# Konfigurieren der AD-Authentifizierung (LDAP) und Benutzeridentität auf von FMC verwalteten FTD für AnyConnect-Clients

## Inhalt

Einleitung Voraussetzungen Anforderungen Verwendete Komponenten Hintergrundinformationen Konfigurieren Netzwerkdiagramm und -szenario Active Directory-Konfigurationen Ermitteln der LDAP-Basis-DN und Gruppen-DN **FTD-Konto erstellen** AD-Gruppen erstellen und AD-Gruppen Benutzer hinzufügen (optional) Kopieren Sie die LDAPS SSL-Zertifikatwurzel (nur für LDAPS oder STARTTLS erforderlich). **FMC-Konfigurationen** Lizenzierung überprüfen Setup-Bereich Konfigurieren von AnyConnect für die AD-Authentifizierung Identitätsrichtlinie aktivieren und Sicherheitsrichtlinien für Benutzeridentität konfigurieren NAT-Ausnahme konfigurieren **Bereitstellen** Überprüfung Abschließende Konfiguration **AAA-Konfiguration** AnyConnect-Konfiguration AnyConnect verwenden und Richtlinien für die Zugriffskontrolle überprüfen Mit FMC-Verbindungsereignissen überprüfen Fehlerbehebung Fehlerbehebung LDAP-Debugger Verbindung zum LDAP-Server kann nicht hergestellt werden Ungültiger Bindungs-Anmelde-DN und/oder falsches Kennwort LDAP-Server konnte den Benutzernamen nicht finden Falsches Kennwort für den Benutzernamen AAA testen Paketerfassung Windows Server-Ereignisanzeige - Protokolle

## Einleitung

In diesem Dokument wird beschrieben, wie die AD-Authentifizierung für AnyConnect-Clients konfiguriert wird, die eine Verbindung mit Cisco Firepower Threat Defense (FTD) herstellen.

## Voraussetzungen

#### Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Grundkenntnisse der RA VPN-Konfiguration auf FMC
- Grundkenntnisse der LDAP-Serverkonfiguration auf FMC
- Grundkenntnisse von Active Directory (AD)

#### Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Microsoft Server 2016
- FMCv mit 6.5.0
- FTDv mit 6.5.0

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

#### Hintergrundinformationen

In diesem Dokument wird beschrieben, wie Sie die Active Directory (AD)-Authentifizierung für AnyConnect-Clients konfigurieren, die eine Verbindung zu Cisco FirePOWER Threat Defense (FTD) herstellen, das vom FirePOWER Management Center (FMC) verwaltet wird.

Die Benutzeridentität wird in den Zugriffsrichtlinien verwendet, um AnyConnect-Benutzer auf bestimmte IP-Adressen und Ports zu beschränken.

### Konfigurieren

#### Netzwerkdiagramm und -szenario



inside



outside



Windows Server

AnyConnect Client

Der Windows-Server ist mit IIS und RDP vorkonfiguriert, um die Benutzeridentität zu testen. In diesem Konfigurationsleitfaden werden drei Benutzerkonten und zwei Gruppen erstellt.

Benutzerkonten:

- FTD-Administrator: Dieser Parameter wird als Verzeichniskonto verwendet, damit die FTD an den Active Directory-Server gebunden werden kann.
- IT-Administrator: Ein Test-Administratorkonto, mit dem die Benutzeridentität veranschaulicht wird.
- Test User (Testbenutzer): Ein Testbenutzerkonto, mit dem die Benutzeridentität demonstriert wird.

Gruppen:

- AnyConnect Admins: Eine hinzugefügte Testgruppe für IT-Administratoren, die die Benutzeridentität veranschaulicht. Diese Gruppe hat nur RDP-Zugriff auf den Windows Server.
- AnyConnect-Benutzer: Eine Testgruppe, die Test User (Testbenutzer) hinzugefügt wird, um die Benutzeridentität zu veranschaulichen. Diese Gruppe hat nur HTTP-Zugriff auf den Windows Server.

#### Active Directory-Konfigurationen

Um die AD-Authentifizierung und die Benutzeridentität auf FTD ordnungsgemäß zu konfigurieren, sind einige Werte erforderlich.

Alle diese Details müssen auf dem Microsoft-Server erstellt oder erfasst werden, bevor die Konfiguration auf dem FMC durchgeführt werden kann. Die wichtigsten Werte sind:

#### • Domänenname:

Dies ist der Domänenname des Servers. In diesem Konfigurationsleitfaden ist example.com der Domänenname.

#### Server-IP/FQDN-Adresse:

Die IP-Adresse oder der FQDN für die Verbindung zum Microsoft-Server. Wenn ein FQDN verwendet wird, muss ein DNS-Server innerhalb von FMC und FTD konfiguriert werden, um den FQDN aufzulösen.

In diesem Konfigurationsleitfaden lautet der Wert win2016.example.com (wird zu 192.168.1.1 aufgelöst).

#### • Server-Port:

Der vom LDAP-Dienst verwendete Port. Standardmäßig verwenden LDAP und STARTTLS den TCP-Port 389 für LDAP und LDAP über SSL (LDAPS) den TCP-Port 636.

#### Stammzertifizierungsstelle:

Wenn LDAPS oder STARTTLS verwendet wird, ist die Stammzertifizierungsstelle zum Signieren des von LDAPS verwendeten SSL-Zertifikats erforderlich.

#### • Verzeichnisbenutzername und -kennwort:

Dieses Konto wird von FMC und FTD verwendet, um eine Bindung zum LDAP-Server herzustellen, Benutzer zu authentifizieren und nach Benutzern und Gruppen zu suchen.

Zu diesem Zweck wird ein Konto mit dem Namen FTD Admin erstellt.

#### • Distinguished Name (DN) für Basis und Gruppe:

Die Basis-DN ist der Startpunkt für FMC, und die FTD weist das Active Directory an, mit der Suche und Authentifizierung von Benutzern zu beginnen.

Ebenso ist die Gruppen-DN der Ausgangspunkt, an dem FMC dem Active Directory mitteilt, wo nach Gruppen nach Benutzeridentitäten gesucht werden soll.

In diesem Konfigurationsleitfaden wird die Root-Domäne example.com als Basis-DN und Gruppen-DN verwendet.

Für eine Produktionsumgebung ist es jedoch besser, weiter innerhalb der LDAP-Hierarchie einen **Basis-DN** und einen **Gruppen-DN** zu verwenden.

Beispiel für diese LDAP-Hierarchie:



Wenn ein Administrator möchte, dass Benutzer innerhalb der **Marketing-**Organisationseinheit die Basis-DN authentifizieren können, kann dies auf den Root (example.com) festgelegt werden.

Dies ermöglicht es User1 unter der Organisationseinheit **Finanzen** jedoch auch, sich anzumelden, da die Benutzersuche am Stamm beginnt und zu **Finanzen, Marketing** und **Forschung** führt.

Basis-DN eingestellt auf example.com



Um Anmeldungen auf den einzigen Benutzer in der Organisationseinheit **Marketing** und darunter zu beschränken, kann der Administrator stattdessen die Basis-DN auf **Marketing** festlegen.

Jetzt können nur noch User2 und User3 authentifiziert werden, da die Suche bei Marketing

beginnt.

Basis-DN auf "Marketing" gesetzt



Beachten Sie, dass für eine detailliertere Kontrolle innerhalb des FTD, für die Benutzer eine Verbindung herstellen oder Benutzern basierend auf ihren AD-Attributen unterschiedliche Autorisierungen zuweisen dürfen, eine LDAP-Autorisierungszuordnung konfiguriert werden muss.

Weitere Informationen hierzu finden Sie hier: <u>Konfigurieren Sie AnyConnect LDAP-Zuordnung auf</u> <u>Firepower Threat Defense (FTD)</u>.

Diese vereinfachte LDAP-Hierarchie wird in diesem Konfigurationsleitfaden verwendet, und der DN für den Stamm example.com wird sowohl für den Basis-DN als auch für den Gruppen-DN verwendet.



Ermitteln der LDAP-Basis-DN und Gruppen-DN

1. Öffnen Sie Active Directory-Benutzer und -Computer.

=	Best match
ŵ	Active Directory Users and Computers Desktop app
	Settings >
	8 Edit local users and groups
	🚩 Change User Account Control settings
	User Accounts
	Select users who can use remote desktop
۲	
	users
-	ዶ 🗅 렪 🛢 👗 📕

2. Klicken Sie mit der linken Maustaste auf die **Stammdomäne** (um den Container zu öffnen), klicken Sie mit der rechten Maustaste auf die **Stammdomäne**, und klicken Sie dann unter **Ansicht** auf **Erweiterte Funktionen**.



3. Dies ermöglicht die Anzeige zusätzlicher Eigenschaften unter den AD-Objekten. Um beispielsweise den DN für den Stamm example.com zu finden, klicken Sie mit der rechten Maustaste auf example.com, und wählen Sie dann **Eigenschaften aus**.

Active Directory Users and Computers	-	D X			
File Action View Help	File Action View Help				
💠 🔿 📶 🟥 🖾 🧔 📓 🖬 📷 🗏 🐮 🗑 🦉 🚨 🎘					
Active Directory Users and Com Saved Queries Saved Queries Saved Queries Saved Queries Saved Queries Saved Queries Saved Queries Saved Queries Saved Queries Saved Queries Delegate Control Delegate Control Default cont Default cont New Sum Default cont New Default cont Default cont Default cont Default cont Default cont Default cont Default cont Default cont Default cont Sum Default cont Sum Default cont Default cont Default cont Default cont Default cont Default cont Sum Default cont Sum Default cont Sum Default cont Default cont Default cont Sum Default cont Su	ainer for up ainer for do ainer for sec ainer for or ainer for ma tion for stor m settings ainer for up fications co				
or a provide content selection.					

4. Wählen Sie unter **Eigenschaften** die Registerkarte **Attributeditor**. Suchen Sie unter den **Attributen** den **DistinguishedName**, und klicken Sie dann auf **Anzeigen**.

example.	com Propertie	5				?	х
General	Managed By	Object	Security	Attribut	te Editor		
Attribute	88:						_
Attribu	ite	Value	e				^
dc		exam	nple				
defau	tLocalPolicyOb	j knot	set>				
descri	lption	knot	set>				
deskt	opProfile	knot	set>				
displa	yName	knot	set>				
displa	vNamePrintable	< knot	set>	-			
disting	guishedName	DC-	example_D	C=com			
domai	inPolicyObject	Knot	set>				
domai	inReplica	<not< td=""><th>set&gt;</th><td></td><td></td><td></td><td></td></not<>	set>				
dSAS	ignature	{ V1:	: Flags = 0	0; Later	ncySecs =	: 0; DsaGuio	
dSCo	rePropagationD	0x0 :	=()				
eFSP	olicy	<not< td=""><th>set&gt;</th><td></td><td></td><td></td><td></td></not<>	set>				
exten	sionName	<not< td=""><th>set&gt;</th><td></td><td></td><td></td><td></td></not<>	set>				
flags		<not< td=""><th>set&gt;</th><td></td><td></td><td></td><td>~</td></not<>	set>				~
<						>	
W	ew					Fiter	
	OK		Cancel		Apply	Hel	p

5. Dadurch wird ein neues Fenster geöffnet, in das die DN kopiert und später in FMC eingefügt werden kann. In diesem Beispiel ist die Stamm-DN DC=example,DC=com.

