set> (not set> (not set>) (not set> (not set>) (not set> (not set>) (not set> (not set>) (not set> (not set>) (not set>) (not set>) (not set> (not set>) (not set>)	nt Tim		
eneral Managed By O Attributes: Attribute cn controlAccessRights creationTime dc defaultLocalPolicyObj description desktopProfile displayName displayNamePrintable distinguishedName domainPolicyObject domainReplica	Value (not set> (not set> 4/29/2020 2:43:49 PM Eastern Daylight example (not set> (not set>) (not set> (not set> (not set>) (not set> (not set>) (not set> (not set> (not set>) (not set> (not set>) (not set> (not set>) (not set> (not set>) (not set> (not set>) (not set> (not set>) (not set>) (not set> (not set>) (not	nt Tim		
eneral Managed By O Attributes: Attribute cn controlAccessRights creationTime dc defaultLocalPolicyObj description desktopProfile displayName displayName displayName distinguishedName domainPolicyObject domainReplica dSASignature	bject Security Attribute Editor Value <pre> value </pre> </pre> </pre> <pre> value <pre> value <pre> value <pre> value <pre> value </pre> </pre> </pre> </pre> </pre> </pre> <pre> value </pre> </pre> </pre> </pre> <pre> value </pre> <pre> value </pre> </pre> </pre> </pre> </pre> <pre> value <pre> value <pre> value <pre> value <pre> value </pre> </pre> </pre> </pre> </pre> </pre> <pre> value <pre> value <pre> value <pre> value <pre> value </pre> </pre> </pre> </pre> <pre> value <pre> value <pre> value <pre> value </pre> </pre> </pre> <pre> value <pre> value <pre> value <pre> value <pre> value <pre> value </pre> <pre> value </pre> </pre> </pre> <pre> value <pre> value <pre> value </pre> </pre> </pre> </pre> </pre> <pre> value <pre> value </pre> </pre> </pre> </pre> </pre> </pre> </pre> <pre> value </pre> <pre> value </pre> <pre> value <pre> value </pre> </pre> <pre> value </pre> <pre> value </pre> <	nt Tim		
eneral Managed By O Attributes: Attribute cn controlAccessRights creationTime dc defaultLocalPolicyObj description desktopProfile displayName displ	bject Security Attribute Editor Value <pre> value </pre> </pre> <pre> value <pre> value <pre> value </pre> </pre> <pre> value </pre> <pre> value </pre> </pre> <pre> value </pre> <pre> value </pre> </pre> <	nt Tim		
eneral Managed By O Attributes: Attributes: Attribute cn controlAccessRights creationTime dc defaultLocalPolicyObj description desktopProfile displayName displayName displayNamePrintable distinguishedName domainPolicyObject domainReplica dSASignature dSCorePropagationD <	Value (not set> (not set> () ])	nt Tim		
emeral Managed By O Attributes: Attribute cn controlAccessRights creationTime dc defaultLocalPolicyObj description desktopProfile displayNamePrintable distinguishedName domainPolicyObject domainReplica dSASignature dSCorePropagationD <	bject Security Attribute Editor Value  (not set> (vit s	nt Tim		

Cette opération peut être effectuée pour plusieurs objets dans **Active Directory**. Par exemple, ces étapes sont utilisées pour rechercher le DN du conteneur **Utilisateur** :

Active Directory Users and C	omputers	-	$\times$
File Action View Help			
🗢 🔿 🙍 🚾 🖌 🗈 👂	Users Properties ? ×		
<ul> <li>Active Directory Users and Q</li> <li>Saved Queries</li> <li>Saved Queries</li> <li>Saved Queries</li> <li>Builtin</li> <li>Computers</li> <li>Domain Controllers</li> <li>ForeignSecurityPrinc</li> <li>LostAndFound</li> <li>Hongram Data</li> <li>System</li> <li>Users</li> <li>NTDS Quotas</li> <li>TPM Devices</li> </ul>	Users Properties ? X General Object Security Attribute Editor Attributes: Attribute Value ^ ^ adminDescription <not set=""> adminDisplayName <not set=""> on Users defaultClassStore <not set=""> defaultClassStore <not set=""> defaultClassStore <not set=""> defaultClassStore <not set=""> displayName <not set=""> fSMORoleOwner <not set=""> instanceType Qx4 = (WRITE) *</not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not>		*
	OK Cancel Apply Help		
<			~

6. La vue **Fonctionnalités avancées** peut être supprimée en cliquant à nouveau avec le bouton droit sur le DN racine, puis sous **Affichage**, cliquez de nouveau sur **Fonctionnalités avancées**.



#### Créer un compte FTD

Ce compte d'utilisateur permet à FMC et au FTD de se lier à Active Directory afin de rechercher des utilisateurs et des groupes et d'authentifier des utilisateurs.

L'objectif de la création d'un compte FTD distinct est d'empêcher tout accès non autorisé à un autre emplacement du réseau si les informations d'identification utilisées pour la liaison sont compromises.

Il n'est pas nécessaire que ce compte soit compris dans l'étendue du DN de base ou du DN de groupe.

1. Dans **Utilisateurs et ordinateurs Active Directory**, cliquez avec le bouton droit sur le conteneur/l'organisation auquel le compte FTD est ajouté.

Dans cette configuration, le compte FTD est ajouté sous le conteneur **Users** sous le nom d'utilisateur <u>ftd.admin@example.com</u>.

Cliquez avec le bouton droit sur Users, puis accédez à New > User.

Active Directory Users and Computers	-	×	
File Action View Help			
🗢 🔿 📶 🥉 🛅 🗶 🖼 Q	i 🗟 🛛 🖬 🗏 📚 🛍 🔻 🚨 🗞		
Active Directory Users and Com Saved Queries Saved Queries Saved Queries Demain Controllers Saved Queries Domain Controllers Saved Queries Domain Controllers Saved Queries Delegate Control Find	me Type Description DefaultAcco User A user account manage Denied ROD Security Group Members in this group c DnsAdmins Security Group DNS Administrators Gro DnsUpdateP Security Group DNS clients who are per Domain Ad Security Group All workstations and ser All domain guests ers Security Group All domain guests ers Security Group All domain users		^
New All Tasks View Refresh Export List Properties Help Subset of the second seco	Computer         Contact         Group         InetOrgPerson         msDS-KeyCredential         msDS-ResourcePropertyList         msDS-ShadowPrincipalContainer         msImaging-PSPs         MSMQ Queue Alias         Printer         VseAllow         User         Shared Folder		~

## 2. Accédez à l'Assistant Nouvel objet - Utilisateur.

New Object - User		Х
🤱 Create in:	example.com/Users	
First name:	FTD Initials:	
Last name:	Admin	
Full name:	FTD Admin	
User logon name:		
ftd.admin	@example.com ~	
User logon name (pre	Windows 2000):	
EXAMPLE\	ftd.admin	
	< Back Next > Cance	4

New Object - User		×
🤱 Create in: examp	ole.com/Users	
Password:	•••••	
Confirm password:	••••••	
User must change passwor	rd at next logon	
User cannot change passw	vord	
Password never expires		
Account is disabled		
		0
	< Back Next >	Cancel
New Object - User		×
New Object - User	ole.com/Users	×
New Object - User Create in: examp When you click Finish, the follow	ole.com/Users owing object will be created:	×
New Object - User Create in: examp When you click Finish, the folk Full name: FTD Admin	ole.com/Users owing object will be created:	×
New Object - User Create in: examp When you click Finish, the folk Full name: FTD Admin User logon name: ftd.admin@	ole.com/Users owing object will be created: /example.com	×
New Object - User Create in: examp When you click Finish, the folk Full name: FTD Admin User logon name: ftd.admin@ The password never expires.	ole.com/Users owing object will be created: /example.com	×
New Object - User Create in: examp When you click Finish, the folk Full name: FTD Admin User logon name: ftd.admin@ The password never expires.	owing object will be created: wample.com	×
New Object - User Create in: examp When you click Finish, the folk Full name: FTD Admin User logon name: ftd.admin@ The password never expires.	ole.com/Users owing object will be created: /example.com	×
New Object - User Create in: examp When you click Finish, the folk Full name: FTD Admin User logon name: ftd.admin@ The password never expires.	ole.com/Users owing object will be created: /example.com	×
New Object - User Create in: examp When you click Finish, the folk Full name: FTD Admin User logon name: ftd.admin@ The password never expires.	owing object will be created: /example.com	×
New Object - User Create in: examp When you click Finish, the folk Full name: FTD Admin User logon name: ftd.admin@ The password never expires.	owing object will be created: wample.com	×

3. Vérifiez que le **compte FTD** est créé. Deux comptes supplémentaires sont créés : **IT Admin** et **Test User**.

Active Directory Users and Computers				-	×
File Action View Help					
🗢 🔿 🖄 📷 🐇 🗈  🗶 🛙	i 🧟 🔒 🔽 🖬	1 🙁 速 🛍 🦷	7 🧕 🗽		
Active Directory Users and Com Saved Queries Saved Queries Save	Name BofaultAcco Denied ROD DnsAdmins	Type User Security Group Security Group	Description A user account manage Members in this group c DNS Administrators Gro		^
	DonsUpdateP Domain Ad Domain Co Domain Co Domain Gue Domain Gue Enterprise A Enterprise K Enterprise R	Security Group Security Group Security Group Security Group Security Group Security Group Security Group Security Group Security Group	DNS clients who are per Designated administrato All workstations and ser All domain controllers i All domain guests All domain users Designated administrato Members of this group Members of this group		
< >>	Group Polic Guest IT Admin Key Admins RAS and IAS Read-only D Schema Ad Test User	Security Group User User Security Group Security Group Security Group Security Group Security Group User	Members in this group c Built-in account for gue Members of this group Members of this group Servers in this group can Members of this group Designated administrato		
	191112 11	<u> </u>			

#### Créer des groupes AD et ajouter des utilisateurs à des groupes AD (facultatif)

Bien qu'ils ne soient pas nécessaires pour l'authentification, les groupes peuvent être utilisés pour faciliter l'application de stratégies d'accès à plusieurs utilisateurs ainsi que l'autorisation LDAP.

Dans ce guide de configuration, les groupes sont utilisés pour appliquer les paramètres de stratégie de contrôle d'accès ultérieurement via l'identité de l'utilisateur dans FMC.

1. Dans **Utilisateurs et ordinateurs Active Directory**, cliquez avec le bouton droit sur le conteneur ou l'unité d'organisation auquel le nouveau groupe est ajouté.

Dans cet exemple, le groupe AnyConnect Admins est ajouté sous le conteneur **Users**. Cliquez avec le bouton droit sur **Users**, puis accédez à **New > Group**.

