Configurer l'authentification AD (LDAP) et l'identité de l'utilisateur sur FTD géré par FDM pour les clients AnyConnect

Contenu

Introduction

L'objectif de ce document est de détailler comment configurer l'authentification Active Directory (AD) pour les clients AnyConnect qui se connectent à un système Cisco Firepower Threat Defense (FTD) géré par Firepower Device Management (FDM). L'identité de l'utilisateur sera utilisée dans les stratégies d'accès afin de restreindre les utilisateurs AnyConnect à des adresses IP et des ports spécifiques.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissance de base de la configuration VPN RA sur FDM
- Connaissance de base de la configuration du serveur LDAP sur FDM
- Connaissances de base en AD

Components Used

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

- Serveur Microsoft 2016
- FTDv exécutant 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.

Configuration

Schéma et scénario du réseau

Le serveur Windows est préconfiguré avec Internet Information Services (IIS) et Remote Desktop Protocol (RDP) afin de tester l'identité de l'utilisateur. Dans ce guide de configuration, trois comptes d'utilisateurs et deux groupes seront créés.

Comptes d'utilisateurs :

- Admin FTD : Ce compte sera utilisé comme compte de répertoire afin de permettre au FTD de se lier au serveur AD.
- Administrateur informatique : Compte administrateur de test utilisé pour démontrer l'identité de l'utilisateur.
- Utilisateur test : Compte utilisateur de test utilisé pour démontrer l'identité de l'utilisateur.

Groupes :

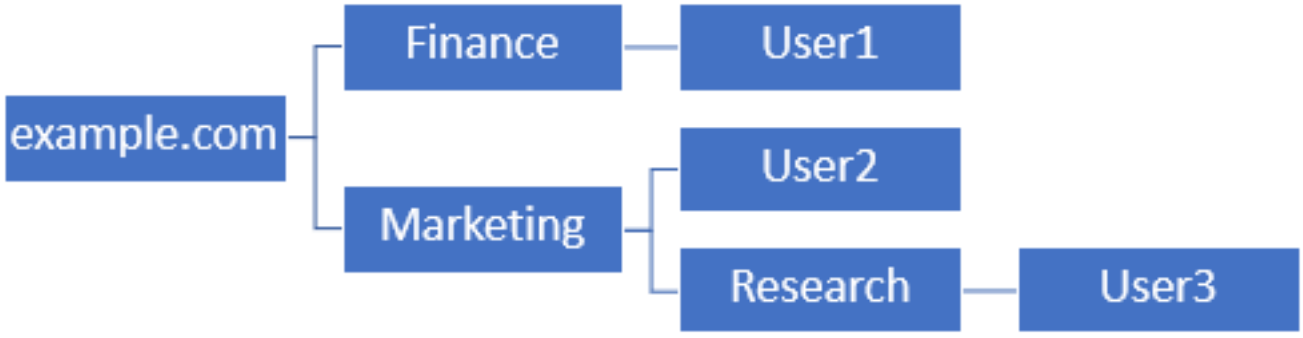
- Administrateurs AnyConnect : Groupe de test auquel l'administrateur informatique sera ajouté afin de démontrer l'identité de l'utilisateur. Ce groupe ne disposera que d'un accès RDP au serveur Windows

- Utilisateurs AnyConnect : Groupe de tests auquel l'utilisateur de test sera ajouté afin de démontrer l'identité de l'utilisateur. Ce groupe ne disposera que d'un accès HTTP au serveur Windows

Configurations AD

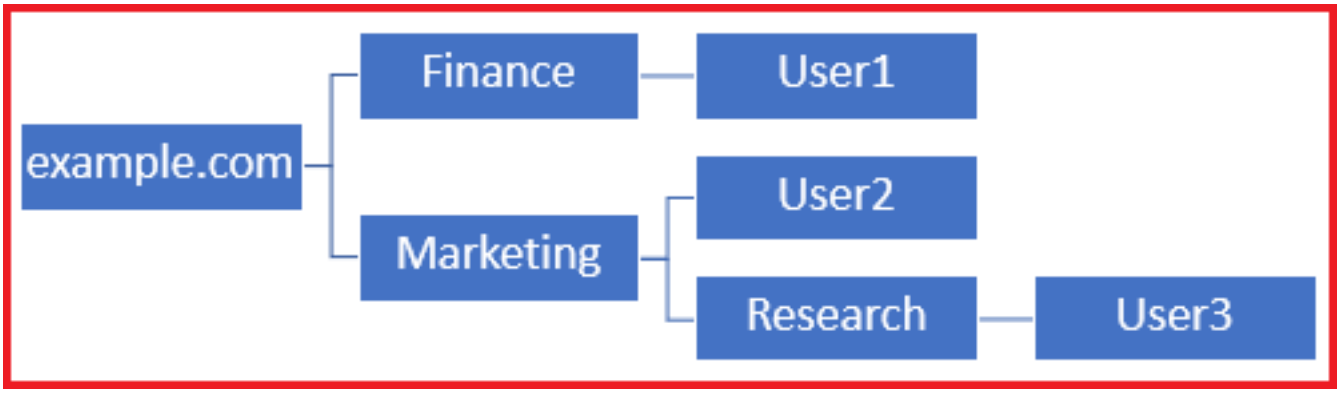
Afin de configurer correctement l'authentification AD et l'identité de l'utilisateur sur FTD, quelques valeurs seront requises. Tous ces détails doivent être créés ou collectés sur Microsoft Server avant que la configuration puisse être effectuée sur FDM. Les principales valeurs sont les suivantes :

- le nom de domaine: Il s'agit du nom de domaine du serveur. Dans ce guide de configuration, exemple.com est le nom de domaine.
- Adresse IP/FQDN du serveur : Adresse IP ou nom de domaine complet utilisé pour atteindre le serveur Microsoft. Si un FQDN est utilisé, un serveur DNS doit être configuré dans FDM et FTD afin de résoudre le FQDN. Dans ce guide de configuration, ces valeurs sont **win2016.example.com** qui prend la résolution 192.168.1.1.
- Port du serveur : Port utilisé par le service LDAP. Par défaut, LDAP et STARTTLS utiliseront le port TCP 389 pour LDAP et LDAP sur SSL (LDAPS) utiliseront 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 FDM et FTD pour établir une liaison avec le serveur LDAP, authentifier les utilisateurs et rechercher les utilisateurs et les groupes. Un compte nommé FTD Admin sera créé à cette fin.
- Nom distinctif de base (DN) : Le DN de base est le point de départ du FDM et le FTD indique à Active Directory de commencer à rechercher des utilisateurs. Dans ce guide de configuration, le domaine racine example.com sera utilisé comme DN de base ; cependant, dans un environnement de production, l'utilisation d'un DN de base plus loin dans la hiérarchie LDAP pourrait être préférable. Par exemple, prenez cette hiérarchie LDAP :



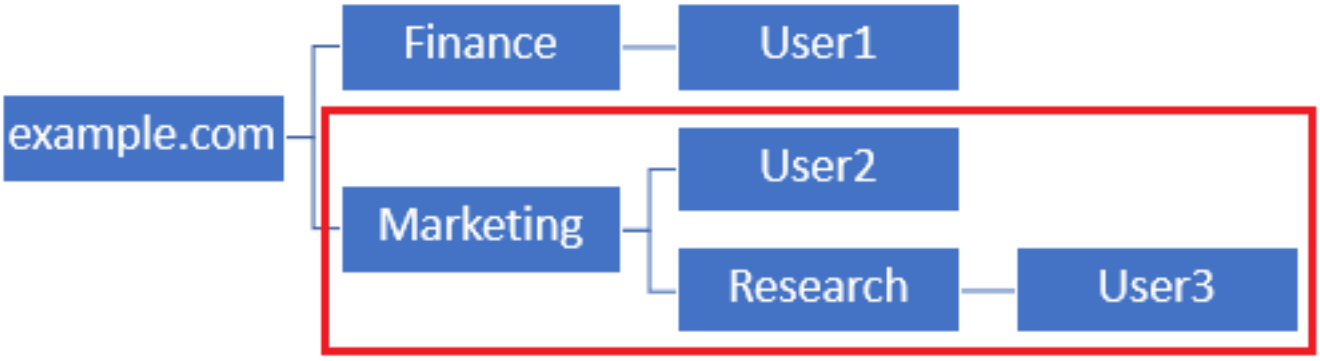
Si un administrateur souhaite que les utilisateurs de l'unité d'organisation Marketing puissent authentifier le DN de base peut être défini sur la racine (exemple.com), cela permettra également à l'utilisateur 1 de l'unité d'organisation Finance de se connecter également puisque la recherche de l'utilisateur commence à la racine et passe à Finance, Marketing et Recherche.

DN de base défini sur exemple.com.



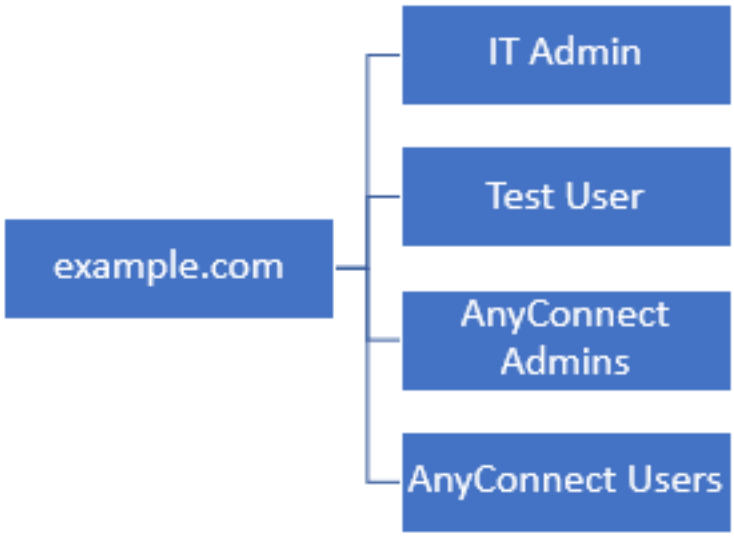
Afin de limiter les connexions aux utilisateurs de l'unité d'organisation Marketing et des niveaux inférieurs, l'administrateur peut à la place définir le DN de base sur Marketing. À présent, seuls l'utilisateur 2 et l'utilisateur 3 pourront s'authentifier, car la recherche commencera à Marketing.

DN de base défini sur Marketing :



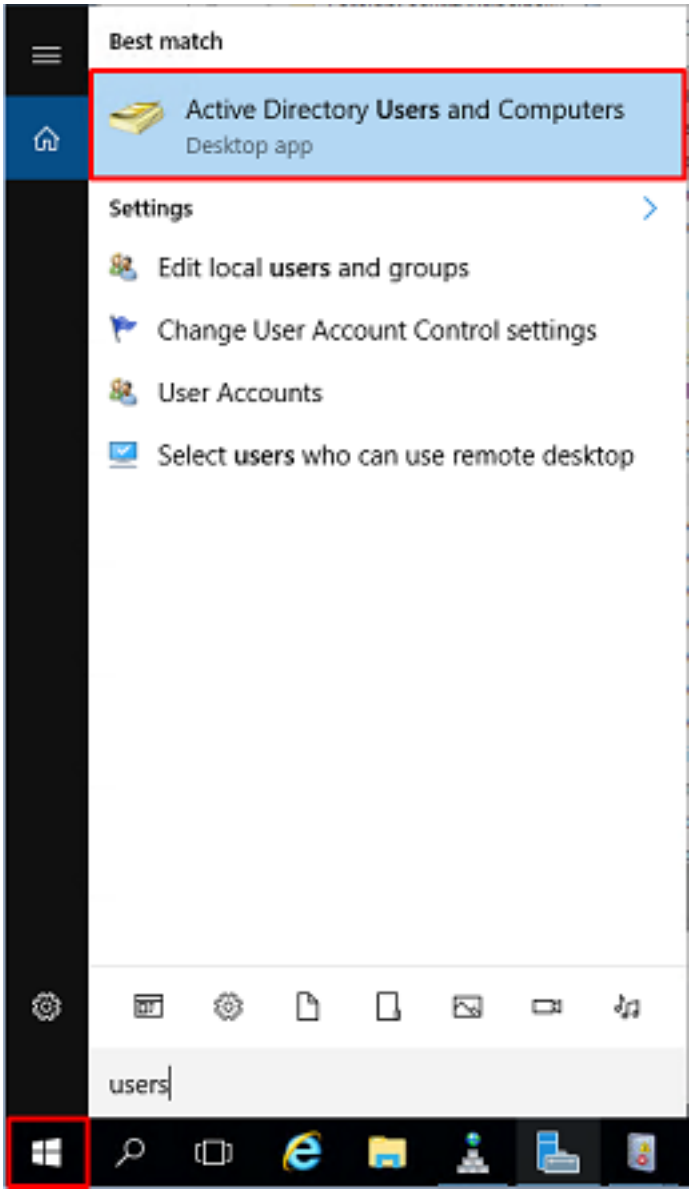
Notez que pour un contrôle plus précis au sein du FTD pour lequel les utilisateurs seront autorisés à se connecter ou à attribuer des autorisations différentes aux utilisateurs en fonction de leurs attributs AD, une carte d'autorisation LDAP devra être configurée.

Cette hiérarchie LDAP simplifiée est utilisée dans ce guide de configuration et le DN de l'exemple racine.com sera utilisé pour le DN de base.

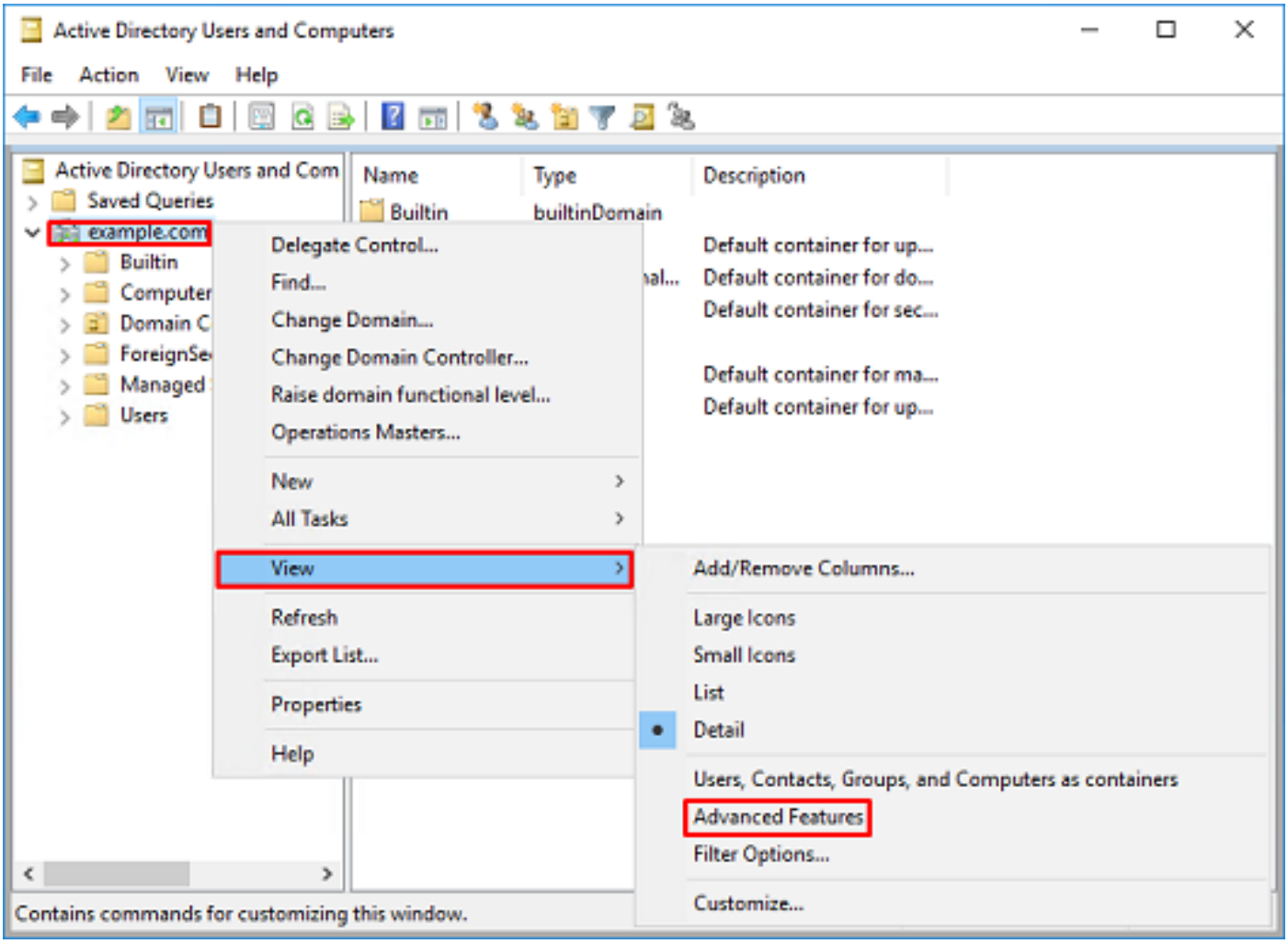


Déterminer le DN de base LDAP

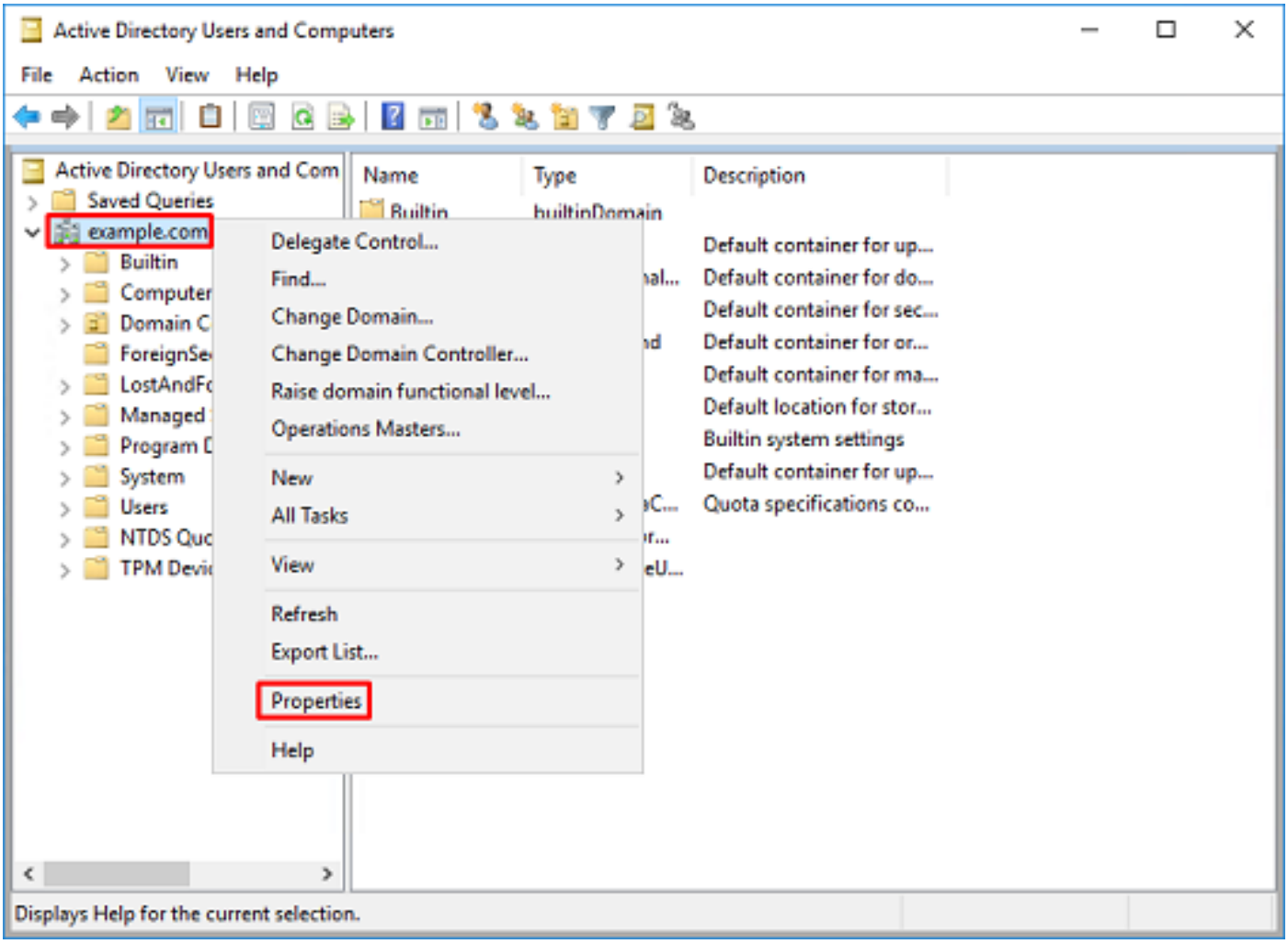
1. Ouvrez Utilisateurs et ordinateurs AD.



