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

Table des matières

Introduction

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

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

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

Composants utilisés

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

- Microsoft 2016 Server
- FMCv version 6.5.0
- FTDv 6.5.0

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

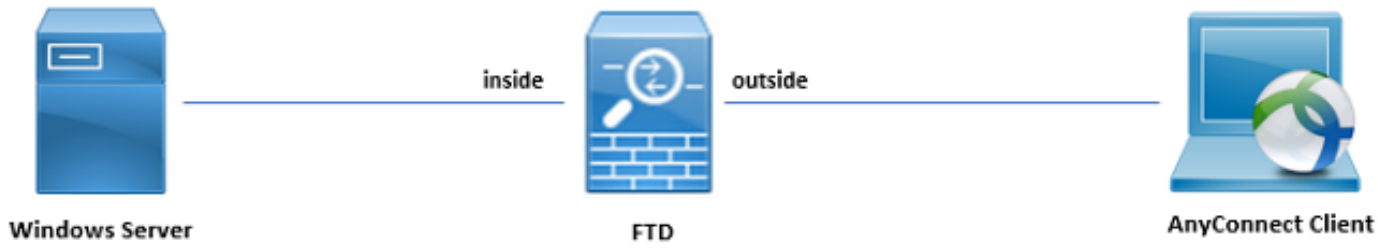
Informations générales

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

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

Configurer

Diagramme et scénario du réseau



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

Comptes utilisateurs:

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

Groupes :

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

Configurations Active Directory

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

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

- le nom de domaine:

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

- Adresse IP/FQDN du serveur :

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

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

- Port du serveur :

Port utilisé par le service LDAP. Par défaut, LDAP et STARTTLS utilisent le port TCP 389 pour LDAP, et LDAP sur SSL (LDAPS) utilise le port TCP 636.

- Autorité de certification racine :

Si LDAPS ou STARTTLS est utilisé, l'autorité de certification racine utilisée pour signer le certificat SSL utilisé par LDAPS est requise.

- Nom d'utilisateur et mot de passe du répertoire :

Il s'agit du compte utilisé par FMC et FTD pour établir une liaison avec le serveur LDAP, authentifier les utilisateurs et rechercher des utilisateurs et des groupes.

Un compte nommé FTD Admin est créé à cette fin.

- **Nom distinctif (DN) de base et de groupe** :

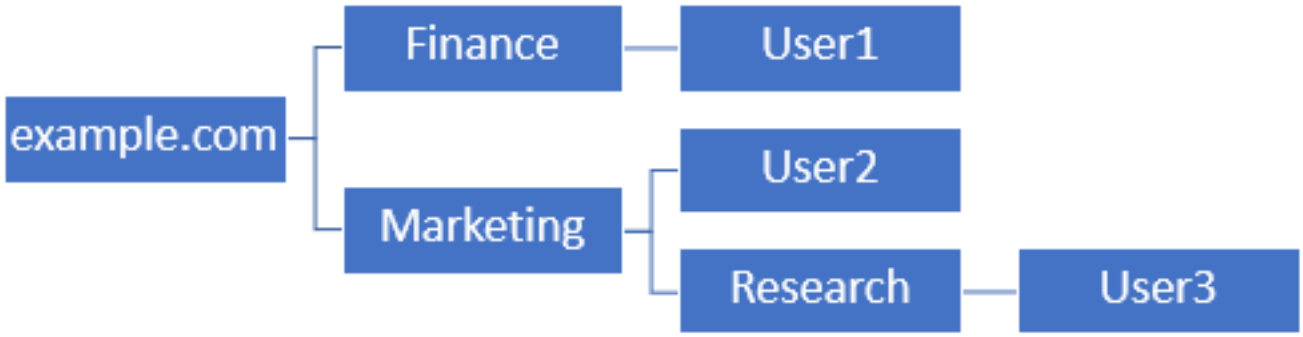
Le DN de base est le point de départ du FMC et le FTD indique à Active Directory de commencer la recherche et l'authentification des utilisateurs.

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

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

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

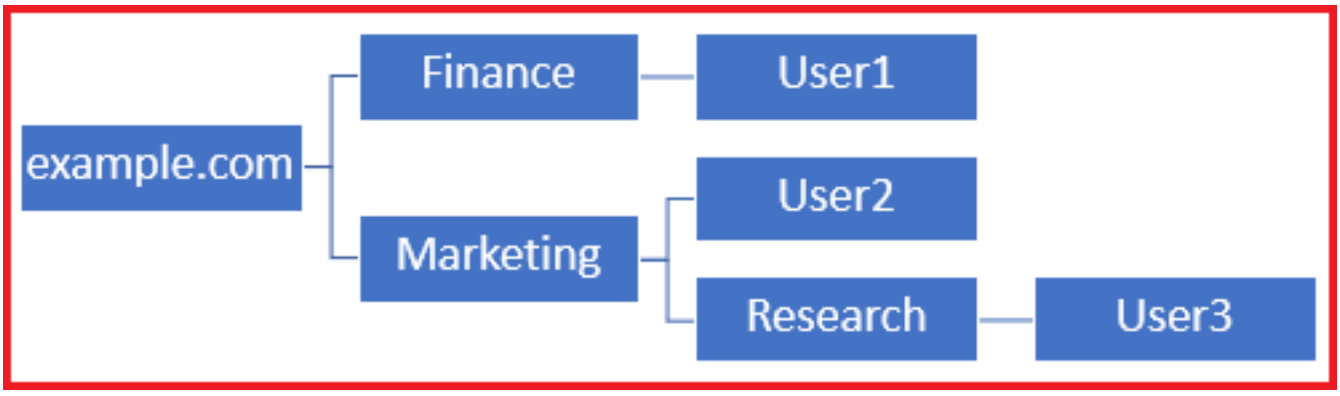
Par exemple, cette hiérarchie LDAP :



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

Cependant, cela permet également à l'utilisateur1 sous l'unité d'organisation **Finance de** se connecter également puisque la recherche de l'utilisateur commence à la racine et passe à **Finance, Marketing** et **Research**.

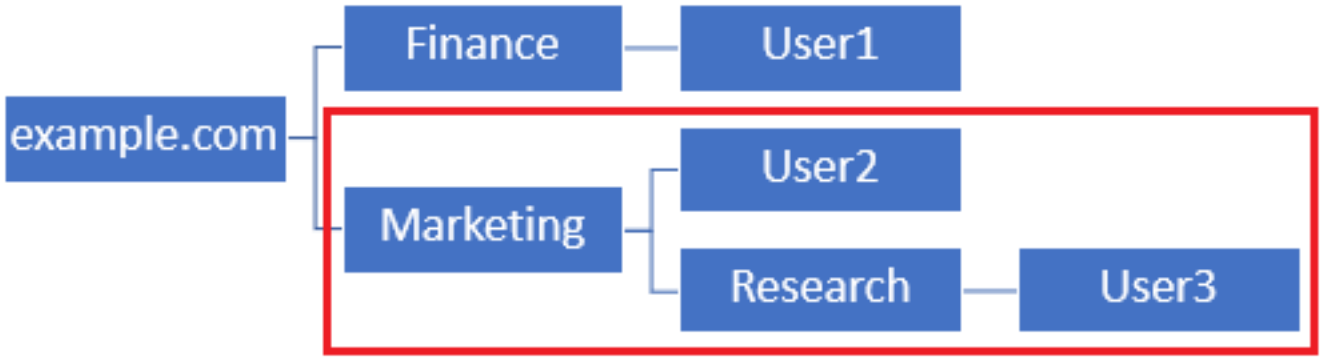
DN de base défini sur example.com



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

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

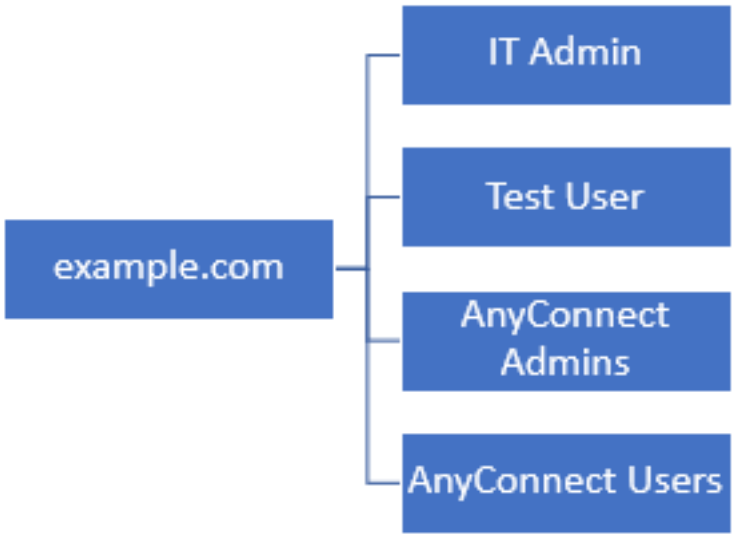
DN de base défini sur Marketing



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

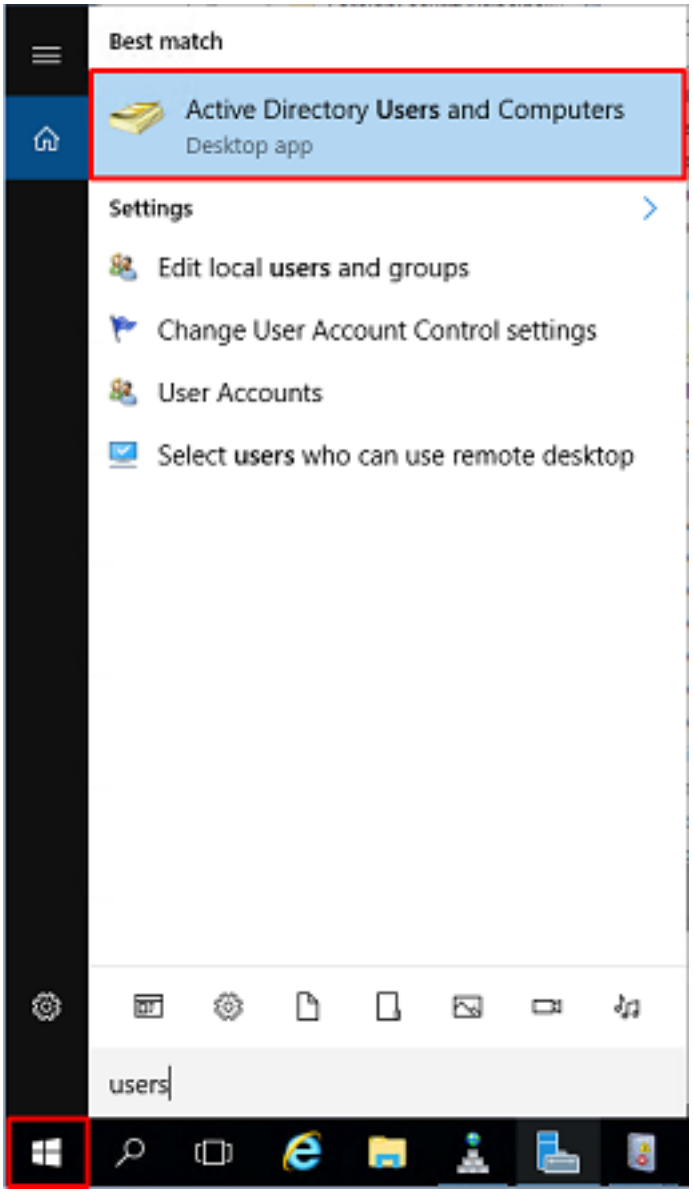
Pour plus d'informations à ce sujet, cliquez ici : Configurez le mappage LDAP AnyConnect sur Firepower Threat Defense (FTD).

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

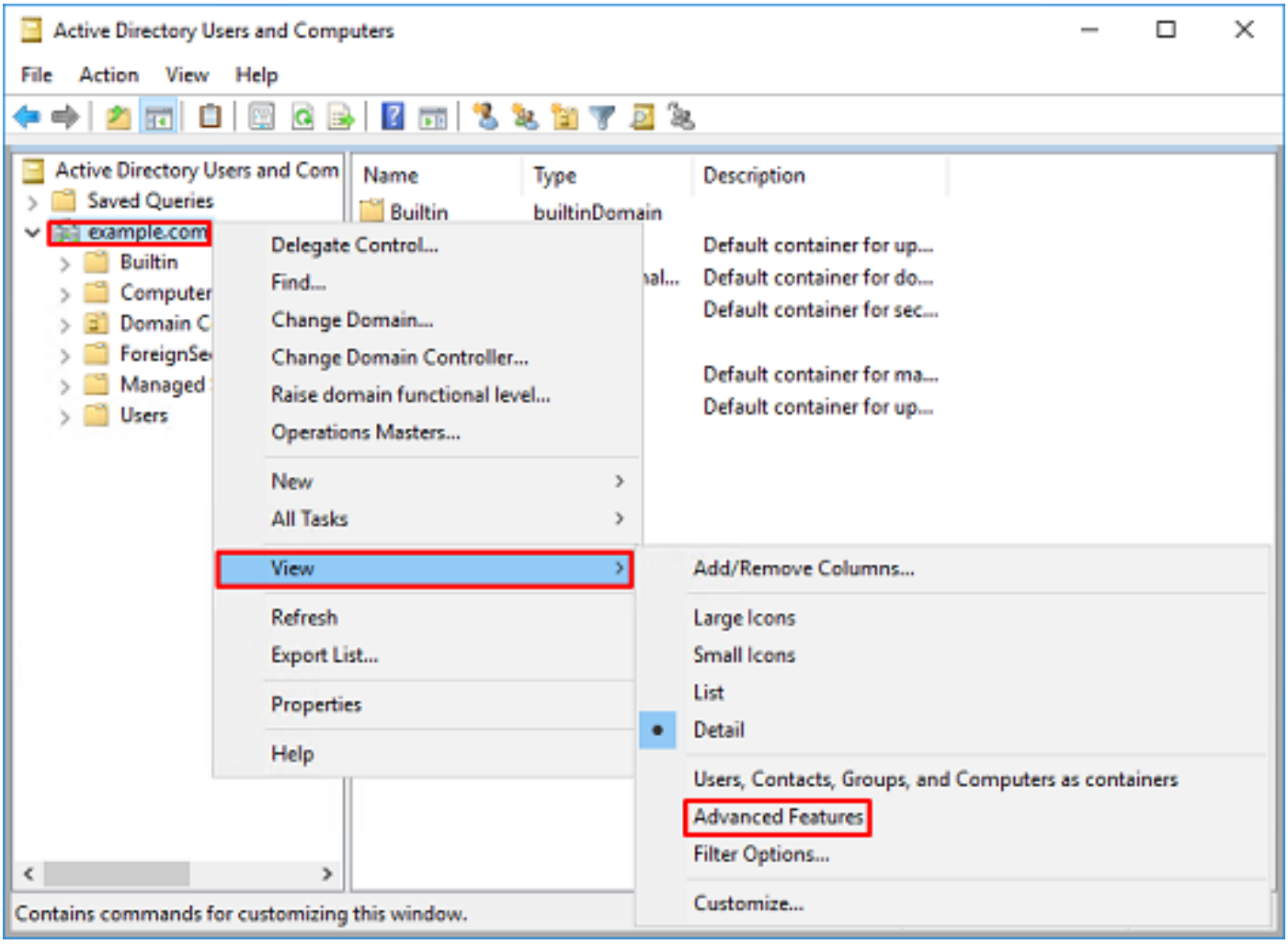


Déterminer le DN de base LDAP et le DN de groupe

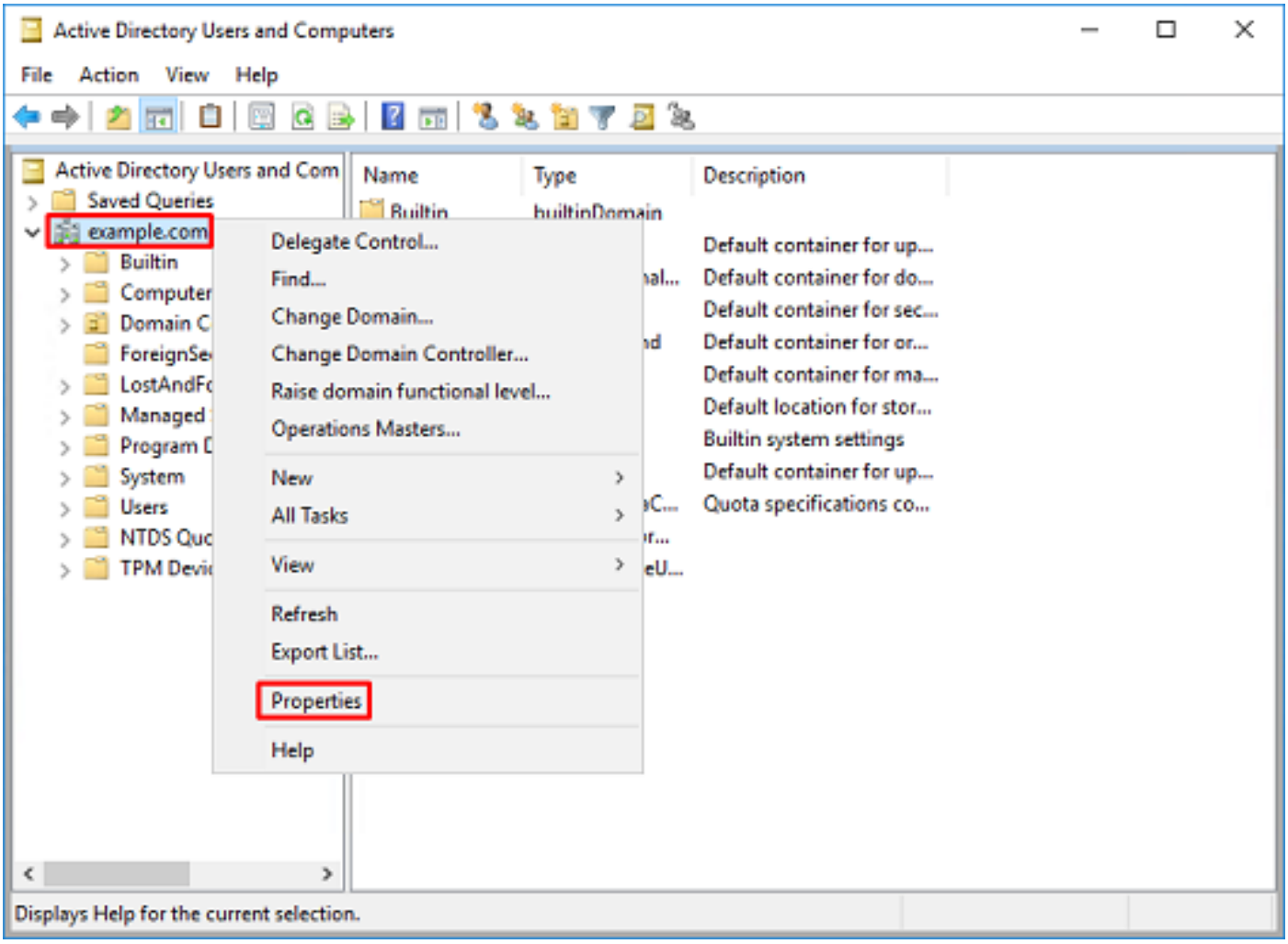
1. Ouvrez **Utilisateurs et ordinateurs Active Directory**.



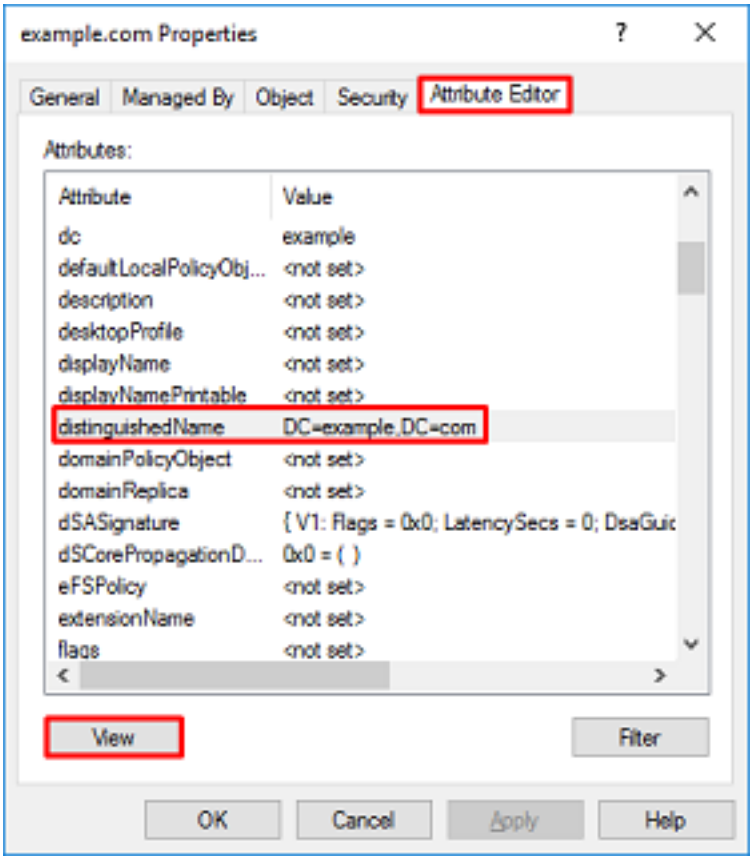
2. Cliquez avec le bouton gauche sur le **domaine racine** (pour ouvrir le conteneur), cliquez avec le bouton droit sur le **domaine racine**, puis sous **Affichage**, cliquez sur **Fonctionnalités avancées**.



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

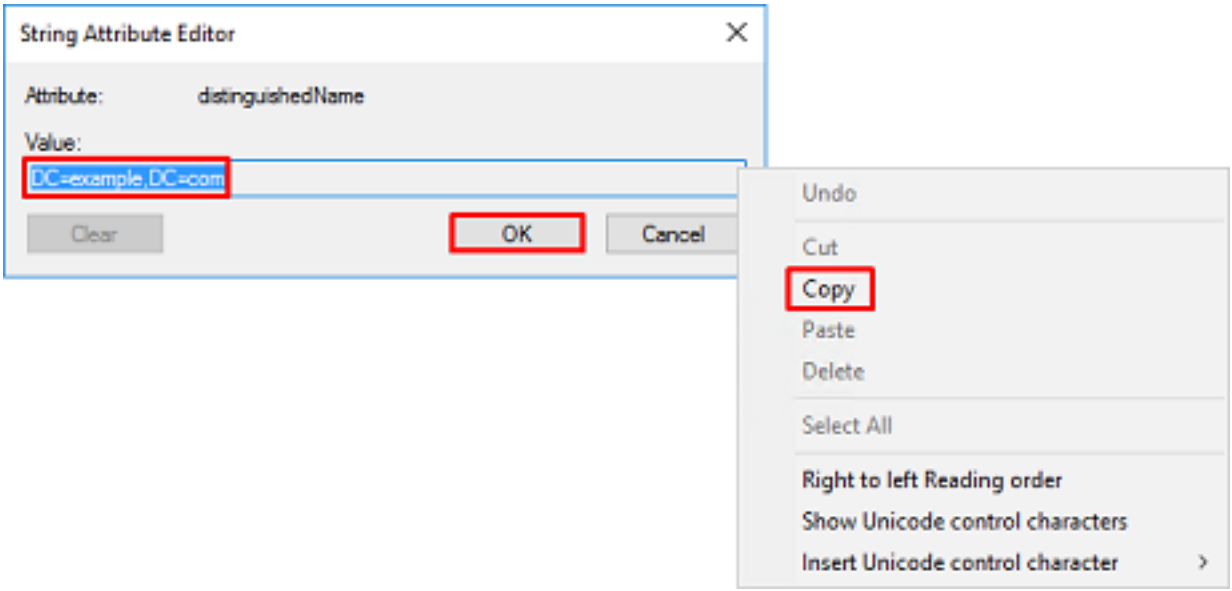


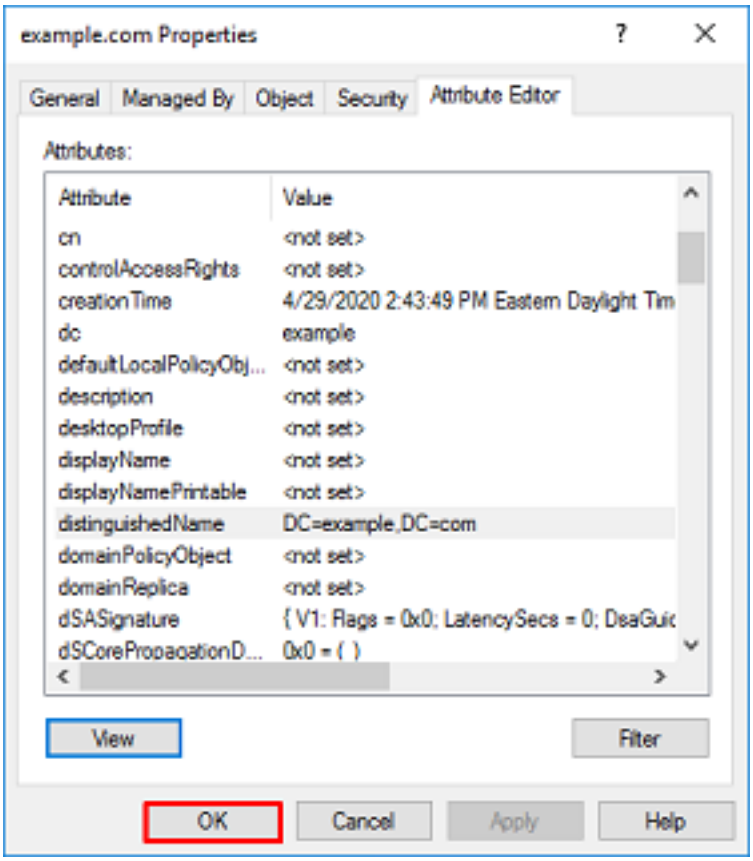
4. Sous **Propriétés**, sélectionnez l'onglet **Éditeur d'attributs**. Recherchez **nomDistinct** sous **Attributs**, puis cliquez sur **Afficher**.



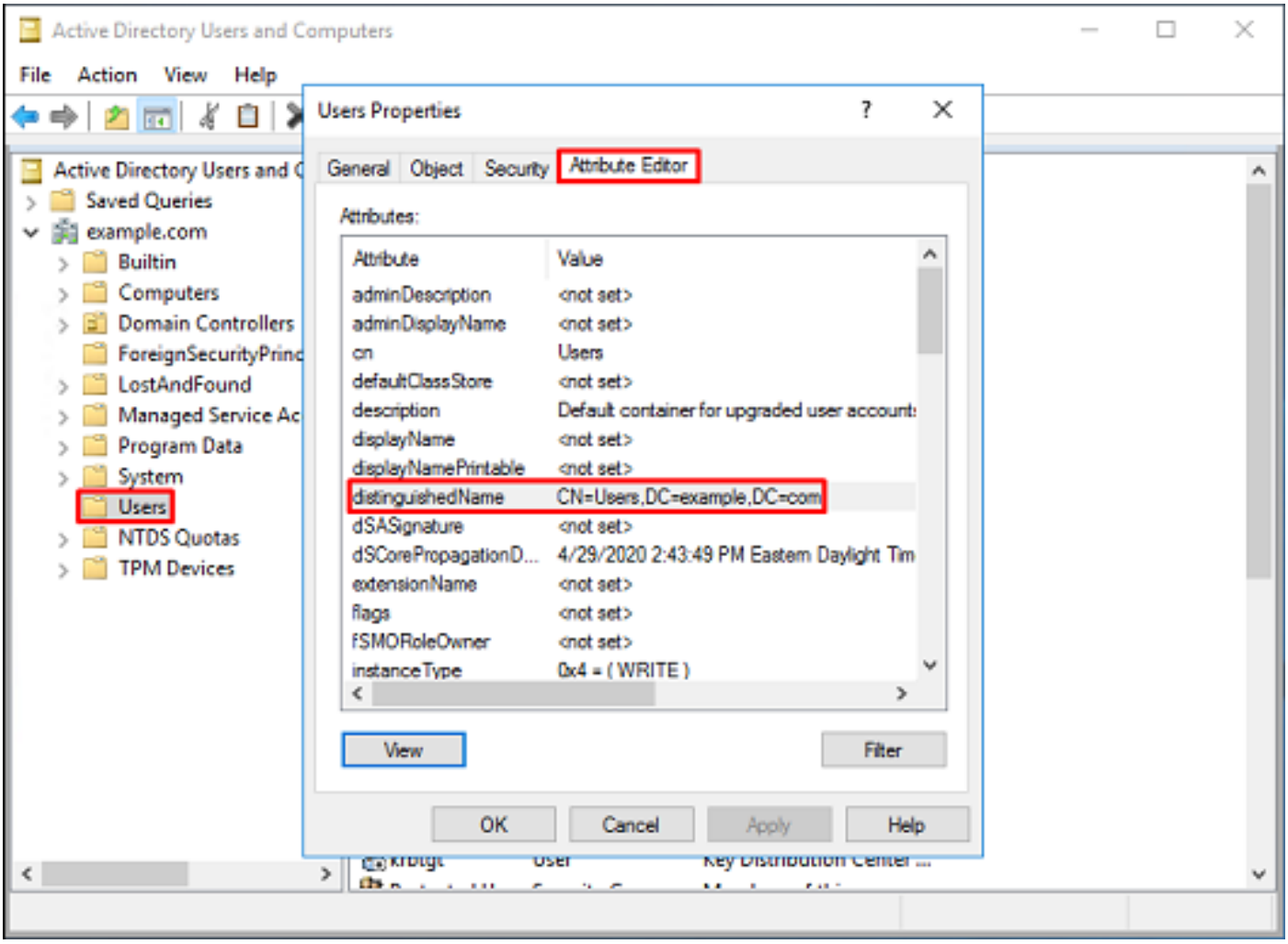
5. Une nouvelle fenêtre s'ouvre, dans laquelle le numéro de répertoire peut être copié et collé dans FMC ultérieurement. Dans cet exemple, le DN racine est DC=example,DC=com.

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

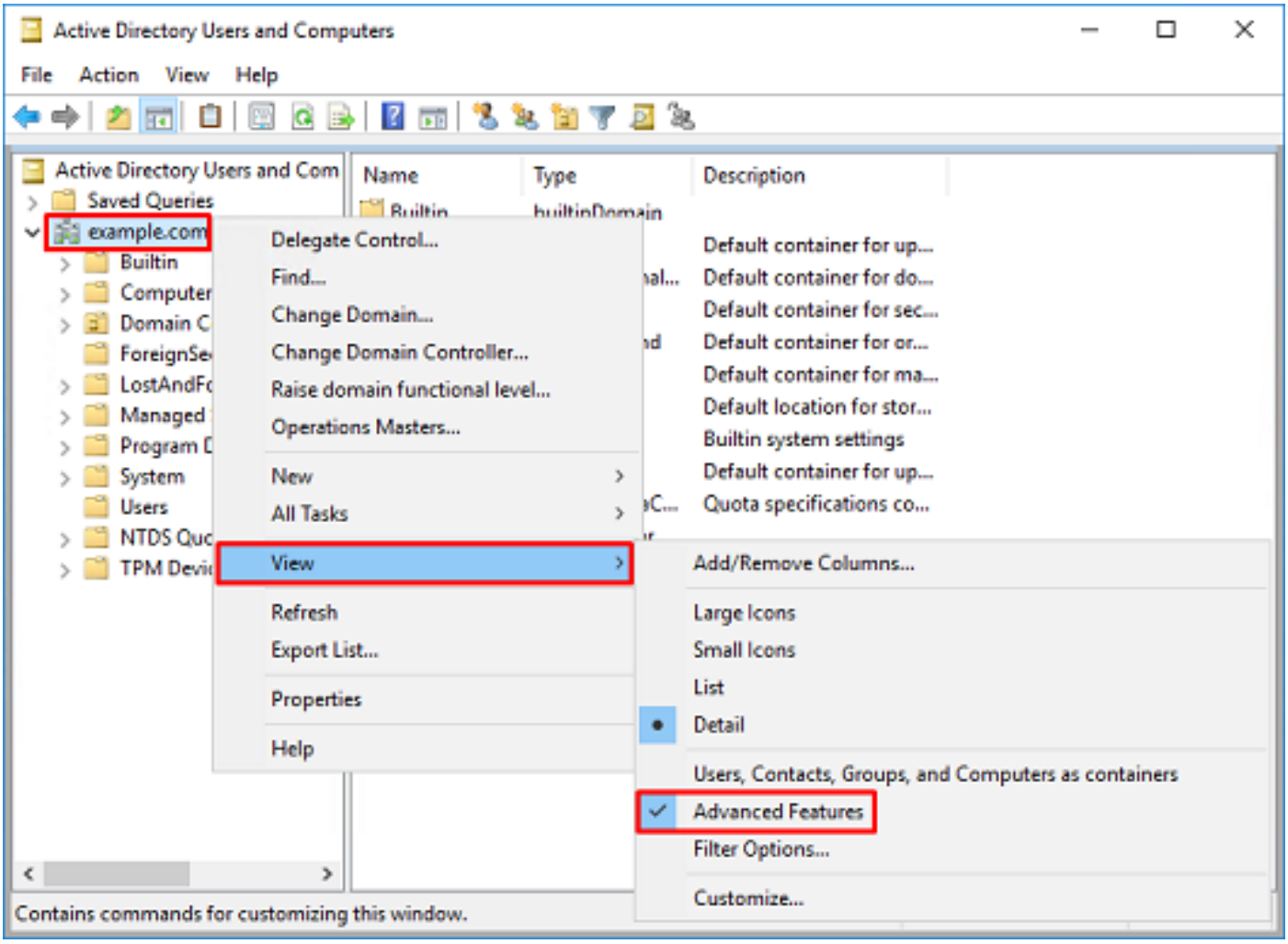




Cette opération peut être effectuée pour plusieurs objets dans **Active Directory**. Par exemple, ces étapes sont utilisées pour rechercher le DN du conteneur **Utilisateur** :



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



Créer un compte FTD

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

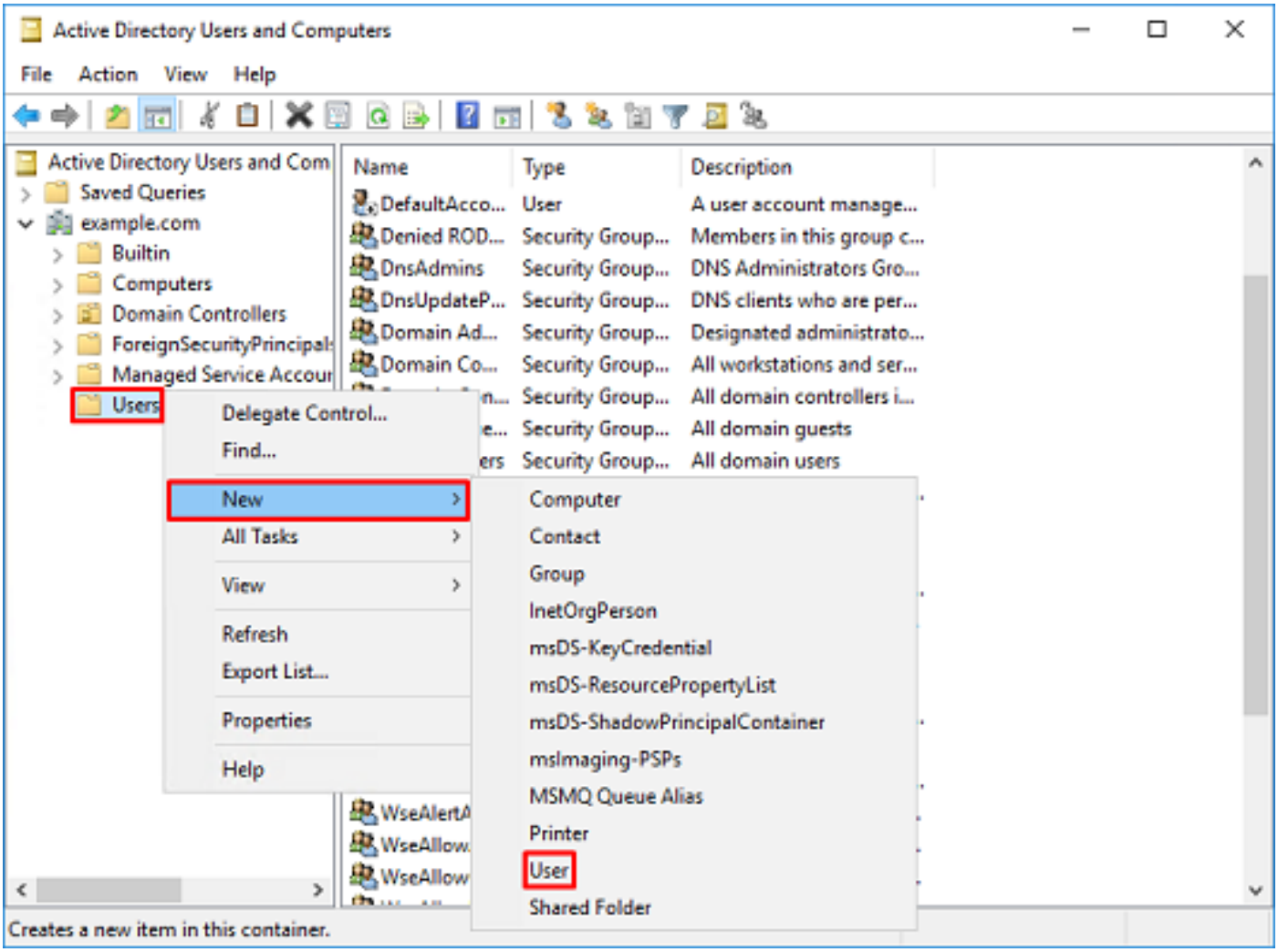
L'objectif de la création d'un compte FTD distinct est d'empêcher tout accès non autorisé à un autre emplacement du réseau si les informations d'identification utilisées pour la liaison sont compromises.