Active Directory Users and Com	puters			-	х
File Action View Help					
🗢 🄿 🙍 🔂 🔝 🐇 🔯	🗉 🖸 📑 🖬	1 🙎 🔌 🛍 🦷	r 🗾 🕱		
Active Directory Users and Com Saved Queries Saved Queries Save	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 Export List Properties Help	> > A Read-only A Schema A Schema A	Computer Contact Group InetOrgPerson msDS-KeyCreder msDS-ResourceP msDS-ShadowPr msImaging-PSPs MSMQ Queue Al Printer User	itial ropertyList incipalContainer ias		
Creates a new item in this container.	mu u u	Shared Folder			

### 2. Accédez à l'Assistant Nouvel objet - Groupe.

ew Object - Group	×
🥵 Create in: exam	ple.com/Users
Group name:	
AnyConnect Admins	
Group name (nre-Windows 20	01):
AnyConnect Admins	
Group scope	Group type
O Domain local	Security
Global	Obstribution
OUniversal	
	OK Cancel

3. Vérifiez que le groupe est créé. Le groupe Utilisateurs AnyConnect est également créé.

Active Directory Users and Computers				_	×
File Action View Help					
🗢 🔿 🙇 📰 🐇 🗶 🔛 🛙	è   🛛 🖬   🐍 🔌 🛍 '	7 🗾 🐍			
Active Directory Users and Com Saved Queries Saved Queries Builtin Sign Computers Sign Domain Controllers Sign ForeignSecurityPrincipals Sign Managed Service Accour Users	Name AnyConnect Admins AnyConnect Users Calo Cert Publishers Cloneable Domain C DefaultAccount DefaultAccount Domain RODC Passw DnsUpdateProxy Domain Admins DosUpdateProxy Domain Computers Domain Computers Domain Computers Domain Guests Domain Guests Domain 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 User Security Group Security Group User User User Security Group	Description Built-in account for ad Members of this group Members of this group t A user account manage Members in this group c DNS Administrators Gro DNS clients who are per DNS clients who are per Designated administrato 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		
,	(m.s		11 1 2.1. <sup>2</sup>		

4. Cliquez avec le bouton droit sur le groupe d'utilisateurs, puis sélectionnez **Propriétés**. Dans cette configuration, l'utilisateur IT Admin est ajouté au groupe AnyConnect Admins et l'utilisateur **Test User** est ajouté au groupe **AnyConnect Users**.

Active Directory Users and Computers					х
File Action View Help					
🗢 🔿 🖄 🚾 🤞 🔀	3 🖪 🕞 🛛 🖬 🔧	ዾ 🛍 🔻 🗾 🎗	5		
Active Directory Users and Com Saved Queries	Name Real AnyConnect Admins	Type Security Group	Description		^
Simple.com      Simple.com	AnyConnect Users Calo Cert Publishers	Security Group User Security Group	Add to a group Buil Move Mer Send Mail Mer All Tasks		
ForeignSecurityPrincipals     Managed Service Account	Cloneable Domain C Security G DefaultAccount User DefaultAccount Security G Domain RODC Passw Security G Domain Admins Security G Domain Admins Security G Domain Computers Security G	Security Group User		>	
> 🔛 Managed Service Accour		Security Group Security Group Security Group Security Group Security Group	Mer Cut DNS Delete DNS Rename Des All v <b>Properties</b>		
	Bomain Controllers	Security Group Security Group	All C Help		
	Domain Users Enterprise Admins Enterprise Key Admins Enterprise Read-only FTD Admin	Security Group Security Group Security Group Security Group User	All domain users Designated administrato Members of this group Members of this group		
	Croup Policy Creator Cuest IT Admin Key Admins	Security Group User User Security Group	Members in this group c Built-in account for gue Members of this group		
Renames the current selection.	m				Ŷ

## 5. Sous l'onglet Membres, cliquez sur Ajouter.

AnyConnect Admins	Properties			?	×
General Members	Aember Of	Managed By			
Members:					
Name	Active Dire	ectory Domain	Services Folder		
					- 1
Add	Remove				
		ОК	Cancel	Дор	ly -

Entrez l'utilisateur dans le champ et cliquez sur Vérifier les noms pour vérifier que l'utilisateur est trouvé. Une fois la vérification effectuée, 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 (it.admin@example.com)	Gheck Names
Advanced	OK Cancel

Vérifiez que l'utilisateur correct a été ajouté, puis cliquez sur le bouton OK. L'utilisateur **Utilisateur test** est également ajouté au groupe **Utilisateurs AnyConnect** en suivant la même procédure.

AnyConn	AnyConnect Admins Properties					
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	App	ply

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

1. Appuyez sur Win+R et entrez mmc.exe. Cliquez ensuite sur OK.

🖅 Run			>
0	Type the name of a prog resource, and Windows	gram, folder, docun will open it for you.	nent, or Internet
Open:	mmc.exe		~
	ОК	Cancel	Browse

2. Accédez à Fichier > Ajouter/Supprimer un composant logiciel enfichable...

ᡖ Co	nsole1 - [C	onsole f	Root]		-	×
😹 File	Action	View	Favorites	Window	Help	 . 8 ×
4	New			Ctrl+N		
	Open			Ctrl+O	Actions	
	Save Ar			Ctrl+S	There are no items to show in this view. Console Root	-
	Add/Rea		un in	ChileM	More Actions	•
	Options.		ip-in	Cut+M		
	1 dnsma	mt				
	2 dsa					
	Exit					
Enables	you to add	l snap-ir	is to or remo	ove them fro	I'm the snap-in console.	

3. Sous Composants logiciels enfichables disponibles, sélectionnez **Certificats**, puis cliquez sur **Ajouter**.

Add or Remove Snap-ins				×			
And of hemore shap 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		<u>R</u> emove				
Active Directory Use	Microsoft Cor		Move <u>U</u> p				
AUSI Edit	Microsoft Cor		Add >				
Certificates	Microsoft Cor						
Component Services	Microsoft Cor						
Device Manager	Microsoft Cor			_			
T Disk Management	Microsoft and	$\checkmark$	Ad <u>vanced</u>				
Description: The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.							
			OK Cancel				

4. Sélectionnez Compte d'ordinateur, puis cliquez sur Suivant.

Certificates snap-in			×
This snap-in will always manage certificates for:          My user account         Service account         Computer account			
	< <u>B</u> ack	<u>N</u> ext >	Cancel

Cliquez sur **Finish** (Terminer).

Select Computer	×
Select the computer you want this snap-in to manage. This snap-in will always manage:      O Local computer: (the computer this console is running on)     Another computer:     Drowse 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. Cliquez maintenant sur OK.

Add or Remove Snap-ins				3	×		
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:			_	S <u>e</u> lected 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	1		
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						
E Disk Management	Microsoft and	¥		Advanced			
Description: The Certificates snap-in allows 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 est délivré au **nom de domaine complet (FQDN)** du serveur Windows. Trois certificats sont répertoriés sur ce serveur.

- Certificat d'autorité de certification délivré à et par l'exemple-WIN2016-CA.
- Certificat d'identité délivré à WIN2016 par example-WIN2016-CA.
- Certificat d'identité délivré à win2016.example.com par example-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 vers win2016.example.com est un certificat qui a été émis automatiquement par le service AC de Windows Server. Double-cliquez sur le certificat pour vérifier les détails.



7. Pour être utilisé comme certificat SSL LDAPS, le certificat doit répondre aux exigences suivantes :

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

• Le certificat comporte l'authentification du serveur sous le champ Enhanced Key Usage.

Sous l'onglet **Details** pour le certificat, sélectionnez **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	
Ent Contraction	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	¢

🙀 Certif	ficate			×
General	Details	Certification Path		
Show:	<al></al>		$\sim$	
Field	bject Key thority Ke L Distribu thority In	Identifier ty 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 Other Name-DS Object Guid=	^
Ke: The The	y Usage umbprint umborint	algorithm	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 Enhanced Key Usage, Server Authentication est présent.

🙀 Certi	ficate			×
General	Details	Certification Path		
Show:	<ai></ai>		~	
Field			Value	^
E Sul Pul Pul	bject blic key blic key pa	arameters	win2016.example.com RSA (2048 Bits) 05 00	
in Ce	rtificate T hanced Ki	emplate Name ey Usage	DomainController Client Authentication (1.3.6.1	
⊕ SM ⊕ Sul ⊮ Au	IME Capa bject Key thority Ke	blittes Identifier v Identifier	[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	Authentic	tion (1.3.6.1.5.5. ation (1.3.6.1.5.5	7.3.2) .7.3.1)	
		E	it Properties Copy to File	
			0	ĸ

8. Une fois que cela est confirmé, sous l'onglet **Chemin d'accès de certification**, sélectionnez le certificat supérieur qui est le certificat d'autorité de certification racine, puis cliquez sur **Afficher le certificat**.

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

9. Ceci ouvre les détails du certificat pour le certificat d'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 Statement	
ОК	

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

📰 Certificate		$\times$
General Details Certification Path		
Show: <all></all>	$\sim$	
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	

10. Accédez à l'Assistant Exportation de certificat qui exporte l'autorité de certification racine au format PEM.

÷	🐓 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.	
	<u>N</u> ext Cance	1

Sélectionner encodé en base 64 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)	
	<ul> <li>Personal Information Exchange - PKCS #12 (.PFX)</li> <li>Include all certificates in the certification path if possible</li> </ul>	
	Delete the private key if the export is successful	
	Export all extended properties	
	Enable certificate privacy	
	<ul> <li>Microsoft Serialized Certificate Store (.SST)</li> </ul>	
	Next Can	cel

Sélectionnez le nom du fichier et l'emplacement d'exportation.

Everificate Export Wizard      File 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	

Cliquez maintenant sur Terminer.

÷	<b>5</b>	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 Canc	el							

11. Allez à l'emplacement et ouvrez le certificat avec un bloc-notes ou un autre éditeur de texte. Affiche le certificat de format PEM. Enregistrez ceci pour plus tard.

#### ----BEGIN CERTIFICATE----

```
MIIDCDCCAfCgAwIBAgIQE4ZG5Z1wT6lONTjooEQyMTANBgkqhkiG9w0BAQsFADAd
MRswGQYDVQQDExJleGFtcGxlLVdJTjIwMTYtQ0EwIBcNMjAwNDI3MTQ1MDU5WhgP
MjA2MDA0MTkxNDUwNTlaMB0xGzAZBgNVBAMTEmV4YW1wbGUtV010MjAxNi1DQTCC
ASIwDQYJKoZIhvcNAQEBBQADqqEPADCCAQoCqqEBAI8qhT719NzSQpoQPh0YT67b
Ya+PngsxMyvkewP33QLTAWw1HW1Tb9Mk5BDWOItTaVsgHwPBfd++M+bLn3AiZnHV
00+k6dVVY/E5qVkEKSGoY+v940S2316lzdwReMOFhgbc2qMertIoficrRhihonuU
Cjyeub3CO+meJUuKom2R47C0D35TUvo/FEHGgXJFaJS1se2UrpN07KEMkfA1LPuM
aob4XE/OzxYQpPa18djsNnskfcFqD/HOTFQN4+SrOhHWlRnUIQBUaLdQaabhipD/
sVs5PneYJX8YKma821uYI6j90YuytmsHBtCieyC062a8BKqOL7N86HFPFkMA3u8C
AwEAAaNCMEAwDgYDVR0PAQH/BAQDAgGGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR00
BBYEFD2fJjf7ER9EM/HCxCVFN5QzqEdvMA0GCSqGSIb3DQEBCwUAA4IBAQB31ZJo
vzwVD3c5Q1nrNP+6Mq62OFpYH91k4Ch9S5g/CEOemhcwg8MDIoxW2dTsjenAEt7r
phFIHZoCoSyjBjMgK3xybmoSeg8vBjCXseYNGEmOc9KW1oFmTOvdNVIb7Xpl1IVa
6tALTt3ANRNgREtxPA6yQbthKGavW0Anfsojk9IcDr2vp0MTj1BCxsTscbubR1+D
dLEFKQqmMeYvkVf+a7a64mqPZsG3Uxo0rd6cZxAPkq/y1cdwNSJFfQV3DqZq+R96
9WLCR3Obig6xyo9Zu+lixcWpdrbADO6zMhbEYEhkhOOjBrUEBBI6Cy83iTZ9ejsk
KgwBJXEu33Pp1W6E
----END CERTIFICATE-----
```

12. (Facultatif) Dans le cas où plusieurs certificats d'identité peuvent être utilisés par LDAPS et où il existe une incertitude quant à savoir lequel est utilisé, ou s'il n'y a pas d'accès au serveur LDAPS, il est possible d'extraire l'autorité de certification racine à partir d'une capture de paquets effectuée sur le serveur Windows ou FTD après.