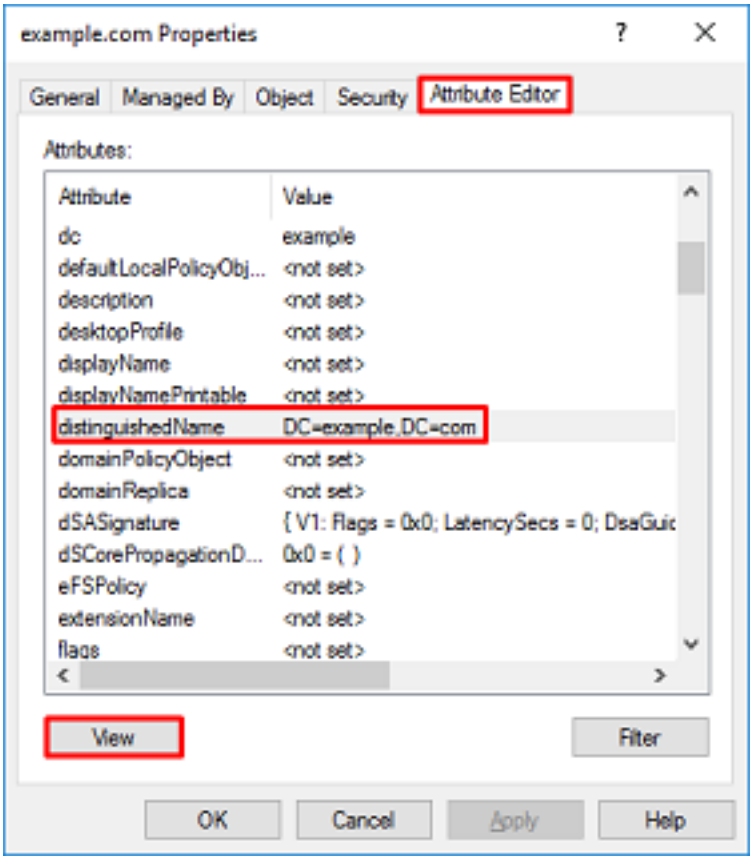
2. Cliquez avec le bouton gauche sur le domaine racine (afin d'ouvrir le conteneur), cliquez avec le bouton droit sur le domaine racine, puis accédez à **Affichage** et cliquez sur **Fonctions avancées**.



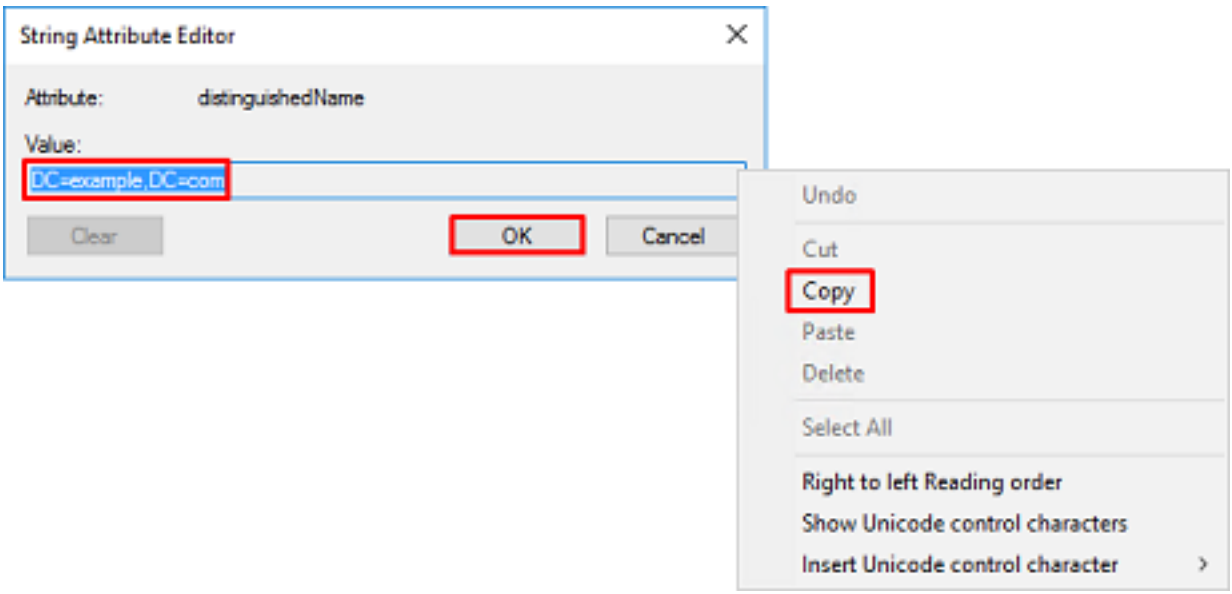
3. Ceci active l'affichage des propriétés supplémentaires sous les objets AD. Par exemple, pour rechercher le DN du fichier exemple.com racine, cliquez avec le bouton droit de la souris sur **exemple.com** puis accédez à **Propriétés**.

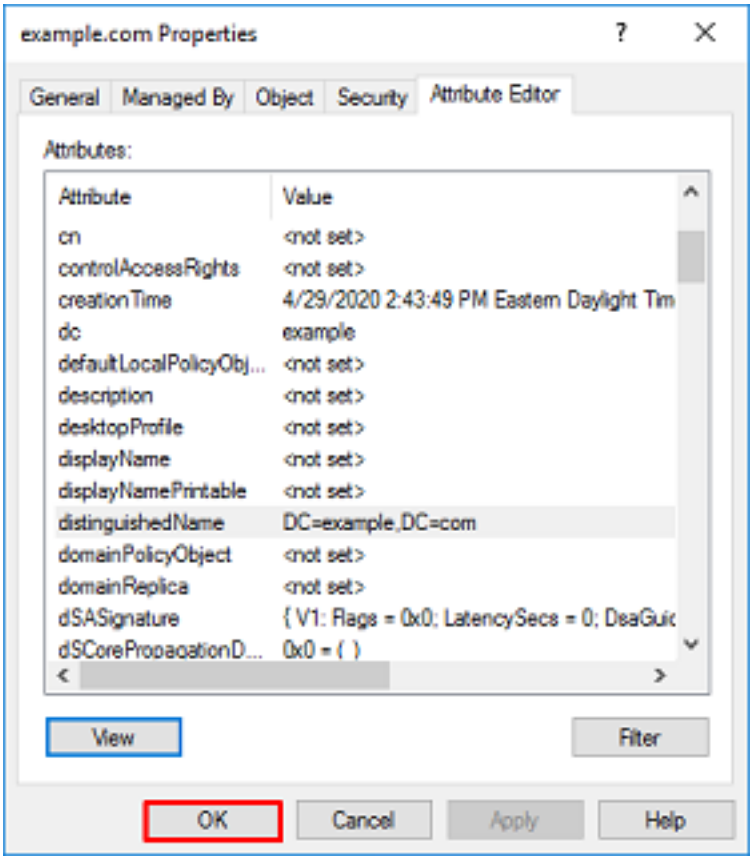


4. Sous **Propriétés**, cliquez sur l'onglet **Éditeur d'attributs**. Recherchez **distinguéName** sous Attributs, puis cliquez sur **Affichage**.

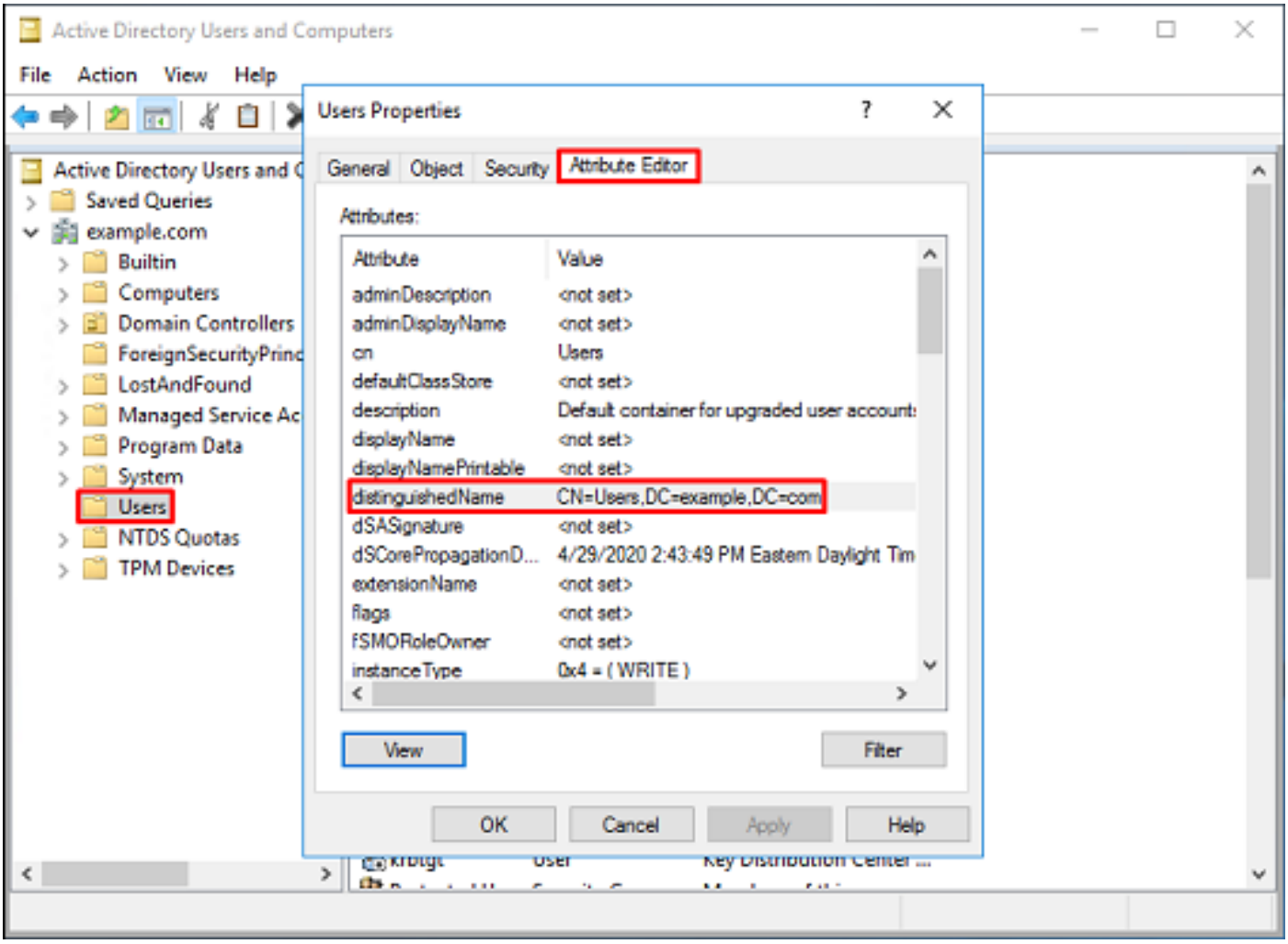


5. Cela ouvrira une nouvelle fenêtre dans laquelle le DN peut être copié et collé dans FDM ultérieurement. Dans cet exemple, le DN racine est DC=exemple, DC=com. Copiez la valeur. Cliquez sur **OK** afin de quitter la fenêtre Éditeur d'attributs de chaîne, puis cliquez à nouveau sur **OK** afin de quitter les Propriétés.

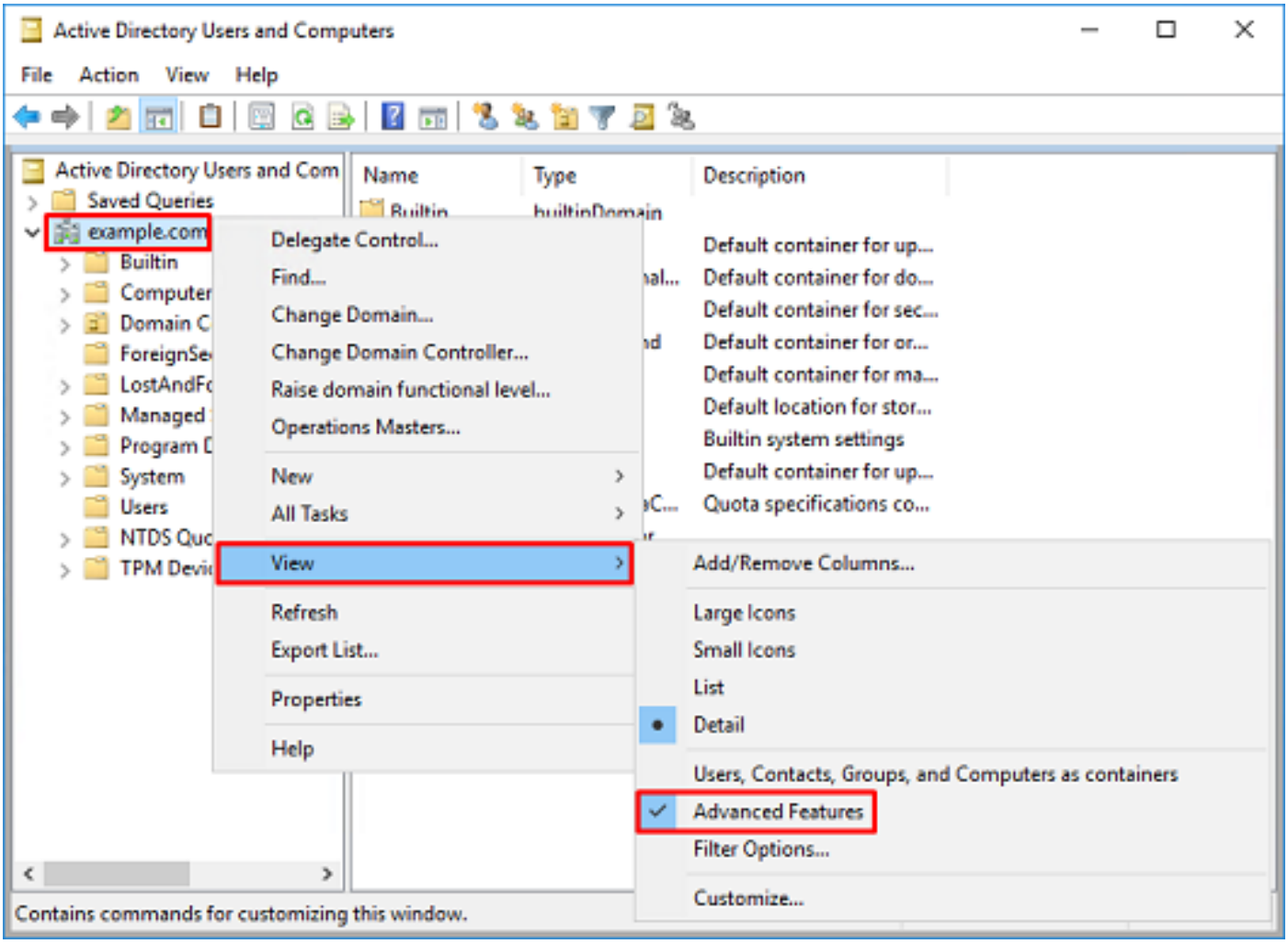




Cela peut être fait pour plusieurs objets dans AD. Par exemple, ces étapes sont utilisées pour rechercher le numéro de répertoire du conteneur utilisateur :



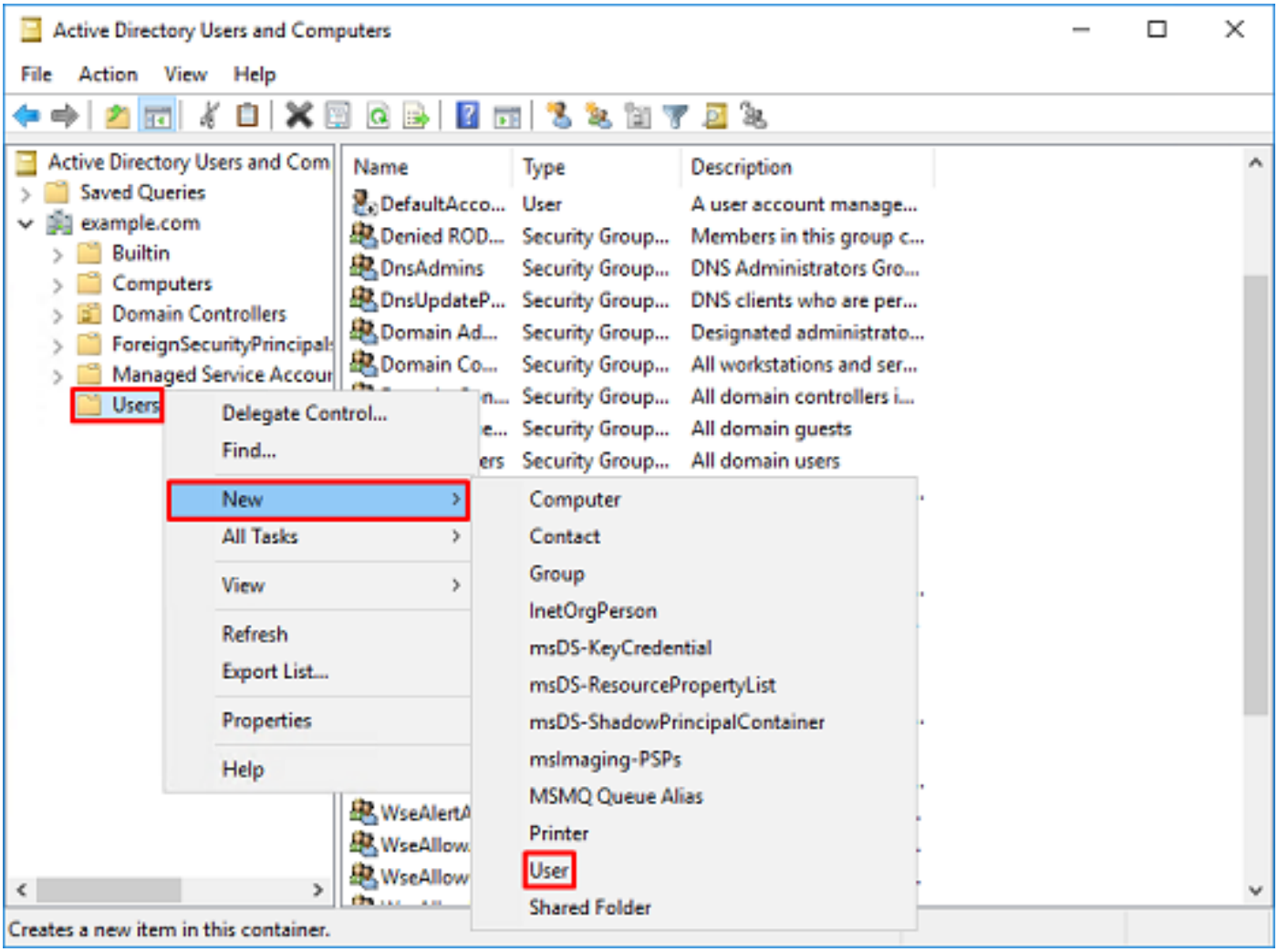
6. La vue Advanced Features (Fonctions avancées) peut être supprimée. Cliquez avec le bouton droit sur le DN racine, accédez à **Affichage** et cliquez une fois de plus sur **Fonctionnalités avancées**.