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

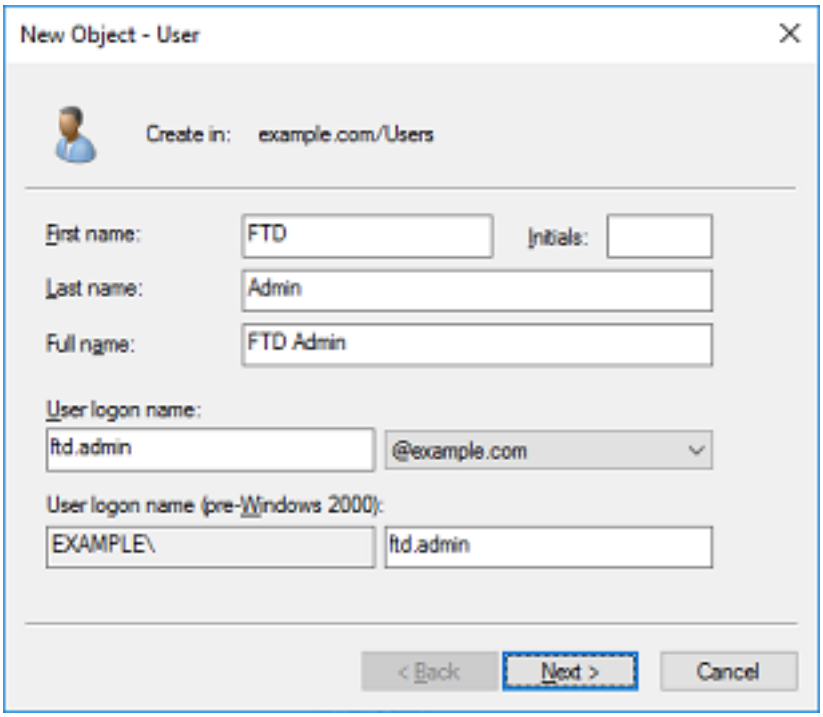
1. Dans **Utilisateurs et ordinateurs Active Directory**, cliquez avec le bouton droit sur le conteneur/l'organisation auquel le compte FTD est ajouté.

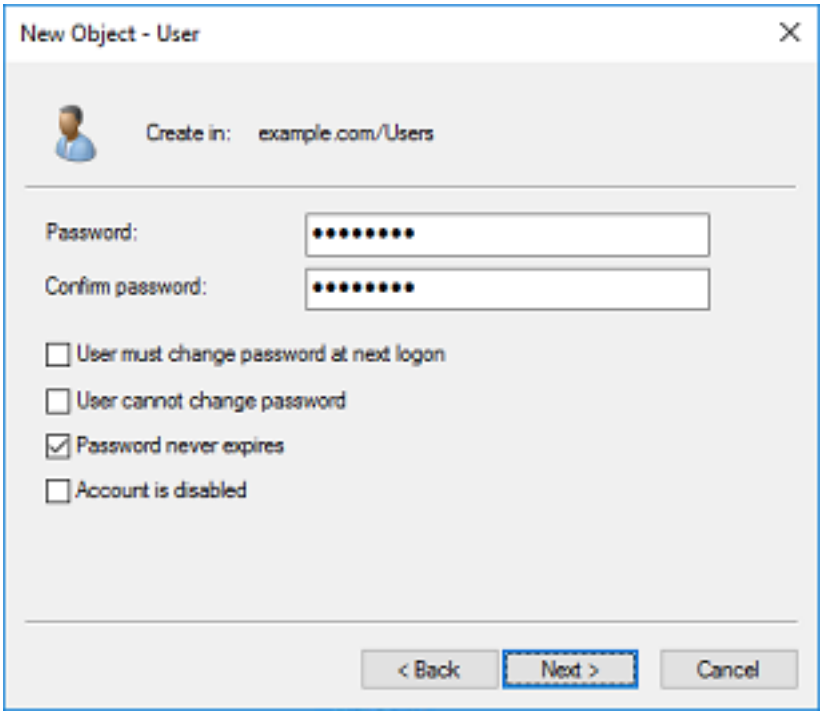
Dans cette configuration, le compte FTD est ajouté sous le conteneur **Users** sous le nom d'utilisateur ftd.admin@example.com.

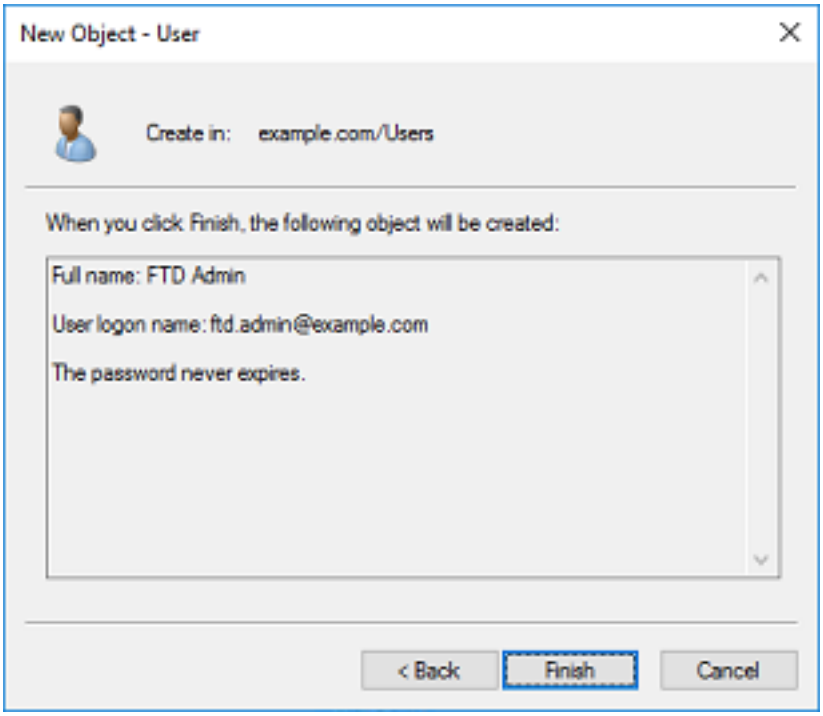
Cliquez avec le bouton droit sur **Users**, puis accédez à **New > User**.



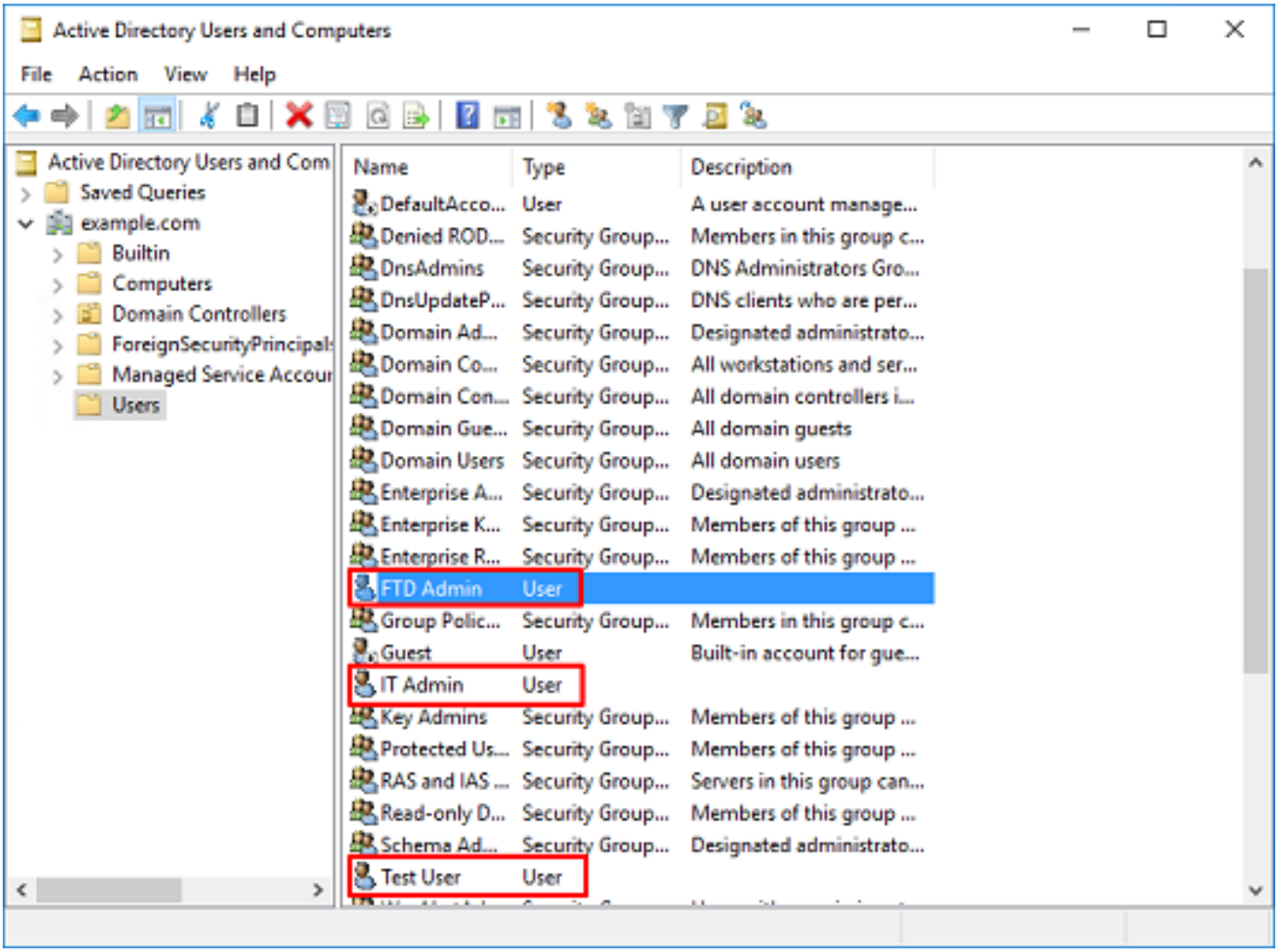
2. Accédez à l'Assistant **Nouvel objet - Utilisateur**.







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



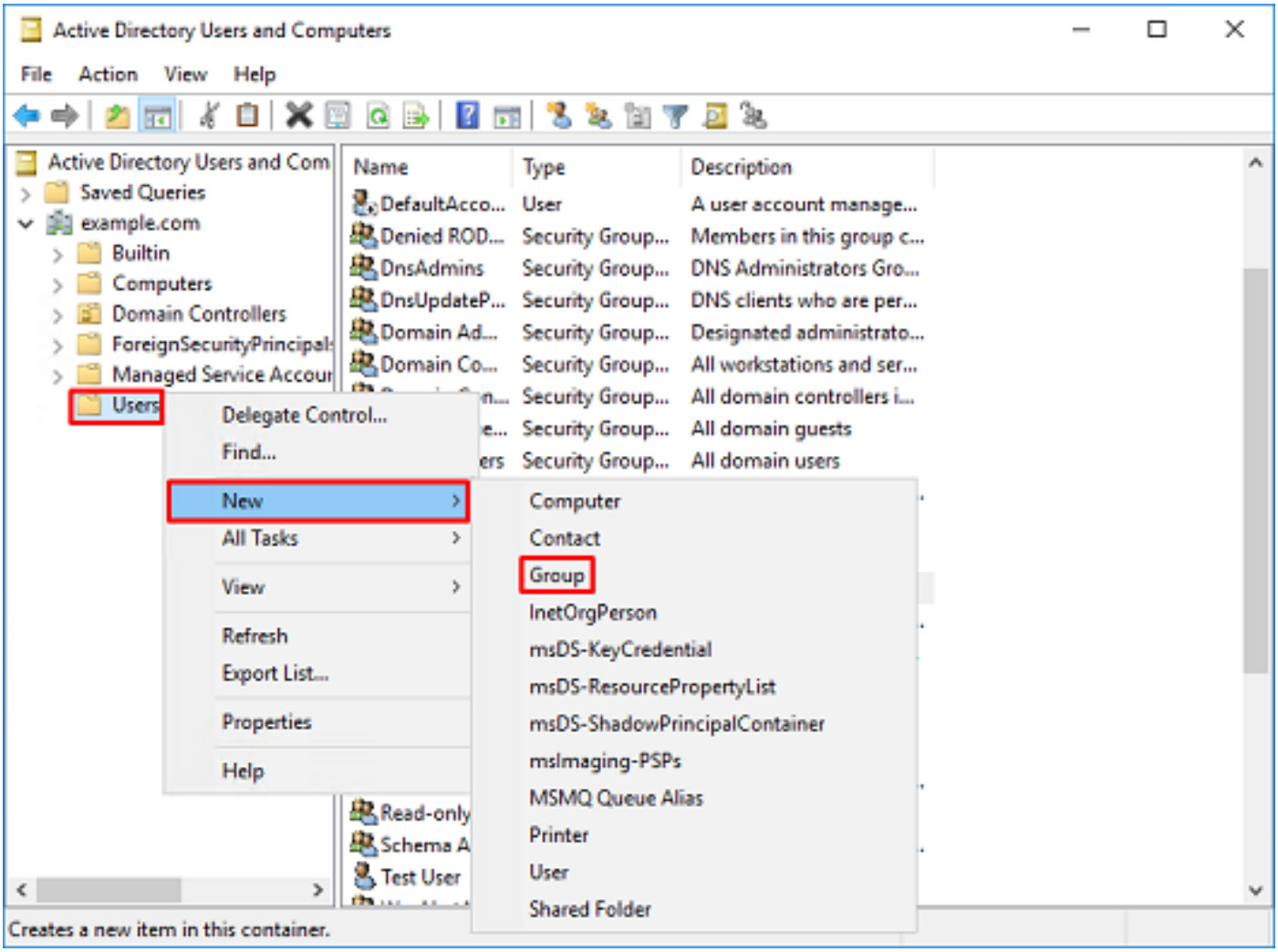
Créer des groupes AD et ajouter des utilisateurs à des groupes AD (facultatif)

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

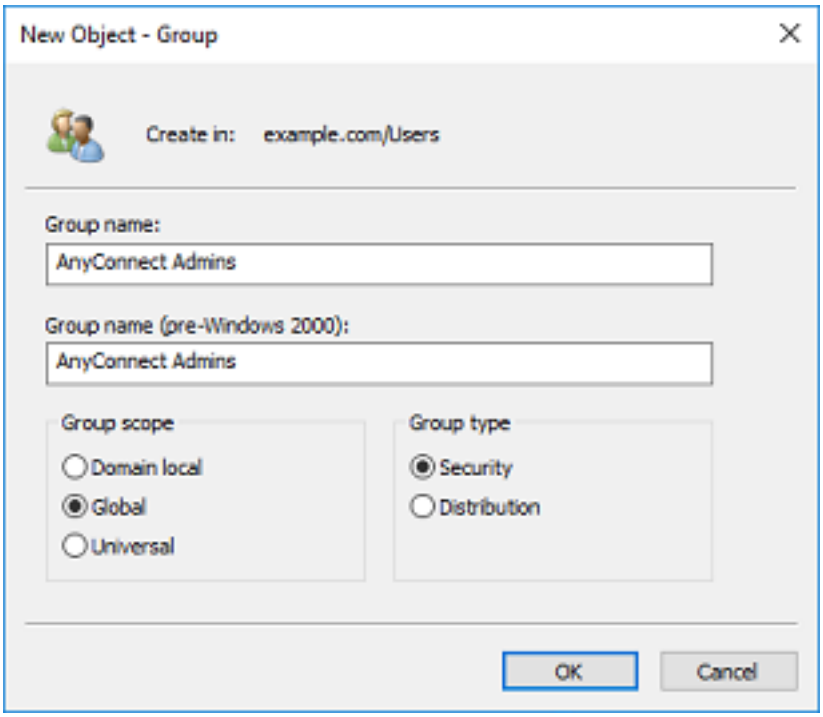
Dans ce guide de configuration, les groupes sont utilisés pour appliquer les paramètres de stratégie de contrôle d'accès ultérieurement via l'identité de l'utilisateur dans FMC.

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

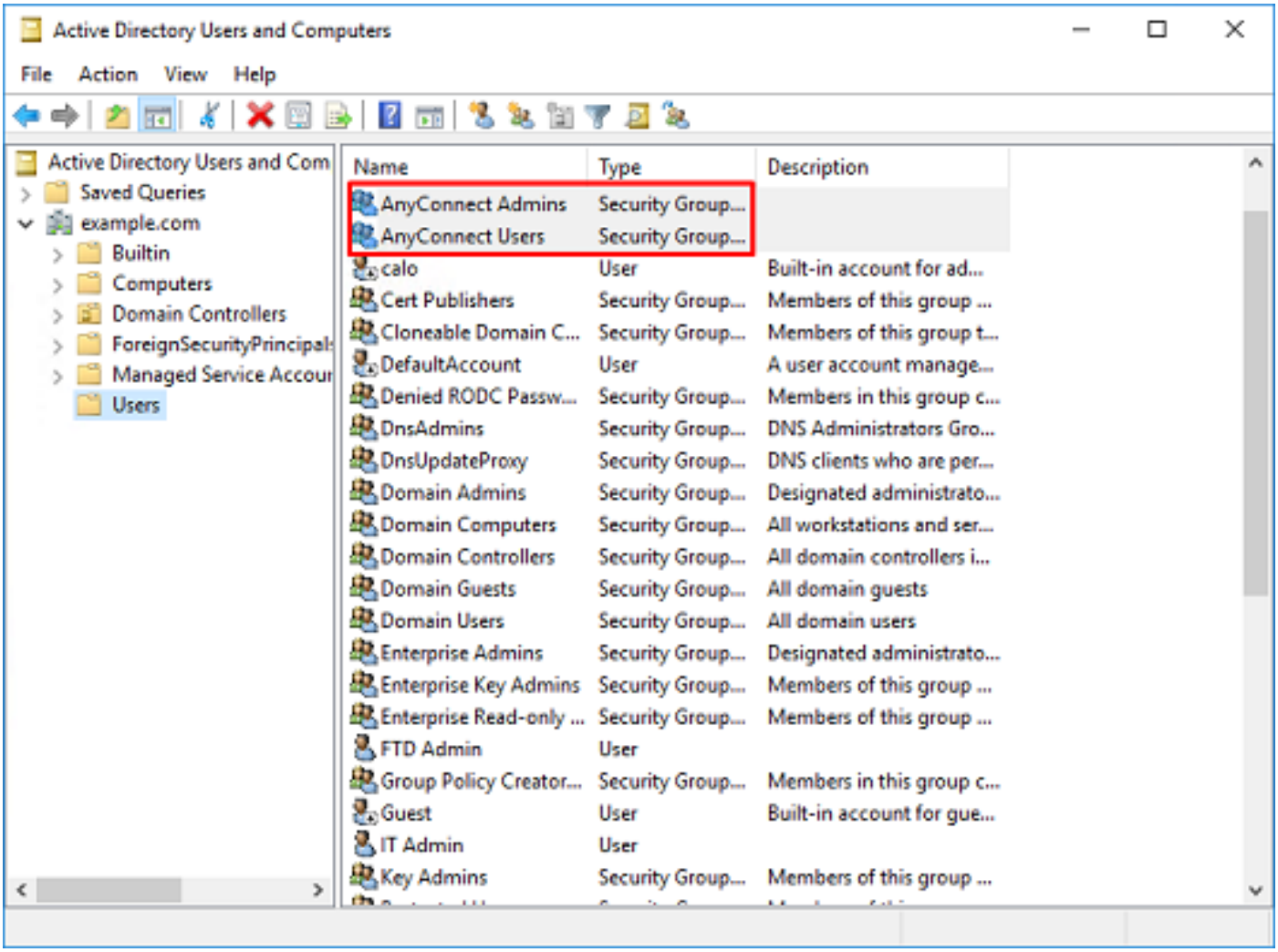
Dans cet exemple, le groupe AnyConnect Admins est ajouté sous le conteneur **Users**. Cliquez avec le bouton droit sur **Users**, puis accédez à **New > Group**.



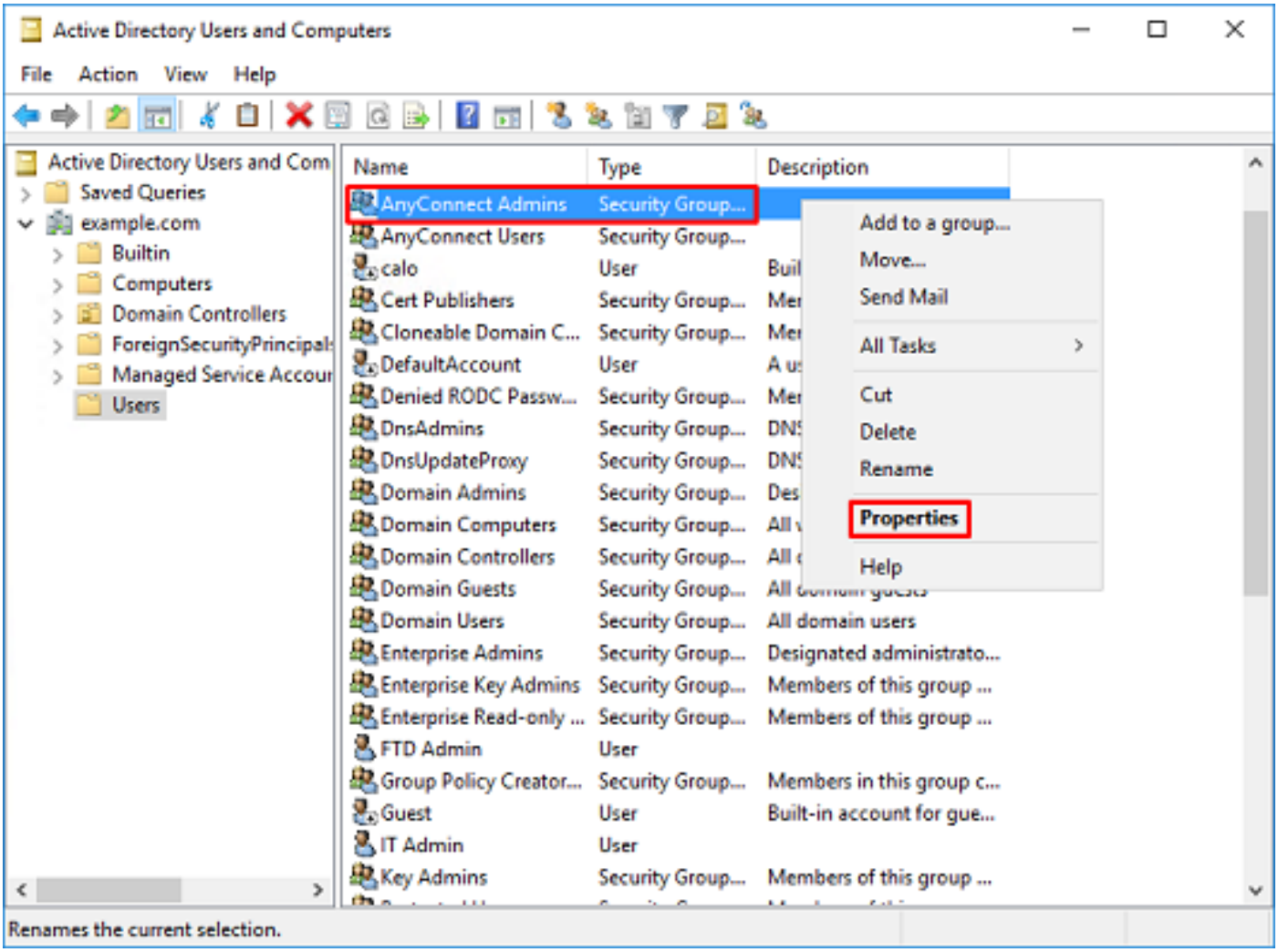
2. Accédez à l'Assistant **Nouvel objet - Groupe**.



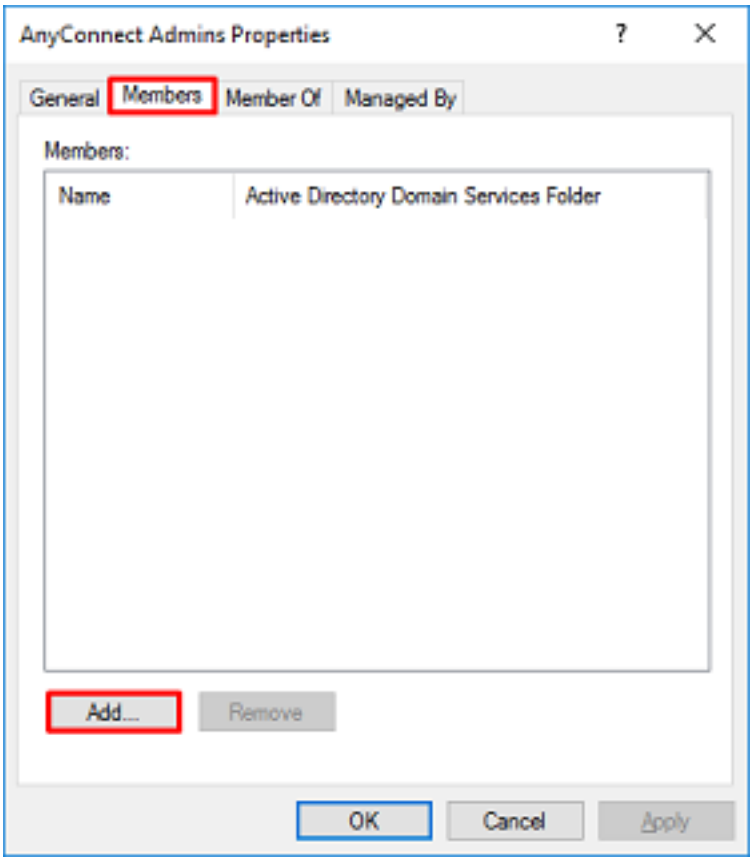
3. Vérifiez que le groupe est créé. Le groupe **Utilisateurs AnyConnect** est également créé.



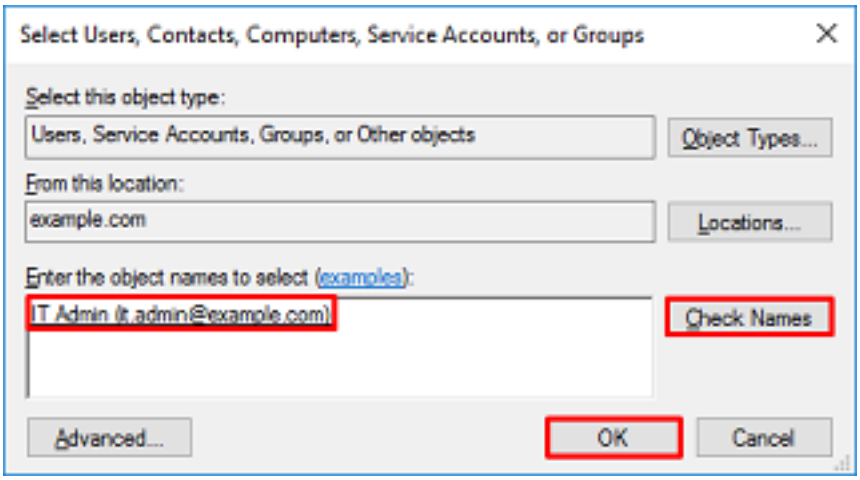
4. Cliquez avec le bouton droit sur le groupe d'utilisateurs, puis sélectionnez **Propriétés**. Dans cette configuration, l'utilisateur IT Admin est ajouté au groupe AnyConnect Admins et l'utilisateur **Test User** est ajouté au groupe **AnyConnect Users**.



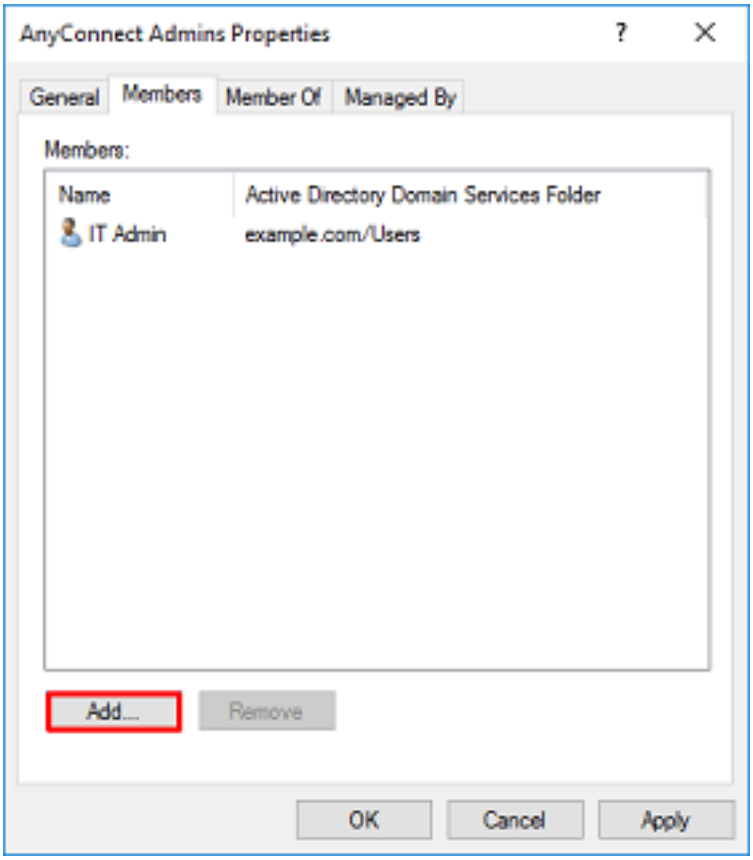
5. Sous l'onglet **Membres**, cliquez sur **Ajouter**.



Entrez l'utilisateur dans le champ et cliquez sur **Vérifier les noms** pour vérifier que l'utilisateur est trouvé. Une fois la vérification effectuée, cliquez sur **OK**.

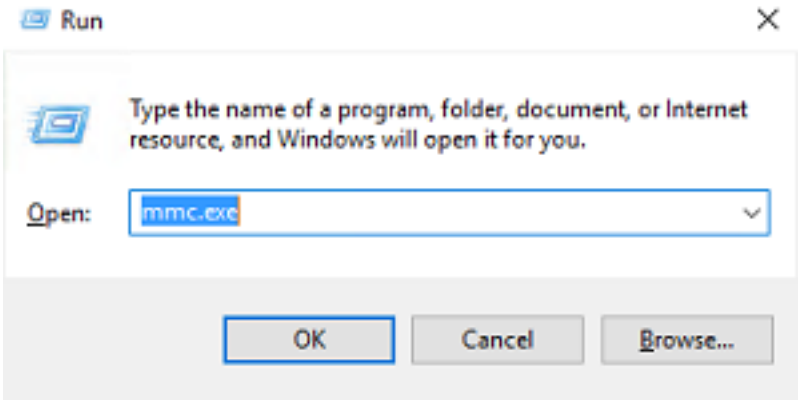


Vérifiez que l'utilisateur correct a été ajouté, puis cliquez sur le bouton OK. L'utilisateur **Utilisateur test** est également ajouté au groupe **Utilisateurs AnyConnect** en suivant la même procédure.

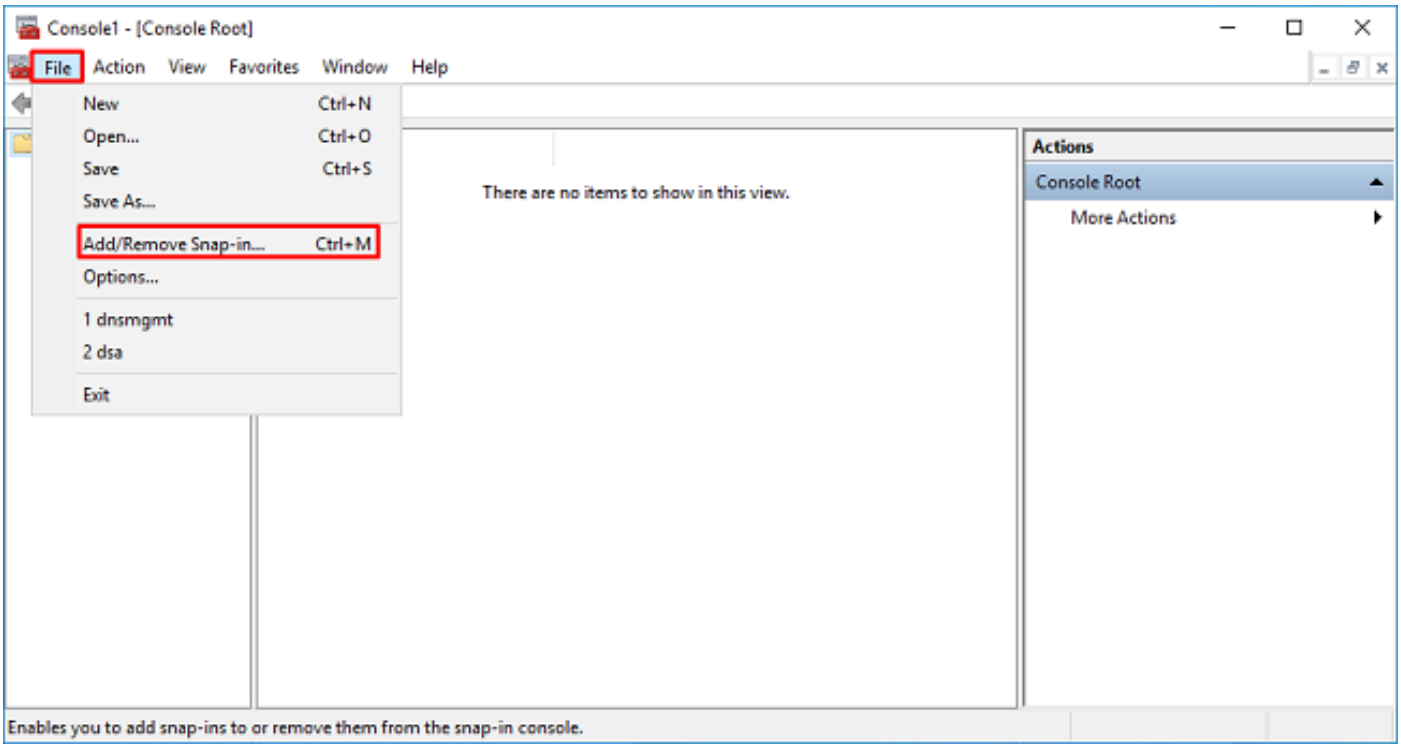


Copier la racine du certificat SSL LDAPS (obligatoire uniquement pour LDAPS ou STARTTLS)

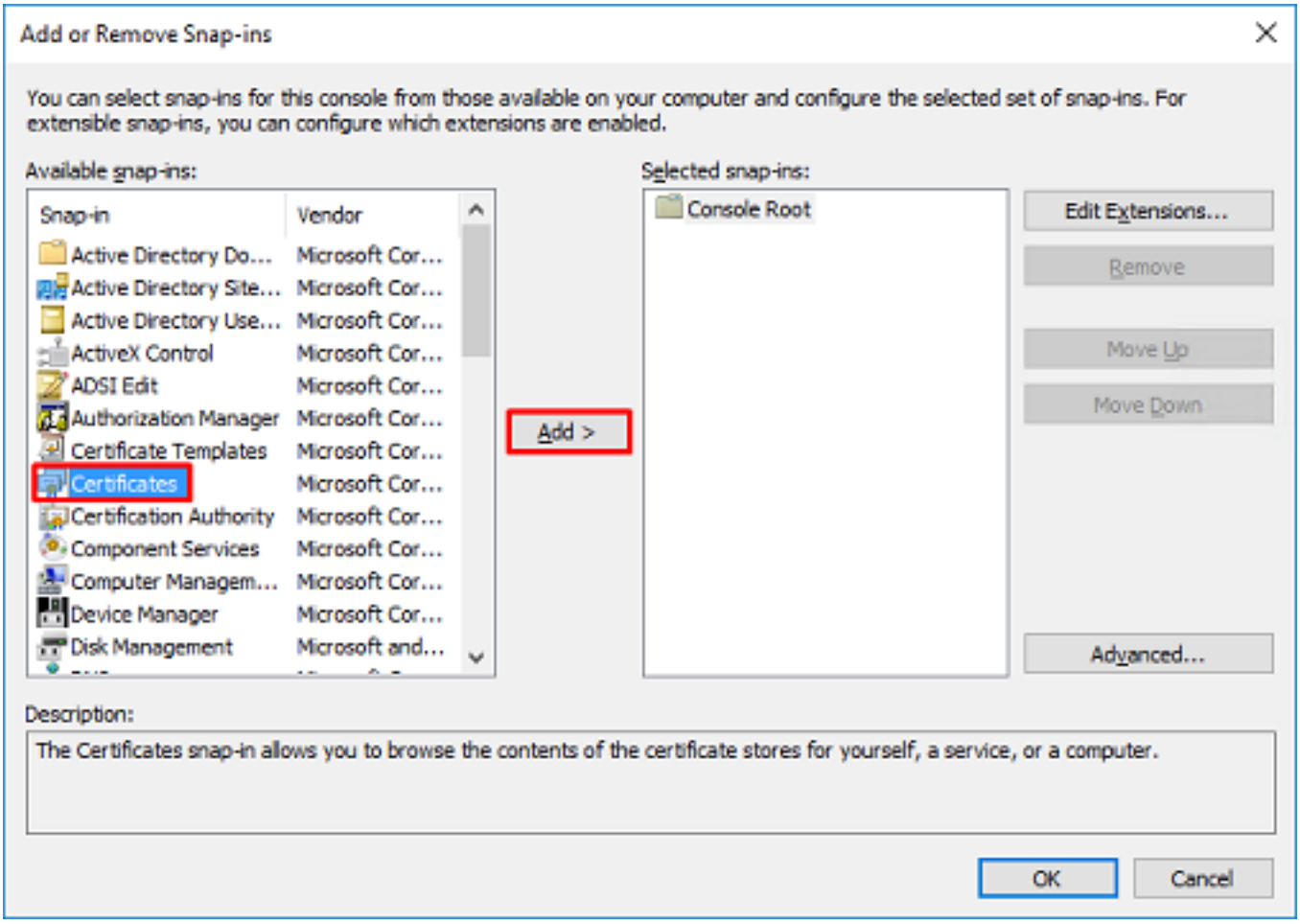
1. Appuyez sur **Win+R** et entrez **mmc.exe**. Cliquez ensuite sur OK.



