

Configurar autenticação do AD (LDAP) e identidade do usuário no FTD gerenciado pelo FMC para clientes AnyConnect

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Diagrama e cenário de rede](#)

[Configurações do Active Directory](#)

[Determinar o DN de base e o DN do grupo do LDAP](#)

[Criar uma conta FTD](#)

[Criar grupos do AD e adicionar usuários aos grupos do AD \(opcional\)](#)

[Copiar a raiz do certificado SSL do LDAPS \(necessário apenas para LDAPS ou STARTTLS\)](#)

[Configurações do FMC](#)

[Verificar licenciamento](#)

[Configurar realm](#)

[Configurar AnyConnect para autenticação do AD](#)

[Ativar política de identidade e configurar políticas de segurança para identidade do usuário](#)

[Configurar isenção de NAT](#)

[Implantar](#)

[Verificar](#)

[Configuração final](#)

[Configuração do AAA](#)

[Configuração do AnyConnect](#)

[Conectar-se ao AnyConnect e verificar regras de política de controle de acesso](#)

[Verificar com eventos de conexão do FMC](#)

[Troubleshoot](#)

[Debugs](#)

[Como trabalhar com as depurações do LDAP](#)

[Não é possível estabelecer uma conexão com o servidor LDAP](#)

[DN de login de vinculação incorreto e/ou senha incorreta](#)

[O servidor LDAP não consegue encontrar o nome de usuário](#)

[Senha incorreta para o nome de usuário](#)

[AAA de teste](#)

[Capturas de pacotes](#)

[Registros do visualizador de eventos do Windows Server](#)

Introduction

Este documento descreve como configurar a autenticação do AD para clientes do AnyConnect que se conectam ao Cisco Firepower Threat Defense (FTD).

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento básico da configuração de RA VPN no FMC
- Conhecimento básico da configuração do servidor LDAP no FMC
- Conhecimento básico do **Active Directory (AD)**

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Microsoft 2016 Server
- FMCv executando 6.5.0
- FTDv executando 6.5.0

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Este documento descreve como configurar a autenticação do Active Directory (AD) para clientes AnyConnect que se conectam ao Cisco Firepower Threat Defense (FTD), gerenciado pelo Firepower Management Center (FMC).

A identidade do usuário é usada nas políticas de acesso para restringir os usuários de AnyConnect a endereços IP e portas específicos.

Configurar

Diagrama e cenário de rede



O Windows Server é pré-configurado com IIS e RDP para testar a identidade do usuário. Neste

guia de configuração, três contas de usuário e dois grupos são criados.

Contas do usuário:

- FTD Admin: Usado como a conta de diretório para permitir que o FTD se vincule ao servidor do Active Directory.
- Administrador de TI: uma conta de administrador de teste usada para demonstrar a identidade do usuário.
- Usuário de teste: uma conta de usuário de teste usada para demonstrar a identidade do usuário.

Grupos:

- Administradores do AnyConnect: um grupo de teste que o administrador de TI adiciona para demonstrar a identidade do usuário. Esse grupo só tem acesso RDP ao Windows Server.
- Usuários do AnyConnect: um grupo de teste em que o usuário de teste é adicionado para demonstrar a identidade do usuário. Esse grupo só tem acesso HTTP ao Windows Server.

Configurações do Active Directory

Para configurar adequadamente a autenticação do AD e a identidade do usuário no FTD, alguns valores são necessários.

Todos esses detalhes devem ser criados ou coletados no Microsoft Server, antes que a configuração seja feita no FMC. Os principais valores são:

- **Nome de domínio:**

Este é o nome de domínio do servidor. Neste guia de configuração, `example.com` é o nome de domínio.

- **Endereço IP/FQDN do servidor:**

O endereço IP ou FQDN usado para acessar o Microsoft Server. Se um FQDN for usado, um servidor DNS deverá ser configurado no FMC e no FTD para resolver o FQDN.

Neste guia de configuração, esse valor é `win2016.example.com` (que resolve para `192.168.1.1`).

- **Porta do servidor:**

A porta usada pelo serviço LDAP. Por padrão, LDAP e STARTTLS usam a porta TCP 389 para LDAP, e LDAP sobre SSL (LDAPS) usa a porta TCP 636.

- **CA raiz:**

Se LDAPS ou STARTTLS for usado, a CA raiz usada para assinar o certificado SSL usado por LDAPS será necessária.

- **Nome de usuário e senha do diretório:**

Esta é a conta usada pelo FMC e pelo FTD para vincular-se ao servidor LDAP, autenticar usuários e procurar usuários e grupos.

Uma conta denominada Administrador de FTD é criada para essa finalidade.

- **Nome distinto (DN) de base e de grupo:**

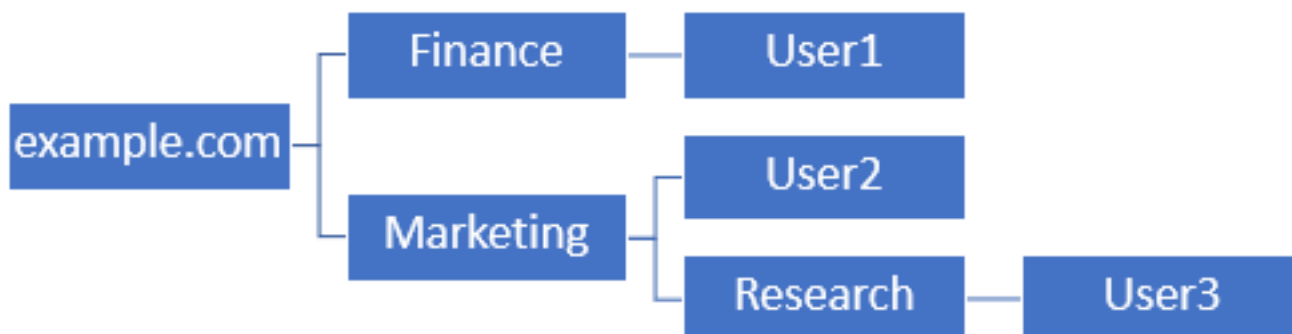
O DN de base é o ponto de partida que o FMC e o FTD informam ao Active Directory para iniciar a pesquisa e autenticar os usuários.

Da mesma forma, o DN de grupo é o ponto de partida que o FMC informa ao Active Directory onde começar a procurar grupos para identidade do usuário.

Neste guia de configuração, o domínio raiz `example.com` é usado como DN base e DN de grupo.

No entanto, para um ambiente de produção, é melhor usar um **DN base** e **DN de grupo** mais adiante na hierarquia LDAP.

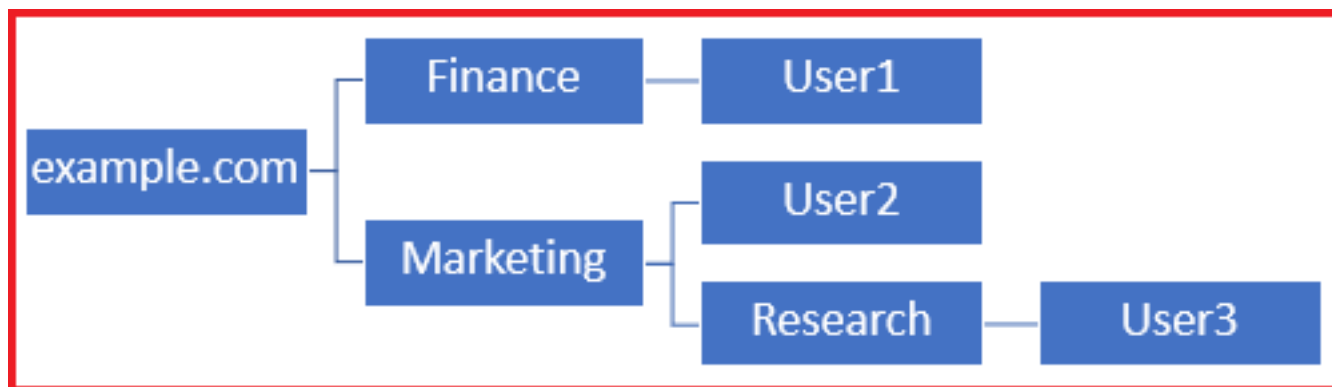
Por exemplo, esta hierarquia LDAP:



Se um administrador deseja que os usuários na unidade organizacional **Marketing** possam autenticar o DN base, ele pode ser definido como a raiz (`example.com`).

No entanto, isso também permite que o Usuário1 na unidade organizacional **Finance** também faça login, uma vez que a pesquisa do usuário começa na raiz e vá para **Finance, Marketing e Research**.

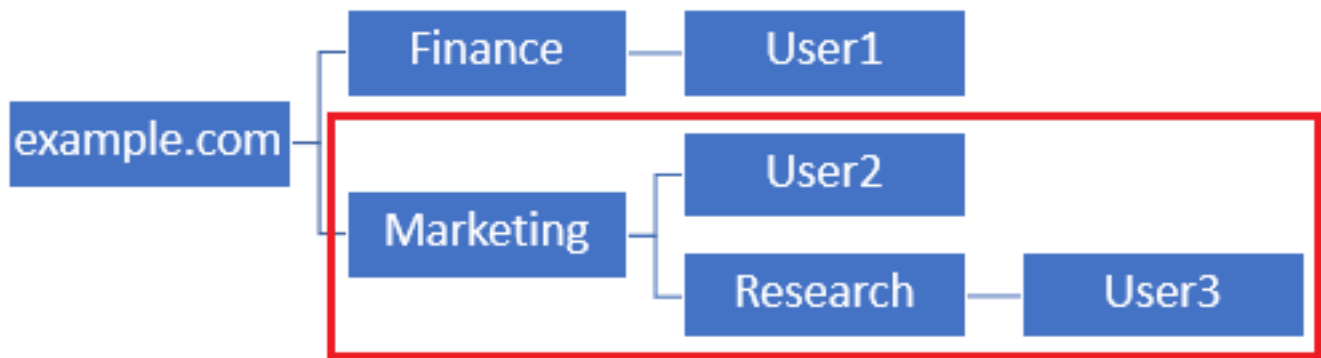
DN de base definido como `example.com`



Para restringir os logins ao único usuário na unidade organizacional de marketing e abaixo, o administrador pode definir o DN de base como `marketing`.

Agora, apenas `User2` e `User3` podem ser autenticados, pois a pesquisa começa em `marketing`.

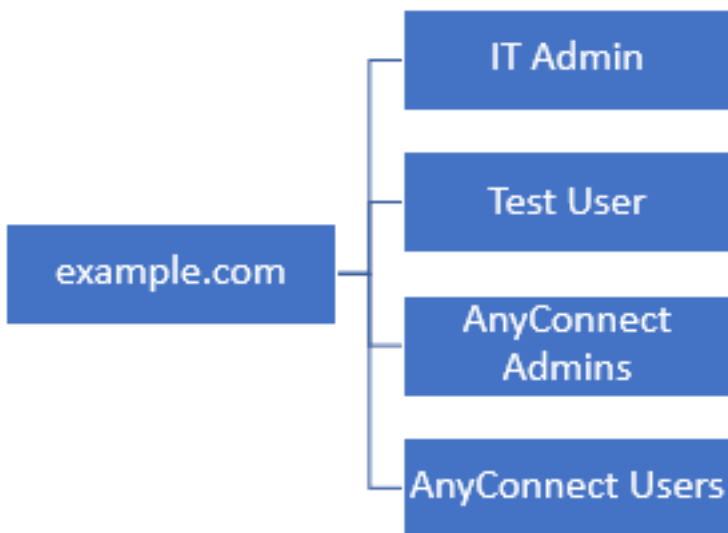
DN de base definido como `marketing`



Observe que, para um controle mais granular no FTD, para o qual os usuários têm permissão para se conectar ou atribuir autorizações diferentes a usuários de acordo com os atributos do AD, um mapa de autorização LDAP precisa ser configurado.

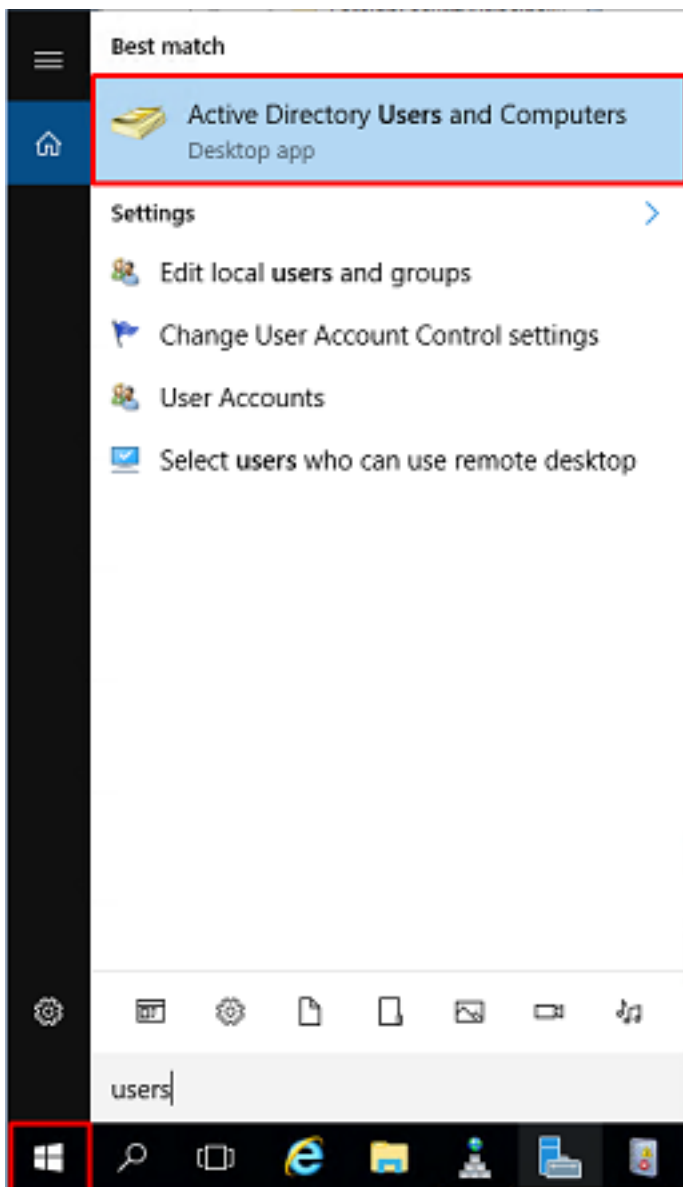
Mais informações sobre isso podem ser encontradas aqui: [Configure o mapeamento LDAP do AnyConnect no Firepower Threat Defense \(FTD\)](#).

Essa hierarquia LDAP simplificada é usada neste guia de configuração e o DN da raiz example.com é usado para o DN de base e o DN de grupo.

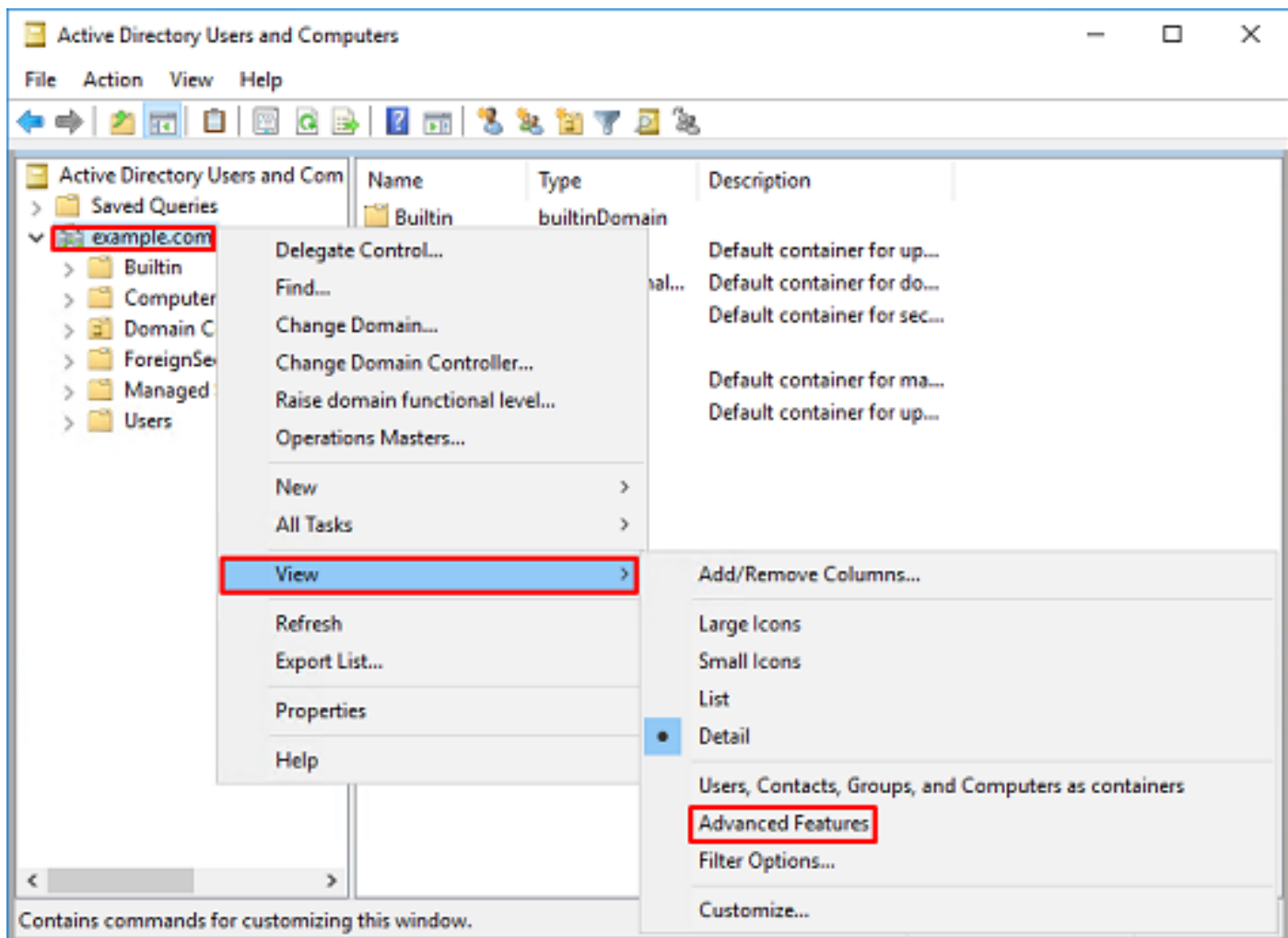


Determinar o DN de base e o DN do grupo do LDAP

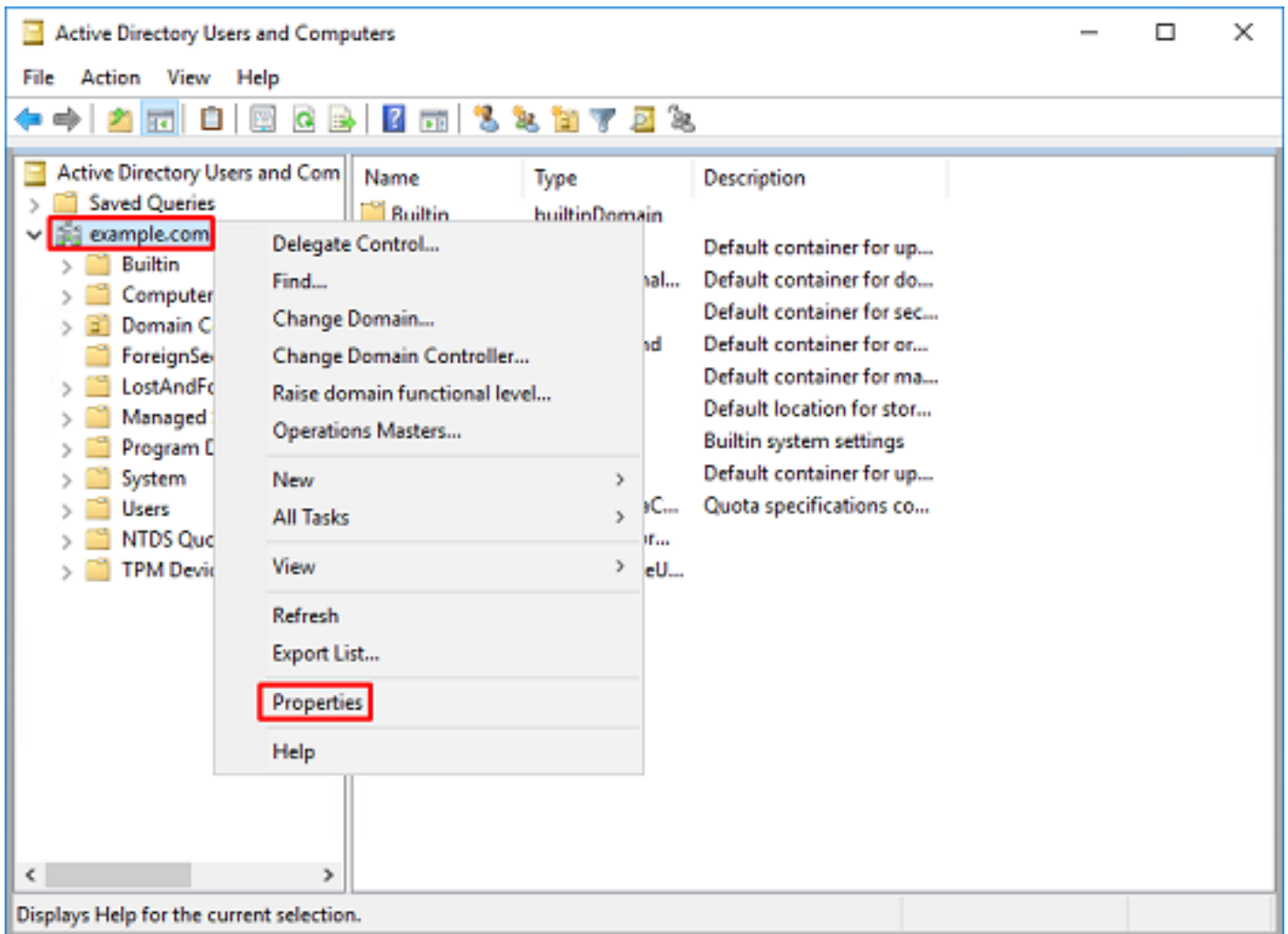
1. Abra **Usuários e Computadores** do Ative Directory.



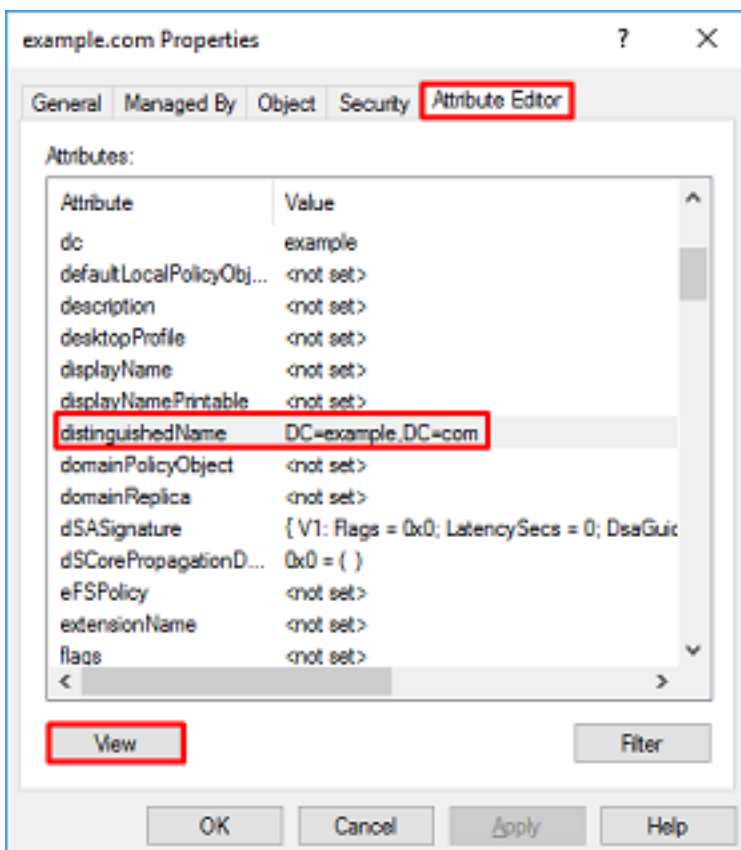
2. Clique com o botão esquerdo do mouse em **domínio raiz** (para abrir o contêiner), clique com o botão direito do mouse no **domínio raiz** e, em **Exibir**, clique em **Recursos avançados**.



3. Isso permite a exibição de propriedades adicionais sob os objetos do AD. Por exemplo, para localizar o DN da raiz example.com, clique com o botão direito do mouse em example.com e escolha **Properties**.

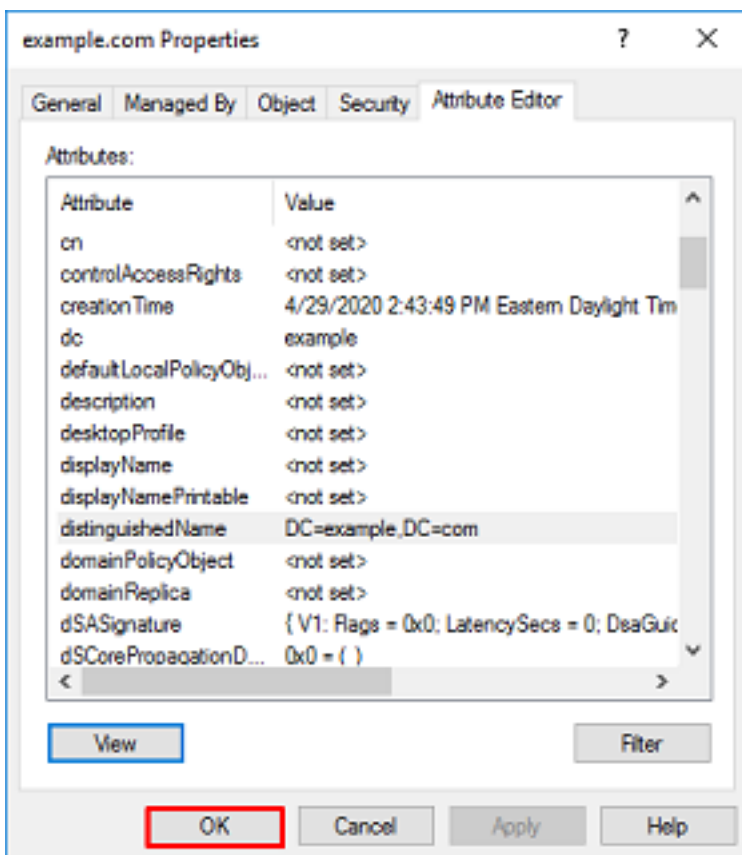
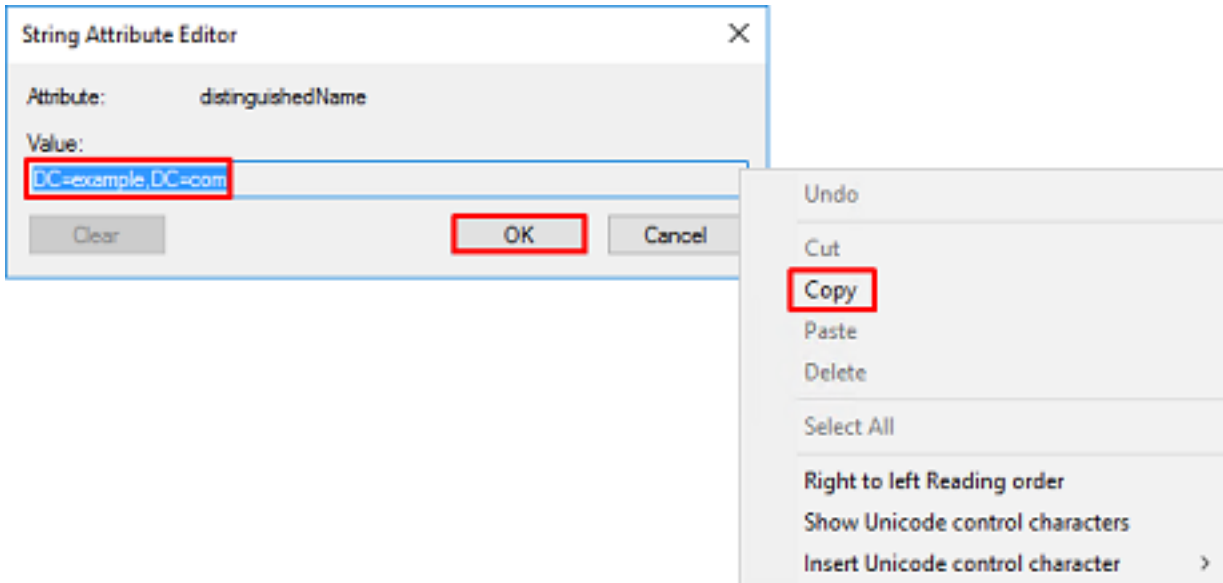


4. Em **Propriedades**, selecione a guia **Editor de Atributos**. Localize **distinguishedName** sob os **Atributos** e clique em **Exibir**.

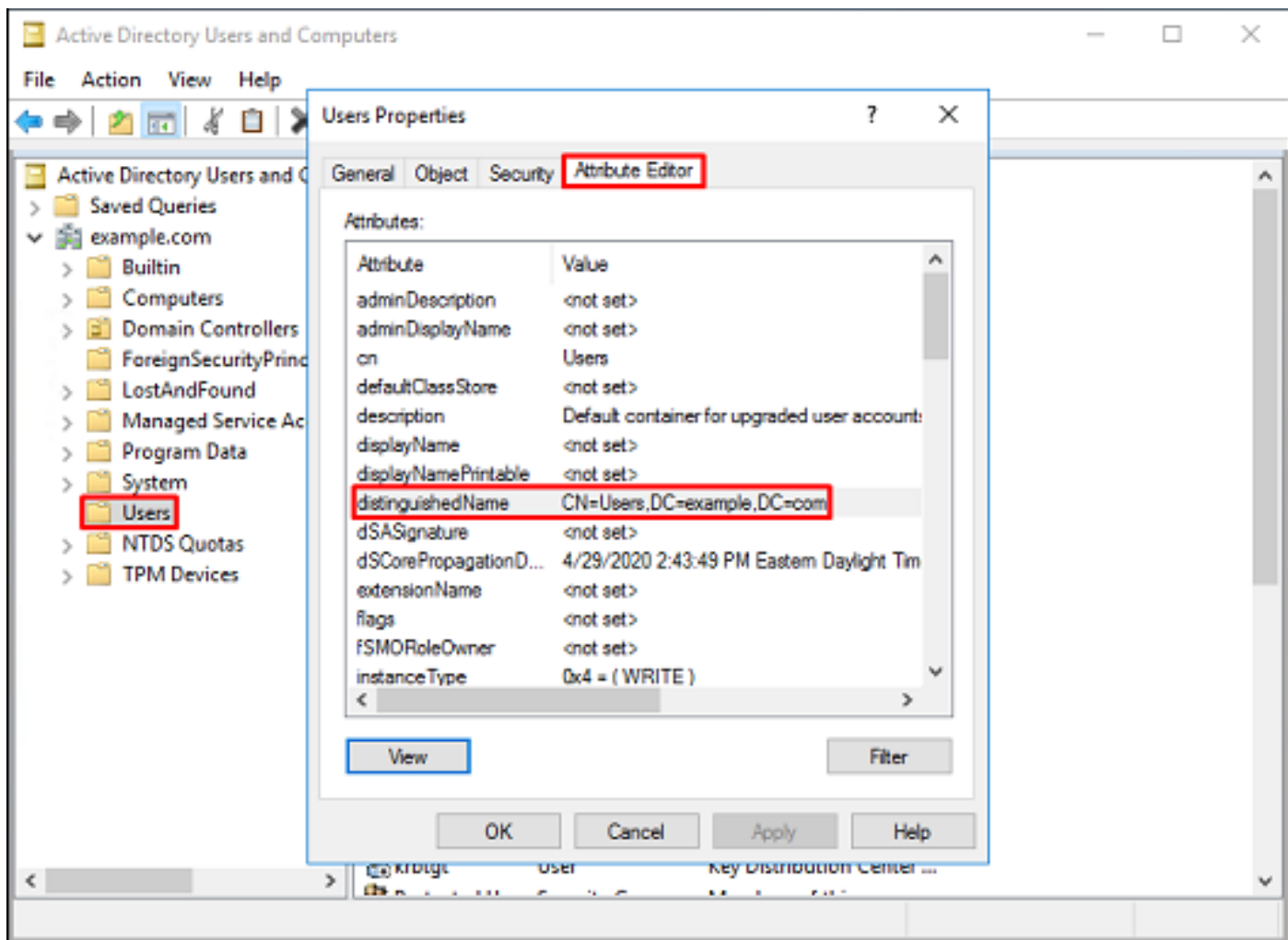


5. Isso abre uma nova janela onde o DN pode ser copiado e colado no FMC posteriormente. Neste exemplo, o DN raiz é DC=example,DC=com.