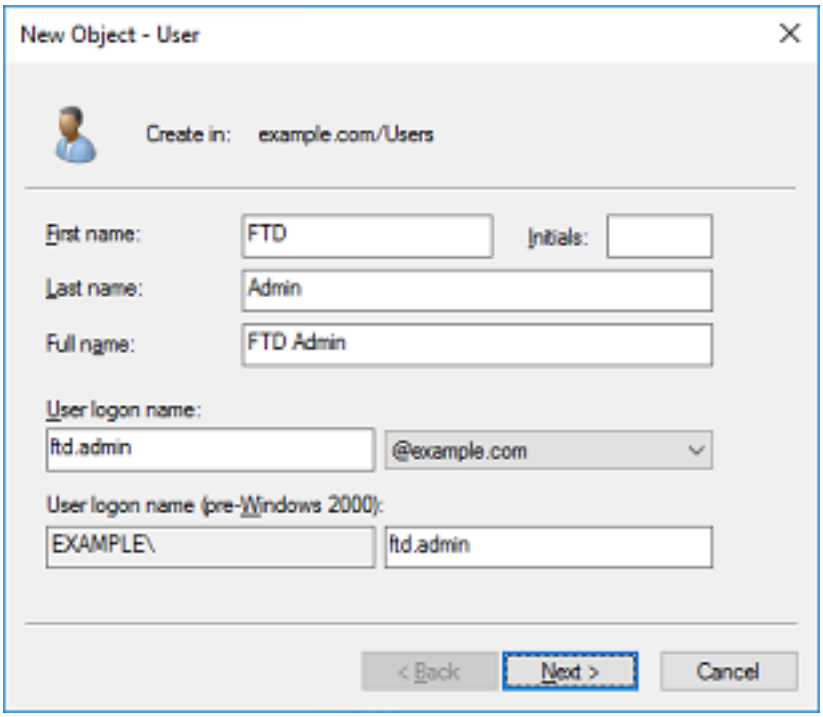
Créer un compte FTD

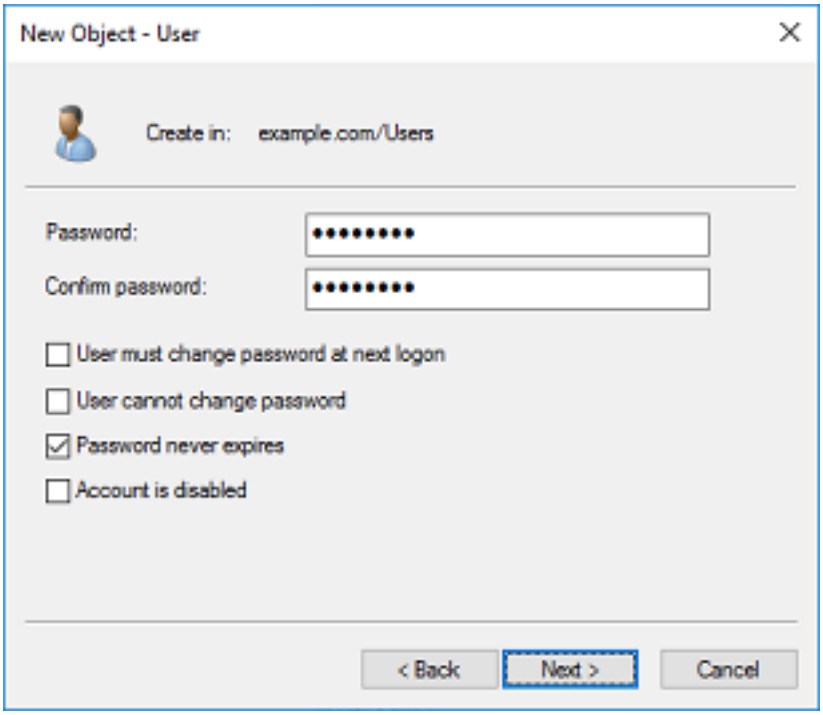
Ce compte d'utilisateur permettra à FDM et au FTD de se lier à l'AD afin de rechercher des utilisateurs et des groupes et de les authentifier. La création d'un compte FTD distinct a pour but d'empêcher tout accès non autorisé ailleurs dans le réseau si les informations d'identification utilisées pour la liaison sont compromises. Ce compte n'a pas besoin d'être compris dans la portée du DN de base.

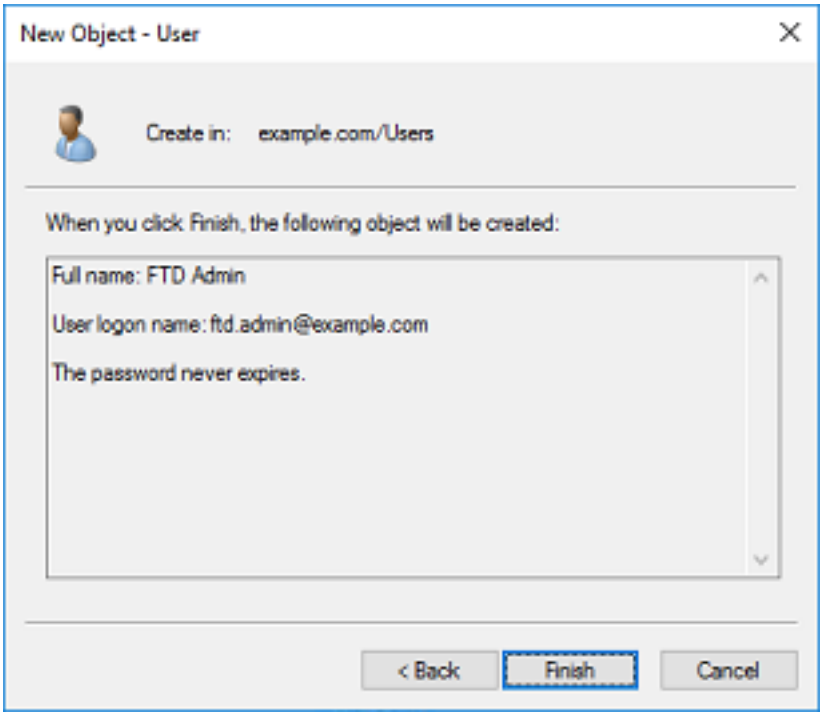
1. Dans **Utilisateurs et ordinateurs Active Directory**, cliquez avec le bouton droit sur le conteneur/l'organisation auquel le compte FTD sera ajouté. Dans cette configuration, le compte FTD sera ajouté sous le conteneur Utilisateurs sous le nom d'utilisateur **ftd.admin@example.com**. Cliquez avec le bouton droit sur **Utilisateurs**, puis cliquez sur **Nouveau > Utilisateur**.



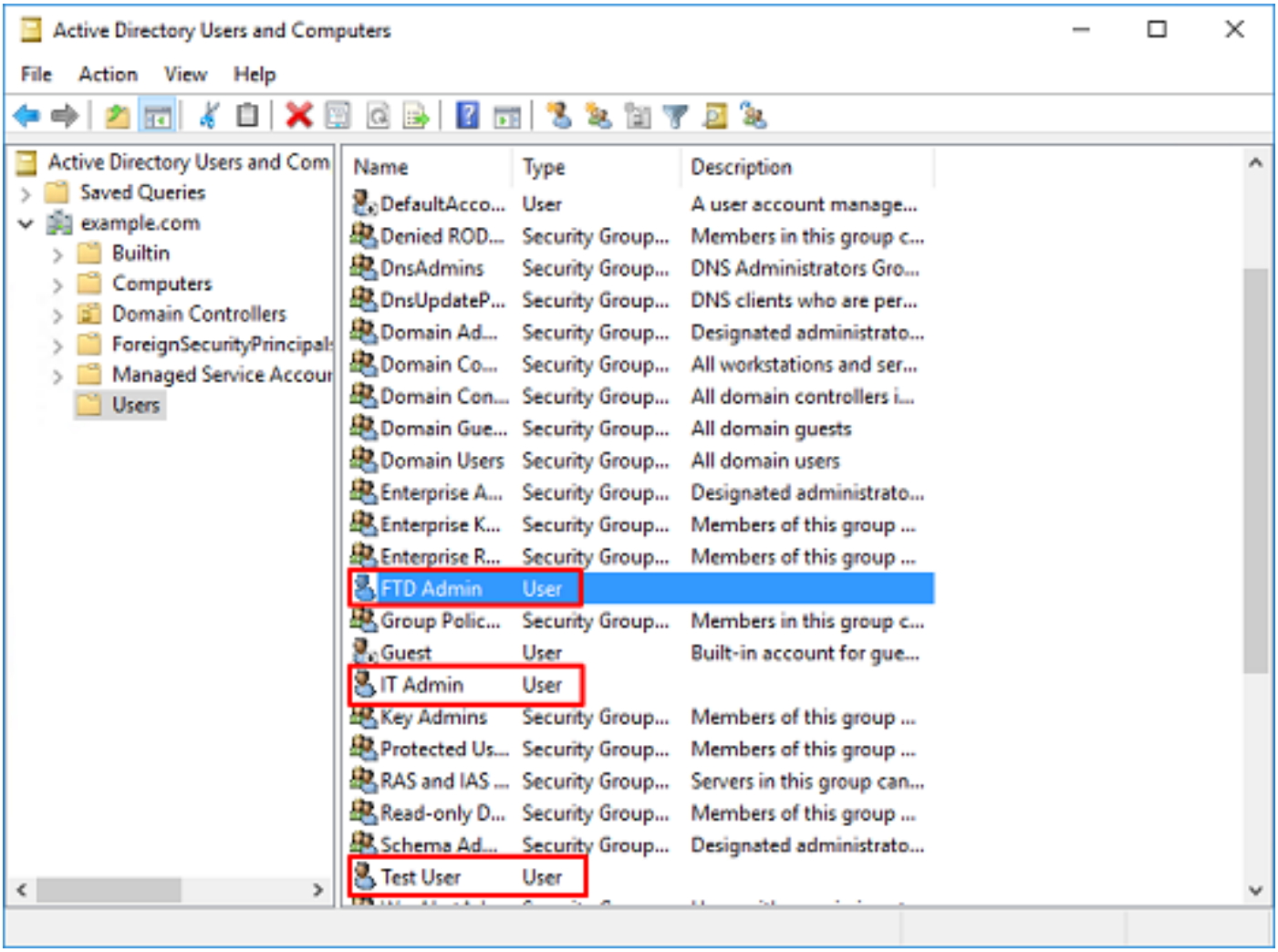
2. Naviguez dans l'Assistant **Nouvel objet - Utilisateur**.







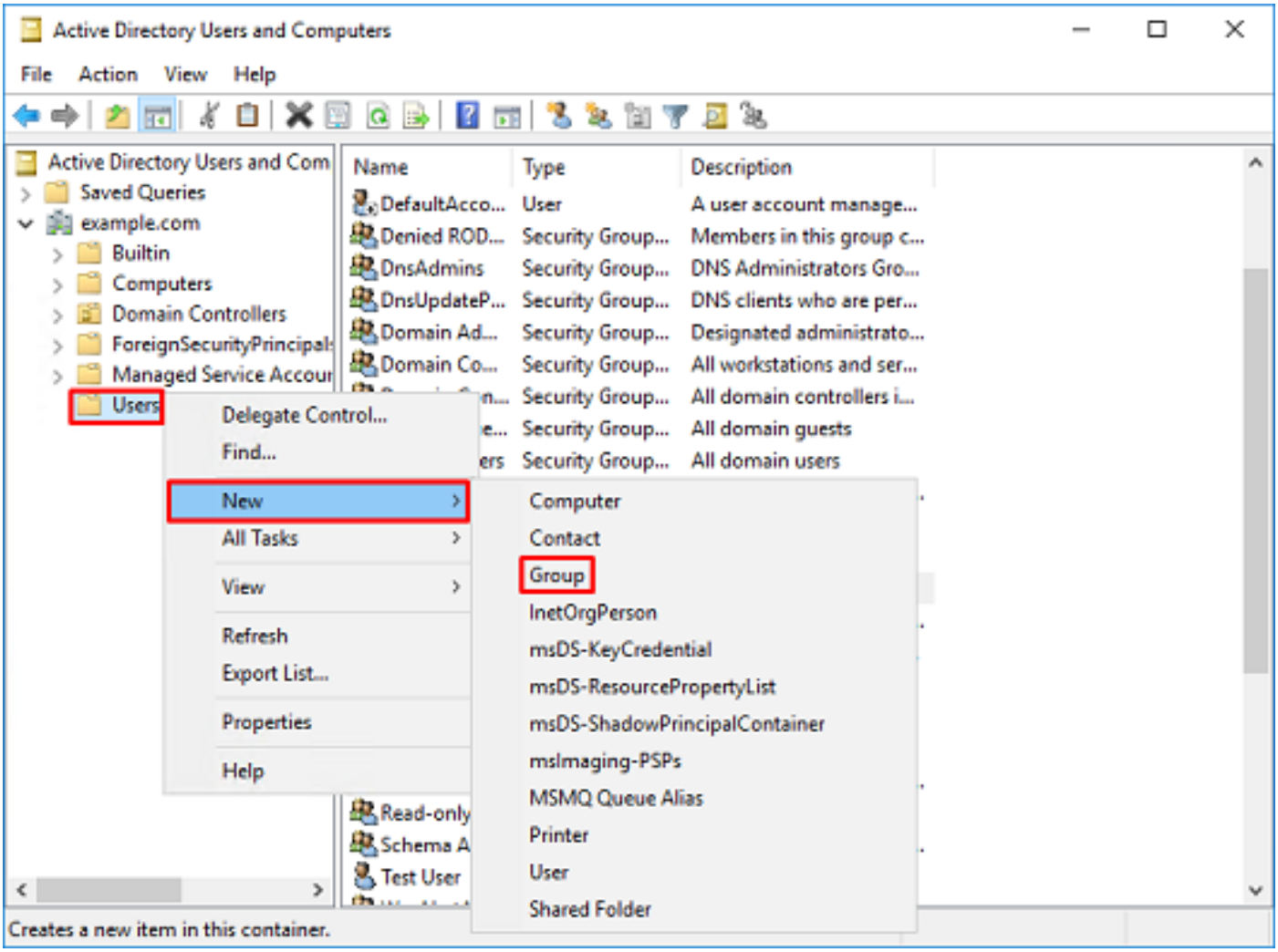
3. Vérifiez que le compte FTD a été créé. En outre, deux comptes supplémentaires ont été créés, **Administrateur informatique** et **Utilisateur de test**.



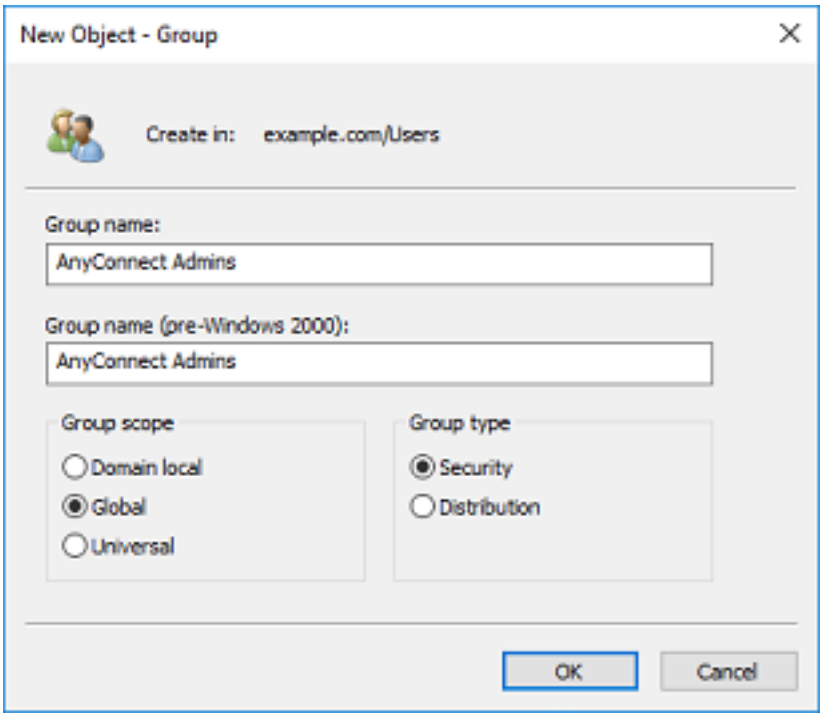
Créer des groupes AD et ajouter des utilisateurs aux groupes AD (facultatif)

Bien qu'ils ne soient pas requis pour l'authentification, les groupes peuvent être utilisés pour faciliter l'application des stratégies d'accès à plusieurs utilisateurs ainsi qu'à l'autorisation LDAP. Dans ce guide de configuration, les groupes seront utilisés pour appliquer ultérieurement les paramètres de stratégie de contrôle d'accès via l'identité de l'utilisateur dans FDM.

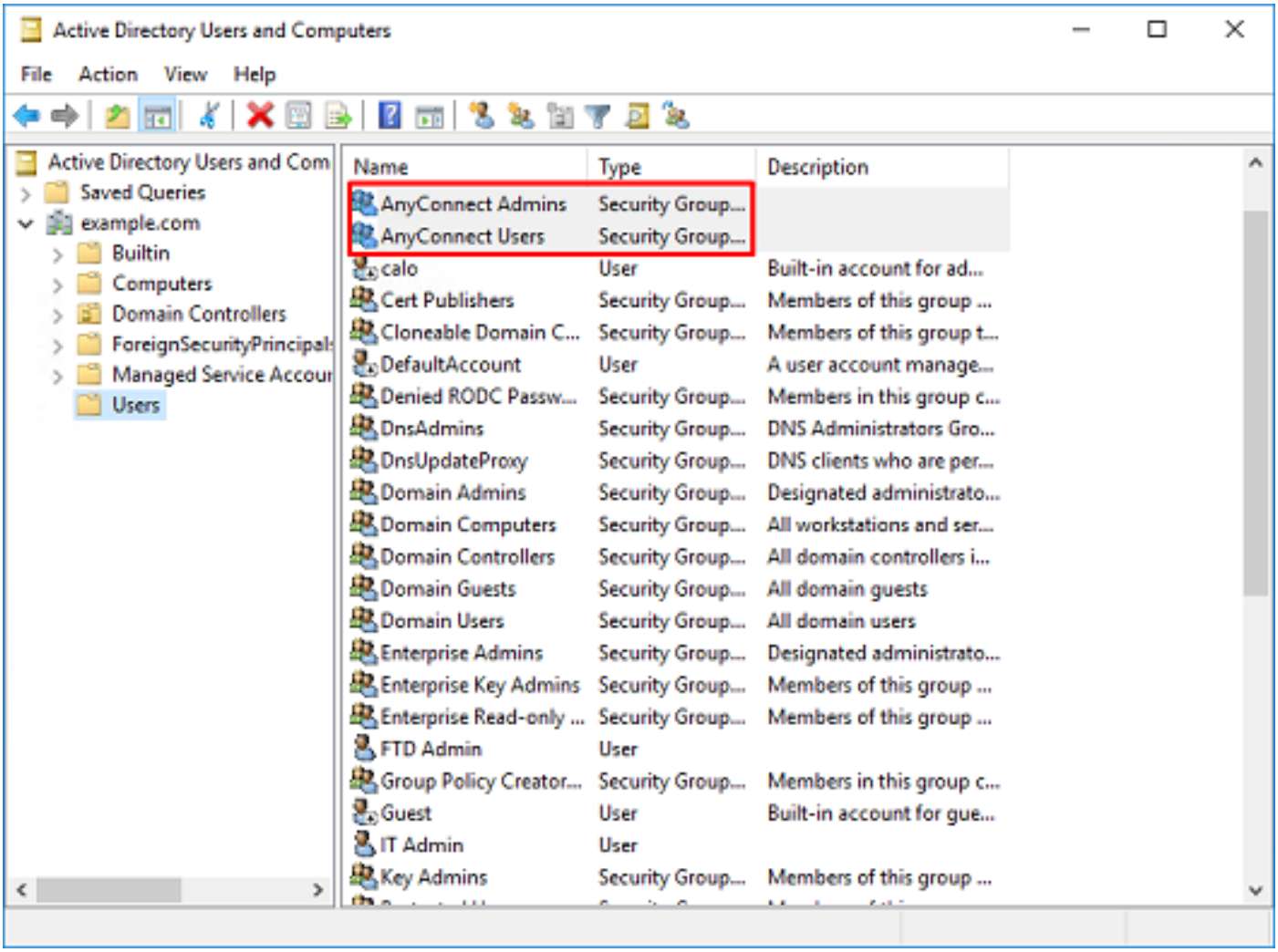
1. Dans **Utilisateurs et ordinateurs Active Directory**, cliquez avec le bouton droit sur le conteneur/l'organisation auquel le nouveau groupe sera ajouté. Dans cet exemple, le groupe **AnyConnect Admins** sera ajouté sous le conteneur Utilisateurs. Cliquez avec le bouton droit sur **Utilisateurs**, puis cliquez sur **Nouveau > Groupe**.