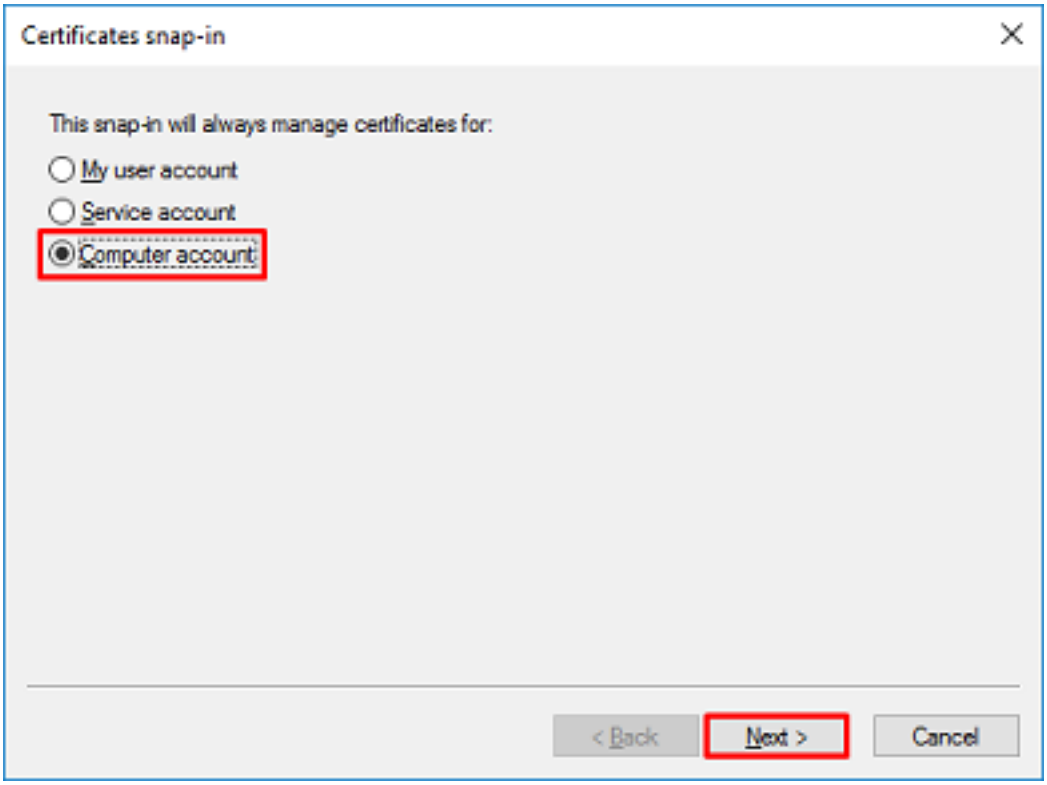
2. Accédez à **Fichier > Ajouter/Supprimer un composant logiciel enfichable...**



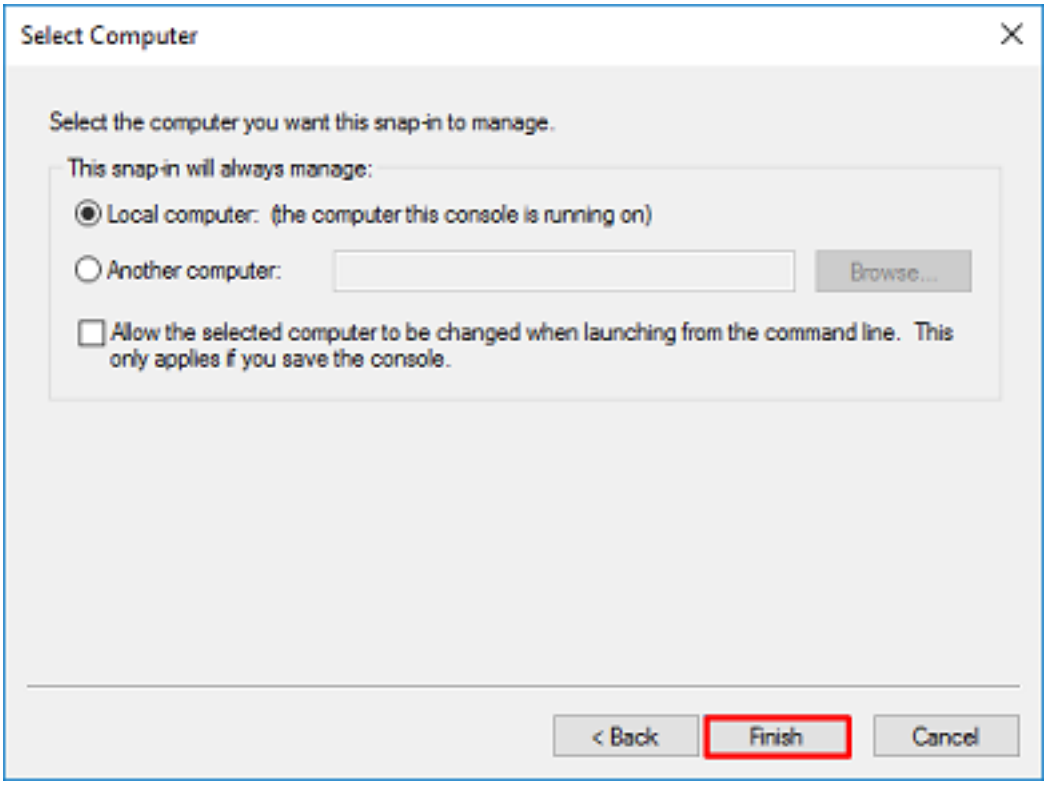
3. Sous Composants logiciels enfichables disponibles, sélectionnez **Certificats**, puis cliquez sur **Ajouter**.



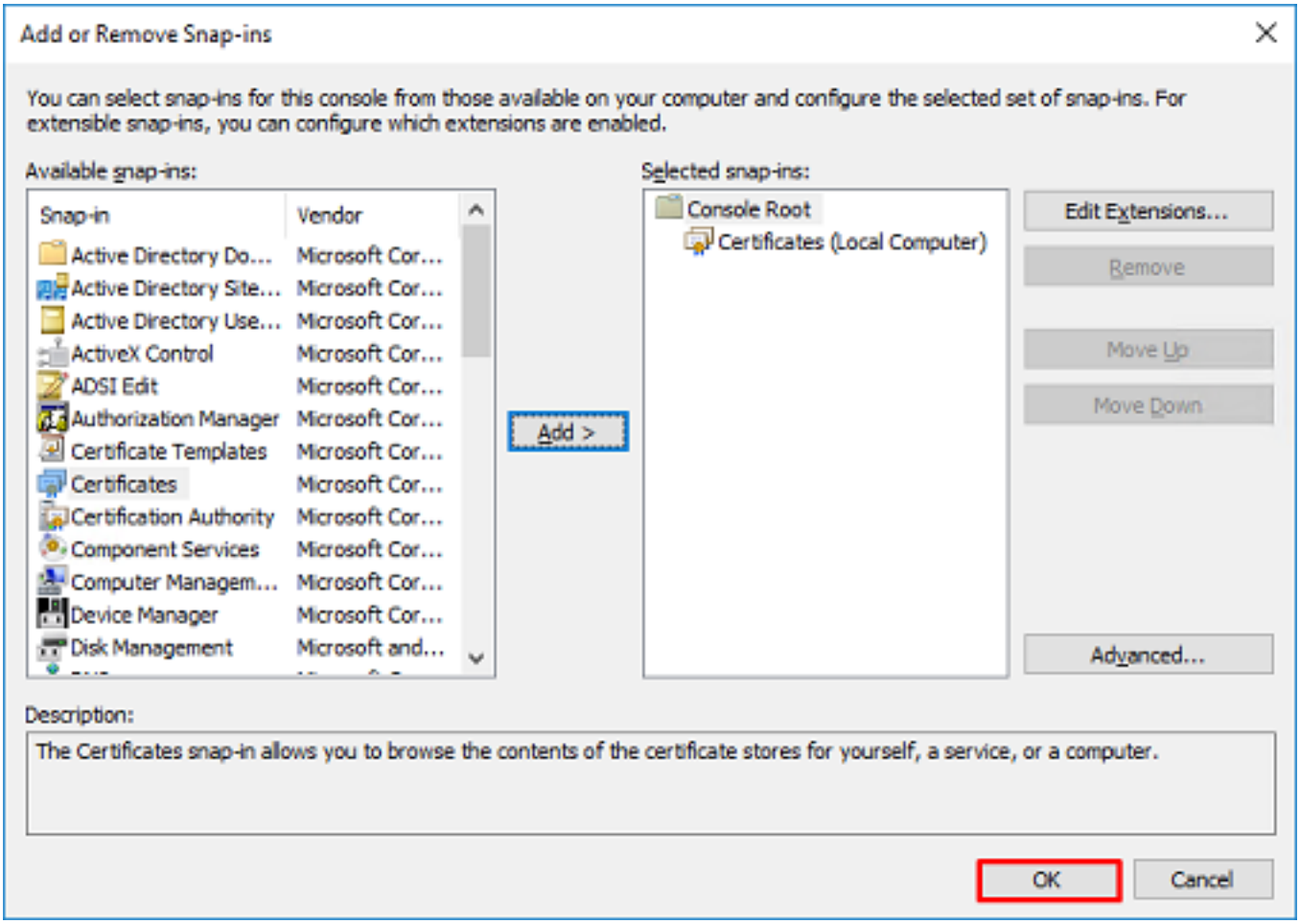
4. Sélectionnez **Compte d'ordinateur**, puis cliquez sur **Suivant**.



Cliquez sur **Finish** (Terminer).



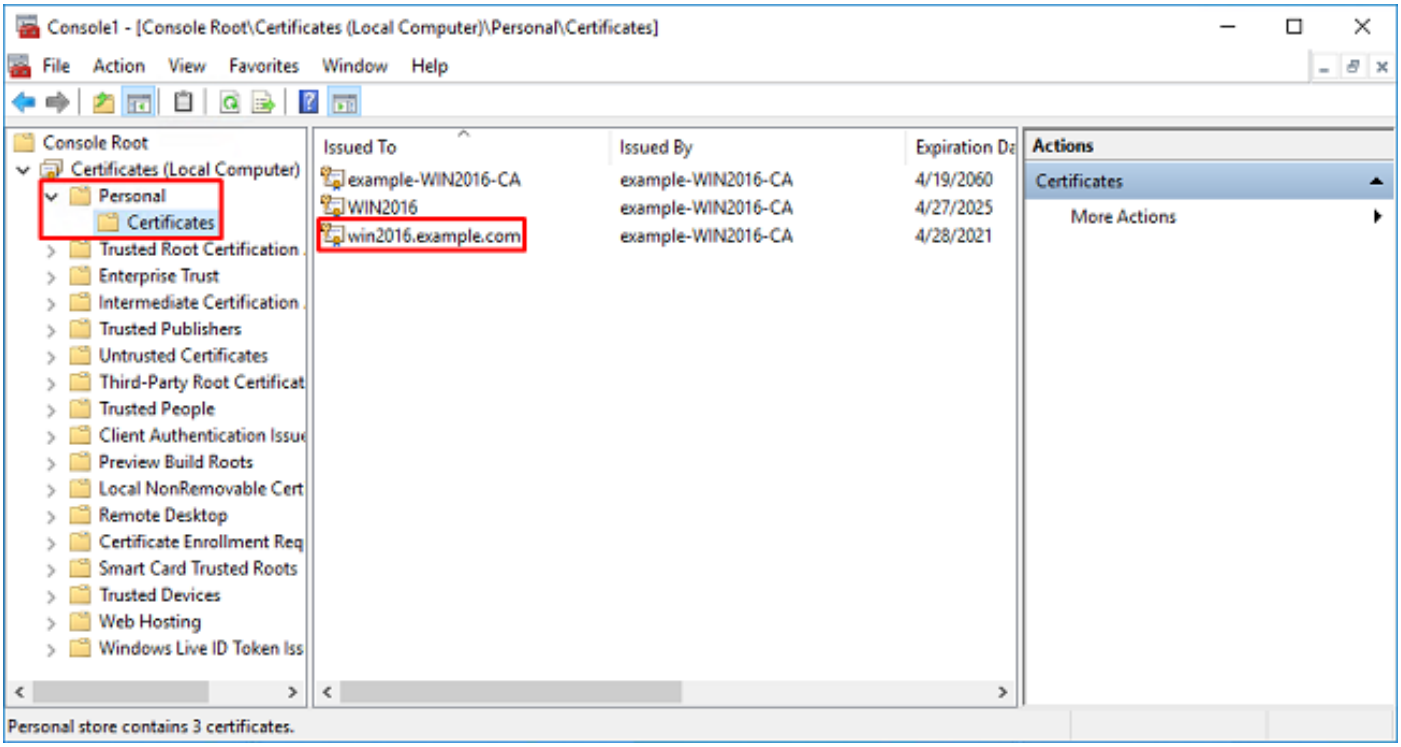
5. Cliquez maintenant sur **OK**.



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

- Certificat d'autorité de certification délivré à et par l'exemple-WIN2016-CA.
- Certificat d'identité délivré à WIN2016 par example-WIN2016-CA.
- Certificat d'identité délivré à win2016.example.com par example-WIN2016-CA.

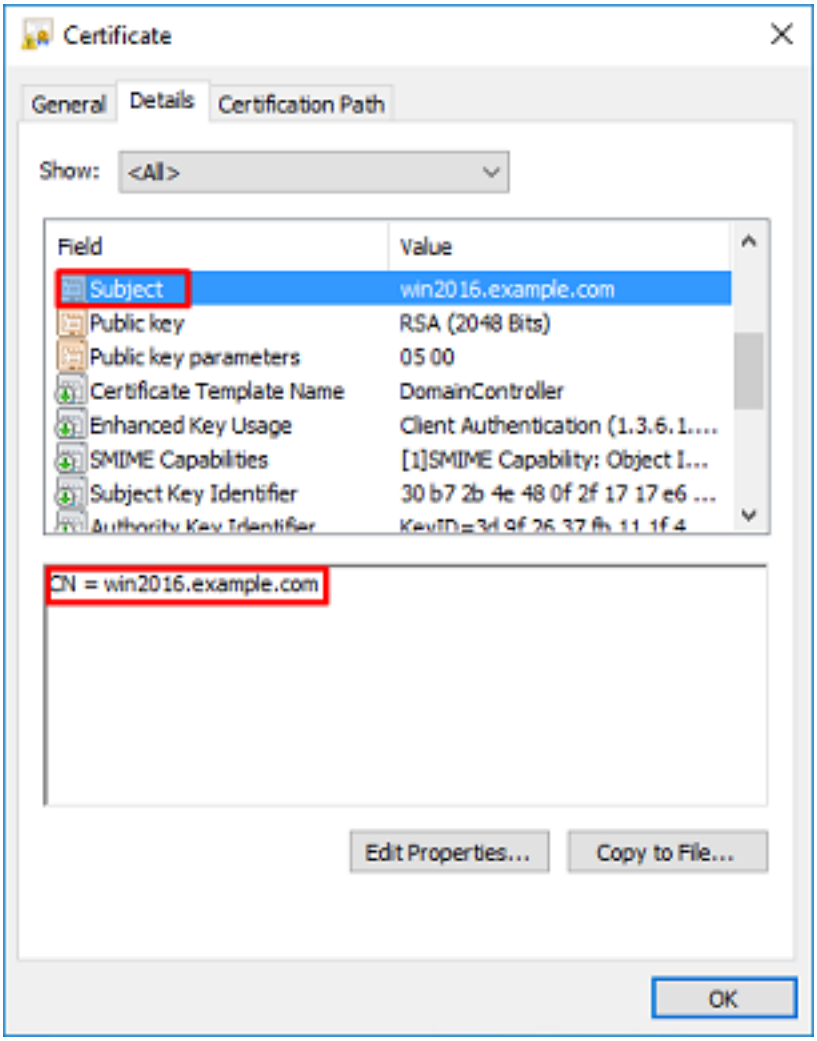
Dans ce guide de configuration, le nom de domaine complet est win2016.example.com et les 2 premiers certificats ne sont donc pas valides pour être utilisés comme certificat SSL LDAPS. Le certificat d'identité émis vers win2016.example.com est un certificat qui a été émis automatiquement par le service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

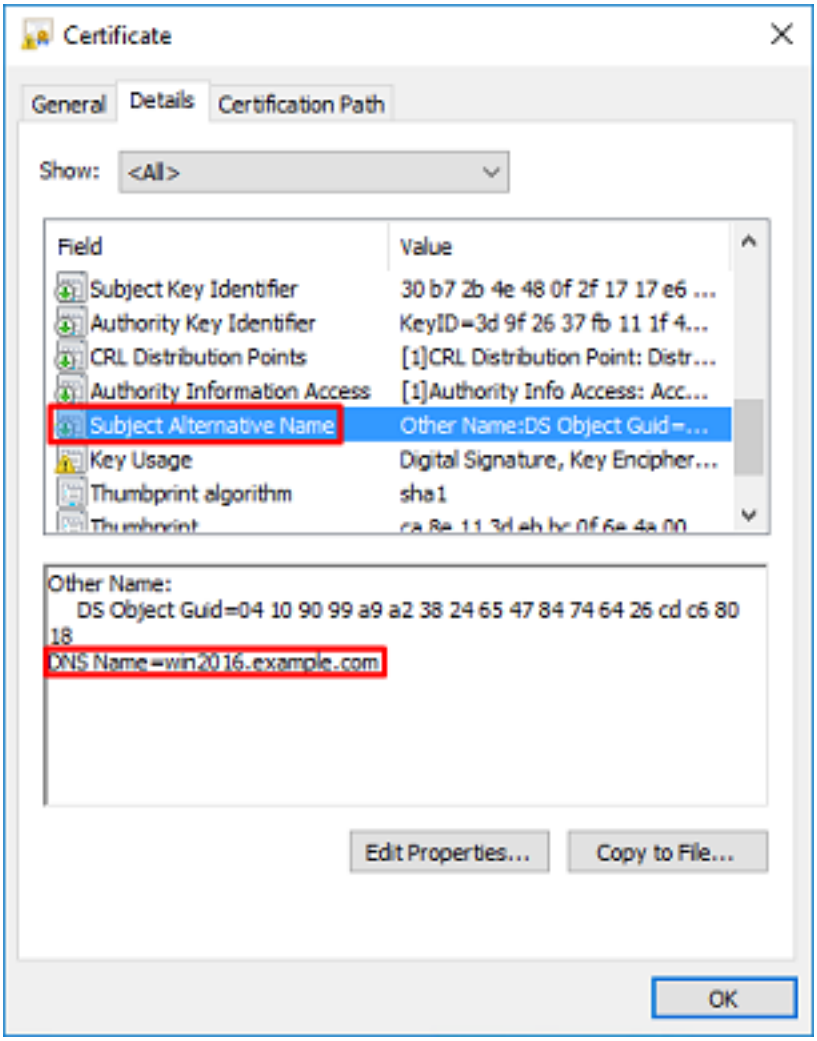


7. Pour être utilisé comme certificat SSL LDAPS, le certificat doit répondre aux exigences suivantes :

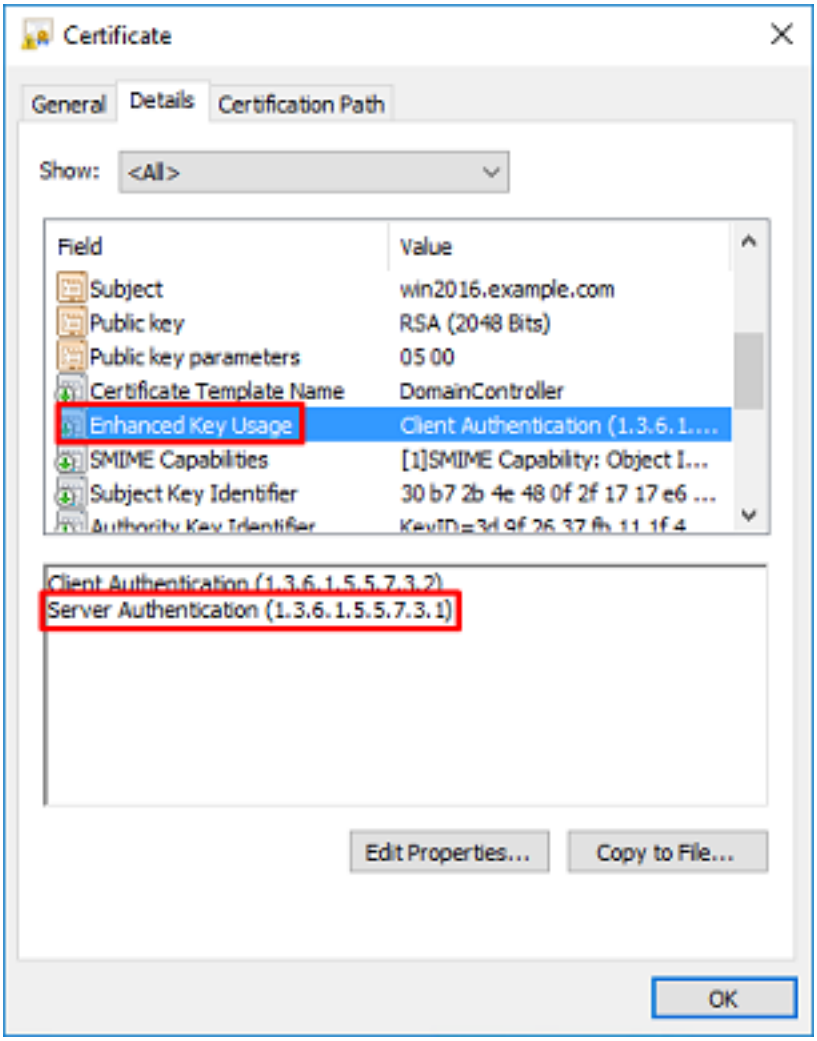
- Le nom commun ou le **nom secondaire de l'objet DNS** correspond au nom de domaine complet du serveur Windows.
- Le certificat comporte l'**authentification du serveur** sous le champ **Enhanced Key Usage**.

Sous l'onglet **Details** pour le certificat, sélectionnez **Subject** and **Subject Alternative Name**, le nom de domaine complet win2016.example.com est présent.

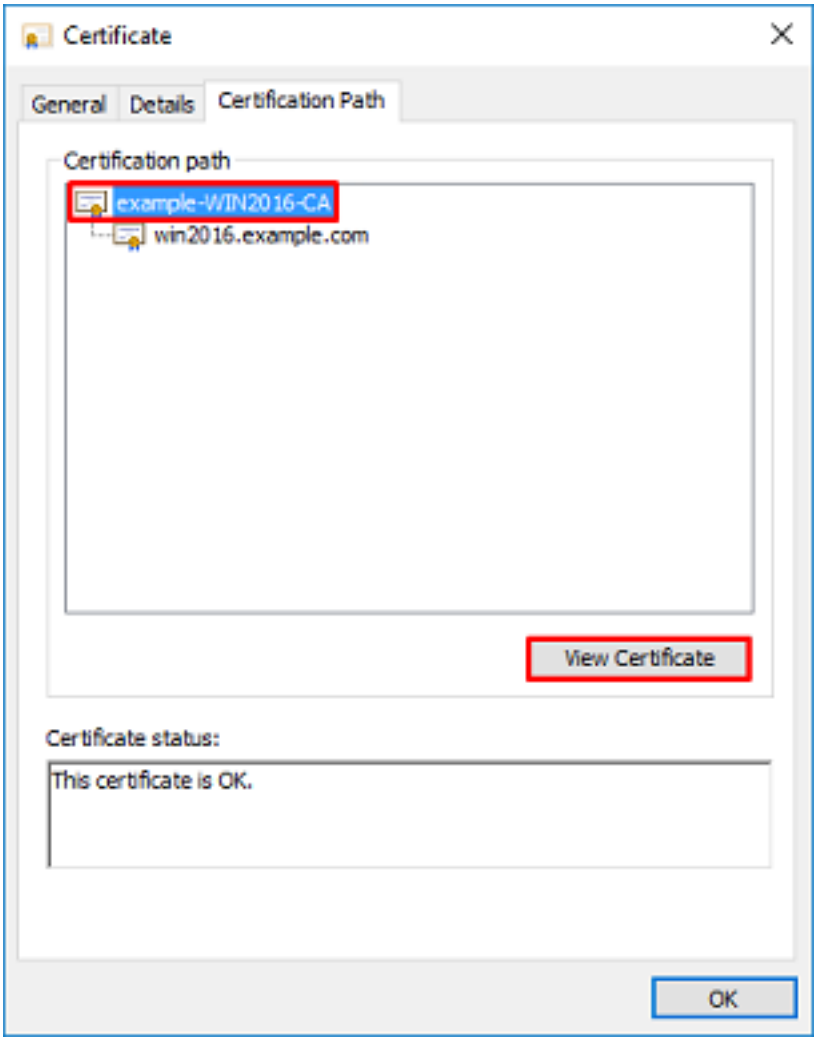

Certificate
General
Details
Certification Path
Show:
<All>
Field
Value
Subject
win2016.example.com
Public key
RSA (2048 Bits)
Public key parameters
05 00
Certificate Template Name
DomainController
Enhanced Key Usage
Client Authentication (1.3.6.1....
SMIME Capabilities
[1]SMIME Capability: Object I...
Subject Key Identifier
30 b7 2b 4e 48 0f 2f 17 17 e6 ...
CN = win2016.example.com
Edit Properties...
Copy to File...
OK



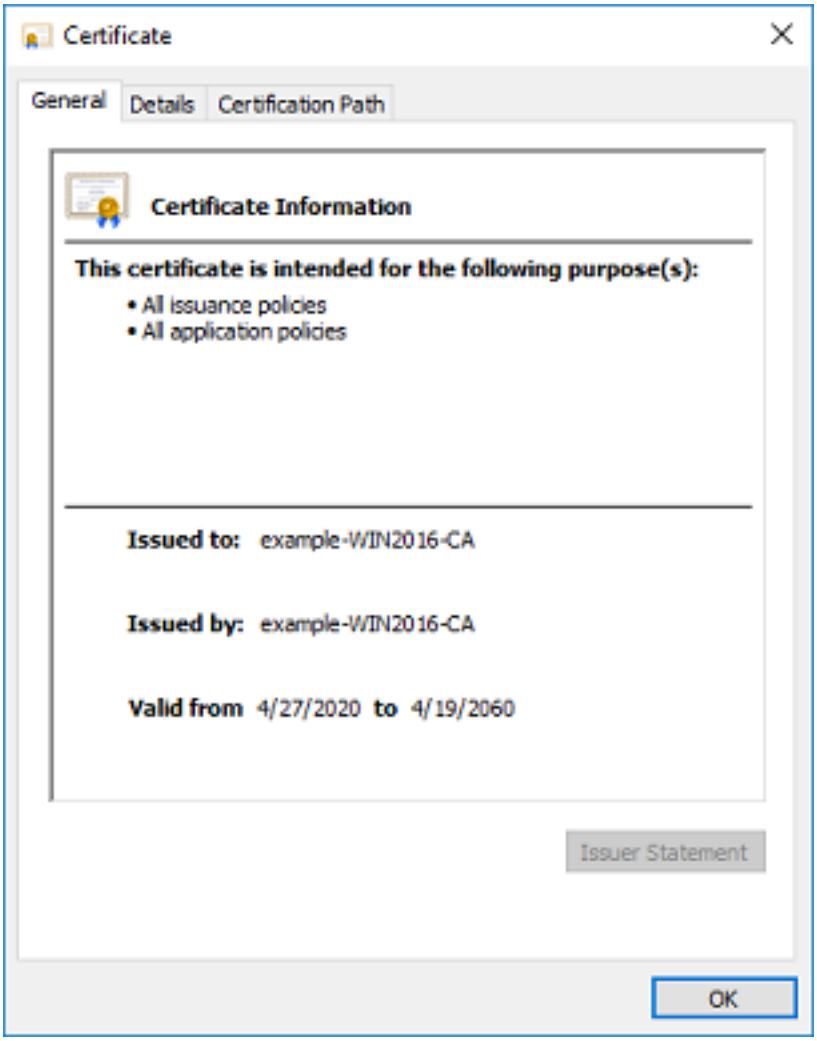
Sous **Enhanced Key Usage**, **Server Authentication** est présent.



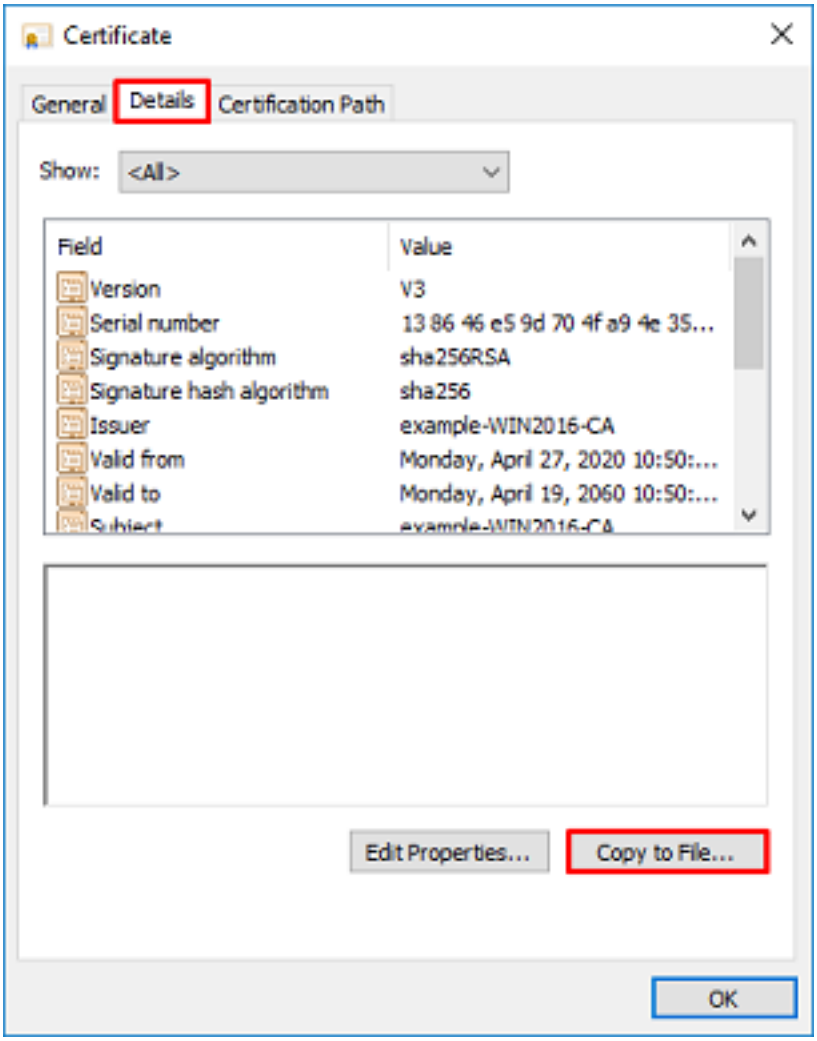
8. Une fois que cela est confirmé, sous l'onglet **Chemin d'accès de certification**, sélectionnez le certificat supérieur qui est le certificat d'autorité de certification racine, puis cliquez sur **Afficher le certificat**.



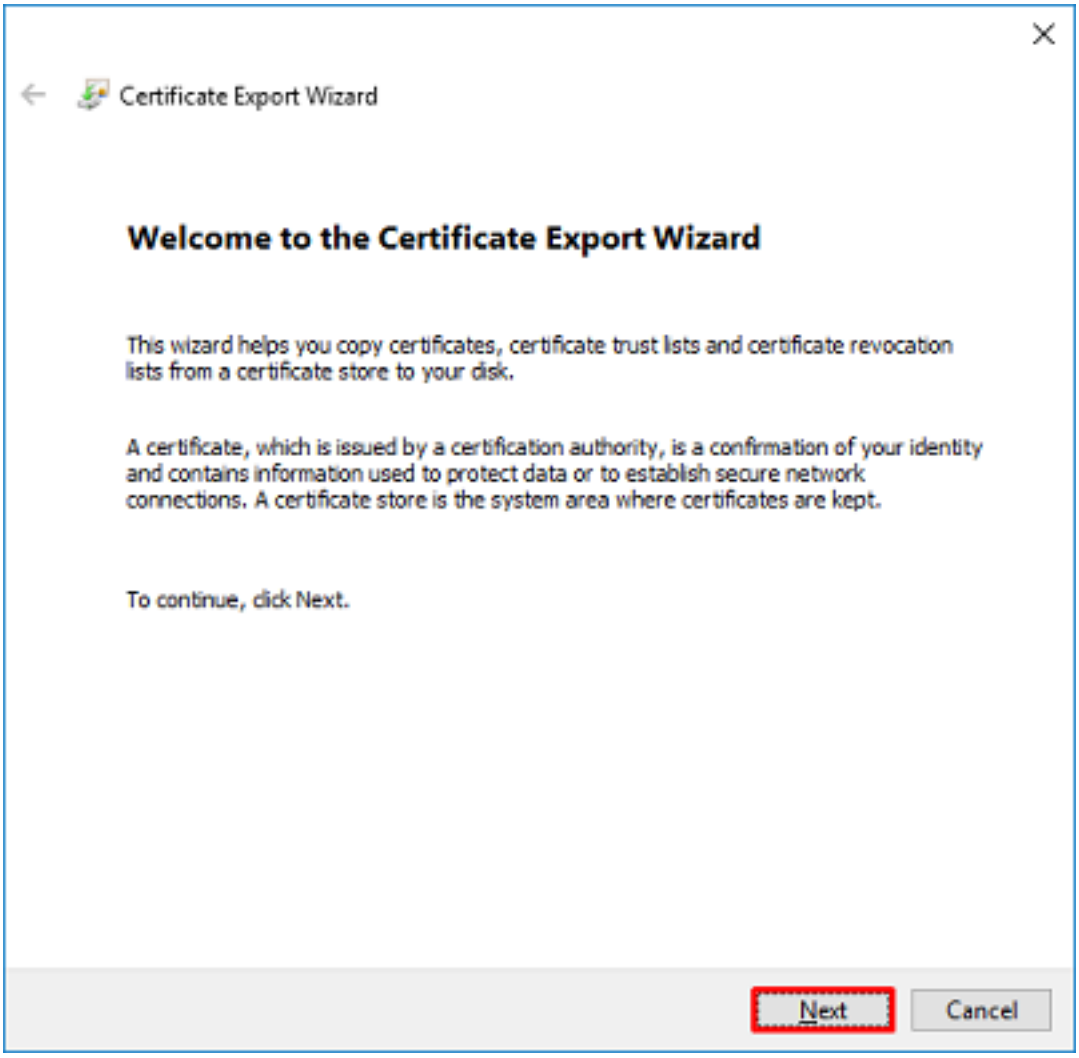
9. Ceci ouvre les détails du certificat pour le certificat d'autorité de certification racine.



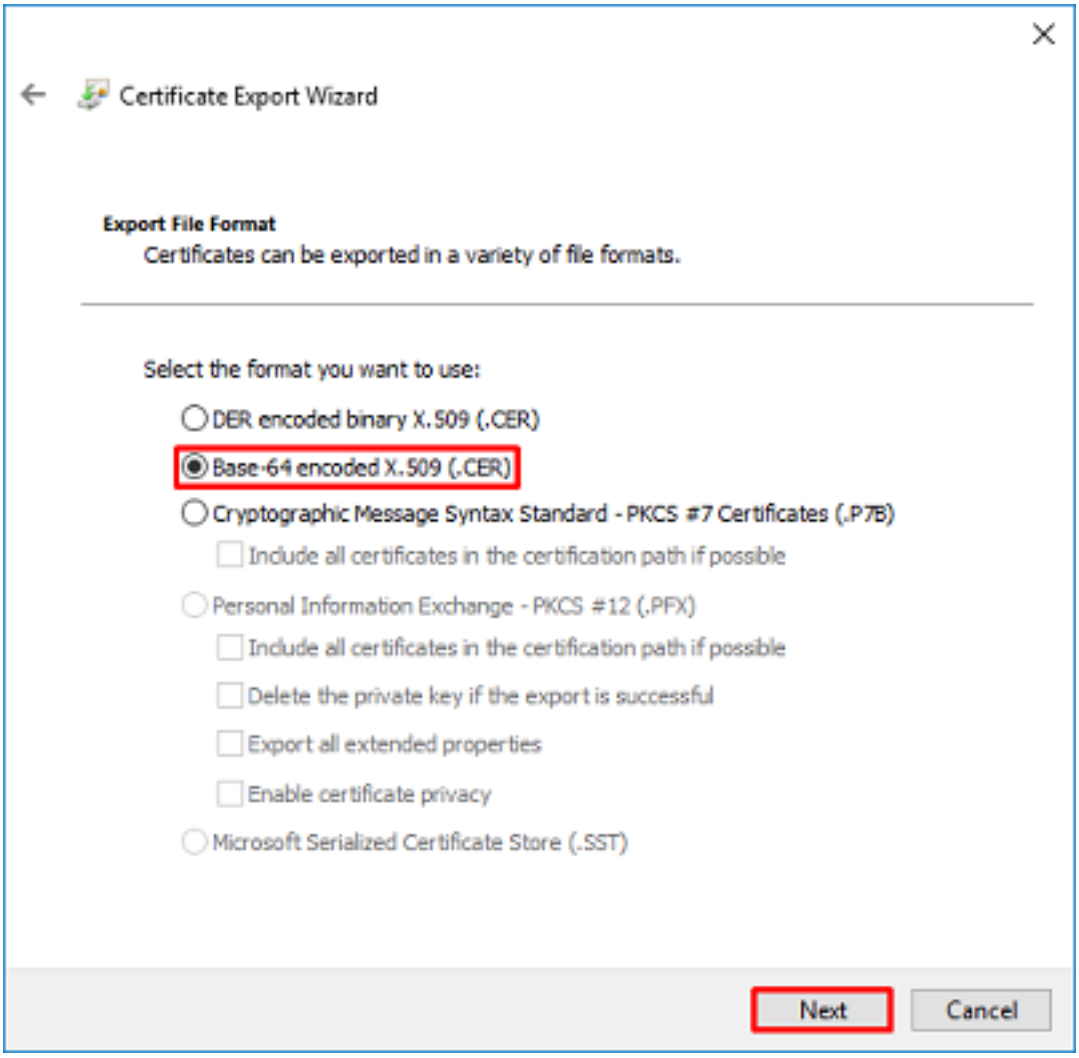
Sous l'onglet **Détails**, cliquez sur **Copier dans un fichier...**



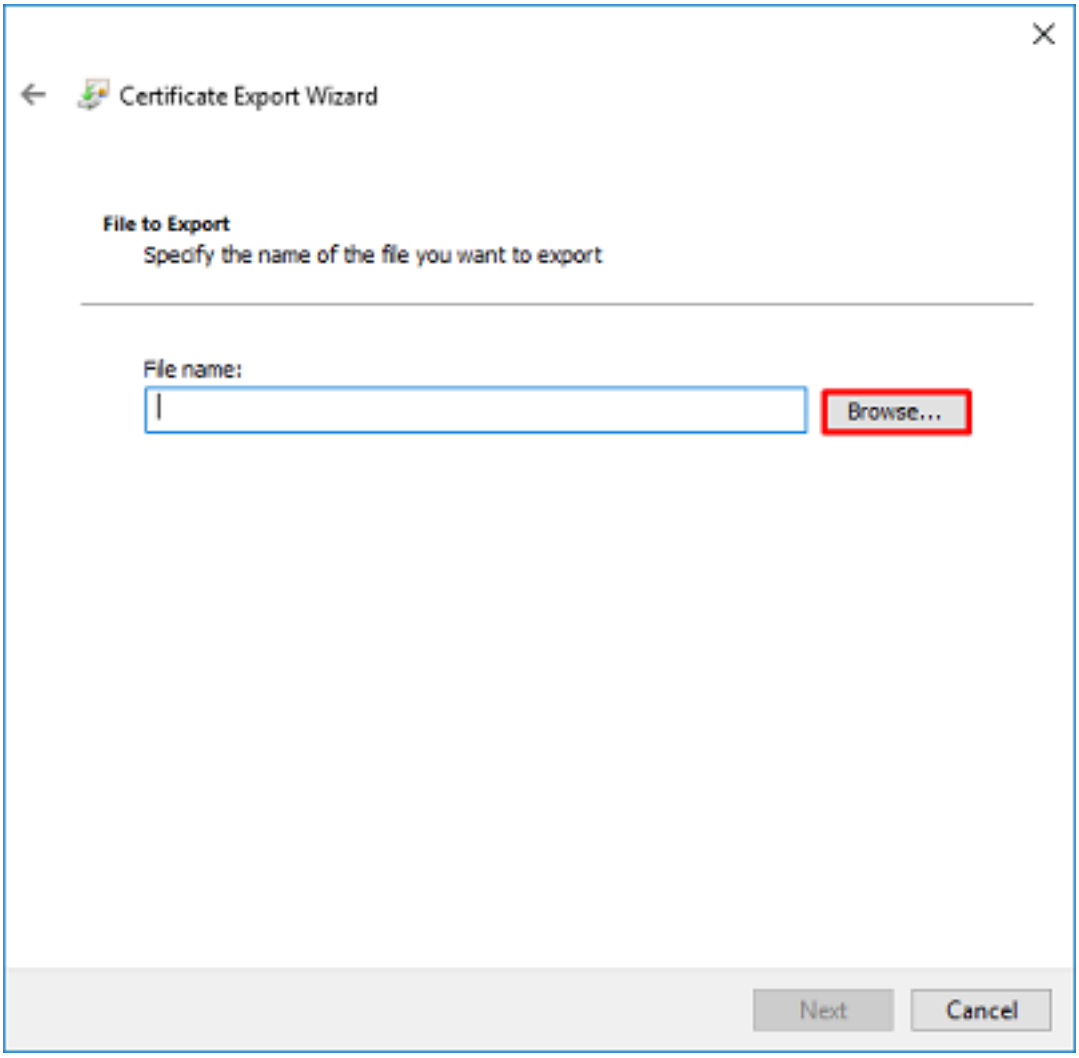
10. Accédez à l'**Assistant Exportation de certificat** qui exporte l'autorité de certification racine au format PEM.