Kopieren Sie den Wert, und speichern Sie ihn für später. Klicken Sie auf **OK**, um das Fenster **Zeichenfolgenattribut-Editor** zu schließen, und klicken Sie erneut auf OK, um die **Eigenschaften** zu beenden.

tribute: distingu	ishedName	
lue:		
C=example,DC=com		Undo
Clear	OK Cancel	Cut
		Conv
		Dasta
		Delete
		Delete
		Select All
		Right to left Reading order
		Show Unicode control characters
		legent lipice de centrel characters
		insert onicode control character
ample.com Properties	ŕ X	
Seneral Managed By (	hiert Security Attribute Editor	
concrete interlayed by t	Sport Scouldy Financial	
Attributes:		
Attribute	Value ^	
cn	<not set=""></not>	
controlAccessRights	<not set=""></not>	
creation Time	4/29/2020 2:43:49 PM Eastern Daylight Tim	
de la companya de la	example	
defaultLocalPolicyObj	<not set=""></not>	
description	(not set)	
desktopProfile	(not set)	
displayNamePrintable	(not set)	
and programmer in tracers	DCaexample DCacom	
distinguishedName		
distinguishedName domainPolicyObject	<not set=""></not>	
distinguishedName domainPolicyObject domainReplica	(not set)	
distinguishedName domainPolicyObject domainReplica dSASignature	<not set=""> <not set=""> { V1: Rags = 0x0; LatencySecs = 0; DsaGuit</not></not>	
distinguishedName domainPolicyObject domainReplica dSASignature dSCorePropagationD	<not set=""> <not set=""> { V1: Rags = 0x0; LatencySecs = 0; DsaGuic 0x0 = ( )</not></not>	
distinguishedName domainPolicyObject domainReplica dSASignature dSCorePropagationD <	<pre><not set=""> <not set=""> &lt;{V1: Rags = 0x0; LatencySecs = 0; DsaGuic 0x0 = ( ) </not></not></pre>	
distinguishedName domainPolicyObject domainReplica dSASignature dSCorePropagationD <	<not set=""> <not set=""> { V1: Rags = 0x0; LatencySecs = 0; DsaGuic 0x0 = ( ) &gt;</not></not>	

Dies kann für mehrere Objekte in **Active Directory** erfolgen. Beispielsweise werden die folgenden Schritte verwendet, um den DN des **User**-Containers zu ermitteln:



6. Die Ansicht **Erweiterte Funktionen** kann entfernt werden, indem Sie erneut mit der rechten Maustaste auf die Stamm-DN klicken. Klicken Sie dann unter **Ansicht** erneut auf **Erweiterte Funktionen**.



#### **FTD-Konto erstellen**

Dieses Benutzerkonto ermöglicht FMC und FTD, eine Bindung mit dem Active Directory herzustellen, um nach Benutzern und Gruppen zu suchen und Benutzer zu authentifizieren.

Durch die Einrichtung eines separaten FTD-Kontos soll verhindert werden, dass Unbefugte an anderen Stellen im Netzwerk auf die für die Bindung verwendeten Anmeldeinformationen zugreifen können.

Dieses Konto muss sich nicht im Bereich des Basis-DN oder Gruppen-DNs befinden.

1. Klicken Sie in **Active Directory User and Computers** mit der rechten Maustaste auf den Container/die Organisation, der/der das FTD-Konto hinzugefügt wird.

In dieser Konfiguration wird das FTD-Konto unter dem Benutzernamen ftd.admin@example.com unter dem Container **Users** hinzugefügt.

Klicken Sie mit der rechten Maustaste auf Benutzer, und navigieren Sie dann zu Neu > Benutzer.

Active Directory Users and Com	puters			-	×
File Action View Help					
🗢 🔿 🙍 🚾 🔏 🗈  🛠 🛙	n 🖸 🔒 🛛 🖬	1 🗏 🔌 🗈 🦷	r 🗾 🔍		
Active Directory Users and Com Saved Queries Saved Queries Saved Queries Saved Queries Saved Queries DefaultAcc Domain Acc Domain Ce DefaultAcc Domain Ce		Type User 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		^
Find	ers	Security Group Computer	All domain users		
All Tasks View	>	Contact Group			
Refresh Export List		InetOrgPerson msDS-KeyCreder msDS-ResourceP	ntial PropertyList		
Properties		msDS-ShadowPr	incipalContainer		
Help	K WseAlertA	msImaging-PSPs MSMQ Queue Al Printer	ias		
< >> Creates a new item in this container.	WseAllow	User Shared Folder			~

### 2. Gehen Sie durch den New Object - User Wizard.

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

New Object - User	×
Create in: example.com/Users	
Password:	
User must change password at next logon User cannot change password Password never expires Account is disabled	
< Back	Next > Cancel
New Object - User	×
New Object - User Create in: example.com/Users When you click Finish, the following object will be c	× zeated:
New Object - User Create in: example.com/Users When you click Finish, the following object will be c Full name: FTD Admin User logon name: ftd.admin@example.com The password never expires.	xeated:

3. Überprüfen Sie, ob das **FTD-Konto** erstellt wurde. Es werden zwei zusätzliche Konten erstellt: **IT-Administrator** und **Testbenutzer**.

Active Directory Users and Computers					х
File Action View Help					
🗢 🔿 🖄 📆 🖌 🗎  🗙 (	🗉 🗟 📑 🚺 🖬	1 🙎 🔌 🛍 🦷	r 🗾 🗽		
<ul> <li>Active Directory Users and Com</li> <li>Saved Queries</li> <li>Saved Queries</li> <li>Builtin</li> <li>Computers</li> <li>Domain Controllers</li> <li>ForeignSecurityPrincipal</li> <li>Managed Service Accounting Users</li> </ul>	Name DefaultAcco DefaultAcco DefaultAcco Donsdmins DosUpdateP Domain Ad Domain Co Domain Co Domain Co Domain Gue Domain Gue Domain Gue Domain Users Enterprise A Enterprise A Enterprise R Enterprise R Enterpris	Type User Security Group Security Group User User User 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 Designated administrato Members of this group Members of this group c Built-in account for gue Members of this group		^
< > >	Schema Ad Test User	Security Group User	Designated administrato		Ŷ
, ,	178.00 01				

#### AD-Gruppen erstellen und AD-Gruppen Benutzer hinzufügen (optional)

Obwohl sie für die Authentifizierung nicht erforderlich sind, können Gruppen verwendet werden, um die Anwendung von Zugriffsrichtlinien auf mehrere Benutzer sowie die LDAP-Autorisierung zu vereinfachen.

In diesem Konfigurationsleitfaden werden Gruppen verwendet, um die Richtlinieneinstellungen für die Zugriffskontrolle später über die Benutzeridentität in FMC anzuwenden.

1. Klicken Sie in **Active Directory-Benutzer und -Computer** mit der rechten Maustaste auf den Container oder die Organisationseinheit, zu dem bzw. der die neue Gruppe hinzugefügt wird.

In diesem Beispiel wird die Gruppe AnyConnect-Administratoren unter dem Container **Benutzer** hinzugefügt. Klicken Sie mit der rechten Maustaste auf **Benutzer**, und navigieren Sie dann zu **Neu > Gruppe**.

Active Directory Users and Com	puters			-	×
File Action View Help					
🗢 🔿 🙇 🚾 🖌 🗈  🗶	🗊 🖸 📑 🖬 🖬	1 🗏 🐮 🛯	r 🔟 🕱		
Active Directory Users and Com Saved Queries Saved Queries Builtin Builtin Computers Domain Controllers ForeignSecurityPrincipal Managed Service Accour Users Delegate Control Find		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. Gehen Sie durch den New Object - Group Wizard.

lew Object - Group	×
🥵 Create in: exam	nple.com/Users
Group name:	
AnyConnect Admins	
Group name (pre-Windows 2)	000):
AnyConnect Admins	
Group scope	Group type
O Domain local	Security
Global	Obstribution
OUniversal	
	OK Cancel

3. Überprüfen Sie, ob die Gruppe erstellt wurde. Die Gruppe **AnyConnect-Benutzer** wird ebenfalls erstellt.

Active Directory Users and Computers					×
File Action View Help					
🗢 🔿 🖄 📰 🕹	è   🛛 🖬   🐍 🔌 🛍 '	7 🗾 🐍			
Active Directory Users and Com Saved Queries Saved Queries Builtin Builtin Computers Solution ForeignSecurityPrincipals Managed Service Accour Users	Name AnyConnect Admins AnyConnect Users Calo Cert Publishers Cloneable Domain C DefaultAccount DefaultAccount DefaultAccount Domain RODC Passw DonsUpdateProxy Domain Admins Domain Admins Domain Computers Domain Computers Domain Computers Domain Guests Domain Guests Domain Users Enterprise 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 Security Group Security Group Security Group Security Group Security Group Security Group 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 DNS clients who are per Designated administrato All workstations and ser All domain controllers i All domain guests All domain guests All domain users Designated administrato Members of this group Members of this group Built-in account for gue		~
	max				

4. Klicken Sie mit der rechten Maustaste auf die Gruppe der Benutzer, und wählen Sie dann **Eigenschaften**. In dieser Konfiguration wird der Benutzer IT-Administrator der Gruppe AnyConnect-Administratoren hinzugefügt, und der Benutzer **Test-Benutzer** wird der Gruppe **AnyConnect-Benutzer** hinzugefügt.

Active Directory Users and Complexity	Active Directory Users and Computers					
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			
<ul> <li>Domain Controllers</li> <li>ForeignSecurityPrincipal:</li> <li>E Managed Service Accour</li> <li>Users</li> </ul>	All Cloneable Domain C Security Group N DefaultAccount User A DefaultAccount Security Group N DisAdmins Security Group D DisUpdateProxy Security Group D Domain Admins Security Group D Domain Computers Security Group A	Security Group User	Mer All Tasks	>		
		Mer Cut DNS Delete DNS Rename Des All v Properties				
	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. Klicken Sie unter Mitglieder auf Hinzufügen.

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

Geben Sie den Benutzer in das Feld ein, und klicken Sie auf **Namen überprüfen**, um zu überprüfen, ob der Benutzer gefunden wurde. Klicken Sie nach der Überprüfung auf **OK**.

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

Vergewissern Sie sich, dass der richtige Benutzer hinzugefügt wurde, und klicken Sie dann auf die Schaltfläche OK. Der Benutzer **Testbenutzer** wird mit denselben Schritten zur Gruppe **AnyConnect-Benutzer** hinzugefügt.

AnyConn	ect Admin	s Properties		?	×
General	Members	Member Of	Managed By		
Membe	na:				_
Name <u>8</u> IT	Admin	Active Dir example.c	ectory Domain Service: com/Users	s Folder	
Ad	d	Remove			
			OK Cano	al An	alv
			Vit	- A	20

Kopieren Sie die LDAPS SSL-Zertifikatwurzel (nur für LDAPS oder STARTTLS erforderlich).

1. Drücken Sie Win+R, und geben Sie mmc.exe ein. Klicken Sie dann auf 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. Navigieren Sie zu Datei > Snap-In hinzufügen/entfernen...

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

3. Wählen Sie unter Verfügbare Snap-Ins die Option **Zertifikate aus,** und klicken Sie dann auf **Hinzufügen**.

Add or Remove Snap-ins You can select snap-ins for t	his console from th	nose	available on your computer and configure the selected set of snap-ins. For	×
Available gnap-ins:	ronngare ninore	AUCI	Selected snap-ins:	
Snap-in	Vendor	^	Console Root Edit Extensions	
Active Directory Do	Microsoft Cor Microsoft Cor		<u>R</u> emove	
Active Directory Use	Microsoft Cor Microsoft Cor		Move Up	
Authorization Manager	Microsoft Cor Microsoft Cor		Add >	
Certificates	Microsoft Cor Microsoft Cor			
Component Services	Microsoft Cor Microsoft Cor			
Disk Management	Microsoft and	~	Ad <u>v</u> anced	
Description: The Certificates snap-in allo	ws you to browse	the	contents of the certificate stores for yourself, a service, or a computer.	
			OK Cancel	

4. Wählen Sie Computerkonto aus, und klicken Sie dann auf Weiter.

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

Klicken Sie auf Beenden.

Select Computer	×
Select the computer you want this snap in to manage. This snap in will always manage:	
< Back Finish Cancel	

#### 5. Klicken Sie nun auf OK.

Add or Remove Snap-ins							×
You can select snap-ins for t extensible snap-ins, you can	this console from the configure which e	iose 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)	Bomouo	
Active Directory Site	Microsoft Cor					Remove	
Active Directory Use	Microsoft Cor						
ActiveX Control	Microsoft Cor					Move Up	
ADSI Edit	Microsoft Cor					Move Down	
Authorization Manager	Microsoft Cor		<u>A</u> dd >			the rest of the second	_
Certificate Templates	Microsoft Cor		Concernance of 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	
			,				
Description:							_
The Certificates snap-in allo	ows you to browse	the	contents of the	certificate stores fo	or yourself, a service,	, or a computer.	
						OK Cancel	
						Cancel	

6. Erweitern Sie den Ordner **Personal**, und klicken Sie dann auf **Zertifikate**. Das von LDAPS verwendete Zertifikat wird an den **vollqualifizierten Domänennamen (Fully Qualified Domain Name, FQDN)** des Windows-Servers ausgegeben. Auf diesem Server sind drei Zertifikate aufgelistet.

