AD-verificatie (LDAP) en gebruikersidentiteit op FTD beheerd door FMC configureren voor AnyConnect-clients

Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Achtergrondinformatie Configureren Netwerkdiagram en -scenario Active Directory-configuraties Bepaal LDAP-basis DN en groep DN Een FTD-account maken AD-groepen maken en gebruikers toevoegen aan AD-groepen (optioneel) Kopieert de SSL-certificaatroet van LDAPS (alleen vereist voor LDAPS of STARTTLS). **FMC-configuraties** Licentie controleren Instellingsgebied AnyConnect configureren voor AD-verificatie Identiteitsbeleid inschakelen en Beveiligingsbeleid voor gebruikersidentiteit configureren NAT-vrijstelling configureren Implementeren Verifiëren Laatste configuratie AAA-configuratie Configuratie AnyConnect Verbinding maken met AnyConnect en toegangscontroleregels controleren Verifiëren met FMC Connection-gebeurtenissen Problemen oplossen Debugs LDAP-debugs werken Kan geen verbinding maken met LDAP-server Binding Login DN en/of wachtwoord niet correct LDAP-server kan de gebruikersnaam niet vinden Onjuist wachtwoord voor de gebruikersnaam AAA testen PacketCapture Logbestanden van Windows Server Event Viewer

Inleiding

Dit document beschrijft hoe u AD-verificatie moet configureren voor AnyConnect-clients die verbinding maken met Cisco Firepower Threat Defence (FTD).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Basiskennis van RA VPN-configuratie op FMC
- Basiskennis van de LDAP-serverconfiguratie op het VCC
- Basiskennis van Active Directory (AD)

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Microsoft 2016-server
- FMCv met 6.5.0
- FTDv met 6.5.0

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Dit document beschrijft hoe u Active Directory (AD)-verificatie kunt configureren voor AnyConnectclients die verbinding maken met Cisco Firepower Threat Defence (FTD), beheerd door Firepower Management Center (FMC).

Gebruikersidentiteit wordt gebruikt in het toegangsbeleid om AnyConnect-gebruikers te beperken tot specifieke IP-adressen en -poorten.

Configureren

Netwerkdiagram en -scenario





outside



Windows Server

AnyConnect Client

Windows-server is vooraf geconfigureerd met IIS en RDP om de gebruikersidentiteit te testen. In deze configuratiehandleiding worden drie gebruikersaccounts en twee groepen aangemaakt.

Gebruikersaccounts:

- FTD Admin: Dit wordt gebruikt als de directory account om de FTD te kunnen binden aan de Active Directory-server.
- IT Admin: een account van een testbeheerder die wordt gebruikt om de identiteit van de gebruiker aan te tonen.
- Testgebruiker: een testgebruikersaccount dat wordt gebruikt om de identiteit van de gebruiker aan te tonen.

Groepen:

- AnyConnect Admins: een testgroep waaraan IT-beheerder wordt toegevoegd om de identiteit van de gebruiker aan te tonen. Deze groep heeft alleen RDP-toegang tot de Windows Server.
- AnyConnect-gebruikers: een testgroep die de testgebruiker toevoegt om de gebruikersidentiteit aan te tonen. Deze groep heeft alleen HTTP-toegang tot de Windowsserver.

Active Directory-configuraties

Om AD-verificatie en gebruikersidentiteit op FTD correct te kunnen configureren, zijn enkele waarden vereist.

Al deze gegevens moeten worden aangemaakt of verzameld op de Microsoft Server voordat de configuratie op FMC kan worden uitgevoerd. De belangrijkste waarden zijn:

• Domeinnaam:

Dit is de domeinnaam van de server. In deze configuratiehandleiding is example.com de domeinnaam.

• IP/FQDN-adres voor servers:

Het IP-adres of FQDN wordt gebruikt om de Microsoft-server te bereiken. Als een FQDN wordt gebruikt, moet een DNS-server worden geconfigureerd binnen FMC en FTD om de FQDN op te lossen.

In deze configuratiehandleiding is deze waarde win2016.example.com (die zich oplost in 192.168.1.1).

Serverpoort:

De poort die wordt gebruikt door de LDAP-service. Standaard gebruiken LDAP en STARTTLS TCP-poort 389 voor LDAP en gebruikt LDAP over SSL (LDAPS) TCP-poort 636.

• Root-CA:

Als LDAPS of STARTTLS wordt gebruikt, is de wortel CA die wordt gebruikt om het SSL certificaat te ondertekenen dat door LDAPS wordt gebruikt vereist.

Gebruikersnaam en wachtwoord map:

Dit is de account die door FMC en FTD wordt gebruikt om te binden aan de LDAP-server en gebruikers te verifiëren en te zoeken naar gebruikers en groepen.

Hiervoor wordt een account met de naam FTD Admin aangemaakt.

• Voornaam (DN) van basis- en groep:

De Base DN is het startpunt FMC en de FTD vertelt de Active Directory om te beginnen met het zoeken naar en authenticeren van gebruikers.

Op dezelfde manier is de Groep DN het uitgangspunt FMC vertelt de Active Directory waar te beginnen zoeken naar groepen voor gebruikersidentiteit.

In deze configuratiegids, wordt het worteldomein example.com gebruikt als Basis DN en Groep DN.

Voor een productieomgeving is het echter beter om een **Base DN** en **Group DN** verder binnen de LDAP-hiërarchie te gebruiken.

Deze LDAP-hiërarchie bijvoorbeeld:



Als een beheerder wil dat gebruikers binnen de organisatorische eenheid **Marketing** de basis-DN kunnen verifiëren kan worden ingesteld op de root (example.com).

Echter, dit maakt het ook mogelijk dat Gebruiker1 onder de **Finance** organisatieafdeling ook inlogt, aangezien het zoeken van de gebruiker begint bij de wortel en gaat naar **Finance, Marketing** en **Research**.

Base-DN ingesteld op example.com



Om logins te beperken tot de enige gebruiker in de **Marketing** organisatorische eenheid en hieronder, kan de beheerder in plaats daarvan de Base DN instellen op **Marketing**.

Alleen Gebruiker2 en Gebruiker3 kunnen nu authenticeren omdat de zoekactie begint bij **Marketing**.



Merk op dat voor meer granulaire controle binnen de FTD waarvoor gebruikers verschillende autorisaties kunnen verbinden of toewijzen op basis van hun AD-kenmerken, een LDAP-autorisatiekaart moet worden geconfigureerd.

Meer informatie hierover kunt u hier vinden: <u>AnyConnect LDAP-mapping configureren op</u> <u>Firepower Threat Defence (FTD)</u>.

Deze vereenvoudigde LDAP-hiërarchie wordt gebruikt in deze configuratiehandleiding en de DN voor de root example.com wordt gebruikt voor zowel de Base-DN als de Groep-DN.



Bepaal LDAP-basis DN en groep DN

1. Open Active Directory-gebruikers en -computers.

=	Best match					
ŵ	<i> Activ</i> Desk	ve Directo top app	ory User	s and C	Comput	ers
	Settings					>
	😣 Edit lo	cal users a	and gro	ups		
	陀 Chang	e User Ao	count C	ontrol	setting	s
	🍇 User A	ccounts				
	👱 Select	users who	o can us	se remo	te desi	ctop
۲	d	> 🗅			₿	切
	users					
-	o م	e	-	1	6	40

2. Klik met de linkermuisknop op **rootdomein** (om de container te openen), klik met de rechtermuisknop op het **rootdomein**, en klik vervolgens onder **Weergave**, op **Geavanceerde functies**.



3. Hierdoor kunnen extra eigenschappen worden weergegeven onder de AD-objecten. Bijvoorbeeld, om DN voor de wortel example.com te vinden, klik example.com met de rechtermuisknop en kies dan **Eigenschappen**.



4. Selecteer onder **Properties** het tabblad **Attribute Editor**. Vind **voornaamNaam** onder de **Kenmerken**, dan klik op **Weergeven**.

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

5. Hierdoor wordt een nieuw venster geopend waarin de DN kan worden gekopieerd en later in het VCC kan worden geplakt. In dit voorbeeld, de wortel DN is DC=example, DC=com.

Kopieert de waarde en slaat deze op voor later. Klik op **OK** om het venster **String Attribute Editor** te verlaten en klik nogmaals op OK om de **Properties** te verlaten.

			^		
rbute: distinguis	shedName				
lue:					
C=example,DC=com			_	Undo	
Clear	0	K Cano	el	Cut	
			_	Conv	
				Dasta	
				Paste	
				Delete	
				Select All	
				Right to left Reading order	r
				Show Unicode control cha	racters
				lacest Unice de control che	ractor
mple.com Properties		7	x		
eneral Managed By O	bject Security Attribute E	idtor			
eneral Managed By O	bject Security Attribute E	idtor			
eneral Managed By O Attributes:	bject Security Attribute E	iditor			
eneral Managed By O Attributes: Attribute	bject Security Attribute E	idtor ,	•		
eneral Managed By O Attributes: Attribute on controlAccessBrints	bject Security Attribute E Value <not set=""></not>	idtor ,	•		
eneral Managed By O Attributes: Attribute cn controlAccessRights creationTime	Value <not set=""> 4/29/2020 2:43:49 PM Ea</not>	idtor stem Davlight Tim	•		
eneral Managed By O Attributes: Attribute cn controlAccessRights creationTime dc	Value <not set=""> <not set=""> 4/29/2020 2:43:49 PM Ea example</not></not>	idtor stem Daylight Tim			
eneral Managed By O Attributes: Attribute cn controlAccessRights creationTime dc defaultLocalPolicyObj	bject Security Attribute E Value <not set=""> <not set=""> 4/29/2020 2:43:49 PM Ea example <not set=""></not></not></not>	iditor stem Daylight Tim			
eneral Managed By O Attributes: Attribute cn controlAccessRights creationTime dc defaultLocalPolicyObj description	bject Security Attribute E Value <not set=""> <not set=""> 4/29/2020 2:43:49 PM Ea example <not set=""> <not set=""></not></not></not></not>	idtor stem Daylight Tim			
eneral Managed By O Attributes: Attribute cn controlAccessRights creationTime dc defaultLocalPolicyObj description desktopProfile	Value <not set=""> <not set=""> </not> </not> 	iditor stem Daylight Tim			
eneral Managed By O Attributes: Attribute cn controlAccessRights creationTime dc defautLocalPolicyObj description desktopProfile displayName	Value <not set=""> <not set=""> </not> </not> 	idtor stem Daylight Tim			
eneral Managed By O Attributes: Attribute cn controlAccessRights creationTime dc defautLocalPolicyObj description desktopProfile displayName displayName	bject Security Attribute E Value <not set=""> <not set=""> 4/29/2020 2:43:49 PM Ea example <not set=""> <not set=""></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>	idtor stem Daylight Tim			
eneral Managed By O Attributes: Attribute cn controlAccessRights creationTime dc defautLocalPolicyObj description desktopProfile displayName displayName displayName	bject Security Attribute E Value <not set=""> <not set=""> 4/29/2020 2:43:49 PM Ea example <not set=""> <not set<="" td=""><td>idtor</td><td></td><td></td><td></td></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>	idtor			
eneral Managed By O Attributes: Attribute cn controlAccessRights creationTime dc defautLocalPolicyObj description desktopProfile displayName displayName displayName displayName displayName	Value <not set=""> <not set=""> <not set=""> </not> </not> <not set=""> <not set=""></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>	iditor stem Daylight Tim			
eneral Managed By O Attributes: Attribute cn controlAccessRights creationTime dc defaultLocalPolicyObj description desktopProfile displayName displayName displayName displayName displayName displayName displayName displayName displayName displayName displayName displayName displayName displayName displayName displayName displayName displayName	Value <pre>cnot set> <not set=""> <not set=""> 4/29/2020 2:43:49 PM Ea example <not set=""> <not set=""></not> <not set=""> <not set=""> <not set=""></not></not> <not set=""></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></pre>	iditor			
eneral Managed By O Attributes: Attribute cn controlAccessRights creationTime dc defautLocalPolicyObj description desktopProfile displayName displayName distinguishedName domainPolicyObject domainReplica dSASignature	Value (not set> (not set> 4/29/2020 2:43:49 PM Ea example (not set> (not set> (no	iditor stem Daylight Tim Secs = 0; DsaGuic			
eneral Managed By O Attributes: Attribute cn controlAccessRights creationTime dc defaultLocalPolicyObj description desktopProfile displayName displayName displayName distinguishedName domainPolicyObject domainPolicyObject domainPolica dSASignature dSCorePropagationD	Value (not set) (not set) 4/29/2020 2:43:49 PM Ea example (not set) (not set) (no	iditor stem Daylight Tim Secs = 0; DsaGuic			
eneral Managed By O Attributes: Attribute cn controlAccessRights creationTime dc defautLocalPolicyObj description desktopProfile displayName displa	bject Security Attribute E Value <not set=""> <not set=""> </not> </not> <not set=""> <not set<="" td=""><td>iditor stem Daylight Tim Secs = 0; DsaGuic ></td><td></td><td></td><td></td></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>	iditor stem Daylight Tim Secs = 0; DsaGuic >			
eneral Managed By O Attributes: Attribute cn controlAccessRights creationTime dc defaultLocalPolicyObj description desktopProfile displayName displ	bject Security Attribute E Value <not set=""> <not set=""> </not> <not set=""> <not set=""></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>	iditor stem Daylight Tim Secs = 0; DsaGuic > Fiter			