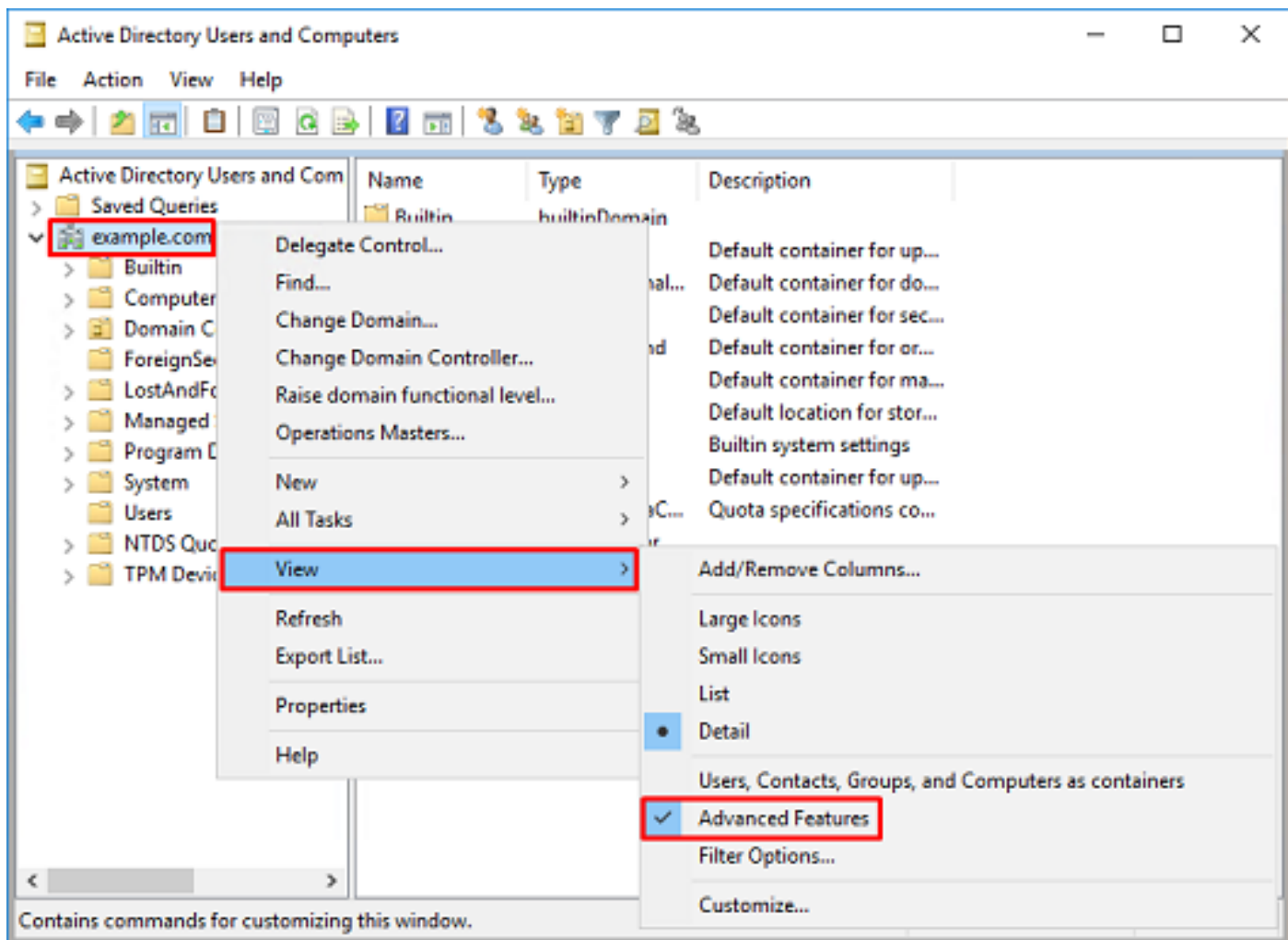
Copie o valor e salve-o para mais tarde. Clique em **OK** para sair da janela Editor de atributos de string e clique em OK novamente para sair das Propriedades.



Essa ação pode ser feita para vários objetos no Active Directory. Por exemplo, estas etapas são usadas para encontrar o DN do contêiner Usuário:



6. A view **Advanced Features** pode ser removida clicando com o botão direito do mouse no DN raiz novamente e, em **View**, clique em **Advanced Features** mais uma vez.



Criar uma conta FTD

Esta conta de usuário permite que o FMC e o FTD sejam vinculados ao Active Directory para procurar usuários e grupos e autenticar usuários.

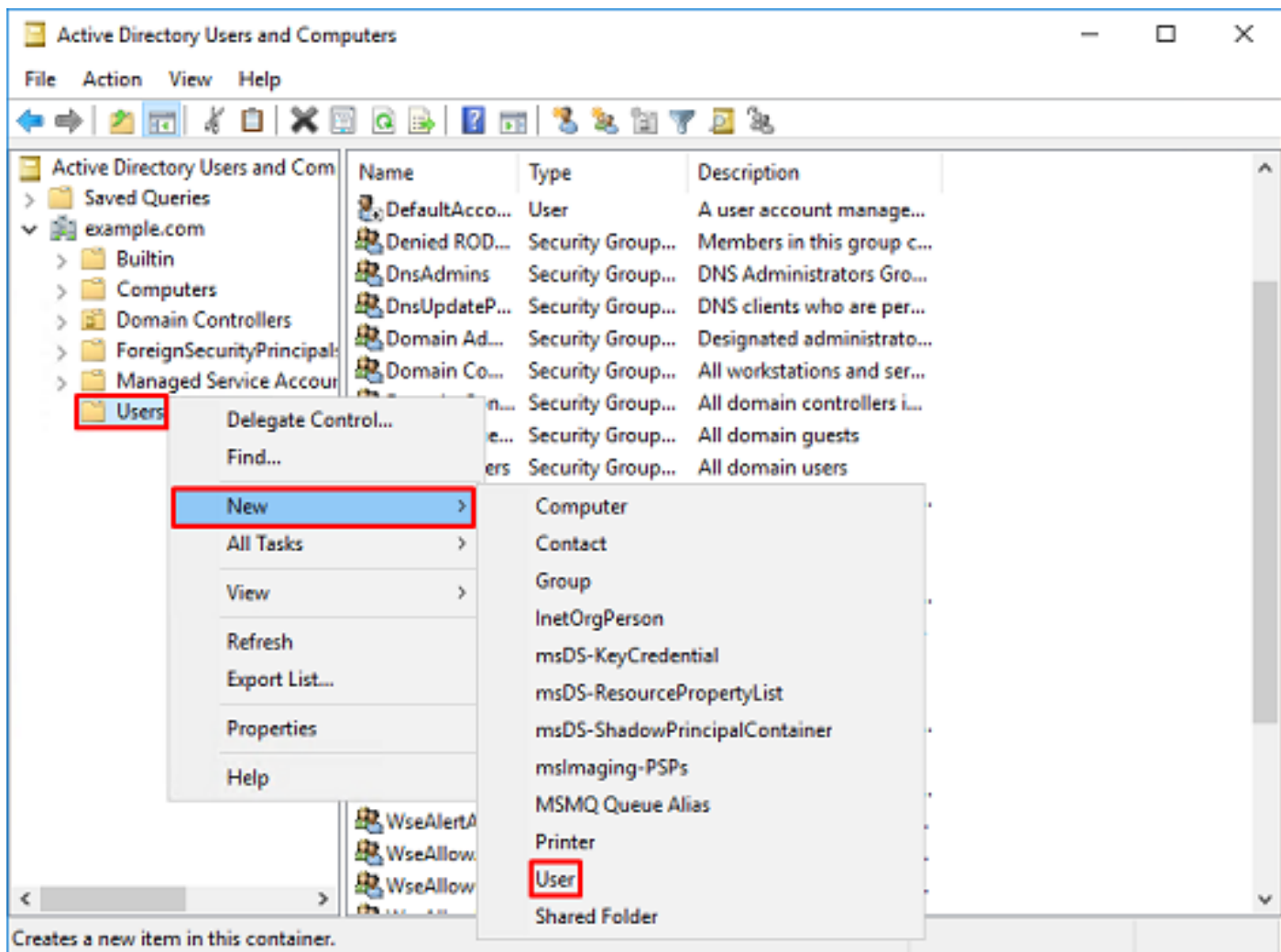
O objetivo de criar uma conta FTD separada é evitar o acesso não autorizado em outro lugar na rede, caso as credenciais usadas para vinculação sejam comprometidas.

Essa conta não precisa estar no escopo do DN de base ou do DN de grupo.

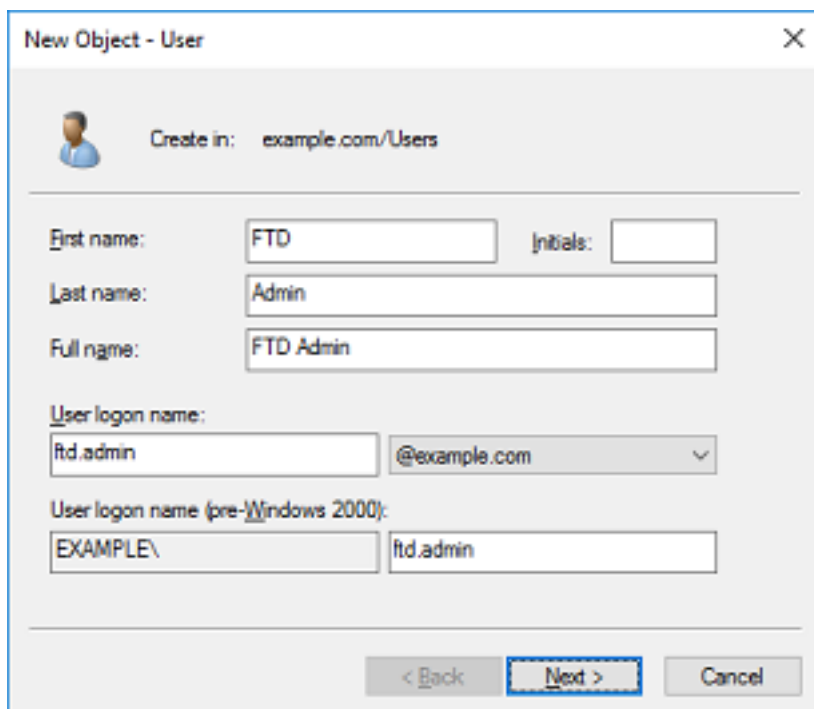
1. Em **Usuários e Computadores do Ative Diretory**, clique com o botão direito do mouse no contêiner/organizacional ao qual a conta FTD é adicionada.

Nessa configuração, a conta FTD é adicionada no contêiner Usuários com o nome de usuário `ftd.admin@example.com`.

Clique com o botão direito do mouse em Usuários e navegue até **Novo > Usuário**.



2. Percorra o Assistente de Novo Objeto - Usuário.



New Object - User

Create in: example.com/Users

Password:

Confirm password:

User must change password at next logon

User cannot change password

Password never expires

Account is disabled

< Back Next > Cancel

New Object - User

Create in: example.com/Users

When you click Finish, the following object will be created:

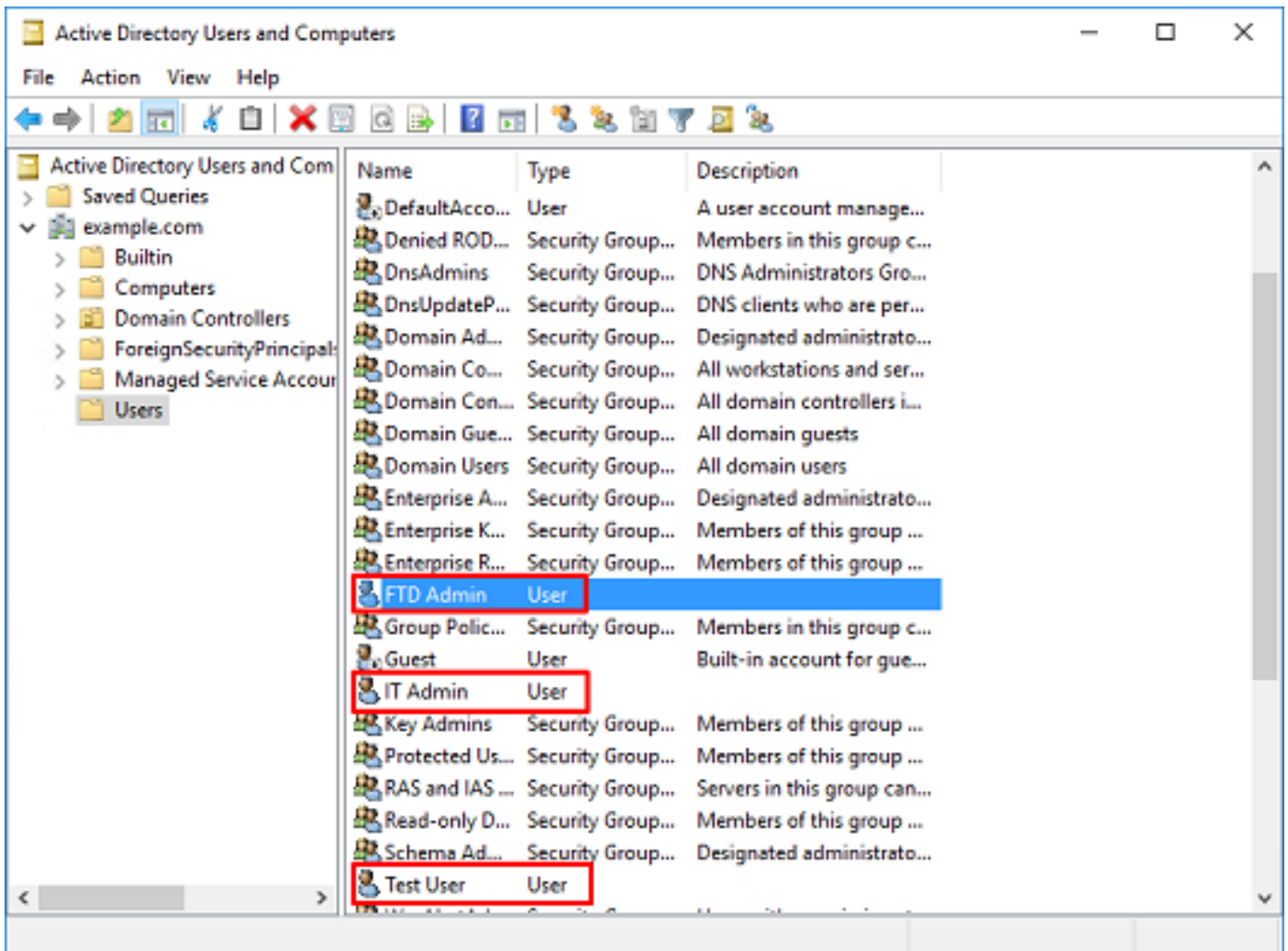
Full name: FTD Admin

User logon name: ftd.admin@example.com

The password never expires.

< Back Finish Cancel

3. Verifique se a **conta FTD** foi criada. Duas contas adicionais são criadas: **administrador de TI** e **usuário de teste**.



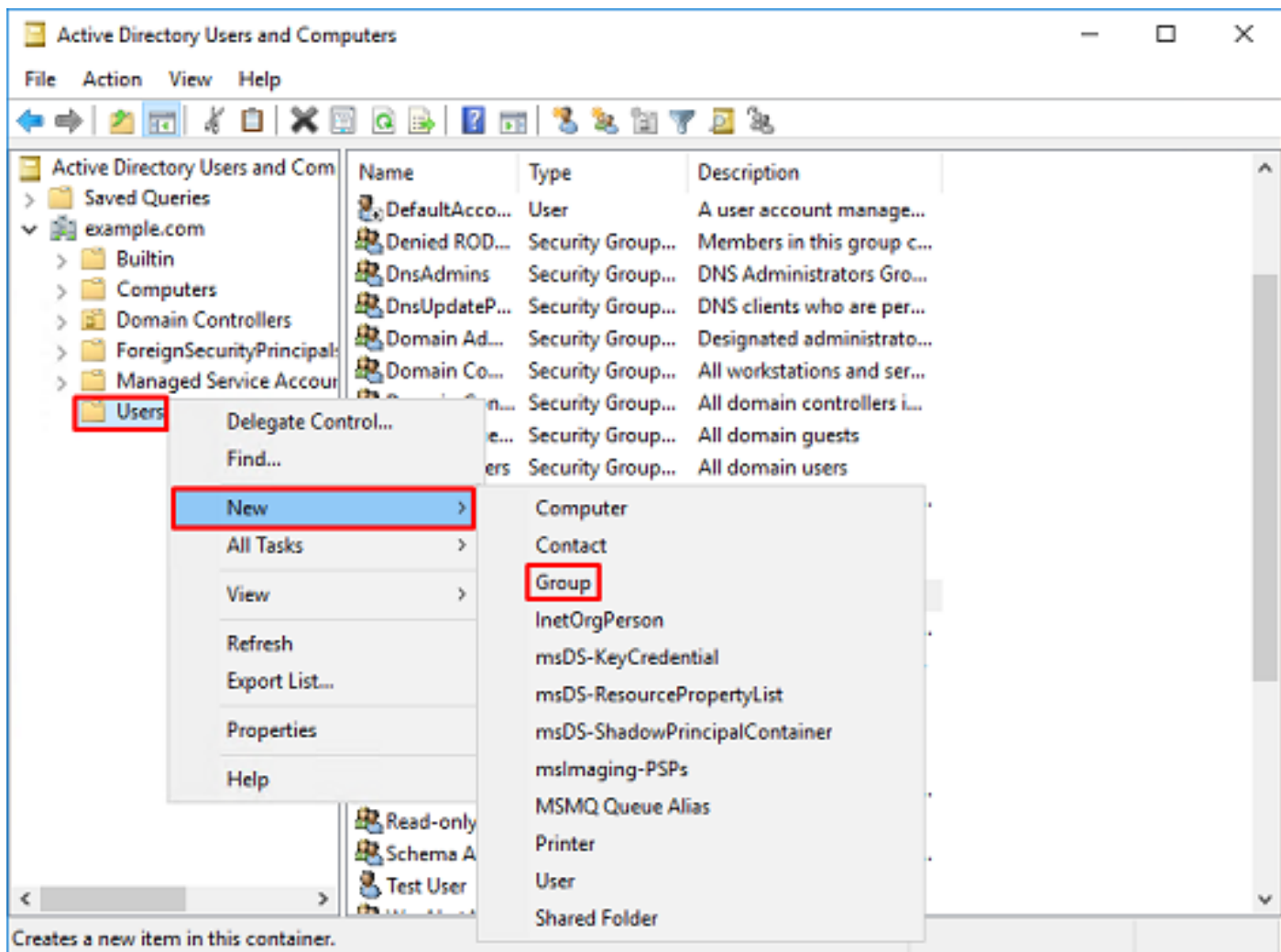
Criar grupos do AD e adicionar usuários aos grupos do AD (opcional)

Embora não sejam necessários para autenticação, os grupos podem ser usados para facilitar a aplicação de políticas de acesso a vários usuários, bem como a autorização LDAP.

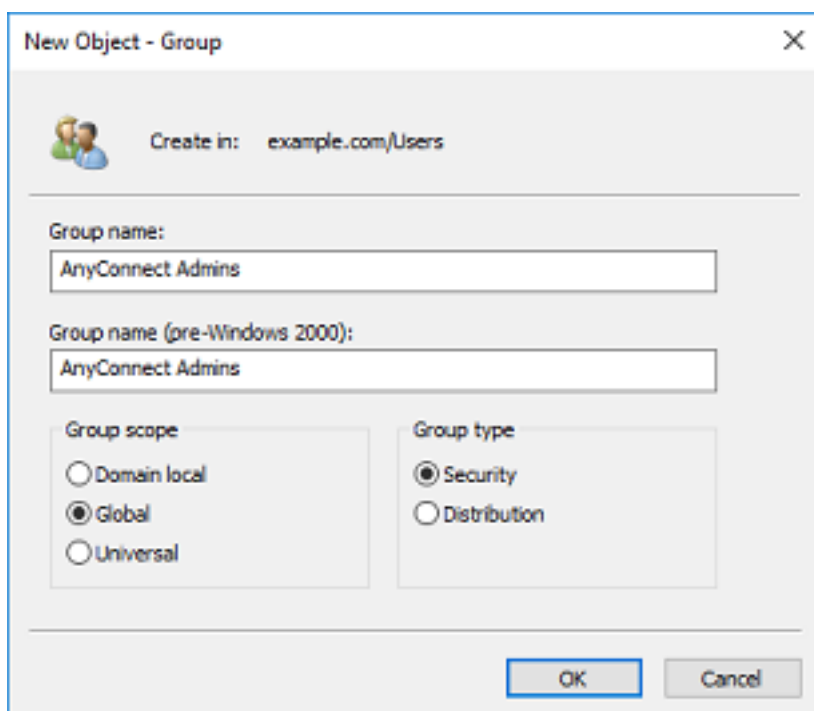
Neste guia de configuração, os grupos são usados para aplicar configurações de política de controle de acesso posteriormente usando a identidade do usuário no FMC.

1. Em **Usuários e Computadores do Active Directory**, clique com o botão direito do mouse no contêiner ou na unidade organizacional à qual o novo grupo será adicionado.

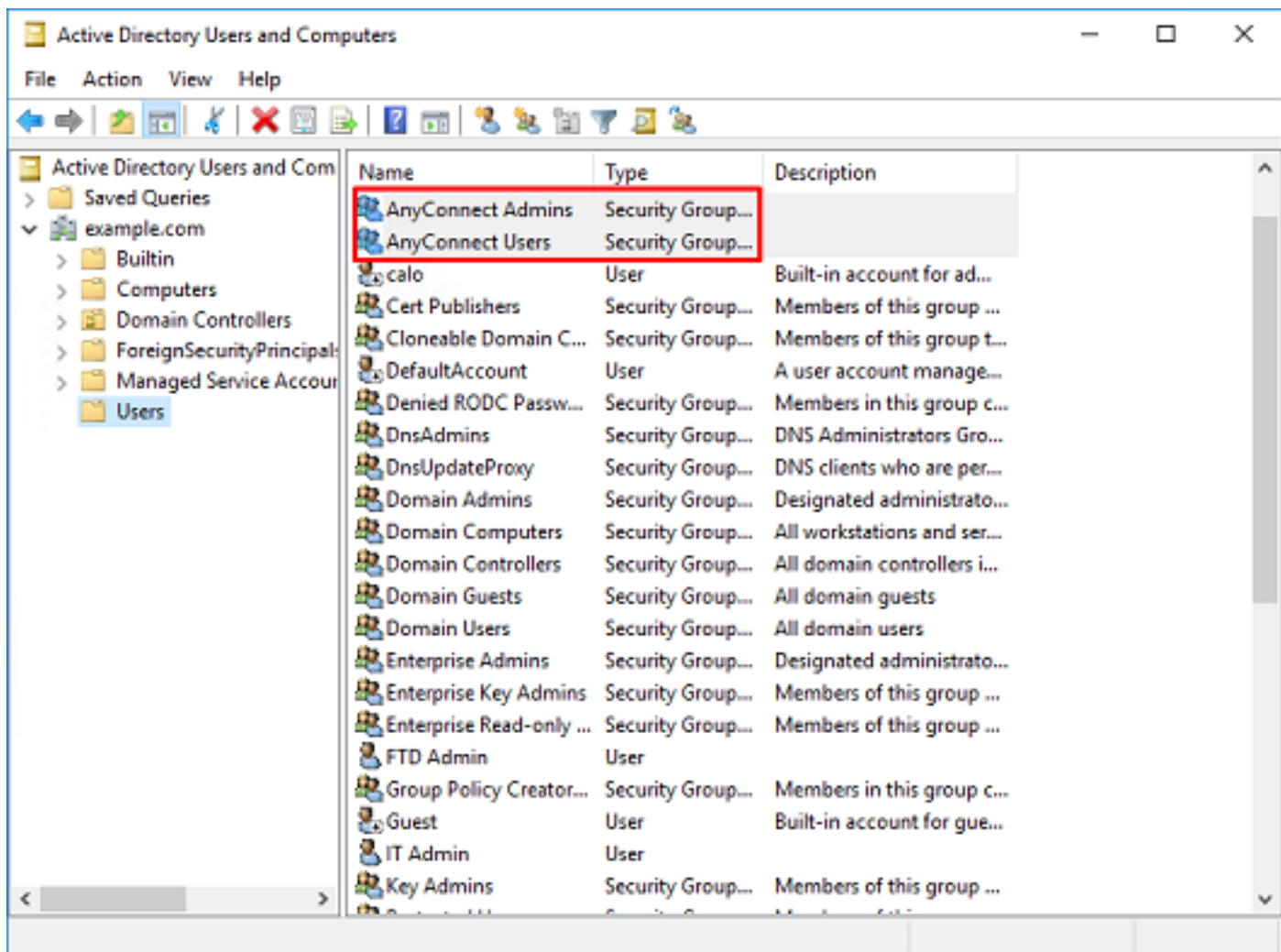
Neste exemplo, o grupo Administradores de AnyConnect é adicionado ao contêiner Usuários. Clique com o botão direito do mouse em **Usuários** e navegue até **Novo > Grupo**.



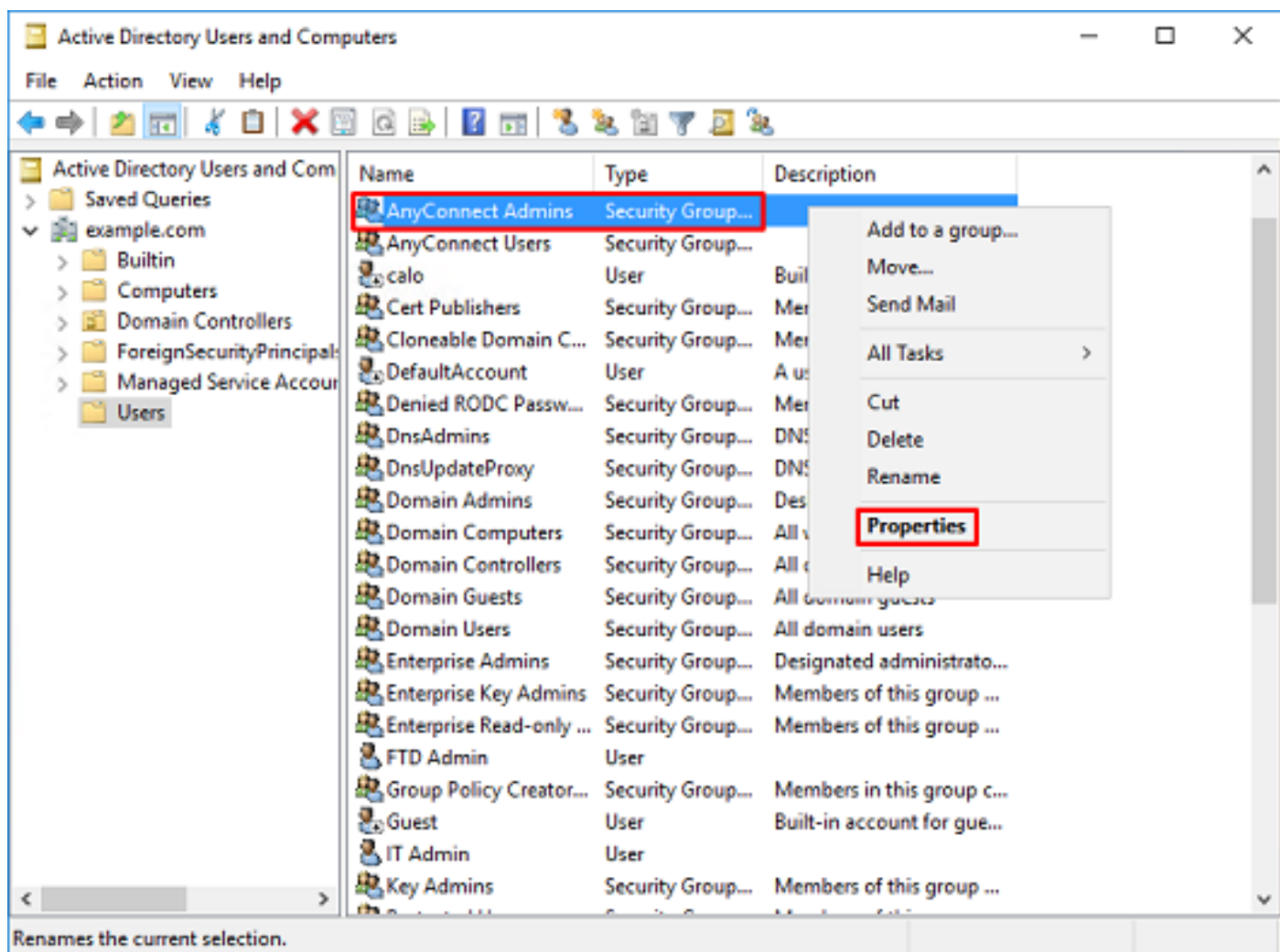
2. Vá para o Assistente de Novo Objeto - Grupo.



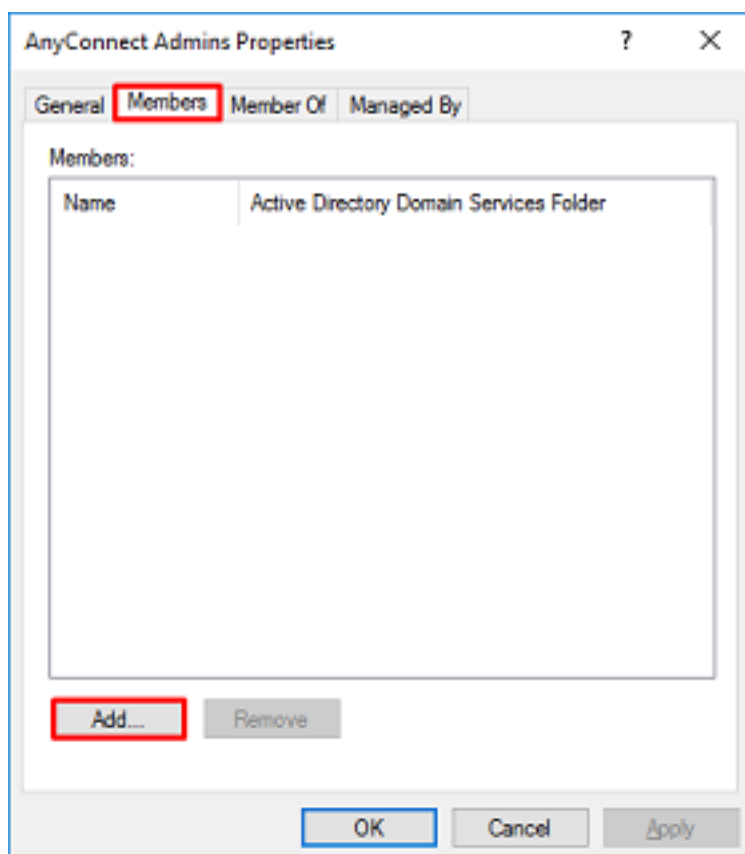
3. Verifique se o grupo foi criado. O grupo Usuários de AnyConnect também foi criado.