### **Configurations FMC**

#### Vérifier les licences

Pour déployer une 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.

1. Accédez à System > Licenses > Smart Licensing.

Overview	Analysis	Policies	Devices	Objects	AMP	Intelligence					Deploy	/ 🔒 <mark>s</mark>	ystem Help 🔻	admin <del>v</del>
						Configuration	Users	Domains	Integration	Updates	Licenses 🔻	Health 🔻	Monitoring •	Tools •
										Sm	art Licenses			
										Cla	ssic Licenses			

2. Vérifiez que les périphériques sont conformes et correctement enregistrés. Assurez-vous que le périphérique est enregistré avec une licence **AnyConnect Apex**, **Plus**, ou **VPN Only**.

Overview Analysis Policies	De	vices Objects	AMP Int	telligence						Deploy 🔒	System Help	• admin
		Co	ofiguration	Users	Domains	Integration	Updates	Licenses +	Smart Licens	ses Health	Monitoring	• Tools
Smart License Status					Cisco Sm	rt Software M		<u> </u>				
Usage Authorization:	٢	Authorized (Last Syn	chronized On M	4ay 03 2020	)							
Product Registration:	0	Registered (Last Ren	ewed On Mar 0	33 2020)								
Assigned Virtual Account:		SEC TAC										
Export-Controlled Features:		Enabled										
Cisco Success Network:		Disabled										
Cisco Support Diagnostics:		Disabled 🕕										
Smart Licenses								[	Filter Devices		× E	dit Licenses
License Type/Device Name					License State	15	Device Type			Domain	Group	
🖻 💋 Firepower Management (	Cent	ter Virtual (2)			0							
🖻 💋 Base (2)					0							
🖻 💋 Mahware (1)					0							
D C Threat (2)					0							
🖻 💋 URL Filtering (2)					0							
4 🥬 AnyConnect Apex (1)					0							
FTD-2 192.168.1.17 · Cisco Firepo	wer	Threat Defense for VM	Ware - v6.3.0		0		Cisco Firepower	r Threat Defense	e for VMWare	Global	N/A	
AnyConnect Plus (0)												
AnyConnect VPN Only (0)												

#### Configurer le domaine

1. Accédez à **Système > Intégration**.

Overview	Analysis	Policies	Devices	Objects	AMP	Intelligence					Deploy	/ <b>Q</b>	System	Help 🔻	admin <del>v</del>
						Configuration	Users	Domains	Integration	Updates	Licenses v	Health	iv Mor	itoring 🔻	Tools <b>v</b>

2. Sous Domaines, cliquez sur Nouveau domaine.

Overview Analysis Policie	s Devices Objects	AMP Intellige	nce					Deploy	0 Sys	tem Help	r admin <del>v</del>
		Con	figuration	Users	Domains	Integratio	updates	Licenses 🔻	Health 🔻	Monitoring	<ul> <li>Tools *</li> </ul>
Cloud Services Realms	Identity Sources	Streamer Host I	nput Client	Smar	rt Software S	atellite					
									K Compa	are realms	New realm
Name	Description	Domain	Туре		Base DN	Gro	oup DN	Group Attri	bute	State	

3. Remplissez les champs appropriés en fonction des informations collectées auprès du serveur Microsoft. Une fois terminé, cliquez sur **OK**.

Varea +	148.45	_		
Name -	CAB-AD			
Description				
Type *	AD	*		
AD Primary Domain *	example.com		ex: domain.com	
AD Join Username			ex: user@domain	
AD Join Password			Test AD Join	
Directory Username *	ftd.admin@example.com		ex: user@domain	
Directory Password *	•••••			
Base DN *	DC=example,DC=com		ex: ou=user,dc=cisco,dc=com	
Group DN *	DC=example,DC=com		ex: ou=group,dc=cisco,dc=com	
Group Attribute	Member	~		
* Required Field				

4. Dans la nouvelle fenêtre, sélectionnez **Répertoire** si ce n'est déjà fait, cliquez sur **Ajouter un répertoire**.

Overview	Analysis	Policies	Devices	Objects	AMP	Intellige	ence			Deploy	/ 🔍 Sys	stem Help 🔻	admin 🔻
				Configur	ration	Users	Domains	Integration	Updates	Licenses 🔻	Health •	Monitoring •	Tools •
LAB-AD	lion											Save 1	Cancel
Directory	Realm Cont	figuration	User Dowr	hoad									
												O A	dd directory

Renseignez les détails relatifs au serveur AD. Notez que si le nom de domaine complet est utilisé, FMC et FTD ne peuvent pas se lier correctement à moins que DNS ne soit configuré pour résoudre le nom de domaine complet.

Pour configurer DNS pour FMC, accédez à **System > Configuration** et sélectionnez **Management Interfaces**.

Afin de configurer DNS pour le FTD, naviguez vers **Devices > Platform Settings**, créez une nouvelle stratégie, ou modifiez une stratégie actuelle, puis allez dans DNS.

Add directory		? ×
Hostname / IP Address	win2016.example.com	
Port	389	
Encryption	○ STARTTLS ○ LDAPS	
SSL Certificate	<ul> <li>O</li> </ul>	
	OK Test Ca	incel

Si LDAPS ou STARTTLS est utilisé, cliquez sur le symbole + vert, donnez un nom au certificat et copiez le certificat CA racine au format PEM. Cliquez sur **Save** lorsque vous avez terminé.

Import Trusted Certificate Authority	? ×
Name: LDAPS_ROOT	
Certificate Data or, choose a file: Browse	
BEGIN CERTIFICATE MIIDCDCCAfCgAwIBAgIQE4ZG5Z1wT6lONTjooEQyMTANBgkqhkiG9w0BAQsFADAd MRswGQYDVQQDExJleGFtcGxlLVdJTjIwMTYtQ0EwIBcNMjAwNDI3MTQ1MDU5WhgP MjA2MDA0MTkxNDUwNTlaMB0xGzAZBgNVBAMTEmV4YW1wbGUtV0lOMjAxNi1DQTCC ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAI8ghT719NzSQpoQPh0YT67b Ya+PngsxMyvkewP33QLTAWw1HW1Tb9Mk5BDWOITTaVsgHwPBfd++M+bLn3AiZnHV OO+k6dVVY/E5qVkEKSGoY+v940S2316lzdwReMOFhgbc2qMertIoficrRhihonuU Cjyeub3CO+meJUuKom2R47C0D35TUvo/FEHGgXJFaJS1se2UrpNO7KEMkfA1LPuM aob4XE/OzxYQpPa18djsNnskfcFqD/HOTFQN4+SrOhHWlRnUIQBUaLdQaabhipD/ sVs5PneYJX8YKma821uYI6j90YuytmsHBtCieyC062a8BKqOL7N86HFPFkMA3u8C AwEAAaNCMEAwDgYDVR0PAQH/BAQDAgGGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0O BBYEFD2fJjf7ER9EM/HCxCVFN5QzqEdvMA0GCSqGSIb3DQEBCwUAA4IBAQB31ZJo vzwVD3c5Q1nrNP+6Mq62OFpYH91k4Ch9S5g/CEOemhcwg8MDIoxW2dTsjenAEt7r phFIHZoCoSyjBjMgK3xybmoSeg8vBjCXseYNGEmOc9KW10FmTOvdNVIb7Xpl1IVa 6tALTt3ANRNgREtxPA6yQbthKGavW0Anfsojk9IcDr2vp0MTjlBCxsTscbubRI+D dLEFKQqmMeYvkVf+a7a64mqPZsG3Uxo0rd6cZxAPkq/ylcdwNSJFfQV3DgZg+R96 9WLCR3Obig6xyo9Zu+lixcWpdrbADO6zMhbEYEhkhO0jBrUEBBI6Cy83iTZ9ejsk KgwBJXEu33PpIW6E FND CERTIFICATE	
	$\sim$
Encrypted, and the password is:	
Save	Cancel

Sélectionnez l'autorité de certification racine nouvellement ajoutée dans la liste déroulante en regard de SSL Certificate et cliquez sur STARTTLS ou LDAPS.
Edit directory	? ×
Hostname / IP Address	win2016.example.com
Port	636
Encryption	◯ STARTTLS
SSL Certificate	LDAPS_ROOT 🗸 📀
	OK Test Cancel

Cliquez sur Test pour vous assurer que FMC peut se lier correctement avec le nom d'utilisateur et le mot de passe de répertoire fournis à l'étape précédente.

Étant donné que ces tests sont initiés à partir du FMC et non par l'intermédiaire d'une des interfaces routables configurées sur le FTD (telles qu'une connexion interne, externe ou dmz), une connexion réussie (ou ayant échoué) ne garantit pas le même résultat pour l'authentification AnyConnect, car les demandes d'authentification LDAP AnyConnect sont initiées à partir de l'une des interfaces routables FTD.

Pour plus d'informations sur le test des connexions LDAP à partir du FTD, consultez les sections Test AAA et Capture de paquets dans la zone Dépannage.



5. Sous **Téléchargement utilisateur**, téléchargez les groupes qui sont utilisés pour l'identité de l'utilisateur dans les étapes ultérieures.

Cochez la case **Télécharger les utilisateurs et les groupes** et la colonne **Groupes disponibles** affiche les groupes configurés dans Active Directory.

Les groupes peuvent être inclus ou exclus, mais par défaut, tous les groupes situés sous le DN du groupe sont inclus.

Des utilisateurs spécifiques peuvent également être inclus ou exclus. Tous les groupes et utilisateurs inclus peuvent être sélectionnés ultérieurement pour l'identité de l'utilisateur.

Une fois terminé, cliquez sur Save (enregistrer).

Overview Analysis Policies Devices Objects AMP Intel	ligence			Deploy	0 System	Help 🔻 a	idmin 🔻
	Configuration Users	Domains Integration	n Upd	lates Licenses •	Health  Moni	toring •	Tools <b>*</b>
LAB-AD Enter Description				You have uns	aved changes 🔡	Save	Cancel
Directory Realm Configuration User Download							
Download users and groups							
Begin automatic download at a v p <sub>N</sub> v America/New York Repeat Every	24 V Hours						
Available Groups 😋	Groups to Include (2)			Groups to Exclude (0	0		
Search by name	💣 AnyConnect Admins		8	None			
🝰 AnyConnect Admins	AnyConnect Users		8				
🛃 DnsUpdateProxy							
A WseRemoteAccessUsers							
A WseInvisibleToDashboard							
Allowed RODC Password Replication Group Add to							
A Enterprise Key Admins Include							
Domain Admine Add to							
A WseAlertAdministrators							
A Event Log Readers							
A Replicator							
🝰 Domain Guests							
🍰 Windows Authorization Access Group							
Account Operators							
🝰 Hyper-V Administrators 🗸 🗸	Enter Liner Indusian			Enter Liner Evolution			
n System Managed Accounts Group	enter user Indusion		Add	Enter User Exclusion			Add

### 6. Activez le nouveau domaine.

Overview Analysis Policie	es Devices Object	ts AMP I	ntelligence							Deploy	🛛 🔍 Sy	stem He	lp <del>v</del> admin <del>v</del>
			Configur	ation U	lsers	Domains	Integra	stion	Updates	Licenses 🔻	Health <b>*</b>	Monitori	ng 🔻 🛛 Tools 🔻
Cloud Services Realms	Identity Sources	eStreamer	Host Inpu	ut Client	Smar	rt Software	Satellite						
											M Comp	are realms	🔾 New realm
Name	Description	Domain		Туре	E	Base DN		Group C	NN .	Group Att	ibute	State	
LAB-AD		Global		AD	C	C=example,D0	-com	DC=exa	mple,DC=com	member			ቷ 🥒 🔁 🖯

7. Si LDAPS ou STARTTLS est utilisé, l'autorité de certification racine doit également être approuvée par le FTD. Pour ce faire, accédez d'abord à **Périphériques > Certificats**.