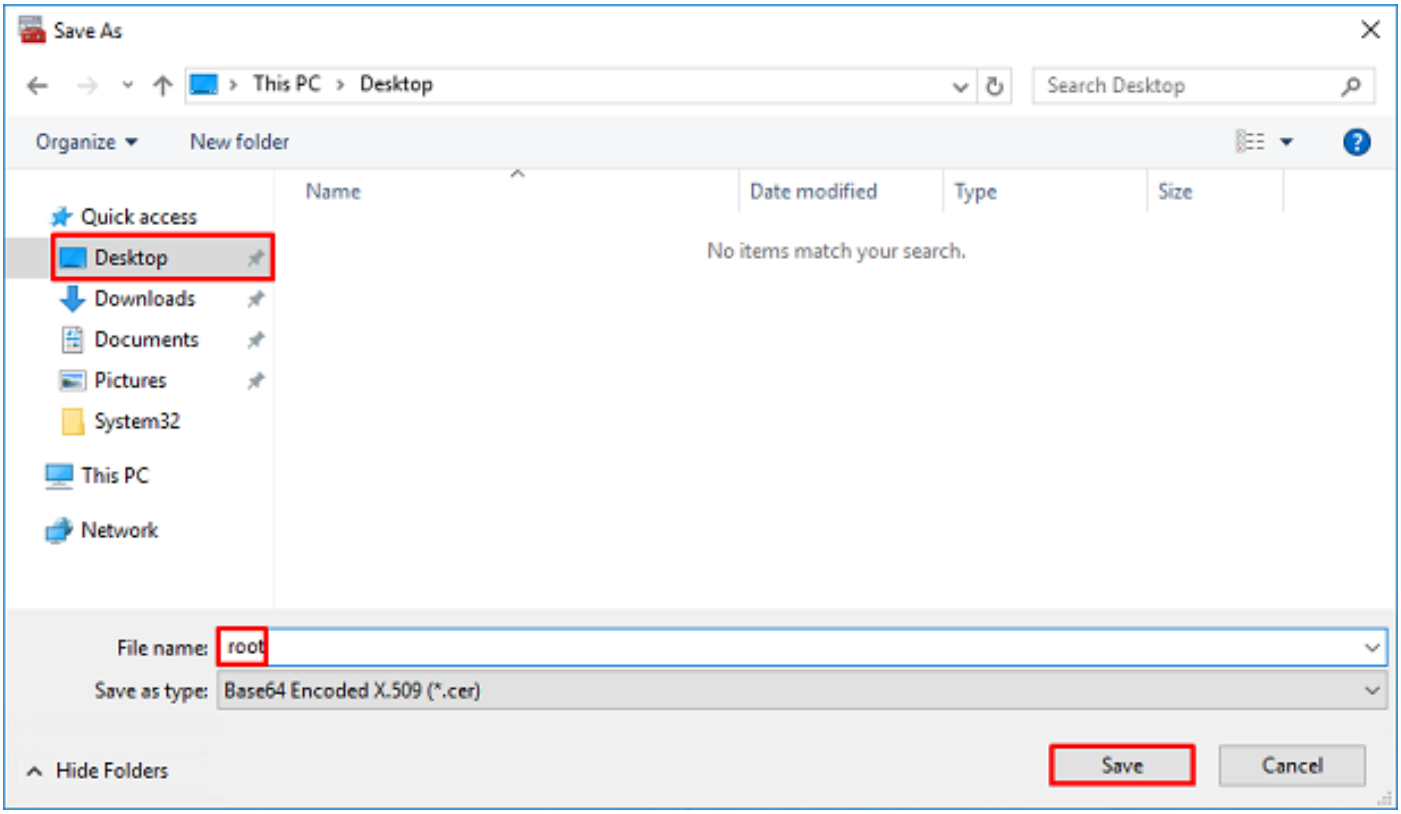


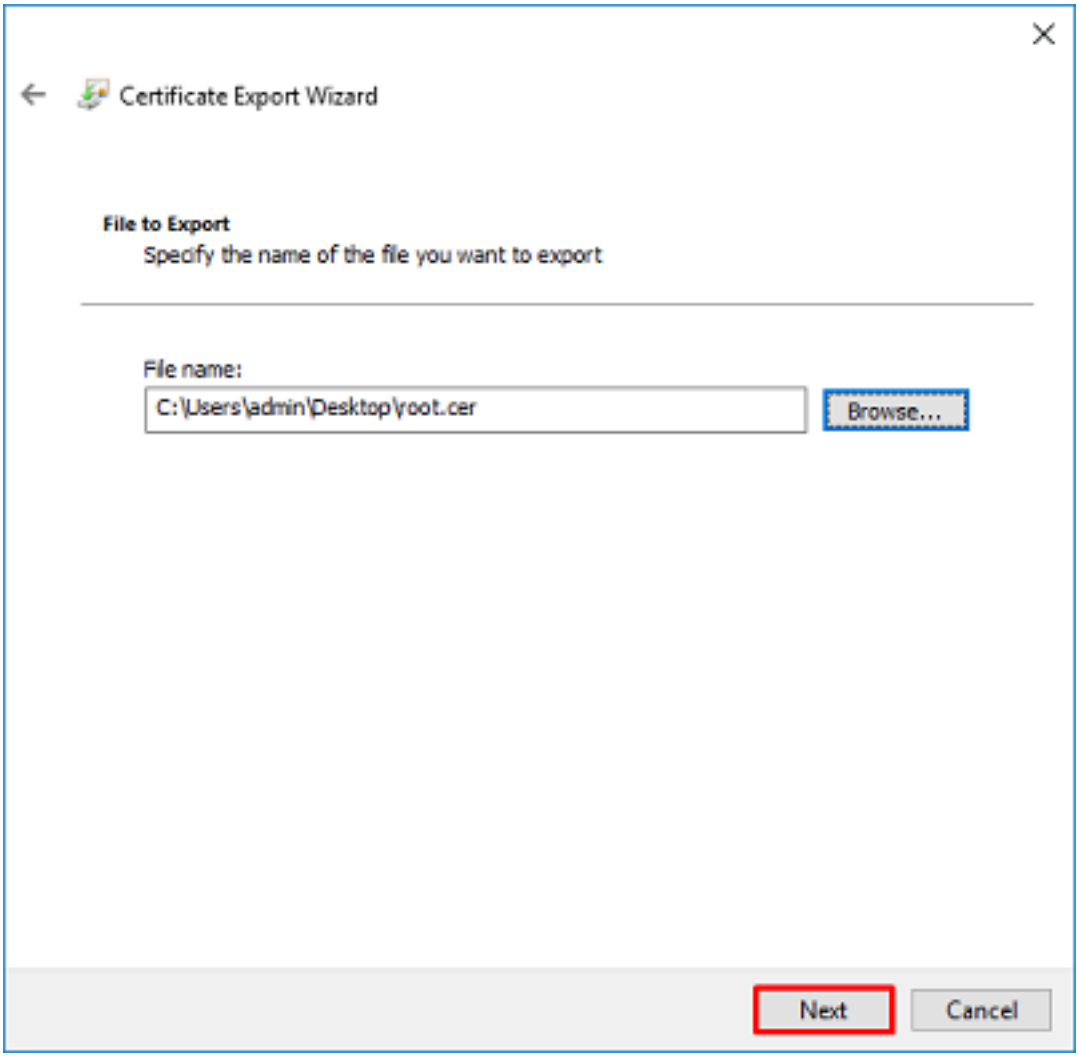
Sélectionner **encodé en base 64 X.509**



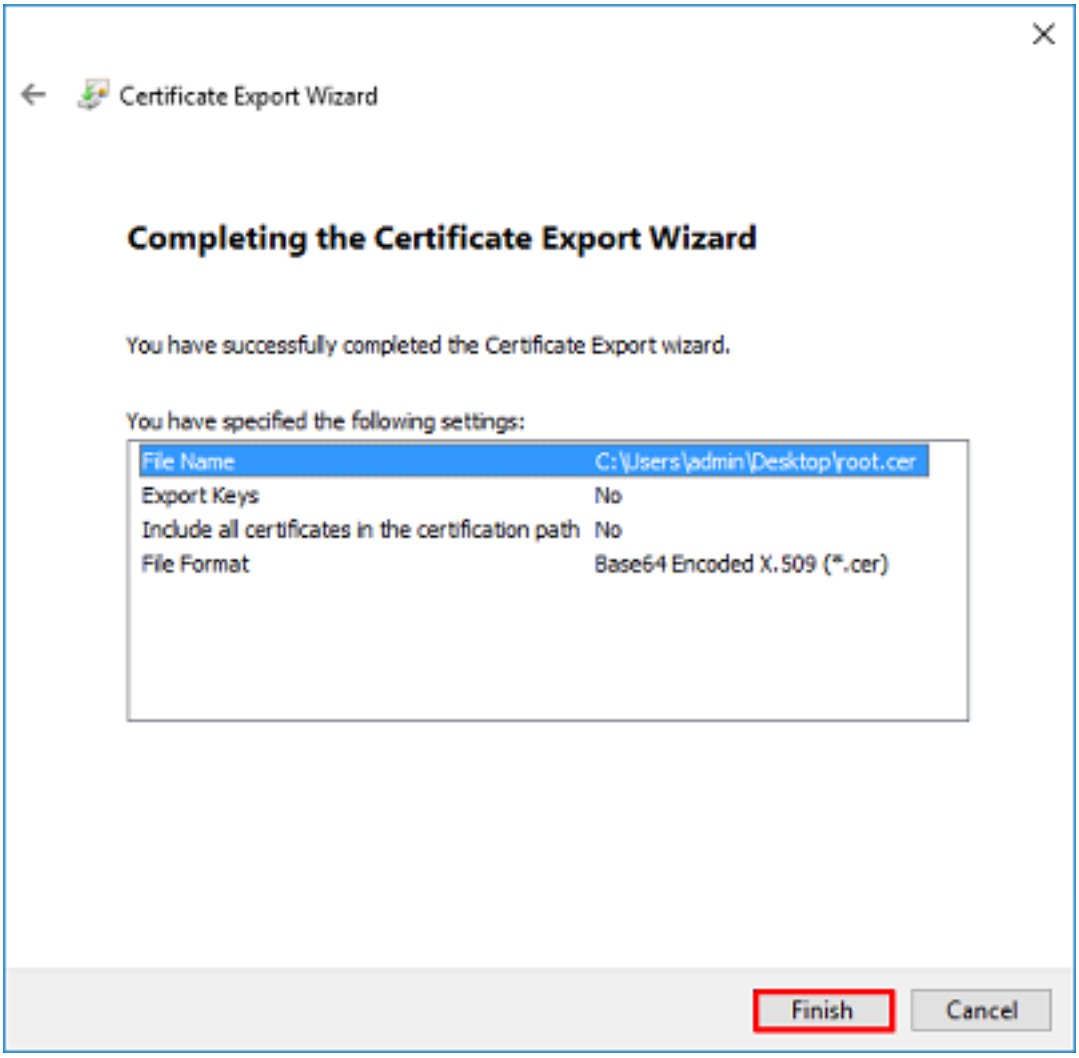
Sélectionnez le nom du fichier et l'emplacement d'exportation.


Certificate 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
Search Desktop
Organize
New folder
Quick access
Desktop
Downloads
Documents
Pictures
System32
This PC
Network
Name
Date modified
Type
Size
No items match your search.
File name:
root
Save as type:
Base64 Encoded X.509 (*.cer)
Hide Folders
Save
Cancel



Cliquez maintenant sur **Terminer**.



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

```
-----BEGIN CERTIFICATE-----
MIIDCDCCAfCgAwIBAgIQE4ZG5Z1wT6lONTjooEQyMTANBgkqhkiG9w0BAQsFADAd
MRswGQYDVQQDExJleGFtcGxlLVdJTjIwMTYtQ0EwIBcNMjAwNDI3MTQ1MDU5WhgP
MjA2MDA0MTkxNDUwNTlaMB0xGzAZBgNVBAMTEmV4YW1wbGUtV0lOMjAxNi1DQTCC
ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAI8ghT719NzSQpoQPh0YT67b
Ya+PngsxMyvkewP33QLTAWw1HW1Tb9Mk5BDWOItTaVsgHwPBfd++M+bLn3AiZnHV
OO+k6dVVY/E5qVkEKSGoY+v940S2316lzdwReMOFhgbc2qMertIoficrRhihonuU
Cjyeub3CO+meJUuKom2R47C0D35TUvo/FEHGgXJFaJS1se2UrpNO7KEMkfA1LPuM
aob4XE/OzxYQpPa18djsNnskfcFqD/HOTFQN4+SrOhHWlRnUIQBUaLdQaabhipD/
sVs5PneYJX8YKma821uYI6j90YuytmsHBtCieyC062a8BKqOL7N86HFPFkMA3u8C
AwEAAaNCMEAwDgYDVR0PAQH/BAQDAgGGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0O
BBYEFD2fJjf7ER9EM/HCxCVFN5QzqEdvMA0GCSqGSIb3DQEBCwUAA4IBAQB31ZJo
vzwVD3c5Q1nrNP+6Mq62OFpYH91k4Ch9S5g/CEOemhcwg8MDIoxW2dTsjenAEt7r
phFIHZoCoSyjBjMgK3xybmoSeg8vBjCXseYNGEmOc9KW1oFmTOvdNVIb7Xpl1IVa
6tALTt3ANRNgREtxPA6yQbthKGavW0Anfsojk9IcDr2vp0MTjlBCxsTscbubRl+D
dLEFKQqmMeYvkVf+a7a64mqPZsG3Uxo0rd6cZxAPkq/ylcdwNSJFfQV3DgZg+R96
9WLCR3Obig6xyo9Zu+lixcWpdrbADO6zMhbEYEhkhOOjBrUEBBI6Cy83iTZ9ejsk
KgwBJXEu33PplW6E
-----END CERTIFICATE-----
```

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

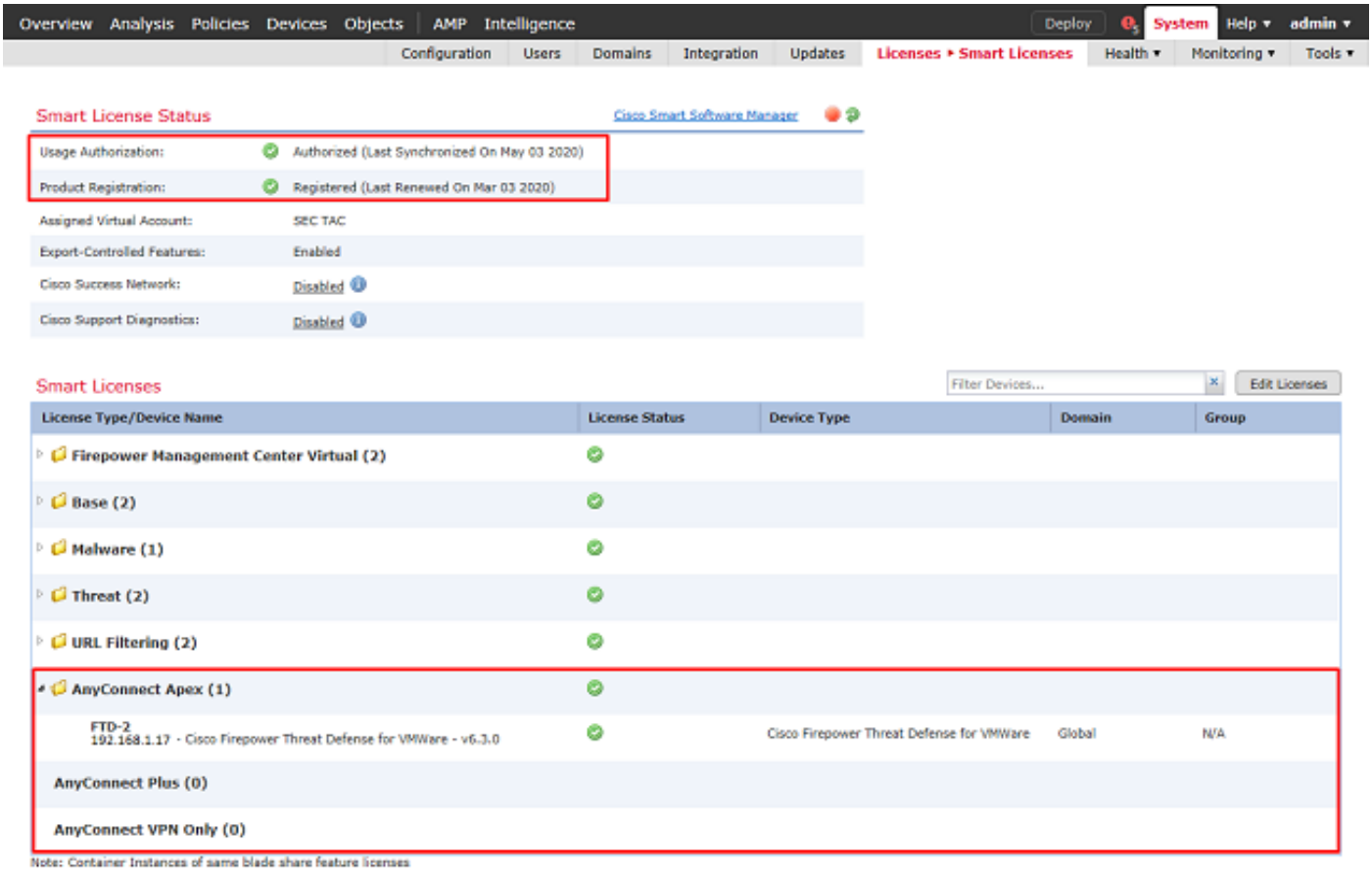
Configurations FMC

Vérifier les licences

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

1. Accédez à **System > Licenses > Smart Licensing**.

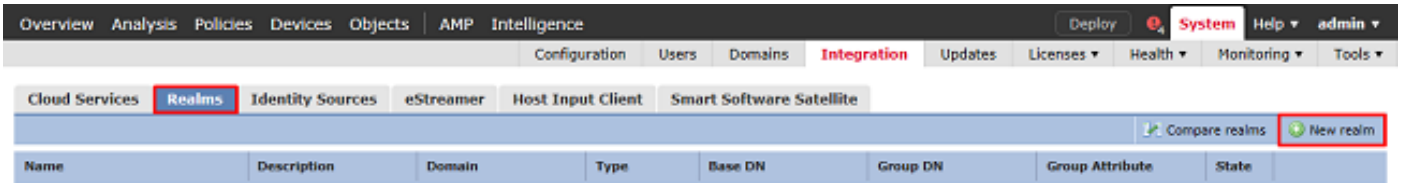
2. Vérifiez que les périphériques sont conformes et correctement enregistrés. Assurez-vous que le périphérique est enregistré avec une licence **AnyConnect Apex**, **Plus**, ou **VPN Only**.



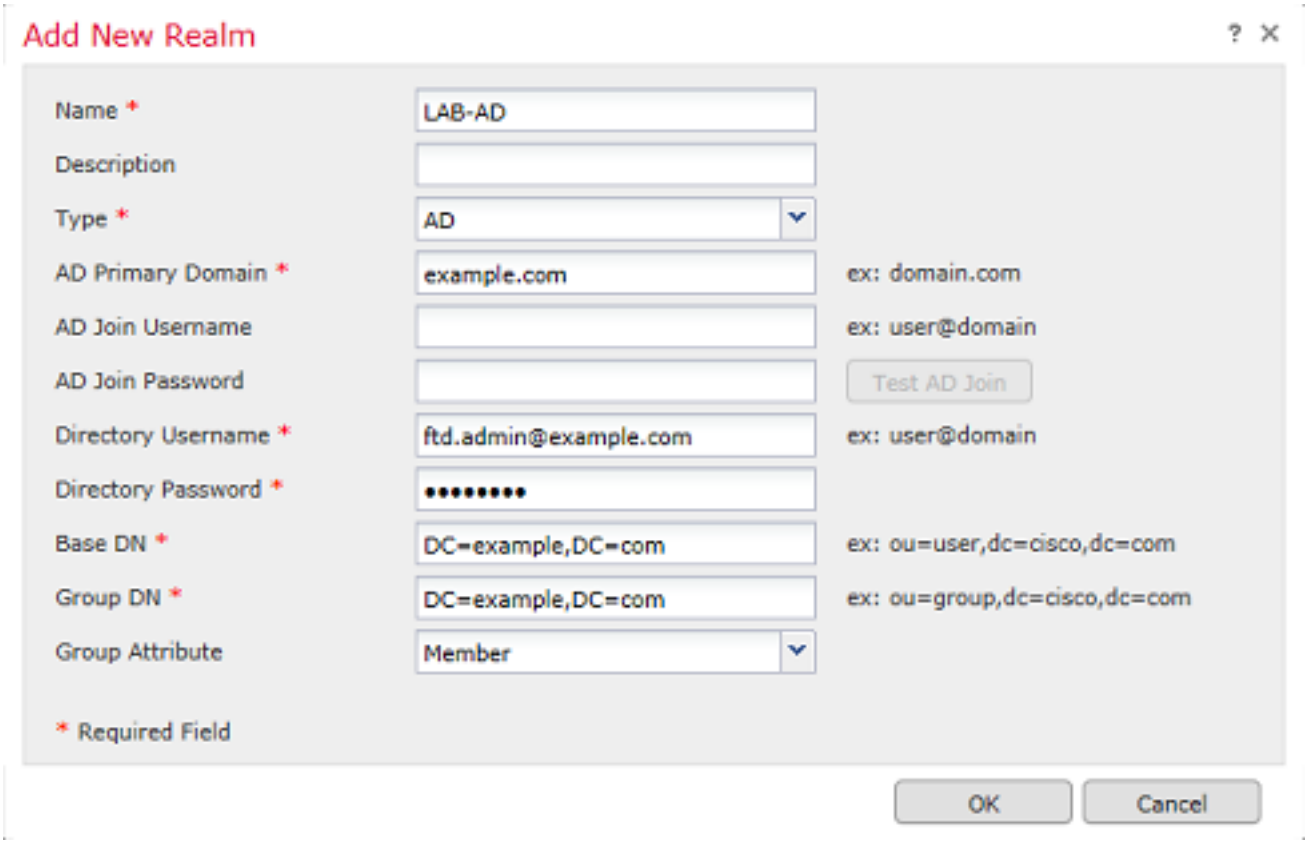
Configurer le domaine

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

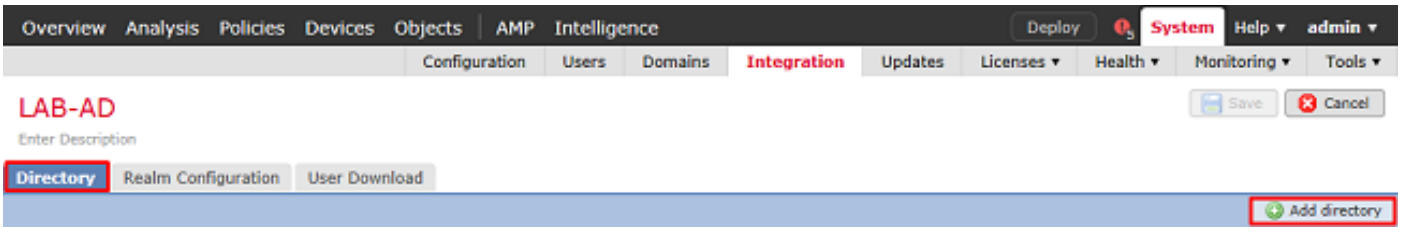
2. Sous **Domaines**, cliquez sur **Nouveau domaine**.



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



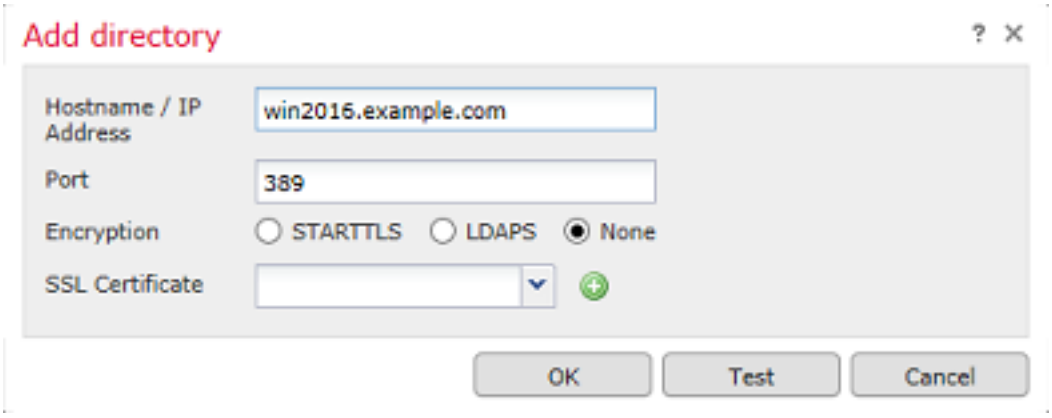
4. Dans la nouvelle fenêtre, sélectionnez **Répertoire** si ce n'est déjà fait, cliquez sur **Ajouter un répertoire**.



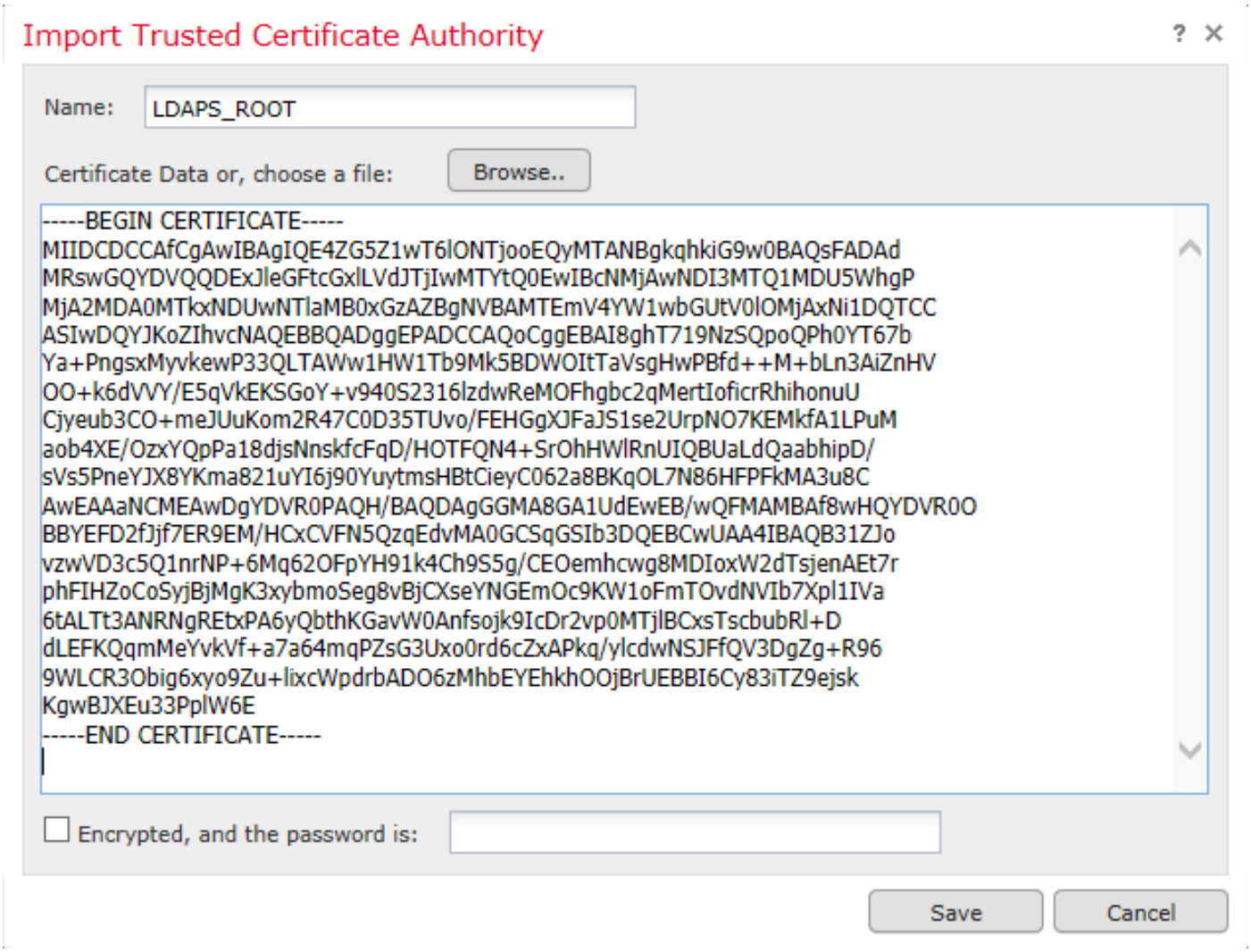
Renseignez les détails relatifs au serveur AD. Notez que si le nom de domaine complet est utilisé, FMC et FTD ne peuvent pas se lier correctement à moins que DNS ne soit configuré pour résoudre le nom de domaine complet.

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

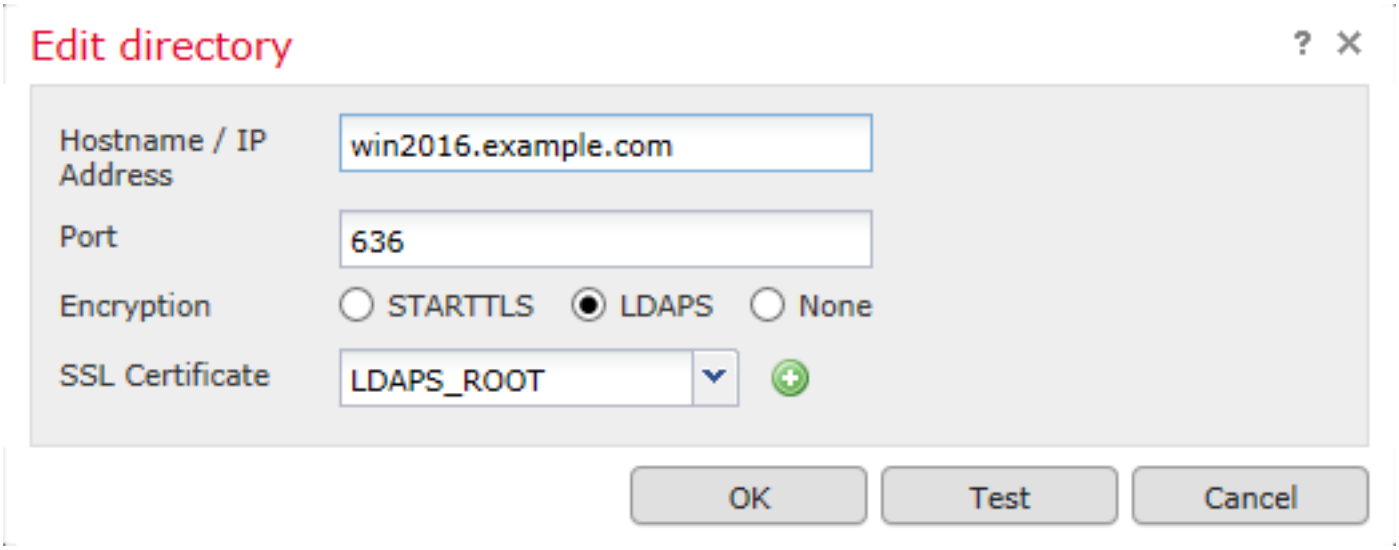
Afin de configurer DNS pour le FTD, naviguez vers **Devices > Platform Settings**, créez une nouvelle stratégie, ou modifiez une stratégie actuelle, puis allez dans DNS.



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



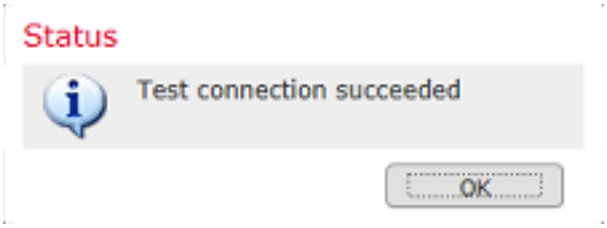
Sélectionnez l'autorité de certification racine nouvellement ajoutée dans la liste déroulante en regard de SSL Certificate et cliquez sur STARTTLS ou LDAPS.



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

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

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



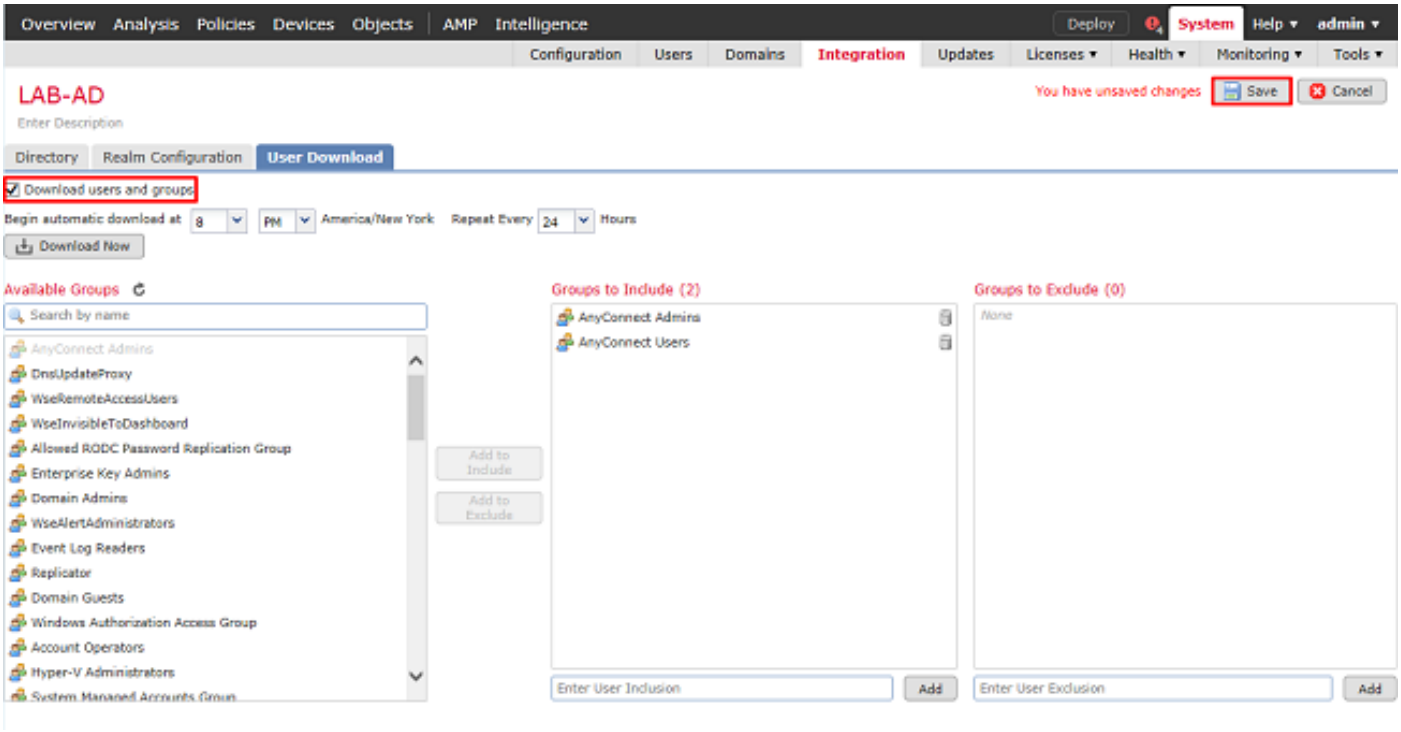
5. Sous **Téléchargement utilisateur**, téléchargez les groupes qui sont utilisés pour l'identité de l'utilisateur dans les étapes ultérieures.

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

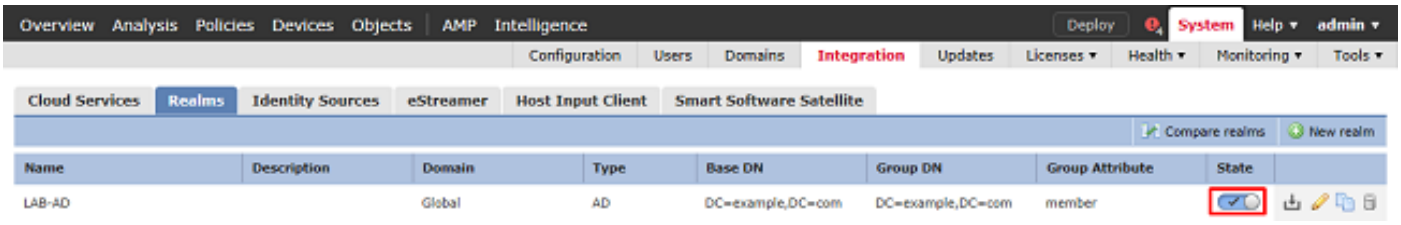
Les groupes peuvent être inclus ou exclus, mais par défaut, tous les groupes situés sous le DN du groupe sont inclus.