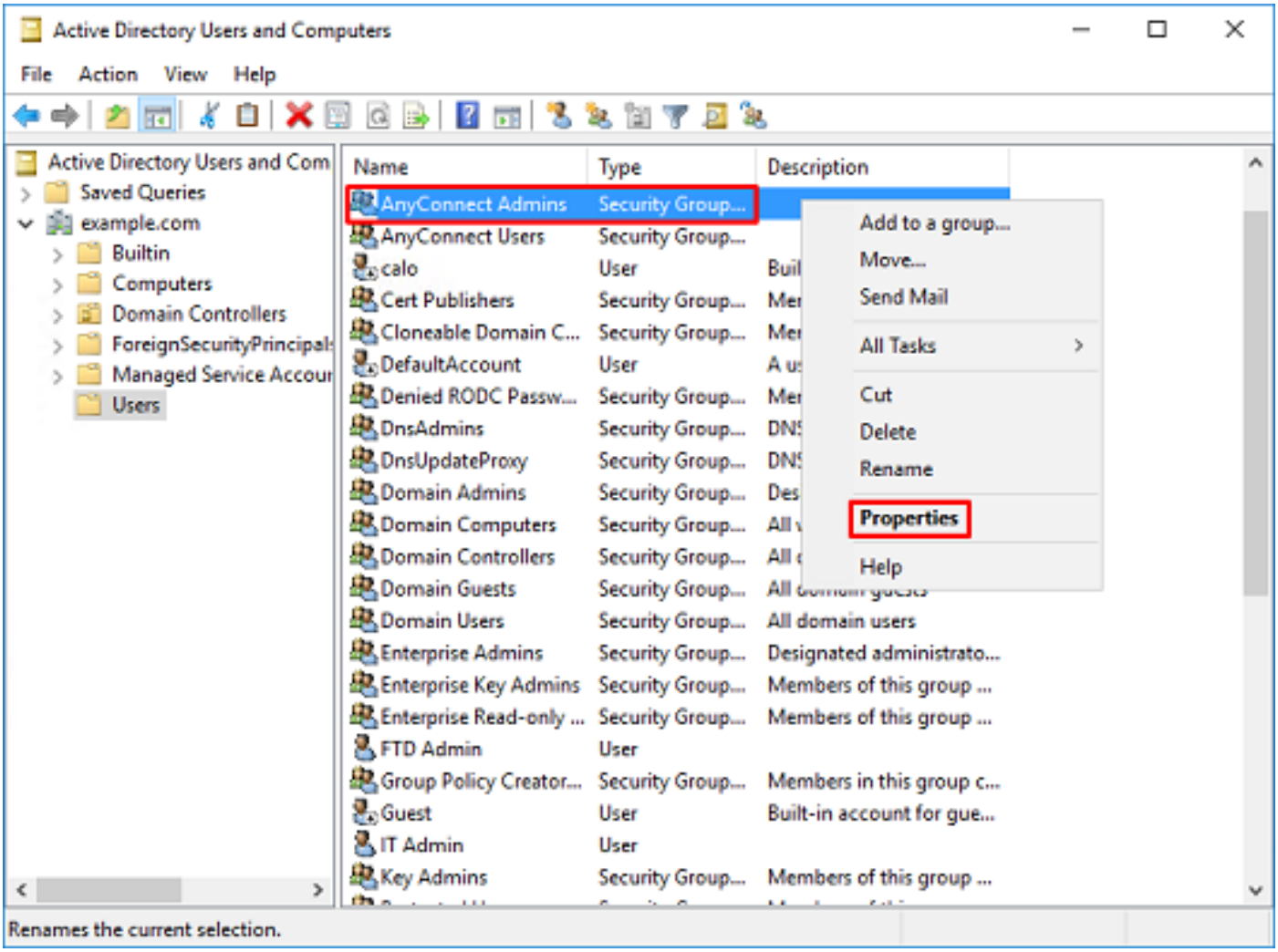
2. Naviguez dans l'Assistant **Nouvel objet - Groupe** comme indiqué dans l'image.



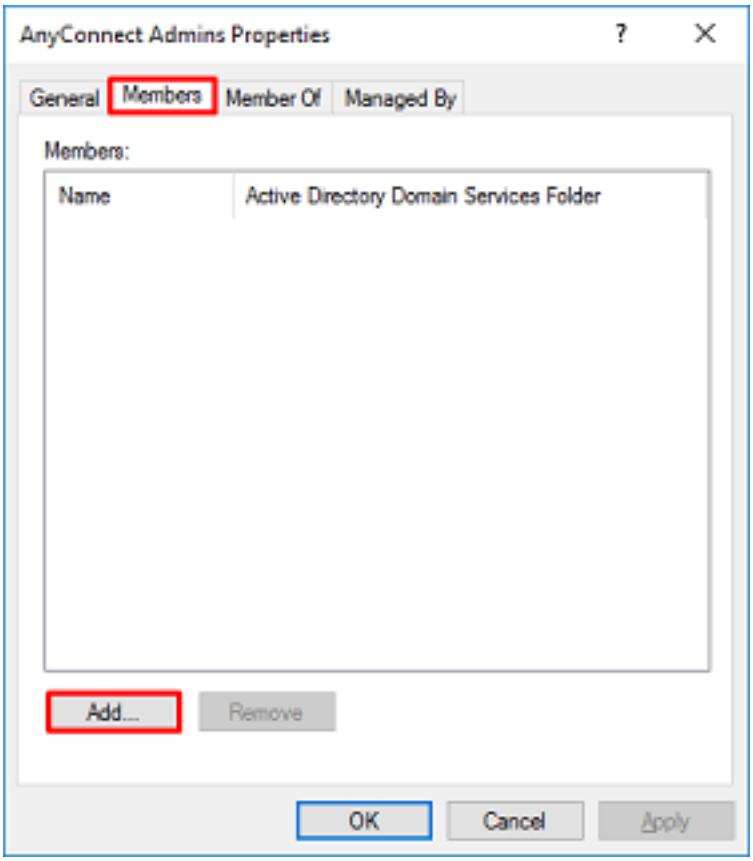
3. Vérifiez que le groupe a été créé. Le groupe **Utilisateurs AnyConnect** a également été créé.



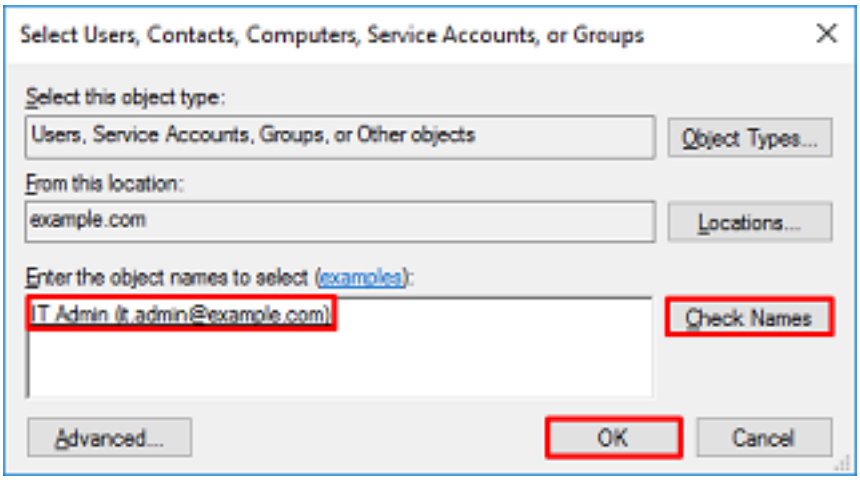
4. Cliquez avec le bouton droit sur le groupe auquel les utilisateurs seront ajoutés, puis sélectionnez **Propriétés**. Dans cette configuration, l'utilisateur **Administrateur informatique** sera ajouté au groupe **Administrateurs AnyConnect** et l'utilisateur **Test User** sera ajouté au groupe **Utilisateurs AnyConnect**.



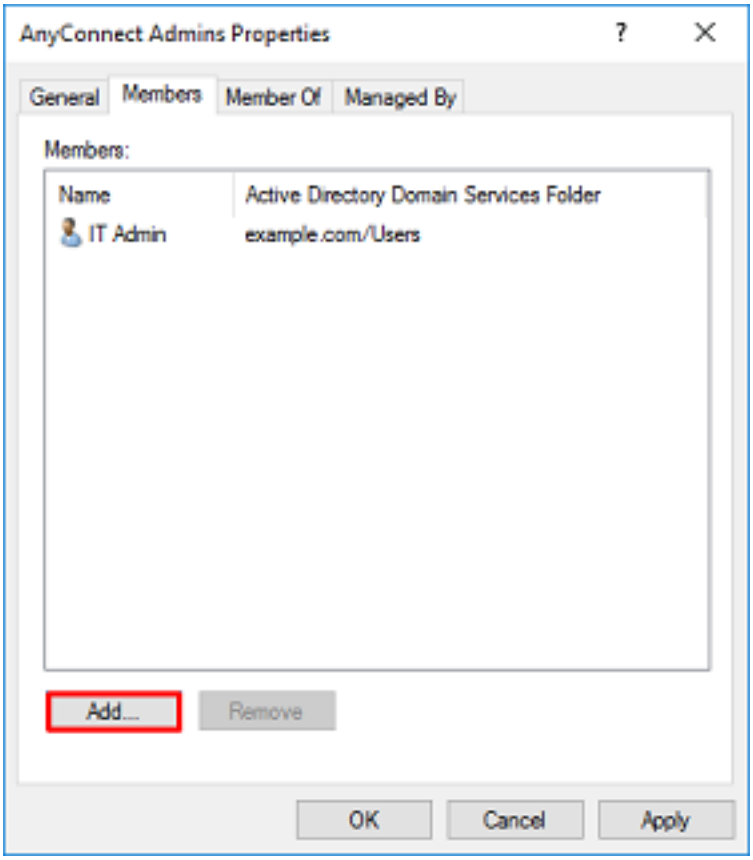
5. Cliquez sur l'onglet **Membres**, puis sur **Ajouter** comme indiqué dans l'image.



Entrez l'utilisateur dans le champ et cliquez sur le bouton **Vérifier les noms** afin de vérifier que l'utilisateur est trouvé. Une fois vérifié, cliquez sur **OK**.

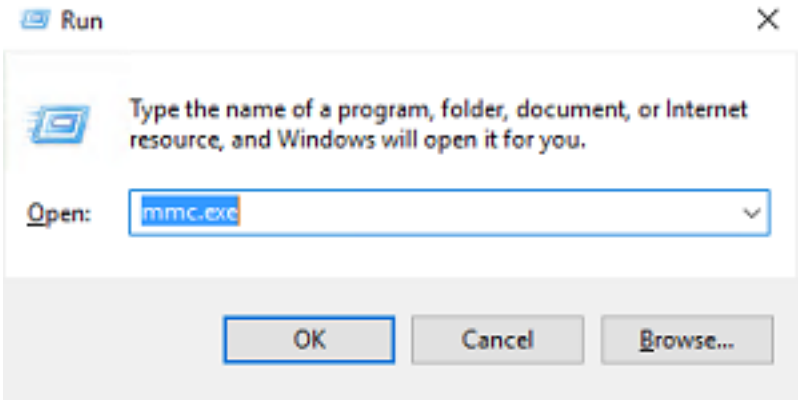


Vérifiez que l'utilisateur correct est ajouté, puis cliquez sur le bouton **OK**. L'utilisateur Test User est également ajouté au groupe d'utilisateurs AnyConnect à l'aide des mêmes étapes.

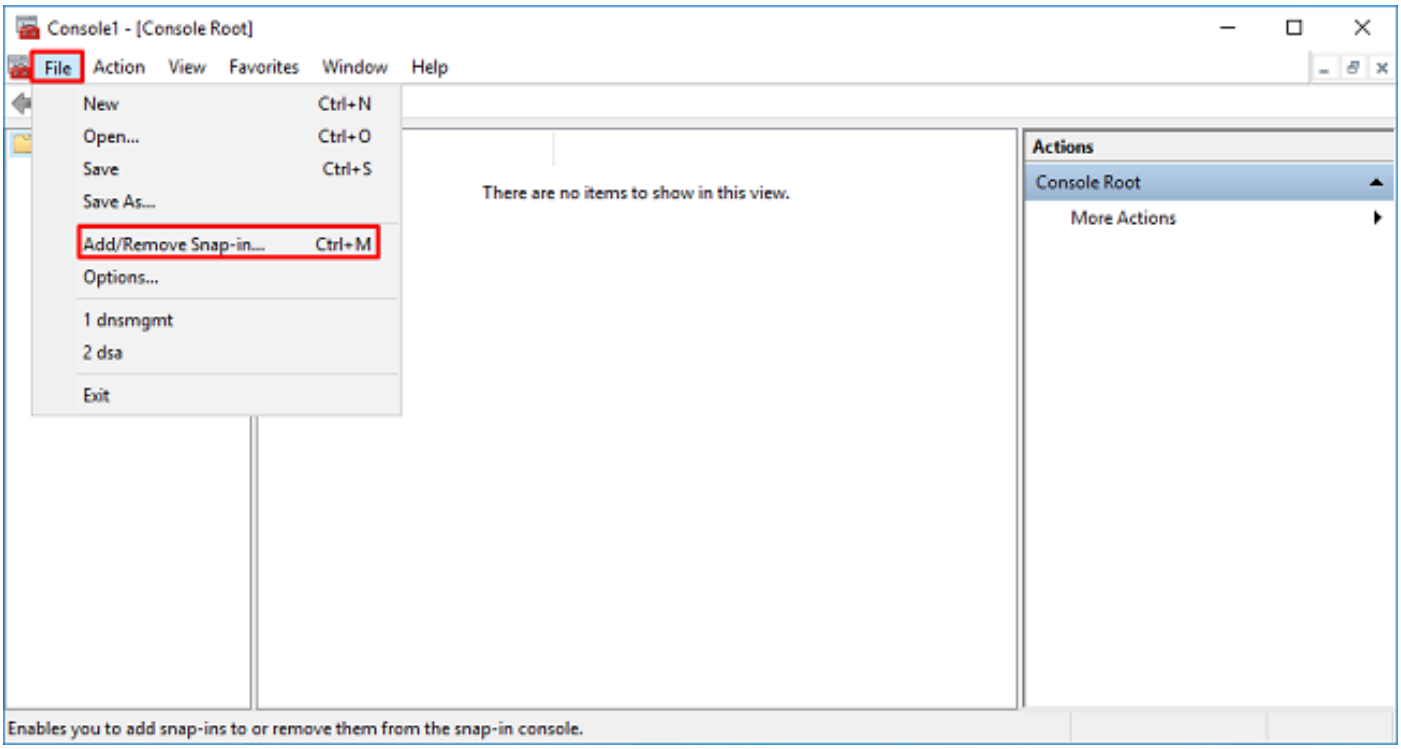


Copier la racine du certificat SSL LDAPS (obligatoire uniquement pour LDAPS ou STARTTLS)

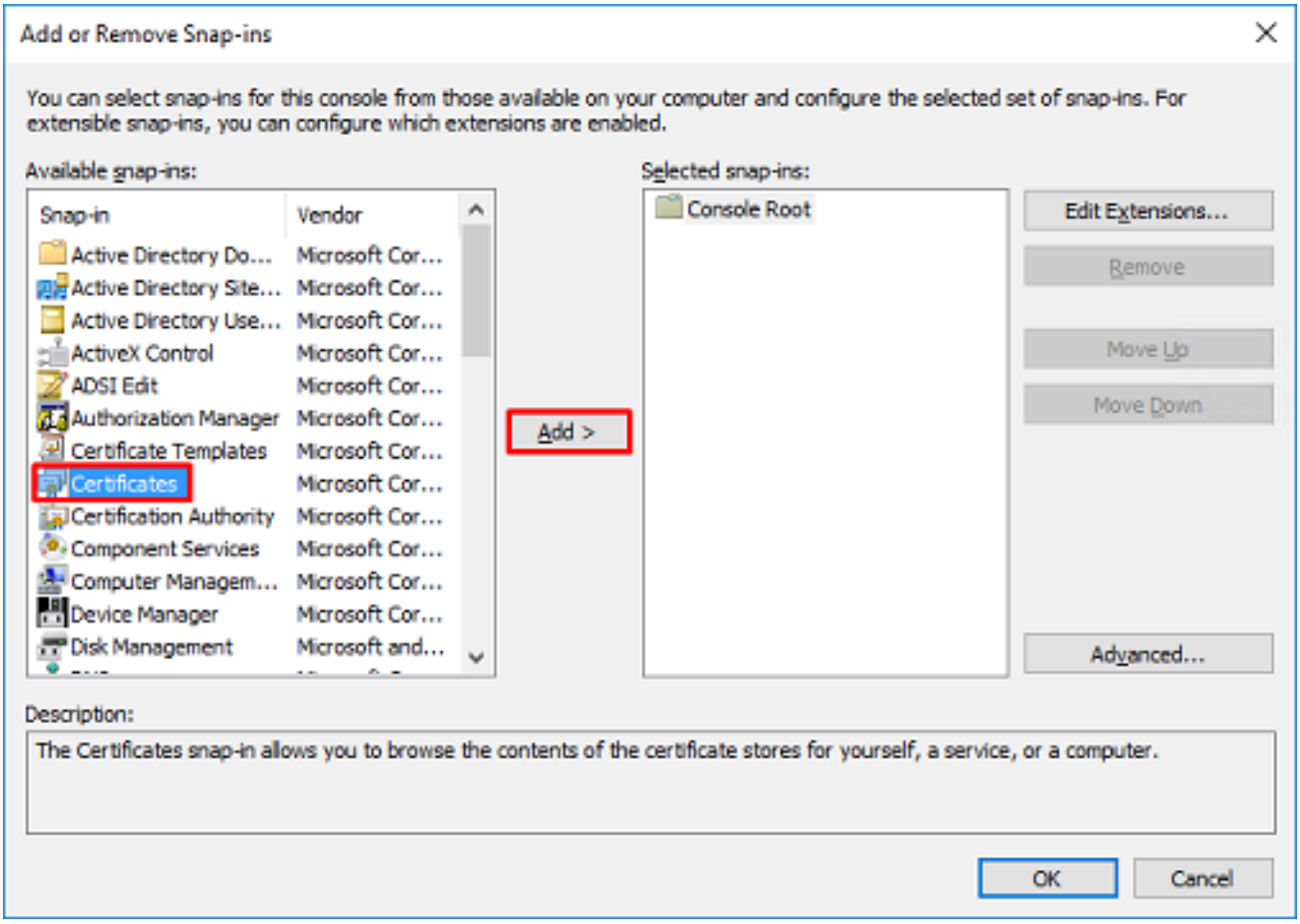
1. Appuyez sur **Win+R** et tapez **mmc.exe**. Click OK.



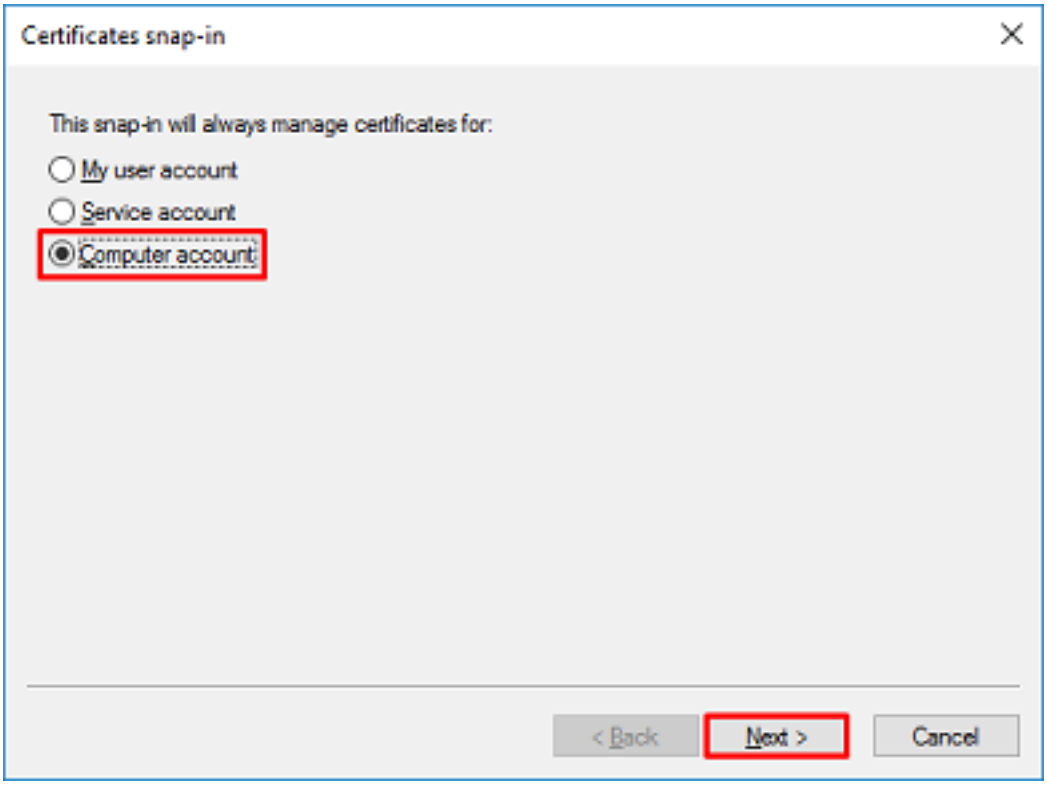
2. Accédez à **Fichier > Ajouter/Supprimer un composant logiciel enfichable...** comme le montre l'image.