Overview Analysis	Policie	s Dev	ices	Objects	AMP In	telligence		Deploy	0	System	Help 🔻	admin 🔻
Device Management	NAT	VPN V	QoS	Platform	Settings	FlexConfig	Certificates					

Cliquez sur Ajouter en haut à droite.

Overview Analysis	Policie	es Devi	ices 0	bjects	AMP 1	Intelligence		Deploy	0,	System	Help 🔻	admin v	
Device Management	NAT	VPN •	QoS	Platform	n Settings	FlexConfig	Certificates						
											0	Add	

Sélectionnez le FTD, la configuration LDAP est ajoutée, puis cliquez sur le symbole + vert.

Add New Certificate	2	? ×
Add a new certificate to t identify certificate.	he device using cert enrollment object whi	ich is used to generate CA and
Device":	FTD-2	¥
Cert Enrollment*:	Select a certificate entrollment object	¥ 🖸
		Add Cancel

Attribuez un **nom** au point de confiance, puis choisissez **Inscription manuelle** dans la liste déroulante **Type d'inscription**. Collez ici le certificat d'autorité de certification racine PEM, puis cliquez sur **Save**.

Add Cert Enrollme	nt	? ×
Name*	LDAPS_ROOT	
Description		
CA Information	Certificate Parameters Key Revocation	
Enrollment Type:	Manual 👻	^
CA Certificate:*	MIIDCDCCAfCgAwIBAgIQE4ZG5Z1wT6lONTjooEQyMTANBgkqhki G9w0BAQsFADAd MRswGQYDVQQDExJleGFtcGxlLVdJTjIwMTYtQ0EwIBcNMjAwNDI 3MTQ1MDU5WhgP MJA2MDA0MTkxNDUwNTlaMB0xGzAZBgNVBAMTEmV4YW1wbGU tV0lOMjAxNi1DQTCC ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAI8ghT719N zSQpoQPh0YT67b Ya+PngsxMyvkewP33QLTAWw1HW1Tb9Mk5BDWOItTaVsgHwPBf d++M+bLn3AiZnHV OO+k6dVVY/E5qVkEKSGoY+v940S2316lzdwReMOFhgbc2qMertIo ficrRhihonuU Cjyeub3CO+me3UuKom2R47C0D35TUvo/FEHGgXJFaJS1se2UrpN O7KEMkfA1LPuM aob4XE/OzxYQpPa18djsNnskfcFqD/HOTFQN4+SrOhHWlRnUIQBU aLdQaabhipD/ sVs5PneYJX8YKma821uYI6j90YuytmsHBtCieyC062a8BKgOL7N86	~
Allow Overrides		
	Save	Cancel

Vérifiez que le point de confiance créé est sélectionné, puis cliquez sur Add.

Add New Certificate		? ×
Add a new certificate to th identify certificate.	e device using cert enrollment object whic	h is used to generate CA and
Device*:	FTD-2	~
Cert Enrollment*:	LDAPS_ROOT	<b>~</b> ©
Cert Enrollment Details:		
Name:	LDAPS_ROOT	
Enrollment Type:	Manual	
SCEP URL:	NA	
		Add Cancel

Le nouveau point de confiance apparaît sous le FTD. Bien qu'il mentionne que l'importation de certificat d'identité est requise, il n'est pas nécessaire pour les besoins du FTD pour être en mesure d'authentifier le certificat SSL envoyé par le serveur LDAPS et donc ce message peut être ignoré.

Overview Analysis Polic	ies Devices Object	ts AMP Intelli	gence	Deploy 🔒	System	Help 🔻	admin 🔻
Device Management NAT	VPN VOS Pla	tform Settings Fl	lexConfig Certificates				
						0	Add
Name	Domain	Enrollment Type	Status				
4 🗐 FTD-1							
FTD-1-PKCS12	Global	PKCS12 file	CA LD			£ ¢	
4 🗐 FTD-2							
FTD-2-PKCS12	Global	PKCS12 file	CA 🔍 ID			£ ¢	
FTD-2-Selfsigned	Global	Self-Signed	S CA LD			v?	6
LDAPS_ROOT	Global	Manual	🔍 CA 🔺 ID 📤 Idea	ntity certificate import requir	red	P 🗘	6

### Configurer AnyConnect pour l'authentification AD

1. Ces étapes supposent qu'aucune stratégie de VPN d'accès à distance n'a déjà été créée. Si une stratégie a été créée, cliquez sur le bouton Modifier de cette stratégie et passez à l'étape 3.

#### Accédez à **Devices > VPN > Remote Access**.

Overview Analysis	Policies	Device	s Obje	ects AMP Intell	igence			(	Deploy	e	System	Help 🔻	admin 🔻
Device Management	NAT	VPN •	QoS	Platform Settings	FlexConfig	Certificates							
		Site To S	iite										
		Remote	Access										
		Troubles	hooting	]									

Cliquez sur Add pour créer une nouvelle stratégie VPN d'accès à distance



2. Exécutez l'**Assistant Stratégie VPN d'accès à distance**. Sous **Policy Assignment**, spécifiez un nom pour la stratégie et les périphériques auxquels la stratégie est appliquée.

Overview Analysis Polic	cies Devices Objects	AMP Intelligence		Deploy	🤱 System Help 🕶 admin 🔻
Device Management NAT	VPN • Remote Access	QoS Platform Settings	FlexConfig Certificates		
Remote Access VPN F	Policy Wizard				
1 Policy Assignment	Connection Profile	3 AnyConnect	Access & Certificate	S Summary	
Targete	ed Devices and Protocols				~
This wize a new us	ard will guide you through the requer-defined connection profile.	uired minimal steps to configure	the Remote Access VPN policy with	Before You Start	
				Before you start, ensure the fo configuration elements to be in p	lowing lace to
Name:*	PTD-2-RA-Policy			complete Remote Access VPN Policy	•
Descripti	ion:		0	Authentication Server Configure Realm or RADIUS Server	Group
VDN Devit	territer Place Planess	10.0	~	to authenticate VPN clients.	
Terreted	maximum Available Devices	NEV2	Selected Devices	AnyConnect Client Package Nake sure you have AnyConnect p	ackage
Targeteo	Search		∰ PTD-2 6	for VPN Client downloaded or you the relevant Cisco credentials to do	a have wnload
	FTD-1		_	it during the wizard.	
	PTD-2			Device Interface Interfaces should be already configu	ned on
				targeted <u>devices</u> so that they can b as a security zone or interface or	e used oup to
				enable VPN access.	
		Add			
					×
				Back	Next Cancel

Sous **Profil de connexion**, spécifiez le nom du **profil de connexion** qui est également utilisé comme alias de groupe que les utilisateurs d'AnyConnect voient lorsqu'ils se connectent.

Spécifiez le domaine précédemment créé sous Authentication Server.

Spécifiez la méthode d'attribution des adresses IP aux clients AnyConnect.

Spécifiez la stratégie de groupe par défaut utilisée pour ce profil de connexion.

Overview Analysis Policies Devices Objects AMP	Intelligence	Deploy 🔍 System Help 🔻 admin	•
Device Management NAT VPN • Remote Access QoS	Platform Settings FlexConfig Certificates		
Remote Access VPN Policy Wizard			
1 Policy Assignment 2 Connection Profile 3	AnyConnect > (a) Access & Certificate > (5) Summary		
Connection Profile:			^
Connection Profiles specify the tunn accomplished and how addresses an	I group policies for a VPN connection. These policies pertain to creating the tunnel itself, he assigned. They also include user attributes, which are defined in group policies.	ow AAA is	
Connection Profile Name:*	General		
	This name is configured as a connection alias, it can be used to connect to the VIN gateway		4
Authentication, Authorization &	ccounting (AAA):		
Specify the method of authentication	(AAA, certificates or both), and the AAA servers that will be used for VPN connections.		
Authentication Method:	AAA Only 👻		
Authentication Server:*	LAB-AD V G+ (Realm or RADJUS)		
Authorization Server:	V (RADIUS)		
Accounting Server:	V Q (RADIUS)		
Client Address Assignment:			
Client IP address can be assigned fin assignment is tried in the order of A	m AAA server, DHCP server and IP address pools. When multiple options are selected, IP a A server, DHCP server and IP address pool.	address	
Use AAA Server (RADIUS	eniy) 🕕		
Use DHCP Servers			
M Use IP Address Pools			
IPv4 Address Pools:	AnyConnect-Pool 🥜		
IPv6 Address Pools:	/		
Group Policy: A group policy is a collection of user or create a Group Policy object.	oriented session attributes which are assigned to client when a VPN connection is establish	ted. Select	
Group Policy:*	DfltGrpPolicy 👻 🔾		
	Edit Group Policy		~
		Back Next Cancel	

Sous AnyConnect, téléchargez et spécifiez les packages AnyConnect utilisés.



Sous Access & Certificate, spécifiez l'interface à laquelle les utilisateurs d'AnyConnect accèdent pour AnyConnect.

Créez et/ou spécifiez le certificat utilisé par le FTD lors de la connexion SSL.

Assurez-vous que la case à cocher **Bypass Access Control policy** for decrypted traffic (sysopt permit-vpn) est laissée décochée afin que l'identité utilisateur créée ultérieurement prenne effet pour les connexions RAVPN.

Overview Analysis Policies Devices Objects AMP	Intelligence	Deploy	🔍 System	Help 🔻	admin 🔻
Device Management NAT VPN > Remote Access QoS	Platform Settings FlexConfig Certificates				
Remote Access VPN Policy Wizard					
Policy Assignment     2 Connection Profile     3	AnyConnect 🔰 🖪 Access & Certificate 🔰 🌖 Summary 🔄				
Network Interface for I	ncoming VPN Access				
Select or create an Interface connections.	Group or a Security Zone that contains the network interfaces users will access for VPN	i .			í í
Interface group/Security Zo	ne:" outside-zone V Q+				
	Enable DTLS on member interfaces				
Device Certificates					
Device certificate (also called certificate which is used to as	Identity certificate) identifies the VPN gateway to the remote access clients. Select a thenticate the VPN gateway.				
Certificate Enrollment:*	FTD-2-Selfsigned Y				
	Enroll the selected certificate object on the target devices				
Access Control for VPN	Traffic				
All decrypted traffic in the VP bypass decrypted traffic from	I tunnel is aubjected to the Access Control Policy by default. Select this option to the Access Control Policy.				
Bypass Access Control po This option bypasses the AAA server are still applied	icy for decrypted traffic (sysopt permit-vpn) ccess Control Policy Inspection, but VPN filter ACL and authorization ACL downloaded from to VPN traffic.				
		Back	Next	<b>_ _ _ _</b>	ancel

### Sous Summary, vérifiez la configuration et cliquez sur Finish.



3. Sous Remote Access VPN Policy, cliquez sur edit pour le profil de connexion approprié.

Overview Analysis Policies Devices Object	AMP Intelligence	Deploy 🔍 System Help 🔻 admin 🔻
Device Management NAT VPN + Remote Acces	QoS Platform Settings FlexConfig Certificates	
FTD-2-RA-Policy		Save Save
Connection Profile Access Interfaces Advan	ed	Policy Assignments (1)
		0
Name	AAA Group Policy	
DefaultWEBVPNGroup	Authentication: None E DitGrpPolicy Authorization: None Accounting: None	<b>/</b> Ü
General	Authentication: LAB-AD (AD) Authorization: form Accounting: form	<b>2</b> 3

Assurez-vous que le serveur d'authentification est défini sur le domaine créé précédemment.