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

Une fois terminé, cliquez sur **Save** (enregistrer).

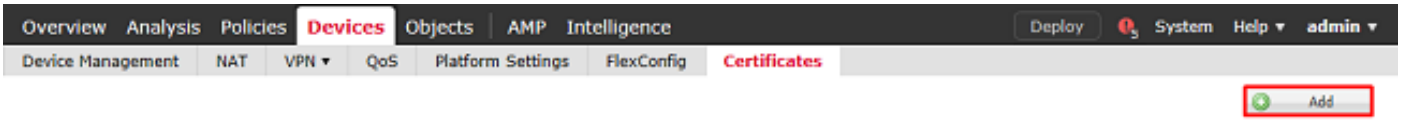


6. Activez le nouveau domaine.

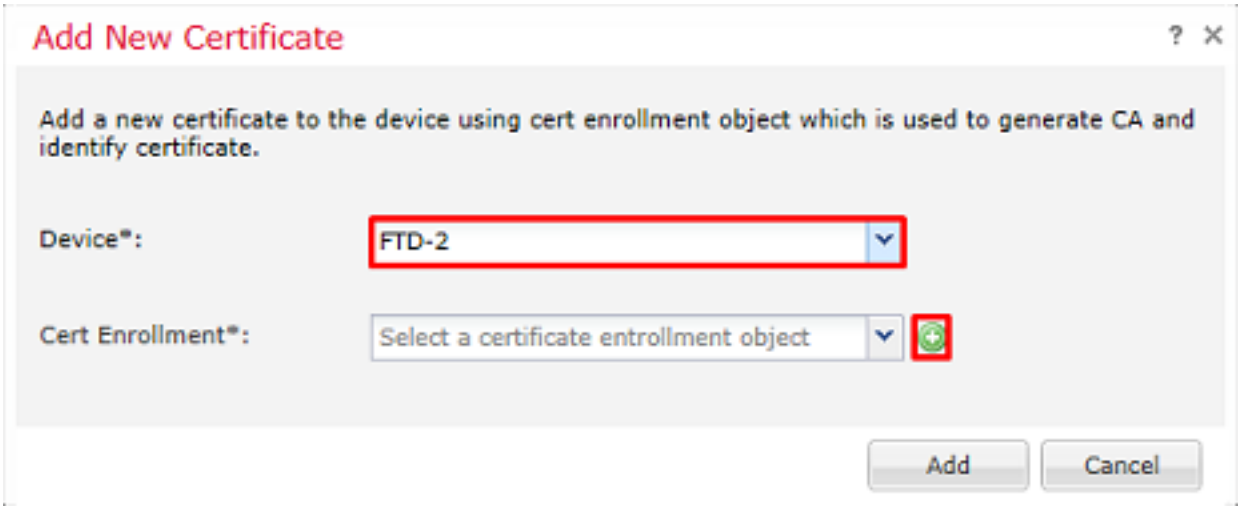


7. Si LDAPS ou STARTTLS est utilisé, l'autorité de certification racine doit également être approuvée par le FTD. Pour ce faire, accédez d'abord à **Périphériques > Certificats**.

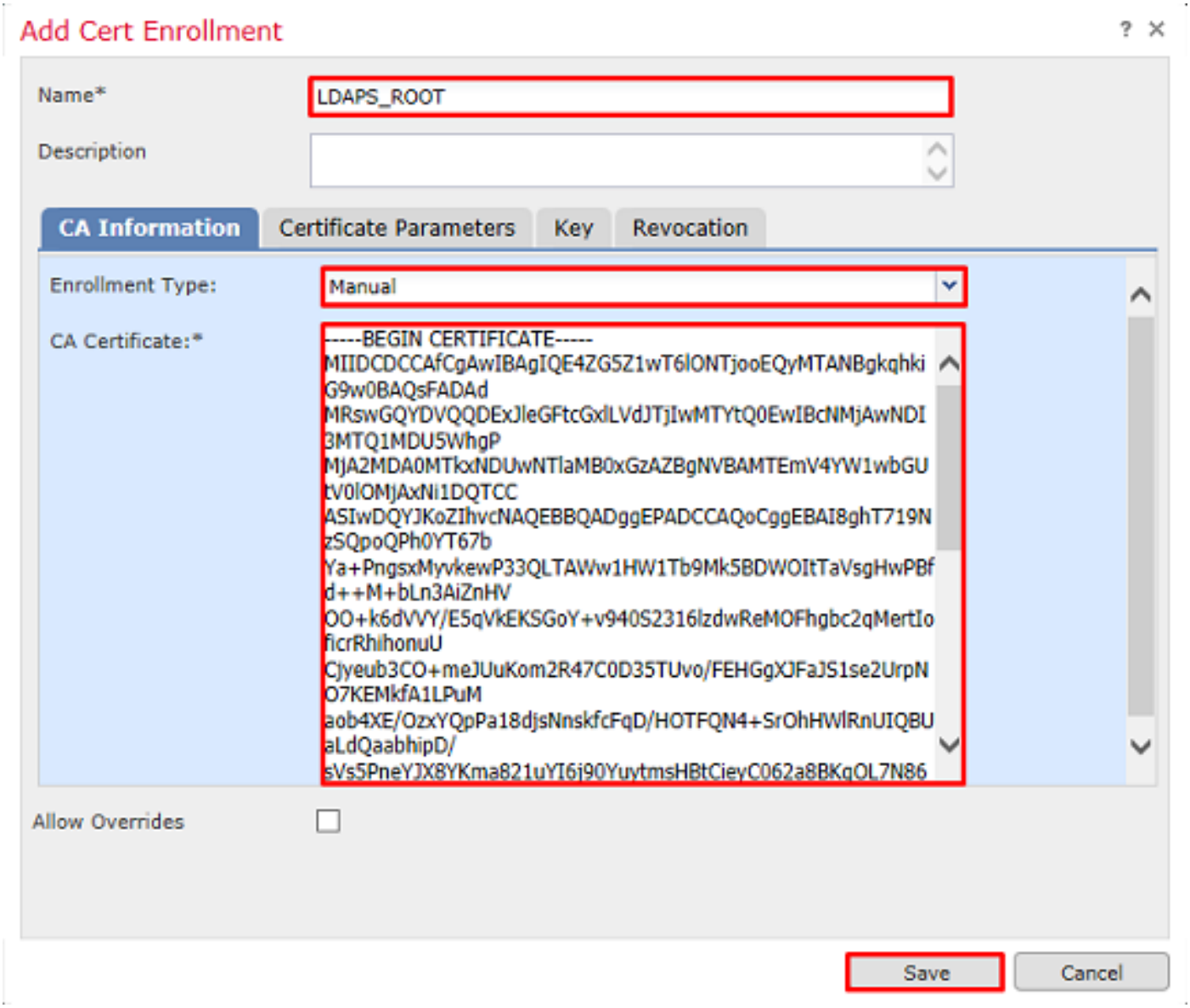
Cliquez sur Ajouter en haut à droite.



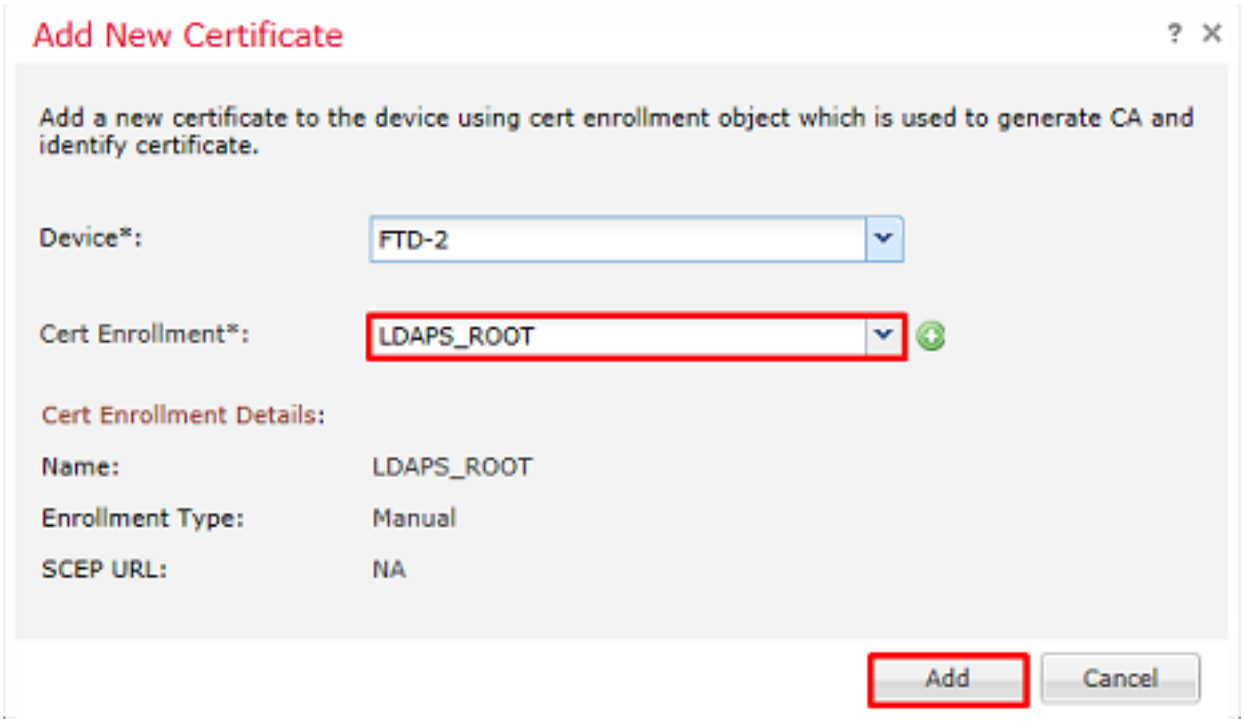
Sélectionnez le FTD, la configuration LDAP est ajoutée, puis cliquez sur le symbole + vert.



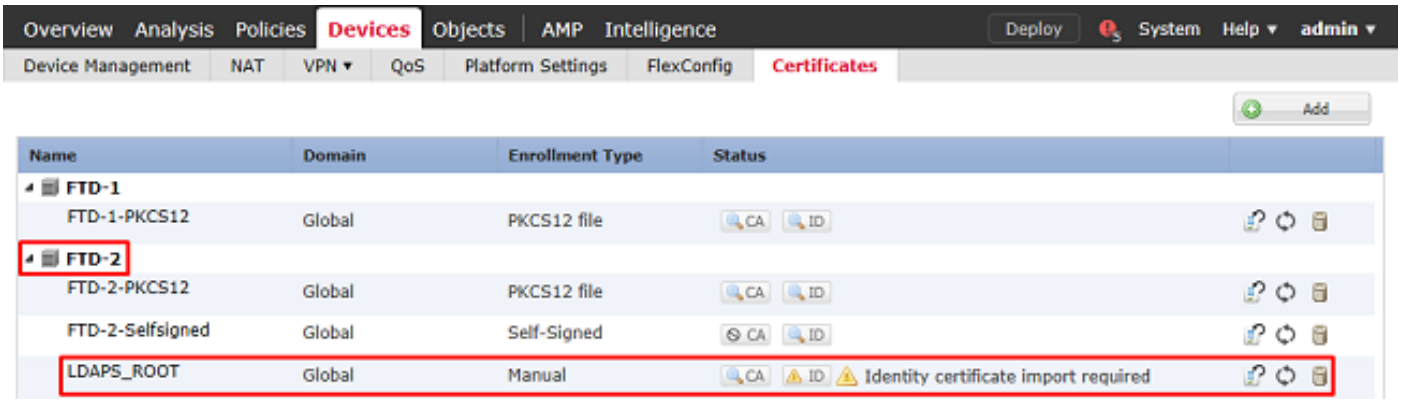
Attribuez un **nom** au point de confiance, puis choisissez **Inscription manuelle** dans la liste déroulante **Type d'inscription**. Collez ici le certificat d'autorité de certification racine PEM, puis cliquez sur **Save**.



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



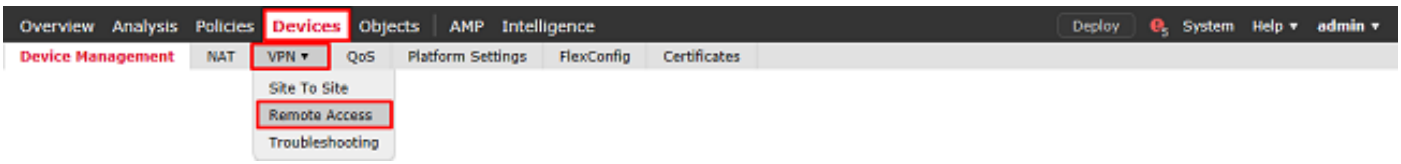
Le nouveau point de confiance apparaît sous le FTD. Bien qu'il mentionne que l'importation de certificat d'identité est requise, il n'est pas nécessaire pour les besoins du FTD pour être en mesure d'authentifier le certificat SSL envoyé par le serveur LDAPS et donc ce message peut être ignoré.



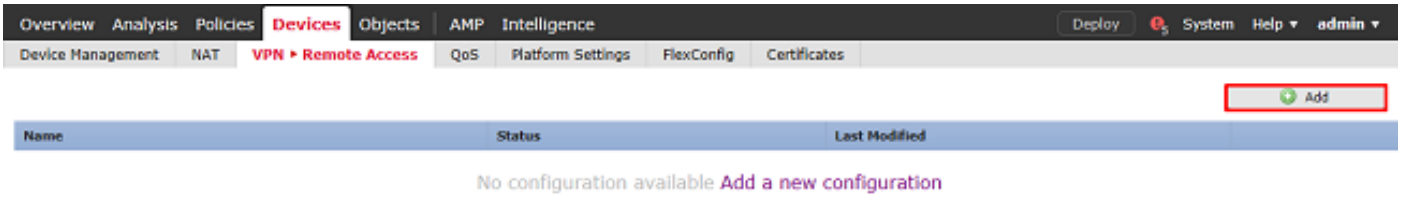
Configurer AnyConnect pour l'authentification AD

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

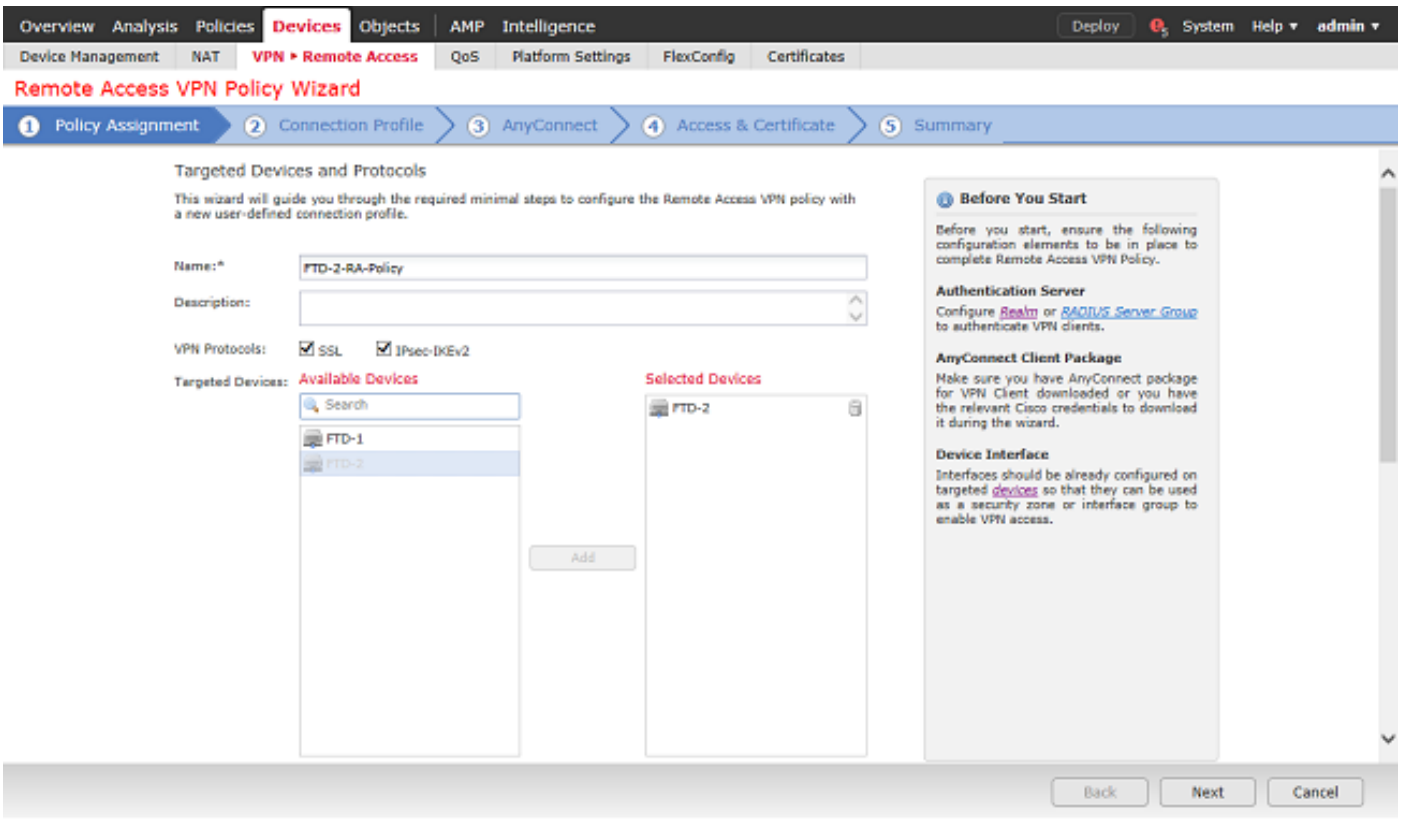
Accédez à **Devices > VPN > Remote Access**.



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



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

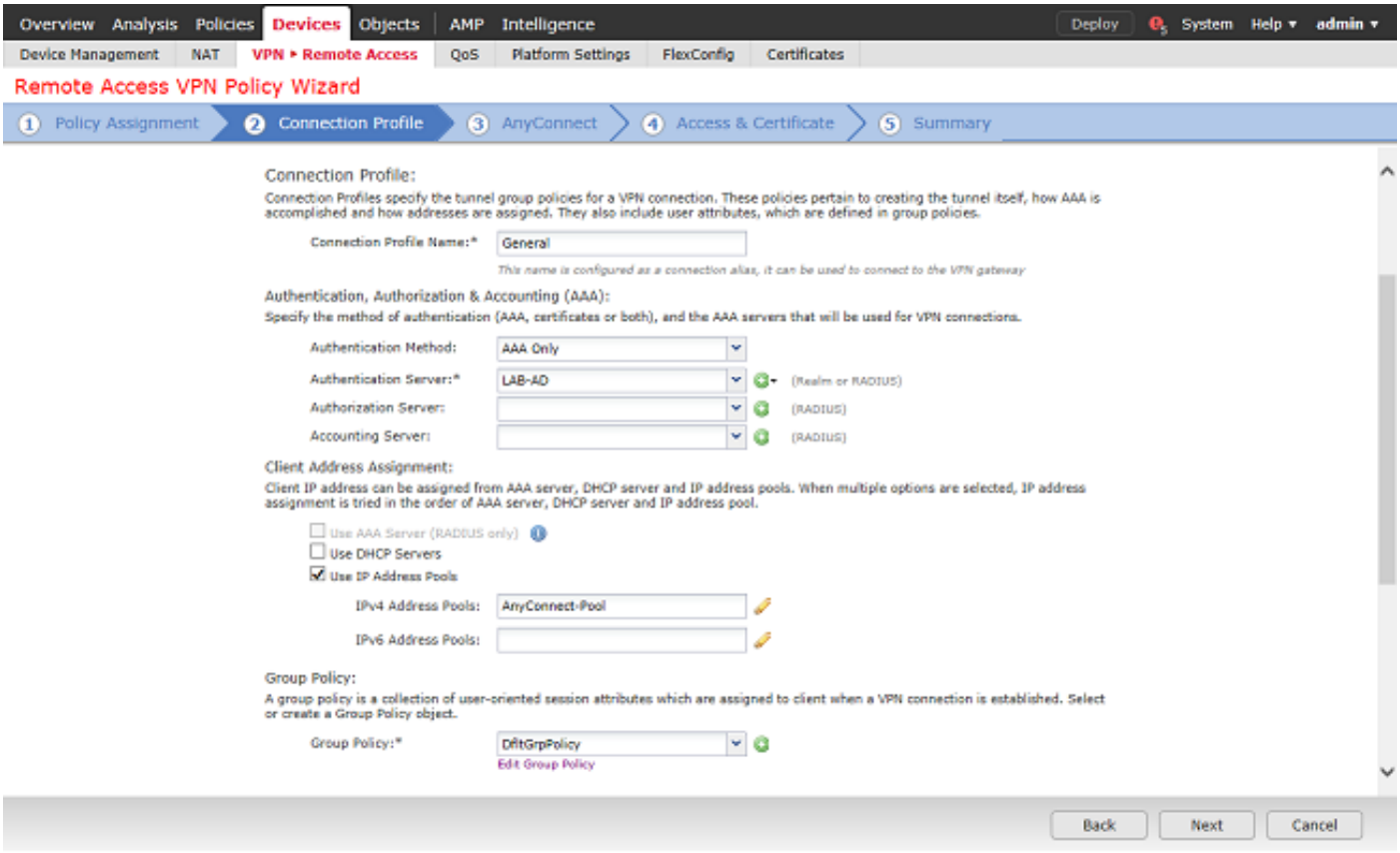


Sous **Profil de connexion**, spécifiez le nom du **profil de connexion** qui est également utilisé comme alias de groupe que les utilisateurs d'AnyConnect voient lorsqu'ils se connectent.

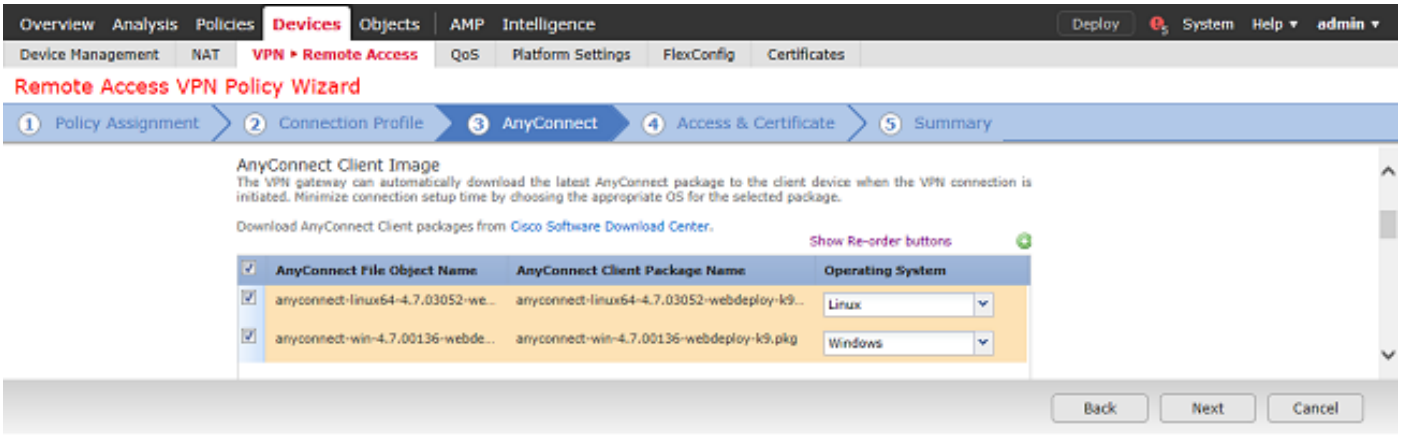
Spécifiez le domaine précédemment créé sous **Authentication Server**.

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

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



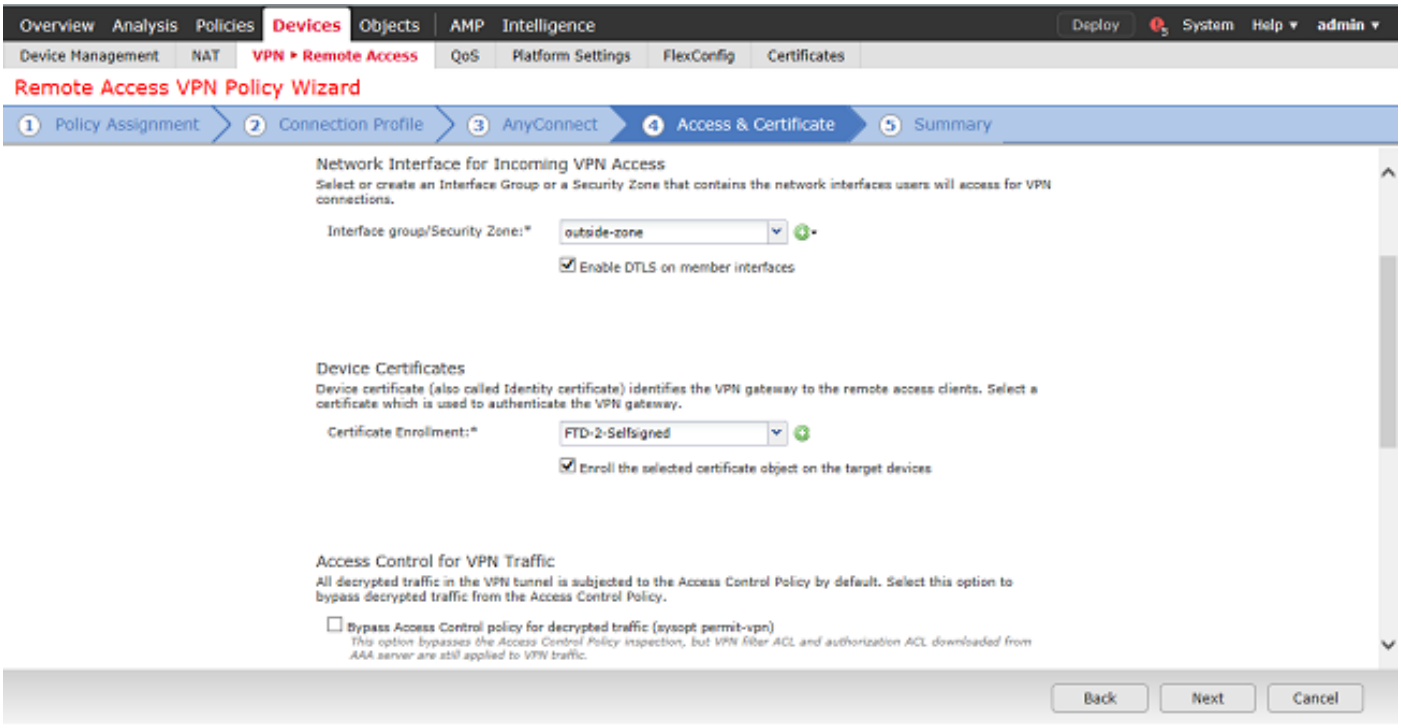
Sous AnyConnect, téléchargez et spécifiez les packages AnyConnect utilisés.



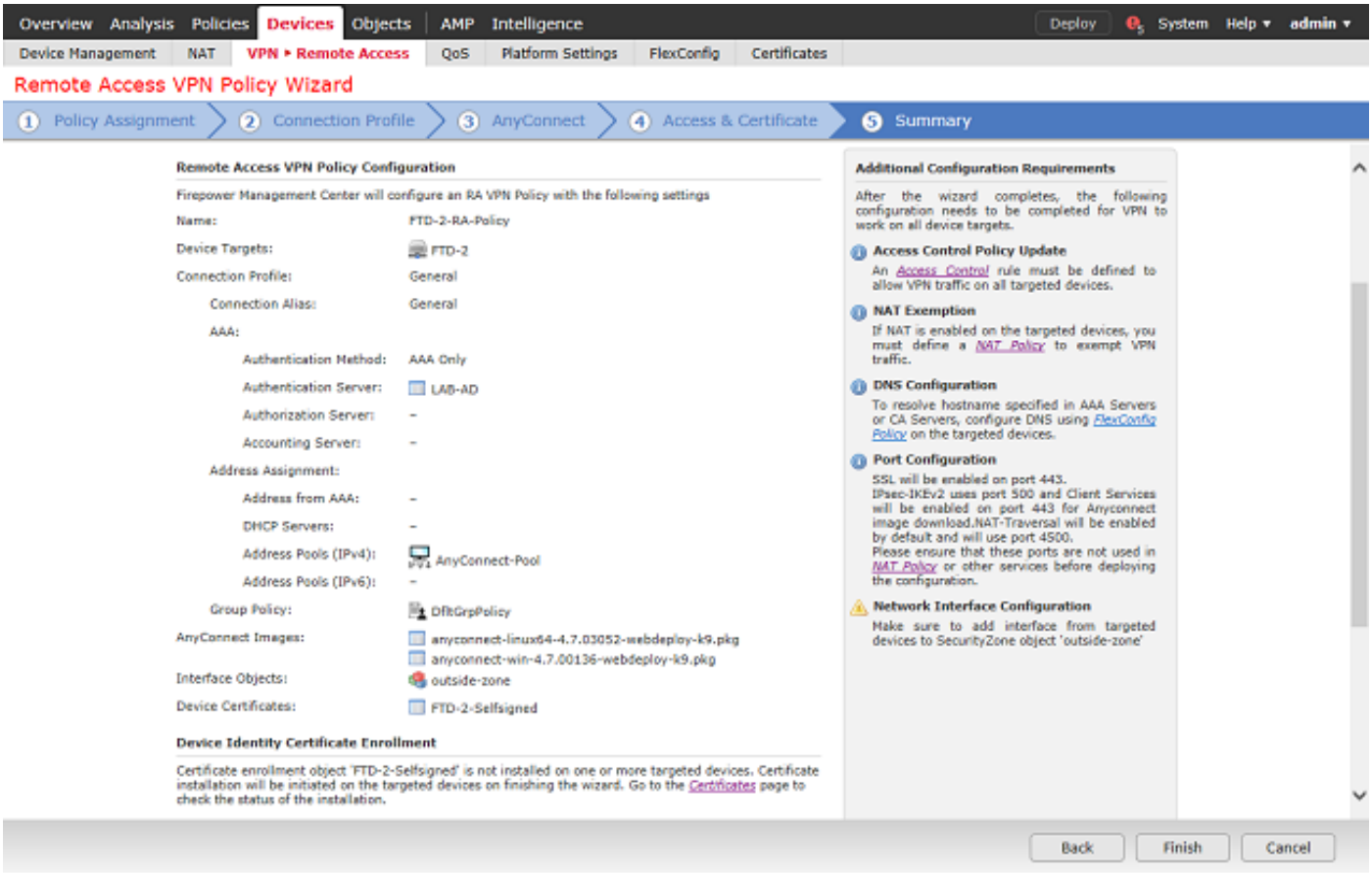
Sous **Access & Certificate**, spécifiez l'interface à laquelle les utilisateurs d'AnyConnect accèdent pour AnyConnect.

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

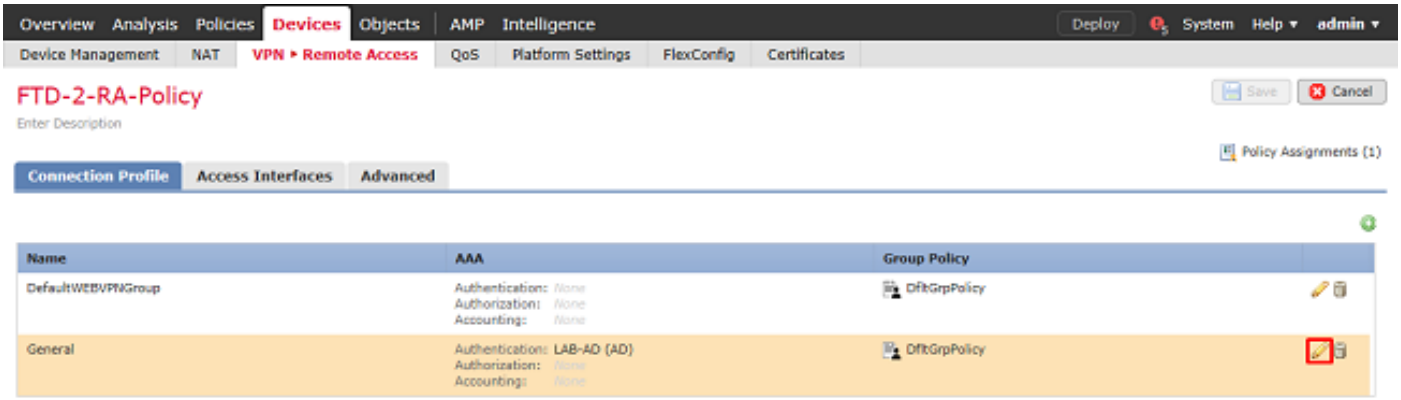
Assurez-vous que la case à cocher **Bypass Access Control policy** for decrypted traffic (sysopt permit-vpn) est laissée décochée afin que l'identité utilisateur créée ultérieurement prenne effet pour les connexions RAVPN.



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



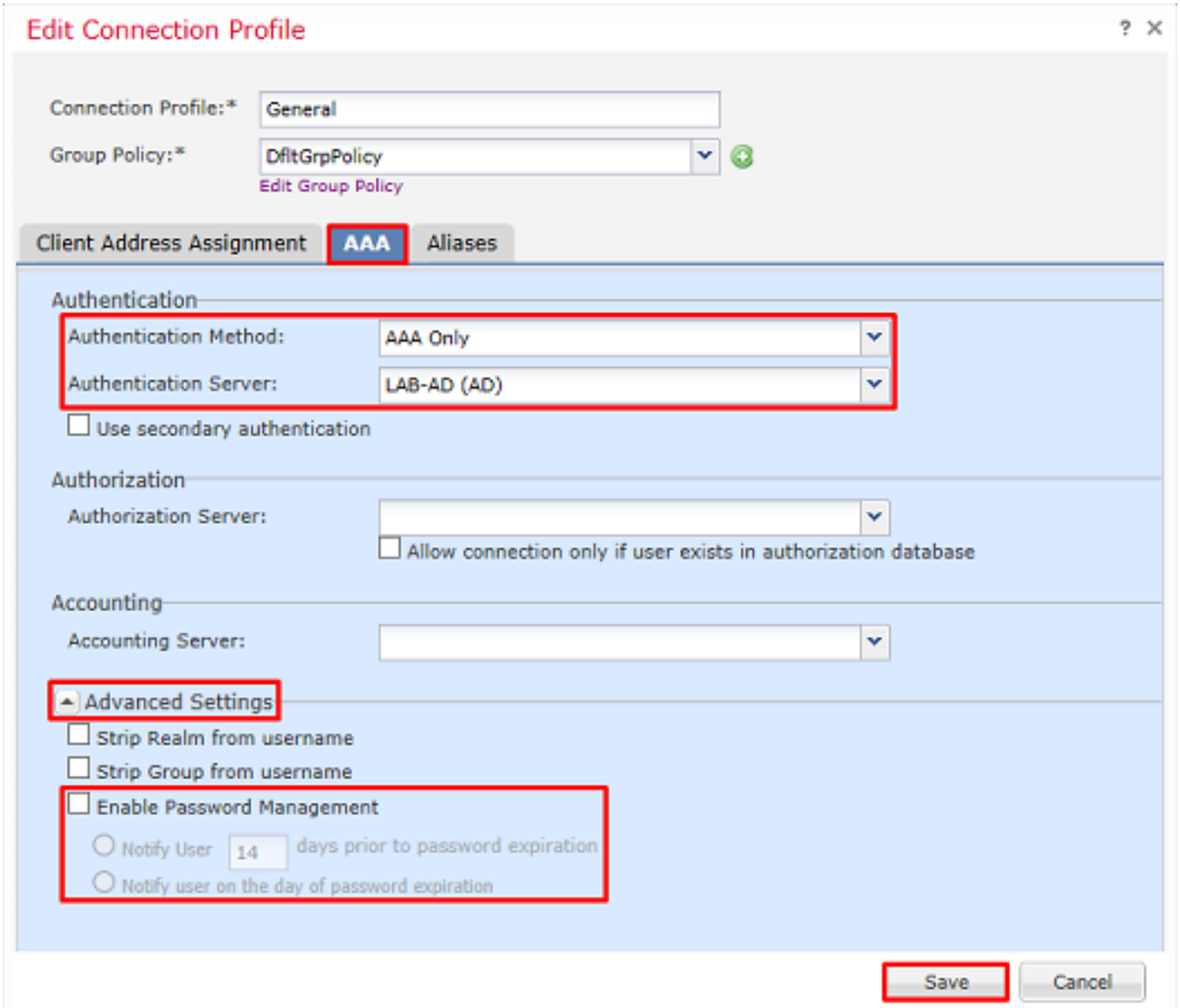
3. Sous **Remote Access VPN Policy**, cliquez sur **edit** pour le profil de **connexion** approprié.



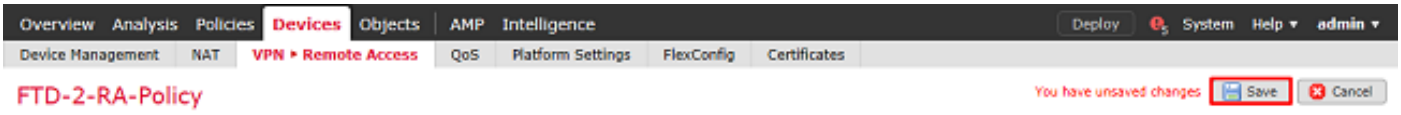
Assurez-vous que le serveur d'authentification est défini sur le domaine créé précédemment.

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

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



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

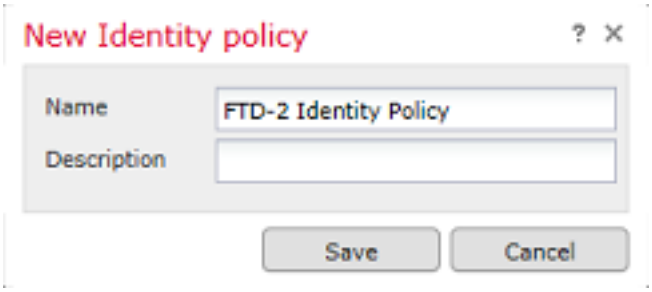


Activer la stratégie d'identité et configurer les stratégies de sécurité pour l'identité utilisateur

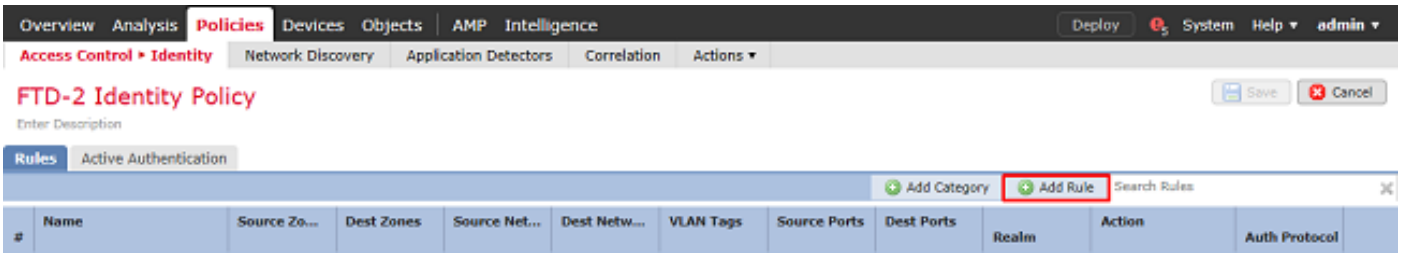
1. Accédez à **Politiques > Contrôle d'accès > Identité**.