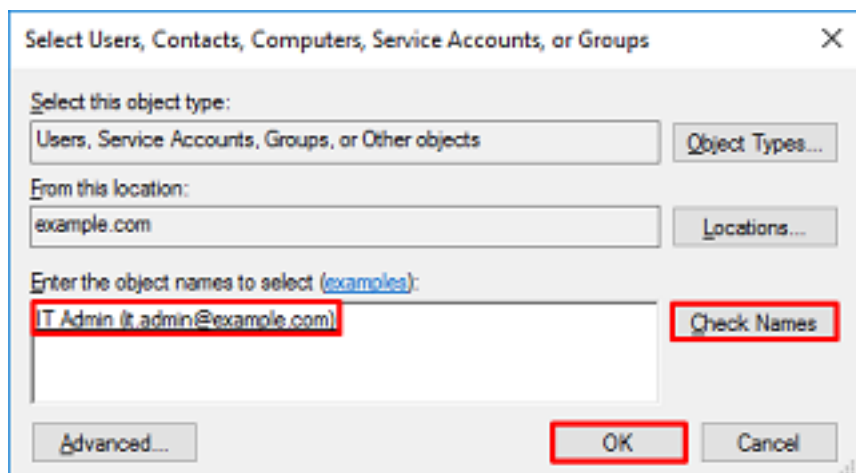
4. Clique com o botão direito do mouse no grupo do(s) usuário(s) e escolha **Propriedades**. Nesta configuração, o usuário Administrador de TI é adicionado ao grupo Administradores de AnyConnect e o usuário de teste é adicionado ao grupo Usuários de AnyConnect.



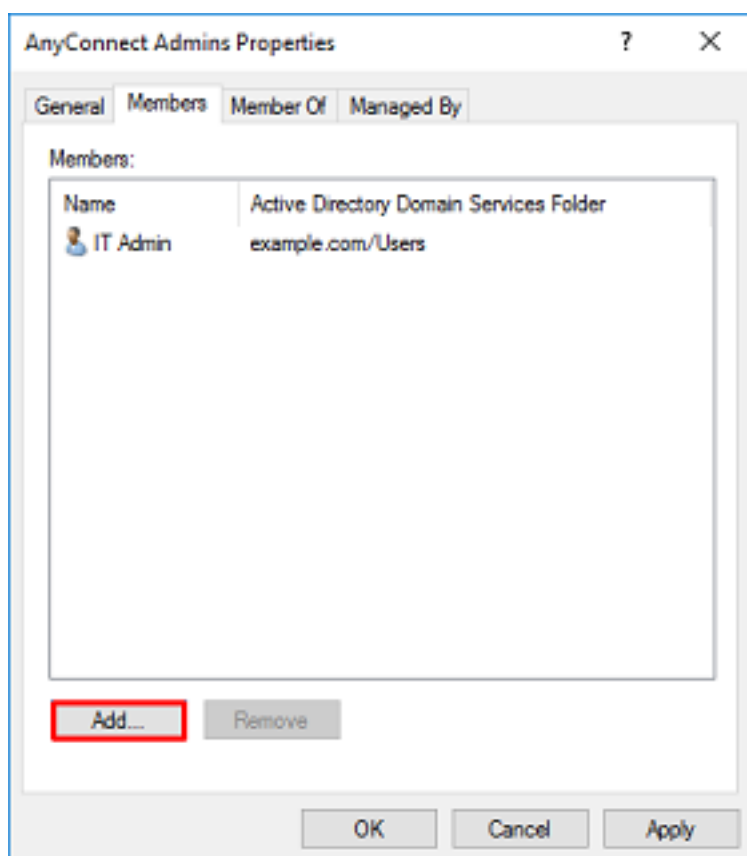
5. Na guia **Membros**, clique em **Adicionar**.



Insira o usuário no campo e clique em **Check Names** para verificar se o usuário foi encontrado. Depois de verificado, clique em **OK**.

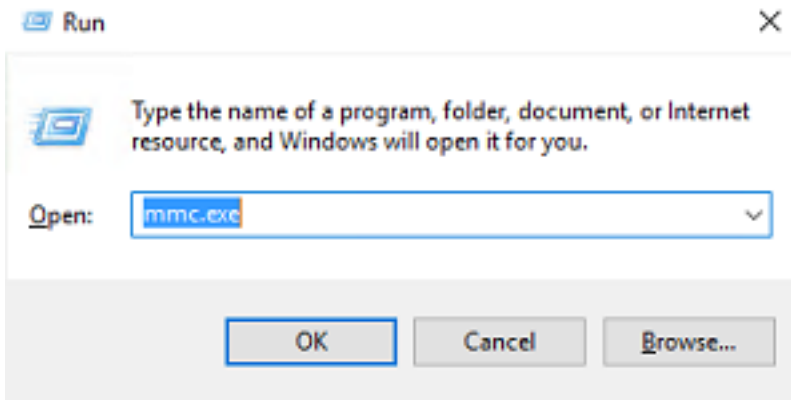


Verifique se o usuário correto foi adicionado e clique no botão OK. O usuário de teste também é adicionado ao grupo Usuários de AnyConnect seguindo as mesmas etapas.

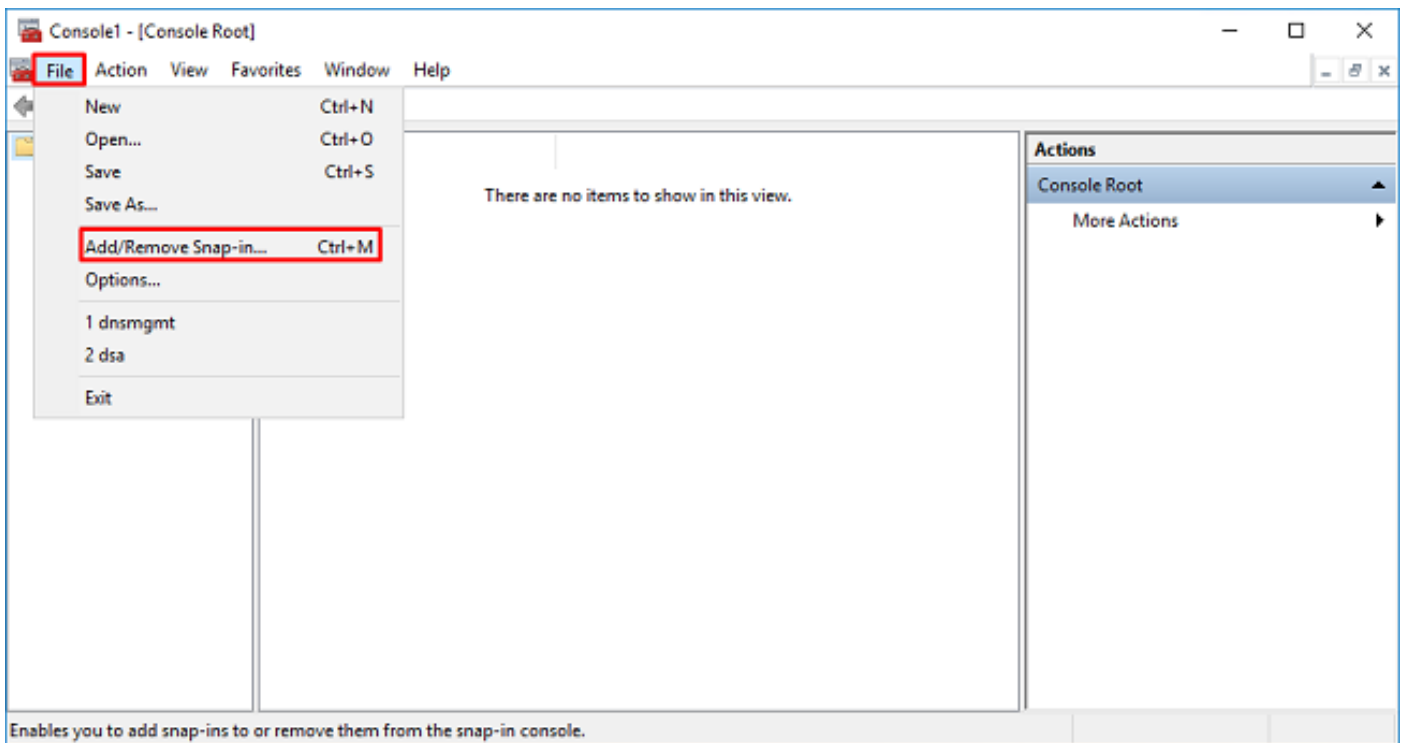


Copiar a raiz do certificado SSL do LDAPS (necessário apenas para LDAPS ou STARTTLS)

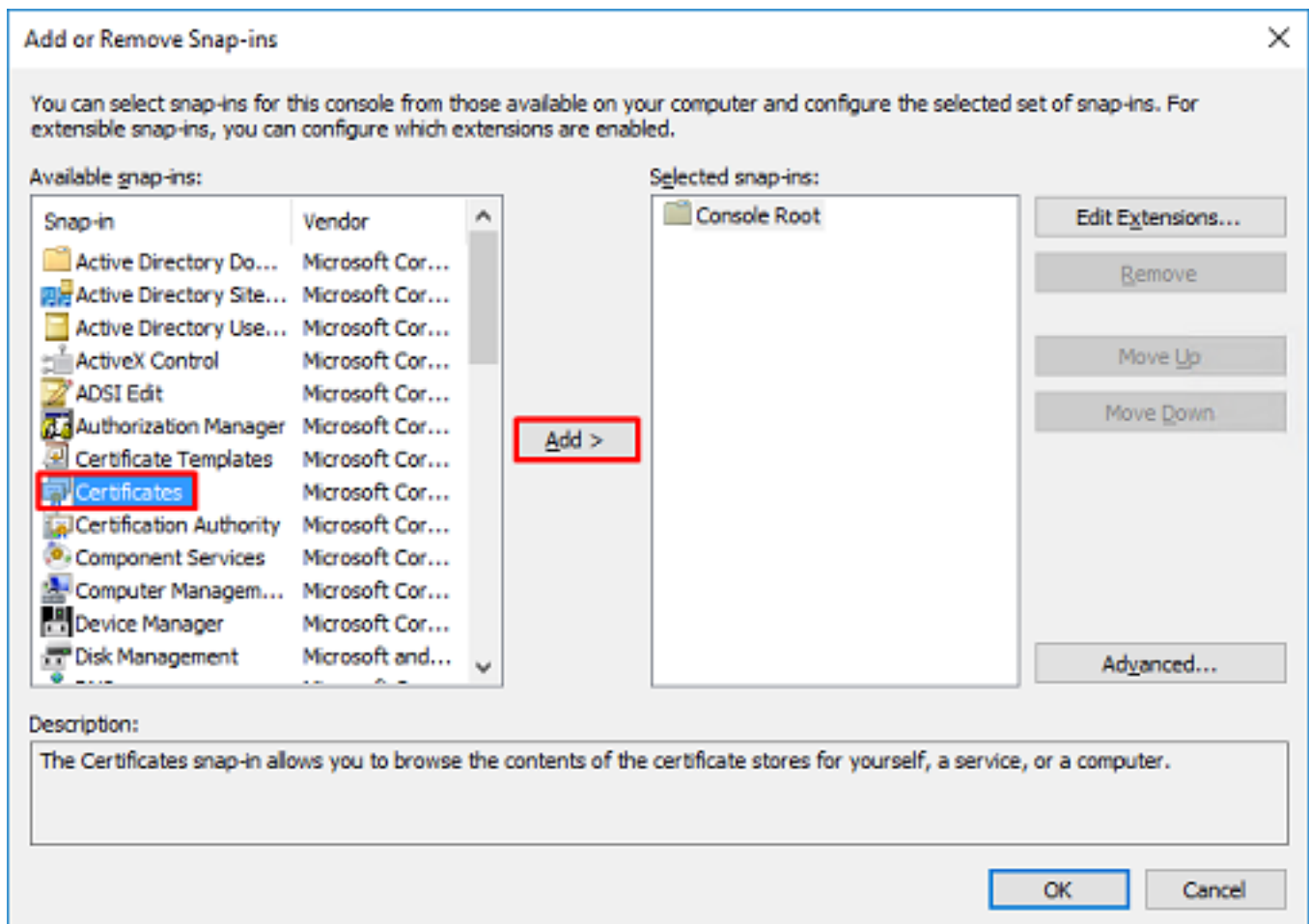
1. Pressione **Win+R** e digite **mmc.exe**. em seguida, clique em OK.



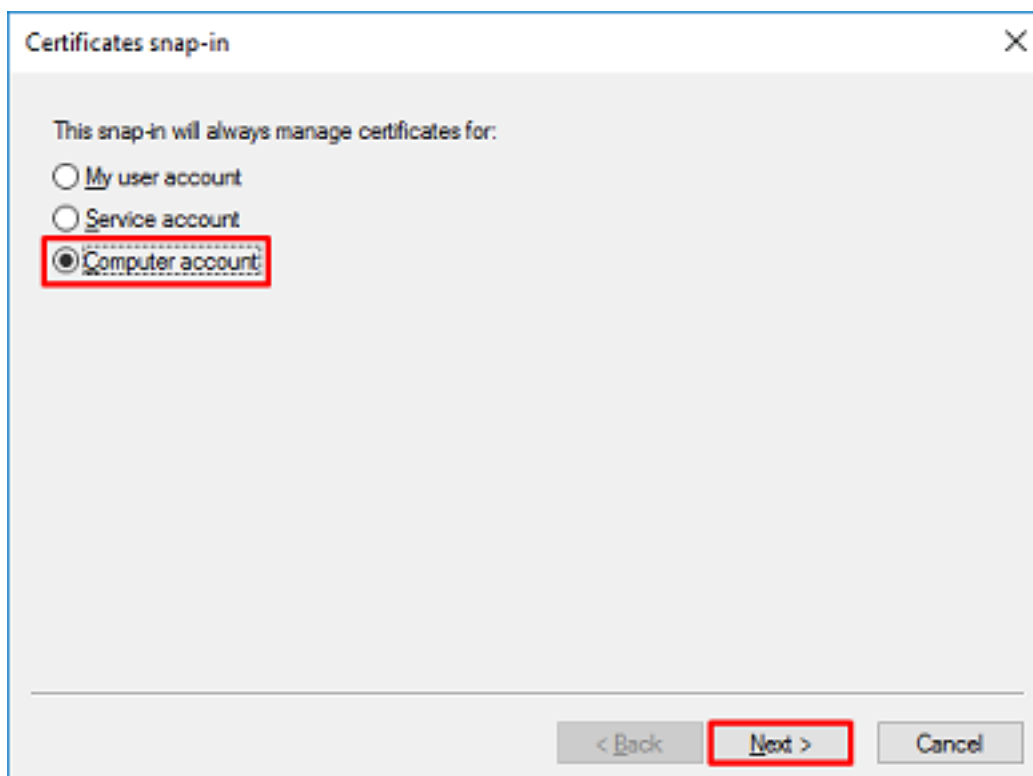
2. Navegue até **Arquivo > Adicionar/Remover Snap-in...**



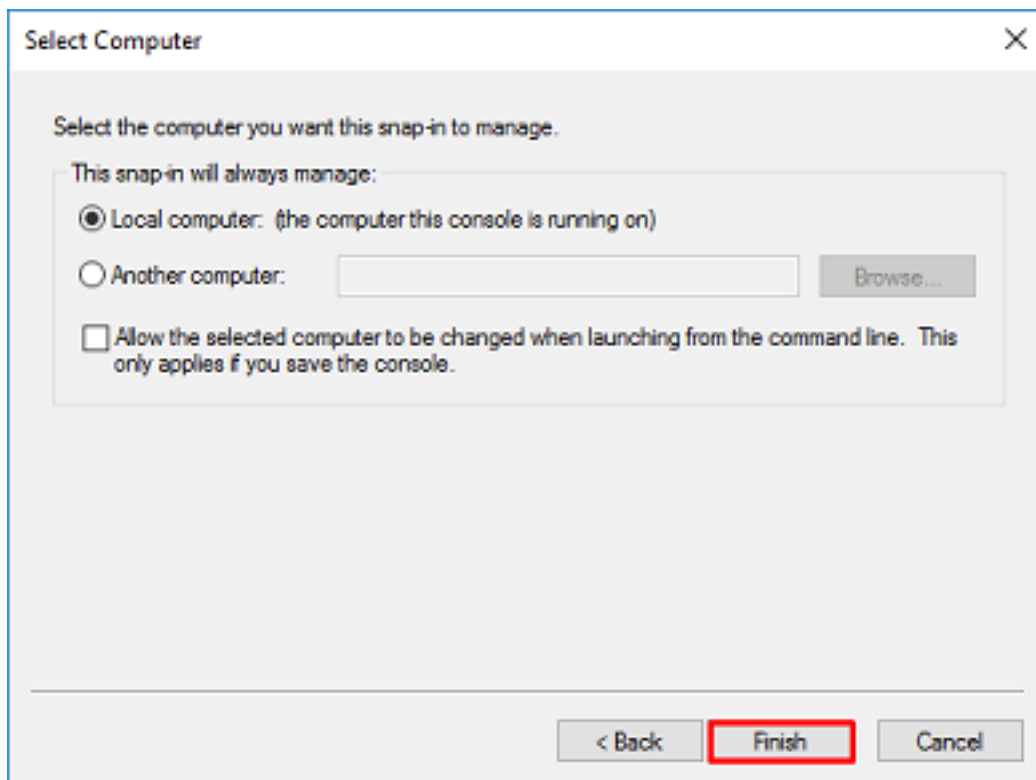
3. Em Snap-ins disponíveis, selecione **Certificados** e clique em **Adicionar**.



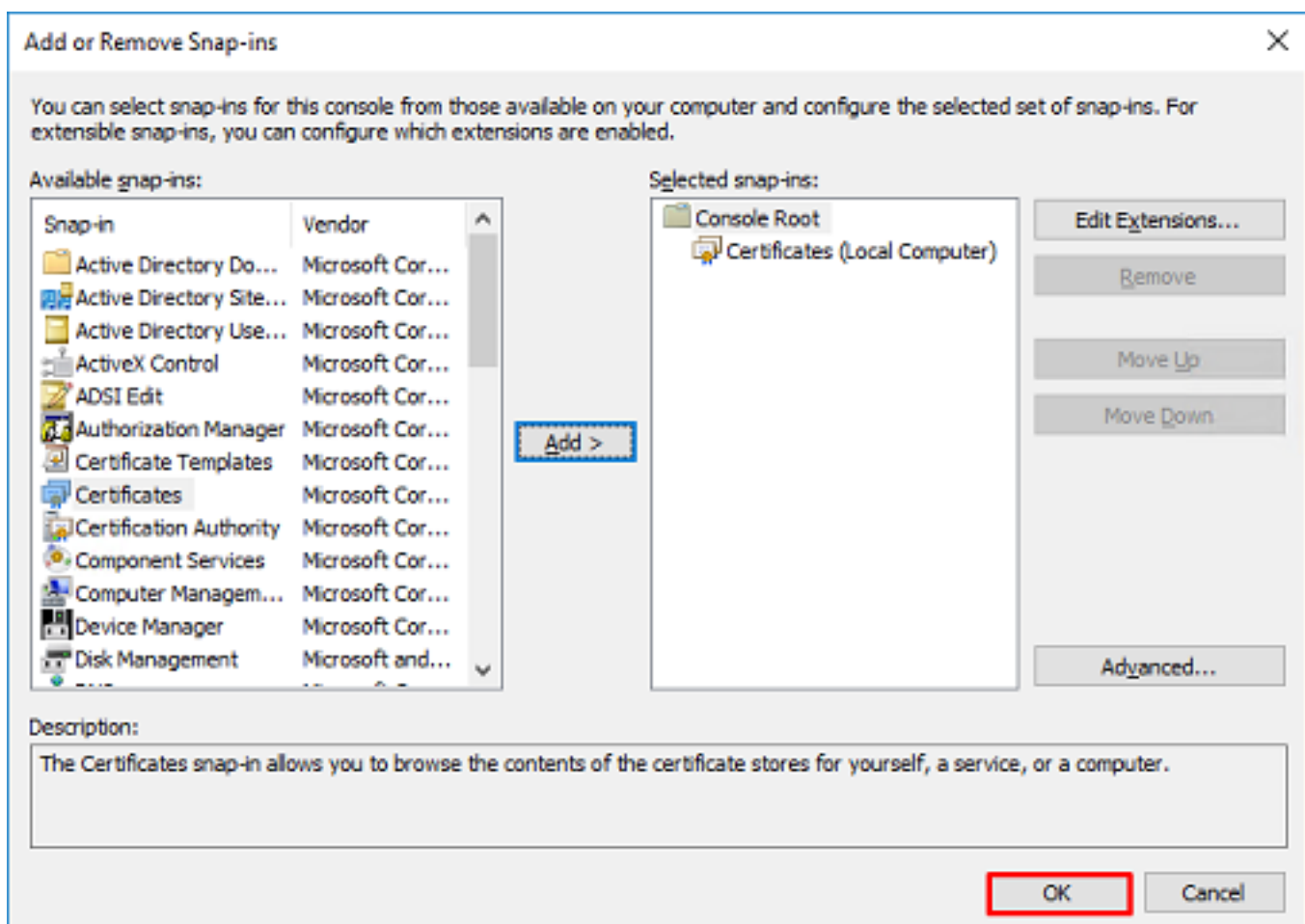
4. Selecione **Conta do computador** e clique em **Avançar**.



Clique em **Finish**.



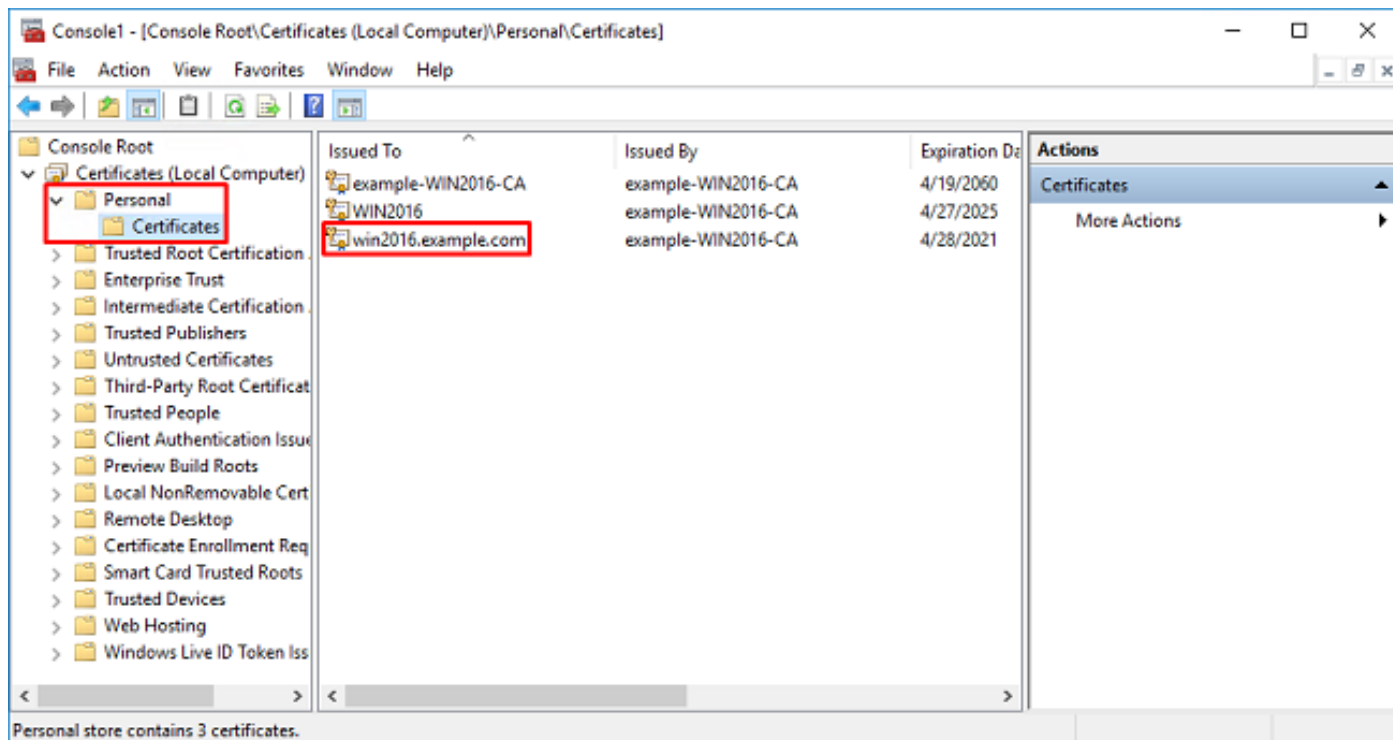
5. Agora clique em **OK**.



6. Expanda a pasta **Pessoal** e clique em **Certificados**. O certificado usado pelo LDAPS é emitido para o **Fully Qualified Domain Name (FQDN)** do servidor Windows. Neste servidor, há 3 certificados listados.

- Um certificado de CA emitido para e por example-WIN2016-CA.
- Um certificado de identidade emitido para WIN2016 por example-WIN2016-CA.
- Um certificado de identidade emitido para win2016.example.com por example-WIN2016-CA.

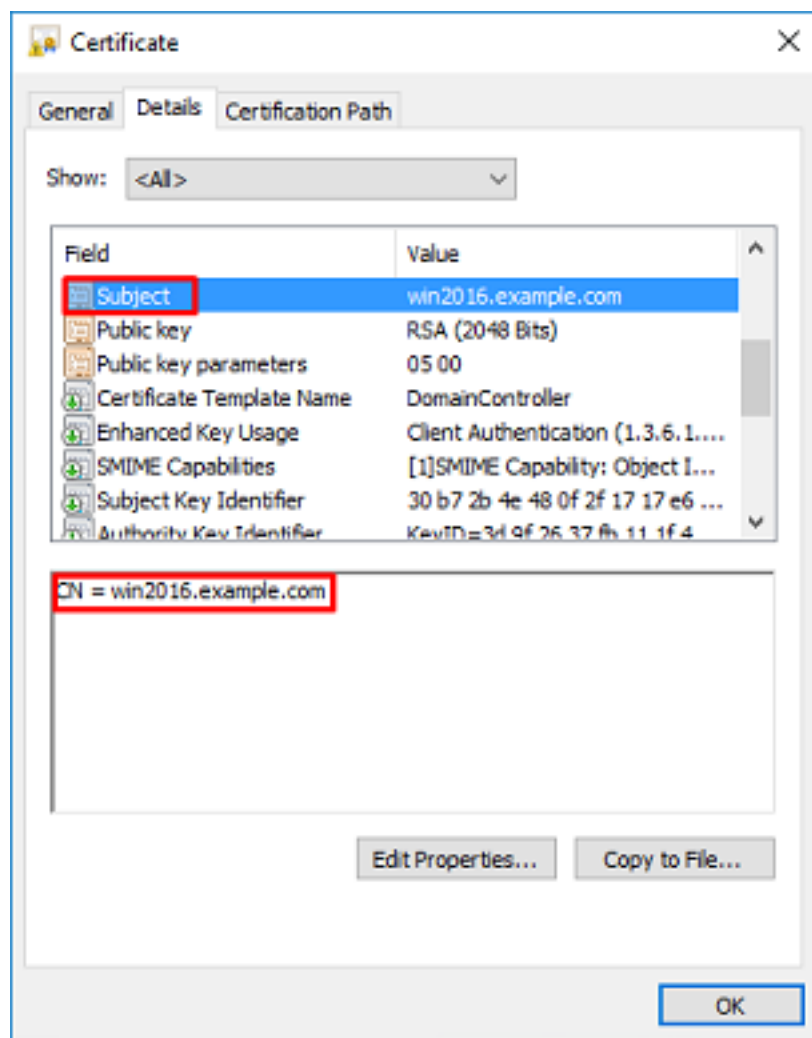
Neste guia de configuração, o FQDN é win2016.example.com e, portanto, os dois primeiros certificados não são válidos para uso como o certificado SSL do LDAPS. O certificado de identidade emitido para win2016.example.com é um certificado emitido automaticamente pelo serviço de CA do Windows Server. Clique duas vezes no certificado para verificar os detalhes.