Sous **Advanced Settings**, **Enable Password Management** peut être coché pour permettre aux utilisateurs de modifier leur mot de passe avant ou après l'expiration de leur mot de passe.

Cependant, ce paramètre nécessite que le domaine utilise LDAPS. Si des modifications ont été apportées, cliquez sur **Enregistrer**.

Edit Connection Pr	ofile		? ×
Connection Profile:* Group Policy:*	General DfltGrpPolic Edit Group Po	y v C	
Client Address Assign	ment AA	A Aliases	
Authentication			
Authentication Meth	iod:	AAA Only 💙	
Authentication Serv	er:	LAB-AD (AD)	
Use secondary a	uthentication		
Authorization			
Authorization Serve	r:	¥	
		Allow connection only if user exists in authorization databas	e
Accounting			
Accounting Server:		<b>v</b>	
Advanced Settin	gs		
Strip Realm from	username		
Strip Group from	username		
Enable Password     Notify User     Notify user on the second secon	Managemen days price he day of passe	t or to password expiration vord expiration	
		Save	Cancel

Une fois terminé, cliquez sur Enregistrer en haut à droite.



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

1. Accédez à Politiques > Contrôle d'accès > Identité.



Créez une nouvelle stratégie d'identité.

Overview Analysis Policies Devices Objects A	MP Intelligence	Deploy 🧕 System Help 🔻 admin 🔻					
Access Control + Identity Network Discovery Applicati	on Detectors Correlation Actions •						
		Object Management Access Control					
Identity Policy	Domain	Status Last Modified					
There are no policies created. Add a new policy							

Spécifiez un nom pour la nouvelle stratégie d'identité.

Name	FTD-2 Identity Policy
Description	

2. Cliquez sur Ajouter une règle.



3. Spécifiez un **nom** pour la nouvelle règle. Assurez-vous qu'elle est activée et que l'action est définie sur Authentification passive.

Cliquez sur l'onglet **Domaine et paramètres** et sélectionnez le domaine créé précédemment. Cliquez sur **Add** lorsque vous avez terminé. Add Rule

Name RAVPN		🗹 Enabl	led Insert	into Category	~	Standard Rules	~
Action Passive Authentic	ation	✓ Realm: LAB-AD (AD)	Authentication Protocol:	HTTP Basic Exclude I	HTTP User-	Agents: None	
Remote access VPN	I sessions are actively au	thenticated by VPN. Other sessio	ons use the rule Action.				
Zones Networks	VLAN Tags Ports					Realm & S	ettings
Realm *			<b>v</b> <i>A</i>				
	LAB-AD (AD)	the encet he established	- W				
U use active authenticat	ion if passive of VPN iden	toty cannot be established					
* Required Field							
						Add C	ancel

# 4. Cliquez sur Enregistrer.

Overview Analysis Pol	icies Device	es Objects	AMP Intelli	igence				Dep	ploy 🧛 System	Help <del>v</del> ad	lmin <del>v</del>
Access Control > Identity	Network Disc	covery Appl	cation Detectors	Correlation	Actions •						
FTD-2 Identity Policy You have unsaved changes Save Cancel											
Rules Active Authentication	1										
							Add Categor	y 🛛 🔘 Add Rule	Search Rules		×
# Name	Source Zo	Dest Zones	Source Net	Dest Netw	VLAN Tags	Source Ports	Dest Ports	Realm	Action	Auth Protoco	4
Administrator Rules											
This category is empty											
Standard Rules											
1 RAVPN	any	any	any	any	any	any	any	LAB-AD	Passive Authentication	none	/8
Root Rules											
This category is empty											

Displaying 1 - 1 of 1 rules  $\ |<\ <\$  Page  $\boxed{1-}$  of 1  $\ >\ >|$   $\ \Cit{C}$ 

5. accédez à **Politiques > Contrôle d'accès > Contrôle d'accès**.

Overview Analysis Policies Devices Objects AMP Intelligence	Deploy	🧛 System	Help 🔻	admin <del>v</del>
Access Control > Identity Network Discovery Application Detectors Correlation Actions •				
Access Control				
Intrusion				
Malware & File				
DNS				
Identity				
SSL				
Prefilter				

6. Modifiez la stratégie de contrôle d'accès sous laquelle le FTD est configuré.

Overview Analysis Policies	Devices Objects	AMP Intelligence				Deploy	B <sub>2</sub> System	Help 🔻	admin 🔻
Access Control > Access Control	Network Discovery	Application Detectors	Correlation	Actions *					
					Object Management Intru	sion Network	Analysis Policy	DNS Impo	ort/Export
								🔾 New i	Policy
Access Control Policy		Status			Last Modified				
Default-Policy		Targeting 1 o Up-to-date o	levices n all targeted device	es	2020-05-04 09:15:56 Modified by "admin"			ħ 0 <mark>2</mark>	0

7. Cliquez sur la valeur en regard de Politique d'identité.



Sélectionnez la stratégie d'identité créée précédemment, puis cliquez sur OK.

Identity Policy	
FTD-2 Identity Policy	¥ 🦉
Revert to Defaults	OK Cancel

8. Cliquez sur **Add Rule** pour créer une nouvelle règle ACP. Ces étapes créent une règle permettant aux utilisateurs du groupe AnyConnect Admins de se connecter aux périphériques du réseau interne à l'aide du protocole RDP.

Overview Analysis Policies Devices	s Objects AMP Intelligence		Deploy 🔒	System Help 🔻 admin 🔻				
Access Control > Access Control Netwo	ork Discovery Application Detectors	Correlation Actions •						
Default-Policy Enter Description			You have unsaved changes Analyze Hit Cou	nts 🔚 Save 🛛 🕄 Cancel				
Prefilter Policy: Default Prefilter Policy: FTD-2 Identity Policy: FTD-2 Identity Policy								
			Inheritance Set	tings   📑 Policy Assignments (1)				
Rules Security Intelligence HTTP Respo	onses Logging Advanced							
曲 Filter by Device		Show Rule Conflicts 🥹	🔾 Add Category 🔹 Add Rule 🚔 Sea	rch Rules 🛛 🖓				
# Name Sourc Dest Z S	Sourc Dest N VLAN Users	Applic Sourc Dest P	URLs Sourc Dest S Action	• • • • •				
<ul> <li>Mandatory - Default-Policy (-)</li> </ul>								
There are no rules in this section. Add Rule or Add	Category							
➡ Default - Default-Policy (-)								
There are no rules in this section. Add Rule or Add	Category							
Default Action			Access Control: Block All Traffic	¥ 🔳				

Displaying 0 - 0 of 0 rules  $|\langle \langle Page | \underline{1} \rangle$  of  $1 > | \rangle C |$  Rules per page: 100 -

Spécifiez un nom pour la règle. Assurez-vous que la règle est activée et qu'elle comporte l'action appropriée.

Sous l'onglet **Zones**, spécifiez les zones appropriées pour le trafic intéressant.

Le trafic RDP initié par les utilisateurs entre dans le FTD provenant de l'interface de zone externe et sort de la zone interne.

Add Rule							? ×
Name AC RDP Access		Enabled	Insert	into Mandatory			
Action 🖌 Allow	V D B t	h .F					
Zones Networks VLAN	Tags Users Applications A	Ports URLs	SGT/ISE Attributes		Inspection	Logging	Comments
Available Zones 🗳		Source Zones	(1)	Destinati	on Zones (1)		
🔍 side	×	🔒 outside-zor	ie .	🛅 🚠 inside	-zone		<u>ii</u>
슈 inside-zone 슈 outside-zone	Add to Source Add to Destination						
						Add	Cancel

Sous Networks, définissez les réseaux source et de destination.

L'objet AnyConnect\_Pool inclut les adresses IP attribuées aux clients AnyConnect.

L'objet Inside Net inclut le sous-réseau du réseau interne.

Add Ru	le											
Name	AC RDP Access				🖌 En	abled		Insert	into Manda	tory		~
Action	Allow			V V D /8	<b>1</b> 5							
Zone	s Networks VLA	N Tags U	sers	Applications	Ports	URLs	SGT/ISE	Attributes		Inspection	Logging	Comments
Availabl	le Networks 🖸		0		Source	e Netwo	rks (1)			Destination Networks	(1)	
🔍 Sear	rch by name or value					Source		Original (	Client	📰 Inside_Net		ū
	Networks	Geolocation			📄 Ar	yConned	_Pool		6			
Insid	de_Net I-Benchmark-Tests I-Link-Local I-Multicast I-Private-10.0.0.0-8 I-Private-172.16.0.0-12 I-Private-192.168.0.0-16 I-Private-All-RFC1918 i-IPvi-Manned		~	Add To Source Networks Add to Destination	Enter	an IP ado	fress		Add	Enter an IP address		Add
											Add	Cancel

Sous Utilisateurs, cliquez sur le domaine créé précédemment sous Domaines disponibles, cliquez sur le groupe/utilisateur approprié sous Utilisateurs disponibles, puis cliquez sur Ajouter à la règle.

Si aucun utilisateur ou groupe n'est disponible dans la section Utilisateurs disponibles, assurezvous que FMC a pu télécharger les Utilisateurs et les Groupes sous la section Domaine et que les Groupes/Utilisateurs appropriés sont inclus.

Les utilisateurs/groupes spécifiés ici sont vérifiés du point de vue source.

Par exemple, avec ce qui a été défini dans cette règle jusqu'à présent, le FTD évalue que le trafic provient de la zone externe et est destiné à la zone interne, provient du réseau dans l'objet AnyConnect\_Pools et est destiné au réseau dans l'objet Inside\_Net, et le trafic provient d'un utilisateur dans le groupe Administrateurs AnyConnect.

Add Ri	ıle													? ×
Name	AC RE	DP Access			Vala	E E	nabled	I	insert	into Mandato	ory 🍾	·		
Zone	is N	letworks	VLAN Tags	Users	Applications	Ports	URLs	SGT/ISE Attrib	utes			Inspection	Logging	Comments
Availab	ile Rea rch by cial Ide	name or va	lue		Available Usen Search by n LAB-AD/* AnyConnect AnyConnect AnyConnect Ladmin Ladmin Ladmin	ame or va Admins Users	alue		A	dd to Rule	Selected	Users (1) AD/AnyConnect	: Admins	ū
													Add	Cancel

Sous Ports, des objets RDP personnalisés ont été créés et ajoutés pour autoriser les ports TCP et UDP 3389. Notez que le protocole RDP aurait pu être ajouté sous la section **Applications**, mais pour des raisons de simplicité, seuls les ports sont vérifiés.