- Ein Zertifizierungsstellenzertifikat, das von example-WIN2016-CA ausgegeben wird.
- Ein Identitätszertifikat, das von example-WIN2016-CA für WIN2016 ausgestellt wurde.
- Ein von example-WIN2016-CA an win2016.example.com ausgestelltes Identitätszertifikat.

In diesem Konfigurationsleitfaden lautet der FQDN win2016.example.com. Daher sind die ersten beiden Zertifikate nicht als LDAPS SSL-Zertifikat gültig. Das an win2016.example.com ausgestellte Identitätszertifikat ist ein Zertifikat, das automatisch vom Windows Server-Zertifizierungsstellendienst ausgestellt wurde. Doppelklicken Sie auf das Zertifikat, um die Details zu überprüfen.



7. Um als LDAPS SSL Zertifikat verwendet werden zu können, muss das Zertifikat folgende Anforderungen erfüllen:

• Der allgemeine Name oder der **alternative Name für den DNS-Betreff** stimmt mit dem FQDN von Windows Server überein.

• Das Zertifikat verfügt im Feld Erweiterte Schlüsselverwendung über Serverauthentifizierung.

Wählen Sie auf der Registerkarte **Details** für das Zertifikat **Subject (Betreff)** und **Subject Alternative Name (Alternativer Name des Betreffs) aus**, um den FQDN win2016.example.com aufzurufen.

🙀 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	Identifier y Identifier tion Points formation Access	Value 30 b7 2b 4e 48 0f 2f 17 17 e6 KeyID=3d 9f 26 37 fb 11 1f 4 [1]CRL Distribution Point: Distr [1]Authority Info Access: Acc	^
Ker The The The	y Usage umbprint	algorithm	Digital Signature, Key Encipher sha1 ca 8e 11 3d eb bc 0f 6e 4a 00	*
Other N DS ( 18 DNS Na	lame: Object Gu me=win2	id=04 10 90 99 a9 016.example.com	a2 38 24 65 47 84 74 64 26 cd c6 8	D
		Ed	It Properties Copy to File	
			0	(

Unter Erweiterte Schlüsselverwendung ist die Serverauthentifizierung vorhanden.

🙀 Certi	ficate			×
General	Details	Certification Path		
Show:	<al></al>		~	
Field			Value	^
E Su E Pu E Pu	bject blic key blic key p	arameters	win2016.example.com RSA (2048 Bits) 05 00	
Ce	rtificate T	emplate Name	DomainController	
Client /	IIME Capa bject Key thority Ka Authenticz Authenticz	bilities Identifier Widentifier Mon (1.3.6.1.5.5.) ation (1.3.6.1.5.5.)	[1]SMIME Capability: Object I 30 b7 2b 4e 48 0f 2f 17 17 e6 KevID=3d 9f 26 37 fb 11 1f 4	×
		Ed	it Properties Copy to File	

8. Nachdem dies bestätigt wurde, wählen Sie auf der Registerkarte **Zertifizierungspfad** das oberste Zertifikat aus, das das Stammzertifikat der Zertifizierungsstelle ist, und klicken Sie dann auf **Zertifikat anzeigen**.

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

9. Dadurch werden die Zertifikatdetails für das Stammzertifikat der Zertifizierungsstelle geöffnet.

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	

Klicken Sie auf der Registerkarte Details auf In Datei kopieren...

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. Gehen Sie durch den **Zertifikatexport-Assistenten**, der die Stammzertifizierungsstelle im PEM-Format exportiert.

÷	🐓 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, click Next.	
	<u>N</u> ext Cance	

Wählen Sie Base-64-codiertes X.509 aus

t File Format iertificates can be exported in a variety of file forma	its.
elect the format you want to use:	
O DER encoded binary X.509 (.CER)	
Base-64 encoded X.509 (.CER)	
O Cryptographic Message Syntax Standard - PK	CS #7 Certificates (.P7B)
Include all certificates in the certification p	ath if possible
O Personal Information Exchange - PKCS #12 (.	PFX)
Include all certificates in the certification p	ath if possible
Delete the private key if the export is suc	cessful
Export all extended properties	
Enable certificate privacy	
<ul> <li>Microsoft Serialized Certificate Store (.SST)</li> </ul>	

Wählen Sie den Namen der Datei und den Speicherort aus, in den sie exportiert wird.

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

		×
÷	🚰 Certificate Export Wizard	
	File to Export	
	Specify the name of the file you want to export	
		_
	File name:	
	C:\Users\admin\Desktop\root.cer Browse	
	Next Cance	4

Klicken Sie nun auf Fertig stellen.

÷	4	Certificate Export Wizard		×									
		Completing the Certificate Exp	port 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 Cance	el le									

11. Gehen Sie nun zum Ort und öffnen Sie das Zertifikat mit einem Notizblock oder einem anderen Texteditor. Zeigt das Zertifikat im PEM-Format an. Speichern Sie das für später.

#### ----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. (Optional) Falls es mehrere Identitätszertifikate gibt, die von LDAPS verwendet werden können und Unsicherheit darüber besteht, welche davon verwendet wird, oder wenn kein Zugriff auf den LDAPS-Server besteht, ist es möglich, die Root-CA aus einer Paketerfassung zu extrahieren, die auf dem Windows-Server oder FTD danach durchgeführt wird.

#### **FMC-Konfigurationen**

#### Lizenzierung überprüfen

Um eine AnyConnect-Konfiguration bereitzustellen, muss der FTD beim Smart Licensing-Server registriert werden, und es muss eine gültige Plus-, Apex- oder VPN Only-Lizenz auf das Gerät angewendet werden.

1. Navigieren Sie zu System > Licenses > Smart Licensing (System > Lizenzen > Smart Licensing).

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

2. Stellen Sie sicher, dass die Geräte die Compliance-Anforderungen erfüllen und erfolgreich registriert wurden. Stellen Sie sicher, dass das Gerät mit einer **AnyConnect Apex-, Plus-** oder **VPN Only-Lizenz** registriert ist.

verview Analysis Policies	De	evices Objects AMP Intelligence					(	Deploy 🔒 Sys	tem Help	• <b>•</b> admin
		Configuration Users	D	omains Integration	Up	dates	Licenses + Smart Lice	nses Health *	Monitorin	g 🔻 Took
Smart License Status				Cisco Smart Software M	anager	• 9				
Usage Authorization:	٢	Authorized (Last Synchronized On May 03 2020	)							
Product Registration:	Ø	Registered (Last Renewed On Mar 03 2020)								
Assigned Virtual Account:		SEC TAC								
Export-Controlled Features:		Enabled								
Cisco Success Network:		Disabled 🕕								
Cisco Support Diagnostics:		Disabled 🕕								
Smart Licenses			_				Filter Devices		×	Edit Licenses
License Type/Device Name			Lie	cense Status	Devio	e Type		Domain	Group	
Firepower Management	Cent	ter Virtual (2)	0	)						
🖻 🟳 Base (2)			0	)						
🖻 🟳 Mahware (1)			0	)						
🖻 🟳 Threat (2)			0	)						
URL Filtering (2)			0							
4 🥬 AnyConnect Apex (1)			0	)						
FTD-2 192.168.1.17 · Cisco Firepo	wer	Threat Defense for VMWare - v6.3.0	0		Cisco F	irepower	Threat Defense for VMWare	Global	N/A	
AnyConnect Plus (0)										
AnyConnect VPN Only (0)										

#### Setup-Bereich

1. Navigieren Sie zu **System > Integration**.

Overview Analysis	Policies	Devices	Objects	АМР	Intelligence					Deploy	🦳 🔒 <mark>s</mark>	iystem Help 🔻	admin 🔻
					Configuration	Users	Domains	Integration	Updates	Licenses *	Health *	Monitoring •	Tools *

2. Klicken Sie unter Bereiche auf Neuer Bereich.

Overview Analysis Policies Devic	es Objects AMP Intellige	nce			Deploy 🔍 🔍	rstem Help +	admin 🔻
	Cor	figuration Users	Domains Integ	ration Updates I	Licenses • Health •	Monitoring •	Tools 🔻
Cloud Services Realms Identity	Sources eStreamer Host )	nput Client Sm	art Software Satellite				
🕑 Compare realms 🕓 New rea							
Name Descript	ion Domain	Туре	Base DN	Group DN	Group Attribute	State	

3. Füllen Sie die entsprechenden Felder basierend auf den Informationen vom Microsoft-Server gesammelt. Klicken Sie abschließend auf **OK**.

lame *	LAB-AD		
Description			
Гуре *	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
Sroup Attribute	Member	~	

4. Wählen Sie im neuen Fenster Verzeichnis aus, falls noch nicht ausgewählt, und klicken Sie auf Verzeichnis hinzufügen.

Overview	Analysis	Policies	Devices	Objects A	4P Intellig	ence			Deploy	🖉 🔍 Sys	tem Help 🔻	admin 🔻
				Configuratio	n Users	Domains	Integration	Updates	Licenses 🔻	Health 🔻	Monitoring •	Tools •
LAB-AD Cancel								Cancel				
Directory	Realm Conf	iguration	User Dowr	nload								
											Q A	dd directory

Geben Sie die Details für den AD-Server an. Beachten Sie, dass bei Verwendung des FQDN FMC und FTD nur dann eine erfolgreiche Bindung herstellen können, wenn DNS für die Auflösung des FQDN konfiguriert ist.

Um DNS für FMC einzurichten, navigieren Sie zu **System > Configuration**, und wählen Sie **Management Interfaces (Verwaltungsschnittstellen)**.

Um DNS für die FTD einzurichten, navigieren Sie zu **Devices > Platform Settings,** erstellen Sie eine neue Richtlinie, oder bearbeiten Sie eine aktuelle Richtlinie, und wechseln Sie dann zu DNS.

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

Wenn LDAPS oder STARTTLS verwendet wird, klicken Sie auf das Symbol Grün +, geben Sie dem Zertifikat einen Namen, und kopieren Sie das Zertifikat der Stammzertifizierungsstelle im PEM-Format. Klicken Sie abschließend auf **Speichern**.

Import Trusted Certificate Authority	? ×
Name: LDAPS_ROOT	
Certificate Data or, choose a file: Browse	
BEGIN CERTIFICATE MIIDCDCCAfCgAwIBAgIQE4ZG5Z1wT6lONTjooEQyMTANBgkqhkiG9w0BAQsFADAd MRswGQYDVQQDExJleGFtcGxlLVdJTjIwMTYtQ0EwIBcNMjAwNDI3MTQ1MDU5WhgP MjA2MDA0MTkxNDUwNTlaMB0xGzAZBgNVBAMTEmV4YW1wbGUtV0lOMjAxNi1DQTCC ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAI8ghT719NzSQpoQPh0YT67b Ya+PngsxMyvkewP33QLTAWw1HW1Tb9Mk5BDWOItTaVsgHwPBfd++M+bLn3AiZnHV OO+k6dVVY/E5qVkEKSGoY+v940S2316lzdwReMOFhgbc2qMertIoficrRhihonuU Cjyeub3CO+meJUuKom2R47C0D35TUvo/FEHGgXJFaJS1se2UrpNO7KEMkfA1LPuM aob4XE/OzXYQpPa18djsNnskfcFqD/HOTFQN4+Sr0hHWIRnUIQBUaLdQaabhipD/ SvSSPneYJX8YKma821uY16j90YuytmsHBtCieyC062a8BKqOL7N86HFPFKMA3u8C AwEAAaNCMEAwDgYDVR0PAQH/BAQDAgGGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0O BBYEFD2fJjf7ER9EM/HCxCVFN5QzqEdvMA0GCSqGSIb3DQEBCwUAA4IBAQB31ZJo vzwVD3c5Q1nrNP+6Mq62OFpYH91k4Ch9S5g/CEOemhcwg8MDIoxW2dTsjenAEt7r phFIHZoCoSyjBjMgK3xybmoSeg8vBjCXseYNGEmOc9KW10FmTOvdNVIb7Xpl1IVa 6tALTt3ANRNgREtxPA6yQbthKGavW0Anfsojk9IcDr2vp0MTjIBCxsTscbubRI+D dLEFKQqmMeYvkVf+a7a64mqPZsG3Uxo0rd6cZxAPkq/ylcdwNSJFfQV3DgZg+R96 9WLCR3Obig6xyo9Zu+lixcWpdrbADO6zMhbEYEhkhOOjBrUEBBI6Cy83iTZ9ejsk KgwBJXEu33PpIW6E END CERTIFICATE	< ~
Save Can	cel

Wählen Sie die neu hinzugefügte Stammzertifizierungsstelle aus dem Dropdown-Menü neben SSL-Zertifikat aus, und klicken Sie auf STARTTLS oder LDAPS.
Edit directory	? ×
Hostname / IP Address	win2016.example.com
Port	636
Encryption	○ STARTTLS
SSL Certificate	LDAPS_ROOT 💙 😳
	OK Test Cancel

Klicken Sie auf Test, um sicherzustellen, dass FMC eine erfolgreiche Bindung mit dem im vorherigen Schritt angegebenen Benutzernamen und Kennwort für das Verzeichnis herstellen kann.