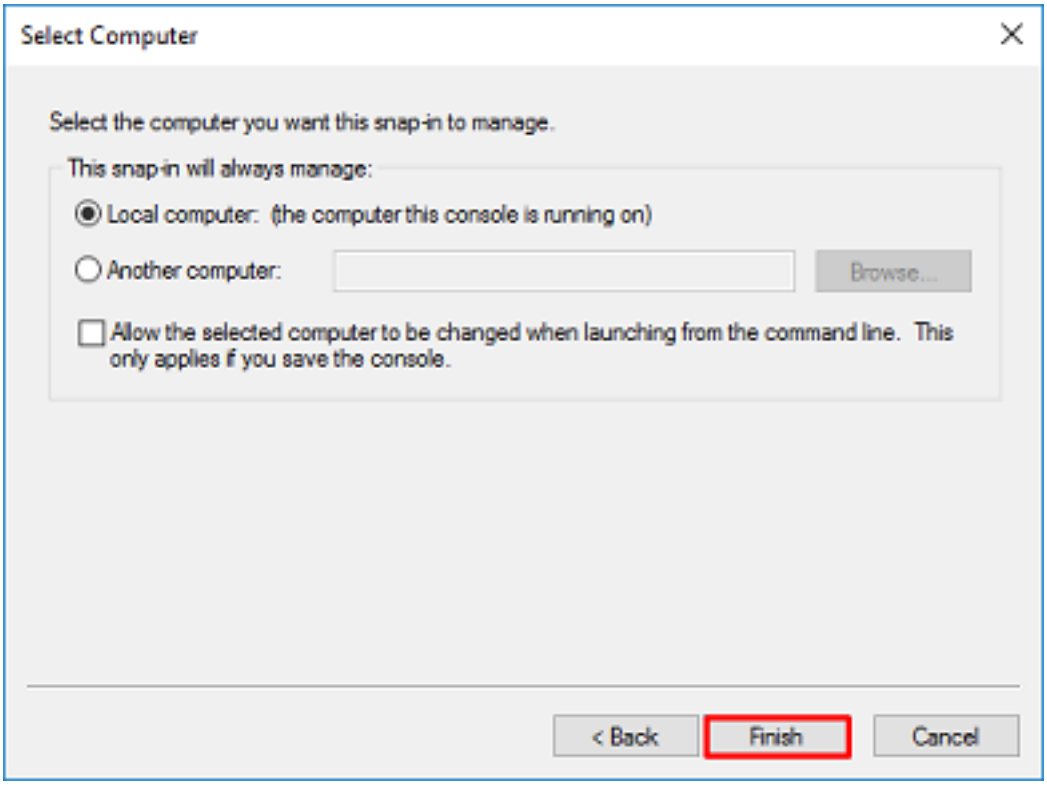
3. Sous les composants logiciels enfichables disponibles, cliquez sur **Certificats**, puis sur **Ajouter**.



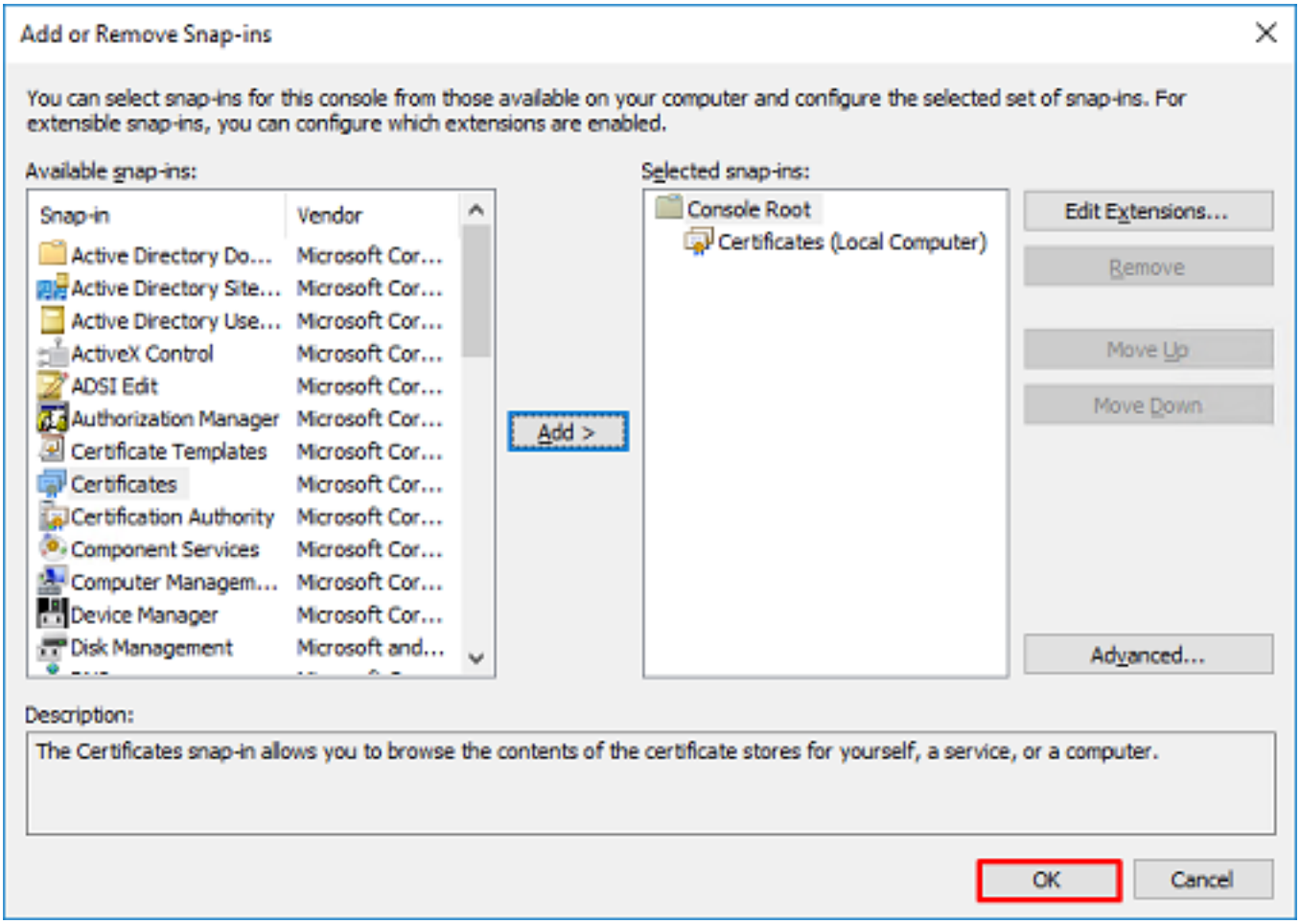
4. Sélectionnez **Compte d'ordinateur**, puis cliquez sur **Suivant** comme indiqué dans l'image.



Cliquez sur Finish.



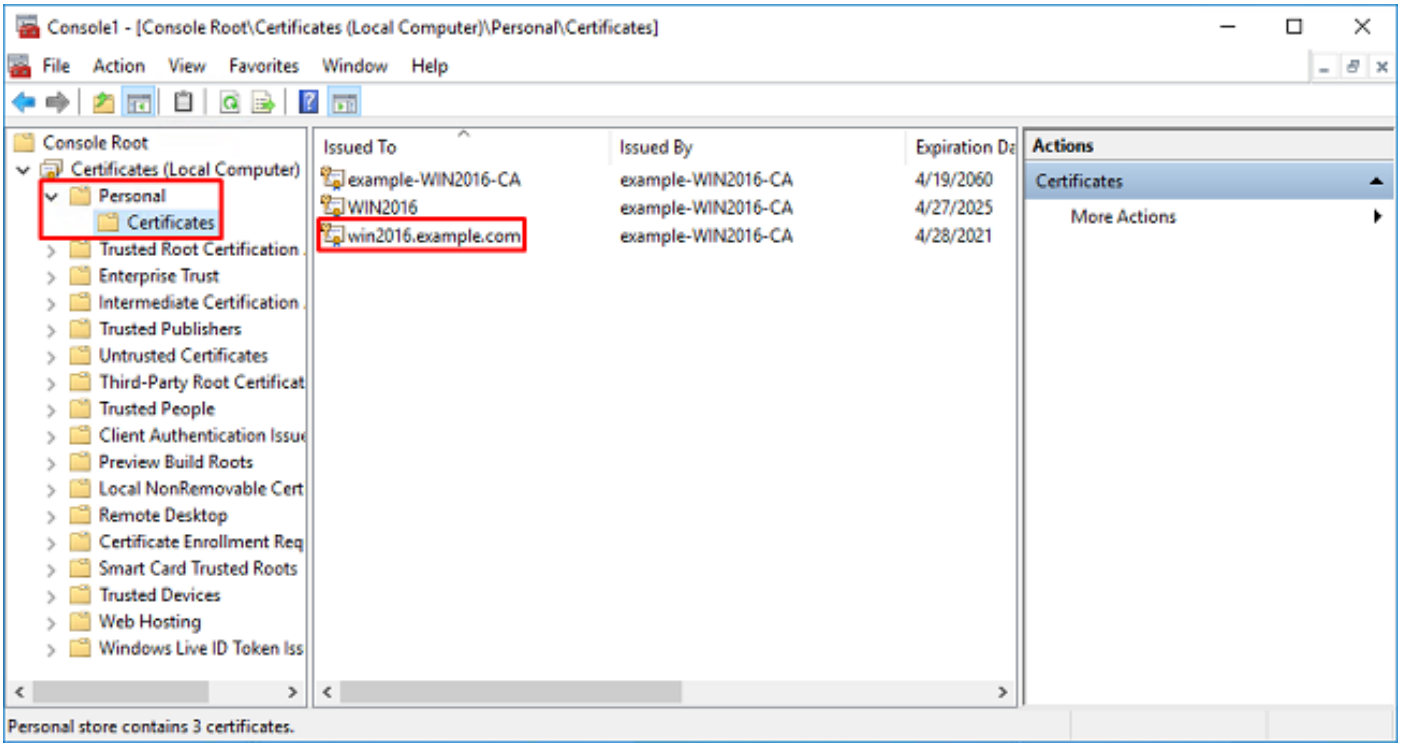
5. Click OK.



6. Développez le dossier **Personnel**, puis cliquez sur **Certificats**. Le certificat utilisé par LDAPS doit être délivré au nom de domaine complet (FQDN) du serveur Windows. Sur ce serveur, 3 certificats sont répertoriés.

- Certificat CA délivré à et par exemple-WIN2016-CA.
- Certificat d'identité délivré au WIN2016 par exemple-WIN2016-CA.
- Certificat d'identité émis pour win2016.example.com par exemple-WIN2016-CA.

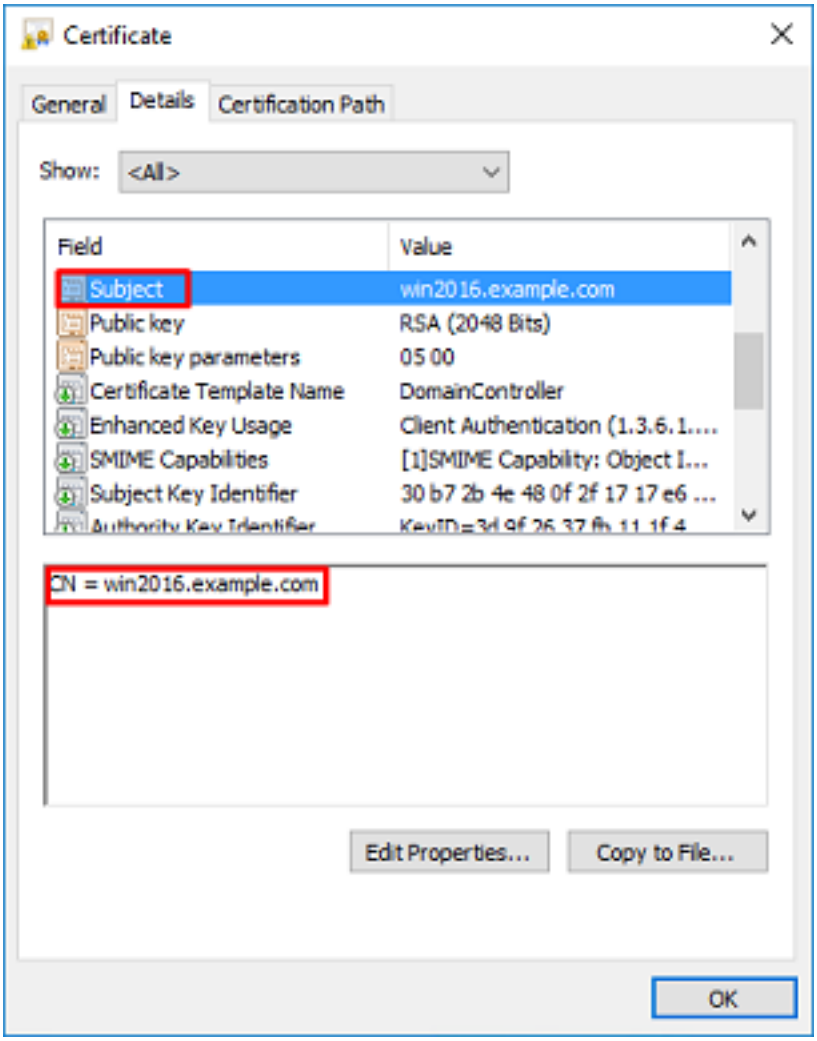
Dans ce guide de configuration, le nom de domaine complet est win2016.example.com et les 2 premiers certificats ne sont donc pas valides pour être utilisés comme certificat SSL LDAPS. Le certificat d'identité émis pour win2016.example.com est un certificat qui a été automatiquement émis par le service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

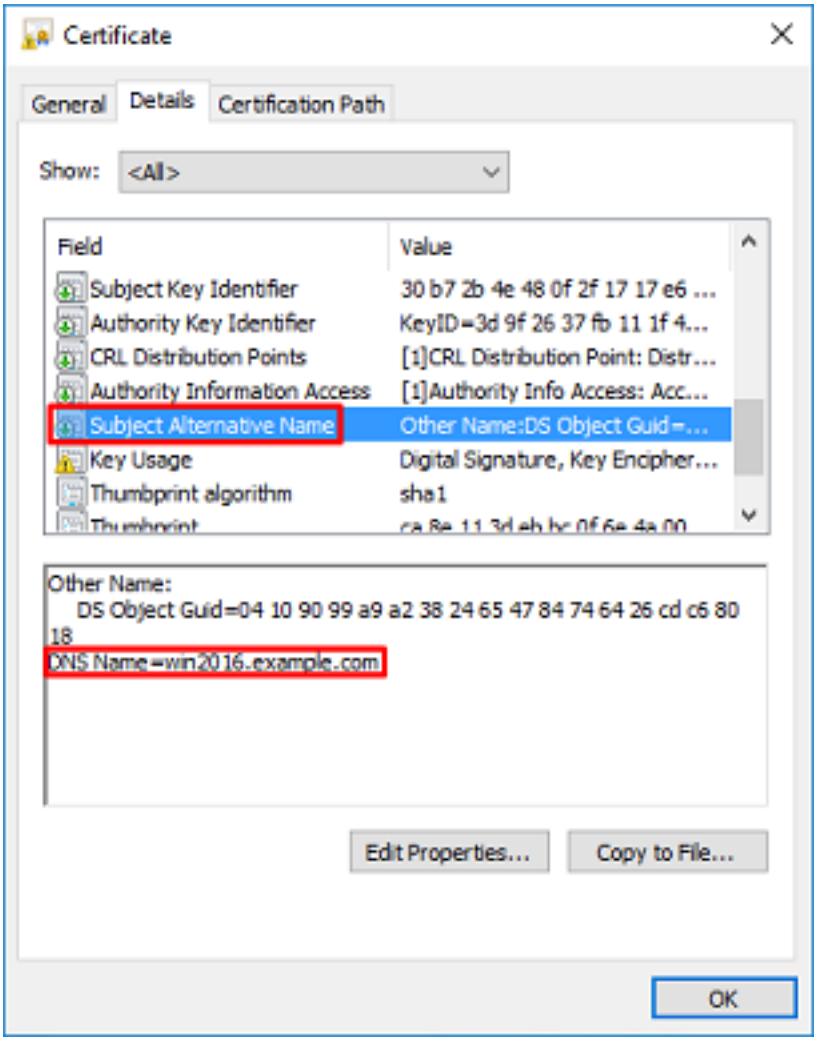


7. Afin d'être utilisé comme certificat SSL LDAPS, le certificat doit satisfaire aux conditions suivantes :

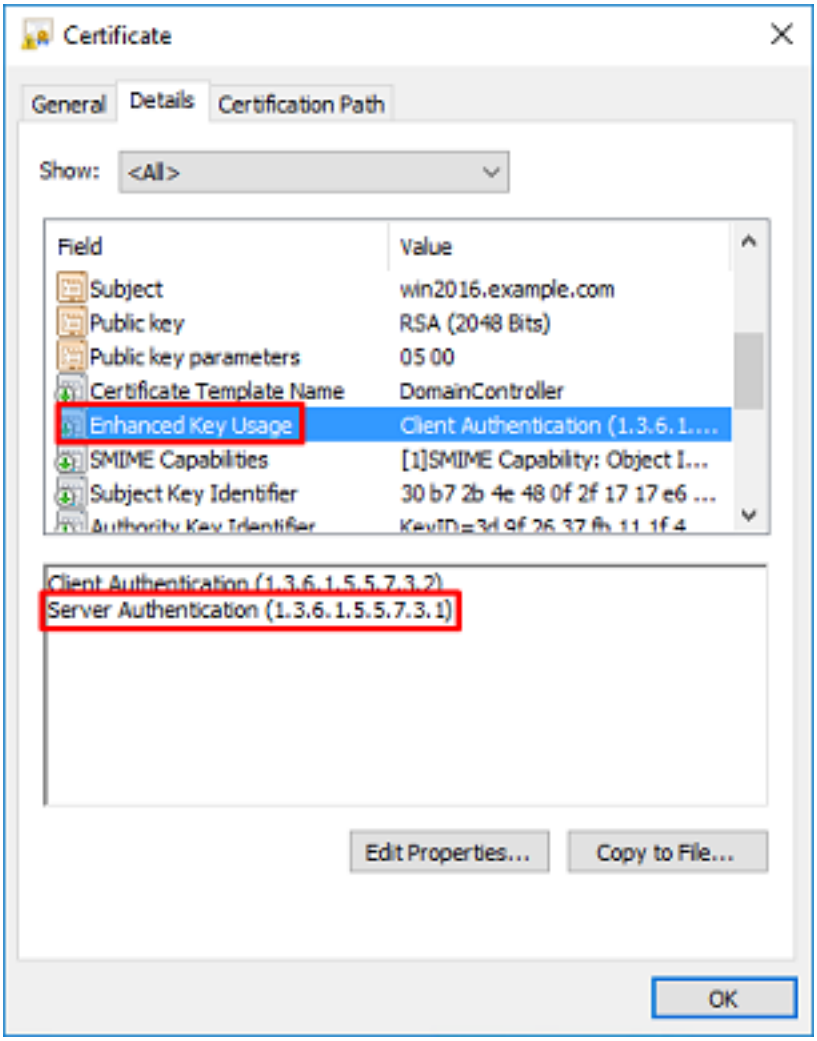
- Le nom commun ou le nom secondaire de l'objet DNS correspond au nom de domaine complet de Windows Server.
- Le certificat possède l'authentification du serveur sous le champ Utilisation de clé améliorée.

Sous l'onglet Détails du certificat, sous **Subject** and **Subject Alternative Name**, le nom de domaine complet **win2016.example.com** est présent.