Name AC RDP Access     Action        Zones        Zones        VLAN Tags        Ports           Zones        Zones              Zones <b>Add to</b> <b>Add to</b> <b>DNS_over_ICP Add to</b> <b>Destination Add to</b> <b>Destination Add to</b> <b>Destination Add to</b> <b>Destination Destination Destination</b> </th <th>Add Rule</th> <th></th> <th></th> <th></th> <th></th> <th>? ×</th>	Add Rule					? ×
Action Allow Zones Networks VLAN Tags Users Applications Ports URLs SGT/ISE Attributes Inspection Logging Comments Available Ports C Selected Source Ports (0) Selected Destination Ports (2) Search by name or value Add to DNS_over_TCP Add to DNS_over_UDP Add to Destination PTD-3-FDM FTP-3-FDM	Name AC RDP Access		Enabled	Insert	into Mandatory 👻	
Zones       Networks       VLAN Tags       Users       Applications       Ports       URLs       SGT/ISE Attributes       Inspection       Logging       Comments         Available Ports       C       Selected Source Ports (0)       Selected Destination Ports (2)         Search by name or value       any       PDP-TCP       PRDP-TCP       PRDP-UDP       PRDP-U	Action 🖋 Allow	• 003	3 th J			
Available Ports       Selected Source Ports (0)       Selected Destination Ports (2)         Search by name or value       any         AOL       Bittorrent         DNS_over_TCP       Add to         DNS_over_UDP       Add to         FMC-HTTPS       Add to         PrO3-SSH       Destination         FTD-3-SSH       FTD	Zones Networks VLAN Tags	Users Applications	Ports URLs	SGT/ISE Attributes	Inspection	Logging Comments
AOL AOL Bittorrent DNS_over_TCP FMC-HTTPS FTD-3-FDM FTP FTP	Available Ports 🗳	0	Selected Source	e Ports (0)	Selected Destination F	Ports (2)
Protocol Y Port Enter Add Protocol TCP (6) Y Port Enter a Add	Search by name or value  AOL  Sittorrent  DNS_over_TCP  DNS_over_UDP  FNC-HTTPS  FNC-SSH  FTD-3-FDM  FTD-3-SSH  FTP  HTTP	Add to Source Add to Destination	Protocol		Add Protocol TCP (6)	<ul> <li>Port Enter a Add</li> </ul>

Enfin, sous **Journalisation**, la **fonction Se connecter à la fin de la connexion** est vérifiée pour une vérification supplémentaire ultérieure. Cliquez sur **Add** lorsque vous avez terminé.

Add Rule ✓ Enabled Name AC RDP Access ¥ Insert into Mandatory V O B A 🕁 🗾 Action 🖌 Allow Inspection Logging Zones Networks VLAN Tags Users Applications Ports URLs SGT/ISE Attributes Comments Log at Beginning of Connection Log at End of Connection File Events: Log Files Send Connection Events to: Event Viewer Syslog Server (Using default syslog configuration in Access Control Logging) Show Overrides SNMP Trap Select an SNMP Alert Configuration... Y 0 Add Cancel

9. Une règle supplémentaire est créée pour l'accès HTTP afin de permettre aux utilisateurs du groupe AnyConnect User d'accéder au site Web Windows Server IIS. Cliquez sur Save.

Overview Analysis Policies Devices	Objects AMP Intelligence	Deploy 🍳 System Help 🔻 admin
Access Control > Access Control Network	iscovery Application Detectors Correlation Actions •	
Default-Policy Enter Description		You have unsaved changes 🛛 Analyze Hit Counts 🛛 🔚 Save 🛛 🕲 Cance
Prefilter Policy: Default Prefilter Policy	551. Policy: None	Identity Policy: <u>FTD-2 Identity Policy</u>
		🏣 Inheritance Settings   🖳 Policy Assignments (1
Rules Security Intelligence HTTP Response	Logging Advanced	
# Filter by Device	Show Rule	Conflicta 🖶 😳 Add Category 🗳 Add Rule 📑 Search Rules
# Name Source Zo Dest Zone	Source Networks Dest Netwo V Users	A S Dest Ports U S D Action
<ul> <li>Mandatory - Default-Policy (1-2)</li> </ul>		
1 AC RDP Access A outside-zone A inside-z	ne 🚍 AnyConnect_Pool 🚔 Inside_Net 🛛 Arc 🖨 LAB-AD/AnyConnect Admi	ns Any Any 🏂 RDP-TCP Any Any Any VAllow 🗍 🕞 🚖 📑 0 🥒
2 AC HTTP Access In outside-zone III inside-z	ne 🚊 AnyConnect_Pool 👼 Inside_Net 🛛 🛷 🖉 LAB-AD/AnyConnect Users	a Any Any PHTTP - Any Any Any VAllow 🛈 🖸 🗟 🖄 🗾 0 🕜 I
▼ Default - Default-Policy (-)		
There are no rules in this section. Add Rule or Add Cate	2017	
Default Action		Access Control: Block All Traffic

Displaying 1 - 2 of 2 rules |< < Page 1 of 1 > >| C | Rules per page: 100 \*

? X

### **Configurer l'exemption NAT**

Si certaines règles NAT affectent le trafic AnyConnect, telles que les règles PAT Internet, il est important de configurer les règles d'exemption NAT afin que le trafic AnyConnect ne soit pas affecté par la NAT.

#### 1. Accédez à Périphériques > NAT.

Overview Analysis	s Polici	es Dev	ices	Objects AMP	Intelligence			Deploy	0,	System	Help 🔻	admin 🔻
Device Management	NAT	VPN •	QoS	Platform Setting:	s FlexConfig	Certificates						

Sélectionnez la stratégie NAT appliquée au FTD.

Overview Analysis	Policies	Devices	Objects	AMP In	itelligence			Deploy	<b>e</b> ,	System	Help 🔻	admin v
Device Management	NAT \	/PN V Q	oS Platfor	rm Settings	FlexConfig	Certificates						
											🔾 New	Policy
NAT Policy				De	vice Type		Status					
FTD-2-NAT-Policy				The	eat Defense		Targeting 1 devices Up-to-date on all targeted	devices			<b>D</b> B	/ 6

2. Dans cette stratégie NAT, il y a une PAT dynamique à la fin de laquelle la PAT affecte tout le trafic (y compris le trafic AnyConnect) sortant de l'interface externe vers l'interface externe.

Pour empêcher que le trafic AnyConnect ne soit affecté par la NAT, cliquez sur **Add Rule** dans le coin supérieur droit.

Overview A	nalysis	Policies Devi	ces Objects	AMP Inte	lligence			Depl	oy 🔒 :	System Help 🔻	admin 🔻
Device Manage	ment l	VPN *	QoS Platfor	m Settings	FlexConfig	Certificates					
FTD-2-NA Enter Description	AT-Poli	cy						🔔 s	how Warning	s 📔 Save	Cancel
Rules										E Policy A	ssignments (1
B Filter by Device										0	Add Rule
					Original Pack	et 🗾 🔪		Translated Packet			
# Direction	Туре	Source Interface Object	Destination Interface Object	Original Sources	Original Destination	Orig Service	Translated Sources	Translated Destinations	Trans Services	Options	
▼ NAT Rules Befo	re										
▼ Auto NAT Rules	;										
= +	Dynamic	🥞 any	🚠 outside-zone	🚌 obj-any			🥵 Interface			🝓 Dns:false	/8
<ul> <li>NAT Rules After</li> </ul>	r										
						Displayin	g 1-1 of 1 rows 🕅	< Page 1 of	1 > >	C Rows per p	age: 100 •

3. Configurez une règle d'exemption NAT, assurez-vous qu'il s'agit d'une règle NAT manuelle de type statique. Il s'agit d'une règle NAT bidirectionnelle qui s'applique au trafic AnyConnect.

Avec ces paramètres, lorsque le FTD détecte le trafic provenant de Inside\_Net et destiné à l'adresse IP AnyConnect (définie par AnyConnect\_Pool), la source est traduite en la même valeur (Inside\_Net) et la destination est traduite en la même valeur (AnyConnect\_Pool) lorsque le trafic entre dans la zone inside\_zone et sort de la zone outside\_zone. Cela contourne essentiellement la NAT lorsque ces conditions sont remplies.

Add NAT Rule								? ×
NAT Rule:	Manual NAT Rul	e 👻	Insert:	In Cat	egory	✓ NAT Rules Befo	xe Y	
Type:	Static	~	🗹 Enable					
Description:								0
Interface Objects	Translation	PAT Pool	Advanced					
Available Interface Obj	jects C		Source	Interface Objects (1)	C	Destination Interface	Objects (1)	
🔍 zone		×	📩 insid	le-zone	6	📸 outside-zone		6
🚠 inside-zone								
and outside-zone		Ad	ld to urce					
		A	ld to					
		Dest	ination					
							OK Can	cel

Add NAT Rule					?
NAT Rule:	Manual NAT Rule	Insert:	In Category	▼ NAT Rules Before ▼	
Type:	Static 💌	Enable			
Description:					0
Interface Objects	ranslation PAT Pool	Advanced			
Original Packet			Translated Packet		
Original Source:*	Inside_Net	× 0	Translated Source:	Address	~
Original Destination:	Address	*		Inside_Net	<b>~</b> O
	AnyConnect_Pool	<b>~</b> ()	Translated Destination:	AnyConnect_Pool	<b>~</b> 0
Original Source Port:		¥ 0	Translated Source Port:		<b>~</b> 0
Original Destination Po	rt:	¥ ()	Translated Destination Port:		<ul> <li>O</li> </ul>
				ок	Cancel

En outre, le FTD est configuré pour effectuer une recherche de route sur ce trafic et non pas le proxy ARP. Cliquez sur **OK** lorsque vous avez terminé.

Add NAT Rule					? ×
NAT Rule:	Manual NAT Rule	Insert:	In Category	NAT Rules Before	•
Type:	Static 🗸 🖌	Enable			
Description:					$\hat{}$
Interface Objects	Translation PAT Pool Adva	anced			
Translate DNS replie	s that match this rule				
Fallthrough to Inter	ace PAT(Destination Interface)				
IPv6					
Net to Net Mapping					
Do not proxy ARP o	Destination Interface				
🗹 Perform Route Look	up for Destination Interface				
Unidirectional					
				ОК	Cancel

4. Cliquez sur Enregistrer.

3	Overview	Analysis	Policies D	evices	Objects	AMP	Intellige	nce				Deploy	0,	System	Help 🔻	admin 🔻
	Device Mana	pement	NAT VPN	• Qo	S Platfor	m Setting	s Flex	Config Certifica	ates							
	FTD-2-N	AT-Pol	icy							You have un	tsaved changes	🔔 Show V	Varning	5) 📙	Save	😫 Cancel
	Rules	_												5	Policy As	signments (1)
đ	Filter by Devic	e.													0	Add Rule
							Orig	jinal Packet			Translated Pack	et				
4	Direction	Туре	Source Interface O	Des bje: Inte	tination rface Object	Original Sources	C I	Original Destinations	Orig Services	Translated Sources	Translated Destinations	Tra	ans rvices	Options	•	
٠	NAT Rules Be	fore														
1	47	Static	å inside-zo	ne 🚠 o	outside-zone	👼 Inside	_Net <u>i</u>	AnyConnect_Pool		📻 Inside_Net	👼 AnyConnec	t_Pool		🥞 Dris: 🥞 routi 🕞 no-p	false e-lookup roxy-arp	/ 6
٠	Auto NAT Rul	es														
2	•	Dynamic	🍓 any		outside-zone	🚌 obj-ar	ny			🍓 Interface				🝓 Dns:	false	Ø 6
•	NAT Rules Af	ter														
									Displaying	1-2 of 2 rows	C < Page 1	of 1 >	×	C R	ows per pa	ige: 100 •

# Déploiement

1. Une fois la configuration terminée, cliquez sur le bouton **Déployer** en haut à droite.



2. Cochez la case en regard du FTD auquel la configuration est appliquée, puis cliquez sur **Déployer**.

Depl	oy Policies Version:2020-05-04 09:40 AM					×
V	Device	Inspect Interruption	Туре	Group	Current Version	٢
1	=/FTD-2	No	FTD		2020-05-04 09:16 AM	
Select	ed devices: 1				Deploy Car	ncel