Dit kan worden gedaan voor meerdere objecten in **Active Directory**. Deze stappen worden bijvoorbeeld gebruikt om de DN van de **User**-container te vinden:

Active Directory Users and C	omputers	-	\times
File Action View Help			
🗢 🔿 🙍 🚾 🖌 🗈 👂	Users Properties ? ×		
 Active Directory Users and Q Saved Queries Saved Queries Saved Queries Builtin Computers Domain Controllers ForeignSecurityPrinc LostAndFound Hongram Data System Users NTDS Quotas TPM Devices 	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. De weergave **Geavanceerde functies** kan worden verwijderd door nogmaals op de hoofdletter DN te klikken en vervolgens onder **Beeld**, klik nogmaals op **Geavanceerde functies**.



Een FTD-account maken

Met deze gebruikersaccount kunnen FMC en FTD met de actieve directory binden om naar gebruikers en groepen te zoeken en gebruikers te verifiëren.

Het doel van het creëren van een afzonderlijke FTD-account is om onbevoegde toegang elders in het netwerk te voorkomen als de referenties die worden gebruikt voor de binding worden gecompromitteerd.

Deze account hoeft niet binnen het bereik van de Base DN of Group DN te vallen.

1. Klik in **Active Directory User and Computers** met de rechtermuisknop op de container/organisatie waaraan de FTD-account wordt toegevoegd.

In deze configuratie wordt de FTD-account toegevoegd onder de **User** container onder de gebruikersnaam <u>ftd.admin@example.com.</u>

Klik met de rechtermuisknop op Gebruikers en navigeer vervolgens naar Nieuw > Gebruiker.

Active Directory	Users and Comp	puters				-	×
File Action View	w Help						
🗢 🔿 🔁 📆	X 🗈 🗙 🛙	i 🧟 🗟 🛛	Þ	1 🗏 🐮 🛯	r 🗾 🔍		
Active Directory I Active Directory I Saved Queries Saved Queri	Users and Com s rs Controllers curityPrincipal: Service Accour Delegate Con Find	Name DefaultAcc Denied ROI DonsAdmins DonsUpdate Domain Ad Domain Co trol	o D s P i n	Type User Security Group Security Group Security Group Security Group Security Group Security Group	Description A user account manage. Members in this group of DNS Administrators Gro. DNS clients who are per. Designated administrato All workstations and ser. All domain controllers i All domain guests		^
	Find New All Tasks View Refresh Export List Reserved		ers	Computer Contact Group InetOrgPerson msDS-KeyCreder msDS-ResourceP msDS-ShadowPr			
< Creates a new item in	Help	WseAlertA WseAllow WseAllow		msImaging-PSP: MSMQ Queue Al Printer User Shared Folder	ias		~

2. Ga door het Nieuwe Voorwerp - de Tovenaar van de Gebruiker.

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

New Object - User		×
🤱 Create in: exam	nple.com/Users	
Password:	•••••	
Comm password: User must change passw User cannot change pass Password never expires Account is disabled	ord at next logon sword	
	< Back Next >	Cancel
New Object - User		×
New Object - User Create in: exam When you click Finish, the for	nple.com/Users	×
New Object - User Create in: exam When you click Finish, the for Full name: FTD Admin User logon name: ftd.admine	nple.com/Users Mowing object will be created: @example.com	×
New Object - User Create in: exan When you click Finish, the for Full name: FTD Admin User logon name: ftd.admin(The password never expires	nple.com/Users Mowing object will be created: @example.com	×

3. Controleer of de **FTD-account** is aangemaakt. Er worden twee extra accounts aangemaakt: **IT-beheerder** en **testgebruiker**.

Active Directory Users and Computers					×
🖾 🗟 📑 🖬	n 🙁 📚 în 🦷	7 🗾 🗽			
Name DefaultAcco DefaultAcco DefaultAcco Donain ROD Donain Ad Domain Ad Domain Co Domain Gue Domain Gue Domain Gue Domain Gue Comain Gue	Type User Security Group Security Group User	Description 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 Members of this group			~
Key Admins Key Admins RAS and IAS Read-only D Schema Ad Test User	Security Group Security Group Security Group Security Group Security Group User	Members of this group Members of this group Servers in this group can Members of this group Designated administrato			~
	Name DefaultAcco DefaultAcco DefaultAcco Denied ROD DonsUpdateP Donain Ad Domain Co Domain Co Domain Gue Domain Gue Domain Gue Domain Gue Domain Gue Domain Gue Domain Gue Domain Gue Comain Gue Domain Gue Reat-only D Read-only D Schema Ad Test User	Imputers Imputers	Imputers Imputers	Imputers — Imputers Imputers Imputers <td>Imputes — — Imputes Imputes Imputes Imputes Imputes Imputes Imputes Imputes Imputes Imputes Imputes Imputes Imputes Imputes Imputes</td>	Imputes — — Imputes Imputes Imputes Imputes Imputes Imputes Imputes Imputes Imputes Imputes Imputes Imputes Imputes Imputes Imputes

AD-groepen maken en gebruikers toevoegen aan AD-groepen (optioneel)

Hoewel dit niet nodig is voor verificatie, kunnen groepen worden gebruikt om het gemakkelijker te maken om toegangsbeleid toe te passen op meerdere gebruikers en LDAP-autorisatie.

In deze configuratiegids worden groepen gebruikt om later via gebruikersidentiteit binnen FMC instellingen voor toegangscontrole toe te passen.

1. Klik in **Active Directory User and Computers** met de rechtermuisknop op de container of de organisatorische eenheid waaraan de nieuwe groep wordt toegevoegd.

In dit voorbeeld wordt de groep AnyConnect Admins toegevoegd onder de container **Gebruikers**. Klik met de rechtermuisknop op **Gebruikers** en navigeer vervolgens naar **Nieuw > Groepen**.

Active Directory Users and Com	puters			-	×
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 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		^
New All Tasks View Refresh Export List Properties Help	> > Read-only Schema A Test User	Computer Contact Group InetOrgPerson msDS-KeyCreder msDS-ResourceP msDS-ShadowPr msImaging-PSPs MSMQ Queue Al Printer User	ntial PropertyList incipalContainer i		
Creates a new item in this container.	(m	Shared Folder			v

2. Ga door de Wizard Nieuw object - Groep.

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

3. Controleer of de groep is gemaakt. De AnyConnect-gebruikersgroep is ook gemaakt.

Active Directory Users and Com	_	×			
File Action View Help					
🗢 🔿 🖄 🚾 🤞 🔛 🗄	è 🛛 🖬 🐍 🔌 🛍 '	🔻 🗾 🙇			
Active Directory Users and Com Saved Queries Saved Queries Substrate Saved Queries Substrate	Name AnyConnect Admins AnyConnect Users Calo Cert Publishers Conceable Domain C DefaultAccount DefaultAccount DefaultAccount Donain RODC Passw DonsAdmins DosUpdateProxy Domain Admins Domain Computers Domain Computers Domain Controllers Domain Guests Domain Guests Domain Users 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 User	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 Designated administrato All workstations and ser All domain controllers i All domain guests All domain guests All domain guests Designated administrato Members of this group Members of this group Built-in account for gue		<
	108 x				

4. Klik met de rechtermuisknop op de groep van de gebruiker(s) en kies vervolgens

Eigenschappen. In deze configuratie wordt de IT-beheerder van de gebruiker toegevoegd aan de groep AnyConnect-beheerders en wordt de **testgebruiker** toegevoegd aan de groep **AnyConnect-gebruikers**.

Active Directory Users and Complexity	puters			-	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	Buil Move Mer Send Mail		
ForeignSecurityPrincipals Managed Service Account	Cloneable Domain C DefaultAccount	Security Group User	Mer All Tasks	>	
Users	Denied RODC Passw DnsAdmins DnsUpdateProxy Domain Admins Domain Computers	Security Group Security Group Security Group Security Group Security Group	Mer Cut DNS Delete DNS Rename Des Alla		
	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. Klik onder het tabblad Leden op Toevoegen.

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

Voer de gebruiker in het veld in en klik op **Namen controleren** om te controleren of de gebruiker gevonden is. Klik na de verificatie op **OK**.

Select Users, Contacts, Computers, Service Accounts, or G	õroups 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

Controleer of de juiste gebruiker is toegevoegd en klik op de knop OK. De gebruiker **Test User** wordt ook toegevoegd aan de groep **AnyConnect-gebruikers** met dezelfde stappen.

AnyConnect Admins Properties	?	×
General Members Member Of Managed By		
Members:		
Name Active Directory Domain Services Folder		
Add Remove		-
OK Cancel	Apply	/

Kopieert de SSL-certificaatroet van LDAPS (alleen vereist voor LDAPS of STARTTLS).

1. Druk op Win+R en voer mmc.exe in. klik vervolgens op OK.

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

2. Navigeer naar Bestand > Magnetisch toevoegen/verwijderen...

ᡖ Cor	nsole1 - [C	onsole f	Root]		-	×
🚡 File	Action	View	Favorites	Window	Help	. 8 ×
4	New			Ctrl+N		
	Open			Ctrl+O	Actions	
	Save Save Ar			Ctrl+S	There are no items to show in this view. Console Root	-
	Add/Rem	ove Sna	ip-in	Ctrl+M	More Actions	•
	Options					
	1 dnsmgr	mt				
	2 dsa					
	Exit					
Enables	you to add	snap-ir	is to or rem	ove them fro	om the snap-in console.	

3. Selecteer onder Beschikbare invoegtoepassingen de optie **Certificaten** en klik vervolgens op **Toevoegen**.

Available gnap-ins:	nis console from tr configure which e	xter	e available on your computer and configure the selected set of shap-ins. For ensions are enabled. Selected shap-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 Up	1
ADSI Edit	Microsoft Cor			
Authorization Manager	Microsoft Cor		Add >	
Certificate Templates	Microsoft Cor			
Certificates	Microsoft Cor			
Certification Authority	Microsoft Cor			
Component Services	Microsoft Cor			
Computer Managem	Microsoft Cor			
Device Manager	Microsoft Cor			
T Disk Management	Microsoft and	\checkmark	Advanced	
Description: The Certificates snap-in allo	ws you to browse	the	e contents of the certificate stores for yourself, a service, or a computer.	
			OK Cancel	

4. Selecteer Computer-account en klik op Volgende.

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

Klik op Finish (Voltooien).