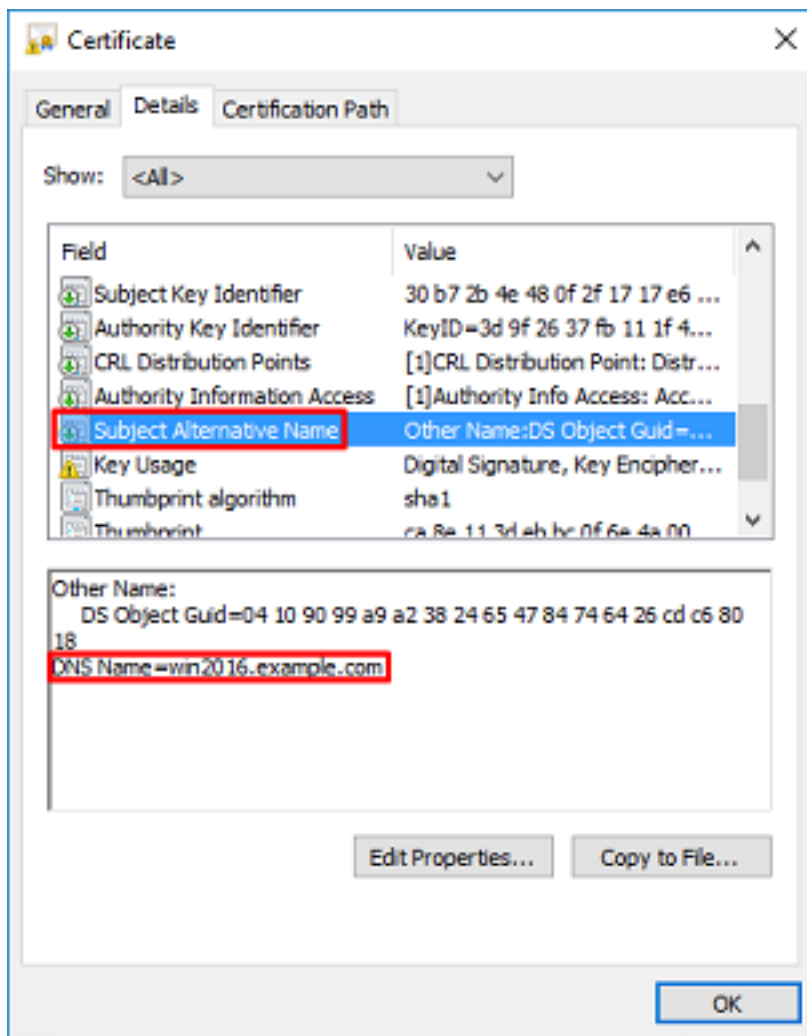


7. Para ser utilizado como certificado SSL LDAPS, o certificado deve cumprir os seguintes requisitos:

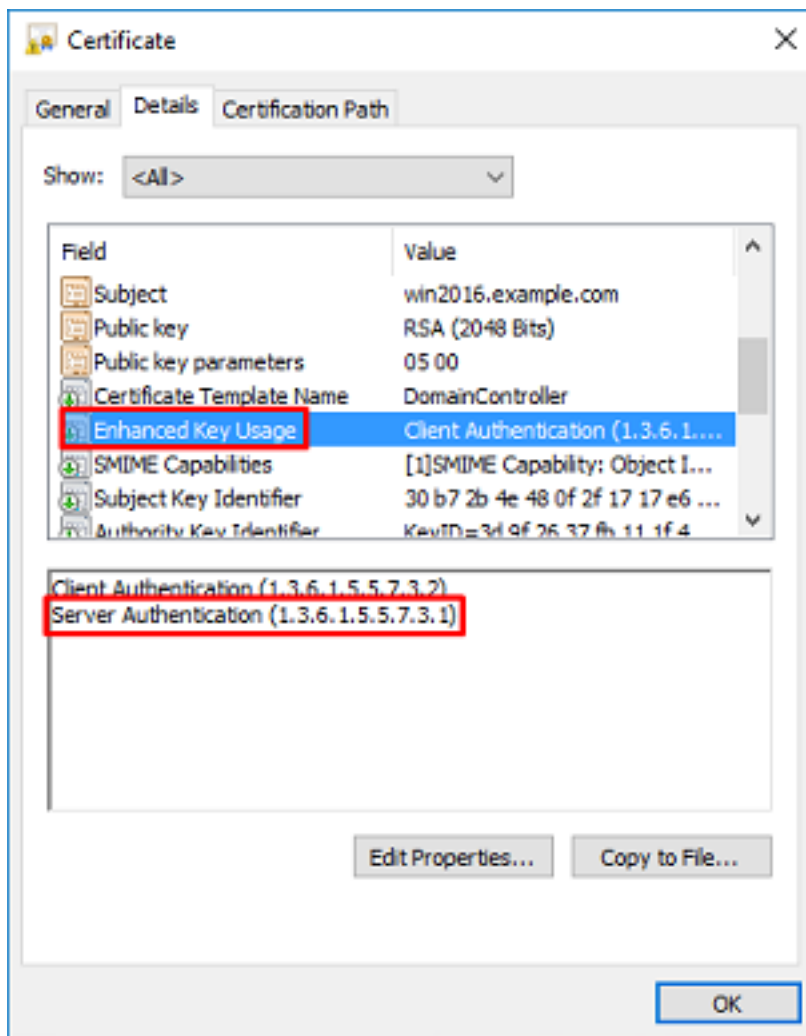
- O nome comum ou nome alternativo do assunto DNS corresponde ao FQDN do Windows Server.
- O certificado tem autenticação de servidor no campo Uso avançado de chave.

Na guia **Detalhes** do certificado, selecione **Assunto** e **Nome alternativo do assunto**. O FQDN win2016.example.com está presente.

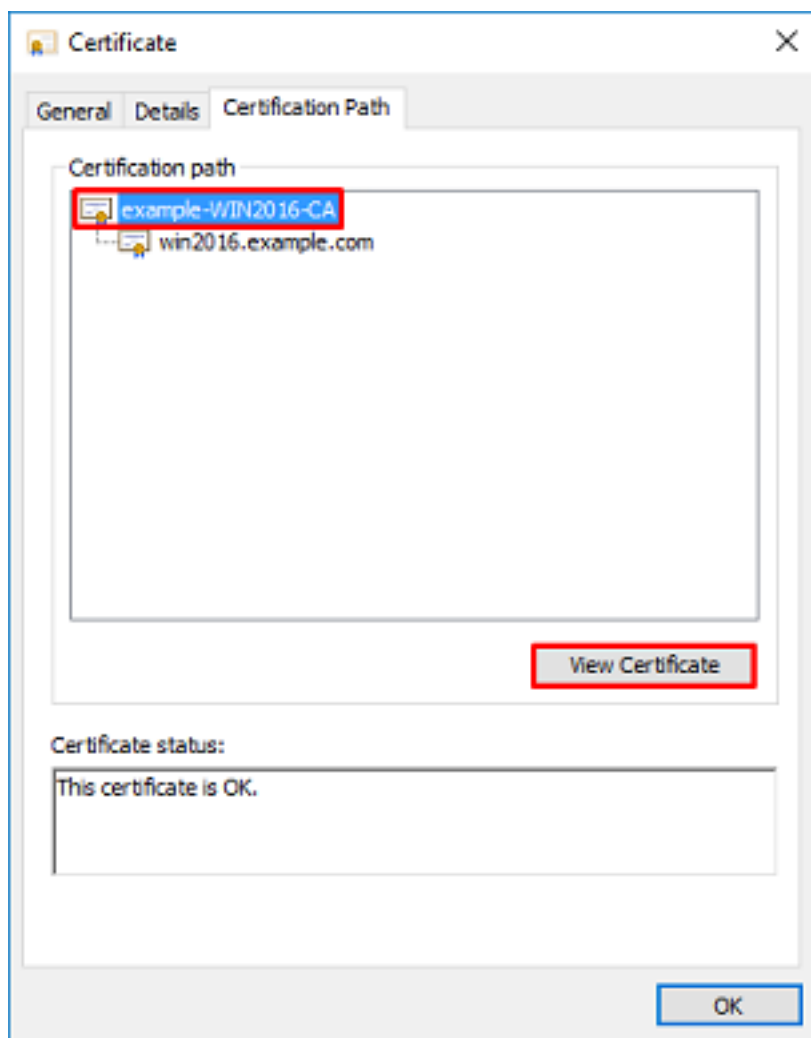




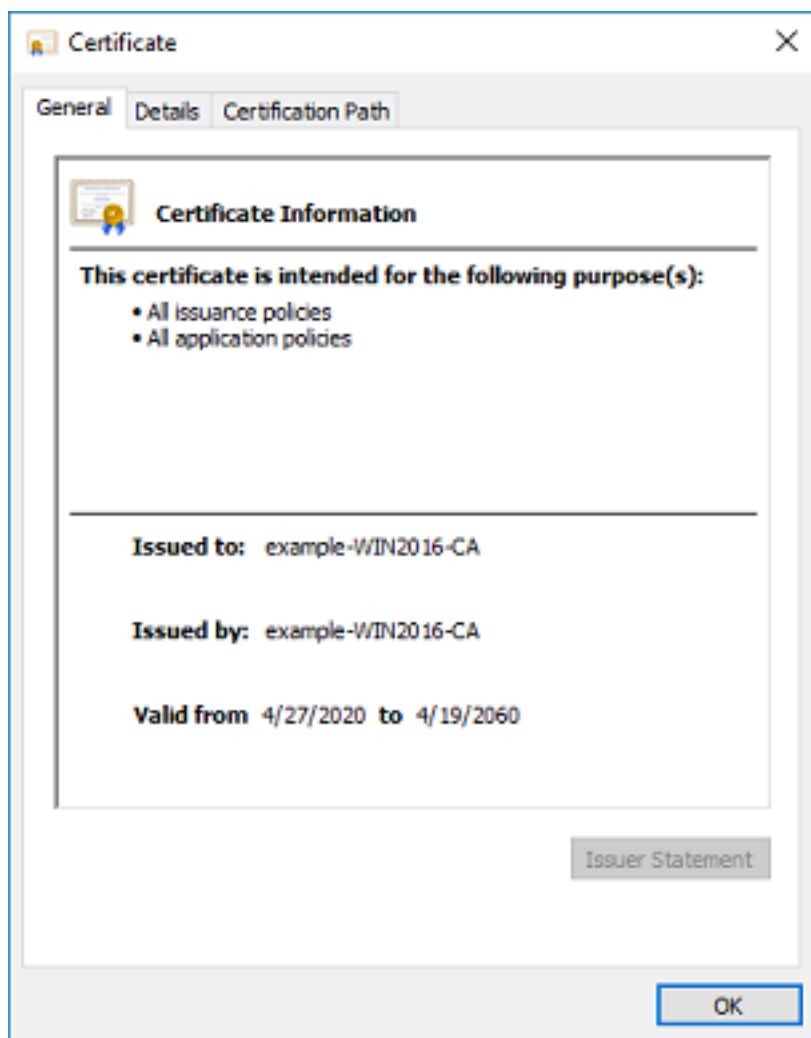
Em **Uso avançado de chave**, a autenticação do servidor está presente.



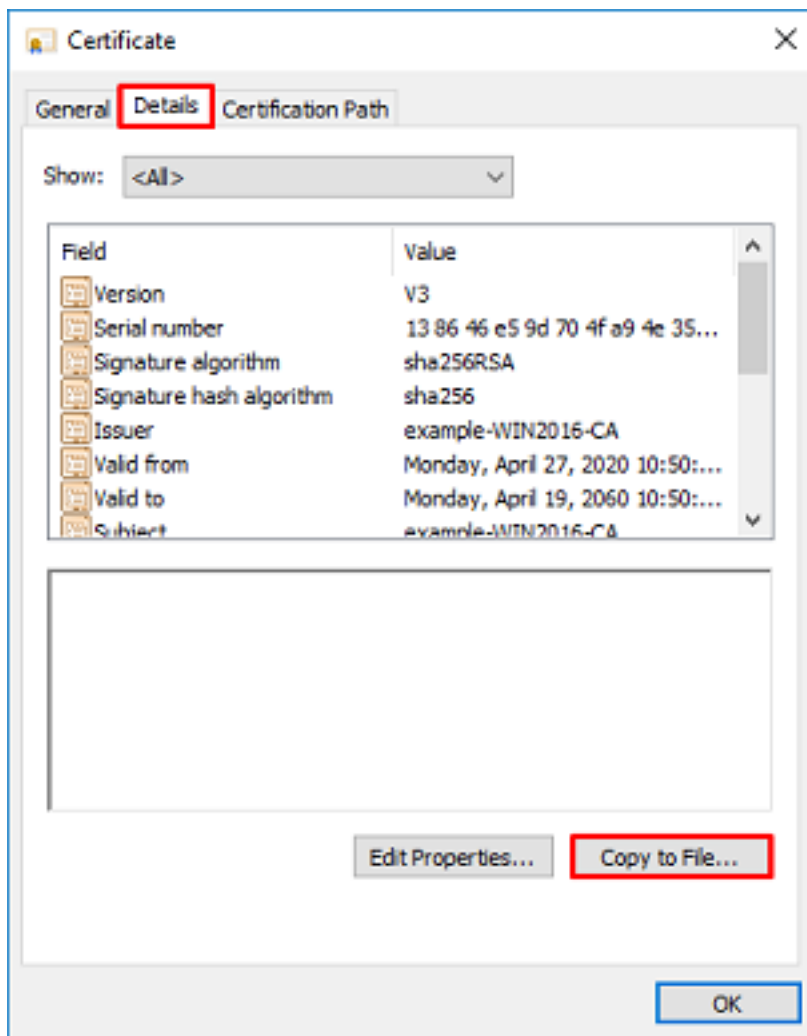
8. Uma vez confirmado, na guia **Caminho de Certificação**, selecione o certificado superior que é o certificado raiz da CA e clique em **Exibir Certificado**.



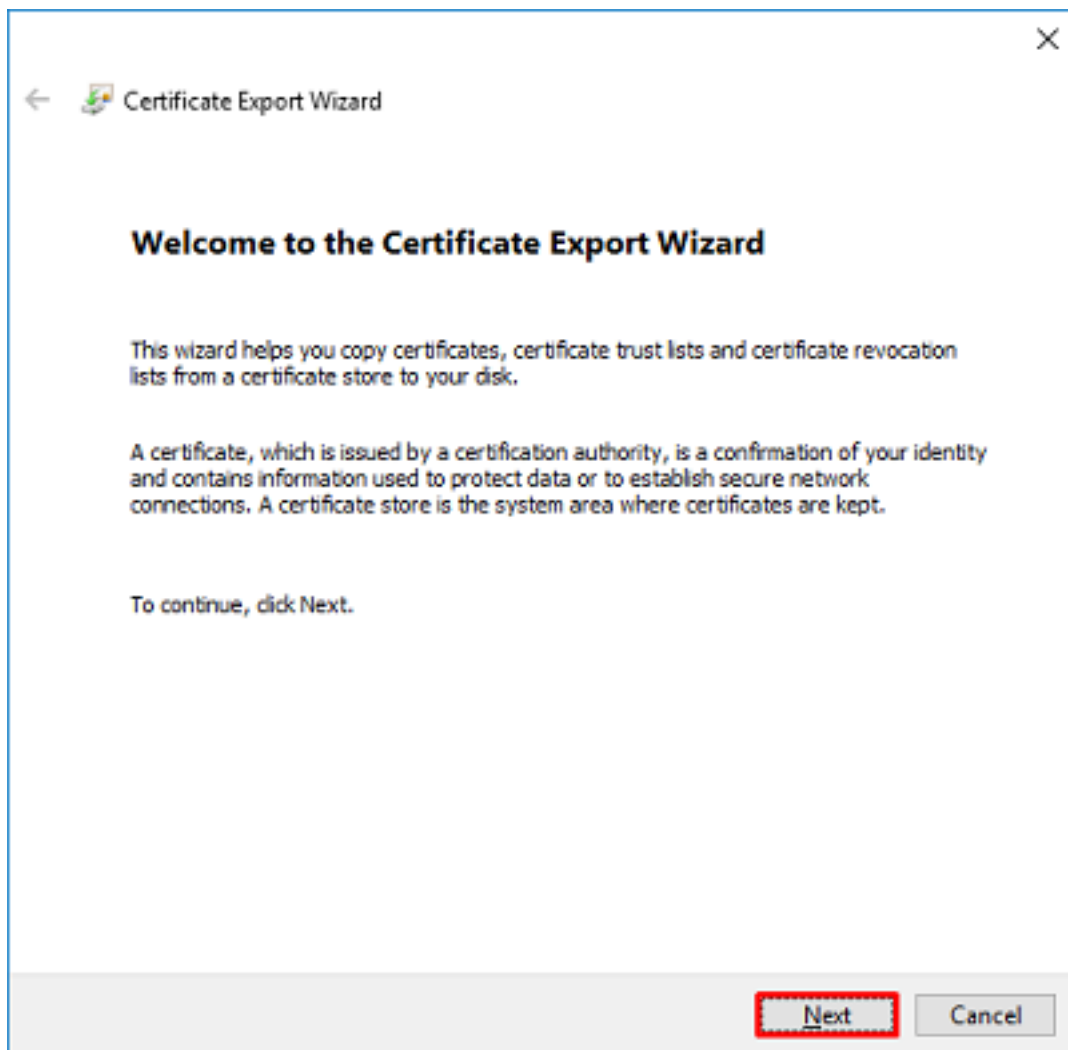
9. Isso abre os detalhes do certificado para o certificado CA raiz.



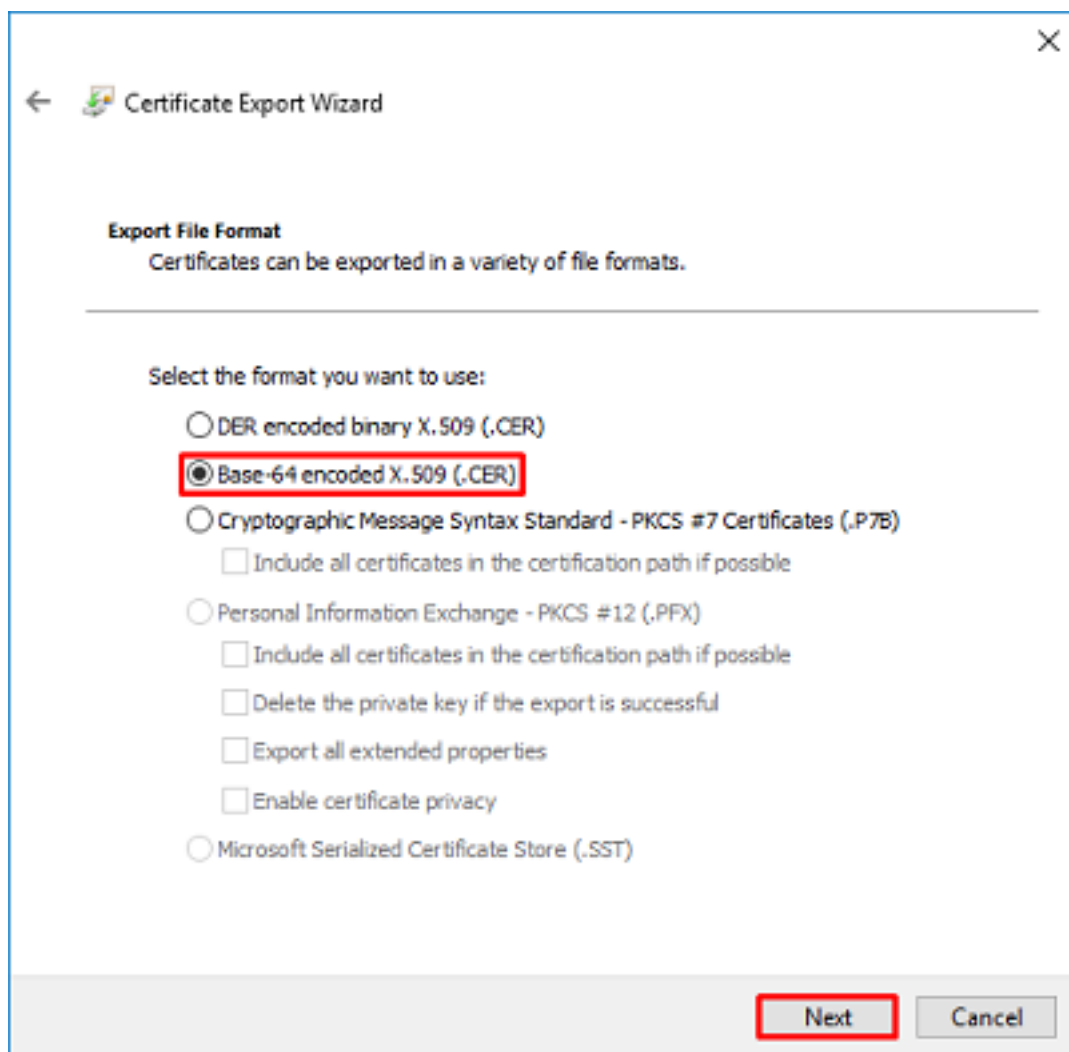
Na guia **Detalhes**, clique em **Copiar para arquivo...**



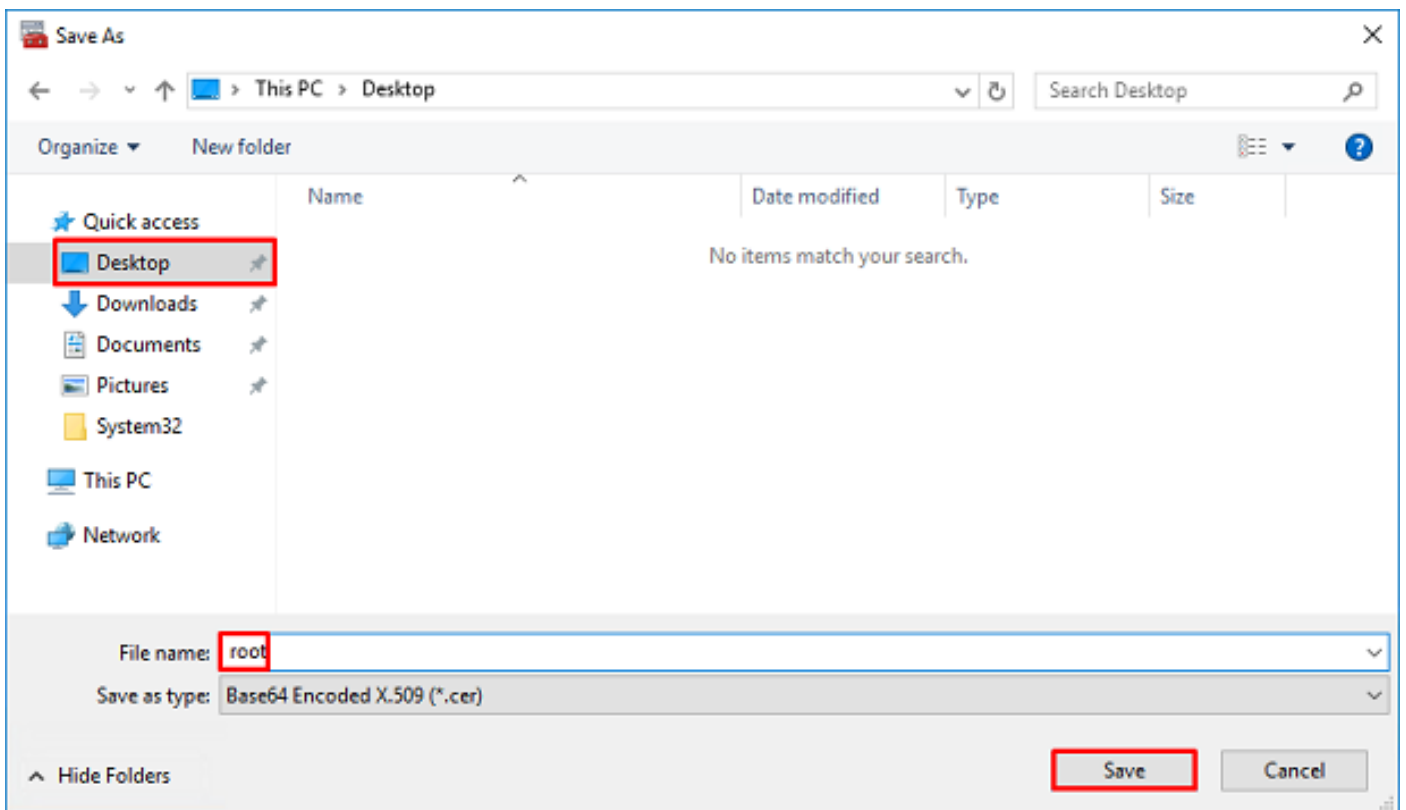
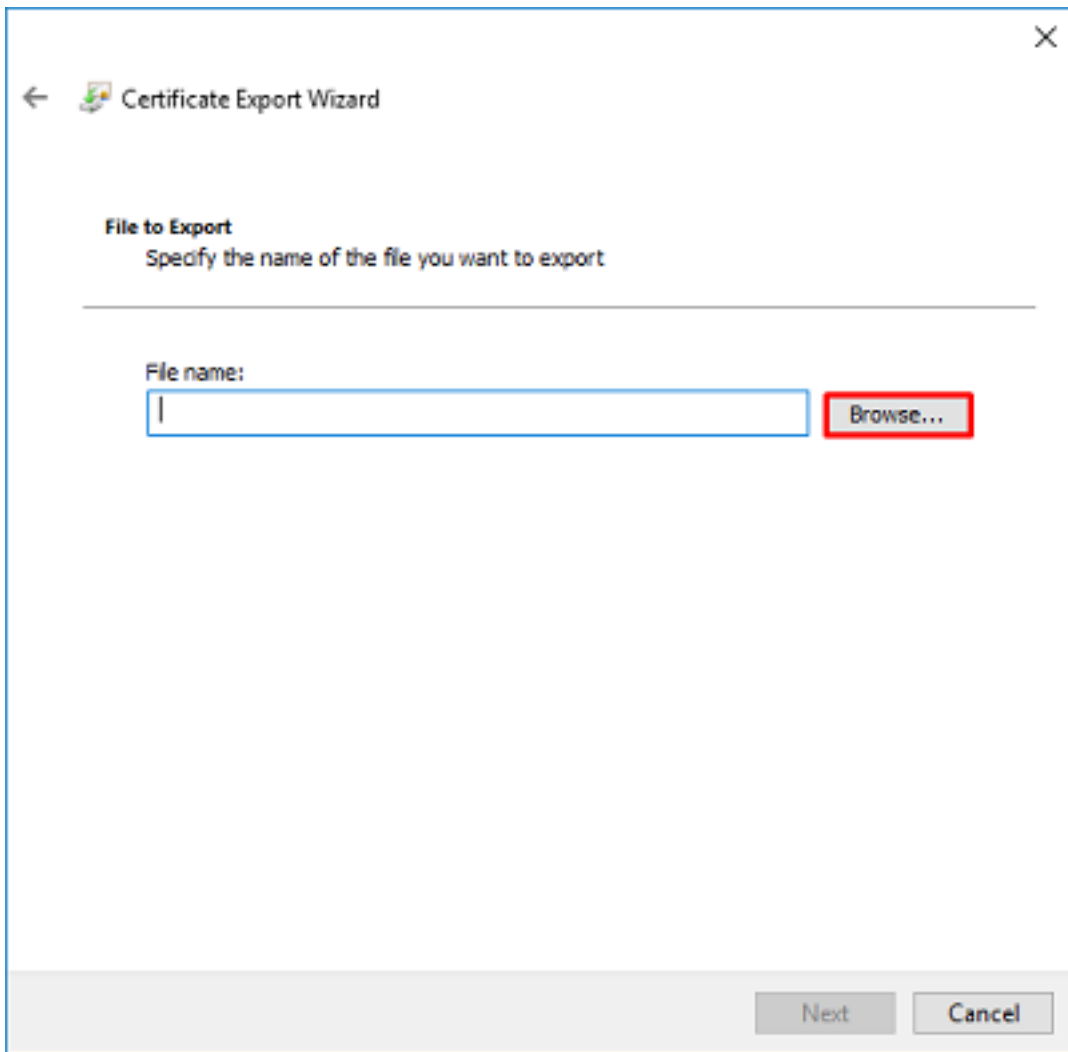
10. Use o **Assistente para Exportação de Certificados** que exporta a CA raiz no formato PEM.

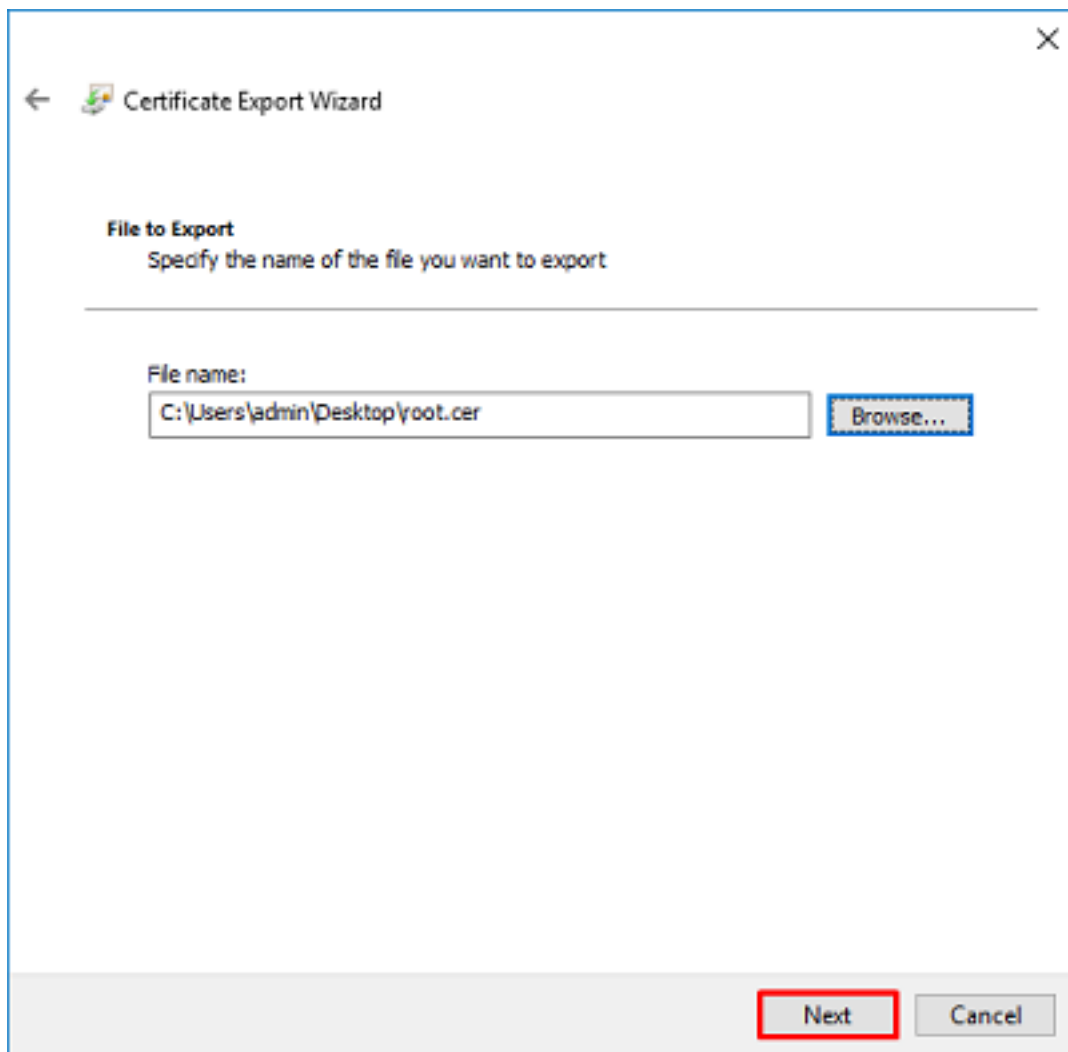


Seleccione X.509 codificado por Base 64

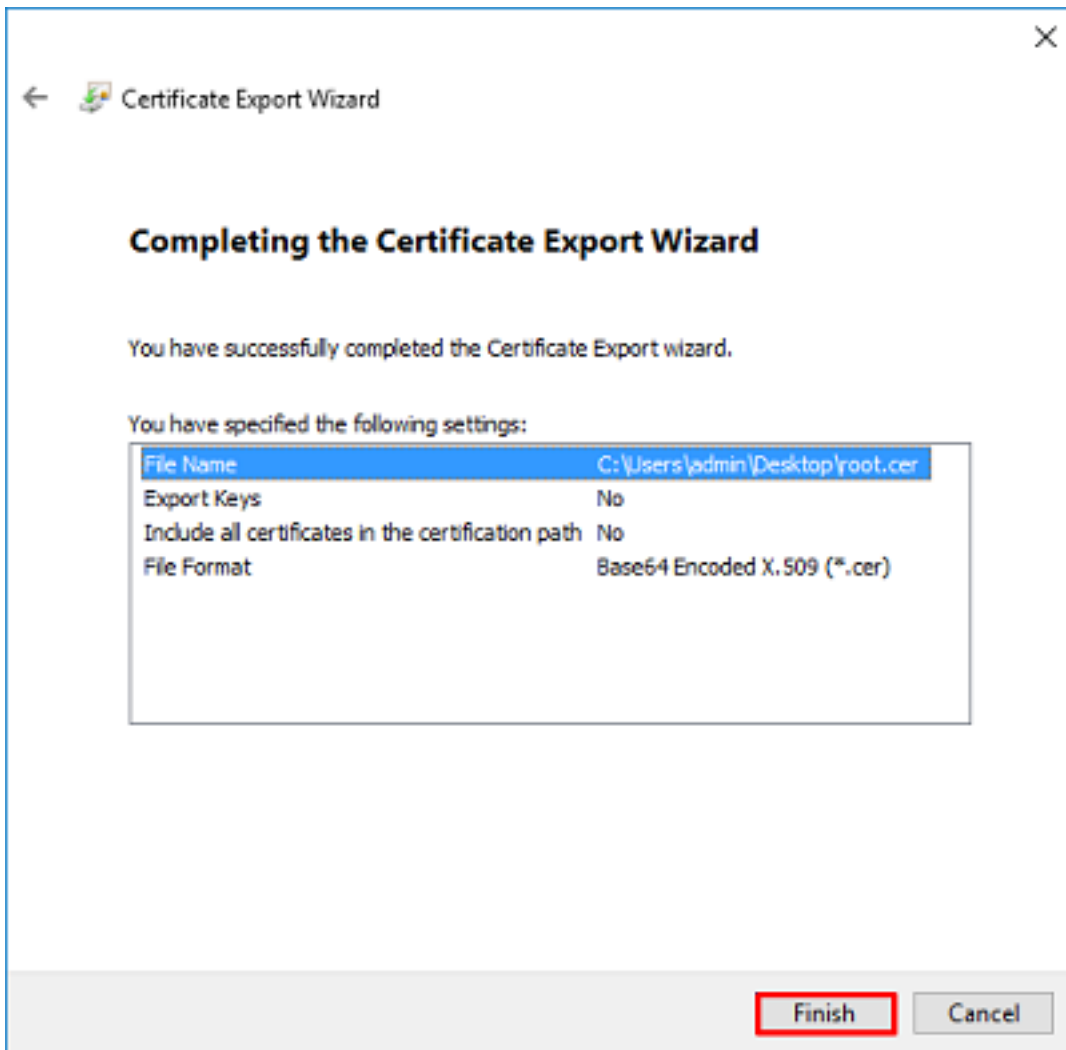


Selecione o nome do arquivo e o local para o qual será exportado.