Da diese Tests vom FMC und nicht über eine der im FTD konfigurierten routingfähigen Schnittstellen (z. B. intern, extern, dmz) initiiert werden, garantiert eine erfolgreiche (oder fehlgeschlagene) Verbindung nicht dasselbe Ergebnis für die AnyConnect-Authentifizierung, da AnyConnect LDAP-Authentifizierungsanforderungen von einer der FTD-routingfähigen Schnittstellen initiiert werden.

Weitere Informationen zum Testen von LDAP-Verbindungen aus dem FTD finden Sie in den Abschnitten Test AAA und Packet Capture im Bereich Troubleshooting (Fehlerbehebung).

Status	
$(\mathbf{i})$	Test connection succeeded
	(

5. Laden Sie unter **Benutzer-Download** die Gruppen herunter, die in späteren Schritten für die Benutzeridentität verwendet werden.

Aktivieren Sie das Kontrollkästchen **Benutzer und Gruppen herunterladen**, und die Spalte für **Verfügbare Gruppen** wird mit den in Active Directory konfigurierten Gruppen ausgefüllt.

Gruppen können ein- oder ausgeschlossen werden, standardmäßig sind jedoch alle Gruppen enthalten, die unter der Gruppen-DN zu finden sind.

Bestimmte Benutzer können ebenfalls ein- oder ausgeschlossen werden. Alle enthaltenen Gruppen und Benutzer können zu einem späteren Zeitpunkt als Benutzeridentitäten ausgewählt werden.

Klicken Sie abschließend auf Speichern.

Overview Analysis Policies Devices Objects AMP Intel	ligence			Deploy	\varTheta System Help	▼ admin ▼
	Configuration Users	Domains Integratio	on Upd	lates Licenses •	Health  Monitoring	y ▼ Tools ▼
LAB-AD				You have unsay	ved changes 🔚 Save	😮 Cancel
Enter Description						
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					
🗄 Download Now						
Available Groups 😋	Groups to Include (2)			Groups to Exclude (0)		
Search by name	💣 AnyConnect Admins		8	Nana		
AnyConnect Admins	🝰 AnyConnect Users		8			
A DnsUpdateProxy						
A WseRemoteAccessUsers						
A WseInvisibleToDashboard						
Allowed RODC Password Replication Group Add to						
A Enterprise Key Admins Include						
Add to Add to						
A WseAlertAdministrators						
A Event Log Readers						
A Replicator						
🝰 Domain Guests						
A Windows Authorization Access Group						
Account Operators						
🝰 Hyper-V Administrators 🗸 🗸 🗸	Patro Hara Industra			Patro Hara Datation		
💑 System Managed Accounts Group	Enter User Inclusion		Add	Enter User Exclusion		Add

#### 6. Aktivieren Sie den neuen Bereich.

Overview Analysis Polici	es Devices Objec	ts AMP I	ntelligence							Deploy	0 Sy	stem He	p∗ admin∗
			Configur	ation (	Jsers	Domains	Integra	tion	Updates	Licenses 🔻	Health <b>*</b>	Monitori	ng 🔻 🛛 Tools 🔻
Cloud Services Realms	Identity Sources	eStreamer	Host Inp	ut Client	Smar	rt Software	Satellite						
											M Comp	are realms	O New realm
Name	Description	Domain		Туре	6	Base DN		Group C	IN .	Group Att	ribute	State	
LAB-AD		Global		AD	C	DC=example,D0	-com	DC-exa	nple,DC=com	member			🕁 🥒 🛅 🖯

7. Wenn LDAPS oder STARTTLS verwendet wird, muss die Stammzertifizierungsstelle auch von der FTD als vertrauenswürdig eingestuft werden. Navigieren Sie dazu zunächst zu **Geräte > Zertifikate**.

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

Klicken Sie oben rechts auf Hinzufügen.

Overview Analysis	Polic	ies Dev	ices	bjects AMP In	telligence		Deploy	) 🔍	System	Help 🔻	admin <del>v</del>
Device Management	NAT	VPN •	QoS	Platform Settings	FlexConfig	Certificates					
										0	Add

Wählen Sie das FTD aus. Die LDAP-Konfiguration wird hinzugefügt, und klicken Sie dann auf das grüne + Symbol.

Add New Certificate	2	? ×
Add a new certificate to t 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

Geben Sie dem Vertrauenspunkt einen **Namen**, und wählen Sie dann im Dropdown-Menü **Anmeldetyp** die Option **Manuelle** Anmeldung aus. Fügen Sie hier das PEM-Stammzertifikat ein, und klicken Sie dann auf **Speichern**.

Add Cert Enrollme	nt	? ×
Name*	LDAPS_ROOT	
Description		
CA Information	Certificate Parameters Key Revocation	
Enrollment Type:	Manual 👻	^
CA Certificate:*	<ul> <li>MIIDCDCCAfCgAwIBAgIQE4ZG5Z1wT6lONTjooEQyMTANBgkqhki</li> <li>G9w0BAQsFADAd</li> <li>MRswGQYDVQQDExJleGFtcGxlLVdJTjIwMTYtQ0EwIBcNMjAwNDI</li> <li>3MTQ1MDU5WhgP</li> <li>MjA2MDA0MTkxNDUwNTlaMB0xGzAZBgNVBAMTEmV4YW1wbGU</li> <li>tv0lOMjAxNi1DQTCC</li> <li>ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAI8ghT719N</li> <li>zSQpoQPh0YT67b</li> <li>Ya+PngsxMyvkewP33QLTAWw1HW1Tb9Mk5BDWOItTaVsgHwPBf</li> <li>d++M+bLn3AiZnHV</li> <li>OO+k6dVVY/E5qVkEKSGoY+v940S2316lzdwReMOFhgbc2qMertIo</li> <li>ficrRhihonuU</li> <li>Cjyeub3CO+meJUuKom2R47C0D35TUvo/FEHGgXJFaJS1se2UrpN</li> <li>O7KEMkfA1LPuM</li> <li>aob4XE/OzxYQpPa18djsNnskfcFqD/HOTFQN4+SrOhHWlRnUIQBU</li> <li>aLdQaabhipD/</li> <li>sVs5PneYJX8YKma821uYI6j90YuvtmsHBtCievC062a8BKqOL7N86</li> </ul>	~
Allow Overrides		
	Save	Cancel

Vergewissern Sie sich, dass der erstellte Vertrauenspunkt ausgewählt ist, und klicken Sie dann auf **Hinzufügen**.

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	Y
Cert Enrollment*:	LDAPS_ROOT	<b>~</b> ©
Cert Enrollment Details:		
Name:	LDAPS_ROOT	
Enrollment Type:	Manual	
SCEP URL:	NA	
		Add Cancel

Der neue Vertrauenspunkt erscheint unter der FTD. Obwohl erwähnt wird, dass ein Import von Identitätszertifikaten erforderlich ist, ist es für die FTD nicht erforderlich, das vom LDAPS-Server gesendete SSL-Zertifikat zu authentifizieren, sodass diese Nachricht ignoriert werden kann.

Overview Analysis P	Policies Devices Obj	ects AMP Intel	lligence	Deploy 🔍 System	m Help <del>v</del>	admin 🔻
Device Management N	AT VPN VQoS	Platform Settings	FlexConfig Certificates			
					0	Add
Name	Domain	Enrollment Type	Status			
4 🗐 FTD-1						
FTD-1-PKCS12	Global	PKCS12 file	CA ID		£ ¢	
4 🗐 FTD-2						
FTD-2-PKCS12	Global	PKCS12 file	CA CA ID		£ ¢	
FTD-2-Selfsigned	Global	Self-Signed	S CA Q ID		£ ¢	
LDAPS_ROOT	Global	Manual	🔍 CA 🔥 ID 🛓 Ide	ntity certificate import required	P ¢	) 🗎

#### Konfigurieren von AnyConnect für die AD-Authentifizierung

1. Bei diesen Schritten wird davon ausgegangen, dass noch keine VPN-Richtlinie für den Remote-Zugriff erstellt wurde. Wenn eine solche erstellt wurde, klicken Sie auf die Schaltfläche zum Bearbeiten für diese Richtlinie, und fahren Sie mit Schritt 3 fort.

Navigieren Sie zu Geräte > VPN > Remotezugriff.

Overview Analysis	Policies	Device	s Obje	ects AMP Intel	ligence			Deploy	0	System	Help 🔻	admin 🔻
Device Management	NAT	VPN •	QoS	Platform Settings	FlexConfig	Certificates						
		Site To S	ite									
		Remote /	Access									
		Troubles	hooting									

Klicken Sie auf Hinzufügen, um eine neue VPN-Richtlinie für den Remote-Zugriff zu erstellen.



2. Schließen Sie den Assistenten für VPN-Richtlinien für den Remotezugriff ab. Geben Sie unter Richtlinienzuweisung einen Namen für die Richtlinie und die Geräte an, auf die die Richtlinie angewendet wird.

Overview Analysis Policies De	vices Objects AMP In	ntelligence		Deploy 🔒 Syste	m Help <del>v</del> admin v
Device Management NAT VPN	Remote Access QoS I	Platform Settings	FlexConfig Certificates		
Remote Access VPN Policy	Wizard				
1 Policy Assignment 2 C	onnection Profile $>3$ A	nyConnect > (4	) Access & Certificate >	S Summary	
Targeted Devic This wizard will gui a new user-defined	es and Protocols de you through the required minima connection profile.	l steps to configure the	Remote Access VPN policy with	Before You Start	^
Name:* Description:	PTD-2-RA-Policy		¢	configuration elements to be in place to complete Remote Access VPN Policy. Authentication Server Configure <u>Readm</u> or <u>8401US</u> Server Group to authenticate VPN clients.	
Targeted Devices:	M SSL M IPsec-IKEv2 Available Devices	Se	elected Devices	AnyConnect Client Package Make sure you have AnyConnect package for VPN Client downloaded or you have the relevant Cisco credentials to download	
	₩ FTD-1	Add		Device Interface Interfaces should be already configured on bargeted dynamics so that they can be used as a security zone or interface group to enable VPN access.	
				Back Nex	t Cancel

Geben Sie unter **Verbindungsprofil** den Namen des **Verbindungsprofils an**, das auch als Gruppenalias verwendet wird, den AnyConnect-Benutzer sehen, wenn sie eine Verbindung herstellen.

Geben Sie den Bereich an, der zuvor unter Authentifizierungsserver erstellt wurde.

Methode angeben AnyConnect-Clients werden IP-Adressen zugewiesen.

Geben Sie die Standardgruppenrichtlinie an, die für dieses Verbindungsprofil verwendet wird.