Select Computer	×
Select the computer you want this snap-in to manage. This snap-in will always manage: Local computer: (the computer this console is running on) Another computer: Browse Another computer: Browse Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.	
< Back Finish Cancel	

5. Klik nu op **OK**.

Add or Remove Snap-ins							×
You can select snap-ins for t extensible snap-ins, you can	his console from the configure which e	nose xter	available on you nsions are enable	ur computer and cor ed.	nfigure the selected s	et of snap-ins. For	
Available snap-ins:				Selected snap-ins:			
Snap-in	Vendor	^		Console Root		Edit Extensions	
Active Directory Do	Microsoft Cor			Certificates	(Local Computer)	Domouo	
Active Directory Site	Microsoft Cor					Remove	
Active Directory Use	Microsoft Cor						
ActiveX Control	Microsoft Cor	-				Move <u>U</u> p	
ADSI Edit	Microsoft Cor					Move Down	
Authorization Manager	Microsoft Cor		<u>A</u> dd >			Hove Bown	-
Certificate Templates	Microsoft Cor		been The second				
Certificates	Microsoft Cor						
Certification Authority	Microsoft Cor						
Component Services	Microsoft Cor						
Computer Managem	Microsoft Cor						
Device Manager	Microsoft Cor						
T Disk Management	Microsoft and	\checkmark				Advanced	
•		-	1				
Description:							_
The Certificates snap-in allo	ws you to browse	the	contents of the	certificate stores fo	or yourself, a service,	, or a computer.	
					_		
						OK Cancel	

6. Vouw de **persoonlijke** map uit en klik vervolgens op **Certificaten**. Het door LDAPS gebruikte certificaat wordt afgegeven aan de **volledig gekwalificeerde domeinnaam (FQDN)** van de Windows-server. Op deze server staan 3 certificaten vermeld.

- Een CA-certificaat afgegeven aan en door voorbeeld-WIN2016-CA.
- Een identiteitsbewijs afgegeven aan WIN2016 door voorbeeld-WIN2016-CA.
- Een identiteitsbewijs afgegeven aan win2016.example.com door voorbeeld-WIN2016-CA.

In deze configuratiehandleiding is de FQDN win2016.example.com en dus zijn de eerste 2 certificaten niet geldig voor gebruik als het LDAPS SSL-certificaat. Het identiteitscertificaat dat wordt afgegeven aan win2016.example.com is een certificaat dat automatisch is afgegeven door de Windows Server CA-service. Dubbelklik op het certificaat om de gegevens te controleren.

🚡 Console1 - [Console Root\Certific	ates (Local Computer)\Personal\C	[ertificates]		-	o x
🚟 File Action View Favorites	Window Help				_ 8 ×
🗢 🏟 🖄 📆 📋 🙆 🞼					
Console Root Certificates (Local Computer) Certificates Certificates	Issued To Carample-WIN2016-CA	Issued By example-WIN2016-CA example-WIN2016-CA	Expiration Da 4/19/2060 4/27/2025	Actions Certificates More Actions	<u>م</u> ۲
Trusted Root Certification . Enterprise Trust Intermediate Certification . Trusted Publishers Untrusted Certificates Third-Party Root Certificat	Egi win2016.example.com	example-WIN2016-CA	4/28/2021		
Trusted People Client Authentication Issue Preview Build Roots E Local NonRemovable Cert Remote Desktop					
Certificate Enrollment Req Smart Card Trusted Roots Trusted Devices Web Hosting Windows Live ID Token Iss					
Personal store contains 3 certificates.	٢		>		

7. Om als SSL-certificaat van het LDAPS te worden gebruikt, moet het certificaat aan de volgende eisen voldoen:

- De veelvoorkomende naam voor **DNS-onderwerpalternatieve naam** komt overeen met de FQDN-naam van de Windows-server.
- Het certificaat heeft serververificatie in het veld Uitgebreid sleutelgebruik.

Onder het tabblad **Details** voor het certificaat, selecteert u **Onderwerp** en **Onderwerp Alternatieve Naam**, de FQDN win2016.example.com is aanwezig.

🙀 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	¢

🙀 Certil	ficate			×
General	Details	Certification Path		
Show:	<al></al>		~	
Field	bject Key thority Ke L Distribu thority In bject Alte y Usage umbprint a umborint Vame: Dbject Gu me=win2	Identifier y Identifier tion Points formation Access mative Name sigorithm d=04 10 90 99 a9 016.example.com	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= Digital Signature, Key Encipher sha1 ca 8e 11 3d eh b: 0f 6e 4a 00 a2 38 24 65 47 84 74 64 26 cd c6 8	~
		Ed	It Properties Copy to File	
			0	(

Onder Enhanced Key Usage is serververificatie aanwezig.

	X
General Details Certification Path	
Show: <all></all>	~
Field Value	^
Subject win2016. Public key RSA (204 Public key parameters 05 00	example.com 18 Bits)
Certificate Template Name DomainCo	ontroller
Client Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.1)	thentication (1.3.6.1 E Capability: Object I 4e 48 0f 2f 17 17 e6 d 9f 26 37 fb 11 1f 4
Edit Propertie	es Copy to File

8. Zodra dat is bevestigd, selecteert u onder het tabblad **Certificeringspad** het bovenste certificaat dat het basiscertificaat van de CA is en klikt u op **Certificaat bekijken**.

💼 Certificate	×
General Details Certification Path	
Certification path	
	View Certificate
Certificate status: This certificate is OK.	
	ОК

9. Hierdoor worden de certificaatgegevens voor het basiscertificaat van CA geopend.

R Certificate	×									
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										

Klik onder het tabblad Details op Kopiëren naar bestand...

Certificate		×
General Details Certification Path		
Show: <all></all>	~	
Field	Value	^
Version Serial number Signature algorithm Signature hash algorithm Issuer 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	
	OK	:

10. Ga door de wizard Certificaat exporteren en exporteer de root-CA in PEM-indeling.

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

Selecteer Base-64 encoded X.509

Expor	t File Format ertificates can be exported in a variety of file formats.
S	Sect the format you want to use:
	DER encoded binary X.509 (.CER)
	Base-64 encoded X-509 (-CEK) Cruntographic Message Suptay Standard - PKCS #7 Certificates (P7B)
	Indude all certificates in the certification path if possible
	O Personal Information Exchange - PKCS #12 (.PFX)
	Include all certificates in the certification path if possible
	Delete the private key if the export is successful
	Export all extended properties
	Enable certificate privacy
	Microsoft Serialized Certificate Store (.SST)

Selecteer de naam van het bestand en de locatie van de export.

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

		Х
÷	🚰 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 Cance	

Klik nu op Voltooien.

÷	Ş.	Certificate Export Wizard		×									
	Completing the Certificate Export 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. Ga nu naar de locatie en open het certificaat met een blocnote of een andere teksteditor. Dit is het certificaat in PEM-indeling. Bewaar dit voor later.

----BEGIN CERTIFICATE----

```
MIIDCDCCAfCgAwIBAgIQE4ZG5Z1wT6lONTjooEQyMTANBgkqhkiG9w0BAQsFADAd
MRswGQYDVQQDExjleGFtcGxlLVdJTjIwMTYtQ0EwIBcNMjAwNDI3MTQ1MDU5WhgP
MjA2MDA0MTkxNDUwNTlaMB0xGzAZBqNVBAMTEmV4YW1wbGUtV010MjAxNi1DQTCC
ASIwDQYJKoZIhvcNAQEBBQADqqEPADCCAQoCqqEBAI8qhT719NzSQpoQPh0YT67b
Ya+PngsxMyvkewP33QLTAWw1HW1Tb9Mk5BDWOItTaVsgHwPBfd++M+bLn3AiZnHV
OO+k6dVVY/E5qVkEKSGoY+v940S2316lzdwReMOFhgbc2qMertIoficrRhihonuU
Cjyeub3CO+meJUuKom2R47C0D35TUvo/FEHGgXJFaJS1se2UrpN07KEMkfAlLPuM
aob4XE/OzxYQpPa18djsNnskfcFqD/HOTFQN4+SrOhHWlRnUIQBUaLdQaabhipD/
sVs5PneYJX8YKma821uYI6j90YuytmsHBtCieyC062a8BKqOL7N86HFPFkMA3u8C
AwEAAaNCMEAwDgYDVR0PAQH/BAQDAgGGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR00
BBYEFD2fjjf7ER9EM/HCxCVFN5QzqEdvMA0GCSqGSIb3DQEBCwUAA4IBAQB31ZJo
vzwVD3c5Q1nrNP+6Mq62OFpYH91k4Ch9S5g/CEOemhcwg8MDIoxW2dTsjenAEt7r
phFIHZoCoSyjBjMgK3xybmoSeg8vBjCXseYNGEmOc9KW1oFmTOvdNVIb7Xpl1IVa
6tALTt3ANRNgREtxPA6yQbthKGavW0Anfsojk9IcDr2vp0MTjlBCxsTscbubRl+D
dLEFKQqmMeYvkVf+a7a64mqPZsG3Uxo0rd6cZxAPkq/ylcdwNSJFfQV3DqZq+R96
9WLCR3Obig6xyo9Zu+lixcWpdrbADO6zMhbEYEhkhOOjBrUEBBI6Cy83iTZ9ejsk
KgwBJXEu33PplW6E
----END CERTIFICATE-----
```

12. (facultatief) In het geval dat er meerdere identiteitscertificaten zijn die door LDAPS kunnen worden gebruikt en er onzekerheid is over welke certificaten worden gebruikt, of dat er geen toegang tot de LDAPS-server is, is het mogelijk om de wortelkaart te halen uit een pakketopname die op de Windows-server of FTD daarna is uitgevoerd.

FMC-configuraties

Licentie controleren

Om de AnyConnect-configuratie te kunnen implementeren, moet de FTD worden geregistreerd bij de slimme licentieserver en moet een geldige Plus-, Apex- of VPN-licentie alleen op het apparaat worden toegepast.

1. Ga naar Systeem > Licenties > Slimme licenties.



2. Controleer of de apparaten aan de voorschriften voldoen en met succes zijn geregistreerd. Zorg ervoor dat het apparaat is geregistreerd met een **AnyConnect Apex**-, **Plus-** of **VPN-licentie**.

Overview Analysis Policies	De	vices	Object	s AMP	Intelligence							Deploy 🔒	System	Help 🔻 ad	min 1
				Configuratio	on Users	Dom	ains I	ntegration	Upd	ates	Licenses + Smart Licen	Health	 Monit 	toring • 1	tools
Smart License Status						٩	isco Smart I	Software Ma	nager	• >					
Usage Authorization:	٥	Authoriz	red (Last	Synchronized	On Nay 03 2020))									
Product Registration:	0	Register	ed (Last	Renewed On M	4ar 03 2020)										
Assigned Virtual Account:		SEC TAC	:												
Export-Controlled Features:		Enabled													
Cisco Success Network:		Disabled	0												
Cisco Support Diagnostics:		Disabler	0												
Smart Licenses											Filter Devices		×	Edit Licens	es
License Type/Device Name						Licen	se Status		Device	Гуре		Domain	Gro	нир	
Firepower Management 0	Cent	er Virtu	ial (2)			0									
Þ 🟳 Base (2)						٥									
🖻 🟳 Malware (1)						٢									
D Gamma (2)						٥									
🖻 📁 URL Filtering (2)						٥									
🕫 📁 AnyConnect Apex (1)						٥									٦
FTD-2 192.168.1.17 · Cisco Firepo	wer 1	Threat De	fense for	VMWare - v6	3.0	0			Cisco Fin	epower	Threat Defense for VMWare	Global	N/A		
AnyConnect Plus (0)															
AnyConnect VPN Only (0)															
Note: Container Instances of same bla	ede s	hare feat	ure licens	es											_

Instellingsgebied

1. Ga naar **Systeem > Integratie**.

Overview	Analysis	Policies	Devices	Objects	AMP	Intelligence Deploy 🔒 S							System	Help 🔻	admin 🔻
						Configuration	Users	Domains	Integration	Updates	Licenses *	Health	 Mon 	itoring 🔻	Tools *

2. Klik onder Realms op Nieuw domein.

Overview Analysis Policie	s Devices Objects	AMP I	ntelligence					Deploy	🛛 🍳 Sys	tem Help v	admin 🔻
			Configuration	Users	Domains	Integration	Updates	Licenses v	Health v	Monitoring	Tools v
Cloud Services Realms	Identity Sources	eStreamer	Host Input Client	Smar	t Software S	atellite					
K Compare realms								New realm			
Name	Description	Domain	Туре		Base DN	Grou	p DN	Group Attri	bute	State	

3. Vul de juiste velden in op basis van de bij de Microsoft-server verzamelde informatie. Klik op **OK** als u klaar bent.

lame *	LAB-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	~	

4. Selecteer in het nieuwe venster **Directory** als dit nog niet is gekozen en klik op **Map toevoegen**.

Overview	Analysis	Policies	Devices	Objects	AMP	Intellige	ence			Deploy	🕘 🍳 Sys	tem Help 🔻	admin v
				Config	uration	Users	Domains	Integration	Updates	Licenses 🔻	Health v	Monitoring •	Tools •
LAB-AD Enter Descrip) tion											E Save	Cancel
Directory	Realm Cont	figuration	User Down	hoad									
												Q A	dd directory

Vul de gegevens van de AD-server in. Merk op dat als FQDN wordt gebruikt, FMC en FTD niet met succes kunnen binden tenzij DNS wordt gevormd om FQDN op te lossen.