Agora clique em **Concluir**.



11. Agora vá para o local e abra o certificado com um bloco de notas ou algum outro editor de texto. Essa ação mostra o certificado em formato PEM. Salve-o para usar mais tarde.

```
-----BEGIN CERTIFICATE-----
MIIDCCCAfCgAwIBAgIQE4ZG5Z1wT61ONTjooEQyMTANBgkqhkiG9w0BAQsFADAd
MRswGQYDVQQDEeJleGFtcGxlLVdJTjIwMTYtQ0EwIBcNMjAwNDI3MTQ1MDU5WhgP
MjA2MDA0MTkxNDUwNTlAMB0xGzAZBgNVBAMTEmV4YW1wbGUtV01OMjAxNi1lDQTC
ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAl8ghT719NzSQpoQPh0YT67b
Ya+PngsxMyvkewP33QLTAWw1HW1Tb9Mk5BDWOItTaVsgHwPBfd++M+bLn3AiZnHV
OO+k6dVVY/E5qVkeKSGoY+v940S2316lzdWReMOFhgbc2qMertIoficrRihonuU
Cjyeub3CO+meJUuKom2R47C0D35TUvo/FEHGgXJFaJS1se2UrpNO7KEMkfAlLPuM
aob4XE/OzxYQpPa18djsNnskfcFqD/HOTFQN4+SrOhHWlRnUIQBuaLdQaabhipD/
sVs5PneYJX8YKma821uYI6j90YuytmsHBtCieyC062a8BKqOL7N86HFPfKMA3u8C
AwEAAaNCMEAwDgYDVR0PAQH/BAQDAgGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0O
BBYEFD2fJjf7ER9EM/HCxCVFN5QzqEdvMA0GCSqGSIb3DQEBCwUAA4IBAQB3lZJo
vzwVD3c5Q1nrNP+6Mq62OFpYH91k4Ch9S5g/CEOemhcgw8MDIoxW2dTsjenAEt7r
phFIHZoCoSyjBjMgK3xybmoSeg8vBjCXseYNGEm0c9KW1oFmTOvdNVIb7Xp11IVa
6tALTt3ANRNgREtXPA6yQbthKGavW0Anfsojk9IcDr2vp0MTj1BCxsTscubR1+d
dLEFKQqmMeYvkVf+a7a64mqPZsG3Uxo0rd6cZxAPkq/ylcdwNSJFFfQV3DgZg+R96
9WLCR30big6xyo9Zu+lixwPdrbAD06zMhbEYEHkh00jBrUEBBI6Cy83iTZ9ejsk
KgwBJXEu33PplW6E
-----END CERTIFICATE-----
```

12. (Opcional) Na situação em que há vários certificados de identidade que podem ser usados por LDAPS e há incerteza sobre qual é usado, ou não há acesso ao servidor LDAPS, é possível extrair a CA raiz de uma captura de pacote feita no servidor Windows ou FTD após.

Configurações do FMC

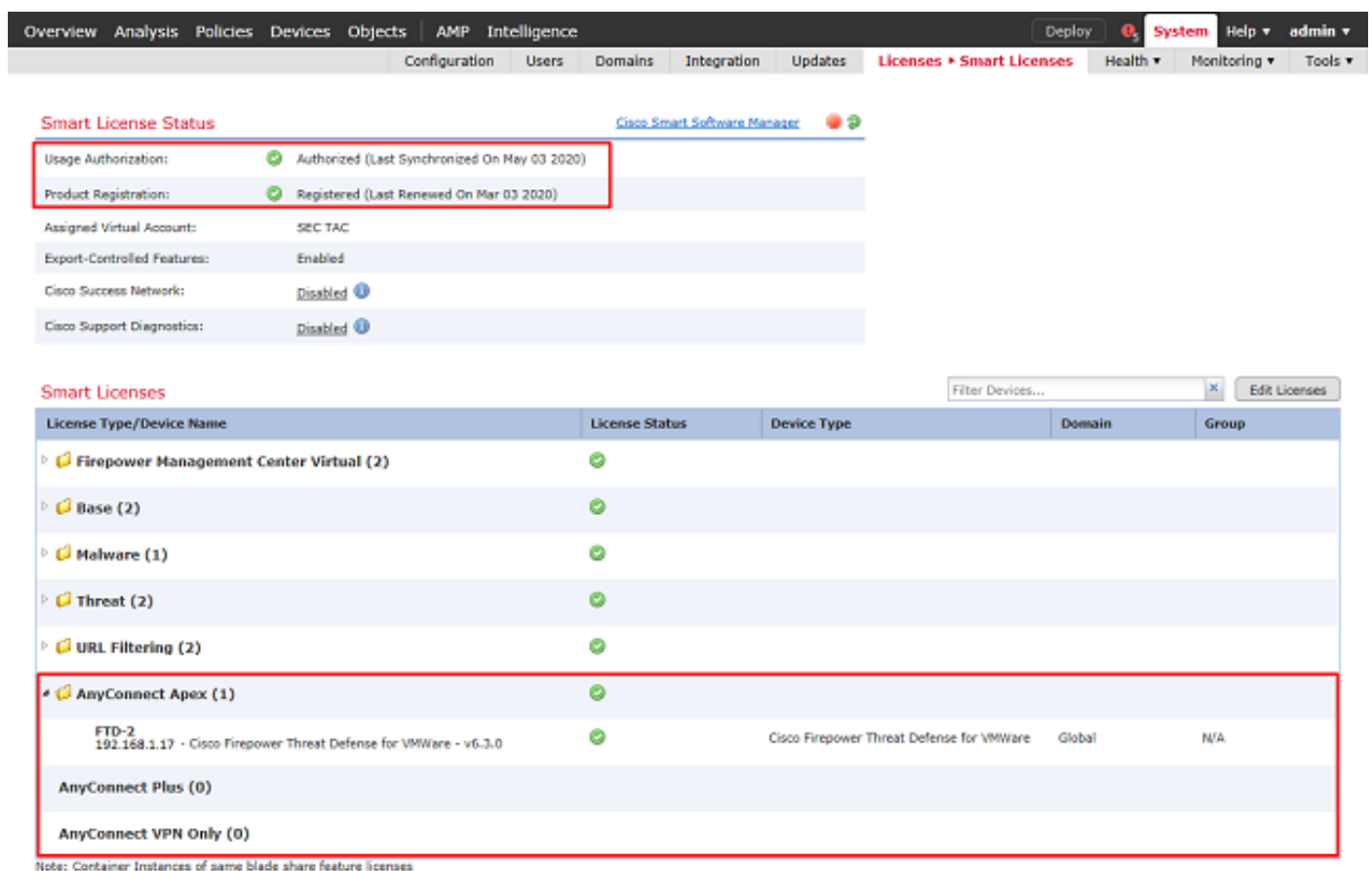
Verificar licenciamento

Para implantar a configuração do AnyConnect, o FTD precisa ser registrado no servidor de Smart Licensing e uma licença válida Plus, Apex ou Somente VPN deve ser aplicada ao dispositivo.

1. Navegue até **Sistema > Licenças > Smart Licensing**.



2. Verifique se os dispositivos estão em conformidade e se foram registrados com êxito. Verifique se o dispositivo foi registrado com uma licença Apex, Plus ou Somente VPN do AnyConnect.



Smart License Status [Cisco Smart Software Manager](#)

Usage Authorization:	✓ Authorized (Last Synchronized On May 03 2020)
Product Registration:	✓ Registered (Last Renewed On Mar 03 2020)
Assigned Virtual Account:	SEC TAC
Export-Controlled Features:	Enabled
Cisco Success Network:	Disabled ⓘ
Cisco Support Diagnostics:	Disabled ⓘ

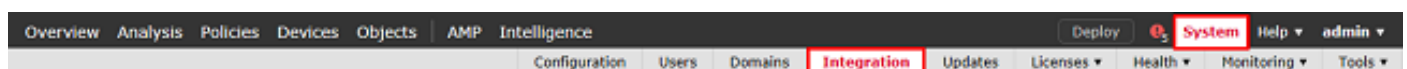
Smart Licenses

License Type/Device Name	License Status	Device Type	Domain	Group
Firepower Management Center Virtual (2)	✓			
Base (2)	✓			
Malware (1)	✓			
Threat (2)	✓			
URL Filtering (2)	✓			
AnyConnect Apex (1)	✓			
FTD-2 192.168.1.17 - Cisco Firepower Threat Defense for VMWare - v6.3.0	✓	Cisco Firepower Threat Defense for VMWare	Global	N/A
AnyConnect Plus (0)				
AnyConnect VPN Only (0)				

Note: Container Instances of same blade share feature licenses

Configurar realm

1. Navegue até **Sistema > Integração**.



2. Em **Territórios**, clique em **Novo território**.



3. Preencha os campos apropriados com base nas informações coletadas do servidor Microsoft. Quando terminar, clique em OK.

Add New Realm

Name * LAB-AD

Description

Type * AD

AD Primary Domain * example.com ex: domain.com

AD Join Username ex: user@domain

AD Join Password Test AD Join

Directory Username * ftd.admin@example.com ex: user@domain

Directory Password * *****

Base DN * DC=example,DC=com ex: ou=user,dc=cisco,dc=com

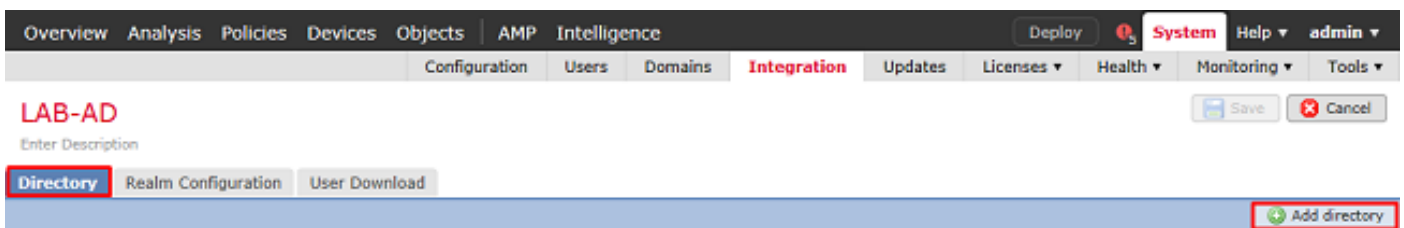
Group DN * DC=example,DC=com ex: ou=group,dc=cisco,dc=com

Group Attribute Member

* Required Field

OK Cancel

4. Na nova janela, selecione **Diretório**, se ainda não tiver sido escolhido, clique em **Adicionar diretório**.



Preencha os detalhes do servidor do AD. Observe que, se o FQDN for usado, o FMC e o FTD não serão vinculados com sucesso, a menos que o DNS esteja configurado para resolver o FQDN.

Para configurar o DNS para o FMC, navegue para **System > Configuration** e selecione **Management Interfaces**.

Para configurar o DNS para o FTD, navegue para **Devices > Platform Settings**, crie uma nova política ou edite uma atual e vá para o DNS.

Add directory ? X

Hostname / IP Address:
 Port:
 Encryption: STARTTLS LDAPS None
 SSL Certificate: +

Se LDAPS ou STARTTLS for usado, clique no símbolo verde +, dê um nome ao certificado e copie o certificado de CA raiz no formato PEM. Clique em **Salvar** quando terminar.

Import Trusted Certificate Authority ? X

Name:

Certificate Data or, choose a file:

```

-----BEGIN CERTIFICATE-----
MIIDCCCAfCgAwIBAgIQE4ZG5Z1wT6lONTjooEQyMTANBgkqhkiG9w0BAQsFADAd
MRswGQYDVQQDEExleGFtZXQxLWVudC9wcm9kdGVudC90EwIBcNMjAwNDI3MTQ1MDU5WhgP
MjA2MDA0MTkxNDUwNTlaMB0xGzAZBgNVBAMTEmV4YW1wbGUtV0lOMjAxNi1DQTCC
ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAl8ghT719NzSQpoQPh0YT67b
Ya+PngsxMyvkewP33QLTAWw1HW1Tb9Mk5BDWOITaVsgHwPBfd++M+bLn3AiZnHV
OO+k6dVVVY/E5qVKEKSGoY+v940S2316lzdWReMOFhgbc2qMertIoficrRihonuU
Cjyeub3CO+meJUuKom2R47C0D35TUvo/FEHGgXJFaJS1se2UrpNO7KEMkfA1LPuM
aob4XE/OzxYQpPa18djsNnskfcFqD/HOTFQn4+SrOhHWIRnUIQBUaLdQaabhipD/
sVs5PneYJX8YKma821uYI6j90YuytmsHBtCieyC062a8BKqOL7N86HFPFkMA3u8C
AwEAAaNCMEAwDgYDVR0PAQH/BAQDAgGGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0O
BBYEFD2fj7ER9EM/HcXCVFN5QzqEdvMA0GCSqGSIb3DQEBCwUAA4IBAQB31ZJo
vzwVD3c5Q1nrNP+6Mq62OFpYH91k4Ch9S5g/CEOemhcgw8MDIoxW2dTsjenAET7r
phFIHZoCoSyjBjMgK3xybmoSeg8vBjCXseYNGEmOc9KW1oFmTOvdNVib7XpI1Iva
6tALTt3ANRNqREtXPA6yQbthKGavW0Anfsojk9IcDr2vp0MTjIBCxsTscubRI+D
dLEFKQqmMeYvkVf+a7a64mqPZsG3Uxo0rd6cZxAPkq/ylcdwNSJFfQV3DgZg+R96
9WLCR30big6xyo9Zu+lixWpdrbADO6zMhbEYEhkhOOjBrUEBBI6Cy83iTZ9ejsk
KgwBJXEu33PplW6E
-----END CERTIFICATE-----

```

Encrypted, and the password is:

Selecione a CA raiz recém-adicionada na lista suspensa ao lado do certificado SSL e clique em STARTTLS ou LDAP.

Edit directory

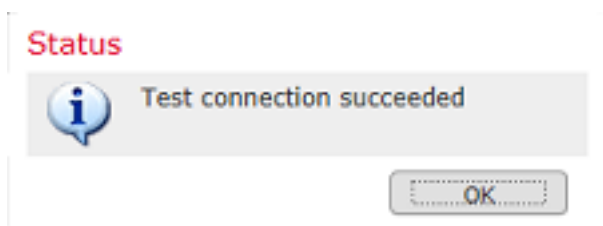


Hostname / IP Address	<input type="text" value="win2016.example.com"/>
Port	<input type="text" value="636"/>
Encryption	<input type="radio"/> STARTTLS <input checked="" type="radio"/> LDAPS <input type="radio"/> None
SSL Certificate	<input type="text" value="LDAPS_ROOT"/>

Clique em Testar para garantir que o FMC possa ser associado com sucesso ao nome de usuário e à senha do diretório fornecidos na etapa anterior.

Como esses testes são iniciados a partir do FMC e não através de uma das interfaces roteáveis configuradas no FTD (como interno, externo, dmz), uma conexão bem-sucedida (ou com falha) não garante o mesmo resultado para a autenticação do AnyConnect porque as solicitações de autenticação LDAP do AnyConnect são iniciadas a partir de uma das interfaces roteáveis do FTD.

Para obter mais informações sobre como testar as conexões LDAP no FTD, revise as seções AAA de teste e Captura de pacotes na área Solução de problemas.



5. Em **Download do Usuário**, faça o download dos grupos que são usados para a identidade do usuário em etapas posteriores.

Marque a caixa **Download users and groups** e a coluna para **Available Groups** será preenchida com os grupos configurados no Active Directory.

Os grupos podem ser incluídos ou excluídos. No entanto, por padrão, todos os grupos encontrados no DN de grupo são incluídos.

Usuários específicos também podem ser incluídos ou excluídos. Os grupos e usuários incluídos estão disponíveis para serem selecionados para a identidade do usuário posteriormente.

Ao concluir, clique em **Save** (Salvar).

LAB-AD

Enter Description

Directory Realm Configuration **User Download**

Download users and groups

Begin automatic download at 8 AM America/New York Repeat Every 24 Hours

Download Now

Available Groups

Search by name

- AnyConnect Admins
- DnsUpdateProxy
- WseRemoteAccessUsers
- WseInvisibleToDashboard
- Allowed RODC Password Replication Group
- Enterprise Key Admins
- Domain Admins
- WseAlertAdministrators
- Event Log Readers
- Replicator
- Domain Guests
- Windows Authorization Access Group
- Account Operators
- Hyper-V Administrators
- System Managed Accounts Group

Groups to Include (2)

- AnyConnect Admins
- AnyConnect Users

Groups to Exclude (0)

None

Enter User Inclusion Add

Enter User Exclusion Add

6. Ative o novo realm.

Cloud Services **Realms** Identity Sources eStreamer Host Input Client Smart Software Satellite

Compare realms New realm

Name	Description	Domain	Type	Base DN	Group DN	Group Attribute	State
LAB-AD		Global	AD	DC=example,DC=com	DC=example,DC=com	member	<input checked="" type="checkbox"/>

7. Se LDAPS ou STARTTLS for usado, a CA raiz também precisa ser confiável pelo FTD. Para fazer isso, primeiro navegue até **Dispositivos > Certificados**.

Overview Analysis Policies **Devices** Objects AMP Intelligence

Device Management NAT VPN QoS Platform Settings FlexConfig **Certificates**

Deploy System Help admin

Add

Clique em Adicionar no canto superior direito.

Overview Analysis Policies **Devices** Objects AMP Intelligence

Device Management NAT VPN QoS Platform Settings FlexConfig **Certificates**

Deploy System Help admin


Add

Selecione o FTD e a configuração LDAP será adicionada; em seguida, clique no símbolo verde +.

Add New Certificate

Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.

Device*:

Cert Enrollment*: 

Dê um nome ao ponto confiável e escolha Inscrição manual no menu suspenso Tipo de inscrição. Cole o certificado de CA raiz em formato PEM aqui e clique em **Salvar**.

Add Cert Enrollment

Name*:

Description:

CA Information | Certificate Parameters | Key | Revocation

Enrollment Type:

CA Certificate*:

```
-----BEGIN CERTIFICATE-----
MIIDCDCCAFcGAWIBAgIQE4ZG5Z1wT6lONTjooEQyMTANBgkqhki
G9w0BAQsFADAd
MRswGQYDVQQQExJleGFtcGxlLVdJTjJlWMTYtQ0EwIBcNMjAwNDI
3MTQ1MDU5WhgP
MjA2MDA0MTkxNDUwNTlaMB0xGzAZBgNVBAMTEmV4YW1wbGU
tV0lOMjAxNi1DQTCC
ASiWdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAI8ghT719N
zSQpoQPh0YT67b
Ya+PngsxMyvkewP33QLTAWw1HW1Tb9Mk5BDWOItaVsgHwPBF
d++M+bLn3AiZnHV
OO+k6dVvY/E5qVkeKSGoY+v940S2316lzdWReMOFhgbc2qMertIo
ficrRhionuU
Cjyeub3CO+meJUuKom2R47C0D35TUvo/FEHGgXJFaJS1se2UrpN
O7KEMkfa1LPuM
aob4XE/OzxYQpPa18djsNnskfcFqD/HOTFQN4+SrOhHWIRnUIQBU
aLdQaabhipD/
sVs5PneYJX8YKma821uYI6j90YuytmsHBTcIeyC062a8BKqOL7N86
```

Allow Overrides:

Verifique se o ponto confiável criado foi selecionado e clique em **Adicionar**.

Add New Certificate

Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.

Device*:

Cert Enrollment*:

Cert Enrollment Details:

Name: LDAPS_ROOT
 Enrollment Type: Manual
 SCEP URL: NA

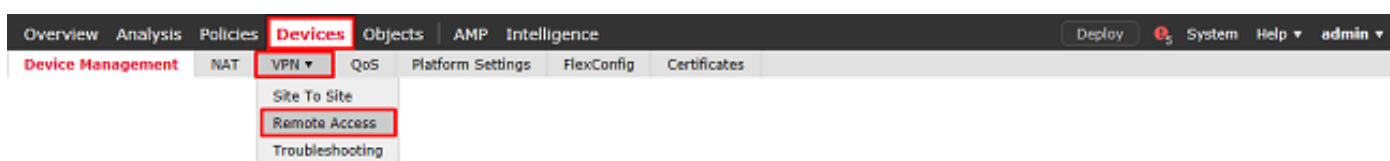
O novo ponto de confiança aparece sob o FTD. Embora mencione que a importação do certificado Identity é necessária, não é necessário para o propósito do FTD ser capaz de autenticar o certificado SSL enviado pelo servidor LDAPS e, portanto, esta mensagem pode ser ignorada.

Name	Domain	Enrollment Type	Status
FTD-1			
FTD-1-PKCS12	Global	PKCS12 file	CA ID
FTD-2			
FTD-2-PKCS12	Global	PKCS12 file	CA ID
FTD-2-Selfsigned	Global	Self-Signed	CA ID
LDAPS_ROOT	Global	Manual	CA ID Identity certificate import required

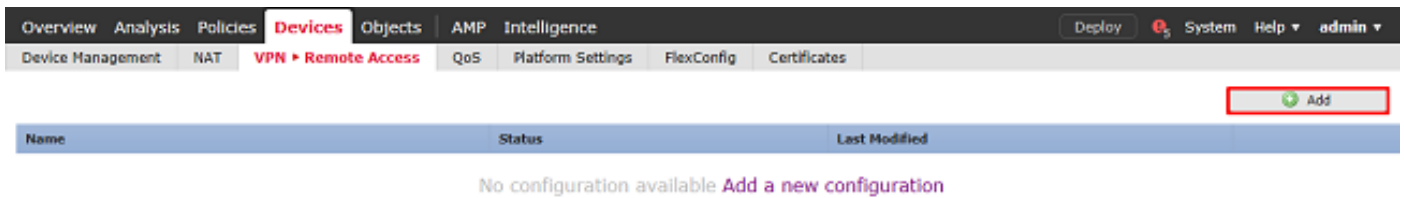
Configurar AnyConnect para autenticação do AD

1. Estas etapas supõem que nenhuma política de vpn de acesso remoto já tenha sido criada. Se uma política já foi criada, clique no botão Editar dessa política e vá para a etapa 3.

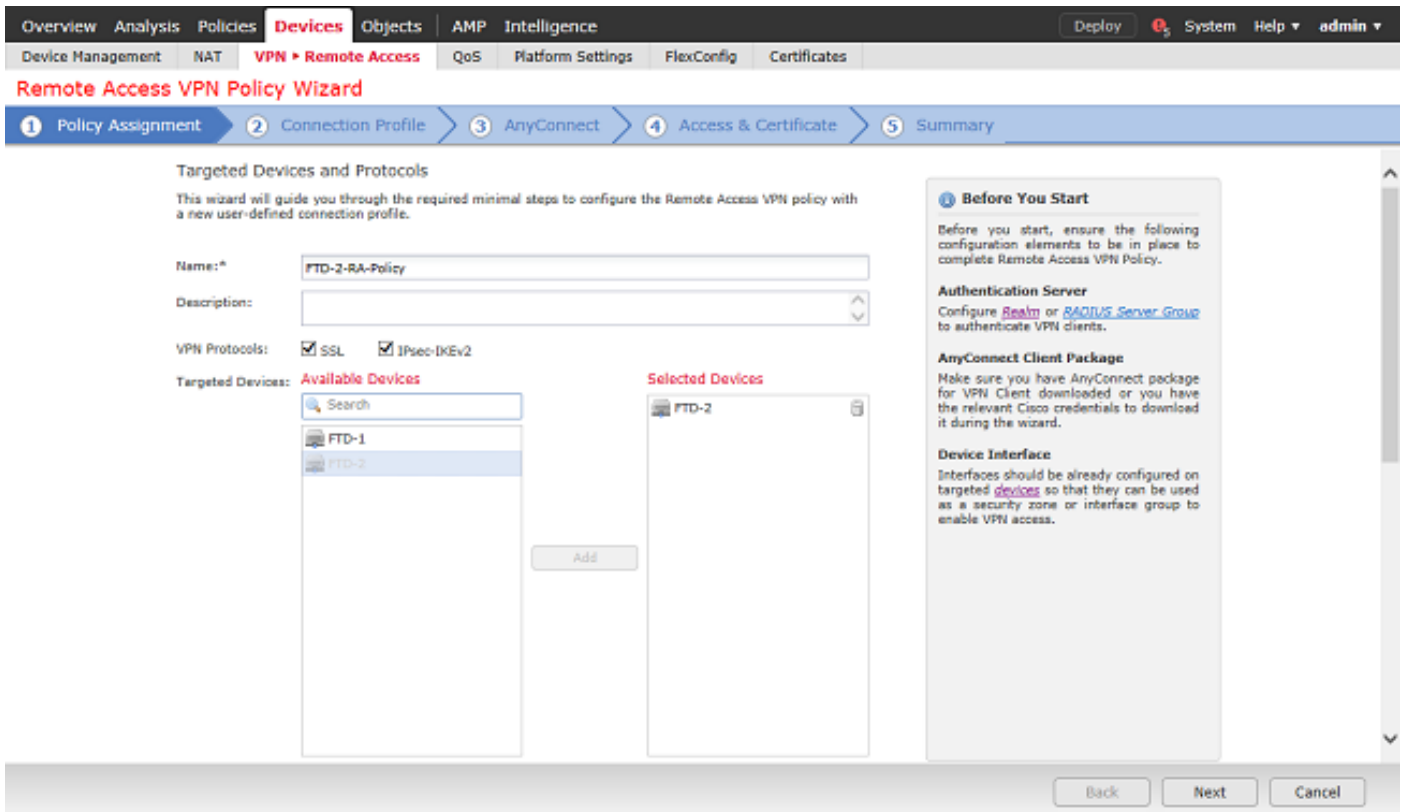
Navegue até **Devices > VPN > Remote Access**.



Clique em **Adicionar** para criar uma nova política de VPN de acesso remoto



2. Conclua o **Assistente de Política de VPN de Acesso Remoto**. Em **Atribuição de política**, especifique um nome para a política e os dispositivos aos quais a política é aplicada.



Em Perfil de conexão, especifique o nome do Perfil de conexão que também é usado como o alias de grupo que os usuários de AnyConnect visualizam quando se conectam.

Especifique o realm criado anteriormente em Servidor de autenticação.

Especifique que os clientes AnyConnect são endereços IP atribuídos.

Especifique a política de grupo padrão usada para esse perfil de conexão.

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help admin

Device Management NAT **VPN > Remote Access** QoS Platform Settings FlexConfig Certificates

Remote Access VPN Policy Wizard

1 Policy Assignment 2 **Connection Profile** 3 AnyConnect 4 Access & Certificate 5 Summary

Connection Profile:
 Connection Profiles specify the tunnel group policies for a VPN connection. These policies pertain to creating the tunnel itself, how AAA is accomplished and how addresses are assigned. They also include user attributes, which are defined in group policies.

Connection Profile Name: *
This name is configured as a connection alias, it can be used to connect to the VPN gateway

Authentication, Authorization & Accounting (AAA):
 Specify the method of authentication (AAA, certificates or both), and the AAA servers that will be used for VPN connections.

Authentication Method:
 Authentication Server: * (Realm or RADIUS)
 Authorization Server: (RADIUS)
 Accounting Server: (RADIUS)

Client Address Assignment:
 Client IP address can be assigned from AAA server, DHCP server and IP address pools. When multiple options are selected, IP address assignment is tried in the order of AAA server, DHCP server and IP address pool.

Use AAA Server (RADIUS only) ⓘ
 Use DHCP Servers
 Use IP Address Pools

IPv4 Address Pools:
 IPv6 Address Pools:

Group Policy:
 A group policy is a collection of user-oriented session attributes which are assigned to client when a VPN connection is established. Select or create a Group Policy object.

Group Policy: * [Edit Group Policy](#)

Back Next Cancel

Em AnyConnect, carregue e especifique os pacotes usados do AnyConnect.

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help admin

Device Management NAT **VPN > Remote Access** QoS Platform Settings FlexConfig Certificates

Remote Access VPN Policy Wizard

1 Policy Assignment 2 Connection Profile 3 **AnyConnect** 4 Access & Certificate 5 Summary

AnyConnect Client Image
 The VPN gateway can automatically download the latest AnyConnect package to the client device when the VPN connection is initiated. Minimize connection setup time by choosing the appropriate OS for the selected package.

Download AnyConnect Client packages from Cisco Software Download Center.

Show Re-order buttons

<input checked="" type="checkbox"/>	AnyConnect File Object Name	AnyConnect Client Package Name	Operating System
<input checked="" type="checkbox"/>	anyconnect-linux64-4.7.03052-we...	anyconnect-linux64-4.7.03052-webdeploy-k9...	Linux
<input checked="" type="checkbox"/>	anyconnect-win-4.7.00136-webde...	anyconnect-win-4.7.00136-webdeploy-k9.pkg	Windows

Back Next Cancel

Em **Acesso e certificado**, especifique a interface que os usuários de AnyConnect acessam para o AnyConnect.

Crie e/ou especifique o certificado usado pelo FTD durante o handshake SSL.

Certifique-se de que a caixa de seleção **Política de controle de acesso de contorno** para tráfego descryptografado (sysopt permit-vpn) esteja desmarcada para que a identidade do usuário criada posteriormente entre em vigor para conexões RAVPN.

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help admin

Device Management NAT **VPN > Remote Access** QoS Platform Settings FlexConfig Certificates

Remote Access VPN Policy Wizard

1 Policy Assignment 2 Connection Profile 3 AnyConnect 4 Access & Certificate 5 Summary

Network Interface for Incoming VPN Access
 Select or create an Interface Group or a Security Zone that contains the network interfaces users will access for VPN connections.

Interface group/Security Zone: * +

Enable DTLS on member interfaces

Device Certificates
 Device certificate (also called Identity certificate) identifies the VPN gateway to the remote access clients. Select a certificate which is used to authenticate the VPN gateway.

Certificate Enrollment: * +

Enroll the selected certificate object on the target devices

Access Control for VPN Traffic
 All decrypted traffic in the VPN tunnel is subjected to the Access Control Policy by default. Select this option to bypass decrypted traffic from the Access Control Policy.

Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)
This option bypasses the Access Control Policy inspection, but VPN filter ACL and authorization ACL downloaded from AAA server are still applied to VPN traffic.

Back Next Cancel

Em **Resumo**, revise a configuração e clique em **Concluir**.