Créez une nouvelle stratégie d'identité.

Spécifiez un **nom** pour la nouvelle **stratégie d'identité**.



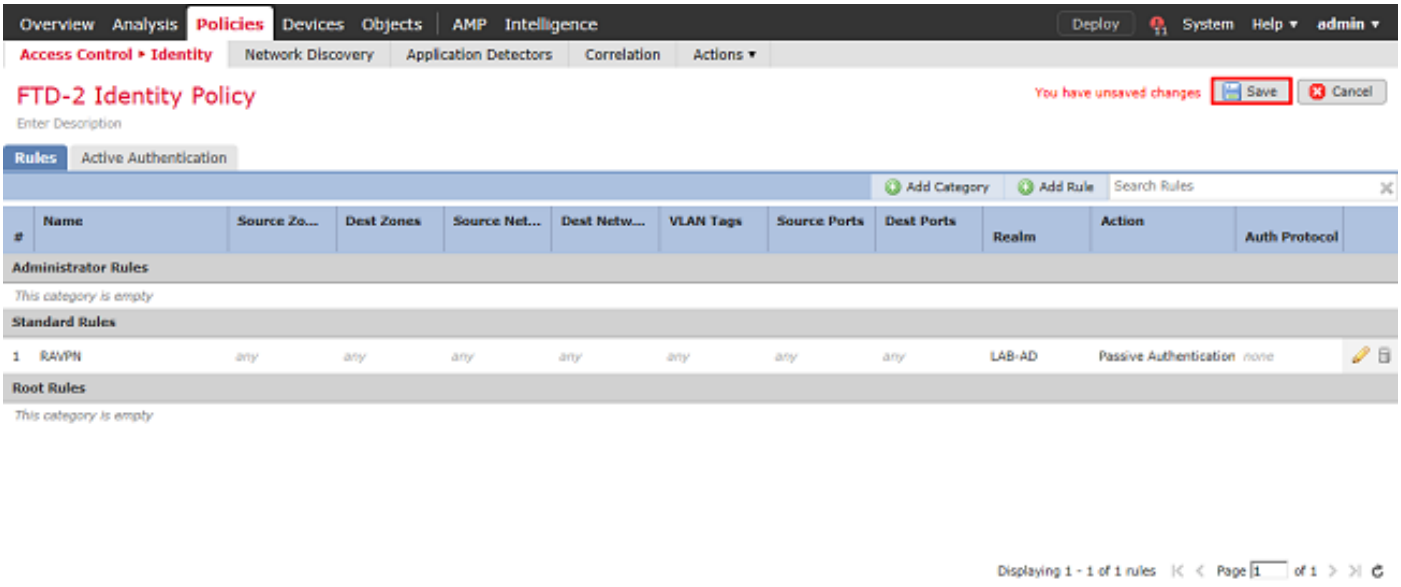
2. Cliquez sur **Ajouter une règle**.



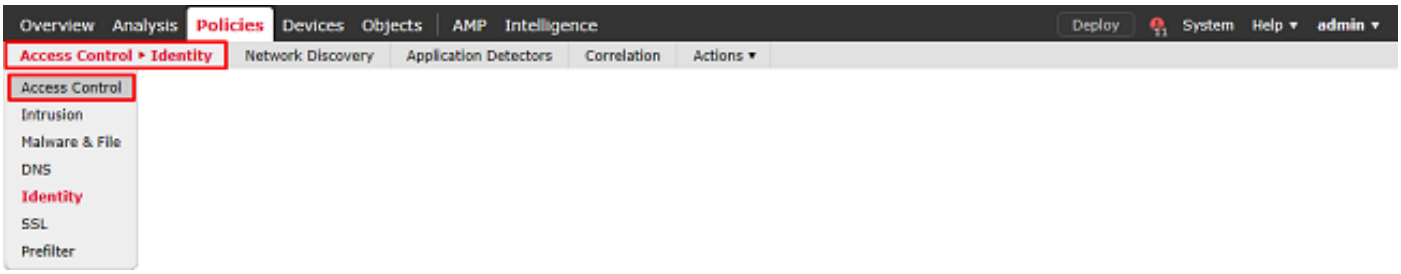
3. Spécifiez un **nom** pour la nouvelle règle. Assurez-vous qu'elle est activée et que l'action est définie sur Authentification passive.

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

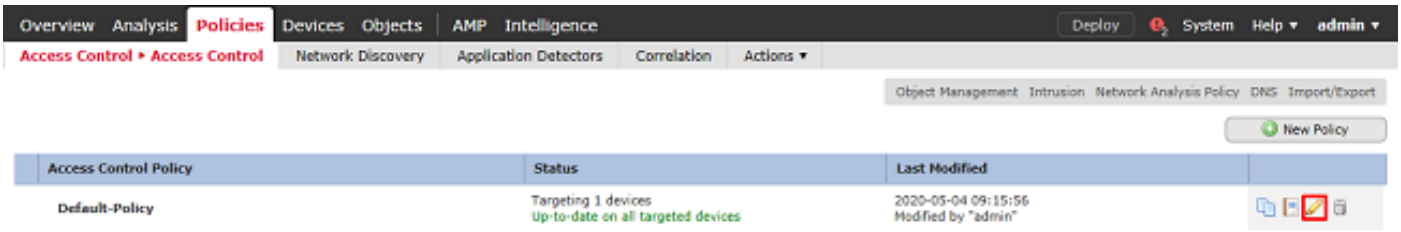
4. Cliquez sur **Enregistrer**.



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

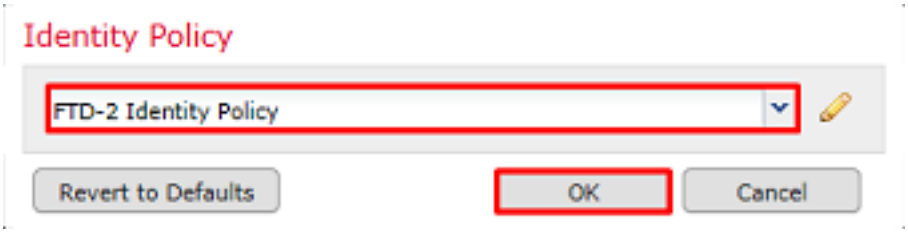


6. Modifiez la **stratégie de contrôle d'accès** sous laquelle le FTD est configuré.

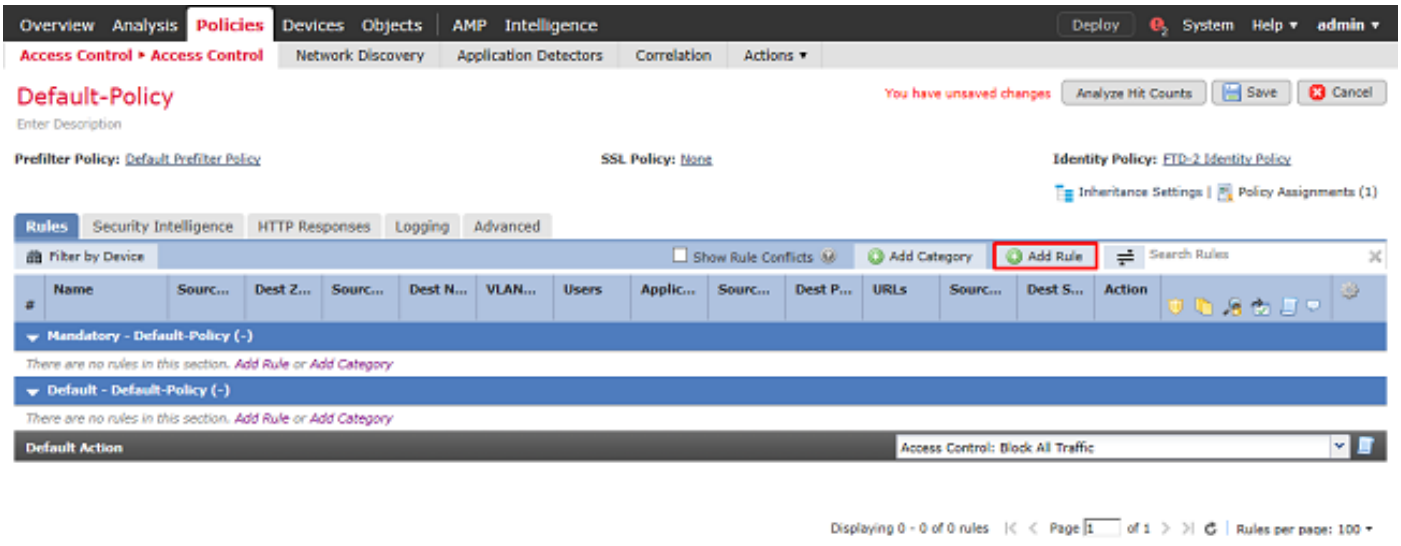


7. Cliquez sur la valeur en regard de **Politique d'identité.**

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



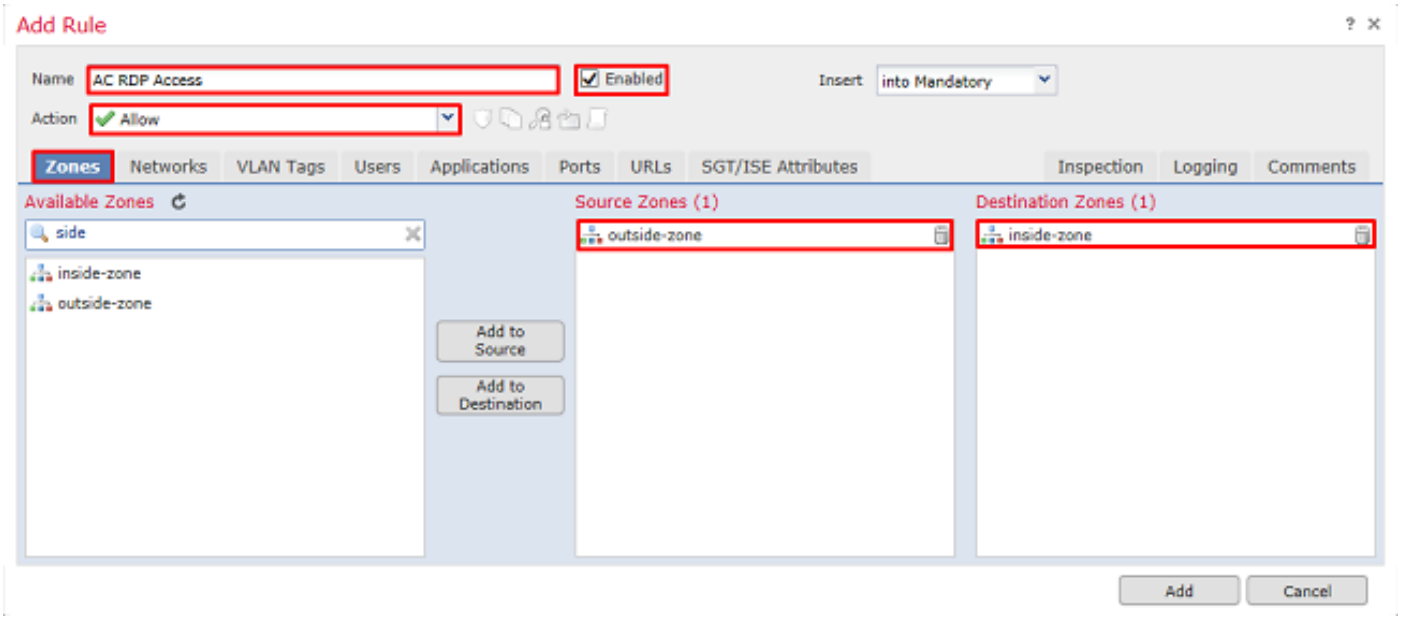
8. Cliquez sur **Add Rule** pour créer une nouvelle règle ACP. Ces étapes créent une règle permettant aux utilisateurs du groupe AnyConnect Admins de se connecter aux périphériques du réseau interne à l'aide du protocole RDP.



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

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

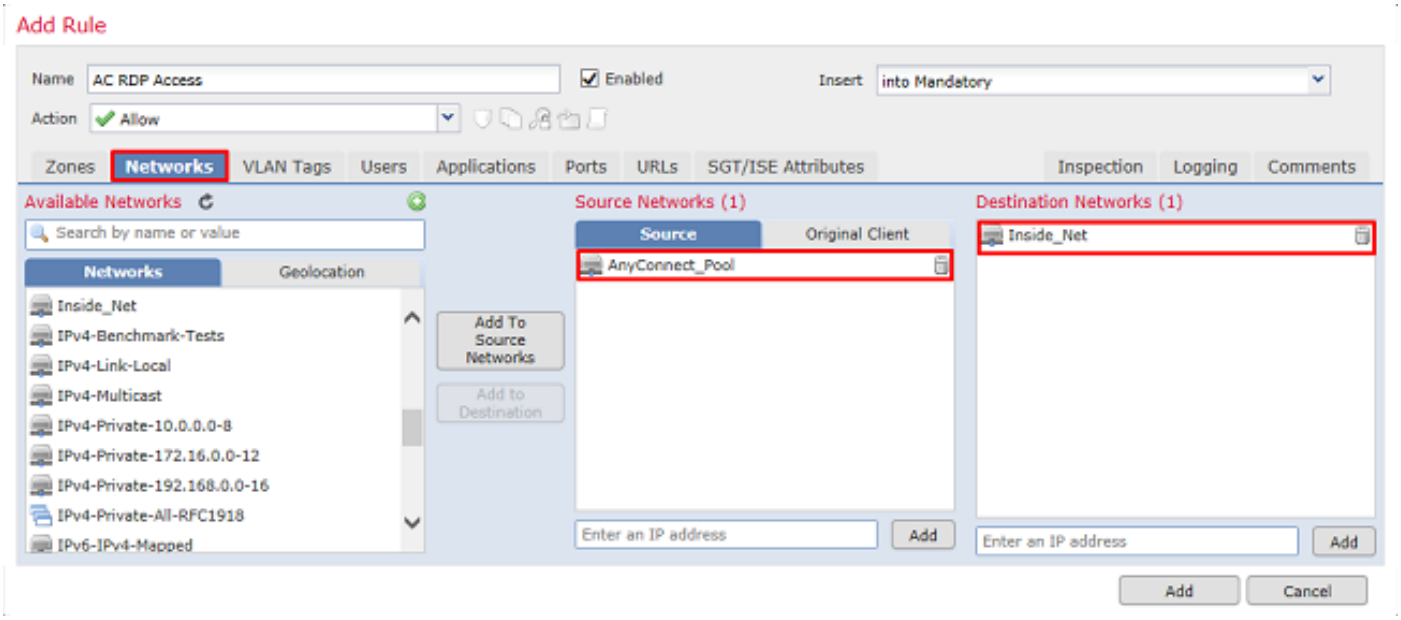
Le trafic RDP initié par les utilisateurs entre dans le FTD provenant de l'interface de zone externe et sort de la zone interne.



Sous **Networks**, définissez les réseaux source et de destination.

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

L'objet Inside_Net inclut le sous-réseau du réseau interne.

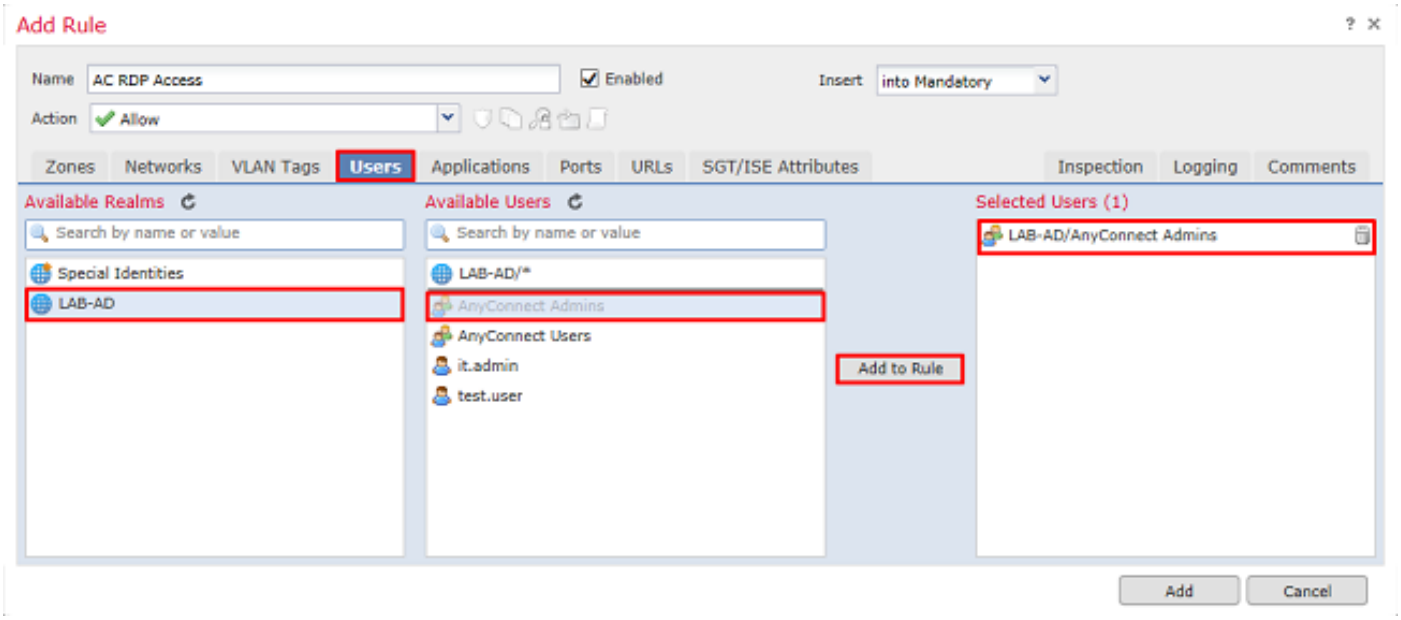


Sous **Utilisateurs**, cliquez sur le domaine créé précédemment sous **Domaines disponibles**, cliquez sur le groupe/utilisateur approprié sous **Utilisateurs disponibles**, puis cliquez sur **Ajouter à la règle**.

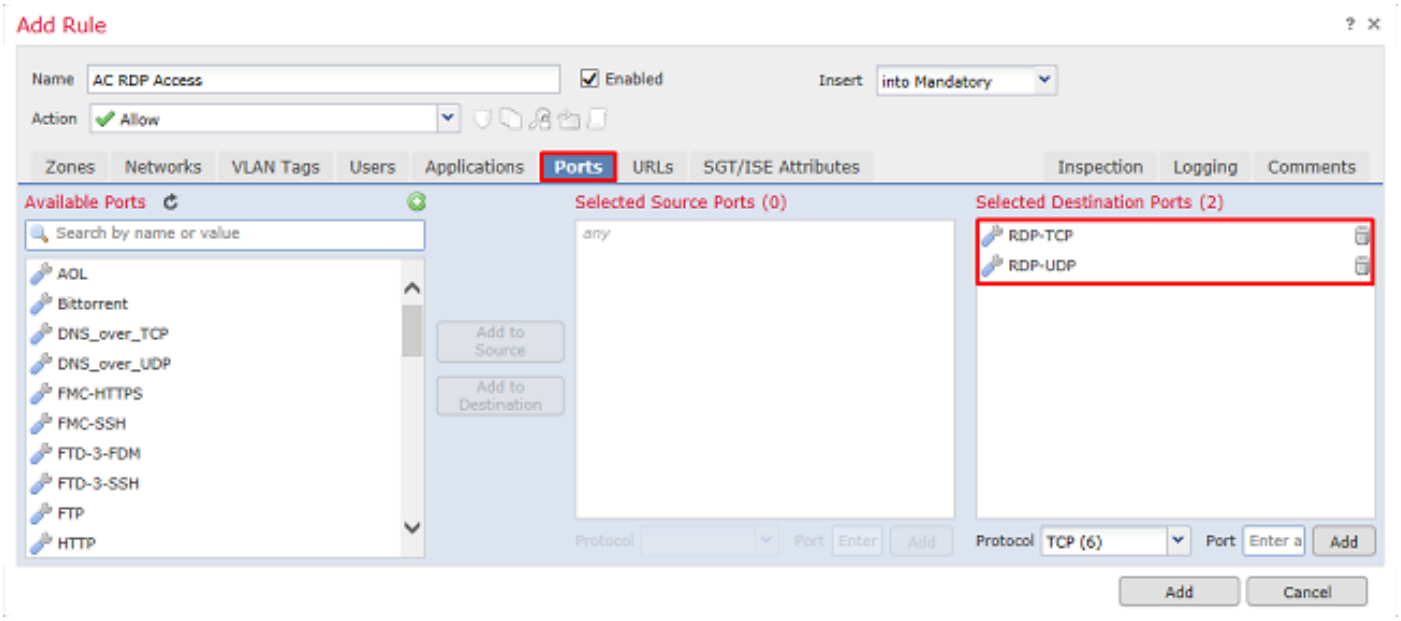
Si aucun utilisateur ou groupe n'est disponible dans la section **Utilisateurs disponibles**, assurez-vous que FMC a pu télécharger les **Utilisateurs** et les **Groupes** sous la section Domaine et que les **Groupes/Utilisateurs** appropriés sont inclus.

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

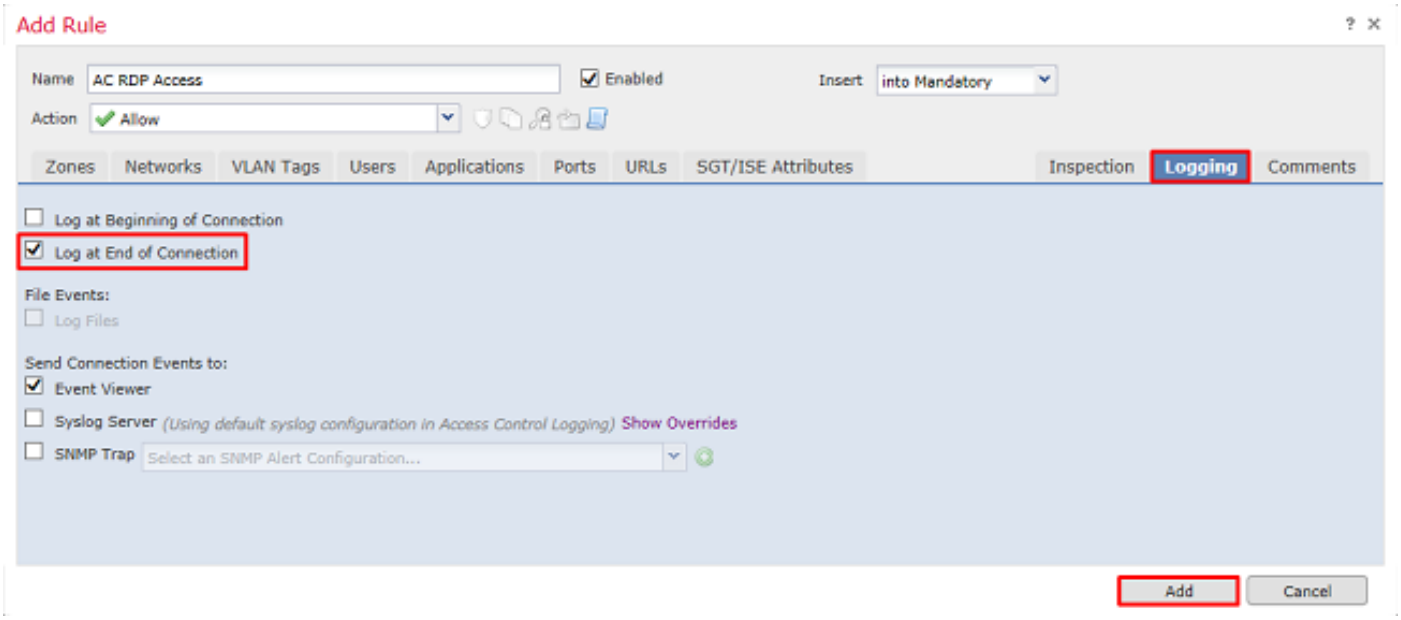
Par exemple, avec ce qui a été défini dans cette règle jusqu'à présent, le FTD évalue que le trafic provient de la zone externe et est destiné à la zone interne, provient du réseau dans l'objet AnyConnect_Pools et est destiné au réseau dans l'objet Inside_Net, et le trafic provient d'un utilisateur dans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



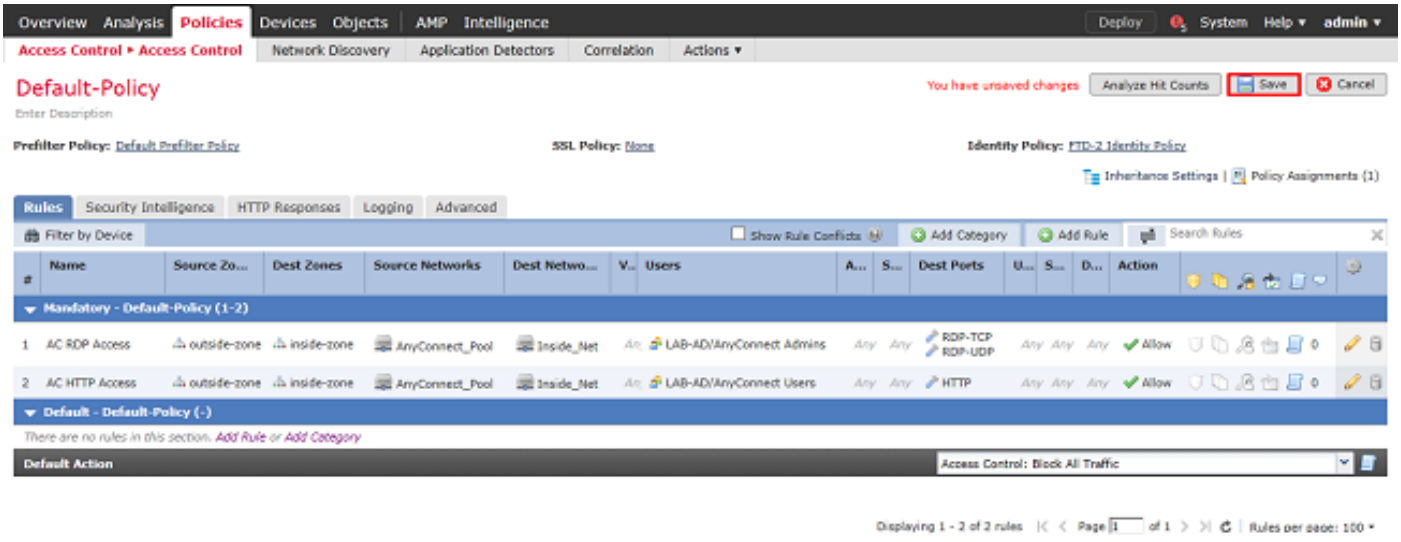
Sous Ports, des objets RDP personnalisés ont été créés et ajoutés pour autoriser les ports TCP et UDP 3389. Notez que le protocole RDP aurait pu être ajouté sous la section **Applications**, mais pour des raisons de simplicité, seuls les ports sont vérifiés.



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



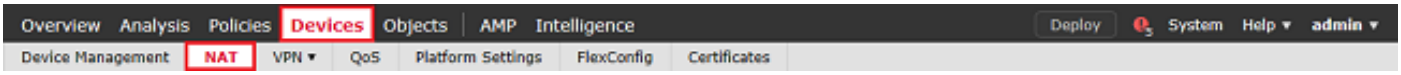
9. Une règle supplémentaire est créée pour l'accès HTTP afin de permettre aux utilisateurs du groupe **AnyConnect User d'**accéder au site Web **Windows Server IIS**. Cliquez sur **Save**.



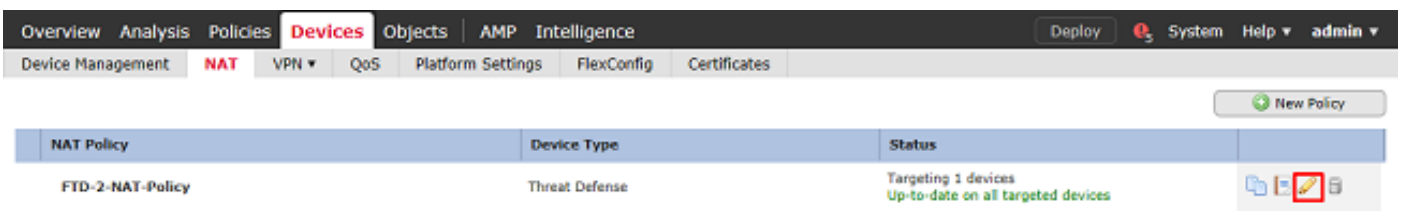
Configurer l'exemption NAT

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

1. Accédez à **Périphériques > NAT**.

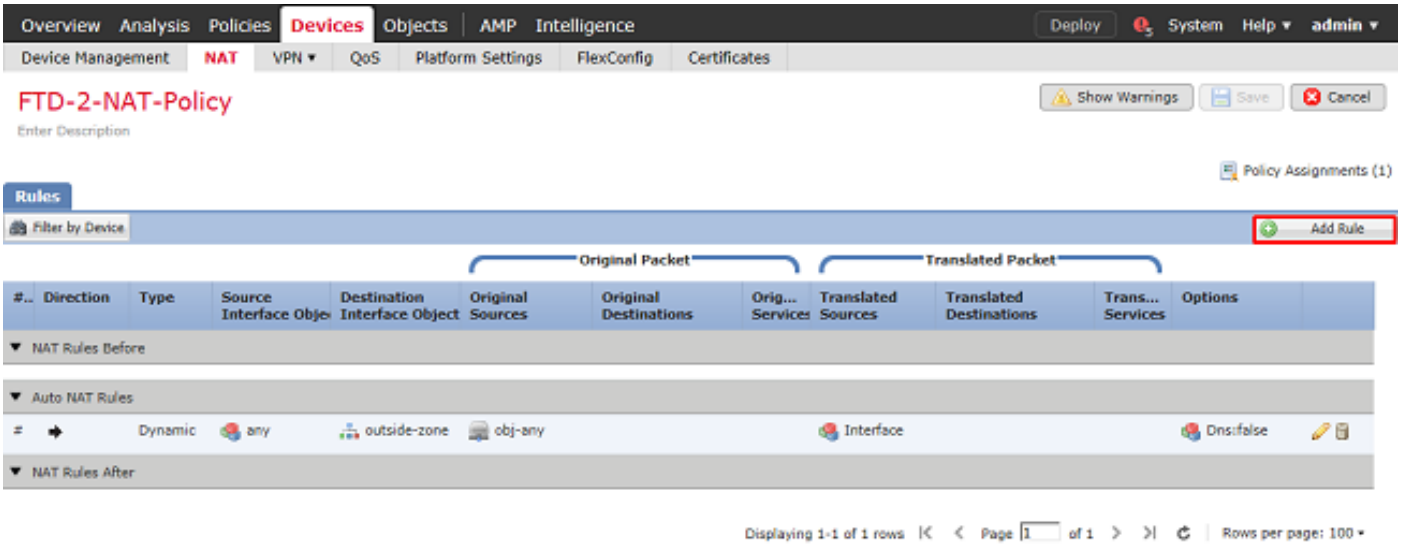


Sélectionnez la stratégie NAT appliquée au FTD.



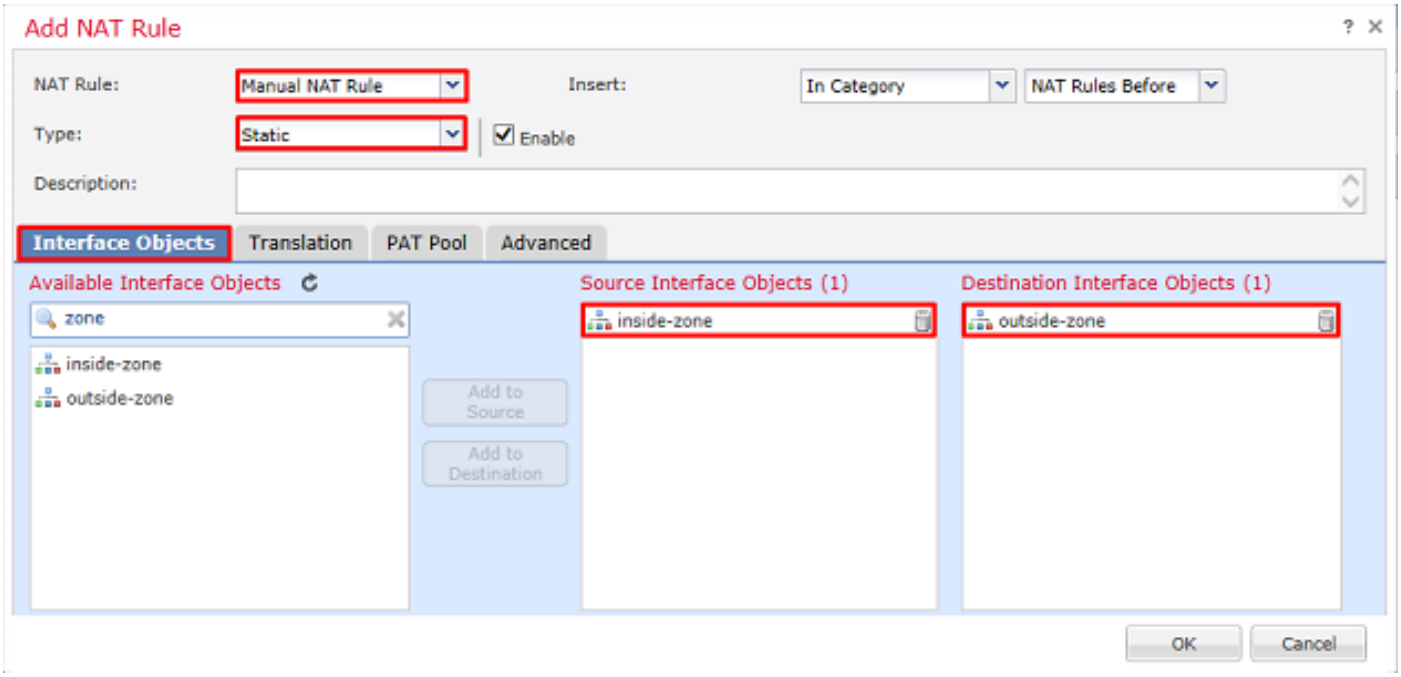
2. Dans cette stratégie NAT, il y a une PAT dynamique à la fin de laquelle la PAT affecte tout le trafic (y compris le trafic AnyConnect) sortant de l'interface externe vers l'interface externe.

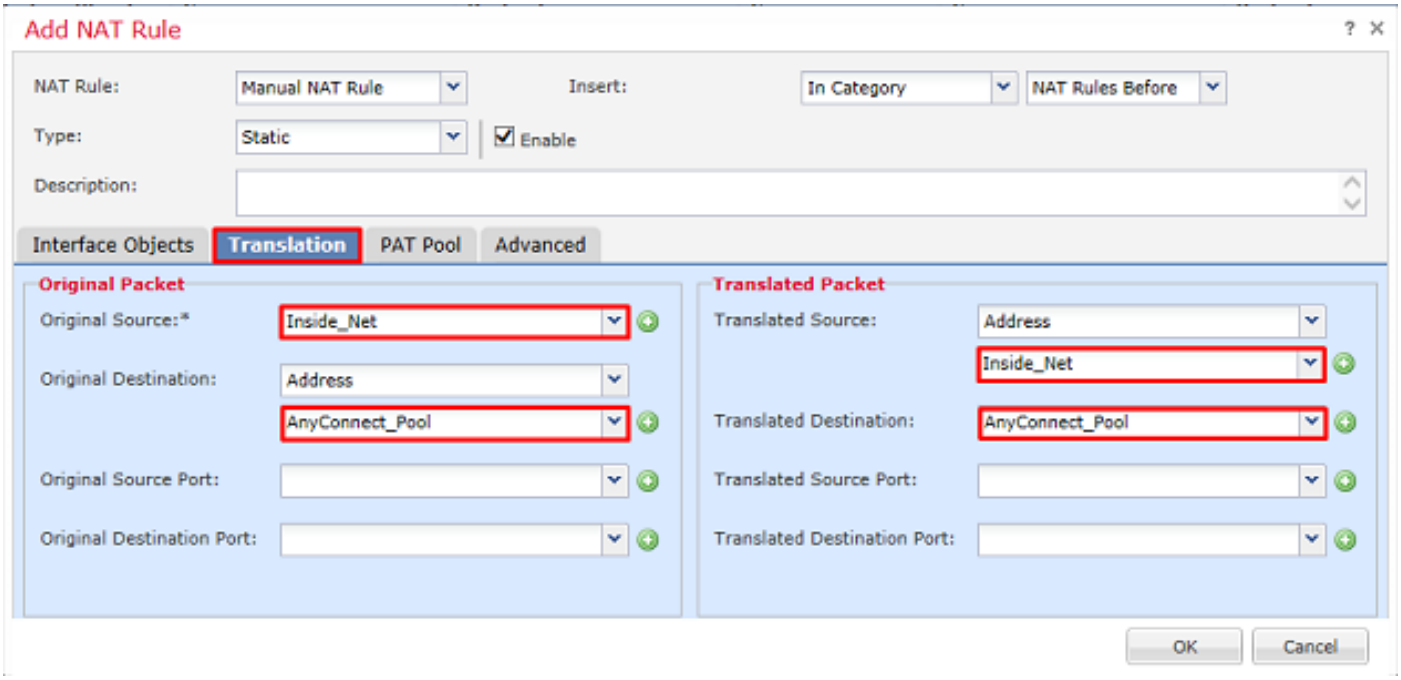
Pour empêcher que le trafic AnyConnect ne soit affecté par la NAT, cliquez sur **Add Rule** dans le coin supérieur droit.