Als u DNS voor FMC wilt instellen, navigeert u naar **System > Configuration** en selecteert u **Management Interfaces**.

Om DNS voor de FTD in te stellen, navigeer naar **Apparaten > Platform-instellingen**, maak een nieuw beleid, of bewerk een huidig beleid dan gaan naar DNS.

Add directory	? ×
Hostname / IP Address	win2016.example.com
Port	389
Encryption	○ STARTTLS ○ LDAPS ④ None
SSL Certificate	✓ ③
	OK Test Cancel

Als LDAPS of STARTTLS wordt gebruikt, klik op het Green +-symbool, geef het certificaat een naam en kopieer het PEM-formaat root CA-certificaat. Klik op **Opslaan** als u klaar bent.

Import Trusted Certificate Authority	? ×
Name: LDAPS_ROOT	
Certificate Data or, choose a file: Browse	
BEGIN CERTIFICATE MIIDCDCCAfCgAwIBAgIQE4ZG5Z1wT6lONTjooEQyMTANBgkqhkiG9w0BAQsFADAd MRswGQYDVQQDExJleGFtcGxlLVdJTjIwMTYtQ0EwIBcNMjAwNDI3MTQ1MDU5WhgP MjA2MDA0MTkxNDUwNTlaMB0xGzAZBgNVBAMTEmV4YW1wbGUtV0lOMjAxNi1DQTCC ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAI8ghT719NzSQpoQPh0YT67b Ya+PngsxMyvkewP33QLTAWw1HW1Tb9Mk5BDW0ItTaVsgHwPBfd++M+bLn3AiZnHV OO+k6dVVY/E5qVkEKSG0Y+v940S2316lzdwReMOFhgbc2qMertIoficrRhihonuU Cjyeub3CO+meJUuKom2R47C0D35TUvo/FEHGgXJFaJS1se2UrpNO7KEMkfA1LPuM aob4XE/OzxYQpPa18djsNnskfcFqD/HOTFQN4+SrOhHWIRnUIQBUaLdQaabhipD/ sVs5PneYJX8YKma821uYI6j90YuytmsHBtCieyC062a8BKqOL7N86HFPFkMA3u8C AwEAAaNCMEAwDgYDVR0PAQH/BAQDAgGGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0O BBYEFD2fJjf7ER9EM/HCxCVFN5QzqEdvMA0GCSqGSIb3DQEBCwUAA4IBAQB31ZJo vzwVD3c5Q1nrNP+6Mq62OFpYH91k4Ch9S5g/CEOemhcwg8MDIoxW2dTsjenAEt7r phFIHZoCoSyjBjMgK3xybmoSeg8vBjCXseYNGEmC9KW10FmTOvdNVIb7Xpl1IVa 6tALTt3ANRNgREtxPA6yQbthKGavW0Anfsojk91cDr2vp0MTjlBCxsTscbubRI+D dLEFKQqmMeYvkVf+a7a64mqPZsG3Uxo0rd6cZxAPkq/ylcdwNSJFfQV3DgZg+R96 9WLCR3Obig6xyo9Zu+lixcWpdrbADO6zMhbEYEhkhOOjBrUEBBI6Cy83iTZ9ejsk KgwBJXEu33PpIW6E	~
END CERTIFICATE	\sim
Encrypted, and the password is:	
Save	Cancel

Selecteer de nieuw toegevoegde root-CA uit de vervolgkeuzelijst naast SSL-certificaat en klik op STARTTLS of LDAPS.
Edit directory	? ×
Hostname / IP Address	win2016.example.com
Port	636
Encryption	○ STARTTLS
SSL Certificate	LDAPS_ROOT 💙 📀
	OK Test Cancel

Klik op Test om er zeker van te zijn dat FMC met succes kan binden met de Directory Gebruikersnaam en het wachtwoord dat in de vorige stap is opgegeven.

Omdat deze tests worden geïnitieerd vanuit het FMC en niet via een van de routeerbare interfaces die op de FTD zijn geconfigureerd (zoals binnenkant, buitenkant, dmz), garandeert een succesvolle (of mislukte) verbinding niet hetzelfde resultaat voor AnyConnect-verificatie omdat AnyConnect LDAP-verificatieaanvragen worden geïnitieerd vanuit een van de FTD routable interfaces.

Zie de secties Test AAA en Packet Capture in het gedeelte Problemen oplossen voor meer informatie over het testen van LDAP-verbindingen vanuit de FTD.

Status	
٩	Test connection succeeded
	OK

5. Download onder **Gebruikersdownload** de groepen die in latere stappen worden gebruikt voor gebruikersidentiteit.

Schakel het selectievakje **Gebruikers en groepen downloaden in** en de kolom **Beschikbare groepen** wordt gevuld met groepen die zijn geconfigureerd binnen Active Directory.

Groepen kunnen worden opgenomen of uitgesloten, maar standaard zijn alle groepen die onder de Groep DN worden gevonden, inbegrepen.

Ook specifieke gebruikers kunnen worden opgenomen of uitgesloten. Alle opgenomen groepen en gebruikers zijn beschikbaar om later te worden geselecteerd voor gebruikersidentiteit.

Als u klaar bent, klikt u op **Opslaan**.

Overview Analysis Policies Devices Objects AMP Intel	ligence			Deploy	🕘 🕘 Syste	m Help 🔻	admin 🔻
	Configuration Users	Domains Integration	Upd	ates Licenses •	Health *	Monitoring •	Tools 🔻
LAB-AD Enter Description				You have un	saved changes	🔚 Save	8 Cancel
Directory Realm Configuration User Download							
Download users and groups							
Begin automatic download at 8 V PM V America/New York Repeat Every	24 V Hours						
Available Groups 😋	Groups to Include (2)			Groups to Exclude (0)		
Search by name	🚔 AnyConnect Admins		- 8	None			
AnyConnect Admins	AnyConnect Users		8				
A 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							
A Domain Guests							
A Windows Authorization Access Group							
Account Operators							
🝰 Hyper-V Administrators 🗸 🗸	Patro Hara ta during			Colora Unio Custinalian			
👶 System Managed Accounts Group	Enter User Indusion		Add	Enter User Exclusion			Add

6. Schakel het nieuwe domein in.

Overview Analysis Polici	es Devices Objec	ts AMP I	ntelligence	:						Deploy	0, Sy	stem Hel	p v admin v
			Configur	ation U	lsers	Domains	Integra	tion	Updates	Licenses 🔻	Health *	Monitori	ng 🔻 🛛 Tools 🔻
Cloud Services Realms	Identity Sources	eStreamer	Host Inp	ut Client	Smar	rt Software !	iatellite						
											Comp	are realms	New realm
Name	Description	Domain		Туре	E	Jase DN		Group D	N	Group Attr	ibute	State	
LAB-AD		Global		AD	C	C=example,D0	-com	DC-exar	nple,DC=com	member			🕁 🥒 🛅 🖯

7. Indien LDAPS of STARTTLS wordt gebruikt, moet de oorspronkelijke CA ook door de FTD worden vertrouwd. Om dit te doen navigeer eerst naar **Apparaten > Certificaten**.

Overview Analysis	Policie	Dev	ices(Objects	AMP I	intelligence		Deploy	0	System	Help 🔻	admin 🔻
Device Management	NAT	VPN V	QoS	Platforn	n Settings	FlexConfig	Certificates					

Klik op Add in de rechterbovenhoek.

Overview Analysis	Polici	es Dev	ices	Objects AMP In	ntelligence		Deploy	0,	System	Help 🔻	admin 🔻
Device Management	NAT	VPN •	QoS	Platform Settings	FlexConfig	Certificates					
										0	A.4.4

Selecteer de FTD, de LDAP configuratie wordt toegevoegd om dan op het Groene + symbool te klikken.

Add New Certificate	e	? ×
Add a new certificate to identify certificate.	the 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

Geef het trustpoint een **Naam** en kies vervolgens **Handmatige** inschrijving uit de vervolgkeuzelijst **Inschrijftype**. Plakt hier het PEM root ca certificaat en klik vervolgens op **Opslaan**.

Add Cert Enrollmer	nt	? >
Name*	LDAPS_ROOT	
Description	\bigcirc	
CA Information	Certificate Parameters Key Revocation	
Enrollment Type:	Manual 💙	^
CA Certificate:*	 BEGIN 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/ sVs5PneYJX8YKma821uYI6j90YuytmsHBtCieyC062a8BKqOL7N86 	~
Allow Overrides		
	Save	Cancel

Controleer dat het gemaakte trustpoint is geselecteerd en klik vervolgens op Toevoegen.

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	~ ©
Cert Enrollment Details:		
Name:	LDAPS_ROOT	
Enrollment Type:	Manual	
SCEP URL:	NA	
		Add Cancel

Het nieuwe trustpoint verschijnt onder het FTD. Hoewel hierin wordt vermeld dat de invoer van een identiteitscertificaat is vereist, is het voor het FTD niet nodig het SSL-certificaat te kunnen verifiëren dat door de LDAPS-server is verzonden, zodat dit bericht kan worden genegeerd.

Overview Analysis	Policies Devices	Objects AMP Intel	ligence	Deploy 🍳 System	Help 🔻	admin 🔻
Device Management	NAT VPN VOS	Platform Settings	FlexConfig Certificates			
					0	Add
Name	Domain	Enrollment Type	Status			
4 🗐 FTD-1						
FTD-1-PKCS12	Global	PKCS12 file	🔍 CA 🔍 ID		£ 🗘	8
4 🗐 FTD-2						
FTD-2-PKCS12	Global	PKCS12 file	CA 🔍 D		¢ 2	6
FTD-2-Selfsigned	Global	Self-Signed	S CA 🔍 ID		î? ¢	6
LDAPS_ROOT	Global	Manual	🔍 CA 🔺 ID 🔺 Ide	ntity certificate import required	P 🗘	8

AnyConnect configureren voor AD-verificatie

1. Bij deze stappen wordt ervan uitgegaan dat er al geen VPN-beleid voor externe toegang is gemaakt. Als er een is gemaakt, klik dan op de bewerkingsknop voor dat beleid en ga naar stap 3.

Navigeer naar Apparaten > VPN > Externe toegang.

Ove	rview Analys	is Polic	cies	Device	s Obj	ects AMP Intel	ligence			Deploy	0	System	Help 🔻	admin 🔻
Dev	ice Managemer	t NA	т	VPN 🔻	QoS	Platform Settings	FlexConfig	Certificates						
				Site To S	ite									
			- 1	Remote /	Access									
			- 0	Troubles	hooting]								

Klik op Add om een nieuw VPN-beleid voor externe toegang te maken



2. Voltooi de **beleidswizard voor externe toegang tot VPN**. Specificeer onder **Beleidstoewijzing** een naam voor het beleid en de apparaten waarop het beleid wordt toegepast.