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help admin

Device Management NAT **VPN > Remote Access** QoS Platform Settings FlexConfig Certificates

Remote Access VPN Policy Wizard

1 Policy Assignment 2 Connection Profile 3 AnyConnect 4 Access & Certificate 5 Summary

Remote Access VPN Policy Configuration

Firepower Management Center will configure an RA VPN Policy with the following settings

Name: FTD-2-RA-Policy

Device Targets: FTD-2

Connection Profile: General

Connection Alias: General

AAA:

- Authentication Method: AAA Only
- Authentication Server: LAB-AD
- Authorization Server: -
- Accounting Server: -

Address Assignment:

- Address from AAA: -
- DHCP Servers: -
- Address Pools (IPv4): AnyConnect-Pool
- Address Pools (IPv6): -

Group Policy: DfltGrpPolicy

AnyConnect Images:

- anyconnect-linux64-4.7.03052-webdeploy-k9.pkg
- anyconnect-win-4.7.00136-webdeploy-k9.pkg

Interface Objects: outside-zone

Device Certificates: FTD-2-Selfsigned

Device Identity Certificate Enrollment

Certificate enrollment object 'FTD-2-Selfsigned' is not installed on one or more targeted devices. Certificate installation will be initiated on the targeted devices on finishing the wizard. Go to the [Certificates](#) page to check the status of the installation.

Additional Configuration Requirements

After the wizard completes, the following configuration needs to be completed for VPN to work on all device targets.

- Access Control Policy Update**
An [Access Control](#) rule must be defined to allow VPN traffic on all targeted devices.
- NAT Exemption**
If NAT is enabled on the targeted devices, you must define a [NAT Policy](#) to exempt VPN traffic.
- DNS Configuration**
To resolve hostname specified in AAA Servers or CA Servers, configure DNS using [FlexConfig Policy](#) on the targeted devices.
- Port Configuration**
SSL will be enabled on port 443. IPsec-IKEv2 uses port 500 and Client Services will be enabled on port 443 for Anyconnect image download. NAT-Traversal will be enabled by default and will use port 4500. Please ensure that these ports are not used in [NAT Policy](#) or other services before deploying the configuration.

Network Interface Configuration
 Make sure to add interface from targeted devices to SecurityZone object 'outside-zone'

Back Finish Cancel

3. Na Política de VPN de Acesso Remoto, clique em editar para o Perfil de Conexão apropriado.

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help admin

Device Management NAT **VPN > Remote Access** QoS Platform Settings FlexConfig Certificates

FTD-2-RA-Policy Save Cancel

Enter Description Policy Assignments (1)

Connection Profile Access Interfaces Advanced

Name	AAA	Group Policy
DefaultWEBVPNGroup	Authentication: None Authorization: None Accounting: None	DfltGrpPolicy
General	Authentication: LAB-AD (AD) Authorization: None Accounting: None	DfltGrpPolicy

Verifique se o servidor de autenticação foi definido para o realm criado anteriormente.

Em **Configurações avançadas**, a opção **Habilitar gerenciamento de senha** pode ser marcada para permitir que os usuários alterem a senha quando a senha expirar ou antes.

No entanto, essa configuração exige que o realm use LDAPS. Se alguma alteração tiver sido feita, clique em **Salvar**.

Edit Connection Profile ? X

Connection Profile:* General

Group Policy:* DfltGrpPolicy Edit Group Policy

Client Address Assignment **AAA** Aliases

Authentication

Authentication Method: AAA Only

Authentication Server: LAB-AD (AD)

Use secondary authentication

Authorization

Authorization Server:

Allow connection only if user exists in authorization database

Accounting

Accounting Server:

Advanced Settings

Strip Realm from username

Strip Group from username

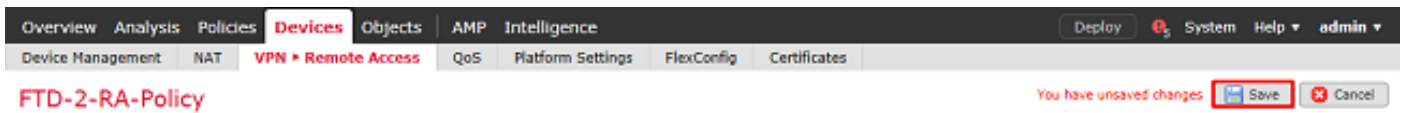
Enable Password Management

Notify User 14 days prior to password expiration

Notify user on the day of password expiration

Save Cancel

Quando terminar, clique em **Salvar** no canto superior direito.



Ativar política de identidade e configurar políticas de segurança para identidade do usuário

1. Navegue até **Policies > Access Control > Identity**.



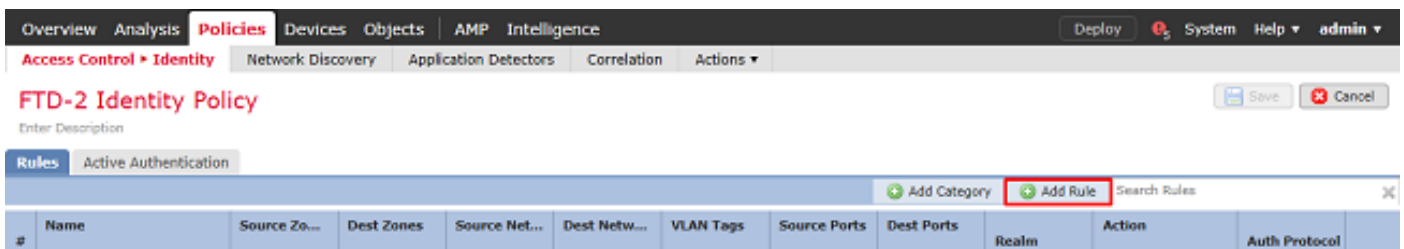
Crie uma nova política de identidade.



Especifique um nome para a nova política de identidade.



2. Clique em **Adicionar Regra**.



3. Especifique um **Nome** para a nova regra. Verifique se ela foi ativada e se a ação foi definida como Autenticação passiva.

Clique na guia **Realm e configurações** e selecione o realm criado anteriormente. Clique em **Add** quando terminar.

Add Rule

Name: Enabled

Insert:

Action: Realm: LAB-AD (AD) Authentication Protocol: HTTP Basic Exclude HTTP User-Agents: None

Remote access VPN sessions are actively authenticated by VPN. Other sessions use the rule Action.

Zones Networks VLAN Tags Ports **Realm & Settings**

Realm *

Use active authentication if passive or VPN identity cannot be established

* Required Field

Add Cancel

4. Clique em Salvar.

Overview Analysis **Policies** Devices Objects AMP Intelligence Deploy System Help admin

Access Control > Identity Network Discovery Application Detectors Correlation Actions

FTD-2 Identity Policy You have unsaved changes **Save** Cancel

Rules Active Authentication

#	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
Root Rules											
This category is empty											

Displaying 1 - 1 of 1 rules Page 1 of 1

5. navegue até Políticas > Access Control > Access Control.

Overview Analysis **Policies** Devices Objects AMP Intelligence Deploy System Help admin

Access Control > Identity Network Discovery Application Detectors Correlation Actions

Access Control

- Intrusion
- Malware & File
- DNS
- Identity**
- SSL
- Prefilter

6. Edite a Política de Controle de Acesso na qual o FTD está configurado.

Overview Analysis **Policies** Devices Objects AMP Intelligence Deploy System Help admin

Access Control > Access Control Network Discovery Application Detectors Correlation Actions

Object Management Intrusion Network Analysis Policy DNS Import/Export

New Policy

Access Control Policy	Status	Last Modified
Default-Policy	Targeting 1 devices Up-to-date on all targeted devices	2020-05-04 09:15:56 Modified by "admin"

7. Clique no valor ao lado de **Política de Identidade**.



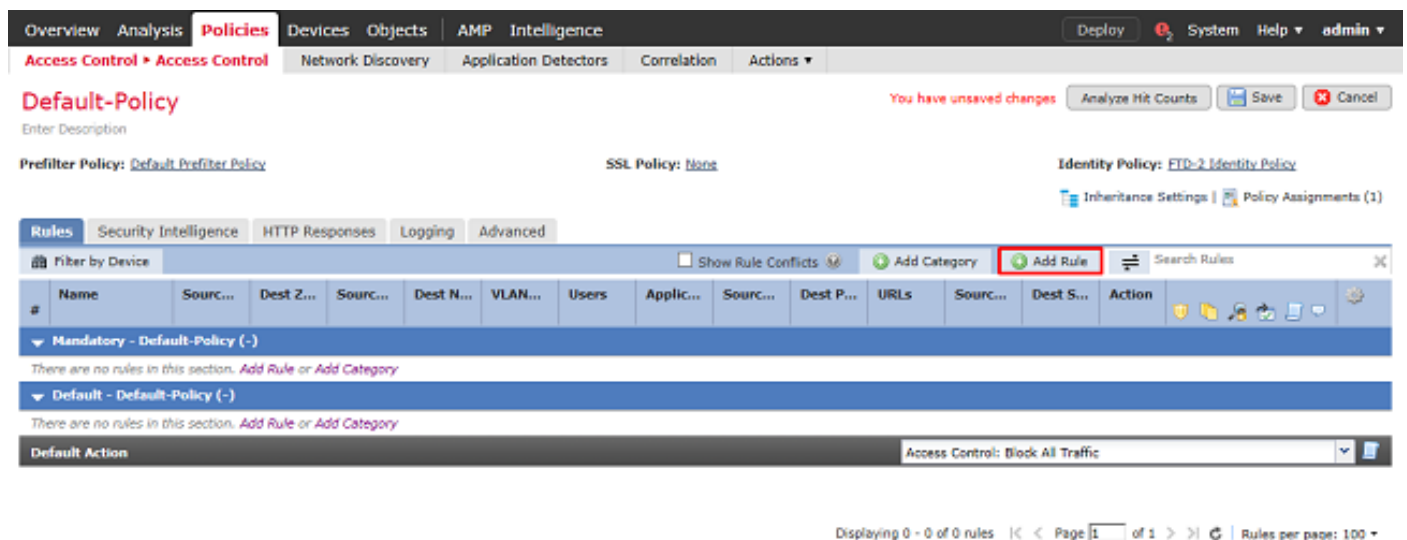
The screenshot shows the 'Policies' configuration page for 'Default-Policy'. The 'Identity Policy' field is highlighted with a red box and contains the value 'None'. Other fields include 'Prefilter Policy' (Default Prefilter Policy) and 'SSL Policy' (None). Buttons for 'Analyze Hit Counts', 'Save', and 'Cancel' are visible.

Selecione a política de identidade criada anteriormente e clique em **OK**.



The screenshot shows the 'Identity Policy' selection dialog. The dropdown menu is open, showing 'FTD-2 Identity Policy' selected and highlighted with a red box. The 'OK' button is also highlighted with a red box. Other buttons include 'Revert to Defaults' and 'Cancel'.

8. Clique em **Adicionar Regra** para criar uma nova regra de ACP. Essas etapas criam uma regra para permitir que o usuário no grupo Administradores de AnyConnect seja conectado aos dispositivos dentro da rede interna usando RDP.

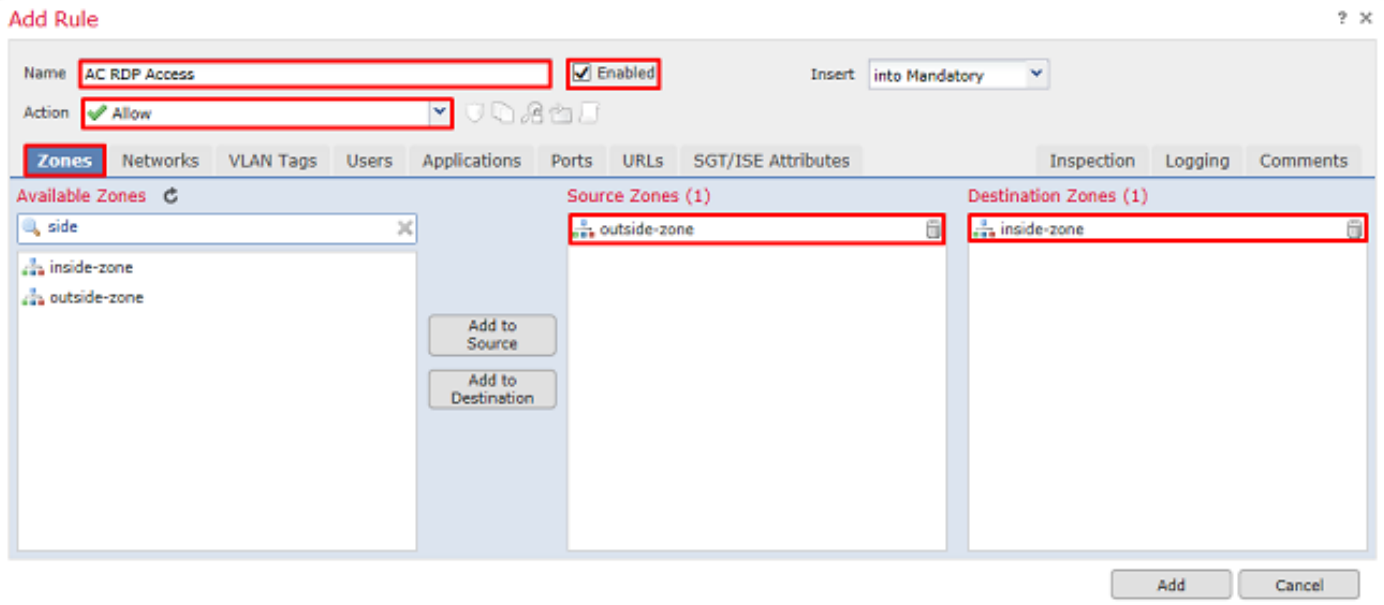


The screenshot shows the 'Rules' configuration page for 'Default-Policy'. The 'Add Rule' button is highlighted with a red box. The page displays a table of rules with columns for Name, Source, Destination, Users, Application, and Action. The 'Default Action' is set to 'Access Control: Block All Traffic'. The 'Add Rule' button is highlighted with a red box.

Especifique um nome para a regra. Verifique se a regra foi ativada e tem a ação adequada.

Na guia **Zonas**, especifique as zonas adequadas para o tráfego de interesse.

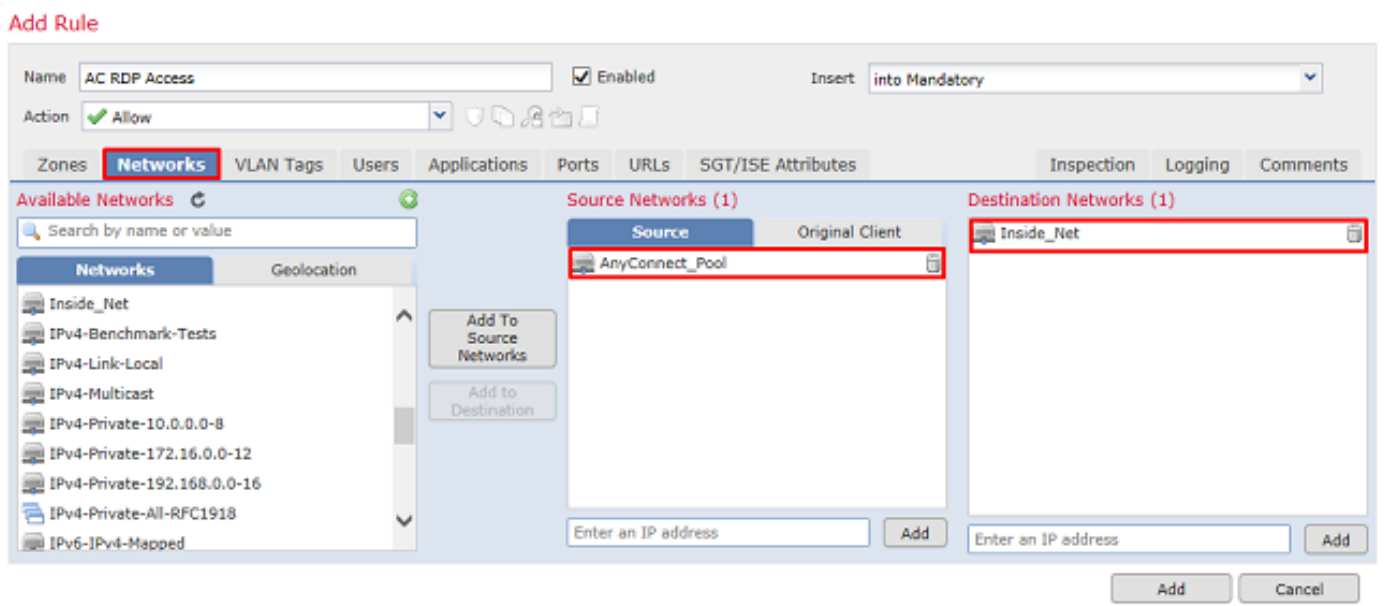
O tráfego RDP iniciado pelos usuários entra no FTD originado pela interface do outside-zone e sai do inside-zone.



Em **Redes**, defina as redes de origem e de destino.

O objeto AnyConnect_Pool inclui os endereços IP atribuídos aos clientes do AnyConnect.

O objeto Inside_Net inclui a sub-rede interna.

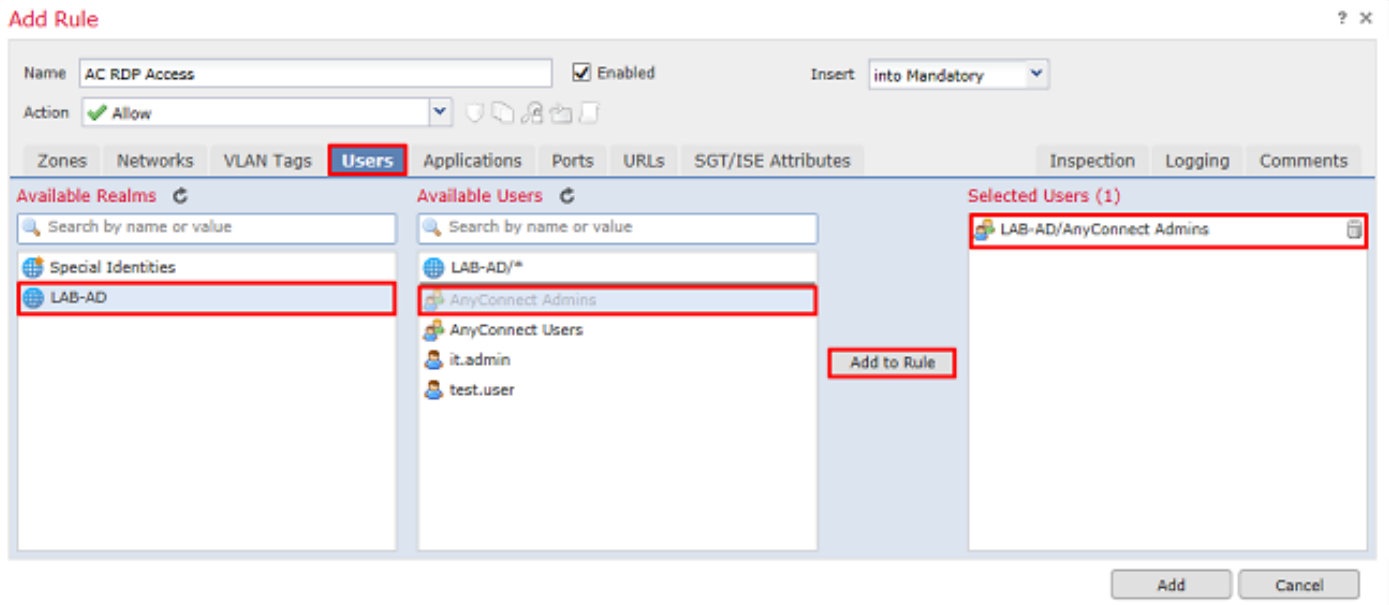


Em **Usuários**, clique no território criado anteriormente em **Territórios disponíveis**, clique no grupo/usuário apropriado em **Usuários disponíveis** e clique em **Adicionar à regra**.

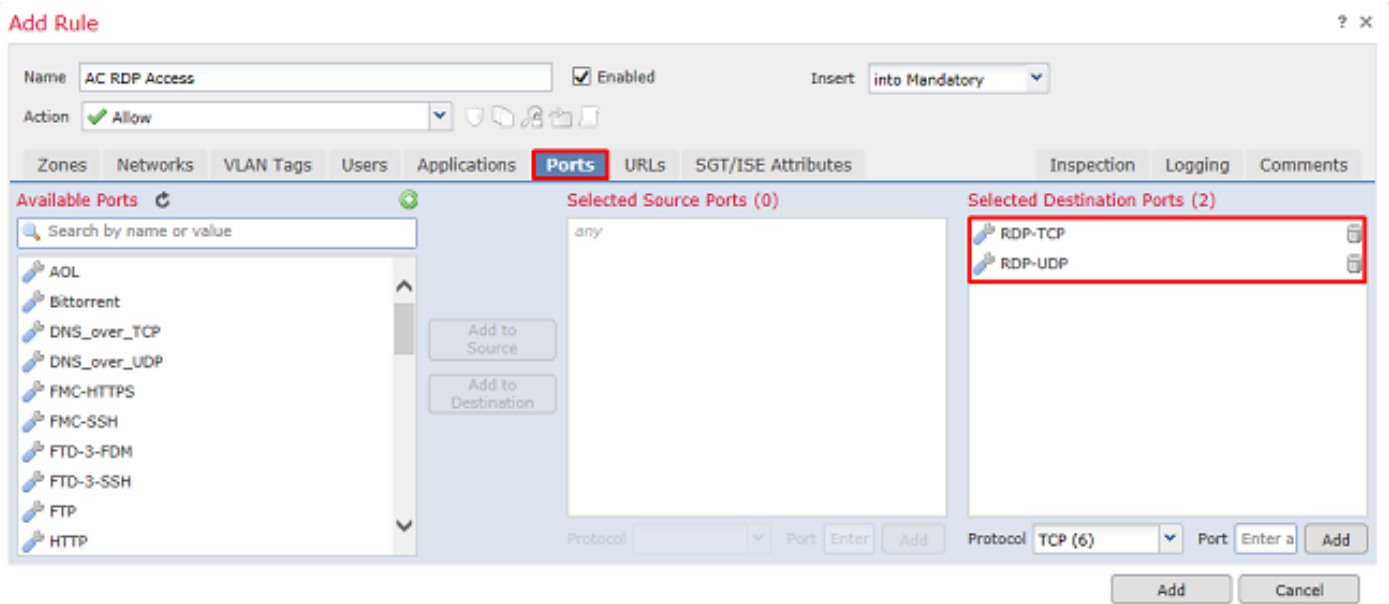
Se não houver usuários ou grupos disponíveis na seção Usuários disponíveis, verifique se o FMC baixou os usuários e grupos na seção Realm e se os Grupos/usuários adequados foram incluídos.

Os usuários/grupos especificados aqui são verificados da perspectiva de origem.

Por exemplo, com o que foi definido nesta regra até agora, o FTD avalia se o tráfego foi originado no outside-zone e destinado ao inside-zone, originado na rede no objeto AnyConnect_Pools e destinado à rede do Inside_Net, e se o tráfego foi originado em um usuário no grupo Administradores de AnyConnect.



Em Portas, os objetos RDP personalizados foram criados e adicionados para permitir a porta TCP e UDP 3389. Observe que não foi possível adicionar RDP na seção Aplicações, mas para simplificar, apenas as portas são verificadas.



Por fim, em Registro, o Registro ao final da conexão é marcado para uma verificação adicional posteriormente. Clique em Adicionar quando terminar.

Add Rule ? x

Name: Enabled Insert:

Action:

Zones Networks VLAN Tags Users Applications Ports URLs SGT/ISE Attributes Inspection **Logging** Comments

Log at Beginning of Connection
 Log at End of Connection

File Events:
 Log Files

Send Connection Events to:
 Event Viewer
 Syslog Server (Using default syslog configuration in Access Control Logging) [Show Overrides](#)
 SNMP Trap

9. Uma regra adicional é criada para o acesso HTTP para permitir que os usuários no grupo **AnyConnect User** acessem o site do **Windows Server IIS**. Click **Save**.

Overview Analysis **Policies** Devices Objects AMP Intelligence Deploy System Help admin

Access Control **Access Control** Network Discovery Application Detectors Correlation Actions

Default-Policy You have unsaved changes

Enter Description

Prefilter Policy: [Default Prefilter Policy](#) SSL Policy: [None](#) Identity Policy: [FTD-2 Identity Policy](#)

Inheritance Settings | Policy Assignments (1)

Rules Security Intelligence HTTP Responses Logging Advanced

Filter by Device Show Rule Conflicts

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	V...	Users	A...	S...	Dest Ports	U...	S...	D...	Action	
▼ Mandatory - Default-Policy (1-2)															
1	AC RDP Access	outside-zone	inside-zone	AnyConnect_Pool	Inside_Net	Any	LAB-AD/AnyConnect Admins	Any	Any	RDP-TCP RDP-UDP	Any	Any	Any	Allow	
2	AC HTTP Access	outside-zone	inside-zone	AnyConnect_Pool	Inside_Net	Any	LAB-AD/AnyConnect Users	Any	Any	HTTP	Any	Any	Any	Allow	
▼ Default - Default-Policy (-)															
There are no rules in this section. Add Rule or Add Category															

Default Action:

Displaying 1 - 2 of 2 rules | Page 1 of 1 | Rules per page: 100

Configurar isenção de NAT

Se houver regras de NAT que afetem o tráfego do AnyConnect, como as regras de PAT da Internet, é importante configurar as regras de isenção de NAT para que o tráfego do AnyConnect não seja afetado pelo NAT.

1. Navegue até **Devices > NAT**.

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help admin

Device Management **NAT** VPN QoS Platform Settings FlexConfig Certificates

Selecione a política de NAT aplicada ao FTD.

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help admin

Device Management **NAT** VPN QoS Platform Settings FlexConfig Certificates

NAT Policy	Device Type	Status	
FTD-2-NAT-Policy	Threat Defense	Targeting 1 devices Up-to-date on all targeted devices	

2. Nesta Política de NAT, há um PAT dinâmico no final do qual o PAT afeta todo o tráfego (incluindo o tráfego do AnyConnect) que sai da interface externa para a interface externa.

Para evitar que o tráfego do AnyConnect seja afetado pelo NAT, clique em **Adicionar regra** na parte superior direita.

FTD-2-NAT-Policy

Rules

Filter by Device

Add Rule

#	Direction	Type	Source Interface Object	Destination Interface Object	Original Sources	Original Destinations	Orig... Services	Translated Sources	Translated Destinations	Trans... Services	Options
NAT Rules Before											
Auto NAT Rules											
=	→	Dynamic	any	outside-zone	obj-any		Interface			Dns:false	
NAT Rules After											

Displaying 1-1 of 1 rows | Page 1 of 1 | Rows per page: 100

3. Configure uma regra de isenção de NAT, certifique-se de que a regra seja Manual NAT Rule with Type Static. Essa é uma regra NAT bidirecional que se aplica ao tráfego do AnyConnect.

Com essas configurações, quando o FTD detecta o tráfego originado em Inside_Net e destinado ao endereço IP do AnyConnect (definido por AnyConnect_Pool), a origem é convertida no mesmo valor (Inside_Net) e o destino é convertido no mesmo valor (AnyConnect_Pool), quando o tráfego entra no inside_zone e sai do outside_zone. Basicamente, isso ignora a NAT quando essas condições são atendidas.

Add NAT Rule

NAT Rule: Manual NAT Rule

Type: Static

Enable

Description:

Interface Objects

Available Interface Objects

zone

inside-zone

outside-zone

Source Interface Objects (1)

inside-zone

Destination Interface Objects (1)

outside-zone

Add to Source

Add to Destination

OK

Cancel

Add NAT Rule ? X

NAT Rule: Manual NAT Rule Insert: In Category NAT Rules Before

Type: Static Enable

Description:

Interface Objects **Translation** PAT Pool Advanced

Original Packet

Original Source:* Inside_Net

Original Destination: Address

AnyConnect_Pool

Original Source Port:

Original Destination Port:

Translated Packet

Translated Source: Address

Translated Destination: Inside_Net

AnyConnect_Pool

Translated Source Port:

Translated Destination Port:

OK Cancel

Além disso, o FTD é definido para executar uma pesquisa de rota nesse tráfego e não o ARP de proxy. Clique em **OK** quando terminar.