Overview Analysis Policies Devices Objects AMP	Intelligence	Deploy 05	System	Help 🔻	admin <del>v</del>
Device Management NAT VPN + Remote Access QoS	Platform Settings FlexConfig Certificates				
Remote Access VPN Policy Wizard					
1) Policy Assignment 2 Connection Profile 3	AnyConnect > (4) Access & Certificate > (5) Summary				
Connection Profile: Connection Profiles specify the tunne accomplished and how addresses are Connection Profile Name:*	group policies for a VPN connection. These policies pertain to creating the tunnel itself, how assigned. They also include user attributes, which are defined in group policies. General This name is configured as a connection alias, it can be used to connect to the VPN gateway	w AAA is			^
Authentication, Authorization & A Specify the method of authentication	(AAA, cartificates or both), and the AAA servers that will be used for VPN connections.				
Authentication Method:	AAA Only 👻				
Authentication Server:*	LAB-AD C. (Realm or RADIUS)				
Authorization Server:	V 🔇 (RADIUS)				
Accounting Server:	V (RADIUS)				
Client Address Assignment:					
Client IP address can be assigned fro assignment is tried in the order of A/	n AAA server, DHCP server and IP address pools. When multiple options are selected, IP ad A server, DHCP server and IP address pool.	idress			
Use AAA Server (RADUS) Use DHCP Servers Use IP Address Pools	nly) 🚺				
IPv4 Address Pools:	AnyConnect-Pool 🧳				
IPv6 Address Pools:	/				
Group Policy: A group policy is a collection of user- or create a Group Policy object.	riented session attributes which are assigned to client when a VPN connection is establishe	d. Select			
Group Policy:*	DftGrpPolicy V C Edit Group Policy				~
		Back	Next	<b>a</b>	ancel

Laden Sie unter AnyConnect die verwendeten AnyConnect-Pakete hoch, und geben Sie sie an.

Overview Analysis Policie	s Devices Objects AMP	Intelligence		Deploy 🔒 System	Help 🔻 admin 🔻
Device Management NAT	VPN + Remote Access QoS	Platform Settings FlexConfig Certific	ates		
Remote Access VPN Po	licy Wizard				
Policy Assignment	<ol> <li>Connection Profile</li> <li>3</li> </ol>	AnyConnect 🔷 🕘 Access & Certific	ate > (5) Summary		
A T ir	nyConnect Client Image he VM gateway can automatically downli itiated. Minimize connection setup time by	ad the latest AnyConnect package to the client choosing the appropriate OS for the selected pack	device when the VPN connection is age.		^
C	ownload AnyConnect Client packages from	Cisco Software Download Center.	These December 1 and the second s		
1	AnyConnect File Object Name	AnyConnect Client Package Name	Operating System		
1	anyconnect-linux64-4.7.03052-we	anyconnect-linux64-4.7.03052-webdeploy-k9	Linux		
I	anyconnect-win-4.7.00136-webde	anyconnect-win-4.7.00136-webdeploy-k9.pkg	Windows 💌		~
			(	Back Next	Cancel

Geben Sie unter Access & Certificate (Zugriff und Zertifikat) die Schnittstelle an, auf die AnyConnect-Benutzer für AnyConnect zugreifen.

Erstellen und/oder spezifizieren Sie das Zertifikat, das vom FTD während des SSL-Handshakes verwendet wird.

Stellen Sie sicher, dass das Kontrollkästchen für die **Richtlinie zur Umgehung der Zugriffskontrolle** für entschlüsselten Datenverkehr (sysopt permit-vpn) nicht aktiviert ist, sodass die später erstellte Benutzeridentität für RAVPN-Verbindungen übernommen wird.

Overview Analysis Policies Devices Objects AMP Inte	ligence	Deploy	🔒 System	Help 🔻	admin 🔻
Device Management NAT VPN > Remote Access QoS Plan	form Settings FlexConfig Certificates				
Remote Access VPN Policy Wizard					
1 Policy Assignment $>$ 2 Connection Profile $>$ 3 Any	Connect 🔰 👌 Access & Certificate 🔰 🌀 Summary 🔄				
Network Interface for Incor Select or create an Interface Group connections.	ning VPN Access or a Security Zone that contains the network interfaces users will access for VPN	I			^
Interface group/Security Zone:*	outside-zone 🗸 🖉 🗸				
	Enable DTLS on member interfaces				
Davies Castification					
Device Certificates Device certificate (also called Iden	ity certificate) identifies the VPN gateway to the remote access clients. Select a				
certificate which is used to authent	icate the VPN gateway.				
Certificate Enrolment:*	FTD-2-Selfsigned Y				
	Control the selected certificate object on the target devices				
Access Control for VPN Traf	fic				
All decrypted traffic in the VPN tun bypass decrypted traffic from the A	nel is subjected to the Access Control Policy by default. Select this option to access Control Policy.				
Bypass Access Control policy fr This option bypasses the Access AAA server are still applied to Vi	r decrypted traffic (sysopt permit-upn) Central Policy Inspection, but VPN filter ACL and authorization ACL downloaded from N traffic.				
		Back	Next	) <b>C</b>	ancel

# Überprüfen Sie unter Übersicht die Konfiguration, und klicken Sie auf Fertig stellen.



3. Klicken Sie unter der VPN-Richtlinie für den Remotezugriff auf Bearbeiten, um das entsprechende Verbindungsprofil anzuzeigen.

Overview Analysis	Policies De	evices	Objects	AMP	Intelligence				Deploy	e	System	Help 🔻	admin 🔻
Device Management	NAT VPN	Remote	e Access	QoS	Platform Settings	FlexConfig	Certificates						
FTD-2-RA-Polic	у											Save	🙁 Cancel
Connection Profile	Access Inter	rfaces	Advanced								<u>e</u>	Policy Ass	gnments (1)
													a
Name				AAA				Group Policy					
DefaultWEBVPNGroup				Authen Author Accourt	tication: None ization: None ting: None			DftGrpPolicy					/0
General				Auther Author Accourt	tication: LAB-AD (AD) ization: ficture ting: ficture			P DftbGrpPolicy					28

Stellen Sie sicher, dass der Authentifizierungsserver auf den zuvor erstellten Bereich festgelegt ist.

Unter Erweiterte Einstellungen kann Kennwortverwaltung aktivieren aktiviert werden, damit Benutzer ihr Kennwort ändern können, wenn oder bevor das Kennwort abläuft.

Diese Einstellung erfordert jedoch, dass der Bereich LDAPS verwendet. Wenn Änderungen vorgenommen wurden, klicken Sie auf **Speichern**.

Edit Connection Pr	ofile		? ×
Connection Profile:* Group Policy:*	General DfltGrpPolic	y V	
Client Address Assign	ment AA	A Aliases	
Authentication			
Authentication Meth	od:	AAA Only	
Authentication Serv	er:	LAB-AD (AD)	
Use secondary a	uthentication		
Authorization			
Authorization Serve	r:	Allow connection only if user exists in authorization database	
		a know connection only it user exists in autionization database	
Accounting			
Accounting Server:		<b>v</b>	
Advanced Setting	gs		
Strip Realm from	username		
Strip Group from	username		
Enable Password     Notify User     Notify user on the second secon	Management days pric ne day of passy	t or to password expiration word expiration	
		Save Cance	d -

Klicken Sie abschließend oben rechts auf Speichern.



Identitätsrichtlinie aktivieren und Sicherheitsrichtlinien für Benutzeridentität konfigurieren

1. Navigieren Sie zu Richtlinien > Zugriffskontrolle > Identität.



Erstellen einer neuen Identitätsrichtlinie

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

Geben Sie einen Namen für die neue Identitätsrichtlinie an.

Name	FTD-2 Identity Policy
Description	

2. Klicken Sie auf Regel hinzufügen.



3. Geben Sie einen **Namen** für die neue Regel an. Stellen Sie sicher, dass sie aktiviert ist und dass Aktion auf Passive Authentifizierung festgelegt ist.

Klicken Sie auf die Registerkarte **Bereich und Einstellungen**, und wählen Sie den zuvor erstellten Bereich aus. Klicken Sie abschließend auf **Hinzufügen**.

Add Rule

ame RAVPN		🖌 Enal	oled Insert	into Category	*	Standard Rules	~
ction Passive Authent	ication	✓ Realm: LAB-AD (AD	Authentication Protocol:	HTTP Basic Exclude I	HTTP User-	Agents: None	
Remote access V	W sessions are actively a	uthenticated by VPN. Other sess	ions use the rule Action.				
Zones Networks	VLAN Tags Ports					Realm & Se	ettings
Dealer *							
eann	LAB-AD (AD)		¥ 6/				
Use active authentic	ation if passive or VPN ide	entity cannot be established					
Required Field							

# 4. Klicken Sie auf Speichern.

Overview Analysis Poli	icies Device	s Objects	AMP Intelli	gence				Dep	oloy 🧛 System	Help 🔻 adı	nin •
Access Control + Identity	Access Control > Identity Network Discovery Application Detectors Correlation Actions •										
FTD-2 Identity Policy You have unsaved changes Save Cancel											
Rules Active Authentication											
							Add Categoria	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											

# 5. navigieren Sie zu **Richtlinien > Zugriffskontrolle > Zugriffskontrolle**.

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

# 6. Bearbeiten Sie die Zugriffskontrollrichtlinie, unter der das FTD konfiguriert ist.

Overview Analysis Policies	Devices Objects	AMP Intelligence				Deploy	🔒 System	Help 🔻	admin <del>v</del>
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"			<b>G</b> 0	2 8

7. Klicken Sie auf den Wert neben Identitätsrichtlinie.



Wählen Sie die zuvor erstellte Identitätsrichtlinie aus, und klicken Sie dann auf OK.

Identity Policy	
FTD-2 Identity Policy	✓
Revert to Defaults	OK Cancel

8. Klicken Sie auf **Regel hinzufügen**, um eine neue AKP-Regel zu erstellen. Mit diesen Schritten wird eine Regel erstellt, die es Benutzern in der Gruppe der AnyConnect-Administratoren ermöglicht, mithilfe von RDP eine Verbindung zu Geräten im Netzwerk herzustellen.

Overview Analysis Policies Devices Ob	jects AMP Intelligence		Deploy 0	System Help 🔻 admin 🔻
Access Control > Access Control Network Dis	overy Application Detectors	Correlation Actions •		
Default-Policy Enter Description			You have unsaved changes Analyze Hit C	sunts 🔚 Save 🛛 😮 Cancel
Prefilter Policy: Default Prefilter Policy	SSL1	Policy: None	Identity Policy:	FTD-2 Identity Policy
			Te Inheritance S	ettings   🛐 Policy Assignments (1)
Rules Security Intelligence HTTP Responses	Logging Advanced			
曲 Filter by Device		Show Rule Conflicts 😣	🔘 Add Category 🛛 🔘 Add Rule 🚔 🏱	sarch Rules 🛛 💢
a Name Sourc Dest Z Sourc	Dest N VLAN Users	Applic Sourc Dest P	URLs Sourc Dest S Action	• to se 🖉 🔍
➡ Mandatory - Default-Policy (-)				
There are no rules in this section. Add Rule or Add Catego	γ			
There are no rules in this section. Add Rule or Add Catego	у			
Default Action			Access Control: Block All Traffic	× .

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

Geben Sie einen Namen für die Regel an. Stellen Sie sicher, dass die Regel aktiviert ist und über die entsprechende Aktion verfügt.

Geben Sie auf der Registerkarte **Zonen** die entsprechenden Zonen für den interessanten Datenverkehr an.

Von Benutzern initiierter RDP-Datenverkehr gelangt über die Schnittstelle der Außenzone in den FTD und gelangt in die Innenzone.

Add Rule											? X
AC RDP Access			<b>.</b> 		nabled	Inse	rt into Mande	story `	•		
Zones Networks	VLAN Tags	Users Ap	pplications	Ports	URLs	SGT/ISE Attribute	s		Inspection	Logging	Comments
Available Zones 🛭 🗯				Sour	ce Zones	(1)		Destinat	ion Zones (1)		
🔍 side		×		- <b>-</b> •	utside-zo	ne	6	🚠 insid	e-zone		ii ii
👍 inside-zone			Add to Source Add to Destination								
										Add	Cancel

Definieren Sie unter Netzwerke die Quell- und Zielnetzwerke.

Das Objekt AnyConnect\_Pool enthält die IP-Adressen, die AnyConnect-Clients zugewiesen sind.

Objekt Inside\_Net enthält das interne Netzwerk-Subnetz.