Overview Analysis Poli	licies Dev	vices Objects	AMP I	ntelligence				Deploy 🧕 Sys	tem Help 🔻 🕯	admin 🔻
Device Management NAT	r VPN ► I	Remote Access	QoS	Platform Settings	FlexConfig	Certificates				
Remote Access VPN	Policy W	/izard								
1 Policy Assignment	2 Cor	nnection Profile	> 3 /	AnyConnect > (Access &	Certificate >	S Summary			
Targe	eted Device	s and Protocols								~
This wiz a new u	izard will guide user-defined or	you through the requirements on profile.	uired minim	al steps to configure t	he Remote Access	VPN policy with	Before Yo	ou Start		
							Before you st configuration e	art, ensure the following lements to be in place to		
Name:*	* [PTD-2-RA-Policy					complete Remo	te Access VPN Policy.		
Descrip	ption:					0	Authenticatio	n Server		
VON Dec	L. E.	Zee - Elener				~	to authenticate	VPN dients.		
Trends	ad Daviessa A	u ssu insect	KEV2		Selected Device		AnyConnect C Nake sure you	lient Package		
Targete	ed Devices:	Q, Search		7	m PTD-2		for VPN Client the relevant Ci	downloaded or you have sco credentials to download		
	i i i	FTD-1		1			it during the wi	zard.		
		PTD-2					Device Interfa Interfaces show	ice Id he already configured on		
							targeted device as a security of	is so that they can be used		
							enable VPN acc	ess.		
				Add						
										Ň
								Back	ext Can	cel

Specificeer onder Verbindingsprofiel de naam van Verbindingsprofiel dat ook wordt gebruikt als de groepalias die AnyConnect-gebruikers zien wanneer ze verbinding maken.

Specificeer het domein dat eerder is gemaakt onder Verificatieserver.

Geef op hoe AnyConnect-clients IP-adressen krijgen toegewezen.

Specificeer het standaardgroepsbeleid dat voor dit verbindingsprofiel wordt gebruikt.

Overview Analysis Policies Devices Objects AMP	Intelligence		Deploy 🔒 S	System Help 🔻	admin v
Device Management NAT VPN + Remote Access QoS	Platform Settings FlexConfig Certifi	cates			
Remote Access VPN Policy Wizard					
1) Policy Assignment 2 Connection Profile 3	AnyConnect > ④ Access & Certific	ate > (5) Summary			
Connection Profile:					^
Connection Profiles specify the tunne accomplished and how addresses an	I group policies for a VPN connection. These policies assigned. They also include user attributes, which a	pertain to creating the tunnel itself, how re defined in group policies.	AAA is		
Connection Profile Name:*	General				
	This name is configured as a connection alias, it can be	used to connect to the VIN gateway			
Authentication, Authorization & A	ccounting (AAA):				
Specify the method of authentication	(AAA, certificates or both), and the AAA servers tha	t will be used for VPN connections.			
Authentication Nethod:	AAA Only 👻				
Authentication Server:*	LAB-AD 👻 🖓 🕻 (1.4	alm or RADJUS)			
Authorization Server:	V) 🖸 V	otus)			
Accounting Server:	✓ ③ (RA	DIUS)			
Client Address Assignment:					
Client IP address can be assigned for assignment is tried in the order of A	m AAA server, DHCP server and IP address pools. W A server, DHCP server and IP address pool.	hen multiple options are selected, 1P add	ress		
Use AAA Server (RADUUS	nly) 🕕				
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 clie	int when a VPN connection is established	. Select		
Group Policy:*	DfltGrpPolicy V				
	Edit Group Policy				~
			Back	Next	Cancel

Upload en specificeer onder AnyConnect de AnyConnect-pakketten die worden gebruikt.

Overview Analysis Policie	es Devices Objects AMP	Intelligence		Deploy 🔒 System	Help 🔻 admin 🔻
Device Management NAT	VPN + Remote Access QoS	Platform Settings FlexConfig Certifica	ites		
Remote Access VPN P	olicy Wizard				
(1) Policy Assignment $>$	2 Connection Profile 3	AnyConnect Access & Certifica	te 🔰 🗿 Summary		
	AnyConnect Client Image The VPN gateway can automatically down initiated. Ninimize connection setup time b	load the latest AnyConnect package to the client d y choosing the appropriate OS for the selected pack	evice when the VPN connection is age.		^
	Download AnyConnect Client packages from	Cisco Software Download Center.			
		S	how Re-order buttons		
	AnyConnect File Object Name	AnyConnect Client Package Name	Operating System		
	anyconnect-linux64-4.7.03052-we	anyconnect-linux64-4.7.03052-webdeploy-k9	Linux		
	anyconnect-win-4.7.00136-webde	anyconnect-win-4.7.00136-webdeploy-k9.pkg	Windows ¥		~
			(Back Next	Cancel

Specificeer onder **Access & Certificate** de interface waartoe AnyConnect-gebruikers toegang hebben voor AnyConnect.

Maak en/of specificeer het certificaat dat door de FTD wordt gebruikt tijdens de SSL-handdruk.

Zorg ervoor dat het aanvinkvakje voor **het beleid** voor **toegangscontrole** voor gedecrypteerd verkeer (sysopt license-vpn) niet is aangevinkt, zodat de gebruikersidentiteit die later wordt gemaakt, van kracht wordt voor RAVPN-verbindingen.

Overview Analysis Policies Devices Objects AMP Intell	gence	Deploy	🔒 System	Help 🔻	admin 🔻
Device Management NAT VPN • Remote Access QoS Platf	orm Settings FlexConfig Certificates				
Remote Access VPN Policy Wizard					
Policy Assignment O Connection Profile O AnyC	onnect 🔰 🕢 Access & Certificate 🔰 🕥 Summary 🔄				
Network Interface for Incom	ing VPN Access				
Select or create an Interface Group connections.	or a Security Zone that contains the network interfaces users will access for VPN				ŕ
Interface group/Security Zone:*	outside-zone 🗸 🖉				
	C Enable DTLS on member interfaces				- 1
Device Certificates					
Device certificate (also called Identit certificate which is used to authentic	y certificate) identifies the VPN gateway to the remote access clients. Select a ate the VPN gateway.				
Certificate Enrollment:*	FTD-2-Selfsigned Y				
	$\overrightarrow{\mathbf{M}}$ Enrol the selected certificate object on the target devices				
Access Control for VPN Traffi	C d is a biasted to the tasses fronted following default, fished this settion to				
bypass decrypted traffic from the Ac	is autjected to the Access Control Policy by default. Select this option to cess Control Policy.				
Bypass Access Control policy for This option bypasses the Access AAA server are atil applied to V79	decrypted traffic (sysopt permit-vpn) antrol Policy inspection, but VPN filter ACL and authorization ACL downloaded from traffic.				
		Back	Next		ancel

Bekijk onder Samenvatting de configuratie en klik op Voltooien.



3. Klik onder het VPN-beleid voor externe toegang op bewerken voor het juiste verbindingsprofiel.

Overview Analysis Policies Devices Objects	AMP Intelligence	Deploy 🧕 System Help 🔻 admin 🔻
Device Management NAT VPN > Remote Access	QoS Platform Settings FlexConfig Certificates	
FTD-2-RA-Policy Enter Description		Save Cancel
Connection Profile Access Interfaces Advanced		Policy Assignments (1)
		0
Name	AAA Group Policy	
DefaultWEBVPNGroup	Authentication: None Et Oft,GrpPolicy Authorization: None Accounting: None	/ 0
General	Authentication: LAB-AD (AD) PL Dft:GrpPolicy Authorization: Intern Accounting: Across	2 3

Zorg ervoor dat de verificatieserver is ingesteld op het domein dat eerder is gemaakt.

Onder **Advanced Settings** kan **Wachtwoordbeheer** worden ingeschakeld om gebruikers in staat te stellen hun wachtwoord te wijzigen wanneer of voordat hun wachtwoord verloopt.

Deze instelling vereist echter dat het gebied LDAPS gebruikt. Als er wijzigingen zijn aangebracht, klikt u op **Opslaan**.

Edit Connection Pr	ofile	1	? ×
Connection Profile:* Group Policy:* Client Address Assign	General DfltGrpPolic Edit Group Po	sy v v v olicy Aliases	
Authentication			
Authentication Meth	od:	AAA Only	
Authentication Serv	er:	LAB-AD (AD)	
Use secondary a Authorization Authorization Serve	uthentication r:	Allow connection only if user exists in authorization database	
Accounting			
Accounting Server:		▼	
Advanced Settin	gs		
Strip Realm from	username		
Strip Group from Enable Password	Management	+	
Notify User Notify user on the second seco	days price	or to password expiration word expiration	
		Save Cancel	

Klik rechtsboven op Opslaan.



Identiteitsbeleid inschakelen en Beveiligingsbeleid voor gebruikersidentiteit configureren

1. Ga naar Beleid > Toegangsbeheer > Identiteit.



Een nieuw identiteitsbeleid maken.

Overview Analysis Policies Devices Object	ts AMP Intelligence		Deploy	🔒 System Help ▼ admin ▼
Access Control > Identity Network Discovery	Application Detectors Corr	relation Actions •		
			(Object Management Access Control
Identity Policy	Domain		Status	Last Modified
		There are no policies cre	eated. Add a new policy	

Specificeer een naam voor het nieuwe identiteitsbeleid.

2. Klik op Regel toevoegen.



3. Geef een **naam op** voor de nieuwe regel. Zorg ervoor dat deze is ingeschakeld en dat de actie is ingesteld op Passieve verificatie.

Klik op het tabblad **Realm & Settings** en selecteer het gebied dat eerder is gemaakt. Klik op **Toevoegen** als u klaar bent.

Add Rule

Name RAVPN			🖌 Enabled	d Insert	into Category	*	Standard Rules	~
Action Passive Authen	tication	*	Realm: LAB-AD (AD)	Authentication Protocol:	HTTP Basic Exclude	HTTP User	Agents: None	
Remote access V	PN sessions are a	ectively authentica	ted by VPN. Other session	s use the rule Action.				
Zones Networks	VLAN Tags	Ports					Realm & S	ettings
Realm *	LAB-AD (A	D)						
Use active authenti	ation if passive o	r VPN identity can	not be established					
 Required Field 								
							Add C	ancel

4. Klik op Opslaan.

Overview Analysis Poli	icies Device	s Objects	AMP Intelli	gence				De	ploy 🧛 System	Help 🔻 ad	min •
Access Control > Identity	Network Disc	overy Appl	cation Detectors	Correlation	Actions *						
FTD-2 Identity Policy You have unsaved changes 🔚 Save 🕲 Cancel											
Rules Active Authentication											
							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 Protocol	
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 i - i of i rules $|\langle \langle Page | i \rangle$ of i $\rangle > |$ C

5. Ga naar **Beleid > Toegangsbeheer > Toegangsbeheer**.

Overview Analysis Policies Devices Object	s AMP Intelligence		(Deploy 🧳	System	Help 🔻	admin 🔻
Access Control > Identity Network Discovery /	Application Detectors Corre	rrelation Actions •					
Access Control							
Intrusion							
Malware & File							
DNS							
Identity							
SSL							
Prefilter							

6. Bewerk het **Toegangscontrolebeleid** waarop de FTD is geconfigureerd.

Overview Analysis Policies	Devices Objects	AMP Intelligence				Deploy	🔒 System	Help 🔻	admin v
Access Control > Access Control	Network Discovery	Application Detectors	Correlation	Actions •					
					Object Management 1	ntrusion Network	Analysis Policy	DNS Imp	ort/Export
								O New	Policy
Access Control Policy		Status			Last Modified				
Default-Policy		Targeting 1 Up-to-date o	devices in all targeted device	es	2020-05-04 09:15:56 Modified by "admin"			G 🛛	2 8

7. Klik op de waarde naast Identiteitsbeleid.



Selecteer het eerder gemaakte identiteitsbeleid en klik op OK.

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

8. Klik op **Regel toevoegen** om een nieuwe ACS-regel te maken. Met deze stappen wordt een regel gemaakt op grond waarvan gebruikers in de AnyConnect Admins-groep met RDP verbinding kunnen maken met apparaten binnen het netwerk.