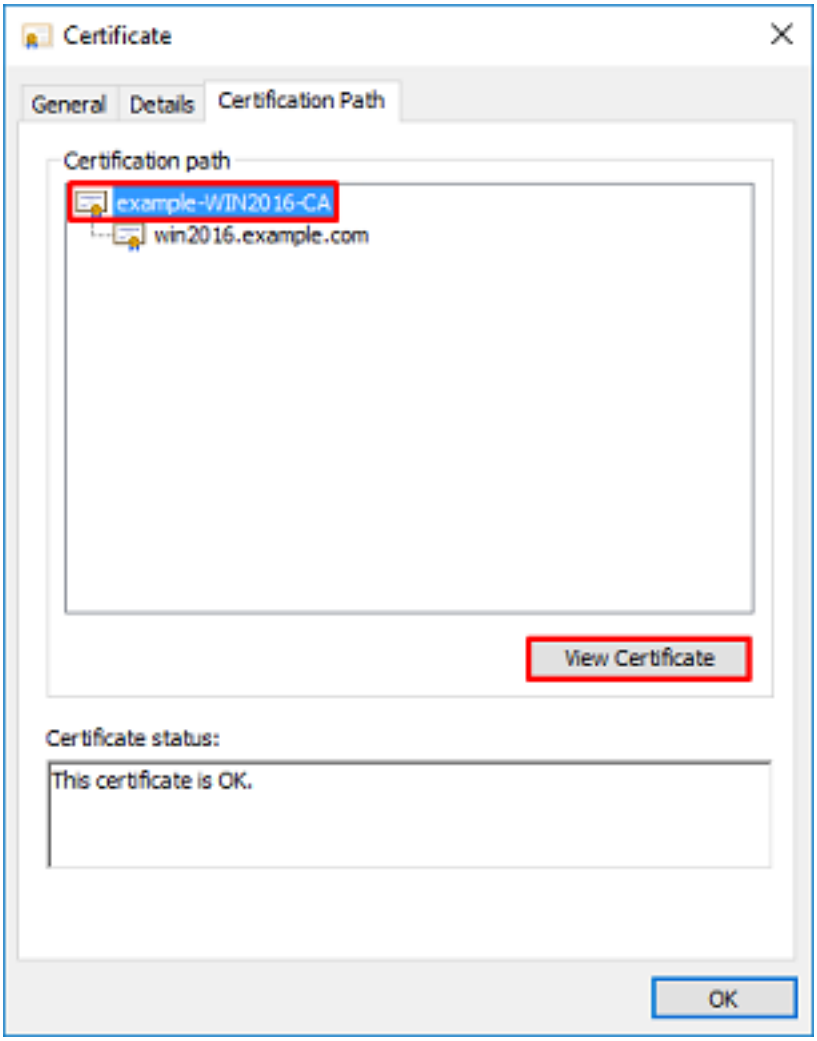

Certificate
General
Details
Certification Path
Show:
<All>
Field
Value
Subject
win2016.example.com
Public key
RSA (2048 Bits)
Public key parameters
05 00
Certificate Template Name
DomainController
Enhanced Key Usage
Client Authentication (1.3.6.1....
SMIME Capabilities
[1]SMIME Capability: Object I...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



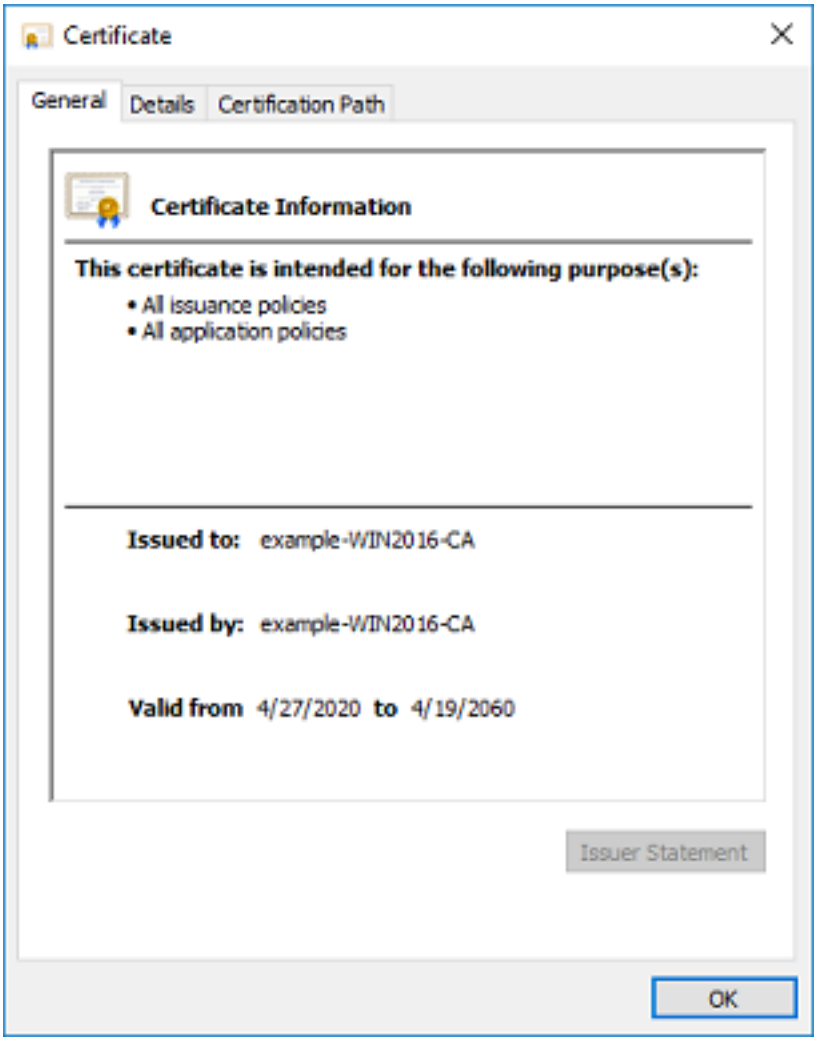
Sous **Utilisation améliorée des clés**, **Authentification du serveur** est présente.



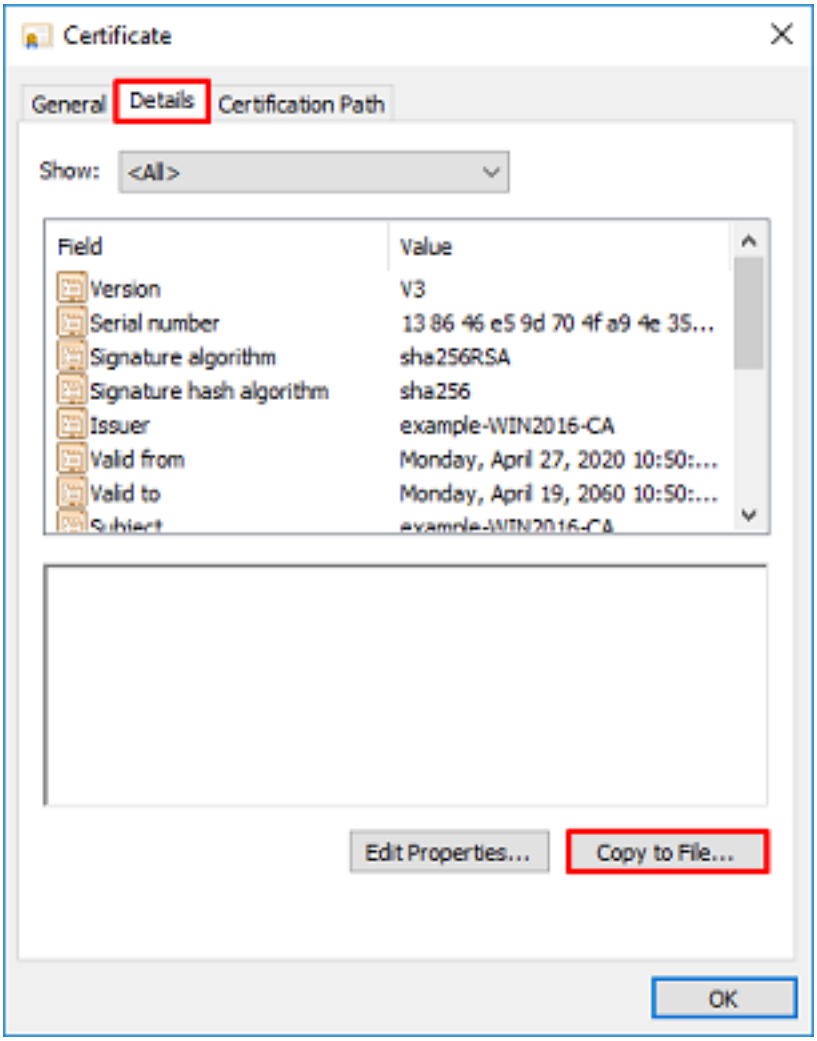
8. Une fois que cela a été confirmé, accédez à l'onglet **Chemin d'accès de la certification**. Cliquez sur le certificat supérieur qui doit être le certificat de l'autorité de certification racine, puis cliquez sur le bouton **Afficher le certificat**.



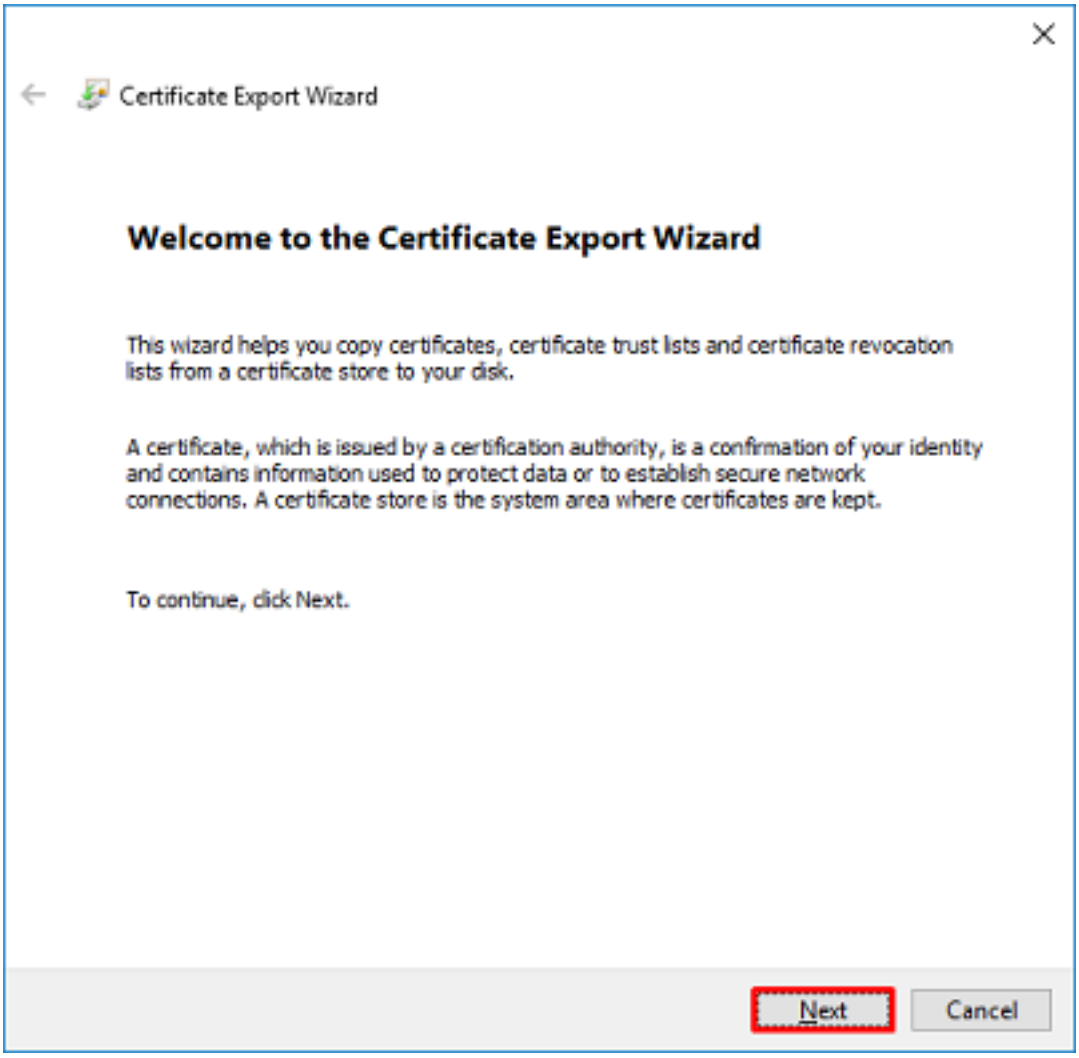
9. Ceci ouvrira les détails du certificat pour le certificat de l'autorité de certification racine.



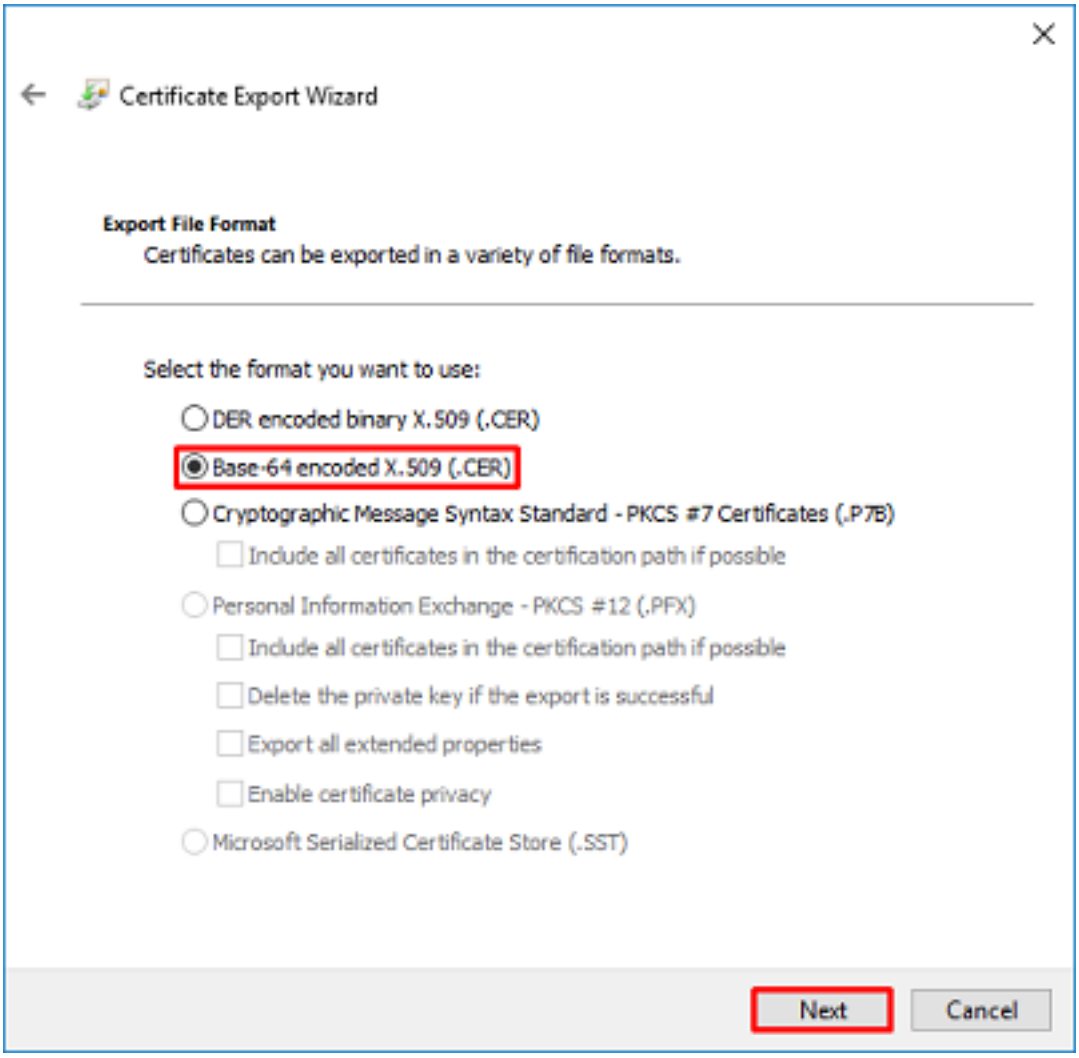
10. Ouvrez l'onglet **Détails**, puis cliquez sur **Copier dans un fichier...** comme le montre l'image.



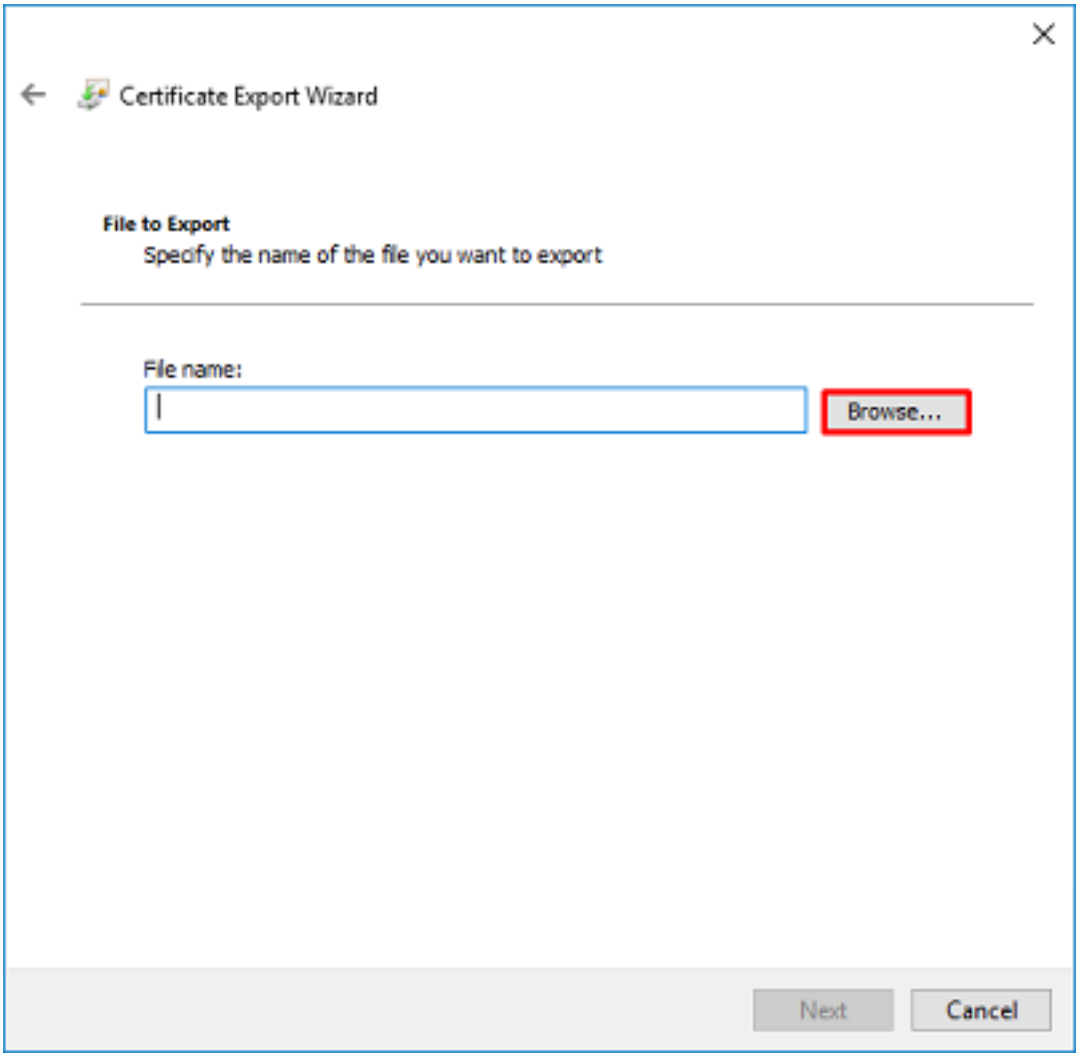
11. Naviguez dans l'Assistant Exportation de certificat qui exportera l'autorité de certification racine au format PEM.