Add Ru	le											
Name	AC RDP Access				🖌 En	abled		Insert	into Manda	tory		~
Action	Allow			V V D /8	t I							
Zone	s Networks VLA	N Tags	Users	Applications	Ports	URLs	SGT/ISE	Attributes		Inspection	Logging	Comments
Availabl	e Networks 🖸		0		Sourc	e Netwo	rks (1)			Destination Networks	(1)	
Sear	ch by name or value					Source		Original (	Client	📰 Inside_Net		6
	Networks	Geolocation	n		📄 Ar	nyConned	_Pool		6			
Inside IPv4	de_Net I-Benchmark-Tests I-Ink-Local I-Multicast I-Private-10.0.0.0-8 I-Private-172.16.0.0-12 I-Private-192.168.0.0-16 I-Private-All-RFC1918 I-Private-All-RFC1918		<	Add To Source Networks Add to Destination	Enter	an IP add	fress		Add	Enter an IP address		Add
											Add	Cancel

Klicken Sie unter **Benutzer** auf den Bereich, der zuvor unter **Verfügbare Bereiche** erstellt wurde, klicken Sie unter **Verfügbare Benutzer** auf die entsprechende Gruppe bzw. den entsprechenden Benutzer, und klicken Sie dann auf **Zur Regel hinzufügen**.

Wenn keine Benutzer oder Gruppen im Abschnitt Verfügbare Benutzer verfügbar sind, stellen Sie sicher, dass FMC die Benutzer und Gruppen im Abschnitt Bereich herunterladen konnte und dass die entsprechenden Gruppen/Benutzer enthalten sind.

Die hier angegebenen Benutzer/Gruppen werden aus der Quellperspektive überprüft.

So bewertet die FTD anhand der bisher in dieser Regel definierten Kriterien, dass der Datenverkehr von der Außenzone zur Innenzone, vom Netzwerk im AnyConnect\_Pools-Objekt und vom Netzwerk im Inside\_Net-Objekt stammt und von einem Benutzer in der Gruppe

### AnyConnect-Administratoren stammt.

Add Ru	le												? ×
Name	AC RDP Access	i		<b>V</b> OD.		inabled	1	Insert	into Mandato	ory Y			
Zone	s Networks	VLAN Tags	Users	Applications	Ports	URLs	SGT/ISE Attrib	utes			Inspection	Logging	Comments
Availab	rch by name or cial Identities -AD	value		Available Usen Search by n LAB-AD/* AnyConnect AnyConnect AnyConnect AnyConnect t.admin test.user	Admins	lue		)	dd to Rule	Selected	Users (1)	t Admins	Ĩ
												Add	Cancel

Unter "Ports" wurden benutzerdefinierte RDP-Objekte erstellt und hinzugefügt, um den TCP- und UDP-Port 3389 zuzulassen. Beachten Sie, dass RDP im Abschnitt "**Anwendungen"** hätte hinzugefügt werden können, aber aus Gründen der Einfachheit werden nur die Ports überprüft.

Add Rule					? ×
Name AC RDP Access		✓ Enabled	Insert into Mand	iatory Y	
Action 🖋 Allow	V 0 .	8 to 5			
Zones Networks VLAN Tags	Users Applications	Ports URLs SGT/I	SE Attributes	Inspection	Logging Comments
Available Ports 🖸	0	Selected Source Ports	(0)	Selected Destination (	Ports (2)
AOL AOL Bittorrent DNS_over_TCP DNS_over_UDP FMC-HTTPS FMC-SSH FTD-3-FDM FTD-3-SSH TD-3-SSH	Add to Source Add to Destinatio	any		ውቅ RDP-TCP ወቅ RDP-UDP	5
иттр	~			Protocol TCP (6)	▼ Port Enter a Add
					Add Cancel

Schließlich wird unter **Protokollierung** das **Protokoll am Ende der Verbindung** zu einem späteren Zeitpunkt auf zusätzliche Verifizierung hin überprüft. Klicken Sie abschließend auf **Hinzufügen**.

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		Inspectio	n Logging	Comments
Log Log File Even Log Send Co	at Beginning of Co at End of Connect nts: Files	onnection ion									
Syst	log Server (Using (	default syslog co	nfiguratio	n in Access Contra	l Logging	) Show O	verrides				
	IP Trap Select an	SNMP Alert Con	figuration.			Y	0				
										Add	Cancel

9. Es wird eine zusätzliche Regel für den HTTP-Zugriff erstellt, um Benutzern innerhalb der Gruppe **AnyConnect-Benutzer** den Zugriff auf die **Windows Server IIS-**Website zu ermöglichen. Klicken Sie auf **Speichern**.

Overview Analysis Policies Devices Obje	cts AMP Intelligence	Deploy 🍳 System Help 🔻 admin 🔻
Access Control + Access Control Network Disco	very Application Detectors Correlation Actions •	
Default-Policy Enter Description		You have unsaved changes 🛛 Analyze Hit Counta 📄 🔚 Save 💽 Cancel
Prefilter Policy: Default Prefilter Policy	55L Policy: None	Identity Policy: <u>FTD-2 Identity Policy</u>
		Ta Inheritance Settings   🖳 Policy Assignments (1)
Rules Security Intelligence HTTP Responses	Logging Advanced	
# Filter by Device	Show Rule Cor	nfictes 😣 😋 Add Category 😋 Add Rule 📫 Search Rules 🗙
# 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 🛛 👼 Inside_Net 🖉 🗛 🖉 LAB-AD/AnyConnect Admins	Any Any 🌽 RDP-UDP Any Any Any 🖌 Allow 🗍 🕥 🔗 🚖 🗐 🖉 🥒
2 AC HTTP Access di outside-zone di inside-zone	aryConnect_Pool 🛛 😹 Inside_Net 🛛 🗛 🖉 LAB-AD/AnyConnect Users	- Any Any PHTTP - Any Any Any VAllow 🛈 🖸 🗟 🖄 🗐 0 🥒 🕄
▼ 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-Ausnahme konfigurieren

Wenn es NAT-Regeln gibt, die sich auf den AnyConnect-Datenverkehr auswirken, z. B. Internet-PAT-Regeln, ist es wichtig, NAT-Freistellungsregeln zu konfigurieren, damit der AnyConnect-Datenverkehr nicht durch die NAT beeinträchtigt wird.

1. Navigieren Sie zu Geräte > NAT.

Overview Analysis	s Polici	es Dev	ices	Objects	AMP 1	Intelligence			Deploy	) <b>Q</b>	System	Help 🔻	admin v
Device Management	NAT	VPN *	QoS	Platfor	m Settings	s FlexConfig	Certificates						

Wählen Sie die auf den FTD angewendete NAT-Richtlinie aus.

Overview Analysis Polici	s Devices Objects AMP	Intelligence	Deploy 🔒 System	Help 🔻 admin 🔻
Device Management NAT	VPN VOS Platform Setti	ngs 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	ħ E <b>∕</b> 8

2. In dieser NAT-Richtlinie gibt es eine dynamische PAT am Ende, die den gesamten Datenverkehr (einschließlich AnyConnect-Datenverkehr) betrifft, der von der externen Schnittstelle zur externen Schnittstelle abgeht.

Um zu verhindern, dass AnyConnect-Datenverkehr von NAT beeinflusst wird, klicken Sie oben rechts auf Add Rule (Regel hinzufügen).

Overview	Analysis	Policies Dev	ices Objects	AMP	Intelligence			Deple	oy 🍳	System H	elp 🔻 admin 🔻
Device Manag	pement	NAT VPN *	QoS Platfor	m Setting	s FlexConfig	Certificates					
FTD-2-N Enter Description	AT-Pol	cy						🔌 s	how Warning	a 📔 🖓	ve Cancel
Rules										E P	olicy Assignments (1)
B Filter by Devic											Add Rule
					Original Pack	et		Translated Packet			
# Direction	Туре	Source Interface Obje	Destination Interface Object	Original Sources	Original Destinatio	Orig Service	Translated Sources	Translated Destinations	Trans Services	Options	
▼ NAT Rules Be	fore										
<ul> <li>Auto NAT Rul</li> </ul>	es										
= +	Dynamic	🥞 any	🚠 outside-zone	🚍 obj-a	ny		🥵 Interface			🥵 Dns:fal	se 🥜 🗐
<ul> <li>NAT Rules Aff</li> </ul>	er.										
						Displavi	ng 1-1 of 1 rows	K < Page 1 of	1 > >	C Rows	per page: 100 ×

3. Konfigurieren Sie eine NAT-Ausnahmeregel. Stellen Sie sicher, dass es sich bei der Regel um eine manuelle NAT-Regel mit dem Typ "Statisch" handelt. Dies ist eine bidirektionale NAT-Regel, die auf AnyConnect-Datenverkehr angewendet wird.

Wenn die FTD anhand dieser Einstellungen Datenverkehr erkennt, der von Inside\_Net stammt und an eine AnyConnect-IP-Adresse gerichtet ist (definiert durch AnyConnect\_Pool), wird die Quelle in denselben Wert (Inside\_Net) und das Ziel in denselben Wert (AnyConnect\_Pool) umgewandelt, wenn der Datenverkehr in die Inside\_Zone eintritt und aus der Outside\_Zone austritt. Dadurch wird NAT im Wesentlichen umgangen, wenn diese Bedingungen erfüllt sind.

dd NAT Rule						
NAT Rule:	Manual NAT Rul	e 👻	Insert:	In Category	Y NAT Rules Before	
Type:	Static	<b>~</b>   (	Enable			
Description:						0
Interface Objects	Translation	PAT Pool	Advanced			~
vailable Interface Ob	ojects C		Source Inter	face Objects (1)	Destination Interface Objects (1)	
🔍 zone		×	🚠 inside-zoo	ne 🗊	and outside-zone	6
🚠 inside-zone		-				
outside-zone		Add	d to			
		Add	d to nation			
					ок с	ancel
					ок с	ancel
dd NAT Rule					ок с	ancel
dd NAT Rule	Manual NAT Rule	8 4	Insert:	In Category	OK C	ancel
dd NAT Rule	Manual NAT Rule	8	Insert:	In Category	OK C	ancel
I <mark>dd NAT Rule</mark> NAT Rule: Type:	Manual NAT Rule Static	e <b>v</b>	Insert:	In Category	OK C	ancel ?
dd NAT Rule NAT Rule: Type: Description:	Manual NAT Rule Static	e 💙	Insert: Insert	In Category	OK C	ancel ?
dd NAT Rule NAT Rule: Type: Description: Interface Objects	Manual NAT Rule Static	e V V PAT Pool	Insert: Enable Advanced	In Category	OK C	ancel ?
dd NAT Rule NAT Rule: Type: Description: nterface Objects Original Packet	Manual NAT Ruk Static Translation	e V V PAT Pool	Insert: Enable Advanced	In Category Translated Packet	OK C	ancel ?
dd NAT Rule NAT Rule: Fype: Description: Interface Objects Original Packet Original Source:*	Manual NAT Rul Static Translation	e V PAT Pool	Insert: Enable Advanced	In Category Translated Packet Translated Source:	OK C	2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2
dd NAT Rule NAT Rule: Type: Description: Interface Objects Original Packet Original Source:*	Manual NAT Ruk Static Translation	e V PAT Pool	Insert: Enable Advanced	In Category Translated Packet Translated Source:	OK C	2 ()
dd NAT Rule NAT Rule: Type: Description: Interface Objects Original Packet Original Source:*	Manual NAT Rul Static Translation Inside_Net Address	e V PAT Pool	Insert: Enable Advanced	In Category Translated Packet Translated Source:	OK C	2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2
dd NAT Rule NAT Rule: Type: Description: Interface Objects Original Packet Original Source:* Original Destination:	Manual NAT Rul Static Translation Inside_Net Address AnyConnet	e V PAT Pool	Insert: Enable Advanced	In Category Translated Packet Translated Source: Translated Destination:	OK C	ancel ? ▼ ▼ ○
dd NAT Rule NAT Rule: Type: Description: Interface Objects Original Packet Original Source:* Original Destination:	Manual NAT Rul Static Iranslation Inside_Net Address AnyConnec	PAT Pool	Insert: Enable Advanced	In Category Translated Packet Translated Source: Translated Destination:	OK     C       V     NAT Rules Before     V       Address     Inside_Net       AnyConnect_Pool	ancel ? ♥ ♥ ◎
Add NAT Rule NAT Rule: Type: Description: Interface Objects Original Packet Original Source:* Original Destination: Original Source Port:	Manual NAT Rul Static Translation Inside_Net Address AnyConnec	e V PAT Pool	Insert: Enable Advanced	In Category Translated Packet Translated Source: Translated Destination: Translated Source Port:	OK     C       V     NAT Rules Before     V       Address     Inside_Net       AnyConnect_Pool	ancel ? ✓
Add NAT Rule NAT Rule: Type: Description: Interface Objects Original Packet Original Source:* Original Destination: Original Source Port: Original Destination Po	Manual NAT Rul Static Translation Inside_Net Address AnyConnec	e V PAT Pool	Insert: Enable  Advanced  Control Contro Control Control Control Control Control Control Control Cont	In Category Translated Packet Translated Source: Translated Destination: Translated Source Port: Translated Destination Port:	OK C	ancel ? ? ♥ 0
dd NAT Rule VAT Rule: Fype: Description: Interface Objects Original Packet Original Source:* Original Destination: Original Destination Po	Manual NAT Rul Static Translation Inside_Net Address AnyConnet	e V PAT Pool	Insert: Enable  Advanced  Control Contro Control Control Control Control Control Control Control Cont	In Category Translated Packet Translated Packet Translated Destination: Translated Source Port: Translated Destination Port:	OK     C       V     NAT Rules Before     V       Address     Inside_Net       AnyConnect_Pool	ancel ? ✓
dd NAT Rule NAT Rule: Type: Description: Interface Objects Original Packet Original Source:* Original Destination: Original Source Port: Original Destination Po	Manual NAT Rul Static Translation Inside_Net Address AnyConnec	PAT Pool	Insert: Enable  Advanced  Control Con	In Category Translated Packet Translated Packet Translated Destination: Translated Source Port: Translated Destination Port:	OK     C       V     NAT Rules Before     V       Address     Inside_Net       AnyConnect_Pool	ancel ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ?