Overview Analysis Policies Devices Object	ts AMP Intelligence	Deploy 🧕 System Help 🔻 admin 🔻
Access Control + Access Control Network Discove	ery Application Detectors Correlation Actions •	
Default-Policy Enter Description		You have unsaved changes 🛛 Analyze Hit Counts 🛛 🔚 Save 🛛 🔞 Cancel
Prefilter Policy: Default Prefilter Policy	SSL Policy: None	Identity Policy: FTD-2 Identity Policy
		🏣 Inheritance Settings 📉 Policy Assignments (1)
Rules Security Intelligence HTTP Responses La	ogging Advanced	
曲 Fiber by Device	Show Rule Conflicts 🥹	🔾 Add Category 🔹 Add Rule 🚔 Search Rules 🗙
a Name Sourc Dest Z Sourc	Dest N.,, VLAN.,, Users Applic.,, Sourc.,, Dest P.,	URLs Sourc Dest S Action 🙂 🐚 🛵 🌚 💷 👳
🖝 Mandatory - Default-Policy (-)		
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 -

Geef een naam op voor de regel. Zorg ervoor dat de regel is ingeschakeld en de juiste actie onderneemt.

Specificeer onder het tabblad **Zones** de juiste zones voor het interessante verkeer.

RDP-verkeer dat door gebruikers wordt geïnitieerd, komt in de FTD-bron vanuit de interface van de buitenzone en verlaat de binnenzone.

Add Rule											? X
Name AC RDP Access					inabled	Insert	into Manda	tory	-		
Action 🖌 Allow			v 0 D 8	8 4 5							
Zones Networks	VLAN Tags	Users	Applications	Ports	URLs	SGT/ISE Attributes			Inspection	Logging	Comments
Available Zones 🗳				Sour	ce Zones	(1)		Destinati	on Zones (1)		
🔍 side		×		÷.	outside-zo	ne	6	🚠 inside	-zone		6
슈 inside-zone 슈 outside-zone			Add to Source Add to Destination								
										Add	Cancel

Definieer onder Netwerken de bron- en doelnetwerken.

Object AnyConnect_Pool bevat de IP-adressen die zijn toegewezen aan AnyConnect-clients.

Voorwerp Inside Net omvat het binnenste netwerksubnetnet.

Add Ru	le												
Name	AC RDP Access				V Er	nabled		Insert	into Manda	tory			~
Action	Allow			V 0 D /8	t []								
Zone	s Networks VLA	AN Tags U	Jsers	Applications	Ports	URLs	SGT/ISE	Attributes			Inspection	Logging	Comments
Availabl	e Networks 🖸		0		Sourc	e Netwo	rks (1)			Destinati	on Networks	(1)	
🔍 Sear	ch by name or value					Source		Original (lient	📰 Inside	_Net		6
	Networks	Geolocation			A	nyConned	_Pool		6				
Inside Section 2014	de_Net I-Benchmark-Tests 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-IPv4-Mapped		^ ~	Add To Source Networks Add to Destination	Enter	r an IP ado	fress		Add	Enter an	IP address		Add
												Add	Cancel

Klik onder Gebruikers op het gebied dat eerder is gemaakt onder Beschikbare interfaces, klik op de juiste groep/gebruiker onder Beschikbare gebruikers en klik vervolgens op Toevoegen aan regel.

Als er onder de sectie Beschikbare gebruikers geen gebruikers of groepen beschikbaar zijn, zorg er dan voor dat het VCC in staat is om de gebruikers en groepen onder de sectie Gebiedsdelen te downloaden en dat de juiste groepen/gebruikers worden opgenomen.

De hier gespecificeerde gebruikers/groepen worden vanuit bronperspectief gecontroleerd.

Met wat tot nu toe in deze regel is gedefinieerd, evalueert de FTD bijvoorbeeld dat het verkeer afkomstig is van de buitenzone en bestemd is voor de binnenzone, afkomstig is van het netwerk in het AnyConnect_Pools-object en bestemd is voor het netwerk in het Inside_Net-object, en dat het

verkeer afkomstig is van een gebruiker in de AnyConnect Admins-groep.

Add Ri	ile											? ×
Name	AC RDP Access			E E	nabled	I	insert	into Mandato	ory `	•		
Action	Allow		💌 🔍 🔍 💌	805								
Zone	s Networks VLAN Tags	Users	Applications	Ports	URLs	SGT/ISE Attrib	utes			Inspection	Logging	Comments
Availab	le Realms 🖸		Available Users	c					Selected	Users (1)		
🔍 Sea	rch by name or value		🔍 Search by n	ame or va	lue				💰 LAB-	AD/AnyConnect	t Admins	
📑 Spe	cial Identities		IAB-AD/*						_			
🜐 LAB	i-AD		AnyConnect	Admins								
			AnyConnect	Users								
			ait.admin 🚨				A	dd to Rule				
			a test.user									
											add	Cancel
											Add	Cancel

Onder Ports zijn aangepaste RDP-objecten gemaakt en toegevoegd om TCP- en UDP-poort 3389 toe te staan. Merk op dat RDP onder de sectie **Toepassingen** had kunnen worden toegevoegd maar voor eenvoud worden alleen de poorten gecontroleerd.

Name AC RDP Access Action Allow Zones Networks VLAN Tags Users Applications Available Ports URLs SGT/ISE Attributes Inspection Available AoL AoL Add to Source DNS_over_TCP DNS_over_UDP Add to Source Add to Source Add to Source PMC-HTTPS Add to Destination PRC-SSH FTD-3-FDM FTD-3-SSH FTP Protocol Protocol TCP (6) Pot Enter Add	Add Ru	le												? ×
Action Allow Zones Networks VLAN Tags Users Applications Ports URLs SGT/ISE Attributes Available Ports C Selected Destination Ports (2) Action Ac	Name	AC RDP Access				V E	nabled	1	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) AOL AOL PRD-TCP PRD-UDP Add to Source Add to Source Add to PMC-HTTPS Add to PTD-3-SFDM Add to PTD-3-SFM Protocol TDP-TD Protocol TCP (6) Port Enter a	Action	Allow			V 0 D.	8115								
Available Ports Selected Source Ports (0) Selected Destination Ports (2)	Zone	s Networks	VLAN Tags	Users	Applications	Ports	URLs	SGT/ISE Attrib	outes		1	Inspection	Logging	Comments
AOL AOL AOL Bittorrent CDNS_over_TCP CDNS_over_UDP FMC-HTTPS FTD-3-FDM FTD-3-FDM FTD-3-SSH FTD-3-SSH FTD-3-SSH FTD-3-FDM FTD-3-FDM FTD-3-SSH	Availabl	e Ports 🖒		0		Selec	ted Sour	rce Ports (0)		Se	ected D	estination I	Ports (2)	
	AOL AOL AOL AOL AOL AOL AOL AOL	ch by name or va prrent i_over_TCP i_over_UDP -HTTPS -SSH -3-FDM -3-SSH	lue	^	Add to Source Add to Destination	Protor				Add Pro	PRDP-UC	ερ (6)	V Port	Enter a Add

Ten slotte wordt onder **Logging**, **Log at End of Connection** later gecontroleerd voor extra verificatie. Klik op **Toevoegen** als u klaar bent.

Add Rule

Name	AC RDP Access					Enabled	Insert	into Mandatory	*			
Action	Allow			• • • •	3 🖄 🗾							
Zone	s Networks	VLAN Tags	Users	Applications	Ports	URLs	SGT/ISE Attributes		Inspe	ction	Logging	Comments
Log File Ever Log Send Co Send Co	at Beginning of Co at End of Connecti hts: Files nnection Events to ht Viewer og Server (Using d	nnection on : :	nfiguratio	n in Access Contro	of Logging) Show O	verrides					
SNM	Select an 1	SNMP Alert Con	figuration.	**		v	G					
											Add	Cancel

9. Er wordt een extra regel voor HTTP-toegang gecreëerd om gebruikers binnen de groep **AnyConnect-gebruikers** toegang tot de website van **Windows Server IIS** te geven. Klik op **Save** (Opslaan).

Overview Analysis Policies Devices Obje	ects AMP Intelligence	Deploy 0, System Help 🔻	admin v
Access Control > Access Control Network Disc	very Application Detectors Correlation Actions •		
Default-Policy Enter Description		You have unserved changes Analyze Hit Counts	8 Cancel
Prefilter Policy: Default Prefilter Policy	SSL Policy: None	Identity Policy: <u>FTD-2 Identity Policy</u>	
		Ta Inheritance Settings 🖳 Policy Assi	prmenta (1)
Rules Security Intelligence HTTP Responses	Logging Advanced		
B Filter by Device	Show Rule Co	mflicta 👪 🔾 Add Category 🔾 Add Rule 📫 Search Rules	×
a Name Source Zo Dest Zones	Source Networks Dest Netwo V. Users	A., S., Dest Ports U., S., D., Action	. °
 Mandatory - Default-Policy (1-2) 			
1 AC RDP Access	anyConnect_Pool as Inside_Net Arc & LAB-AD/AnyConnect Admins	Any Any 🏂 RDP-TCP Any Any Any Any Villow 🗍 🕞 🚖 🗐	/ 6
2 AC HTTP Access do outside-zone do inside-zone	😹 AnyConnect_Pool 🛛 😹 Inside_Net 🖉 🗛 🖨 LAB-AD/AnyConnect Users	Any Any PHTTP - Any Any Any VAllow 🛈 🗅 🗷 🖄 🗾	/ 8
▼ Default - Default-Policy (-)			
There are no rules in this section. Add Rule or Add Category			
Default Action		Access Control: Block All Traffic	× 🔳

Displaying 1 - 2 of 2 rules $|\langle \langle | Page | 1 | of 1 \rangle \rangle | | C | Rules per page: 100 *$

NAT-vrijstelling configureren

Als er NAT-regels zijn die invloed hebben op AnyConnect-verkeer, zoals Internet PAT-regels, is het belangrijk om NAT-vrijstellingsregels te configureren zodat AnyConnect-verkeer niet NATbeïnvloed is.

1. Navigeer naar **apparaten > NAT**.

Overview Analy	ysis	Policies	Device	25	Objects AMP	Inte	elligence		Deploy	e,	System	Help 🔻	admin v
Device Managemen	nt	NAT	VPN *	QoS	Platform Setting	gs	FlexConfig	Certificates					

Selecteer het NAT-beleid dat op de FTD wordt toegepast.

? X

Overview Analysis I	Policies Devices Objects	AMP Intelligence		Deploy	🔒 System	Help 🔻 admin 🔻
Device Management	AT VPN VOS Platf	orm Settings FlexConfig	Certificates			
						New Policy
NAT Policy		Device Type		Status		
FTD-2-NAT-Policy		Threat Defense		Targeting 1 devices Up-to-date on all targeted devices		th B 🖉 8

2. In dit NAT-beleid is er een Dynamisch PAT aan het einde dat PAT-invloed heeft op al het verkeer (inclusief AnyConnect-verkeer) dat de buiteninterface naar de buiteninterface perst.

Klik rechtsboven op **Regel toevoegen** om te voorkomen dat het AnyConnect-verkeer NATbeïnvloed wordt.

Oven	view /	malysis	Policies	Device	objects	AMP	Intelligen	ce			0	Deploy 0	System	Help 🔻	admin 🔻
Devio	e Manage	ment	NAT	PN *	QoS Platfo	rm Settin	gs FlexC	onfig Cer	tificates						
FTD Enter D	-2-N/	AT-Poli	icy								(🔔 Show Warn	ings 📔	Save	😫 Cancel
Rules													E	Policy A	ssignments (1)
db filter	by Device													0	Add Rule
							Origi	nal Packet			Translated Pack	et	۱		
# Dir	ection	Туре	Source Interfac	e Obje I	estination nterface Object	Original Sources	Or	riginal estinations	Orig Services	Translated Sources	Translated Destinations	Trans. Service	. Option	\$	
▼ NAT	Rules Bef	re													
▼ Auto	NAT Rule	5													
÷ +		Dynamic	🥞 any	4	outside-zone	💂 obj-a	ny			4 Interface			🧠 Dns	false	N
▼ NAT	Rules Afte	r													
									Diselavine	1-1 of 1 rows	IC C Page 1	(1 > >	L C L R		age: 100 ×

3. Configureer een NAT-vrijstellingsregel en zorg ervoor dat de regel een handmatige NAT-regel is met Type Statisch. Dit is een bidirectionele NAT-regel die van toepassing is op AnyConnect-verkeer.