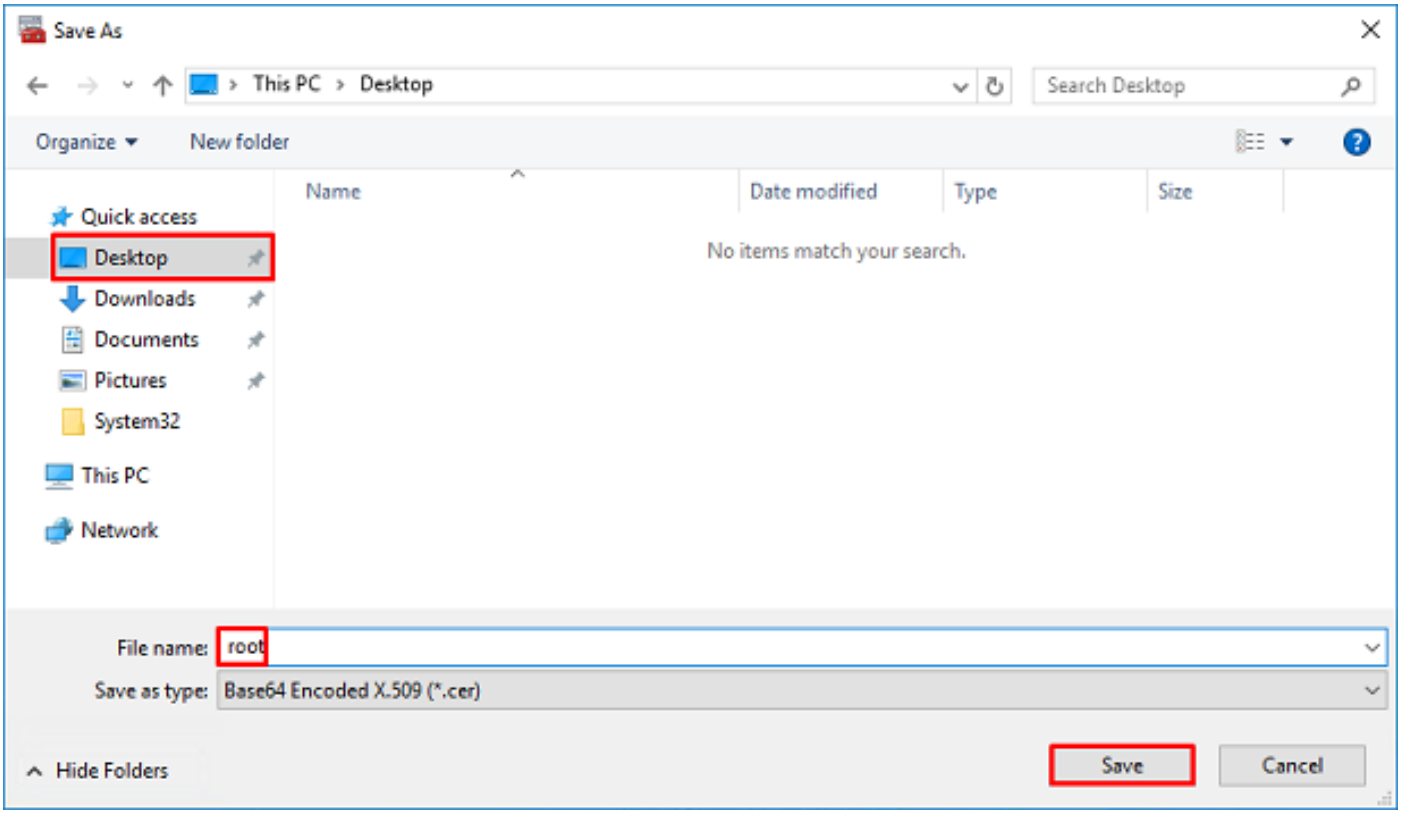


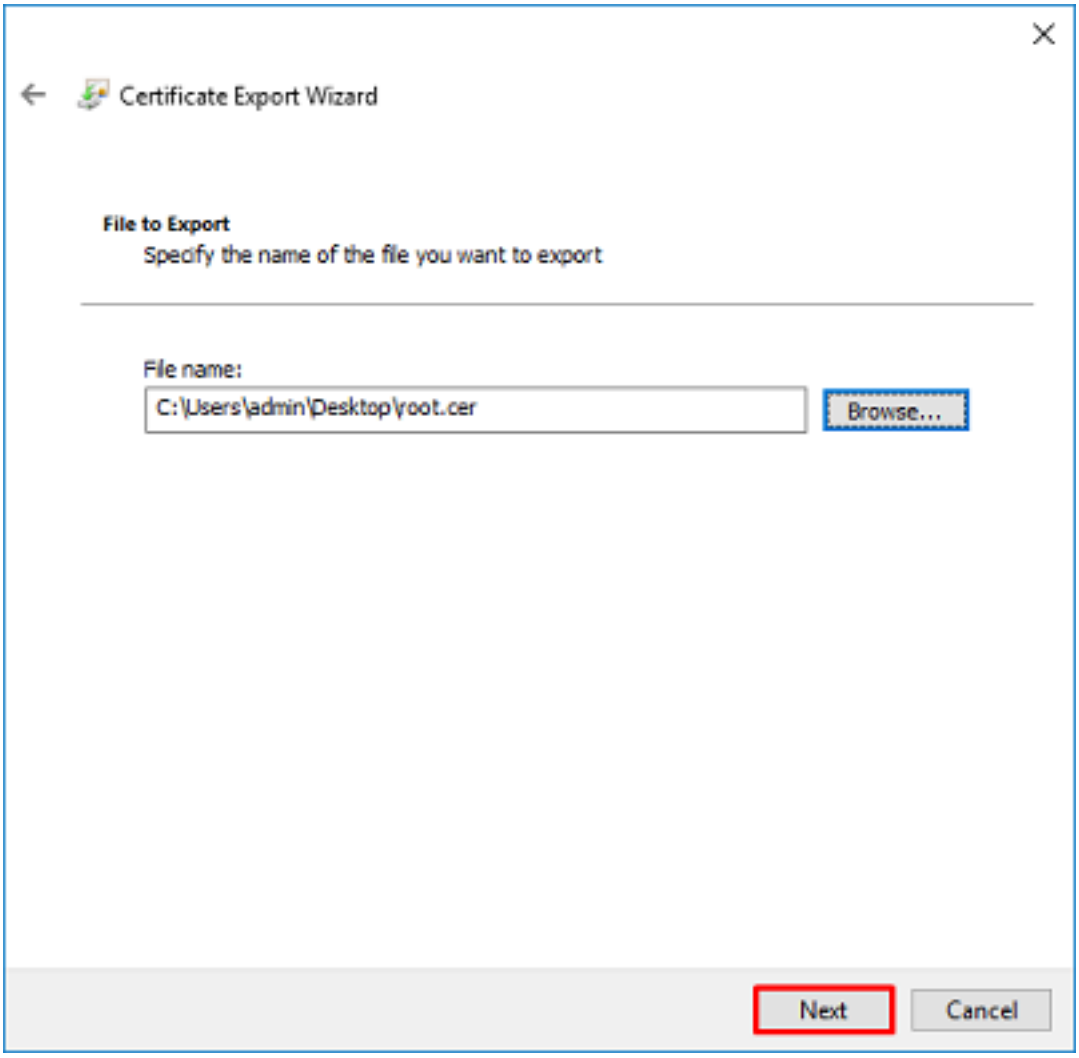
12. Sélectionnez **Base-64 encoded X.509**.



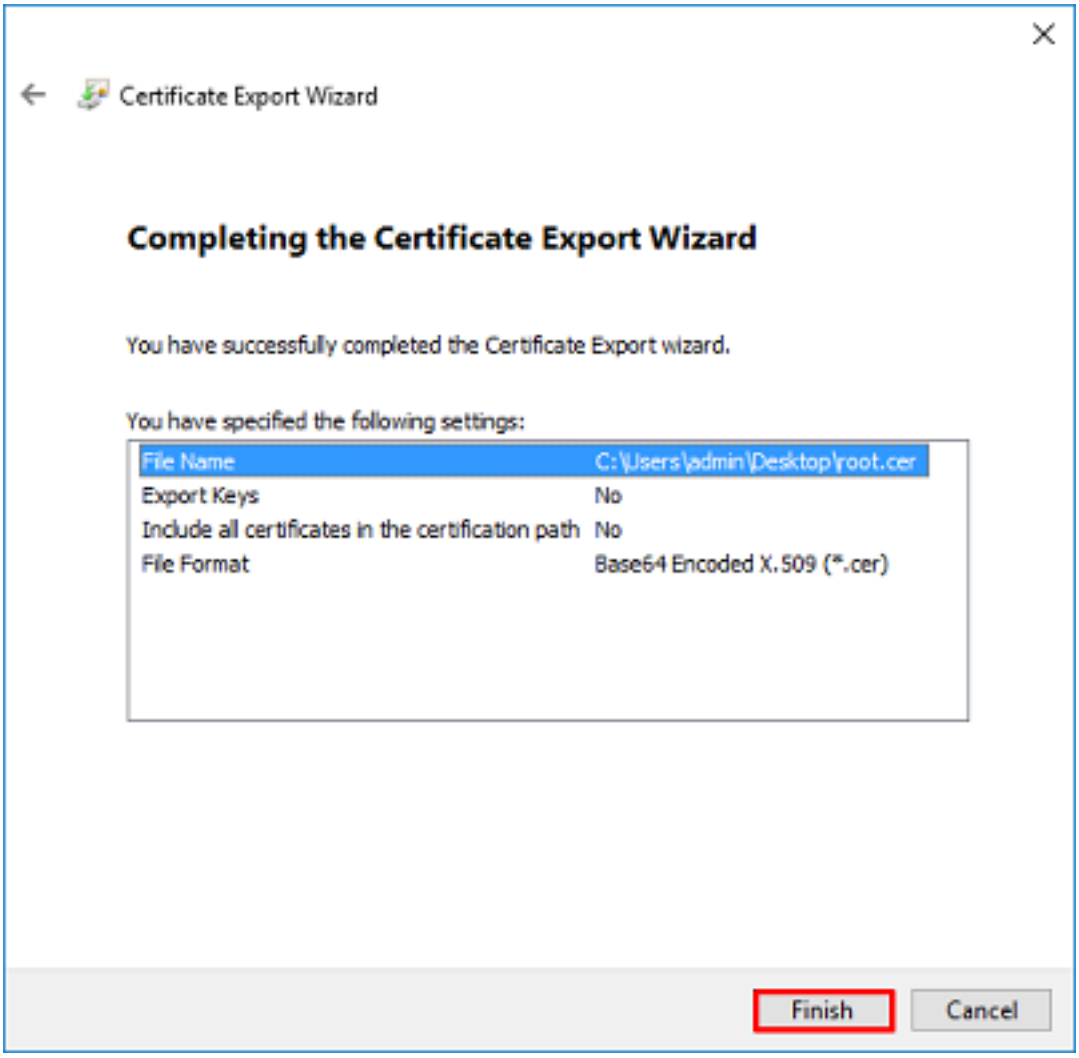
13. Sélectionnez le nom du fichier et l'emplacement vers lequel il sera exporté.


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



14. Cliquez sur Finish.



15. Maintenant, accédez à l'emplacement et ouvrez le certificat à l'aide d'un bloc-notes ou d'un autre éditeur de texte. Le certificat de format PEM s'affiche. Enregistrez ceci pour plus tard.

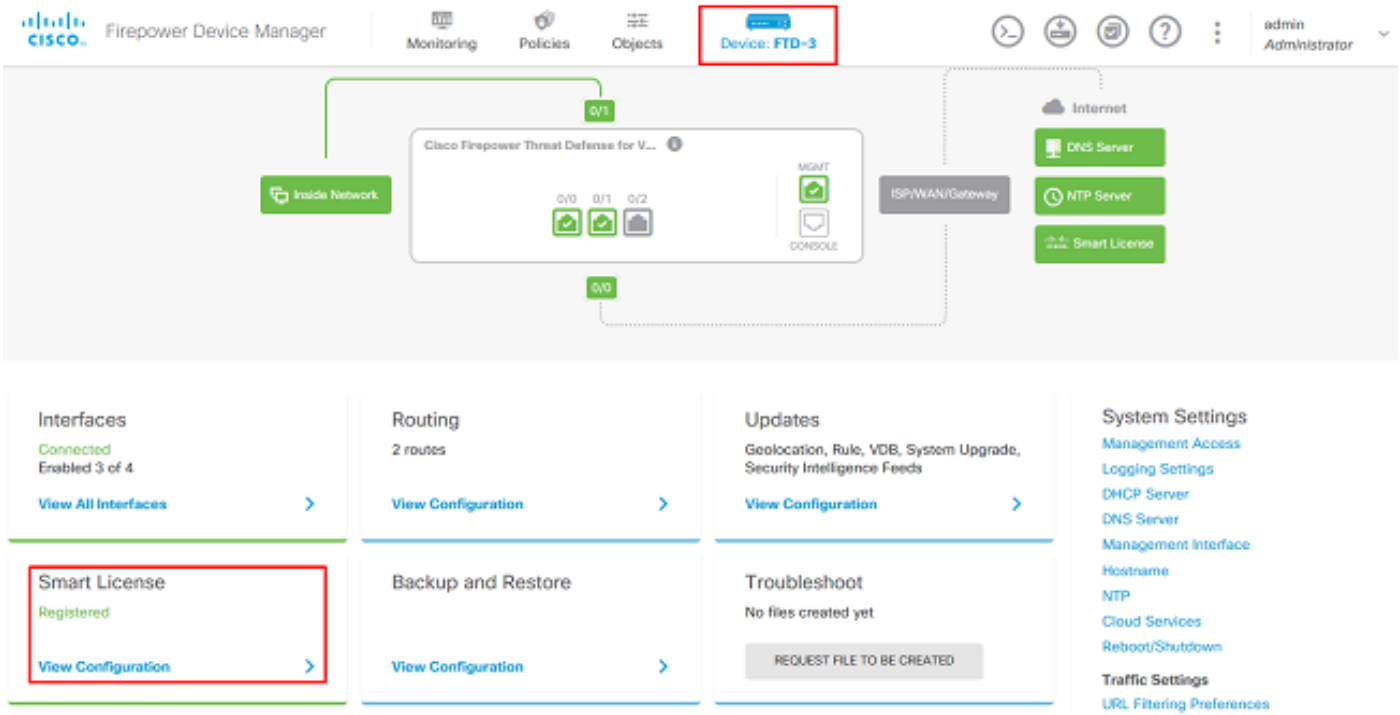
```
-----BEGIN CERTIFICATE-----
MIIDCDCCAfCgAwIBAgIQE4ZG5Z1wT6lONTjooEQyMTANBgkqhkiG9w0BAQsFADAd
MRswGQYDVQQDExJleGFtcGxlLVdJTjIwMTYtQ0EwIBcNMjAwNDI3MTQ1MDU5WhgP
MjA2MDA0MTkxNDUwNTlaMB0xGzAZBgNVBAMTEmV4YW1wbGUtV0lOMjAxNi1DQTCC
ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAI8ghT719NzSQpoQPh0YT67b
Ya+PngsxMyvkewP33QLTAWw1HW1Tb9Mk5BDWOItTaVsgHwPBfd++M+bLn3AiZnHV
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-----
```

Configurations FDM

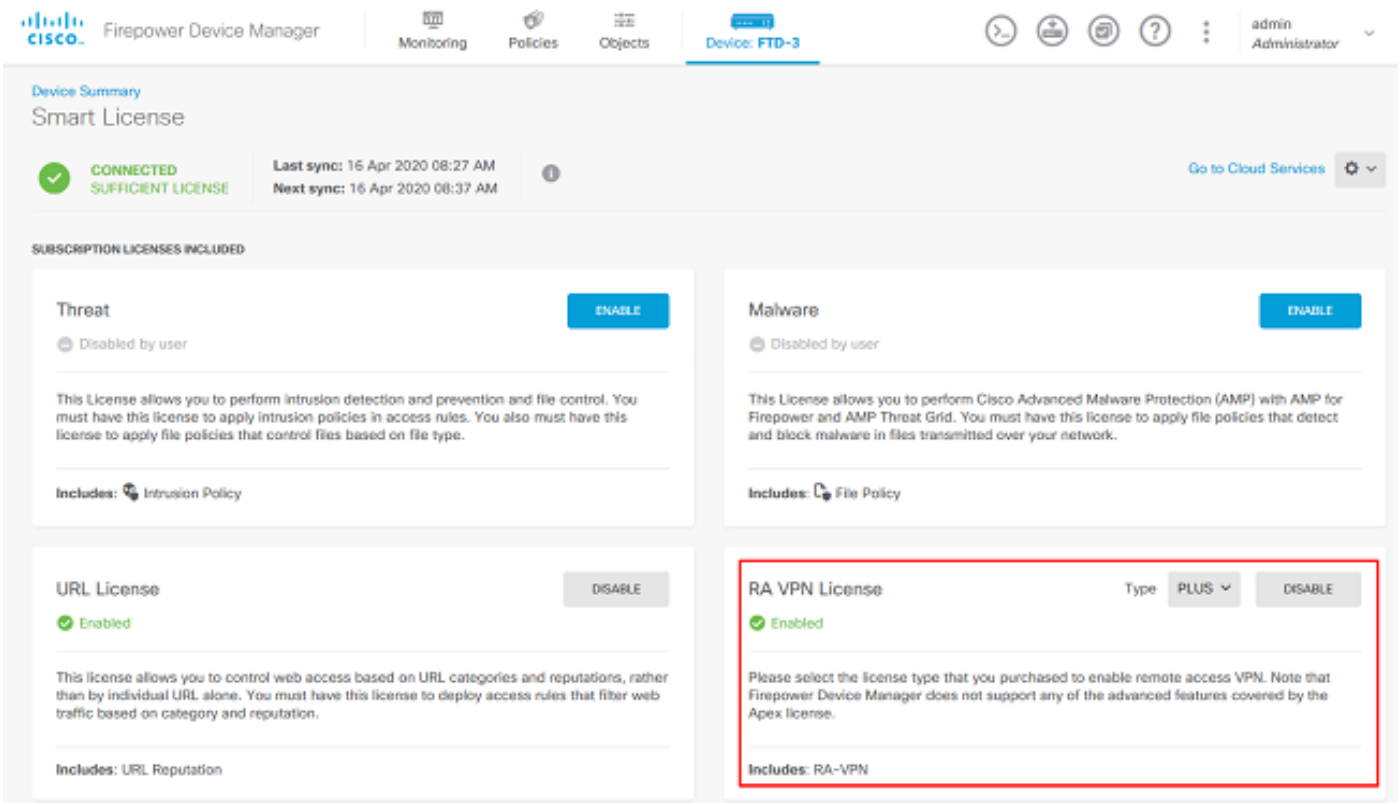
Vérifier la licence

Pour configurer AnyConnect sur FDM, le FTD devra 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 **Device > Smart License** comme indiqué dans l'image.



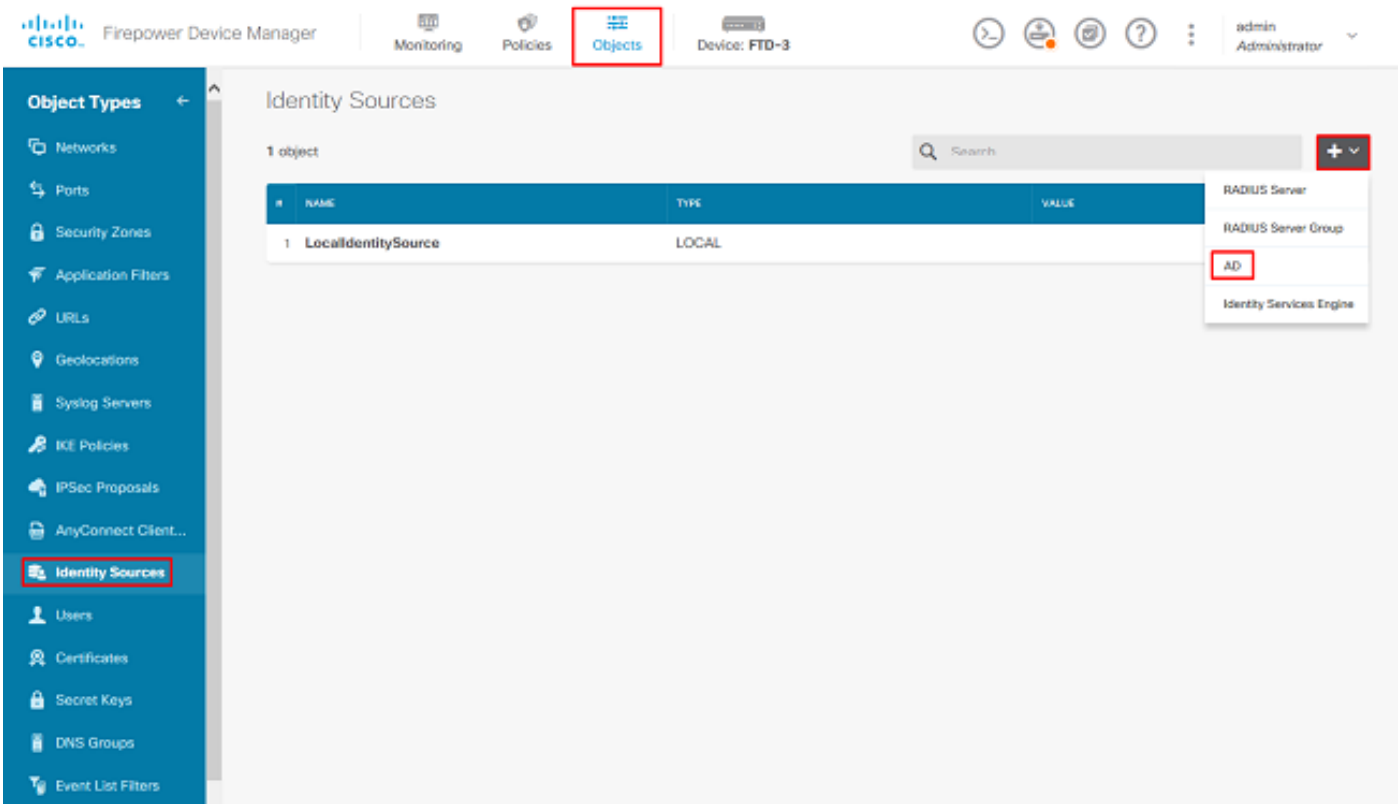
2. Vérifiez que le FTD est enregistré sur le serveur de licences Smart et que la licence AnyConnect Plux, Apex ou VPN Only est activée.