Darüber hinaus ist die FTD so konfiguriert, dass sie eine Routensuche für diesen Datenverkehr und nicht für Proxy-ARP durchführt. Klicken Sie abschließend auf **OK**.

Add NAT Rule					? ×
NAT Rule:	Manual NAT Rule	<ul> <li>Insert:</li> </ul>	In Category	▼ NAT Rules Before ▼	
Type:	Static	✓ 🗹 Enable			
Description:					$\bigcirc$
Interface Objects	Translation PAT Poo	Advanced			
Translate DNS replie	es that match this rule				
Fallthrough to Inter	face PAT(Destination Interfa	sce)			
IPv6					
Net to Net Mapping					
🗹 Do not proxy ARP o	n Destination Interface	1			
🗹 Perform Route Look	up for Destination Interface				
Unidirectional					
				ОК	Cancel

## 4. Klicken Sie auf Speichern.

C	)verview /	nalysis	Policies Devi	ices Objects	AMP I	Intelligence			Dep	iloy 🔒	System H	telp 🔻	admin 🔻
D	evice Manage	ement	NAT VPN *	QoS Platfor	m Settings	s FlexConfig	Certificates						
F	TD-2-N	AT-Poli	cy					You have a	unsaved changes [ 🗻	Show Warning	as 📙 Sa	ave	😫 Cancel
R	ules										<u>e</u> 1	Policy As	signments (
æ	Filter by Device											0	Add Rule
						Original Packe	#		Translated Packet				
*	Direction	Туре	Source Interface Obje	Destination Interface Object	Original Sources	Original Destination	Orig Is Service	Translated Sources	Translated Destinations	Trans Services	Options		
٠	NAT Rules Bef	are											
1	47	Static	🍰 inside-zone	📩 outside-zone	👼 Inside_	Net 📻 AnyConr	nect_Pool	📻 Inside_Net	AnyConnect_Po	al .	🔇 Dessfa 🍓 route-l 🍓 no-pro	ilse lookup xxy-arp	/ 6
۳	Auto NAT Rule	s											
=	+	Dynamic	🥞 any	🚠 outside-zone	📄 obj-anj	У		🍓 Interface			🝓 Dns:fa	ise	J 🕄
٠	NAT Rules Afte	r											
							Displayin	g 1-2 of 2 rows	< < Page 1 0	ri > >l	C Row	s per p	sge: 100 •

### Bereitstellen

1. Wenn die Konfiguration abgeschlossen ist, klicken Sie oben rechts auf die Schaltfläche **Bereitstellen**.



2. Aktivieren Sie das Kontrollkästchen neben dem FTD, auf das die Konfiguration angewendet wird, und klicken Sie dann auf **Bereitstellen**.

Depl	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	

Deploy

Cancel

```
Selected devices: 1
```

# Überprüfung

# Abschließende Konfiguration

### AAA-Konfiguration

```
> 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
```

#### AnyConnect-Konfiguration

```
> 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

AnyConnect verwenden und Richtlinien für die Zugriffskontrolle überprüfen

🚳 Cisco AnyCo	onnect Secu	ire Mobilit	ty Client	—		$\times$		
	VPN: Contacting ftd2.exam	ftd2.exam ple.com	ple.com.	~	Connect			
		🕙 Cisco	o AnyConne	ect   ftd2.	example.c	om		×
<b>¢</b> ()								
		_	Group:	General			~	
			Username:	it.admir	ı			
			Password:	*****	**			
					ОК		Cancel	
🔇 Cisco AnyCo	onnect Secu	ıre Mobilit	ty Client	÷		×		
	VPN: Connected	to ftd2.exa	ample.com.		Discourset			
00-00-10	Tuz,exalli	piercom		×	DISCONNECL	Du 4		
00:00:12					1	PV4		
<b>O</b> ()								

Der Benutzer IT-Administrator gehört zur Gruppe AnyConnect-Administratoren, die über RDP-Zugriff auf den Windows-Server verfügen, jedoch nicht auf HTTP zugreifen können.

Durch das Öffnen einer RDP- und Firefox-Sitzung mit diesem Server wird sichergestellt, dass dieser Benutzer nur über RDP auf den Server zugreifen kann.



Wenn der Benutzer Testbenutzer in der Gruppe AnyConnect-Benutzer angemeldet ist, die zwar HTTP-, aber keinen RDP-Zugriff haben, können wir überprüfen, ob die Regeln für die Zugriffskontrollrichtlinie wirksam werden.

Nemote Desktop Connection — 🗆 🗙	
Remote Desktop	Remote Desktop Connection ×
Tonnection	Remote Desktop can't connect to the remote computer for one of these reasons:
Computer: win2016.example.com ✓ User name: None specified You will be asked for credentials when you connect.	<ol> <li>Remote access to the server is not enabled</li> <li>The remote computer is turned off</li> <li>The remote computer is not available on the network</li> <li>Make sure the remote computer is turned on and connected to the network, and that remote access is enabled.</li> </ol>
Show Optio Connect Help	ОК Неір
IIS Windows Server X 🛠 Options	× + . – – ×
← → C û 🛛 🖉 win2016.example.com	
🕂 Windows Server	
Internet Information Serv	vices
Walcoma Biopurpup Tapustul	
Weicome Bienvenue Tervetul	

# Mit FMC-Verbindungsereignissen überprüfen

Da die Protokollierung in den Regeln der Zugriffskontrollrichtlinie aktiviert wurde, können die Verbindungsereignisse auf jeden Datenverkehr überprüft werden, der diesen Regeln entspricht

Navigieren Sie zu Analyse > Verbindungen > Ereignisse.

Overview Analys	sis Policies D	Devices Object	ts AMP	Intellige	ence		Deploy 🔒	System Help	r admin v
Context Explorer	Connections <b>v</b>	Intrusions •	Files 🔻	Hosts v	Users •	Correlation <b>v</b>	Advanced •	Search	
	Events								
	Security Intellig	ence Events							

In der **Tabellenansicht der Verbindungsereignisse** werden die Protokolle so gefiltert, dass nur Verbindungsereignisse für den IT-Administrator angezeigt werden.

Hier können Sie überprüfen, ob RDP-Datenverkehr zum Server (TCP und UDP 3389) zulässig ist, der Datenverkehr an Port 80 jedoch blockiert wird.

C	vervie	w Analysi	s Policies I	Devices Objects	AMP I	ntelligence		Depl	oy 🔒 System	Help 🔻 admin 🔻
C	ontext	Explorer C	onnections + E	vents Intrusion	ns 🔻 🛛 Files	<ul> <li>Hosts V</li> </ul>	sers • Correlatio	n • Advanced •	Search	
							Bookmark This	Page Report Designe	r Dashboard View B	iookmarks Search •
C	Conn	ection E	ents (switch	workflow)				11 202	0-05-05 14-14-17 - 2	020-05-05 16-21-14
<u>c</u>	onnectio	ins with Applicat	ion Details > Tab	le View of Connectio	n Events				000001414117-2	Expanding
٠	Search	Constraints (Ed	t Search Save Sea	irch)						Disabled Columns
ſ	Jump t	o 🔻								
_										
		Action ×	Initiator × IP	Initiator User ×		Responder × IP	Ingress × Security Zone	Egress X Security Zone	Source Port / × ICMP Type	Destination Port / × ICMP Code
	1	Action ×	Initiator × IP 10.10.10.1	Initiator User ×	\it.admin, LDA	Responder ×         IP           P1         #192.168.1.1	Ingress Security Zone ×	Egress × Security Zone	Source Port / X ICMP Type 62473 / tcp	Destination Port / × ICMP Code
		Action × Allow Block	Initiator × IP 10.10.10.1 10.10.10.1	Initiator User ×	Nit.admin, LDA) Nit.admin, LDA)	Responder ×           IP           P1           IP           IP           IP           IP	Ingress × Security Zone × outside-zone	Earess × Security Zone inside-zone inside-zone	Source Port /         ×           ICMP Type         62473 / tcp           62474 / tcp         62474 / tcp	Destination Port / × ICMP Code 3389 / tcp 80 (http) / tcp
	• • •	Action × Allow Block Block	Initiator × IP 10.10.10.1 10.10.10.1 10.10.10.1	Initiator User ×	Nit.admin, LDA) Nit.admin, LDA) Nit.admin, LDA)	Responder × IP           192.168.1.1           192.168.1.1           192.168.1.1           192.168.1.1	Ingress × Security Zone × outside-zone outside-zone	Egress × Security Zone inside-zone inside-zone	Source Port / X           ICMP Type           62473 / tcp           62474 / tcp           62475 / tcp	Destination Port / ×           ICMP Code           3389 / tcp           80 (http) / tcp           80 (http) / tcp

Für den Benutzer **Test User** können Sie überprüfen, ob der RDP-Datenverkehr zum Server blockiert und der Datenverkehr an Port 80 zulässig ist.

Ove	rview	Analysi	s Policies I	Devices	Objects	AMP	Intelligence				Deploy	y 🔍	System	Help 🔻	admin 🔻
Cont	ext Ex	plorer C	onnections + E	Events	Intrusions •	File	es 🔻 Hosts 🖲	Users •	Correla	tion 💌	Advanced •	Search			
									Bookmark	This Page	Report Designer	Dashboar	d View B	ookmarks	Search •
Conn Conn • Sea	Connection Events (switch workflow)         ionnections with Application Details > Table View of Connection Events         • Search Constraints (Edit Search Save Search)         Jump to														
		Action ×	Initiator × IP	Initiato	r User ×		Respond IP	r × In Se	uress curity Zone	× Lo	curity Zone	Source P ICMP Ty	<u>kort /</u> × pe	Destin ICMP (	ation Port / × Code
4		Block	10.10.10.1	📑 <u>test u</u>	iser (LAB-AD\te	st.user, l	LDAP) 🗐 192.16	8.1.1 out	side-zone	ins	ide-zone	<u>62493 / to</u>	12	3389 / 1	tap
4		Allow	10.10.10.1	📇 test u	iser (LAB-AD\te	st.user, l	LDAP) IS 192.16	8.1.1 out	side-zone	ins	ide-zone	<u>62494 / tr</u>	20	80 (http	<u>b) / tcp</u>

# Fehlerbehebung

# Fehlerbehebung

Dieses Debugging kann in der Diagnose-CLI ausgeführt werden, um Probleme mit der LDAP-Authentifizierung zu beheben: **debug Idap 255** 

Um Probleme mit den Richtlinien für die Benutzeridentitätssteuerung zu beheben, kann der **Systemsupport "firewall-engine-debug"** in clish ausgeführt werden, um zu bestimmen, warum der Datenverkehr unerwartet zugelassen oder blockiert wird.

#### LDAP-Debugger

```
[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
[53]
       dSCorePropagationData: value = 1601010100000.0Z
[53]
       lastLogonTimestamp: value = 132319755825875876
[53] Fiber exit Tx=515 bytes Rx=2659 bytes, status=1
[53] Session End
```

#### Verbindung zum LDAP-Server kann nicht hergestellt werden