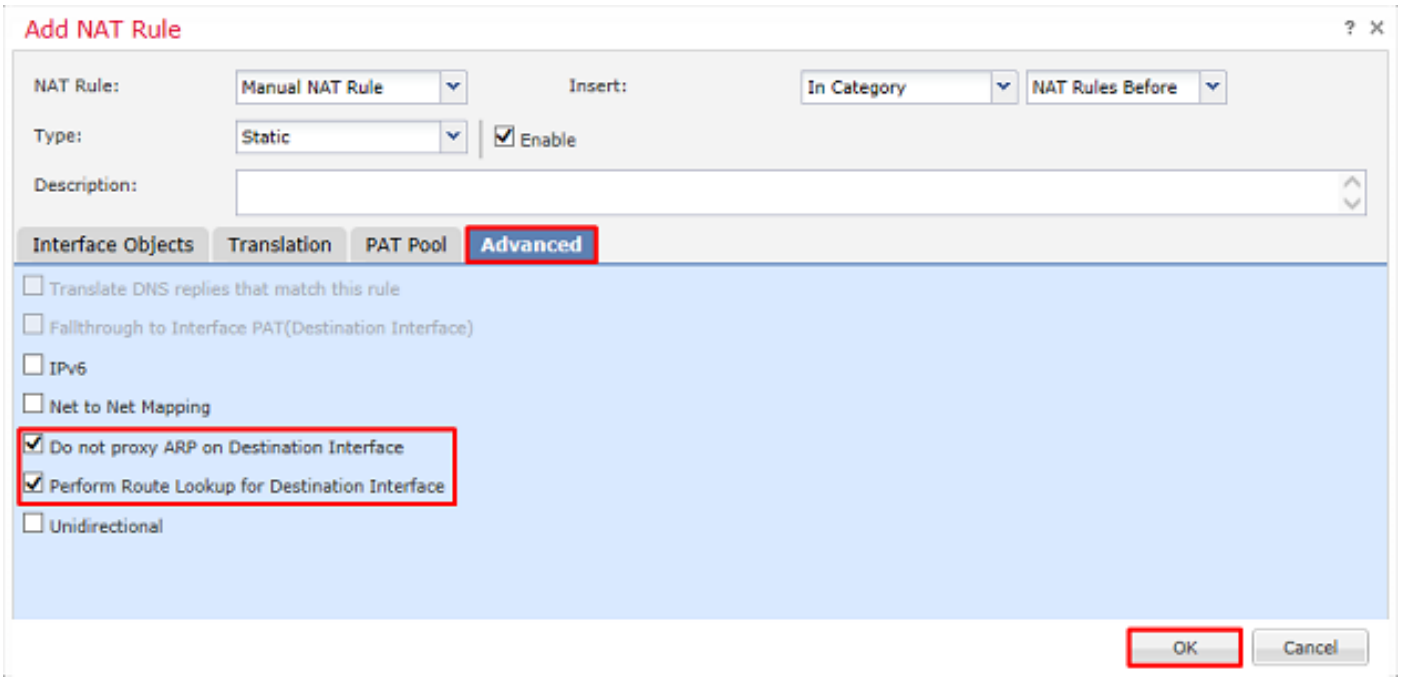
3. Configurez une règle d'exemption NAT, assurez-vous qu'il s'agit d'une règle NAT manuelle de type statique. Il s'agit d'une règle NAT bidirectionnelle qui s'applique au trafic AnyConnect.

Avec ces paramètres, lorsque le FTD détecte le trafic provenant de Inside_Net et destiné à l'adresse IP AnyConnect (définie par AnyConnect_Pool), la source est traduite en la même valeur (Inside_Net) et la destination est traduite en la même valeur (AnyConnect_Pool) lorsque le trafic entre dans la zone inside_zone et sort de la zone outside_zone. Cela contourne essentiellement la NAT lorsque ces conditions sont remplies.

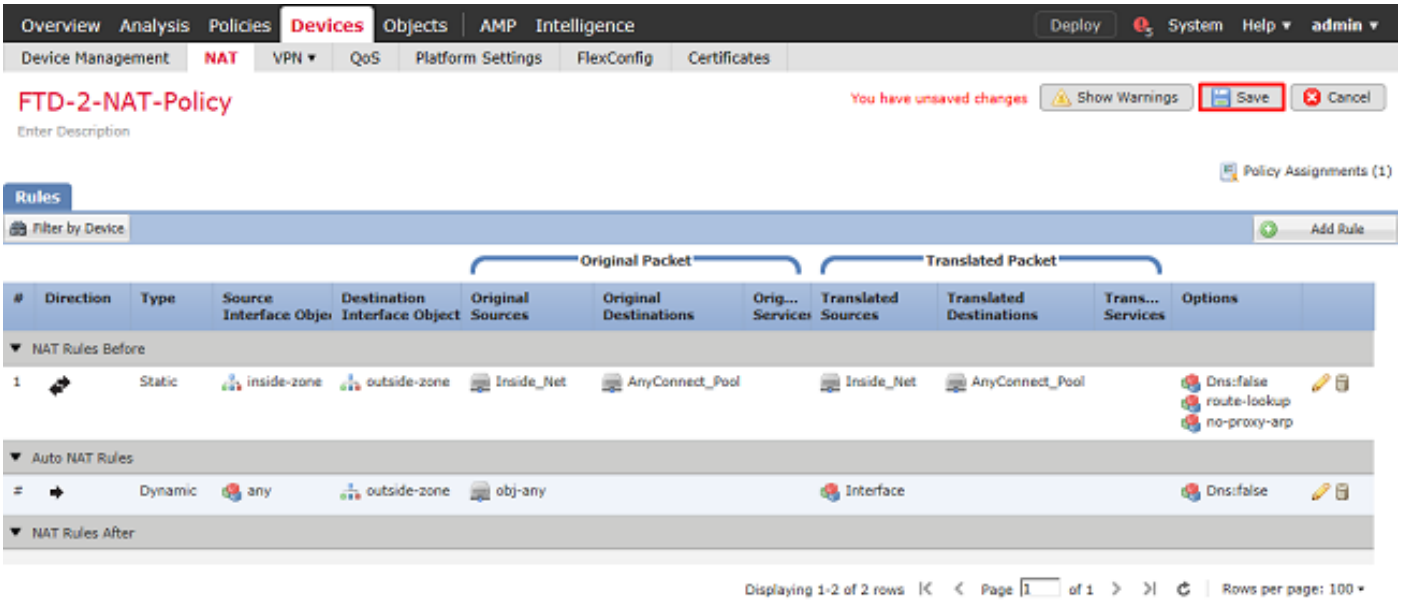




En outre, le FTD est configuré pour effectuer une recherche de route sur ce trafic et non pas le proxy ARP. Cliquez sur **OK** lorsque vous avez terminé.

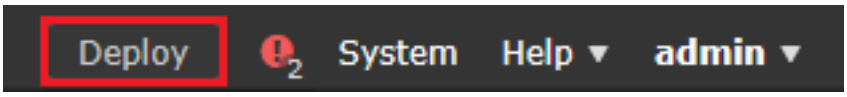


4. Cliquez sur **Enregistrer**.

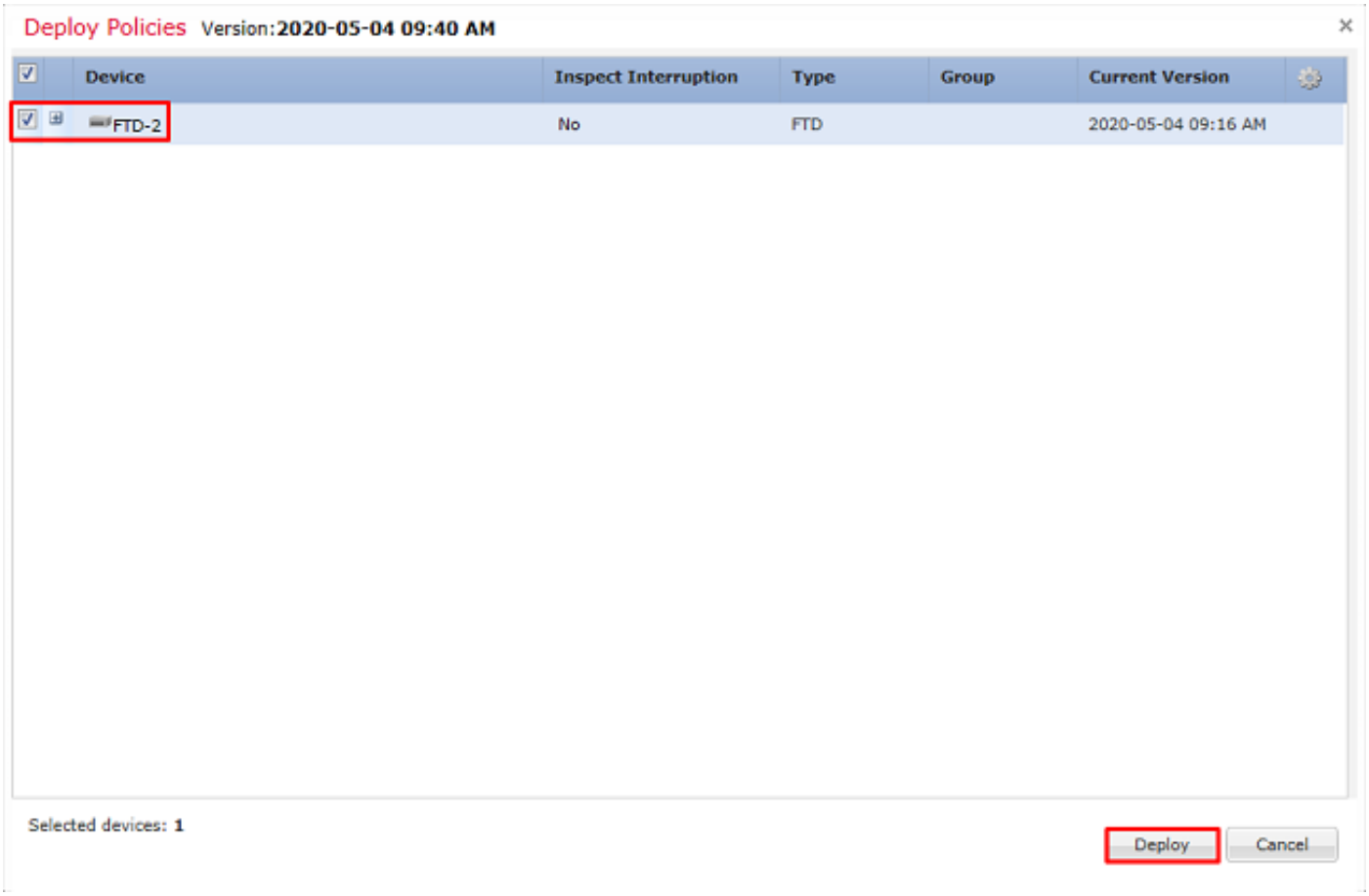


Déploiement

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



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



Vérifier

Configuration finale

Configuration AAA

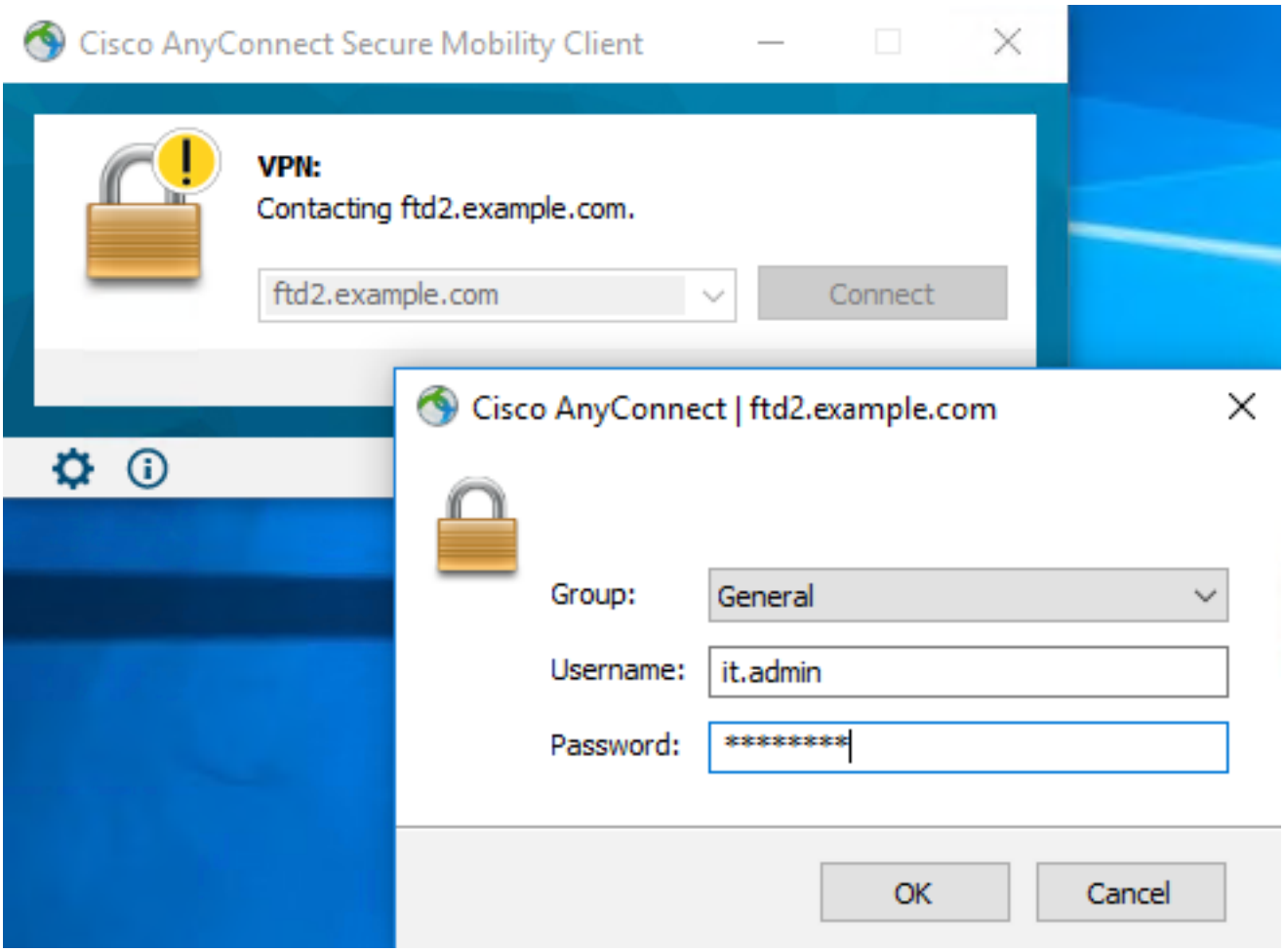
```
> show running-configuration aaa-server
aaa-server LAB-AD protocol ldap
 max-failed-attempts 4
 realm-id 5
aaa-server LAB-AD host win2016.example.com
 server-port 389
 ldap-base-dn DC=example,DC=com
 ldap-group-base-dn DC=example,DC=com
 ldap-scope subtree
 ldap-naming-attribute samaccountname
 ldap-login-password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

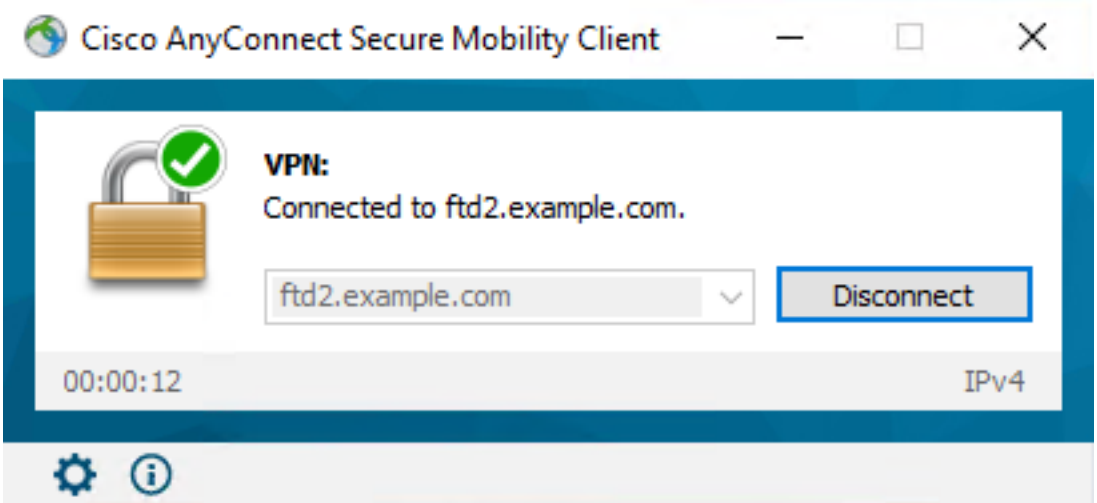
Configuration AnyConnect

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

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

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

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

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

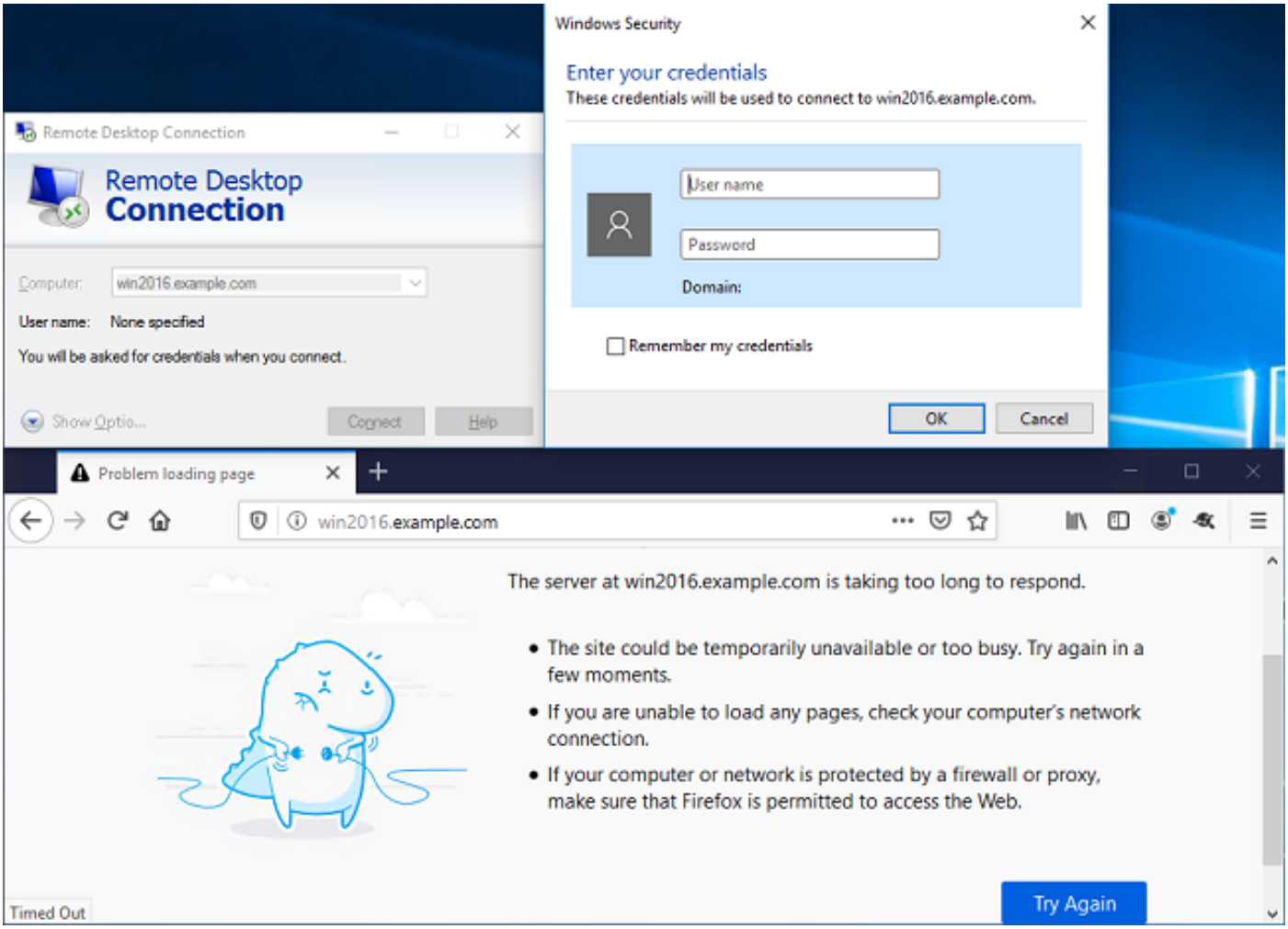
Connexion à AnyConnect et vérification des règles de stratégie de contrôle d'accès



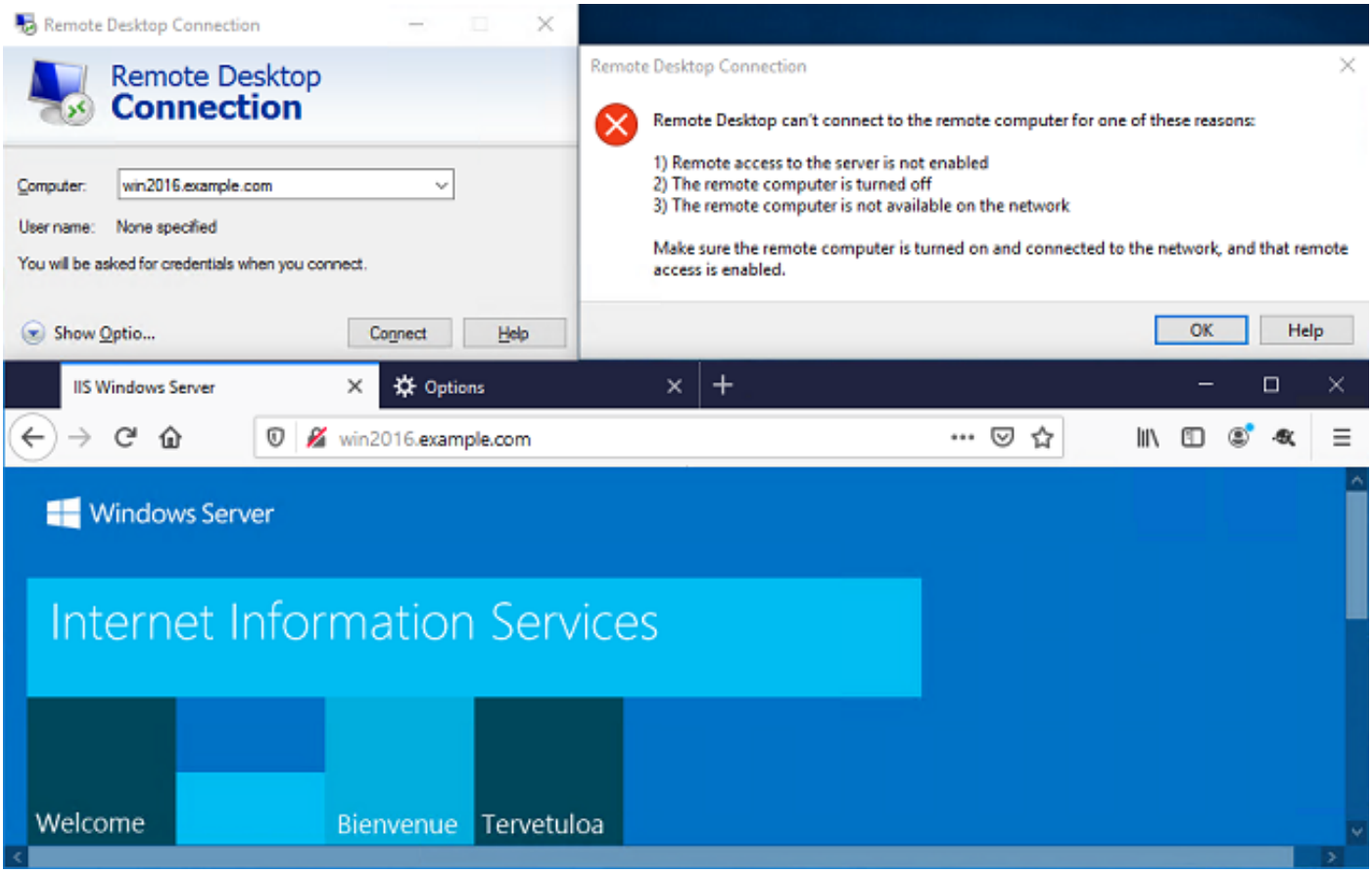


L'utilisateur IT Admin fait partie du groupe AnyConnect Admins qui a un accès RDP au serveur Windows, mais n'a pas accès à HTTP.

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



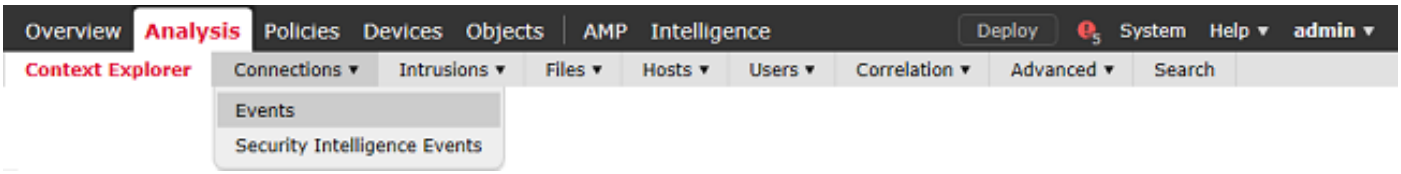
Si vous êtes connecté avec l'utilisateur Utilisateur test qui fait partie du groupe Utilisateurs AnyConnect disposant d'un accès HTTP mais pas d'un accès RDP, nous pouvons vérifier que les règles de stratégie de contrôle d'accès prennent effet.



Vérifier avec les événements de connexion FMC

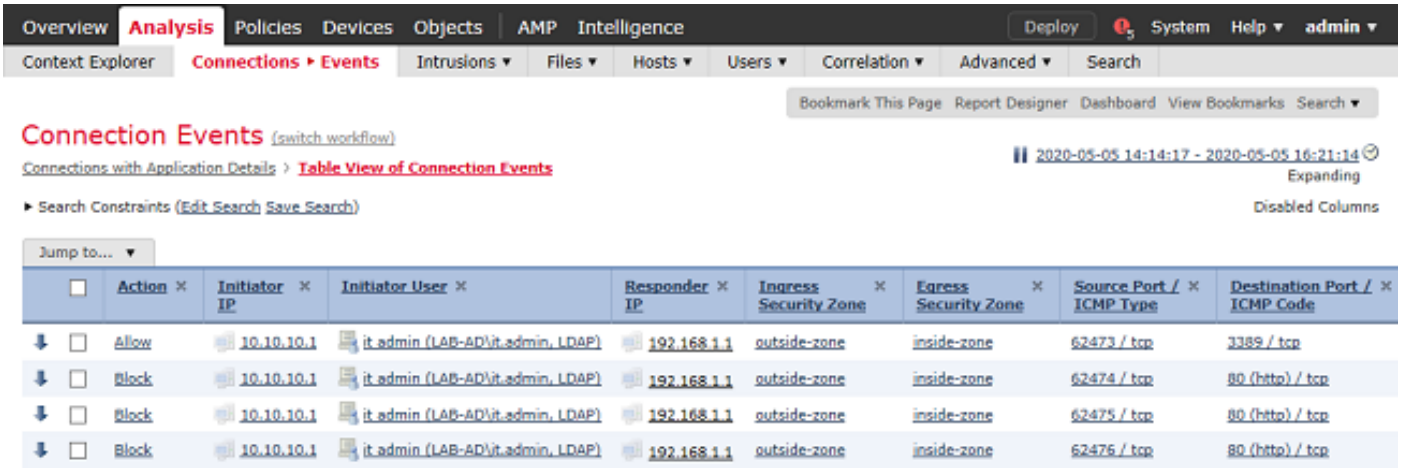
Comme la journalisation a été activée dans les règles de stratégie de contrôle d'accès, les événements de connexion peuvent être vérifiés pour tout trafic correspondant à ces règles

Accédez à **Analysis > Connections > Events**.

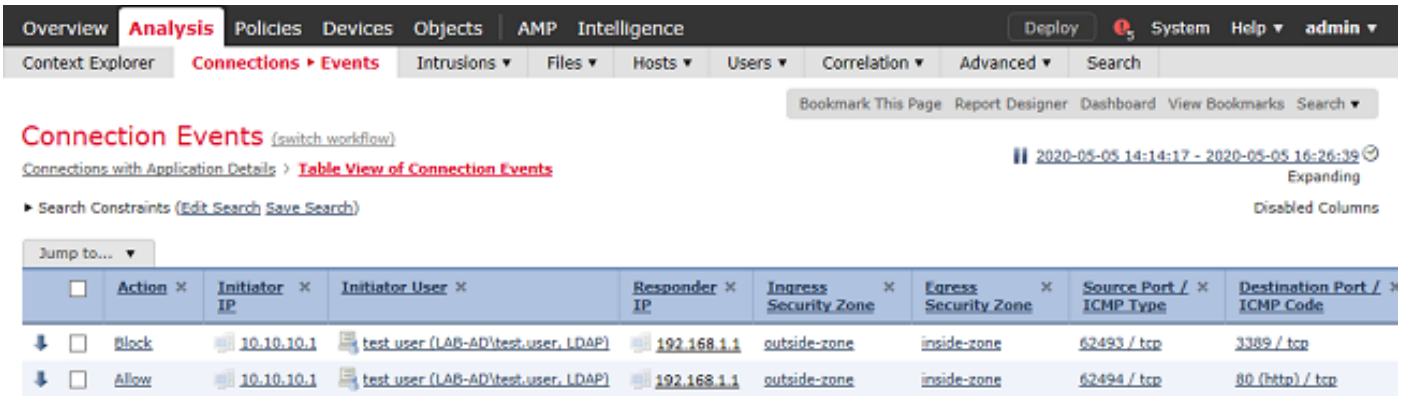


Dans la **vue Tableau des événements de connexion**, les journaux sont filtrés pour afficher uniquement les événements de connexion pour l'administrateur informatique.

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



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



Dépannage

Déboguages

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

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

Débogages LDAP en cours

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

```
        Filter  = [sAMAccountName=it.admin]
        Scope   = [SUBTREE]
[53] User DN = [CN=IT Admin,CN=Users,DC=example,DC=com]
[53] Talking to Active Directory server 192.168.1.1
[53] Reading password policy for it.admin, dn:CN=IT Admin,CN=Users,DC=example,DC=com
[53] Read bad password count 6
[53] Binding as it.admin
[53] Performing Simple authentication for it.admin to 192.168.1.1
[53] Processing LDAP response for user it.admin
[53] Message (it.admin):
[53] Authentication successful for it.admin to 192.168.1.1
[53] Retrieved User Attributes:
[53]    objectClass: value = top
[53]    objectClass: value = person
[53]    objectClass: value = organizationalPerson
[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...;.....j...
[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
```

Impossible d'établir une connexion avec le serveur LDAP

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

Solutions potentielles :

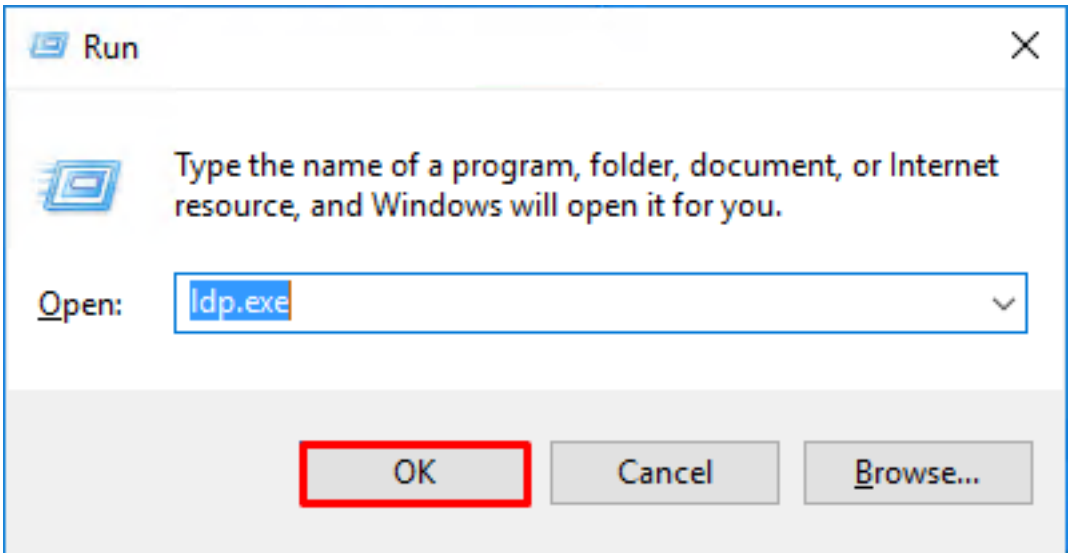
- Vérifiez le routage et assurez-vous que le FTD reçoit une réponse du serveur LDAP.
- Si LDAPS ou STARTTLS est utilisé, assurez-vous que le certificat d'autorité de certification racine correct est approuvé afin que la connexion SSL puisse s'effectuer correctement.
- Vérifiez que l'adresse IP et le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

DN et/ou mot de passe de connexion incorrects

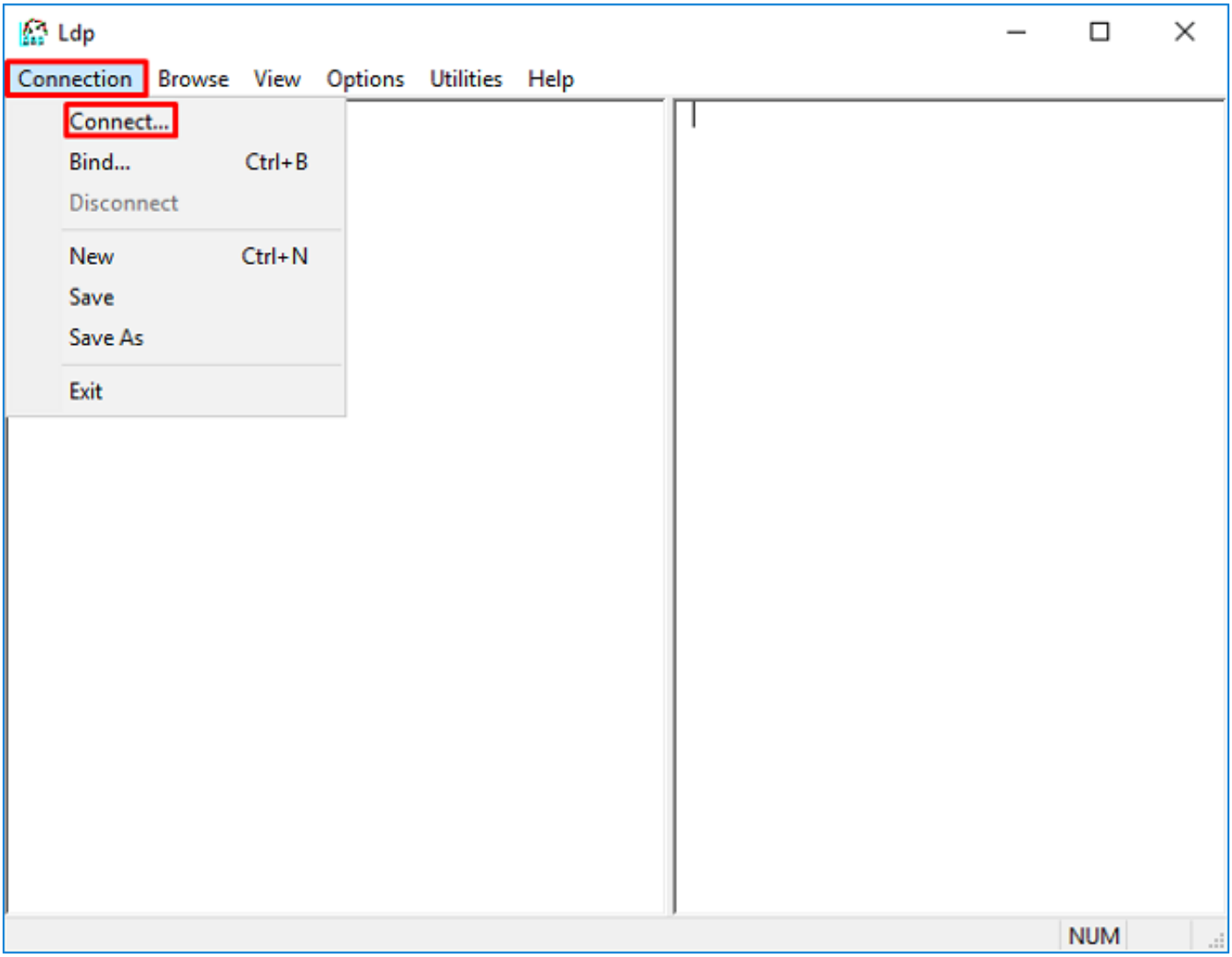
```
[-2147483615] Session Start
[-2147483615] New request Session, context 0x00007f9e65ccdc40, reqType = Authentication
[-2147483615] Fiber started
[-2147483615] Creating LDAP context with uri=ldap://192.168.1.1:389
[-2147483615] Connect to LDAP server: ldap://192.168.1.1:389, status = Successful
[-2147483615]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

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

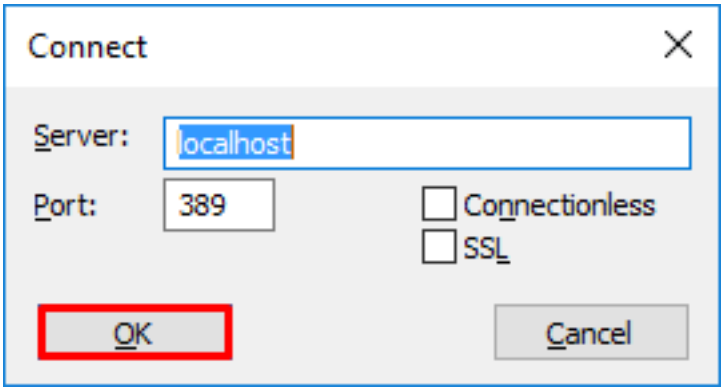
1. Sur le serveur AD, appuyez sur **Win+R** et recherchez **ldp.exe**



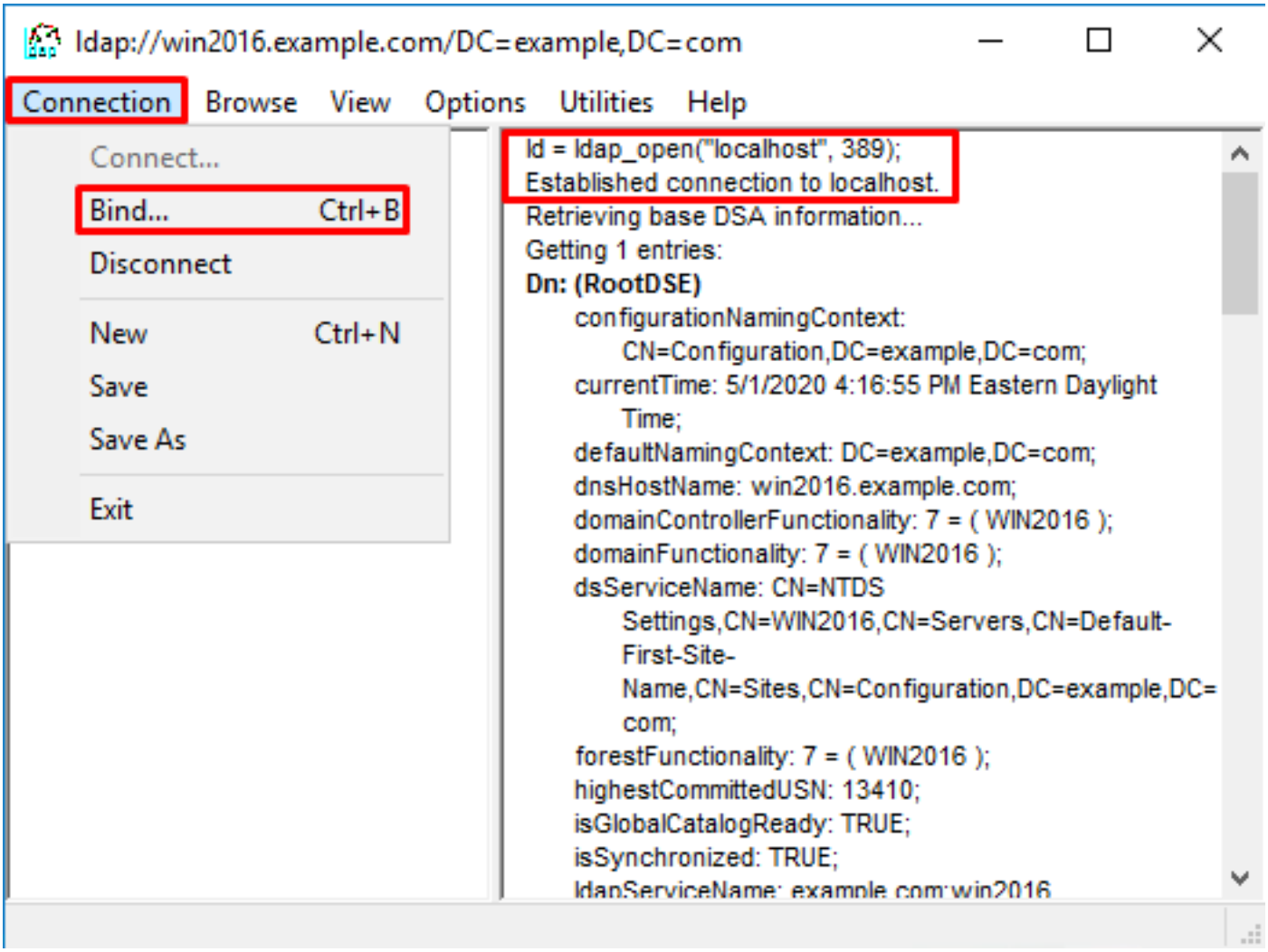
2. Sous **Connexion**, choisissez **Connecter...**



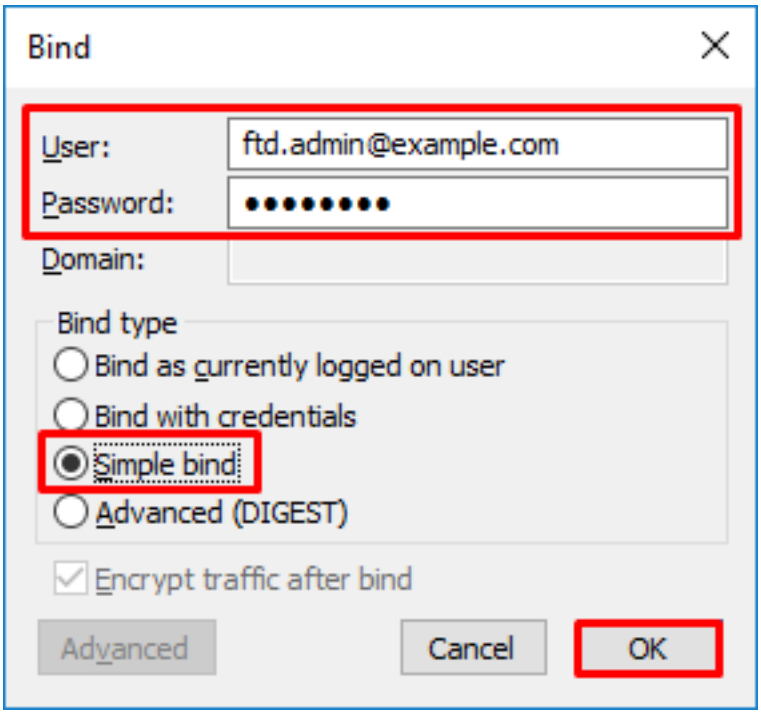
3. Spécifiez localhost pour le serveur et le port approprié, puis cliquez sur **OK**.