# Vérifier

# **Configuration finale**

# **Configuration AAA**

```
> show running-configuration aaa-server
aaa-server LAB-AD protocol ldap
max-failed-attempts 4
realm-id 5
aaa-server LAB-AD host win2016.example.com
server-port 389
ldap-base-dn DC=example,DC=com
ldap-group-base-dn DC=example,DC=com
ldap-scope subtree
ldap-naming-attribute samaccountname
ldap-login-password *****
ldap-login-dn ftd.admin@example.com
server-type microsoft
```

### **Configuration AnyConnect**

```
> show running-config webvpn
webvpn
enable Outside
anyconnect image disk0:/csm/anyconnect-linux64-4.7.03052-webdeploy-k9.pkg 1 regex "Linux"
anyconnect image disk0:/csm/anyconnect-win-4.7.00136-webdeploy-k9.pkg 2 regex "Windows"
anyconnect profiles Lab disk0:/csm/lab.xml
anyconnect enable
tunnel-group-list enable
cache
 no 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-simultaneous-logins 10
vpn-tunnel-protocol ikev2 ssl-client
split-tunnel-policy tunnelspecified
split-tunnel-network-list value Lab
user-authentication-idle-timeout none
webvpn
 anyconnect keep-installer none
 anyconnect modules value dart
 anyconnect ask none default anyconnect
 http-comp none
 activex-relay disable
 file-entry disable
 file-browsing disable
 url-entry disable
```

deny-message none anyconnect ssl df-bit-ignore enable

> show running-config ssl
ssl trust-point FTD-2-SelfSigned outside

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

🚳 Cisco AnyCo	nnect Secure Mob	oility Client	_		×	
	VPN: Contacting ftd2.exa ftd2.example.com	ample.com.	~ C	onnect		
<b>¢</b> (i)	S ci	isco AnyConne	ect   ftd2.ex	ample.com	ı →	<
		Group:	General		~	
		Username:	it.admin			
		Password:	******			
				ОК	Cancel	
🕙 Cisco AnyCo	nnect Secure Mot	oility Client	-		×	
	VPN: Connected to ftd2. ftd2.example.com	example.com.	V Dis	connect		
00:00:12				IPv4	4	
<b>Ö</b> (i)						

L'utilisateur IT Admin fait partie du groupe AnyConnect Admins qui a un accès RDP au serveur Windows, mais n'a pas accès à HTTP.

L'ouverture d'une session RDP et Firefox sur ce serveur permet de vérifier que cet utilisateur ne peut accéder au serveur que via RDP.



Si vous êtes connecté avec l'utilisateur Utilisateur test qui fait partie du groupe Utilisateurs AnyConnect disposant d'un accès HTTP mais pas d'un accès RDP, nous pouvons vérifier que les règles de stratégie de contrôle d'accès prennent effet.

💀 Remote Desktop Connection 🛛 🗌 🗙	
Remote Desktop	Remote Desktop Connection X
Tonnection	Remote Desktop can't connect to the remote computer for one of these reasons:
Computer:         win2016.example.com         ~           User name:         None specified	<ol> <li>Remote access to the server is not enabled</li> <li>The remote computer is turned off</li> <li>The remote computer is not available on the network</li> <li>Make sure the remote computer is turned on and connected to the network, and that remote access is enabled.</li> </ol>
Show Optio Connect Help	OK Help
IIS Windows Server 🗙 🔆 Options	× + – – ×
← → C <sup>a</sup> û 🛛 🖉 win2016.example.com	⊽☆ Ⅲ\ ۩ 📽 🔩 Ξ
🕂 Windows Server	
Internet Information Serv	vices
Welcome Rienvenue Terretul	
Herverue Terveru	

# Vérifier avec les événements de connexion FMC

Comme la journalisation a été activée dans les règles de stratégie de contrôle d'accès, les événements de connexion peuvent être vérifiés pour tout trafic correspondant à ces règles

Accédez à Analysis > Connections > Events.

Overview Analys	sis Policies D	Devices Objec	ts AMF	P Intellige	ence		eploy 🔒	System Help	▼ admin ▼
Context Explorer	Connections <b>v</b>	Intrusions 🔻	Files 🔻	Hosts 🔻	Users v	Correlation <b>v</b>	Advanced 🔻	Search	
	Events								
	Security Intelligence Events								

Dans la **vue Tableau des événements de connexion**, les journaux sont filtrés pour afficher uniquement les événements de connexion pour l'administrateur informatique.

Ici, vous pouvez vérifier que le trafic RDP vers le serveur (TCP et UDP 3389) est autorisé, mais que le trafic du port 80 est bloqué.

C	)verv	view	Analysi	s Policies I	Devices	Objects	AMP	Intelligence			Dep	loy 🔒	System	Help 🔻	admin 🔻
C	onte:	kt Exp	plorer C	onnections + E	vents	Intrusions	▼ File	es 🔻 🛛 Hosts 🔻	Users v	Correlation	<ul> <li>Advanced •</li> </ul>	Search			
										Bookmark This I	Page Report Design	er Dashboar	d View B	ookmarks	Search •
C	Con	neo	ction Ev	ents (switch	workflow)							0.05.05.14	14-17 - 24		
c	onnec	tions	with Applicati	ion Details > Tab	le View of	Connection	Events				1 20	0-05-05 14:	14:17 - 20	E	Expanding
٠	Searc	ch Co	nstraints ( <u>Edi</u>	t Search Save Sea	arch)									Disabl	led Columns
	Jump	p to	. 🔻												
	Jump ]	p to	Action ×	Initiator × IP	Initiator	<u>r User</u> ×		Responde IP	r × Ingre Secu	ss × ity Zone	Egress × Security Zone	Source Pe ICMP Typ	ort/×	Destinat	tion Port / ×
	Jumt ] J	p to	Action ×	Initiator × IP 10.10.10.1	Initiator	<u>r User</u> × nin (LAB-AD\it	admin, L	Responde IP DAP) # 192.16	r × Ingre Secur	ss X ity Zone	Egress X Security Zone	Source Py ICMP Typ 62473 / to	ent / ×	Destinat ICMP Co 3389 / to	<u>tion Port /</u> × de
	Jump ] ] ] ] ]	p to	Action × Allow Block	Initiator × IP 10.10.10.1 10.10.10.1	Initiator	r User × nin (LAB-AD\it nin (LAB-AD\it	admin, L	Responde           IP           DAP1           International           DAP1           International           International	r × Ingre Secur 3.1.1 outsid	ss × ity Zone -zone	Egress X Security Zone inside-zone inside-zone	Source Pr ICMP Typ 62473 / to 62474 / to	2	Destinat ICMP Co 3389 / to 80 (http)	t <u>ion Port /</u> × de 2 / tcp
	Jump ] 4 [ 4 [ 4 ] 4 ]	• to	Action × Allow Block Block	Initiator × IP 10.10.10.1 10.10.10.1 10.10.10.1	Initiator	r.User × nin (LAB-AD\it nin (LAB-AD\it nin (LAB-AD\it	admin, Li admin, Li admin, Li	Responde           IP           DAP1           I 192.16:           DAP1           I 192.16:           DAP1           I 192.16:           DAP1           I 192.16:	r × Ingre Secur \$1.1 outsid \$1.1 outsid \$1.1 outsid	t-zone t-zone t-zone	Egress × Security Zone inside-zone inside-zone inside-zone	Source Pr ICMP Typ 62473 / to 62474 / to 62475 / to	2 2 2 2	Destinat ICMP Co 3389 / tor 80 (http) 80 (http)	t <u>ion Port /</u> × de 2 / tcp / tcp

Pour l'utilisateur **Test User**, vous pouvez vérifier que le trafic RDP vers le serveur est bloqué et que le trafic du port 80 est autorisé.

Overview	Analysi	s Policies	Devices	Objects	AMP Inte	lligence				Deplo	v 🔍	System	Help 🔻	admin 🔻
Context Exp	olorer C	onnections • I	Events	Intrusions •	Files 🔻	Hosts ¥ U	sers v	Correlati	on 🔻	Advanced •	Search			
								Bookmark Th	nis Page	Report Designer	Dashboard	d View Bo	okmarks	Search •
Connections • Search Con Jump to	Bookmark This Page Report Designer Dashboard View Bookmarks Search •         Connection Events (switch workflow)         Connections with Application Details > Table View of Connection Events         • Search Constraints (Edit Search Save Search)         Disabled Columns													
	Action ×	Initiator × IP	Initiator	User ×		Responder × IP	Ing	ress > urity Zone	C Ear	ress × curity Zone	Source P ICMP Typ	<u>ort/</u> ×	Destina ICMP C	ation Port / >
1	Block	10.10.10.1	📑 <u>test us</u>	ser (LAB-AD\test	user, LDAP)	192.168.1.1	outsi	de-zone	insid	de-zone	<u>62493 / to</u>	æ	3389 / t	52
4	Allow	10.10.10.1	📇 <u>test us</u>	ser (LAB-AD\test	user, LDAP)	192.168.1.1	outsi	de-zone	insid	de-zone	62494 / to	æ	80 (http	) / tcp

# Dépannage

# Déboguages

Ce débogage peut être exécuté dans l'interface de ligne de commande de diagnostic pour dépanner les problèmes liés à l'authentification LDAP : **debug Idap 255** 

Pour dépanner les problèmes de politique de contrôle d'accès d'identité d'utilisateur, le **système de support firewall-engine-debug** peut être exécuté en conflit pour déterminer pourquoi le trafic est autorisé ou bloqué de façon inattendue.

### Débogages LDAP en cours

```
[53] Session Start
[53] New request Session, context 0x00002b1d13f4bbf0, 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
[53]
       objectClass: value = person
[53]
       objectClass: value = organizationalPerson
      objectClass: value = user
[53]
      cn: value = IT Admin
[53]
[53]
      sn: value = Admin
[53]
      givenName: value = IT
      distinguishedName: value = CN=IT Admin, CN=Users, DC=example, DC=com
[53]
      instanceType: value = 4
[53]
       whenCreated: value = 20200421025811.0Z
[53]
[53]
       whenChanged: value = 20200421204622.0Z
      displayName: value = IT Admin
[53]
[53]
      uSNCreated: value = 25896
      memberOf: value = CN=AnyConnect Admins,CN=Users,DC=example,DC=com
[53]
      uSNChanged: value = 26119
[53]
      name: value = IT Admin
[53]
[53]
       objectGUID: value = &...J..O..2w...c
[53]
       userAccountControl: value = 512
      badPwdCount: value = 6
[53]
[53]
      codePage: value = 0
      countryCode: value = 0
[53]
[53]
      badPasswordTime: value = 132320354378176394
[53]
      lastLogoff: value = 0
      lastLogon: value = 0
[53]
      pwdLastSet: value = 132319114917186142
[53]
      primaryGroupID: value = 513
[53]
[53]
      objectSid: value = ......{I...;....j...
[53]
      accountExpires: value = 9223372036854775807
[53]
      logonCount: value = 0
      sAMAccountName: value = it.admin
[53]
[53]
       sAMAccountType: value = 805306368
[53]
       userPrincipalName: value = it.admin@example.com
[53]
       objectCategory: value = CN=Person, CN=Schema, CN=Configuration, DC=example, DC=com
       dSCorePropagationData: value = 1601010100000.0Z
[53]
[53]
       lastLogonTimestamp: value = 132319755825875876
[53] Fiber exit Tx=515 bytes Rx=2659 bytes, status=1
[53] Session End
```

#### Impossible d'établir une 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 FTD reçoit une réponse du serveur LDAP.
- 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 utilisés sont corrects. Si un nom d'hôte est utilisé, vérifiez que DNS est en mesure de le résoudre à l'adresse IP correcte.