```
[-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
```

Potenzielle Lösungen:

- Überprüfen Sie die Weiterleitung, und stellen Sie sicher, dass die FTD eine Antwort vom LDAP-Server erhält.
- Wenn LDAPS oder STARTTLS verwendet wird, stellen Sie sicher, dass das richtige Stammzertifikat der Zertifizierungsstelle vertrauenswürdig ist, damit der SSL-Handshake erfolgreich abgeschlossen werden kann.
- Vergewissern Sie sich, dass die richtige IP-Adresse und der richtige Port verwendet werden.
   Wenn ein Hostname verwendet wird, überprüfen Sie, ob DNS in der Lage ist, ihn in die richtige IP-Adresse aufzulösen.

## Ungültiger Bindungs-Anmelde-DN und/oder falsches Kennwort

```
[-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
```

Mögliche Lösung: Überprüfen Sie, ob die Anmelde-DN und das Anmelde-Kennwort richtig konfiguriert sind. Dies kann auf dem AD-Server mit **Idp.exe** überprüft werden. Gehen Sie folgendermaßen vor, um sicherzustellen, dass ein Konto erfolgreich über Idp gebunden werden kann:

1. Drücken Sie auf dem AD-Server Win+R, und suchen Sie nach Idp.exe.

🗐 Run	×
Ø	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. Wählen Sie unter Verbindung die Option Verbinden...



3. Geben Sie localhost für den Server und den entsprechenden Port an, und klicken Sie dann auf OK.

Connect		×
Server:	localhost	
Port:	389	Connectionless
<u>0</u> K		<u>C</u> ancel

4. Die rechte Spalte zeigt Text an, der auf eine erfolgreiche Verbindung hinweist. Navigieren Sie zu **Verbindung > Binden...** 

🔝 Idap://w	in2016.exa	mple.co	om/DC:	example,DC=	=com		_		$\times$
Connection	Browse	View	Optio	ns Utilities	Help				
Connec	:t			ld = ldap_op Established	en("localho connection	st", 389); to localhost.			^
Bind		Ctrl+B		Retrieving b	ase DSA in	formation			
Discon	nect			Getting 1 en Dn: (RootD	tries: SE)				
New		Ctrl+N		configur CN=	rationNamin •Configurat	igContext: ion,DC=examp	le,DC=c	om;	- 1
Save				current	Fime: 5/1/20	020 4:16:55 PM	I Eastern	n Daylight	
Save As	;			Time defaulth	e; laminoCont	ext: DC=exam	nle DC=c	om:	
Exit				dnsHos domain(	tName: win ControllerFu	2016.example inctionality: 7 =	.com; = ( WIN2(	016 );	
				domainF deServi	unctionality	y: 7 = ( WIN201	16 );		
				Sett	tings,CN=W t-Site-	/IN2016,CN=Se	ervers,C	N=Default-	
				Nan com	ne,CN=Site: 1;	s,CN=Configur	ation,DC	=example,	,DC=
				forestFi	inctionality	7 = ( WIN201	6);		
				highest	CommittedU	SN: 13410;			
				isGlobal	CatalogRea	ady: TRUE;			
				IdanSer	viceName	example comit	win2016		$\checkmark$

5. Wählen Sie **Simple Bind** und geben Sie dann den **Benutzernamen** und das **Passwort** des **Verzeichniskontos an**. Klicken Sie auf **OK**.

Bind ×								
<u>U</u> ser: <u>P</u> assword:	ftd.admin@example.com							
Domain: Bind type Bind as currently logged on user Bind with credentials Simple bind Advanced (DIGEST)								
Encrypt traffic after bind       Advanced       Cancel								

Bei erfolgreicher Bindung wird ldp Authentifiziert als: DOMÄNE\Benutzername

🔝 Idap://w	in2016.exa	mple.co	om/DC=ex	ample,DC	=com		_		×	<
Connection	Browse	View	Options	Utilities	Help					
				1.2. 1.2. 1.2. support Max Max Max Max Max Max Max Support support SPN	840.11355 840.11355 840.11355 edLDAPPol PercentDir ReceiveBu Connection BatchRetu DirSyncDu ResultSets ResultSets ValRange; eadMemory edLDAPVe edSASLMe IEGO; EXTE	5.1.4.2255; 5.1.4.2256; 5.1.4.2309; icies (20): Ma SyncReques iffer; InitRecu Is; MaxConn rnMessages ration; MaxT Size; MinResu PerConn; Ma MaxValRang Limit; Syster rsion (2): 3; 3 chanisms (4 RNAL; DIGE	axPoolThr its; MaxDa vTimeout; IdleTime; I ; MaxQue empTable ultSets; axNotifical geTransiti nMemoryL 2; ): GSSAP ST-MD5;	eads; atagramR MaxPage ryDuratio Size; tionPerCo ve; LimitPerce	ecv; Size; n; n; nt;	^
				es = Idap_s unavailable uthenticate	simple_bind >>); // v.3 ed as: 'EXA	_s(ld, 'ftd.ad MPLE\ftd.ad	min@exa min'.	mple.com	ί,	>
Ready										

Ein Versuch, eine Bindung mit einem ungültigen Benutzernamen oder Kennwort herzustellen, führt zu einem Fehler wie den beiden hier gezeigten.

🔝 Idap://win2016.example.com/DC=example,DC=com — 🗆 🗙								×	
Connection	Browse	View	Options	Utilities	Help				
				MaxResultSetSize; MinResultSets; MaxResultSetsPerConn; MaxNotificationPerConn; MaxValRange; MaxValRangeTransitive; ThreadMemoryLimit; SystemMemoryLimitPercent; supportedLDAPVersion (2): 3; 2; supportedSASLMechanisms (4): GSSAPI; GSS- SPNEGO; EXTERNAL; DIGEST-MD5; 					
			r K E S C E ir	es = Idap_s sunavailable rror <49>: I server error comment: Ac rror 0x8009 nvalid	imple_bind_ i>); // v.3 idap_simple_ :: 80090308: cceptSecuri 90308 The to	s(Id, 'wrong _bind_s() fai : LdapErr: DS tyContext er oken supplie	@exampl iled: Invali SID-0C09( ror, data d to the fi	le.com', d Credentia 042A, 52e, v3839 unction is	s V
Ready									

## LDAP-Server konnte den Benutzernamen nicht finden

```
[-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
```

Mögliche Lösung: Vergewissern Sie sich, dass AD den Benutzer mit der vom FTD durchgeführten Suche finden kann. Dies kann auch mit **Idp.exe** durchgeführt werden.

1. Navigieren Sie nach dem erfolgreichen Binden (siehe oben) zu Ansicht > Baum.

Idap://win2016.example.com/DC=example,DC=com								×			
Connection Brow	vse Vie	w Options	Utilities	Help							
		Tree			Ctrl+T			^			
		Enterprise	Configurat	AaxPoolT sts: Max	hreads; Dataorami	Recv:					
	$\checkmark$	Status Bar				vTimeou	t;	0			
		Set Font				s; MaxQu	nldleTime; MaxPageSize s; MaxQueryDuration;				
MaxDirSyncDuration; MaxTempTableSize; MaxResultSetSize; MinResultSets; MaxResultSetsPerConn; MaxNotificationPerCo MaxValRange; MaxValRangeTransitive; ThreadMemoryLimit; SystemMemoryLimitPerce supportedLDAPVersion (2): 3; 2; supportedSASLMechanisms (4): GSSAPI; GSS- SPNEGO; EXTERNAL; DIGEST-MD5;						onn; ent; n',					
<unavailable>); // v.3 Authenticated as: 'EXAMPLE\ftd.admin'.</unavailable>							,				
		[ '						~			

2. Geben Sie die auf dem FTD konfigurierte Basis-DN an, und klicken Sie dann auf  $\mathbf{O}\mathbf{K}$ 

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

3. Klicken Sie mit der rechten Maustaste auf die Basis-DN, und klicken Sie dann auf Suchen.

Idap://win2016.example.com/DC=example,DC=com								_		Х	
Connection	Browse	View	Options	Utilities	Help						
<u> </u>	ple,DC=c	om	Search Virtual L Delete Modify Modify Add chil Compar Advance	ist View DN Id e ed	Ctrl+S Ctrl+D Ctrl+M Ctrl+R Ctrl+A	ci 11 =6 51 51 51 51 51 51 51 51 51 51 51 51 51	pals,DC ID2B9A example 1D2970 xample 1D1AD0 example 1D1AD0 e,DC=co 1D1AA DC=exa 1D1AD0 1D1AD0 1D1AD0 1D1AD0 DC=cor	=examp A00C0 pDC=co C400C0 pDC=co ED00C0 e,DC=co ED00C0 om; 4B00C0 om; 4B00C0 cm; ED00C0 cm; ED00C0	ple,DC=ci 4F79F80: m; 4FD8D50 m; 4FD8D50 om; 4FD8D50 04FD7D83 C=com; 4FD8D50 04FD8D50	om; 5:CN CD:C CD:C CD:C SA:O CD:C	^
		Copy Select al Clear ou	l Itput	Ctrl+C Ctrl+N	2	0 3:43:59 PM Eastern Daylig 2:41:57 PM Eastern Dayligh			rlight ight	,	
Create a new o	document										

4. Geben Sie die gleichen Werte für **Basisdatenbank**, **Filter** und **Bereich** an, wie sie in den Debugs angezeigt werden.

In diesem Beispiel sind dies:

- Basis-DN: dc=beispiel,dc=com
- Filter: samaccountname=it.admi
- Umfang: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 findet 0 Einträge, da es kein Benutzerkonto mit dem samaccountnamen **it.admi** unter der Basis-DN dc=beispiel,dc=com gibt

Ein weiterer Versuch mit dem richtigen samaccountname **it.admin** zeigt ein anderes Ergebnis an. Idp findet 1 Eintrag unter der Basis-DN dc=example,dc=com und druckt diese Benutzer-DN aus.

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

#### Falsches Kennwort für den Benutzernamen

```
[-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
```

Potenzielle Lösung: Vergewissern Sie sich, dass das Benutzerkennwort richtig konfiguriert ist und nicht abgelaufen ist. Ähnlich wie bei der Anmelde-DN führt die FTD eine Bindung mit AD mit den Benutzeranmeldeinformationen durch.

Diese Bindung kann auch in ldp durchgeführt werden, um zu überprüfen, ob das AD denselben Benutzernamen und dasselbe Kennwort erkennen kann. Die Schritte in ldp werden im Abschnitt **Ungültiger Binding Login DN und/oder falsches Kennwort** angezeigt.

Darüber hinaus können die Protokolle der Microsoft Server-**Ereignisanzeige** auf einen möglichen Grund hin überprüft werden.

## AAA testen

Der Befehl test **aaa-server** kann verwendet werden, um einen Authentifizierungsversuch durch die FTD mit einem bestimmten Benutzernamen und Kennwort zu simulieren. Dies kann zum Testen von Verbindungs- oder Authentifizierungsfehlern verwendet werden. Der Befehl lautet **test aaa-server authentication [AAA-server] host [AD IP/hostname]** 

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

# Paketerfassung

Paketerfassungen können verwendet werden, um die Erreichbarkeit zum AD-Server zu überprüfen. Wenn LDAP-Pakete den FTD verlassen, aber keine Antwort erhalten, kann dies auf ein Routing-Problem hinweisen.

Capture zeigt den bidirektionalen LDAP-Datenverkehr an.

```
> 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
```

# Windows Server-Ereignisanzeige - Protokolle

Die Protokolle der **Ereignisanzeige** auf dem AD-Server können detailliertere Informationen darüber bereitstellen, warum ein Fehler aufgetreten ist.

1. Suchen Sie nach der Ereignisanzeige, und öffnen Sie sie.

=	Best match								
ŵ	Event Viewer Desktop app								
	Settings >								
	🖄 View ever	nt logs							
٢	ē ô	ß		2	œ	រុក			
	event								
	ρD	e		1	2	8			

2. Erweitern Sie **Windows-Protokolle**, und klicken Sie auf **Sicherheit**. Suchen Sie mit dem Benutzernamen nach **Audit Failures** (**Überwachungsfehler**), und überprüfen Sie die Fehlerinformationen.


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

## Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.