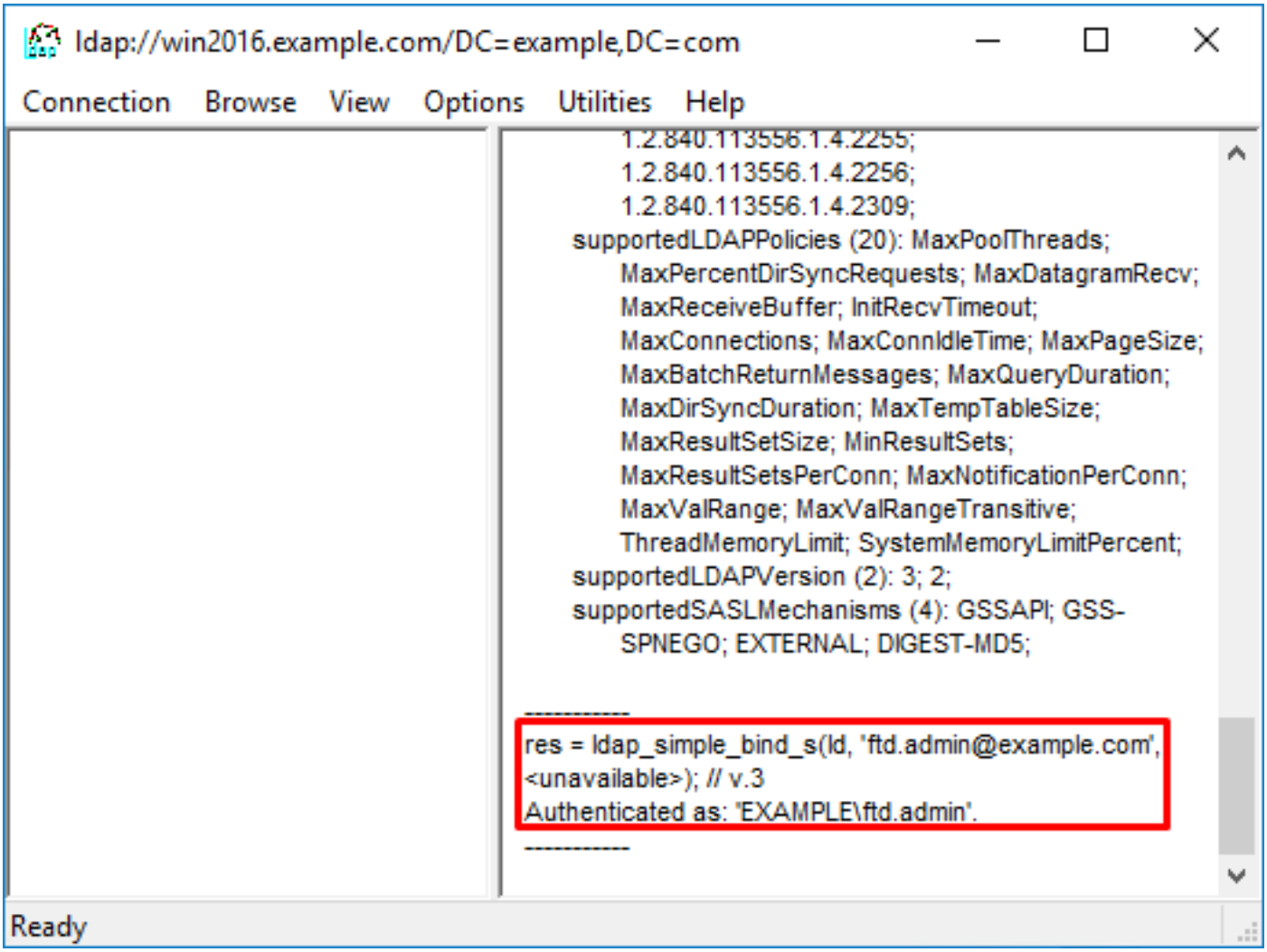
4. La colonne de droite affiche du texte indiquant une connexion réussie. Accédez à **Connexion > Lier...**



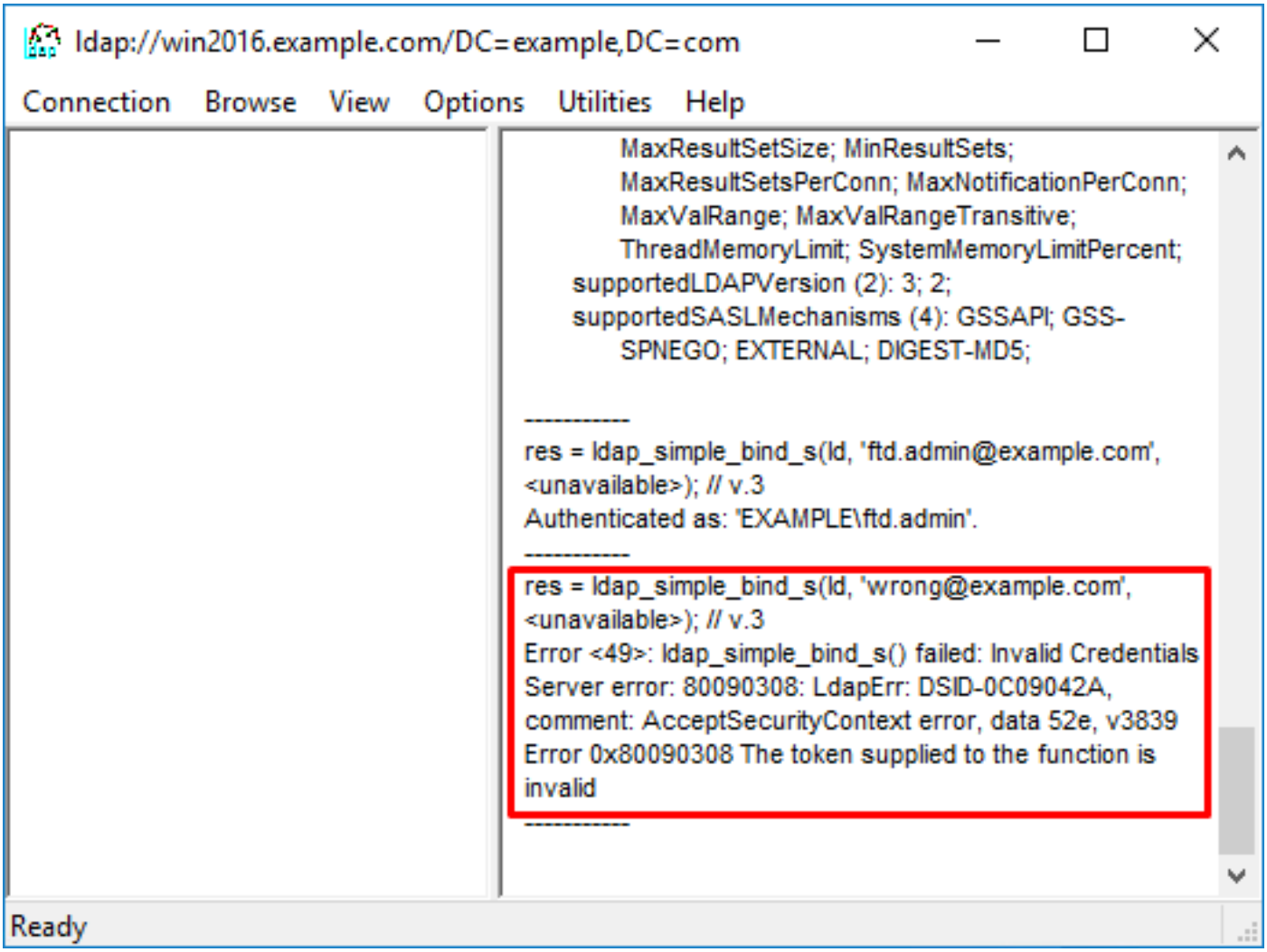
5. Sélectionnez **Simple Bind**, puis spécifiez le **nom d'utilisateur** et le mot de **passe** du **compte d'annuaire**. Click OK.



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



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

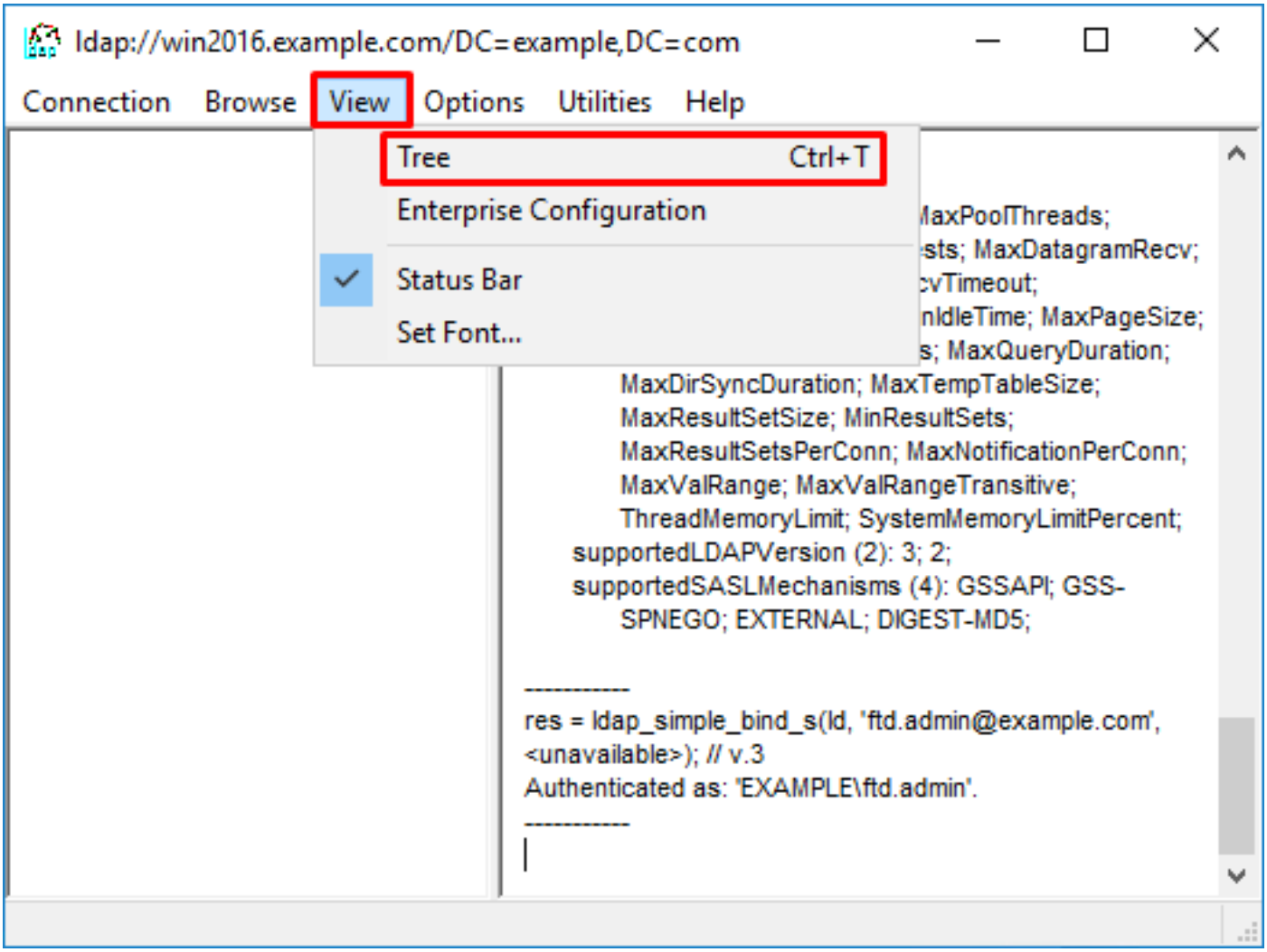


Le serveur LDAP ne trouve pas le nom d'utilisateur

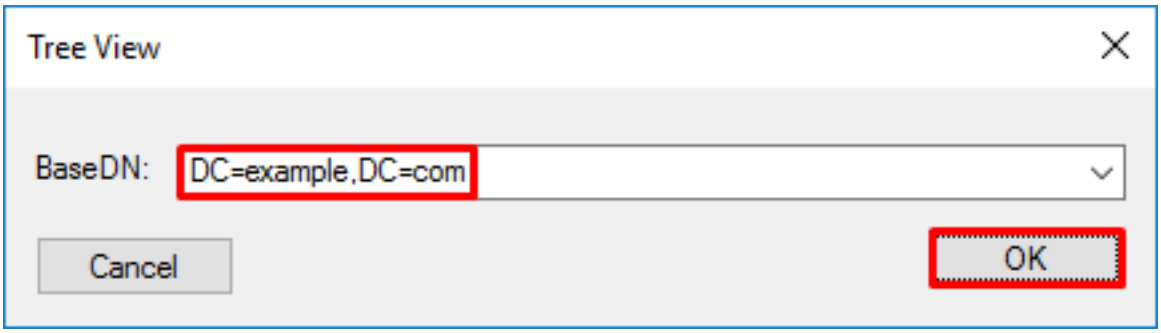
```
[-2147483612] Session Start
[-2147483612] New request Session, context 0x00007f9e65ccdc40, reqType = Authentication
[-2147483612] Fiber started
[-2147483612] Creating LDAP context with uri=ldap://192.168.1.1:389
[-2147483612] Connect to LDAP server: ldap://192.168.1.1:389, status = Successful
[-2147483612]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

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

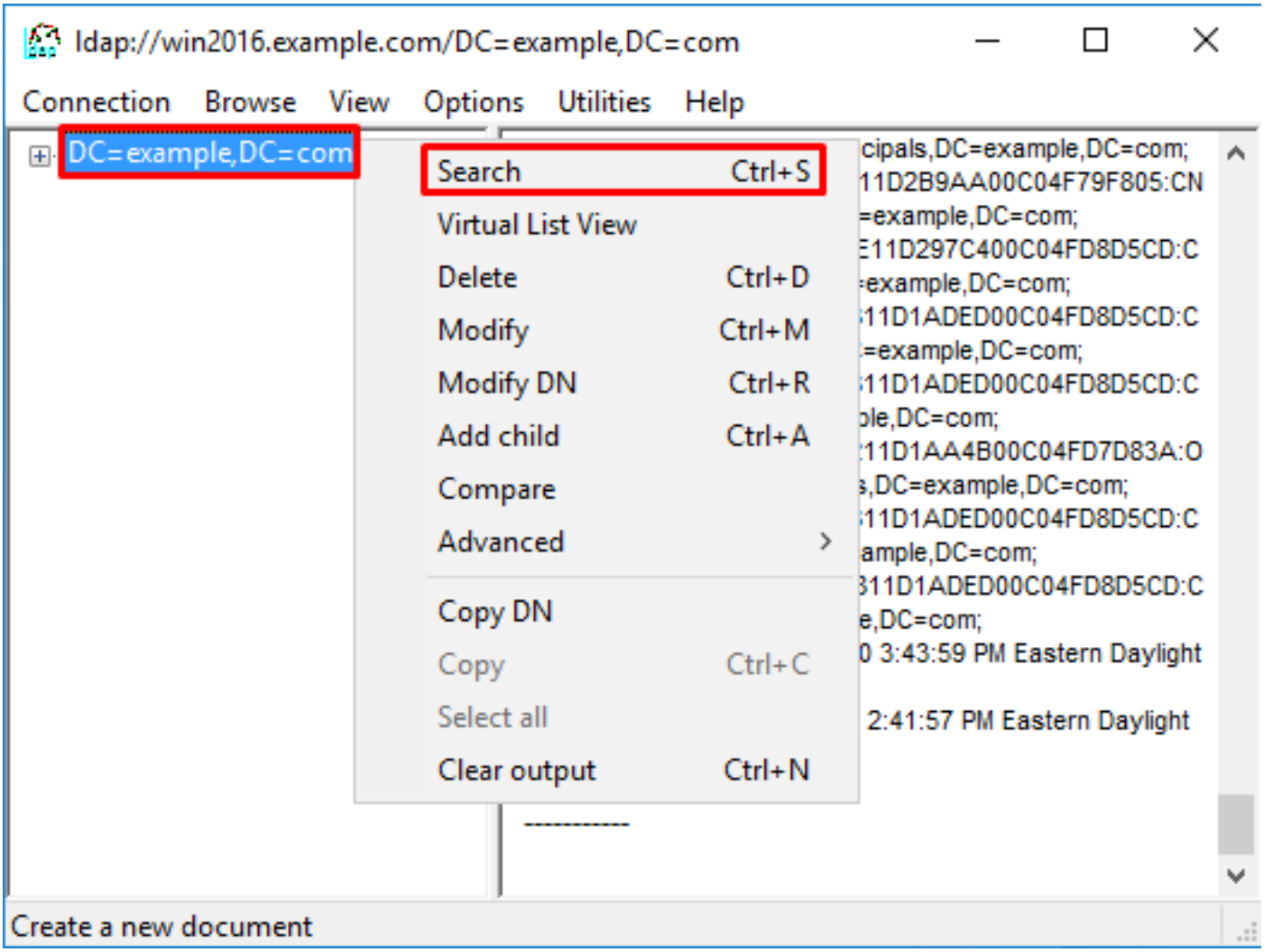
1. Après avoir réussi la liaison comme vu ci-dessus, naviguez à **Affichage > Arborescence**.



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



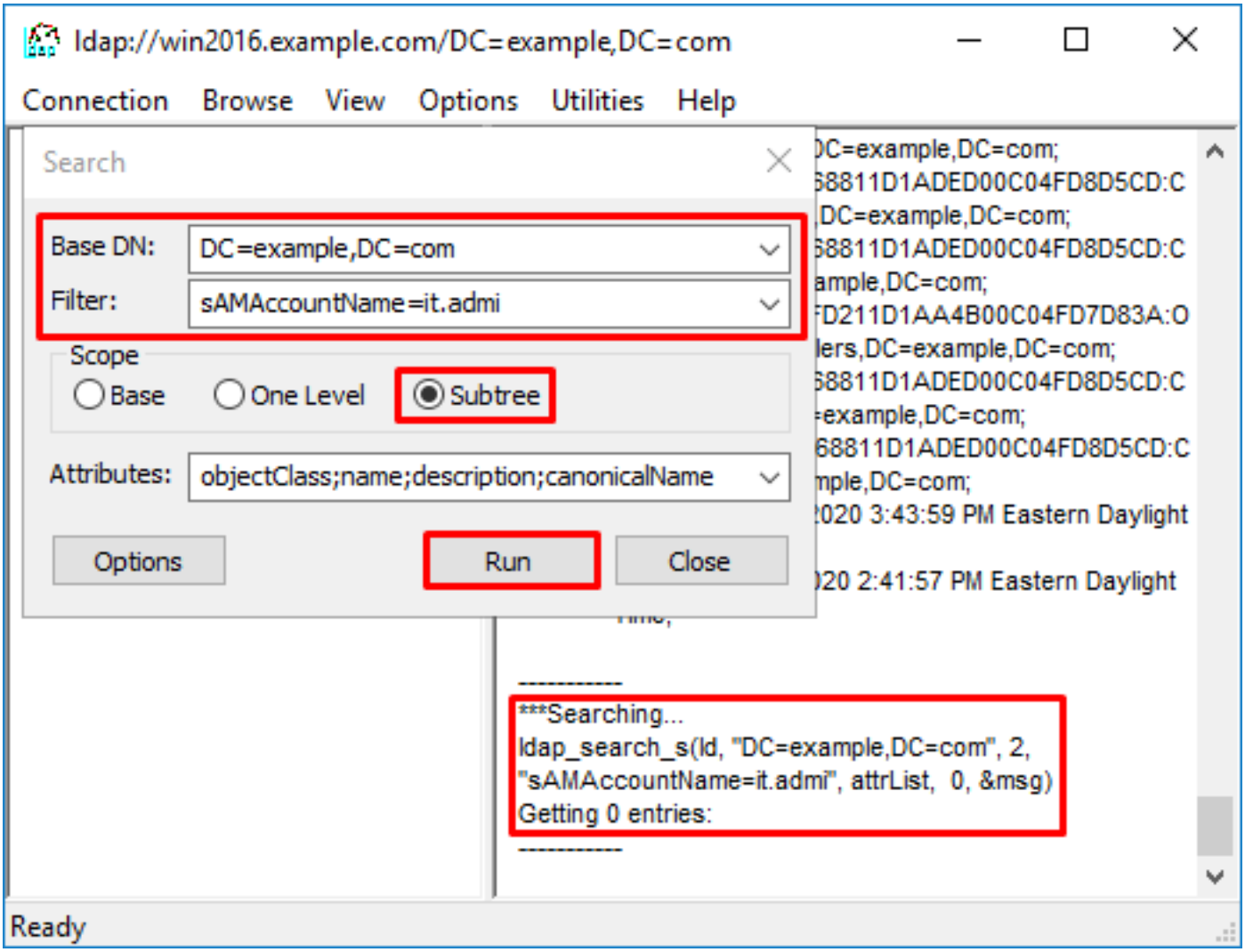
3. Cliquez avec le bouton droit sur le DN de base, puis cliquez sur **Rechercher**.



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

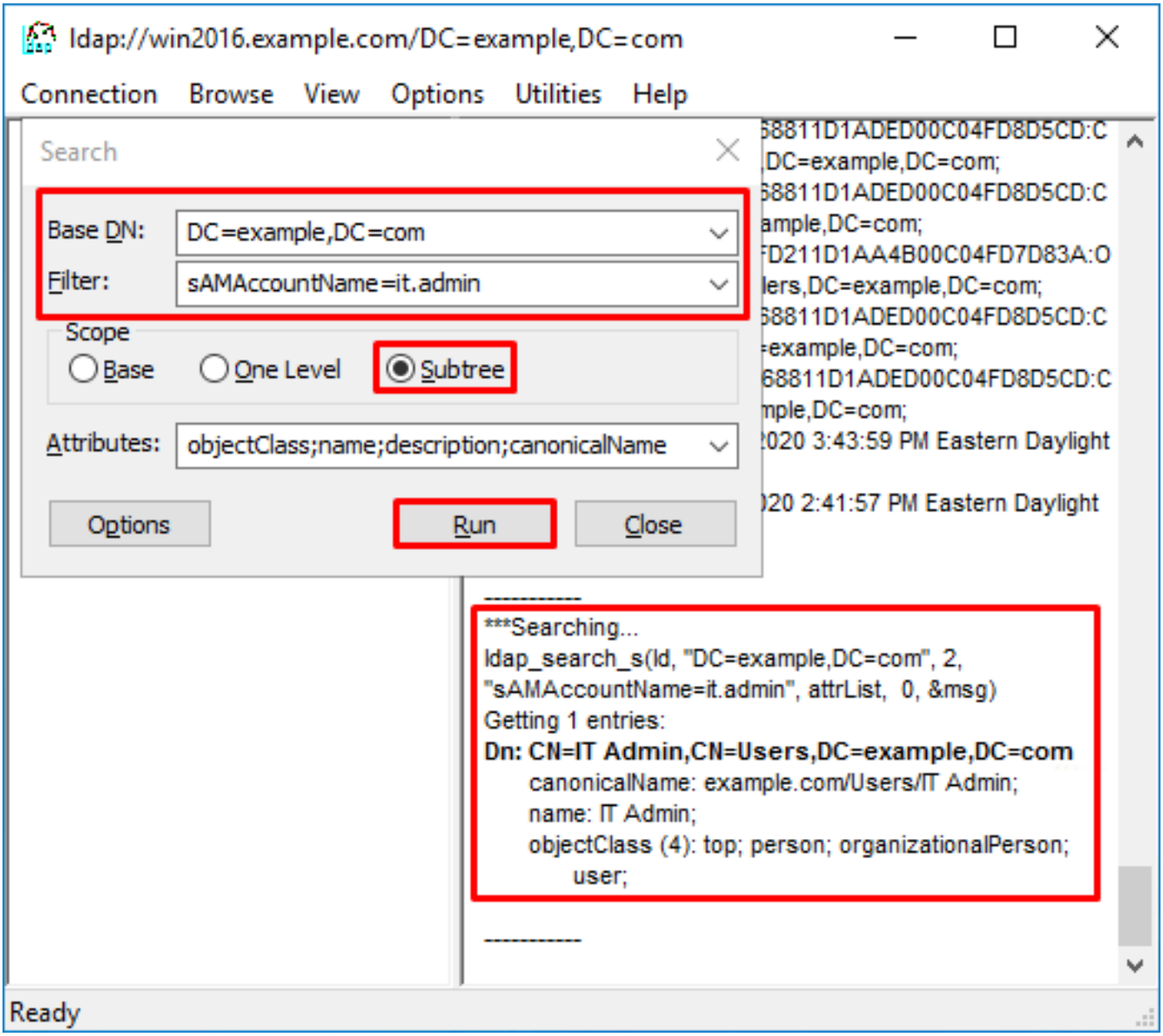
Dans cet exemple, il s'agit des éléments suivants :

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



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

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



Mot de passe incorrect pour le nom d'utilisateur

```
[-2147483613] Session Start
[-2147483613] New request Session, context 0x00007f9e65ccdc40, reqType = Authentication
[-2147483613] Fiber started
[-2147483613] Creating LDAP context with uri=ldap://192.168.1.1:389
[-2147483613] Connect to LDAP server: ldap://192.168.1.1:389, status = Successful
[-2147483613] supportedLDAPVersion: value = 3
[-2147483613] supportedLDAPVersion: value = 2
[-2147483613] LDAP server 192.168.1.1 is Active directory
[-2147483613] Binding as ftd.admin@example.com
[-2147483613] Performing Simple authentication for ftd.admin@example.com to 192.168.1.1
[-2147483613] LDAP Search:
        Base DN = [dc=example,dc=com]
        Filter  = [samaccountname=it.admin]
        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
```

Solution potentielle : vérifiez que le mot de passe utilisateur est configuré correctement et qu'il n'a pas expiré. Tout comme le DN de connexion, le FTD effectue une liaison avec AD avec les informations d'identification de l'utilisateur.

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

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

Test AAA

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

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

> test aaa-server authentication LAB-AD host win2016.example.com
Username: it.admin
Password: ********
INFO: Attempting Authentication test to IP address (192.168.1.1) (timeout: 12 seconds)
INFO: Authentication Successful
```

Captures de paquets

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

La capture montre le trafic LDAP bidirectionnel.

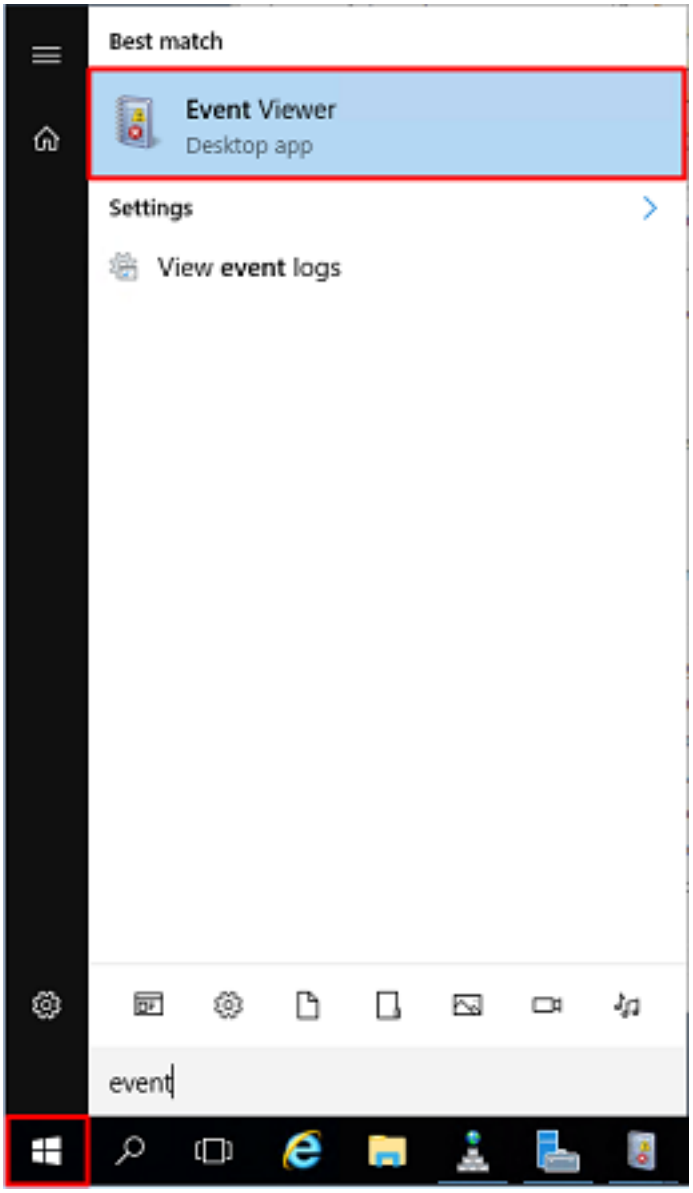
```
> show route 192.168.1.1

Routing entry for 192.168.1.0 255.255.255.0
  Known via "connected", distance 0, metric 0 (connected, via interface)
```

```
  Routing Descriptor Blocks:
  * directly connected, via inside
      Route metric is 0, traffic share count is 1

> capture AD interface inside match tcp any host 192.168.1.1 eq 389

> show capture
capture AD type raw-data interface inside [Capturing - 0 bytes]
  match tcp any host 192.168.1.1 eq ldap

> test aaa-server authentication LAB-AD host win2016.example.com username it.admin password
******
INFO: Attempting Authentication test to IP address (192.168.1.1) (timeout: 12 seconds)
INFO: Authentication Successful

> show capture
capture AD type raw-data interface inside [Capturing - 10905 bytes]
  match tcp any host 192.168.1.1 eq ldap

> show capture AD

54 packets captured

   1: 23:02:16.770712       192.168.1.17.61960 > 192.168.1.1.389: S 3681912834:3681912834(0) win
32768 <mss 1460,nop,nop,timestamp 1061373057 0>
   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
```

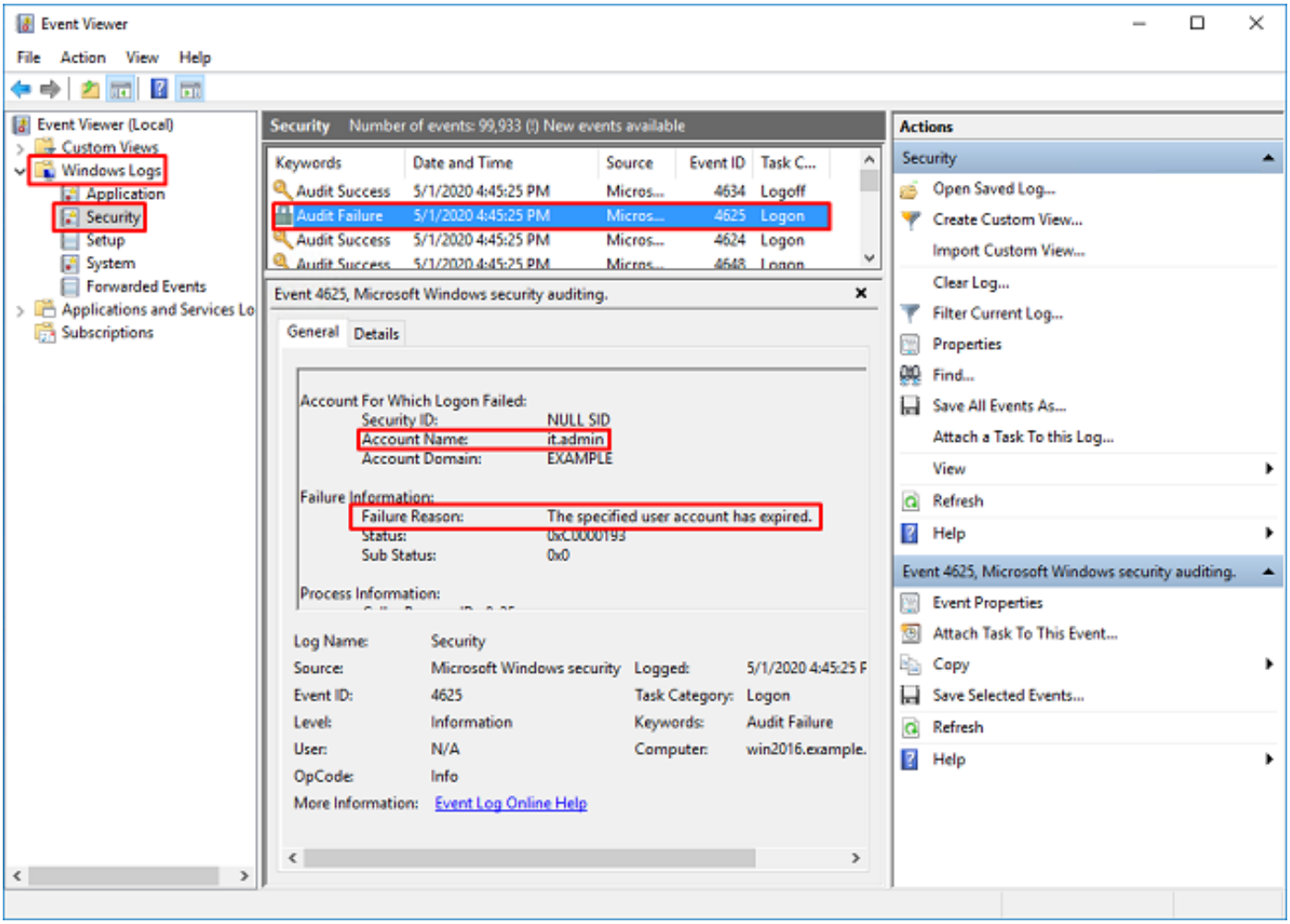
Journaux de l'Observateur d'événements Windows Server

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

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



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



An account failed to log on.

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

Logon Type:3

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

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

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

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

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.