Add NAT Rule ? X

NAT Rule: Manual NAT Rule Insert: In Category NAT Rules Before

Type: Static Enable

Description:

Interface Objects Translation PAT Pool **Advanced**

Translate DNS replies that match this rule

Falthrough to Interface PAT(Destination Interface)

IPv6

Net to Net Mapping

Do not proxy ARP on Destination Interface

Perform Route Lookup for Destination Interface

Unidirectional

OK Cancel

4. Clique em **Salvar**.

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help admin

Device Management NAT VPN QoS Platform Settings FlexConfig Certificates

FTD-2-NAT-Policy You have unsaved changes Show Warnings Save Cancel

Enter Description Policy Assignments (1)

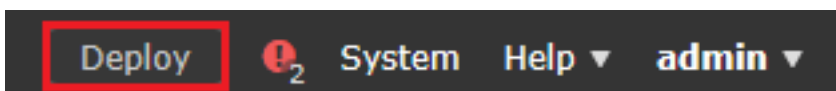
Rules Filter by Device Add Rule

#	Direction	Type	Source Interface Object	Destination Interface Object	Original Packet		Translated Packet			Options
					Original Sources	Original Destinations	Orig... Services	Translated Sources	Translated Destinations	
▼ NAT Rules Before										
1		Static	inside-zone	outside-zone	Inside_Net	AnyConnect_Pool	Inside_Net	AnyConnect_Pool		Dns:false route-lookup no-proxy-arp
▼ Auto NAT Rules										
=		Dynamic	any	outside-zone	obj-any		Interface			Dns:false
▼ NAT Rules After										

Displaying 1-2 of 2 rows Page 1 of 1 Rows per page: 100

Implantar

1. Quando a configuração estiver concluída, clique no botão **Implantar** no canto superior direito.



2. Clique na caixa de seleção ao lado do FTD ao qual a configuração foi aplicada e clique em **Implantar**.

Deploy Policies Version:2020-05-04 09:40 AM

<input checked="" type="checkbox"/>	Device	Inspect Interruption	Type	Group	Current Version
<input checked="" type="checkbox"/>	FTD-2	No	FTD		2020-05-04 09:16 AM

Selected devices: 1

Deploy Cancel

Verificar

Configuração final

Configuração do AAA

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

Configuração do AnyConnect

```
> show running-config webvpn
webvpn
  enable Outside
  anyconnect image disk0:/csm/anyconnect-linux64-4.7.03052-webdeploy-k9.pkg 1 regex "Linux"
  anyconnect image disk0:/csm/anyconnect-win-4.7.00136-webdeploy-k9.pkg 2 regex "Windows"
  anyconnect profiles Lab disk0:/csm/lab.xml
  anyconnect enable
  tunnel-group-list enable
  cache
  no disable
  error-recovery disable
```

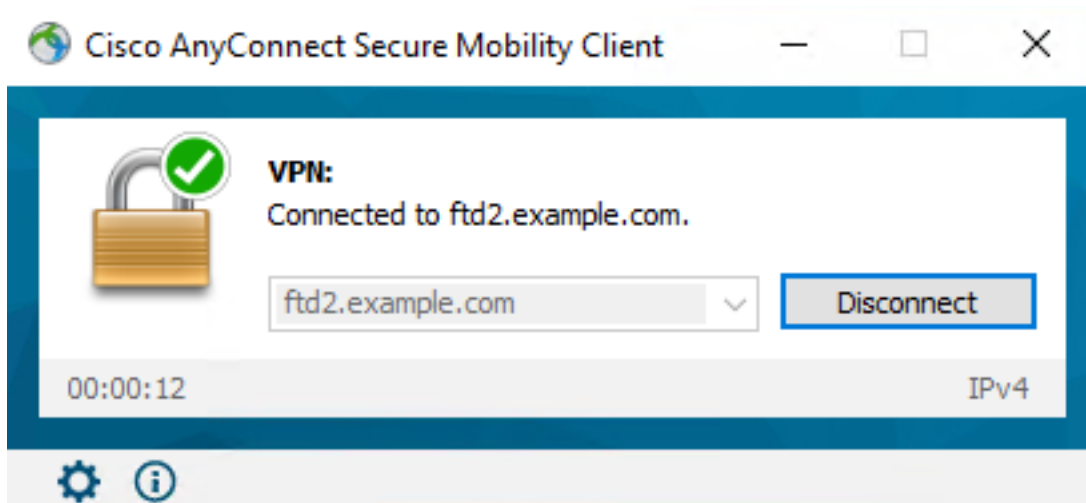
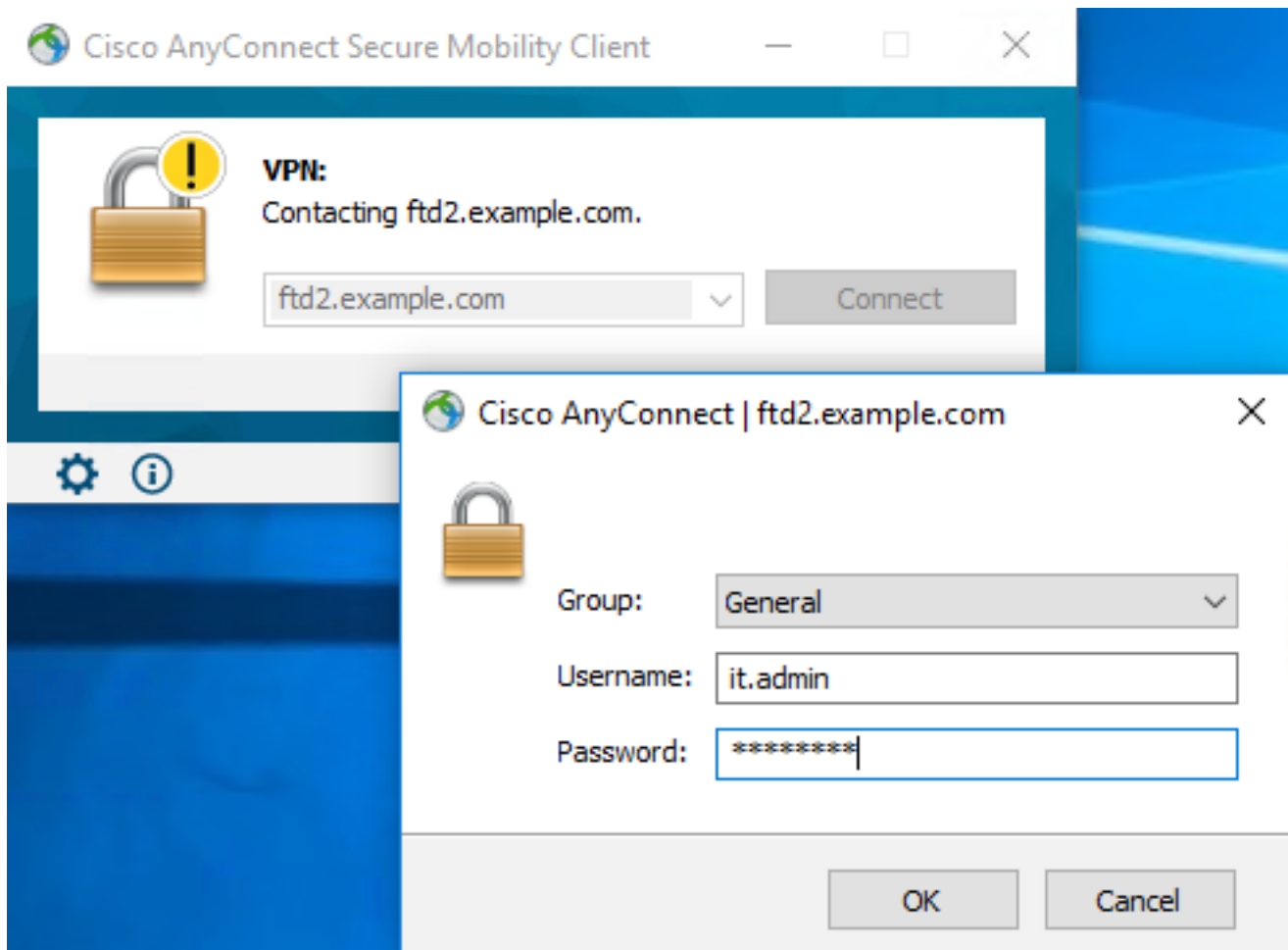
```
> show running-config tunnel-group
tunnel-group General type remote-access
tunnel-group General general-attributes
  address-pool AnyConnect-Pool
  authentication-server-group LAB-AD
tunnel-group General webvpn-attributes
  group-alias General enable
```

```
> show running-config group-policy
group-policy DfltGrpPolicy attributes
  vpn-simultaneous-logins 10
  vpn-tunnel-protocol ikev2 ssl-client
  split-tunnel-policy tunnelspecified
  split-tunnel-network-list value Lab
  user-authentication-idle-timeout none
webvpn
  anyconnect keep-installer none
  anyconnect modules value dart
  anyconnect ask none default anyconnect
  http-comp none
  activex-relay disable
  file-entry disable
  file-browsing disable
  url-entry disable
```

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

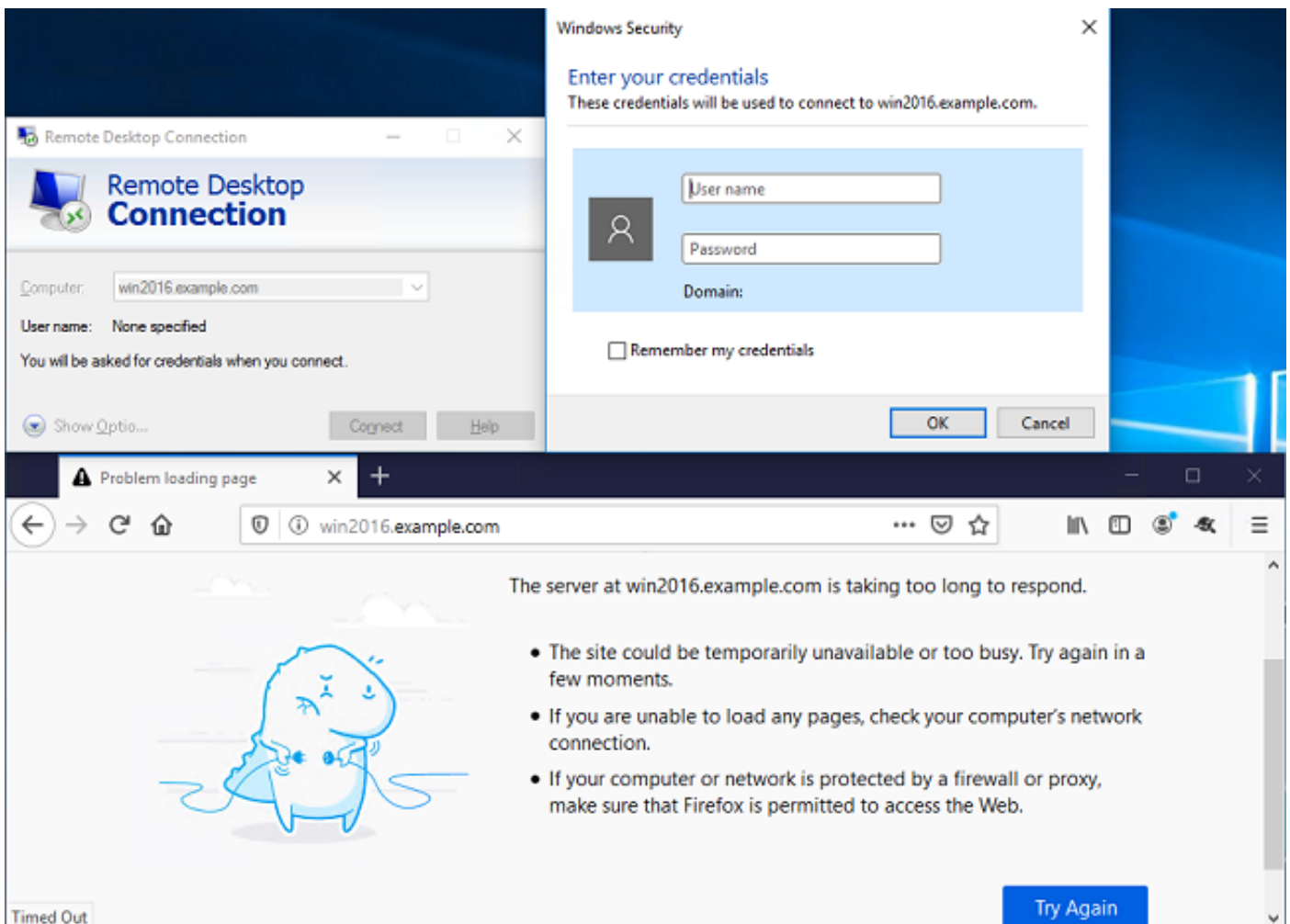
```
> show running-config ssl
ssl trust-point FTD-2-SelfSigned outside
```

Conectar-se ao AnyConnect e verificar regras de política de controle de acesso

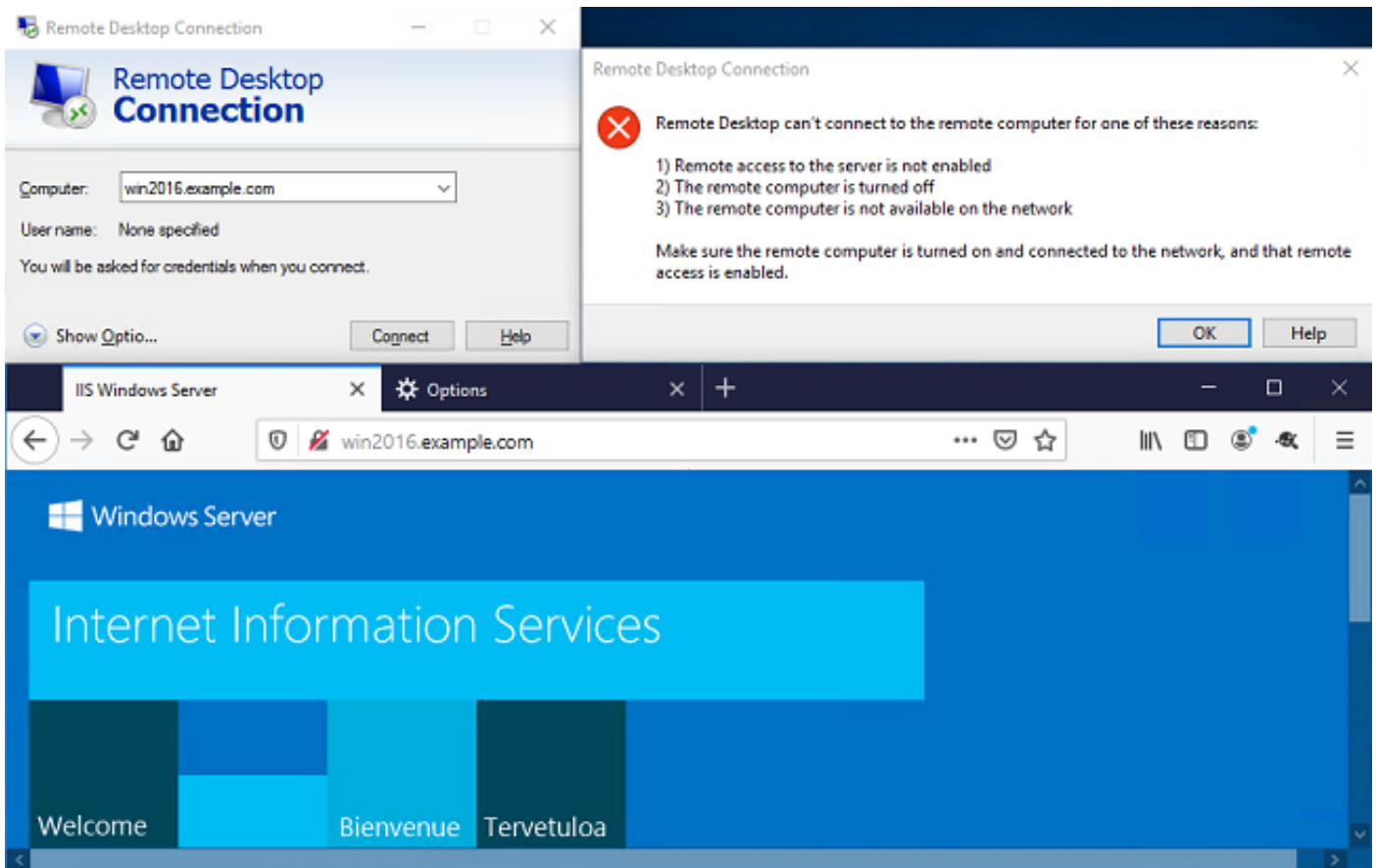


O usuário Administrador de TI está no grupo Administradores de AnyConnect que tem acesso RDP ao Windows Server, mas não tem acesso ao HTTP.

Abrir uma sessão RDP e Firefox para esse servidor verifica se esse usuário só pode acessar o servidor usando RDP.



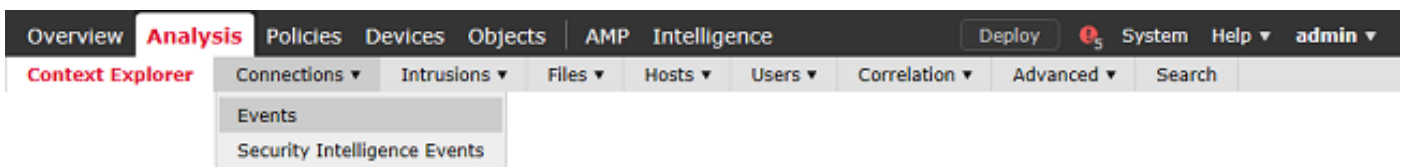
Se estivermos conectados com o usuário de teste que está no grupo Usuários de AnyConnect que tem acesso HTTP, mas não tem acesso RDP, podemos verificar se as regras de política de controle de acesso estão entrando em vigor.



Verificar com eventos de conexão do FMC

Como o registro foi ativado nas regras de política de controle de acesso, os eventos de conexão podem ser verificados para qualquer tráfego que corresponda a essas regras

Navegue até **Análise > Conexões > Eventos**.



Na **Visualização da tabela de eventos de conexão**, os registros são filtrados para mostrar apenas os eventos de conexão para o administrador de TI.

Aqui, você pode verificar se o tráfego RDP para o servidor (TCP e UDP 3389) é permitido, no entanto, o tráfego da porta 80 é bloqueado.

	Action	Initiator IP	Initiator User	Responder IP	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type	Destination Port / ICMP Code
↓	Allow	10.10.10.1	it_admin (LAB-AD\it_admin, LDAP)	192.168.1.1	outside-zone	inside-zone	62473 / tcp	3389 / tcp
↓	Block	10.10.10.1	it_admin (LAB-AD\it_admin, LDAP)	192.168.1.1	outside-zone	inside-zone	62474 / tcp	80 (http) / tcp
↓	Block	10.10.10.1	it_admin (LAB-AD\it_admin, LDAP)	192.168.1.1	outside-zone	inside-zone	62475 / tcp	80 (http) / tcp
↓	Block	10.10.10.1	it_admin (LAB-AD\it_admin, LDAP)	192.168.1.1	outside-zone	inside-zone	62476 / tcp	80 (http) / tcp

Para o usuário de teste, você pode verificar se o tráfego RDP para o servidor está bloqueado e se o tráfego da porta 80 é permitido.

	Action	Initiator IP	Initiator User	Responder IP	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type	Destination Port / ICMP Code
↓	Block	10.10.10.1	test_user (LAB-AD\test_user, LDAP)	192.168.1.1	outside-zone	inside-zone	62493 / tcp	3389 / tcp
↓	Allow	10.10.10.1	test_user (LAB-AD\test_user, LDAP)	192.168.1.1	outside-zone	inside-zone	62494 / tcp	80 (http) / tcp

Troubleshoot

Debugs

Essa depuração pode ser executada na CLI de diagnóstico para solucionar problemas relacionados à autenticação LDAP: **debug ldap 255**

Para solucionar problemas na política de controle de acesso da identidade do usuário, o comando **system support firewall-engine-debug** pode ser executado no Clish para determinar o motivo pelo qual o tráfego está sendo permitido ou bloqueado inesperadamente.

Como trabalhar com as depurações do LDAP

```
[53] Session Start
[53] New request Session, context 0x00002b1d13f4bbf0, reqType = Authentication
[53] Fiber started
[53] Creating LDAP context with uri=ldap://192.168.1.1:389
[53] Connect to LDAP server: ldap://192.168.1.1:389, status = Successful
[53] supportedLDAPVersion: value = 3
[53] supportedLDAPVersion: value = 2
[53] LDAP server 192.168.1.1 is Active directory
[53] Binding as ftd.admin@example.com
[53] Performing Simple authentication for ftd.admin@example.com to 192.168.1.1
[53] LDAP Search:
      Base DN = [DC=example,DC=com]
```

```

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

```

Não é possível estabelecer uma conexão com o servidor LDAP

```

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

```

Possíveis soluções:

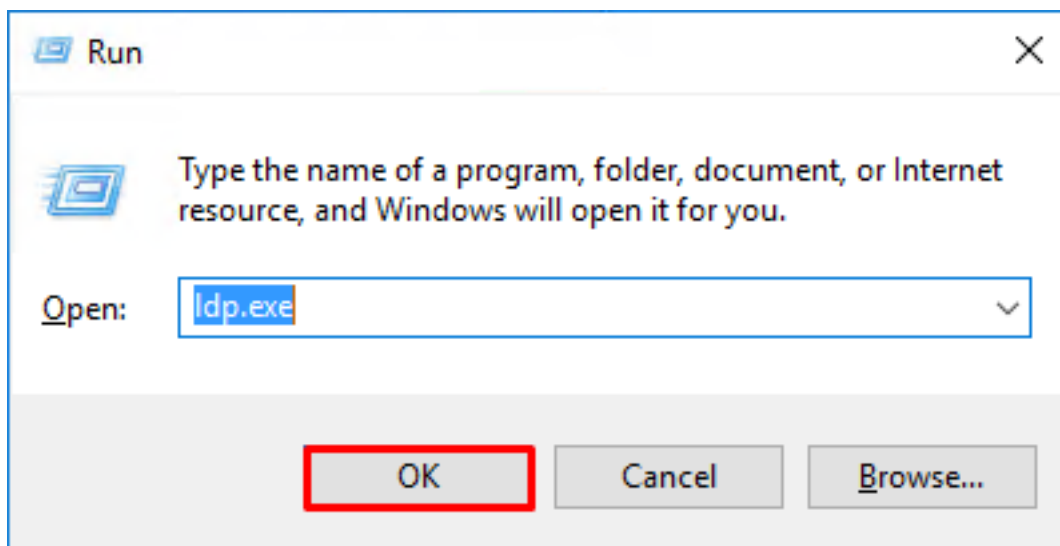
- Verifique o roteamento e certifique-se de que o FTD esteja recebendo uma resposta do servidor LDAP.
- Se LDAPS ou STARTTLS for usado, verifique se o certificado de CA raiz correto é confiável para que o handshake SSL possa ser concluído com sucesso.
- Verifique se a porta e o endereço IP corretos foram usados. Se um nome de host for usado, verifique se o DNS pode resolvê-lo para o endereço IP correto.

DN de login de vinculação incorreto e/ou senha incorreta

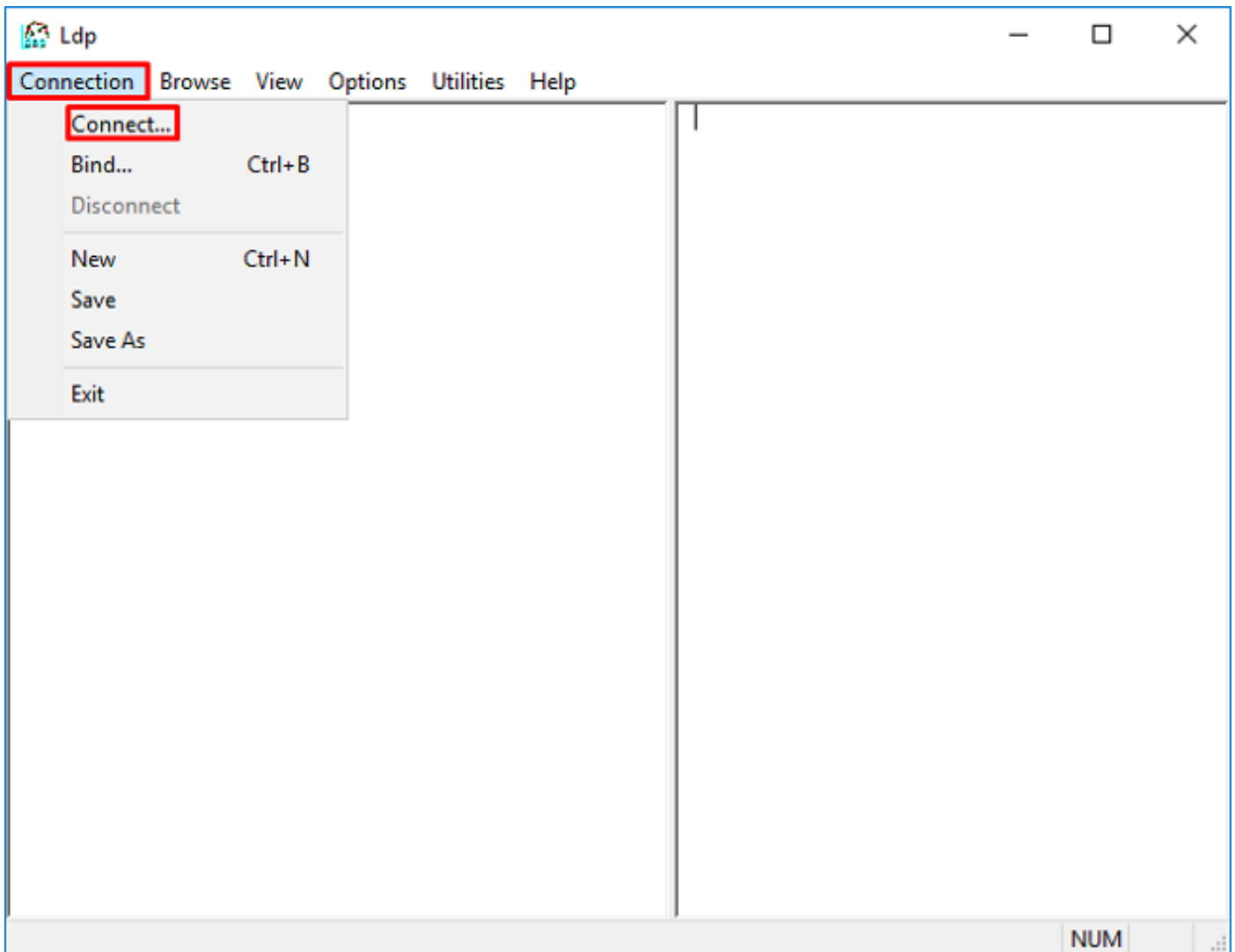
```
[-2147483615] Session Start
[-2147483615] New request Session, context 0x00007f9e65ccdc40, reqType = Authentication
[-2147483615] Fiber started
[-2147483615] Creating LDAP context with uri=ldap://192.168.1.1:389
[-2147483615] Connect to LDAP server: ldap://192.168.1.1:389, status = Successful
[-2147483615] 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
```

Solução em potencial: verifique se o DN de login e a senha de login estão configurados corretamente. Isso pode ser verificado no servidor do AD com **ldp.exe**. Para verificar se uma conta pode ser vinculada usando o ldp, siga estas etapas:

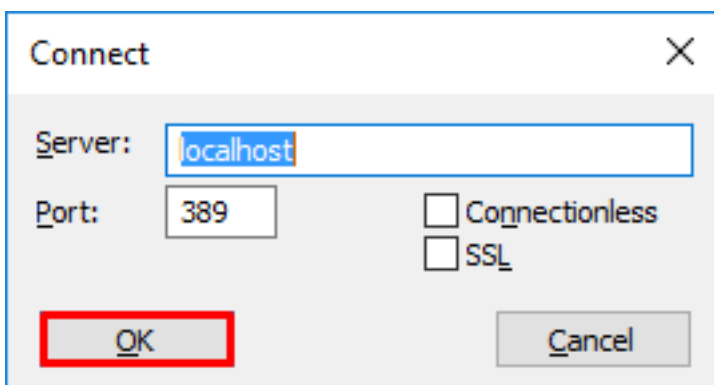
1. No servidor do AD, pressione **Win+R** e procure **ldp.exe**



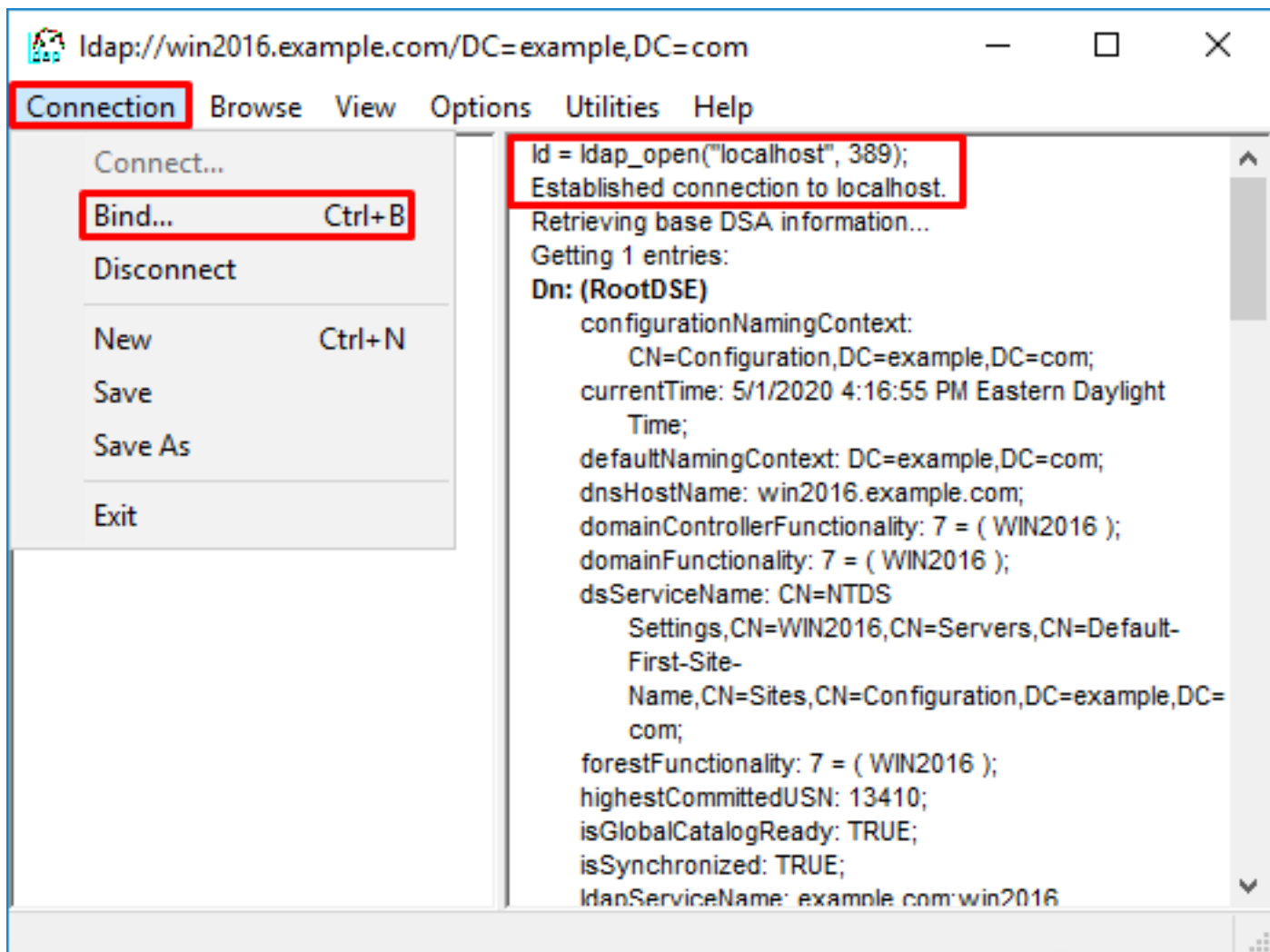
2. Em **Conexão**, escolha **Conectar...**



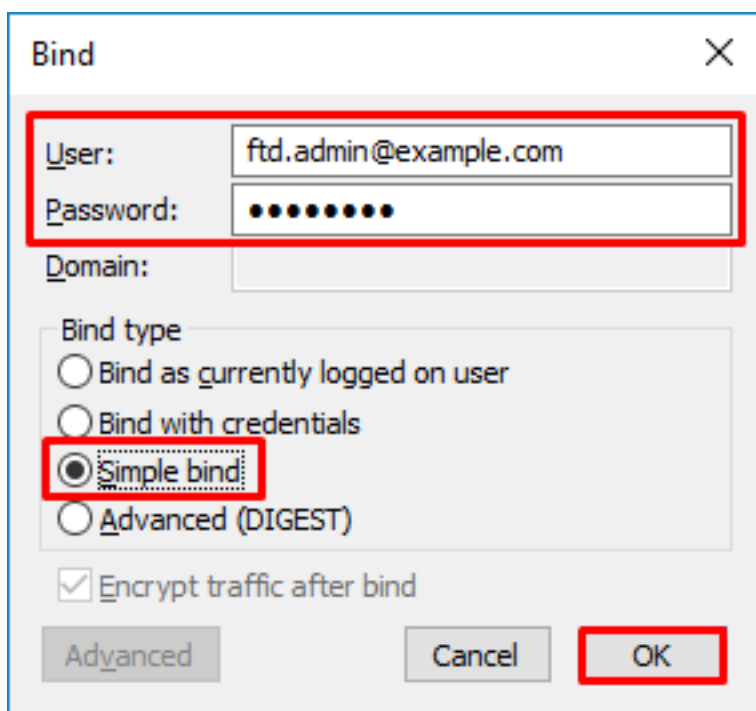
3. Especifique localhost para o servidor e a porta apropriada e clique em **OK**.