Met deze instellingen, wanneer de FTD verkeer detecteert afkomstig van Inside_Net en bestemd voor AnyConnect IP-adres (gedefinieerd door AnyConnect_Pool), wordt de bron vertaald naar dezelfde waarde (Inside_Net) en wordt de bestemming vertaald naar dezelfde waarde (AnyConnect_Pool) wanneer het verkeer binnendringt in de inside_zone en de buitenkant_zone betreedt. Dit passeert NAT in essentie wanneer aan deze voorwaarden wordt voldaan.

Add NAT Rule					? ×
NAT Rule:	Manual NAT Rul	e 🔻	Insert:	In Category	▼ NAT Rules Before ▼
Type:	Static	- I V	Enable		
Description:					
beschption					~
Interface Objects	Translation	PAT Pool A	dvanced		
Available Interface Ol	bjects C		Source Inter	face Objects (1)	Destination Interface Objects (1)
a zone		×	📸 inside-zor	ne 🗒	🚠 outside-zone 🧻
inside-zone		Add to			
outside-zone		Sourc			
		Add to			
		(
					OK Cancel
Add NAT Rule					? >
NAT Rule:	Manual NAT Ru	le 👻	Insert:	In Category	✓ NAT Rules Before ✓
Type:	Static	~ .	Enable		
Description			2113010		
Description:					\sim
Interface Objects	Translation	PAT Pool Ad	vanced		
Original Packet				Translated Packet	
Original Source:*	Inside Ne	ŧ	V ()	Translated Source:	Address
	and a contract				
Original Destination:	Address	-			Inside_Net
Original Destination:	Address	rt Paol	×	Translated Destinations	Inside_Net
Original Destination:	Address AnyConne	ct_Pool	× •	Translated Destination:	Inside_Net Y @ AnyConnect_Pool Y @
Original Destination: Original Source Port:	Address	ct_Pool	 ✓ ✓	Translated Destination: Translated Source Port:	Inside_Net AnyConnect_Pool
Original Destination: Original Source Port: Original Destination P	Address AnyConne	ct_Pool		Translated Destination: Translated Source Port: Translated Destination Port:	Inside_Net AnyConnect_Pool
Original Destination: Original Source Port: Original Destination Po	Address AnyConne	ct_Pool	 <	Translated Destination: Translated Source Port: Translated Destination Port:	Inside_Net AnyConnect_Pool
Original Destination: Original Source Port: Original Destination Po	Address AnyConne	ct_Pool	V	Translated Destination: Translated Source Port: Translated Destination Port:	Inside_Net Y © AnyConnect_Pool Y © Y ©

Daarnaast is de FTD ingesteld om een routerraadpleging uit te voeren op dit verkeer en niet op proxy-ARP. Klik op **OK** als u klaar bent.

Add NAT Rule					? X
NAT Rule:	Manual NAT Rule	▼ Insert:	In Category	▼ NAT Rules Before ▼	
Type:	Static	▼ Enable			
Description:					0
Interface Objects	Translation PAT	Pool Advanced			
Translate DNS repli	es that match this rule				
Fallthrough to Inter	face PAT(Destination Ir	iterface)			
IPv6					
Net to Net Mapping					
🗹 Do not proxy ARP o	n Destination Interface				
Perform Route Look	up for Destination Inte	rface			
Unidirectional					
				ОК	Cancel

4. Klik op Opslaan.

(Overview A	nalysis	Policies Devi	ices Objects	AMP In	ntelligence			Deplo	y 🔍 ;	System Help	▼ admin ▼
(Device Manager	ment	NAT VPN *	QoS Platfor	m Settings	FlexConfig Certif	cates					
F	TD-2-NA	T-Poli	су					You have u	nsaved changes [🚵 Sh	ow Warning	is 🔡 Save	Cancel
R	tules										E Policy	Assignments (1)
æ	Filter by Device										0	Add Rule
						Original Packet			Translated Packet			
*	Direction	Туре	Source Interface Obje	Destination Interface Object	Original Sources	Original Destinations	Orig Services	Translated Sources	Translated Destinations	Trans Services	Options	
٠	NAT Rules Befor	re										
1	47	Static	🐴 inside-zone	🚠 outside-zone	👼 Inside_)	Net 🚔 AnyConnect_Po	ol	📻 Inside_Net	🚃 AnyConnect_Pool		🍓 Dris:false 🍓 route-looku 🍓 no-proxy-a	2 🗐 19
۳	Auto NAT Rules											
=	+	Dynamic	🍓 any	🚠 outside-zone	📄 obj-any	(🍓 Interface			🍓 Dns:false	/ 6
٠	NAT Rules After											
							Displaying	1-2 of 2 rows	< < Page 1 of 1	> >	C Rows per	page: 100 •

Implementeren

1. Wanneer de configuratie is voltooid, klikt u op de knop **Implementeren** rechtsboven.



2. Klik op het selectievakje naast de FTD als de configuratie erop wordt toegepast en klik vervolgens op **Implementeren**.

Dep	oy Policies Version:2020-05-04 09:40 AM					×
V	Device	Inspect Interruption	Туре	Group	Current Version	۲
▼ ±	FTD-2	No	FTD		2020-05-04 09:16 AM	

```
Selected devices: 1
```

Deploy Cancel

Verifiëren

Laatste configuratie

AAA-configuratie

```
> 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
```

Configuratie 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

Verbinding maken met AnyConnect en toegangscontroleregels controleren

🚳 Cisco AnyCo	nnect Secure Mobil	ity Client	_	□ ×	
	VPN: Contacting ftd2.exan ftd2.example.com	nple.com.	~ C(onnect	
	🕤 Ciso	co AnyConne	ect ftd2.exa	mple.com	×
¢ (i)					
		Group:	General		\sim
		Username:	it.admin		
		Password:	*******		
				OK	Cancel
🚳 Cisco AnyCo	nnect Secure Mobil	ity Client	Ξ	□ ×	
	VPN: Connected to ftd2.ex ftd2.example.com	ample.com.	VDise	connect	
00:00:12				IPv4	
Ö (i)					

De gebruiker IT Admin bevindt zich in de groep AnyConnect Admins die RDP-toegang heeft tot de Windows-server, maar heeft geen toegang tot HTTP.

Door een RDP- en Firefox-sessie te openen voor deze server wordt geverifieerd dat deze gebruiker alleen toegang heeft tot de server via RDP.



Indien ingelogd met gebruiker Test Gebruiker die in de groep AnyConnect Gebruikers die als HTTP-toegang maar niet RDP-toegang is, kunnen we verifiëren dat de regels van het toegangscontrolebeleid van kracht worden.

💀 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	 Remote access to the server is not enabled The remote computer is turned off The remote computer is not available on the network Make sure the remote computer is turned on and connected to the network, and that remote access is enabled.
Show Optio Connect Help	OK Help
IIS Windows Server 🗙 🔆 Options	× + – – ×
← → C ^a û 🛛 🖉 win2016.example.com	
🕂 Windows Server	
Internet Information Serv	vices
Welcome Rienvenue Terretul	
Herverue Terveru	

Verifiëren met FMC Connection-gebeurtenissen

Aangezien vastlegging is ingeschakeld in de regels voor toegangsbeleid, kunnen de gebeurtenissen van de verbinding worden gecontroleerd op elk verkeer dat aan die regels voldoet

Navigeer naar Analyse > Verbindingen > Gebeurtenissen.

Overview Analys	sis Policies D	Devices Objec	ts AMP	Intellige	ence		Deploy 05	System Help 🔻	admin 🔻
Context Explorer	Connections v	Intrusions 🔻	Files 🔻	Hosts v	Users v	Correlation v	Advanced 🔻	Search	
	Events								
	Security Intellig	ence Events							

Onder de **Tabelweergave van Verbindingsgebeurtenissen** worden de logs gefilterd om alleen verbindingsgebeurtenissen voor IT-beheerder weer te geven.

Hier kunt u controleren of RDP-verkeer naar de server (TCP en UDP 389) is toegestaan, maar poort 80 wordt geblokkeerd.

C	vervie	w Analy	sis Policies	Devices	Objects	AMP 1	Intelligence			Deplo	y 🔍	System	Help 🔻	admin 🔻
C	ontext	Explorer	Connections + I	Events	Intrusions	 Files 	s 🔻 Hosts 💌 🛛	Isers V Corre	elation •	Advanced 🔻	Search			
								Bookman	k This Page - R	Report Designer	Dashboard	d View Bo	okmarks	Search •
¢	Conn	ection E	vents (switch	workflow)						II. 2020	05.05.14-	14-17 - 24		14-11-140
<u>c</u>	onnectio	ns with Applic	ation Details > Tab	le View of	Connection	Events				1 2020	-03-05 14:	14:17 - 20	<u>20-05-05</u> E	Expanding
•	Search	Constraints (E	dit Search Save Se	arch)									Disab	led Columns
1	Jump t	o 🔻												
	Jump t	Action ×	Initiator × IP	Initiator	<u>r User</u> ×		Responder × IP	Ingress Security Zone	× Egres Secur	s × ity Zone	Source Po ICMP Type	ent/×	Destinat ICMP Co	tion Port / ×
	Jump t	Action ×	Initiator × IP 10.10.10.1	Initiator	<u>r User</u> × nin (LAB-AD\it	admin, LDA	Responder × IP 192.168.1.1	Ingress Security Zone	Eqres Secur inside-	s × ity Zone	Source Po ICMP Type 62473 / top	e <u>nt /</u> × e	Destinat ICMP Co 3389 / to	tion Port / × de 2
	Jump t	Action ×	Initiator × IP 10.10.10.1 10.10.10.1	Initiator it adm	<mark>r User</mark> × nin (LAB-AD\it nin (LAB-AD\it	admin, LD/	Responder × IP AP) III 192.168.1.1 AP) III.102	Ingress Security Zone outside-zone	× Egress Secur inside	s × ity Zone zone zone	Source Po ICMP Type 62473 / tep 62474 / tep	e <u>e</u> 2	Destinat ICMP Co 3389 / to 80 (http)	t <u>ion Port /</u> × a <u>de</u> 2 / tsp
	Jump t	Action × Allow Block Block	Initiator × IP 10.10.10.1 10.10.10.1 10.10.10.1	Initiator I it adm	r.User × nin (LAB-AD\it nin (LAB-AD\it nin (LAB-AD\it	.admin, LD/ .admin, LD/ .admin, LD/	Responder × IP IP IP IP IP IP2.168.1.1 AP1 IP2.168.1.1 AP1 IP2.168.1.1	Ingress Security Zone outside-zone outside-zone outside-zone	× Eares Secur inside inside	s X ity Zone Zone Zone	Source Po ICMP Typ 62473 / tcp 62474 / tcp 62475 / tcp	ent / × e 2 2	Destinat ICMP Co 3389 / to 80 (http) 80 (http)	tion Port / × ede 2 / tcp / tcp

Voor gebruiker **Test Gebruiker**, kunt u verifiëren dat RDP-verkeer naar de server is geblokkeerd en poort 80-verkeer is toegestaan.

(Over	view	Analysi	s Policies I	Devices	Objects	AMP Ir	ntelligence				Deplo	y 🔍	System	Help 🔻	admin 🔻
	Conte	xt Exp	olorer C	onnections • I	Events	Intrusions 🔻	Files	 Hosts * 	Users v	Correlati	on 🔻	Advanced •	Search			
										Bookmark Th	is Page	Report Designer	Dashboard	View Bo	okmarks	Search •
	Connec Connec Sear	nec tions (ch Cor p to	tion Ev with Applicat astraints (Edi	Vents (switch ion Details > Tab t Search Save Sea	workflow) de View of arch)	Connection E	vents					II 2020	-05-05 14:)	14:17 - 20	20-05-05 E Disab	<u>16:26:39</u> ∂ Expanding (ed Columns
			Action ×	Initiator × IP	Initiato	r User ×		Responder IP	× Inc Sec	ress > urity Zone	Eq Se	ress × curity Zone	Source P ICMP Typ	ort/×	Destina ICMP C	ation Port / > Code
	4		Block	10.10.10.1	📑 <u>test u</u>	ser (LAB-AD\te	st.user, LDA	(P) i 192.168	1.1 outs	ide-zone	insi	ide-zone	<u>62493 / to</u>	P	3389 / t	52
	4		Allow	10.10.10.1	📇 test u	ser (LAB-AD\te	st.user, LD/	P) 192.168	1.1 outs	ide-zone	insi	ide-zone	62494 / to	p	80 (http) / tcp

Problemen oplossen

Debugs

Deze debug kan worden uitgevoerd in diagnostische CLI om problemen met LDAP-verificatie op te lossen: **debug Idap 255**

Om problemen op te lossen met het toegangsbeleid van de gebruikersidentiteit, kan de **systeemondersteuning firewall-engine-debug** in clish worden uitgevoerd om te bepalen waarom verkeer onverwacht wordt toegestaan of geblokkeerd.