### DN et/ou mot de passe de connexion 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 nom distinctif (DN) de connexion et le mot de passe de connexion sont configurés correctement. Vous pouvez vérifier cela sur le serveur AD avec **Idp.exe**. Afin de vérifier qu'un compte peut se lier correctement à l'aide de Idp, procédez comme suit :

1. Sur le serveur AD, appuyez sur Win+R et recherchez Idp.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. Sous Connexion, choisissez Connecter...

🔝 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		<u>C</u> ancel

4. La colonne de droite affiche du texte indiquant une connexion réussie. Accédez à **Connexion >** Lier...

🟠 Idap://w	in2016.ex	ample.co	om/DC:	= example, DC	=com		_		×
Connection	Browse	View	Optio	ns Utilities	Help				
Connec Bind Discon New Save Save Save As Exit	nect	Ctrl+B		Id = Idap_op Established Retrieving b Getting 1 en Dn: (RootD configu CN= current Tim defaultM dnsHos domain0 domain0 dosServi Set Firs Nan con forestFit highest( isGlobal isSynch	en ("localho connection ase DSA in tries: SE) rationNamin =Configurati Time: 5/1/20 e; NamingConte tName: win ControllerFu functionality iceName: Cl tings,CN=W st-Site- ne,CN=Sites n; unctionality: CommittedU ICatalogRea tronized: The viceName: Cl	st", 389); to localhost. formation gContext: ion,DC=examp 20 4:16:55 PM ext: DC=examp 2016.example inctionality: 7 = /: 7 = (WIN201 N=NTDS IN2016,CN=Se s,CN=Configur SN: 13410; ady: TRUE; RUE; example.com	le,DC=ci I Easterr ple,DC=c .com; = ( WIN20 16 ); ervers,C ation,DC 6 ); win2016	om; n Daylight com; 016 ); N=Default- ;=example,D	^  C= ↓

5. Sélectionnez **Simple Bind**, 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	rrently logged on user redentials (DIGEST) affic after bind Cancel OK									

Avec une liaison réussie, ldp affiche Authenticated as: DOMAIN\username

🔐 Idap://w	in2016.exa	mple.co	om/DC=ex	ample,DC	=com		_		$\times$	
Connection	Browse	View	Options	Utilities	Help					
			R	1.2. 1.2. 1.2. supporte Max Max Max Max Max Max Max Max	840.113556 840.113556 840.113556 edLDAPPoli PercentDir ReceiveBu Connection BatchRetur DirSyncDu ResultSetS ResultSetS ValRange; edMemory edLDAPVer edSASLMe IEGO; EXTE	5.1.4.2255; 5.1.4.2256; 5.1.4.2309; icies (20): Ma SyncReques ffer; InitRecv ns; MaxConn rnMessages ration; MaxTo ize; MinResu PerConn; Ma MaxValRang Limit; Syster rsion (2): 3; 2 chanisms (4 :RNAL; DIGE _s(Id, 'ftd.ad	axPoolThr sts; MaxDa /Timeout; IdleTime; I ; MaxQuel empTable: ultSets; axNotificat geTransitiv mMemoryL 2; ): GSSAPI ST-MD5; min@exar min".	eads; atagramR MaxPage! ryDuratio Size; tionPerCo ve; .imitPerce l; GSS-	ecv; Size; n; mn; ent;	~
Ready										

Une tentative de liaison avec un nom d'utilisateur ou un mot de passe non valide entraîne un échec tel que les deux suivants.

🔝 Idap://w	in2016.exa	mple.co	om/DC=ex	ample,DC:	=com		_		×
Connection	Browse	View	Options	Utilities	Help				
	MaxResultSetSize; MinResultSets; MaxResultSetsPerConn; MaxNotificationPer MaxValRange; MaxValRangeTransitive; ThreadMemoryLimit; SystemMemoryLimitPer supportedLDAPVersion (2): 3; 2; supportedSASLMechanisms (4): GSSAPI; GSS- SPNEGO; EXTERNAL; DIGEST-MD5; 								
			< E S C E ir	unavailable rror <49>: I erver error omment: Ac rror 0x8009 ivalid	i>); // v.3 dap_simple_ :: 80090308: cceptSecurit 90308 The to	bind_s() fail LdapErr: DS yContext en ken supplie	led: Invali SID-0C090 ror, data d to the f	d Credentia 042A, 52e, v3839 unction is	is V
Ready									

### Le serveur LDAP ne trouve pas le 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. Après avoir réussi la liaison comme vu ci-dessus, naviguez à Affichage > Arborescence.

Idap://win2016.example.com/DC=example,DC=com								-		×		
Connection	Browse	View	v Options	Utilities	Help							
			Tree	C		Ctrl+T				^		
			Enterprise	Enterprise Configuration Status Bar Set Font					NaxPoolThreads; sts; MaxDatagramRecv; cvTimeout; nldleTime; MaxPageSize;			
		~	Set Font									
s; MaxQueryDu MaxDirSyncDuration; MaxTempTableSize; MaxResultSetSize; MinResultSets; MaxResultSetSPerConn; MaxNotificationP MaxValRange; MaxValRangeTransitive; ThreadMemoryLimit; SystemMemoryLimitP supportedLDAPVersion (2): 3; 2; supportedSASLMechanisms (4): GSSAPI; GS SPNEGO; EXTERNAL; DIGEST-MD5; 								ze; nPerCo ; nitPerce GSS- ole.com	nn; :nt;			
1												

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

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

3. Cliquez avec le bouton droit sur le DN de base, puis cliquez sur Rechercher.

Idap://win2016.example.com/DC=example,DC=com -								
Connection Browse	View Opti	ons Utiliti	es Help					
DC= example, DC= co	Sea Virt Del Mo Ado Cor Adv Cop Sele Cle	rch ual List Viev ete dify dify DN d child mpare vanced oy DN oy ect all ar output	Ctrl+S v Ctrl+D Ctrl+M Ctrl+R Ctrl+A Ctrl+A	cipals,DC=example,DC=com; 11D2B9AA00C04F79F805:CN =example,DC=com; 11D297C400C04FD8D5CD:C =example,DC=com; 11D1ADED00C04FD8D5CD:C =example,DC=com; 11D1ADED00C04FD8D5CD:C ole,DC=com; 11D1AA4B00C04FD7D83A:O s,DC=example,DC=com; 11D1ADED00C04FD8D5CD:C ample,DC=com; 311D1ADED00C04FD8D5CD:C e,DC=com; 0 3:43:59 PM Eastern Daylight 2:41:57 PM Eastern Daylight	~			
Create a new document								

4. Spécifiez les mêmes valeurs Base DB, Filter et Scope que celles affichées dans les débogages.

Dans cet exemple, il s'agit des éléments suivants :

- DN de base : dc=exemple, dc=com
- Filtre : samaccountname=it.admi
- Portée:SOUS-ARBORESCENCE

🟠 Idap://w	n2016.example.com/DC=example,DC=com	– 🗆 X	
Connection	Browse View Options Utilities Help		
Search	×	C=example,DC=com; 58811D1ADED00C04FD8D5CD:C DC=example,DC=com;	^
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 $\sim$	68811D1ADED00C04FD8D5CD:C mple,DC=com; 2020 3:43:59 PM Eastern Davlight	
Options	Run Close	)20 2:41:57 PM Eastern Daylight	
	***Searching ldap_search_s(ld, "DC= "sAMAccountName=it.a Getting 0 entries:	example,DC=com", 2, dmī", attrList, 0, &msg)	~
Ready			

ldp trouve 0 entrées en raison de l'absence de compte d'utilisateur portant le nom de compte **it.admi** sous le DN de base dc=example,dc=com

Une autre tentative avec le nom de compte correct **it.admin** affiche un résultat différent. ldp trouve 1 entrée sous le DN de base dc=example,dc=com et imprime ce DN utilisateur.

🔐 Idap://w	in2016.example.	com/DC=ex	ample,DC:	=com		- □ >	<
Connection	Browse View	Options	Utilities	Help			
Search					$\times$	58811D1ADED00C04FD8D5CD:C DC=example,DC=com;	^
Base <u>D</u> N: Filter:	DC=example,DC	C=com ne=it.admin			~	58811D1ADED00C04FD8D5CD:C ample,DC=com; D211D1AA4B00C04FD7D83A:C lers DC=example DC=com;	) )
Scope	O <u>O</u> ne Level	● <u>S</u> ubtree	e			58811D1ADED00C04FD8D5CD:C example,DC=com; 68811D1ADED00C04FD8D5CD:C mple DC=com;	2
<u>A</u> ttributes:	objectClass;nam	e;descriptior	n;canonicalN	lame	$\sim$	020 3:43:59 PM Eastern Dayligh	t
Options		<u>R</u> un		<u>C</u> lose		)20 2:41:57 PM Eastern Daylight	
		k G D	**Searching dap_search sAMAccour Setting 1 ent On: CN=IT A canonica name: IT objectCla user	I _s(Id, "I ntName= tries: Admin,( alName: Admin; ass (4): r;	DC=e =it.ad C <b>N=U</b> exar top;	min", attrList, 0, &msg) <b>Isers,DC=example,DC=com</b> 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 utilisateur est configuré correctement et qu'il n'a pas expiré. Tout comme le DN de connexion, le FTD effectue une liaison avec AD avec les informations d'identification de l'utilisateur.

Cette liaison peut également être effectuée dans ldp pour vérifier que le service AD est capable de reconnaître les mêmes informations d'identification de nom d'utilisateur et de mot de passe. Les étapes dans ldp sont montrées dans la section **Liaison DN de connexion et/ou mot de passe incorrect**.

En outre, les journaux de l'**Observateur d'événements du** serveur Microsoft peuvent être consultés pour une raison potentielle.

# Test AAA

La commande test **aaa-server** peut être utilisée pour simuler une tentative d'authentification à partir du FTD avec un nom d'utilisateur et un mot de passe spécifiques. Cela 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 des paquets LDAP quittent le FTD, mais qu'il n'y a pas de réponse, cela peut indiquer un problème de routage.

La capture 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>
                        192.168.1.1.389 > 192.168.1.17.61960: S 491521506:491521506(0) ack
  2: 23:02:16.772009
3681912835 win 8192 <mss 1460,nop,nop,timestamp 762393884 1061373057>
                           192.168.1.17.61960 > 192.168.1.1.389: . ack 491521507 win 32768
   3: 23:02:16.772039
<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>
   9: 23:02:16.775075
                          192.168.1.17.61960 > 192.168.1.1.389: . ack 491522163 win 32768
<nop,nop,timestamp 1061373061 762393887>
[...]
54 packets shown
```

### Journaux de l'Observateur d'événements Windows Server

Les journaux de l'**Observateur d'événements** sur le serveur AD peuvent fournir des informations plus détaillées sur la raison d'une défaillance.

1. Recherchez et ouvrez l'Observateur d'événements.

=	Best match								
ŵ	Event Viewer Desktop app								
	Settings >								
	🖄 Vie	ever	nt logs						
۲	D1	٢	ß		2	₽	រុជ		
	event								
-	Q	([])	e	-	2		8		

2. Développez **Journaux Windows** et cliquez sur **Sécurité**. Recherchez les échecs d'**audit** avec le nom de compte d'utilisateur et consultez les informations sur les échecs.



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
## 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.