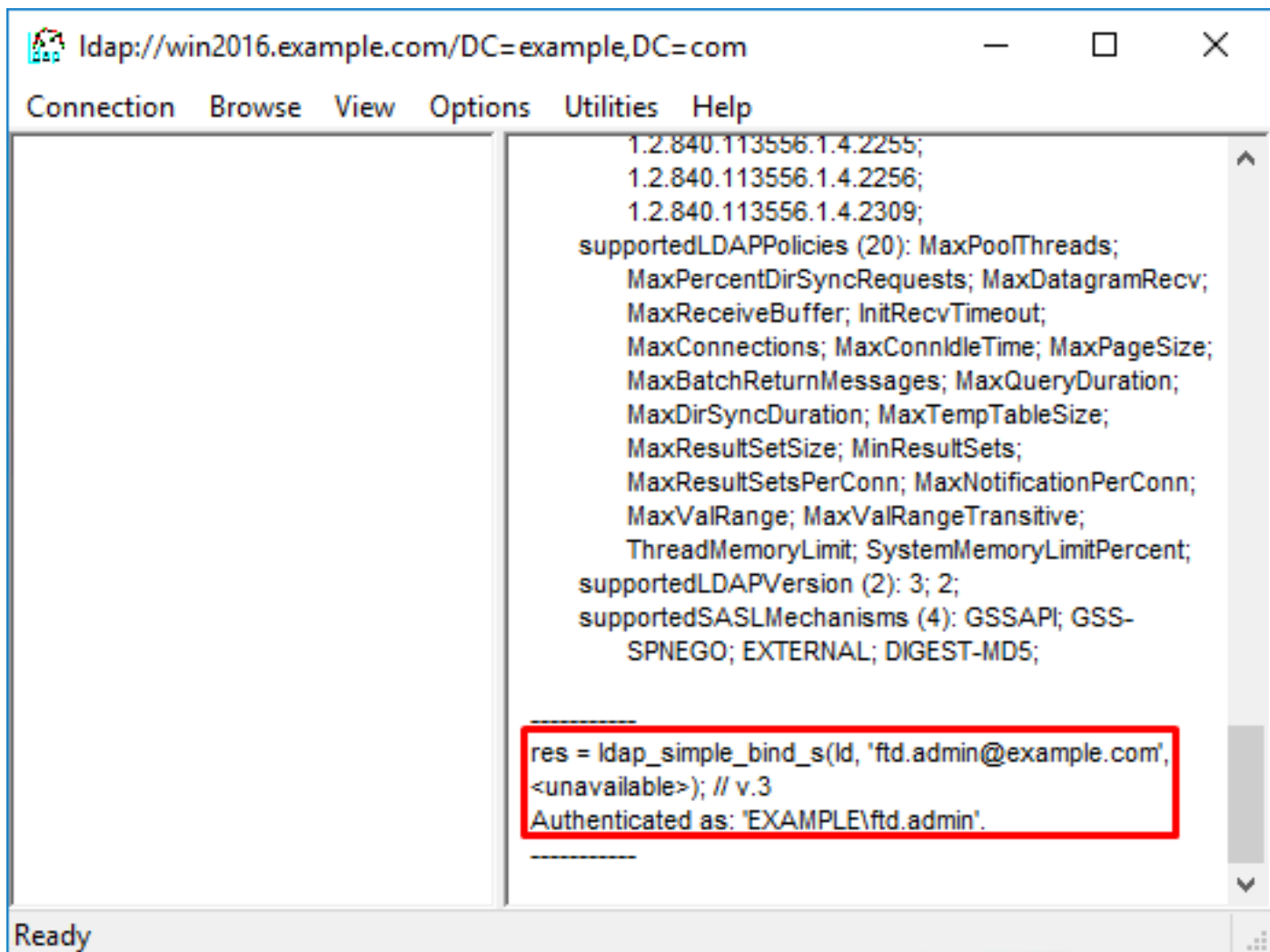
4. A coluna Direita mostra o texto que indica uma conexão bem-sucedida. Navegue até **Conexão > Vincular...**



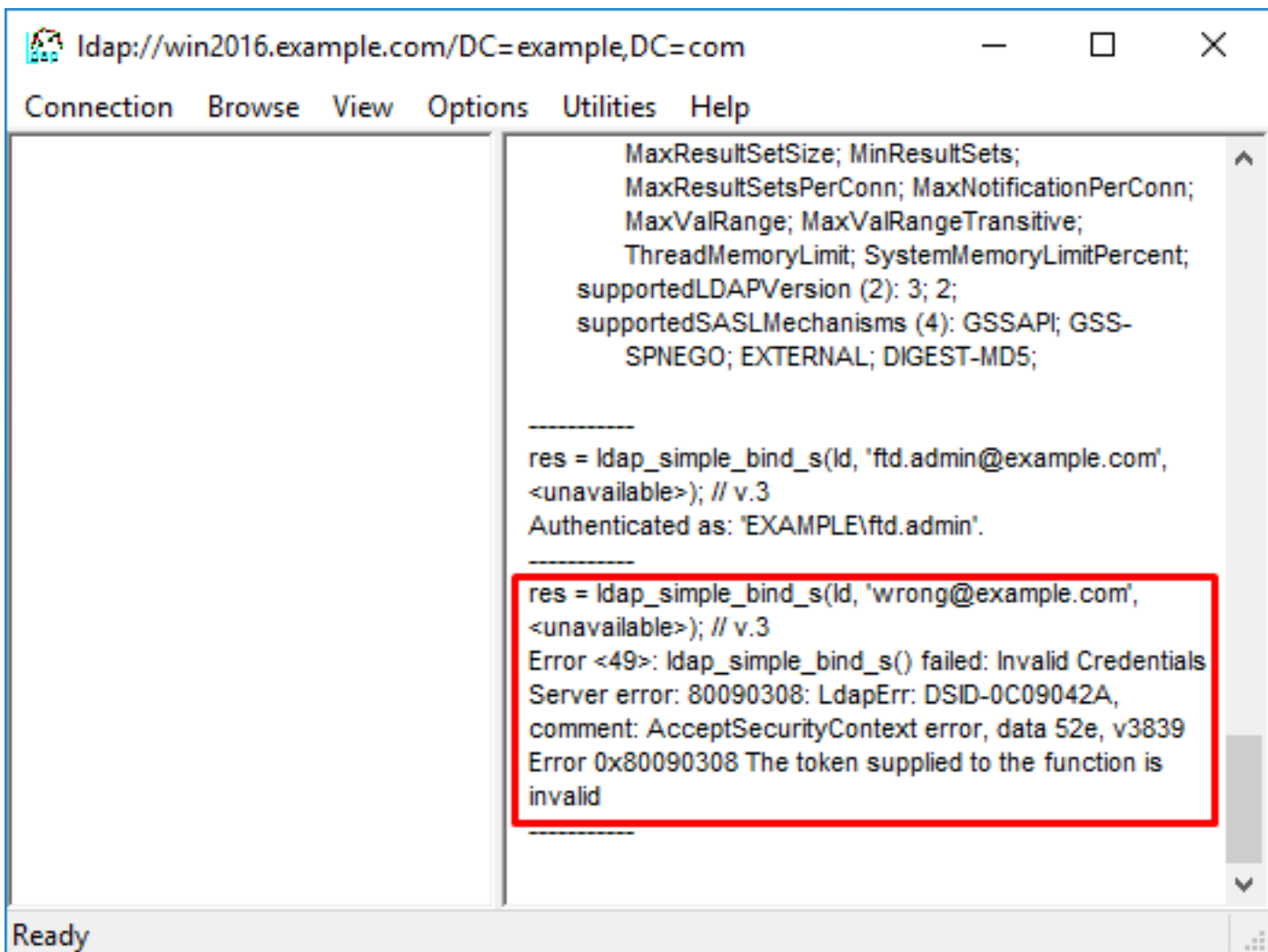
5. Selecione **Bind Simples** e, em seguida, especifique o **Nome de Usuário da Conta do Diretório** e a **Senha**. Click **OK**.



Com uma associação bem-sucedida, Idp mostra Authenticated as: **DOMAIN\username**



Uma tentativa de vinculação com um nome de usuário ou uma senha inválida resulta em uma falha, como as duas vistas aqui.

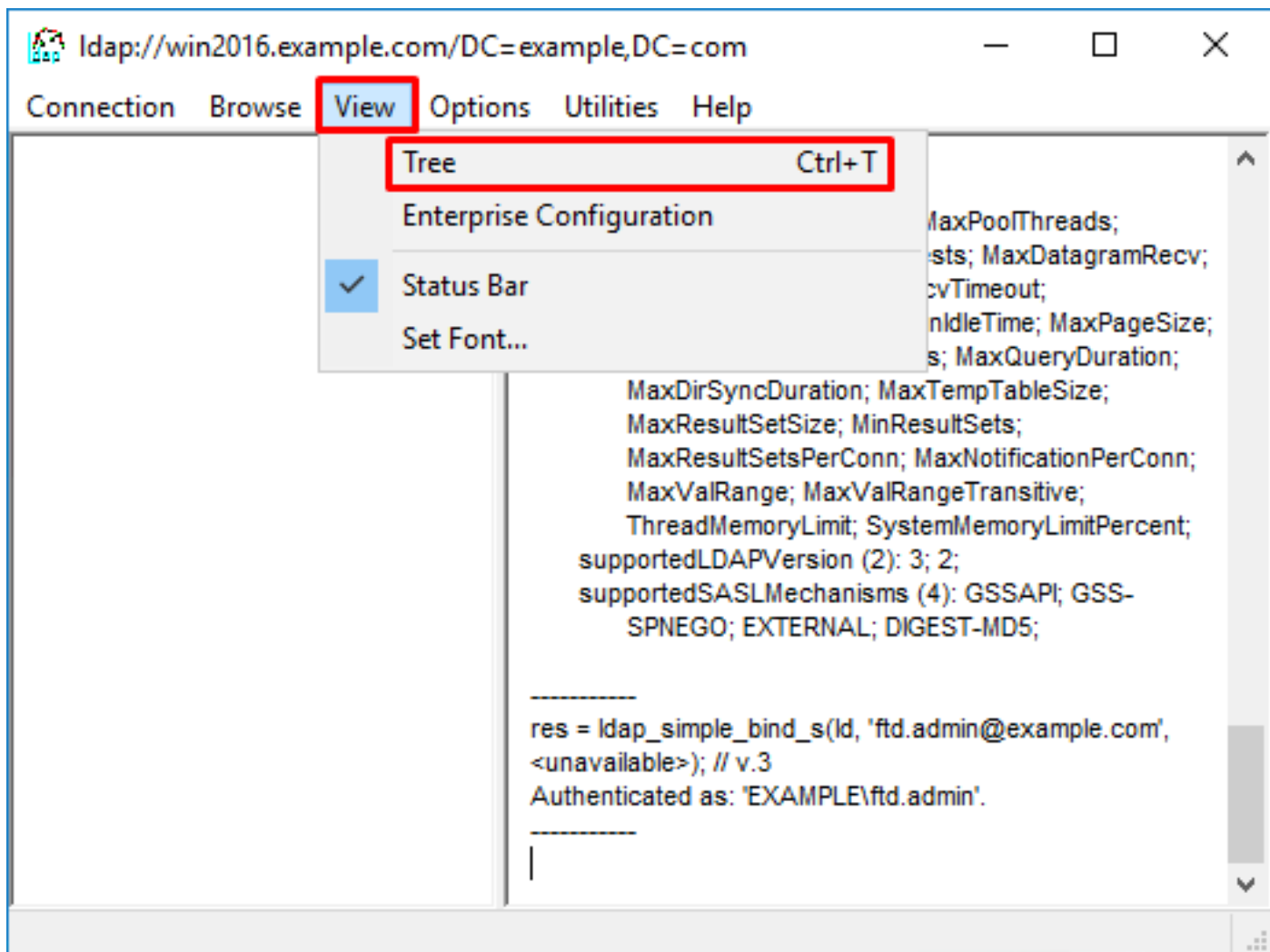


O servidor LDAP não consegue encontrar o nome de usuário

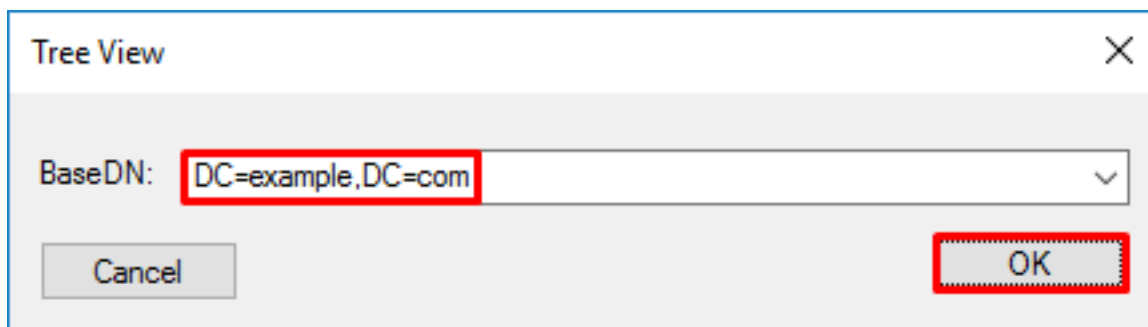
```
[-2147483612] Session Start
[-2147483612] New request Session, context 0x00007f9e65ccdc40, reqType = Authentication
[-2147483612] Fiber started
[-2147483612] Creating LDAP context with uri=ldap://192.168.1.1:389
[-2147483612] Connect to LDAP server: ldap://192.168.1.1:389, status = Successful
[-2147483612] 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
```

Solução potencial: verifique se o AD pode encontrar o usuário com a pesquisa feita pelo FTD. Isso também pode ser feito com o **ldp.exe**.

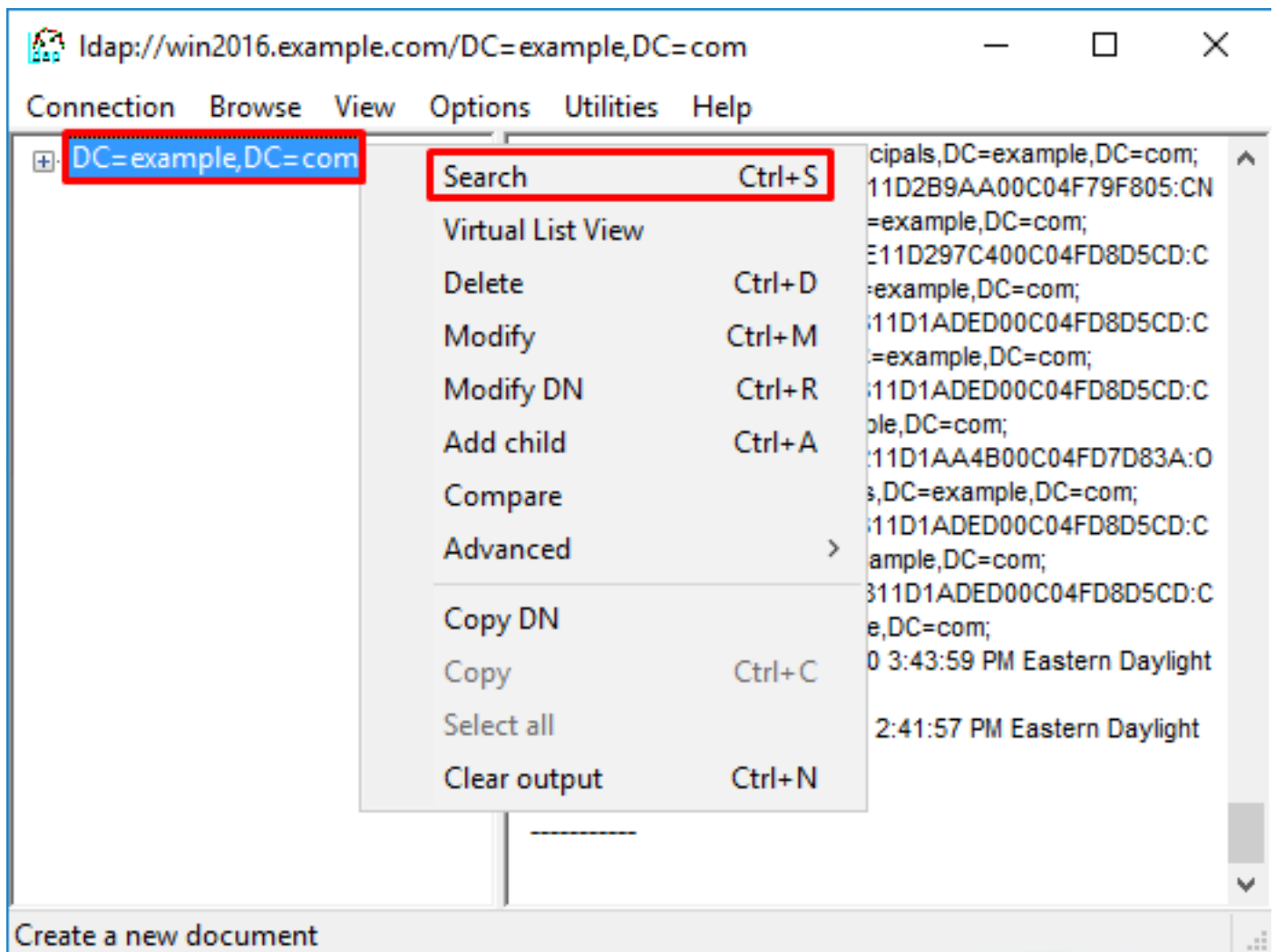
1. Após a vinculação bem-sucedida conforme visto acima, navegue até **Exibir > Árvore**.



2. Especifique o DN de Base configurado no FTD e clique em **OK**



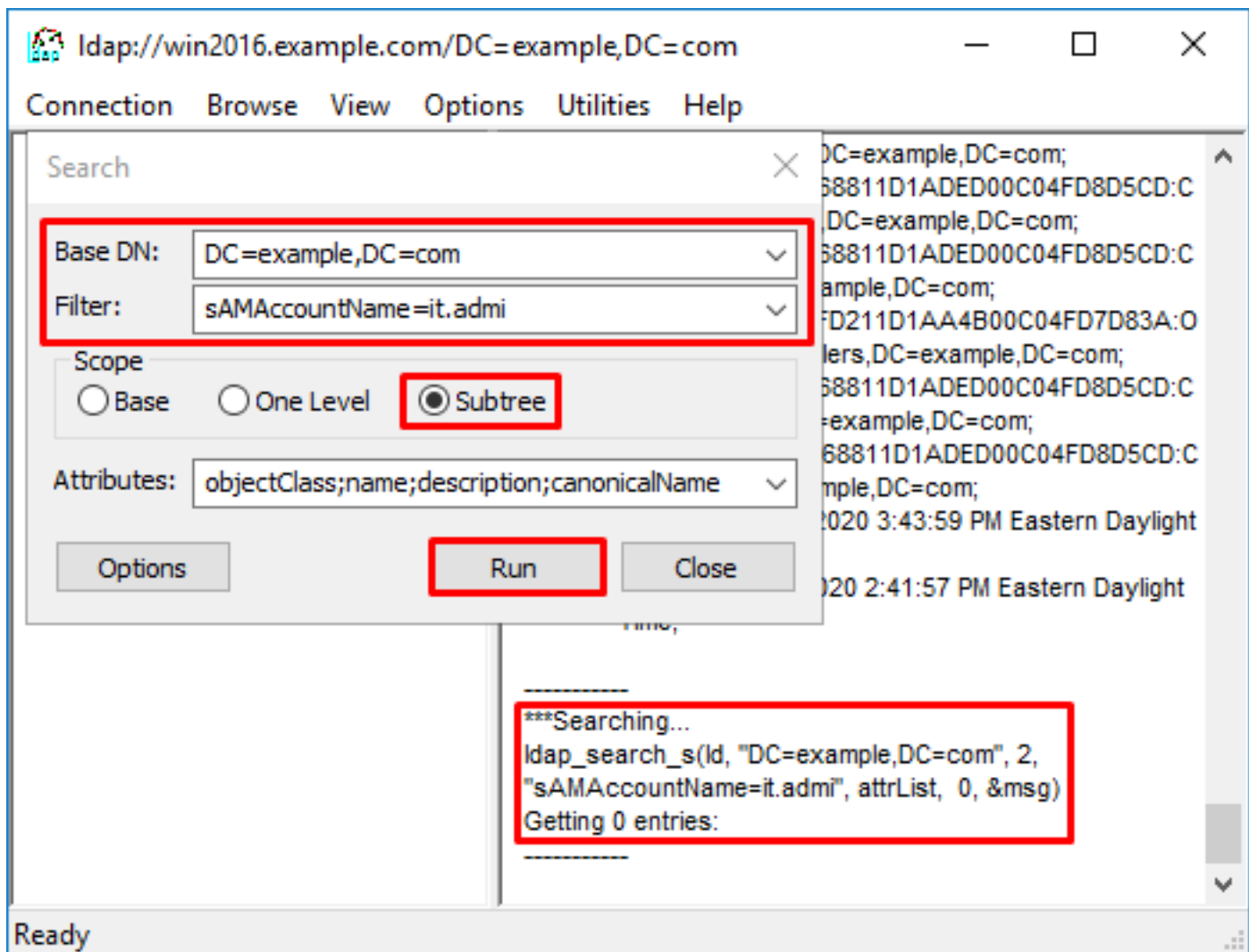
3. Clique com o botão direito do mouse no DN de Base e, em seguida, clique em **Pesquisar**.



4. Especifique os mesmos valores **Base DB**, **Filter** e **Scope** vistos nas depurações.

Neste exemplo, eles são:

- DN base: dc=example,dc=com
- Filtro: samaccountname=it.admi
- Scope:SUBTREE



o Idp localiza 0 entradas porque não há nenhuma conta de usuário com o samaccountname **it.admi** no DN base dc=example,dc=com

Outra tentativa com o samaccountname **it.admin** correto mostra um resultado diferente. Idp localiza 1 entrada sob o DN base dc=example,dc=com e imprime esse DN de usuário.

The screenshot shows a graphical user interface for an LDAP search. A 'Search' dialog box is open, with the following fields and options:

- Base DN:** DC=example,DC=com
- Filter:** sAMAccountName=it.admin
- Scope:** Base, One Level, **Subtree** (selected)
- Attributes:** objectClass;name;description;canonicalName
- Buttons:** Options, **Run** (highlighted), Close

The main window displays the search results in a list view. The first entry is highlighted:

```

68811D1AED00C04FD8D5CD:C
DC=example,DC=com;
68811D1AED00C04FD8D5CD:C
example,DC=com;
FD211D1AA4B00C04FD7D83A:O
lers,DC=example,DC=com;
68811D1AED00C04FD8D5CD:C
=example,DC=com;
68811D1AED00C04FD8D5CD:C
mple,DC=com;
020 3:43:59 PM Eastern Daylight
020 2:41:57 PM Eastern Daylight

```

Below the search results, a text box displays the search details:

```

***Searching...
ldap_search_s(ld, "DC=example,DC=com", 2,
"sAMAccountName=it.admin", attrList, 0, &msg)
Getting 1 entries:
Dn: CN=IT Admin,CN=Users,DC=example,DC=com
canonicalName: example.com/Users/IT Admin;
name: IT Admin;
objectClass (4): top; person; organizationalPerson;
user;

```

The status bar at the bottom of the window shows 'Ready'.

Senha incorreta para o nome de usuário

```

[-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]
      Scope   = [SUBTREE]
[-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
```

Possível solução: verifique se a senha do usuário está configurada corretamente e se não expirou. Semelhante ao DN de Logon, o FTD faz uma associação com o AD com as credenciais do usuário.

Essa vinculação também pode ser feita no ldp para verificar se o AD pode reconhecer as mesmas credenciais de nome de usuário e senha. As etapas no ldp são mostradas na seção **Vinculação do DN de logon e/ou senha incorreta**.

Além disso, os registros do visualizador de eventos do Microsoft Server podem ser analisados quanto aos possíveis motivos.

AAA de teste

O comando `test aaa-server` pode ser usado para simular uma tentativa de autenticação do FTD com um nome de usuário e uma senha específicos. Ele pode ser usado para testar falhas de conexão ou autenticação. O comando é **`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
```

Capturas de pacotes

As capturas de pacotes podem ser usadas para verificar a acessibilidade ao servidor do AD. Se os pacotes LDAP saem do FTD, mas não há resposta, isso pode indicar um problema de roteamento.

A captura mostra o tráfego LDAP bidirecional.

```
> 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

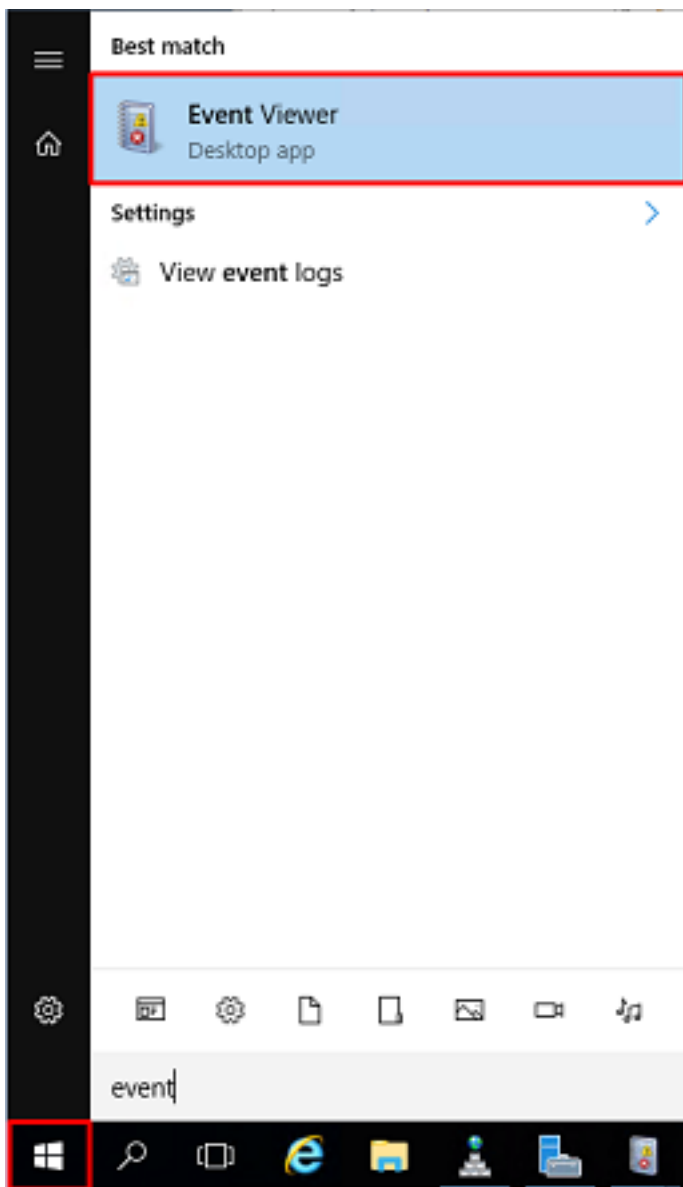
  1: 23:02:16.770712      192.168.1.17.61960 > 192.168.1.1.389: S 3681912834:3681912834(0) win
32768 <mss 1460,nop,nop,timestamp 1061373057 0>
  2: 23:02:16.772009      192.168.1.1.389 > 192.168.1.17.61960: S 491521506:491521506(0) ack
3681912835 win 8192 <mss 1460,nop,nop,timestamp 762393884 1061373057>
  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>
  5: 23:02:16.772924      192.168.1.1.389 > 192.168.1.17.61960: P 491521507:491522141(634) ack
3681912980 win 65160 <nop,nop,timestamp 762393885 1061373059>
  6: 23:02:16.772955      192.168.1.17.61960 > 192.168.1.1.389: . ack 491522141 win 32768
<nop,nop,timestamp 1061373059 762393885>
  7: 23:02:16.773428      192.168.1.17.61960 > 192.168.1.1.389: P 3681912980:3681913024(44)
ack 491522141 win 32768 <nop,nop,timestamp 1061373060 0>
  8: 23:02:16.775030      192.168.1.1.389 > 192.168.1.17.61960: P 491522141:491522163(22) ack
3681913024 win 65116 <nop,nop,timestamp 762393887 1061373060>
  9: 23:02:16.775075      192.168.1.17.61960 > 192.168.1.1.389: . ack 491522163 win 32768
<nop,nop,timestamp 1061373061 762393887>
[...]
54 packets shown

```

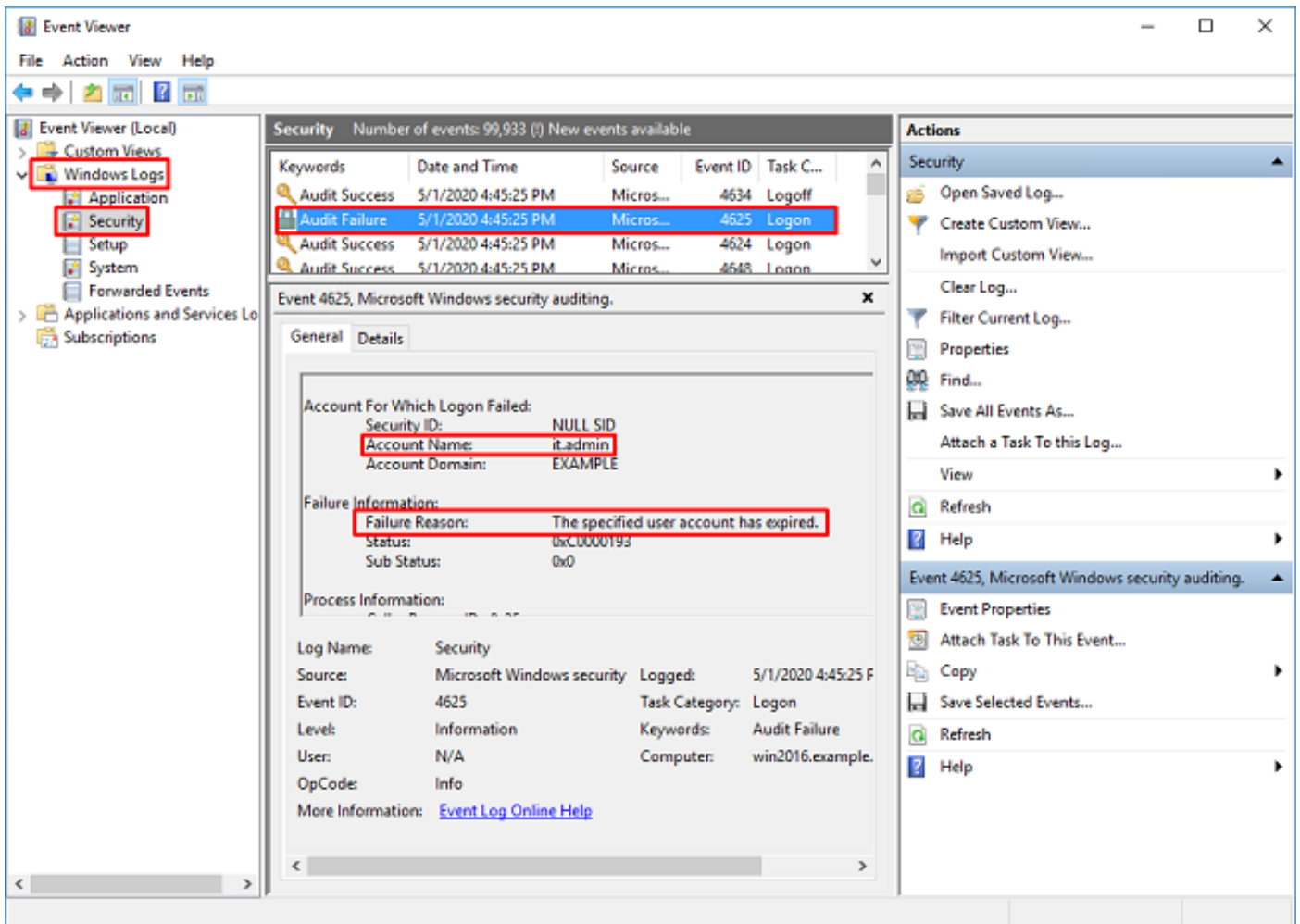
Registros do visualizador de eventos do Windows Server

Os registros do visualizador de eventos no servidor do AD podem fornecer informações mais detalhadas sobre o motivo da falha.

1. Procure e abra o Visualizador de Eventos.



2. Expanda **Logs do Windows** e clique em **Segurança**. Procure por **falhas de auditoria** com o nome da conta do usuário e revise as informações de falha.



An account failed to log on.

Subject:

Security ID:SYSTEM
Account Name:WIN2016\$\nAccount 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

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.