LDAP-debugs werken

```
[53] Session Start
[53] New request Session, context 0x00002bld13f4bbf0, 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....{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
```

Kan geen verbinding maken met LDAP-server

```
[-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
```

Mogelijke oplossingen:

- Controleer de routing en controleer of de FTD een respons ontvangt van de LDAP-server.
- Als LDAPS of STARTTLS wordt gebruikt, zorg ervoor dat het juiste wortel CA certificaat wordt vertrouwd op zodat de SSL handdruk met succes kan voltooien.
- Controleer of het juiste IP-adres en de juiste poort worden gebruikt. Als een hostname wordt gebruikt, controleer of DNS in staat is om het op te lossen naar het juiste IP-adres.

Binding Login DN en/of wachtwoord niet correct

```
[-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
```

Potentiële oplossing: controleer of het aanmeldingswachtwoord en het inlogwachtwoord correct zijn ingesteld. Dit kan worden geverifieerd op de AD-server met **Idp.exe**. Ga als volgt te werk om te controleren of een account met succes bindt met behulp van Idp:

1. Druk op de AD-server op Win+R en zoek naar 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. Kies onder Verbinding Connect...

🔛 Ldp					-		\times
Connection Browse	View C	Options	Utilities	Help			
Bind Disconnect	Ctrl+B						
New Save Save As	Ctrl+N						
Exit							
						NUM	

3. Specificeer localhost voor server en de juiste poort en klik vervolgens op OK.

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

4. De rechterkolom toont tekst die een succesvolle verbinding aangeeft. Navigeren naar **verbinding > binden...**

🔝 Idap://w	vin2016.exa	ample.co	om/DC:	= example, DC	=com		—		×
Connection	Browse	View	Optio	ns Utilities	Help				
Connee Bind Discon New Save Save As Exit	ct nect	Ctrl+B		Id = Idap_op Established Retrieving b Getting 1 en Dn: (RootD configu CN= current Tim defaultM dnsHos domainf dsServi Set Firs Nan con forestFi highest isGlobal isSynch	en ("localho connection ase DSA in tries: SE) rationNamin =Con figurati Time: 5/1/20 e; VamingConte thame: win ControllerFu Functionality iceName: CP tings,CN=W st-Site- me,CN=Sites n; unctionality: CommittedU ICatalogRea pronized: TF viceName: (1)	st", 389); to localhost. formation gContext: ion,DC=examp 20 4:16:55 PM ext: DC=exam 2016.example inctionality: 7 = /: 7 = (WIN201 N=NTDS IN2016,CN=Se s,CN=Configur SN: 13410; ady: TRUE; RUE; example.com	le,DC=c I Easter ple,DC=c .com; = (WIN2 I6); ervers,C ation,DC 6); win2016	com; n Daylight com; 016); N=Default- C=example,D)C=
									-1

5. Selecteer **Simple Bind** en specificeer vervolgens de **Directory Account Gebruikersnaam** en **Wachtwoord**. Klik op **OK**.

Bind	×						
<u>U</u> ser: Password:	ftd.admin@example.com						
<u>D</u> omain:							
Bind type Bind as <u>c</u> u Bind with c <u>Simple bind</u> <u>A</u> dvanced	rrently logged on user redentials (DIGEST) affic after bind						
Ad <u>v</u> anced	Cancel OK						

Met een succesvolle bind, ldp toont Authenticated als: DOMAIN\username

🔐 Idap://w	in2016.exa	mple.co	om/DC=ex	ample,DC	=com		—		×	
Connection	Browse	View	Options	Utilities	Help					
				1.2. 1.2. 1.2. supporte Max Max Max Max Max Max Max Max	840.11355 840.11355 840.11355 edLDAPPol PercentDir ReceiveBu Connection BatchRetu DirSyncDu ResultSets ResultSets ValRange; edLDAPVe edSASLMe IEGO; EXTR imple_bind i>); // v.3 ed as: 'EXA	6.1.4.2255; 6.1.4.2256; 6.1.4.2309; licies (20): M SyncReques Iffer; InitRec ns; MaxConr rnMessages Iration; MaxT Size; MinRes PerConr; Max MaxValRan /Limit; System rsion (2): 3; echanisms (4 ERNAL; DIGE	axPoolThr sts; MaxDa vTimeout; hldleTime; I s; MaxQue empTable ultSets; axNotificat geTransiti mMemoryL 2; !): GSSAPI :ST-MD5; Imin@exar min'.	eads; atagramR MaxPage! ryDuratio Size; tionPerCo ve; .imitPerce l; GSS- mple.com	ecv; Size; n; nn; ent;	~
Ready										:

Een poging een bind met een ongeldige gebruikersnaam of wachtwoord resulteert in een mislukking zoals de twee die hier worden gezien.

Idap://win2016.example.com/DC=example,DC=com — 🗌								×	
Connection	Browse	View	Options	Utilities	Help				
			r A E S C E	Max Max Max Three supporte supporte SPN es = Idap_s unavailable cuthenticate es = Idap_s unavailable rror <49>: I server error comment: Ac irror 0x8009 tvalid	ResultSets ResultSets ValRange; eadMemory edLDAPVer edSASLMed EGO; EXTE imple_bind_ e>); // v.3 ed as: 'EXAl imple_bind_ e>); // v.3 dap_simple cceptSecur 90308 The f	ize; MinRes PerConn; Ma MaxValRan Limit; Syster sion (2): 3; chanisms (4 RNAL; DIGE _s(Id, 'ftd.ad MPLE\ftd.ad _s(Id, 'wron _bind_s() fa : LdapErr: D ityContext e token suppli	ultSets; axNotificat geTransitiv mMemoryL 2; 4): GSSAPI SST-MD5; 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5	ionPerConn /e; imitPercent; ; GSS- nple.com', le.com', d Credentia 042A, 52e, v3839 unction is	ls
Ready]						*

LDAP-server kan de gebruikersnaam niet vinden

```
[-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
```

Potentiële oplossing: Controleer dat AD de gebruiker kan vinden met de zoekactie uitgevoerd door de FTD. Dit kan ook met **Idp.exe** worden gedaan.

1. Nadat u met succes de bovenstaande binding hebt uitgevoerd, navigeert u naar Beeld > Boom.

Idap://win2016.example.com/DC=example,DC=com										×	
Connection	Browse	View	/ Option	s Utilities	Help						
			Tree			Ctrl+T					^
			Enterprise	/a	/axPoolThreads;						
		~	Status Ba	r	sı v	s, maxu Timeout;	atagramik	ecv,			
			Set Font				nk s;	dleTime; MaxQue	MaxPage ryDuratio	Size; in;	
MaxDirSyncDu MaxResultSets MaxResultSets MaxValRange; ThreadMemory supportedLDAPVe supportedSASLMe SPNEGO; EXT						Duration; M etSize; MinF etsPerConn ge; MaxValF oryLimit; Sy Version (2): Mechanism (TERNAL; D	ation; MaxTempTableSize; ze; MinResultSets; erConn; MaxNotificationPerConn; laxValRangeTransitive; imit; SystemMemoryLimitPercent; sion (2): 3; 2; hanisms (4): GSSAPI; GSS- NAL; DIGEST-MD5;				
res = ldap_simple_bind_s(ld, 'ftd.admin@example.com', <unavailable>); // v.3 Authenticated as: 'EXAMPLE\ftd.admin'.</unavailable>							r,				
				I							۷

2. Specificeer de Base-DN die op de FTD is geconfigureerd en klik op $\mathbf{O}\mathbf{K}$

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

3. Klik met de rechtermuisknop op de Base-DN en klik vervolgens op Zoeken.

🔝 Idap://win2	2016.exa	- 🗆 X					
Connection E	Browse	View	Options	Utilities	Help		
<mark>DC=exampl</mark>	le,DC=c	m	Search Virtual L Delete Modify Modify Add chil Compar Advance Copy DN Copy Select al Clear ou	ist View DN d e ed N	Ctrl+S Ctrl+D Ctrl+M Ctrl+R Ctrl+A > Ctrl+C Ctrl+C	cipals,DC=example,DC=com; 11D2B9AA00C04F79F805:CN =example,DC=com; 11D297C400C04FD8D5CD:C =example,DC=com; 11D1ADED00C04FD8D5CD:C =example,DC=com; 11D1ADED00C04FD8D5CD:C ple,DC=com; 11D1AA4B00C04FD7D83A:O 3,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 do	cument		1				

4. Specificeer dezelfde Base DB-, Filter- en Scope-waarden als in de debugs.

In dit voorbeeld zijn dit:

- Dc=voorbeeld, dc=com
- Filter: samaccountname=it.admi
- Toepassingsgebied:SUBTREE

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

ldp vindt 0 items te wijten aan er is geen gebruikersaccount met de naam **it.admi** onder de Base DN dc=example,dc=com

Een andere poging met de juiste samaccountnaam **it.admin** toont een ander resultaat. Idp vindt 1 ingang onder de Base DN dc=example, dc=com en drukt die gebruiker DN.

🔐 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 N=U exar top;	min", attrList, 0, &msg) Isers,DC=example,DC=com mple.com/Users/IT Admin; person; organizationalPerson;	
Ready							

Onjuist wachtwoord voor de gebruikersnaam

```
[-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
```

Potentiële oplossing: controleer of het gebruikerswachtwoord correct is geconfigureerd en of het niet is verlopen. Net als bij de Login DN doet de FTD een bind tegen AD met de gebruikersreferenties.

Dit bind kan ook worden gedaan in ldp om te verifiëren dat de AD in staat is om dezelfde gebruikersnaam en wachtwoordreferenties te herkennen. De stappen in ldp worden weergegeven in de sectie **Binding Login DN en/of onjuist wachtwoord**.

Daarnaast kunnen de Microsoft server **Event Viewer** logbestanden worden bekeken om een mogelijke reden.

AAA testen

De test **aaa-server** opdracht kan worden gebruikt om een verificatiepoging van de FTD met een specifieke gebruikersnaam en wachtwoord te simuleren. Hiermee kan worden getest op verbinding- of verificatiefouten. Dit commando is **test aaa-server verificatie [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
```

PacketCapture

Packet-opnamen kunnen worden gebruikt om de bereikbaarheid naar de AD-server te verifiëren. Als LDAP-pakketten de FTD verlaten, maar er is geen respons, kan dit wijzen op een routeringsprobleem.

Capture toont het tweerichtingsverkeer LDAP.

```
> show route 192.168.1.1
Routing entry for 192.168.1.0 255.255.255.0
Known via "connected", distance 0, metric 0 (connected, via interface)
Routing Descriptor Blocks:
```

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

Logbestanden van Windows Server Event Viewer

De **Event Viewer** logt in op de AD-server en kan gedetailleerdere informatie geven over de oorzaak van een fout.

1. Zoek naar en open Event Viewer.

=	Best match									
ŵ	Event Viewer Desktop app									
	Settings	;					>			
	🖄 Vie	ever	nt logs							
۲	10	٢	ß		E3	□	រុក			
	event									
-	Q	(_)	e		2	2	8			

2. Windows-logbestanden uitvouwen en op Beveiliging klikken. Zoek naar auditfouten met de naam van de gebruikersaccount en bekijk de foutinformatie.


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

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.