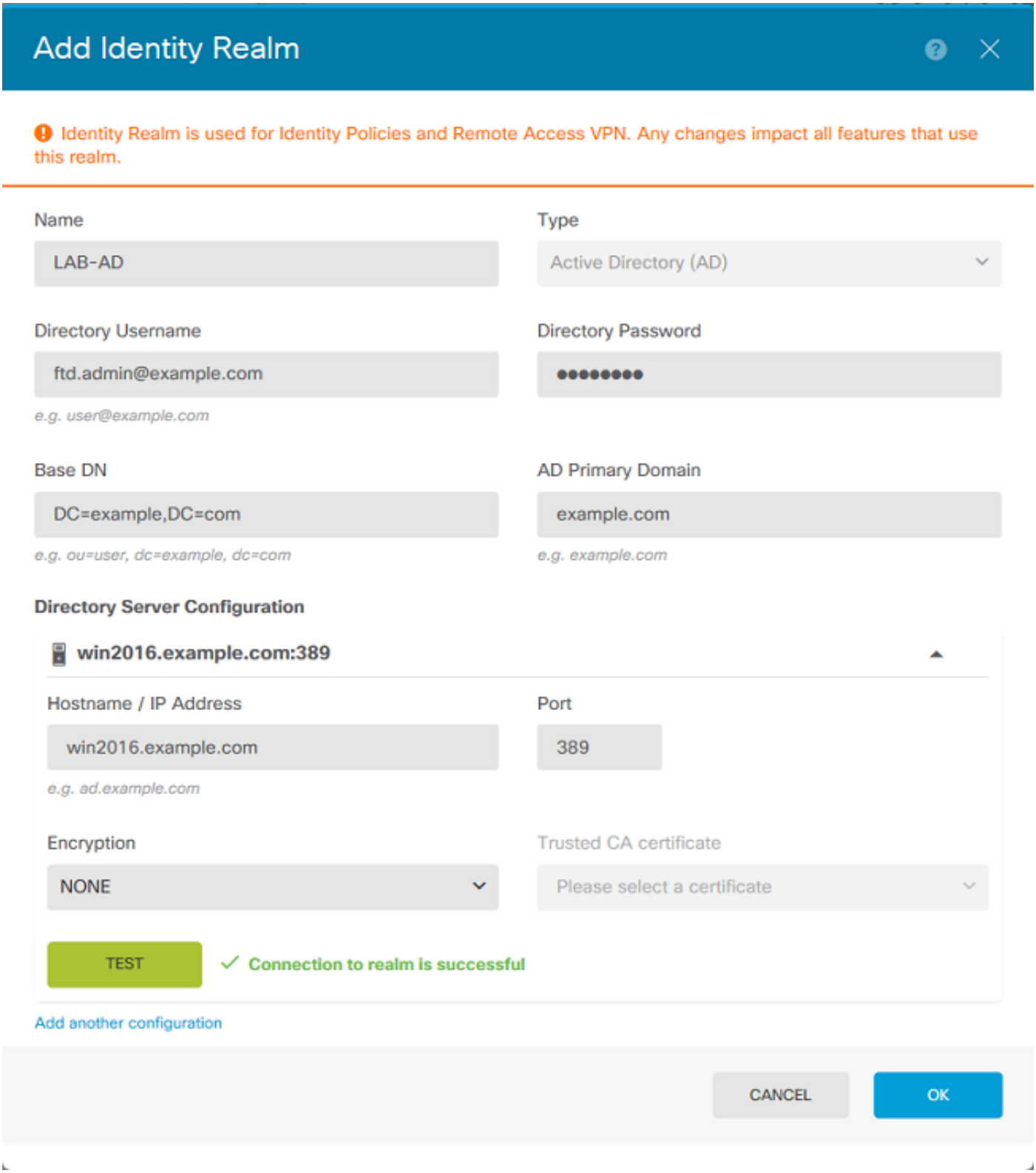
Configurer la source d'identité AD

1. Accédez à **Objets > Sources d'identité**, puis cliquez sur le symbole **+** et sélectionnez **AD** comme

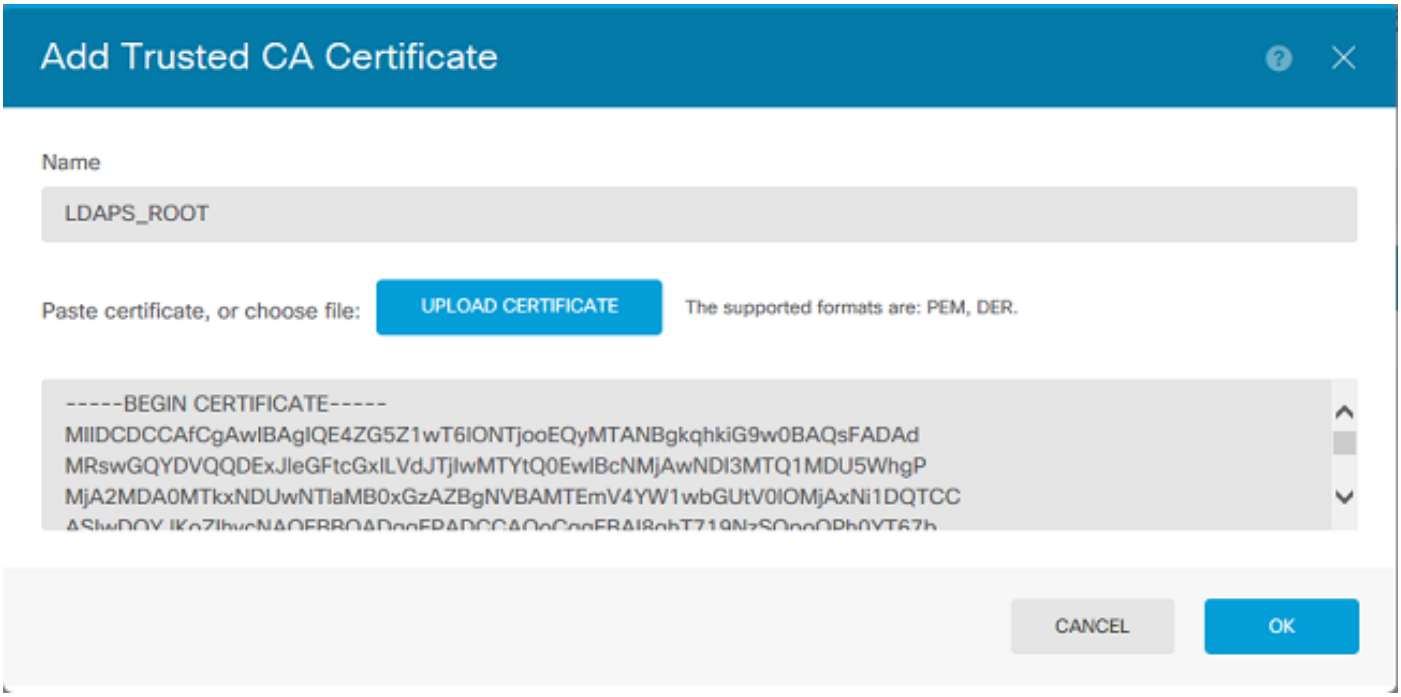
indiqué dans l'image.

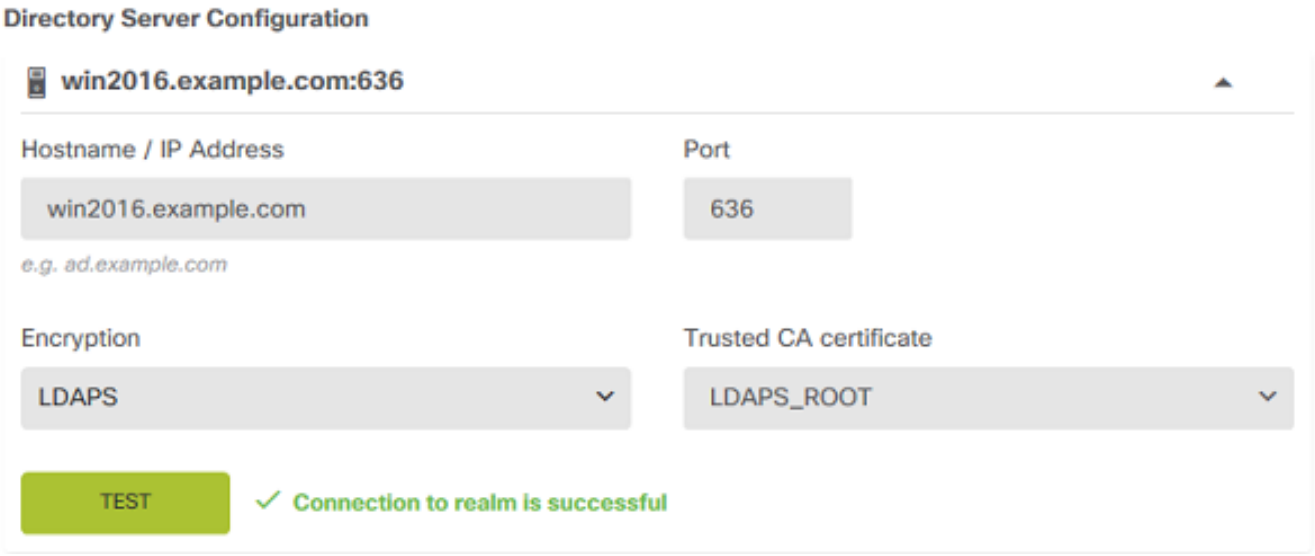


2. Complétez les paramètres appropriés pour le serveur Active Directory avec les informations collectées précédemment. Si un nom d'hôte (FQDN) est utilisé pour le serveur Microsoft au lieu d'une adresse IP, assurez-vous de créer un groupe DNS approprié sous **Objets > Groupe DNS**. Appliquez ensuite ce groupe DNS au FTD en naviguant vers **Device > System Settings > DNS Server**, en appliquant le groupe DNS sous l'**interface de gestion** et **l'interface de données**, puis spécifiez l'interface de sortie appropriée pour les requêtes DNS. Cliquez sur le bouton **Test** afin de vérifier une configuration et une accessibilité réussies à partir de l'interface de gestion de FTD. Puisque ces tests sont initiés à partir de l'interface de gestion du FTD et non par l'une des interfaces routables configurées sur le FTD (telles que interne, externe, dmz), une connexion réussie (ou échouée) ne garantit pas le même résultat pour l'authentification AnyConnect puisque les demandes d'authentification LDAP AnyConnect seront lancées à partir de l'une des interfaces routables du FTD. Pour plus d'informations sur le test des connexions LDAP à partir du FTD, consultez les sections Test AAA et Packet Capture dans la zone Dépannage.



Si LDAPS ou STARTTLS est utilisé, sélectionnez le chiffrement approprié, puis sélectionnez le certificat de CA de confiance. Si l'autorité de certification racine n'est pas déjà ajoutée, cliquez sur **Créer un nouveau certificat d'autorité de certification de confiance**. Indiquez un nom pour le certificat de l'autorité de certification racine, puis collez le certificat de l'autorité de certification racine au format PEM collecté précédemment.

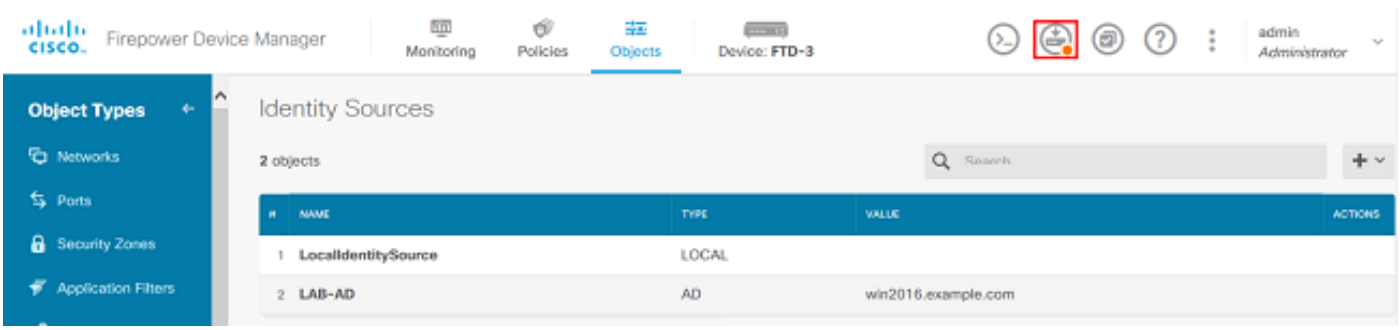




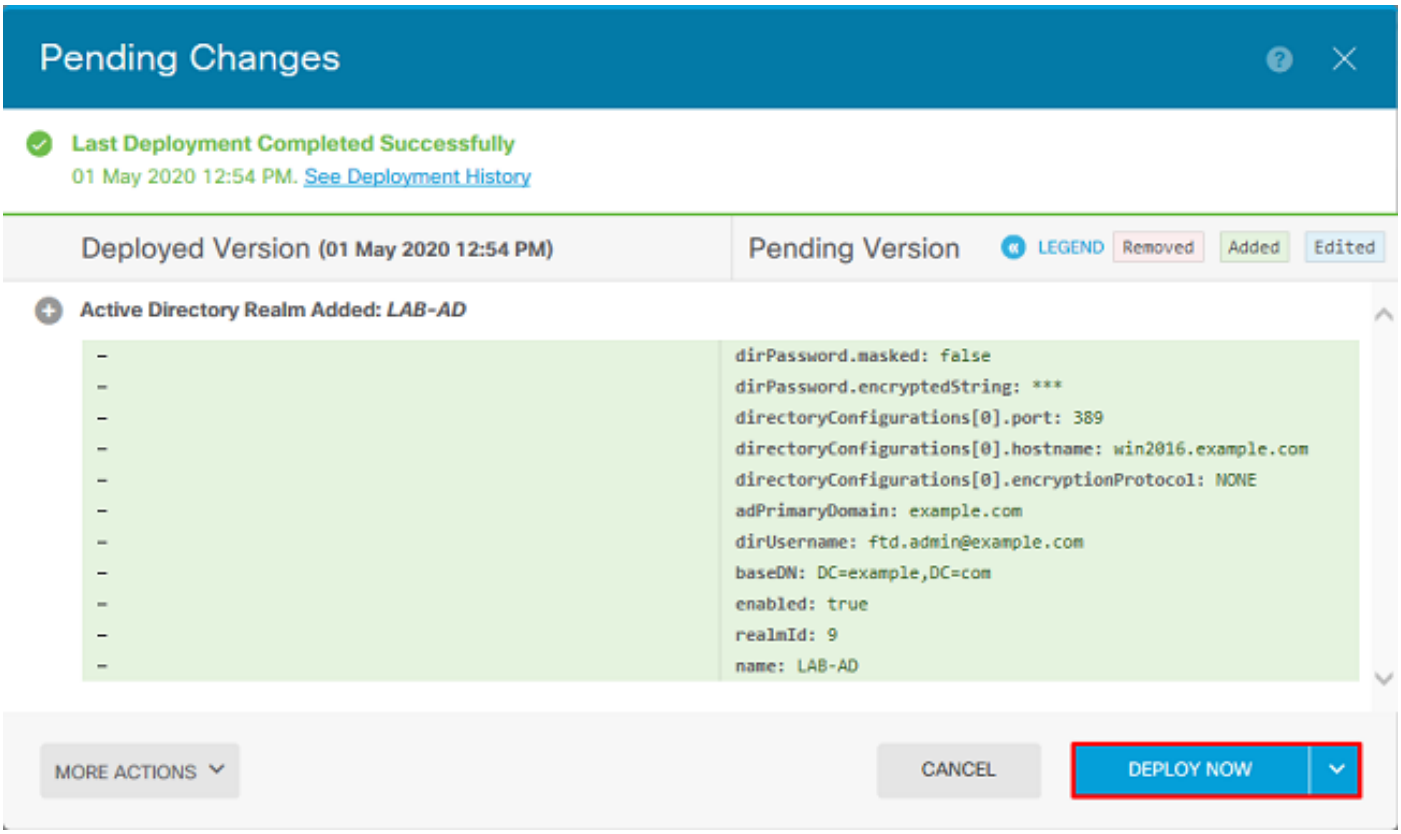
Dans cette configuration, ces valeurs ont été utilisées :

- Name : LAB-AD
- Nom d'utilisateur du répertoire : ftd.admin@example.com
- DN de base : DC=exemple, DC=com
- Domaine principal AD : example.com
- Nom d'hôte/Adresse IP : win2016.example.com
- Port : 389

3. Cliquez sur le bouton **Modifications en attente** en haut à droite, comme illustré dans l'image.



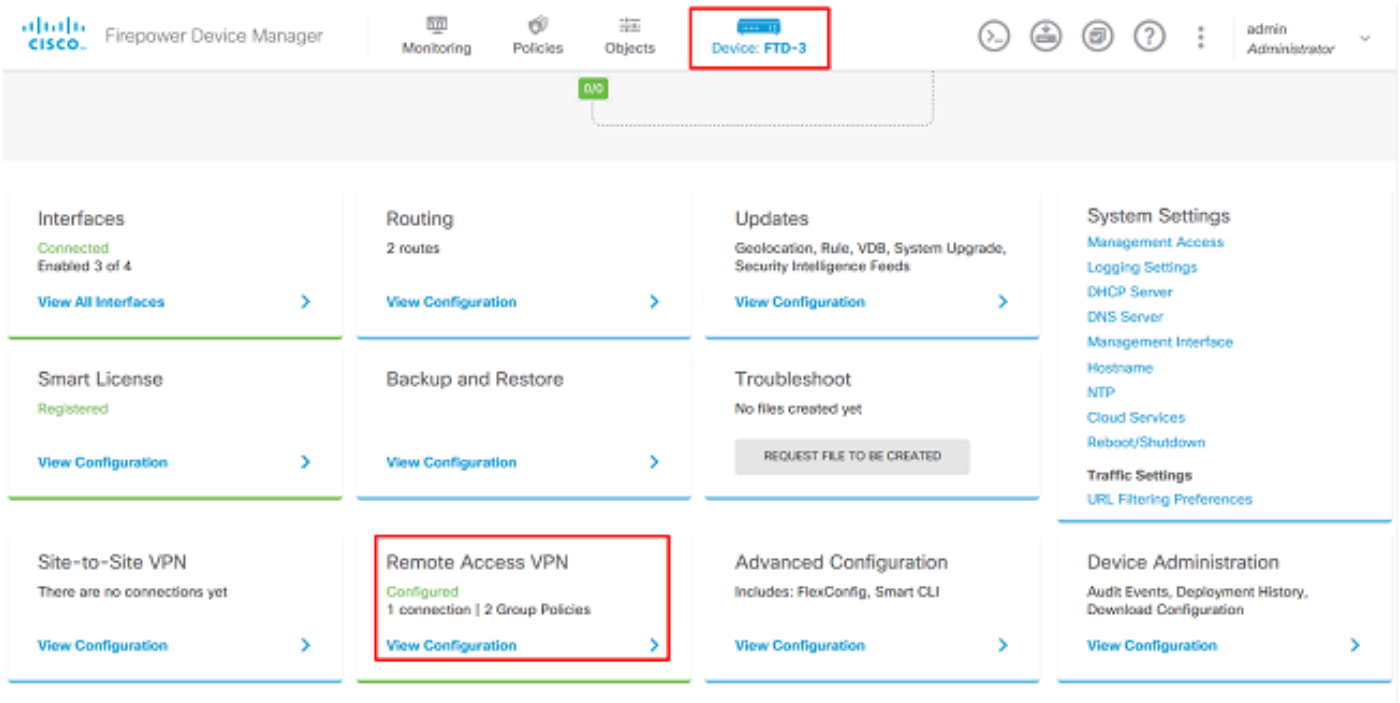
4. Cliquez sur le bouton **Déployer maintenant**.



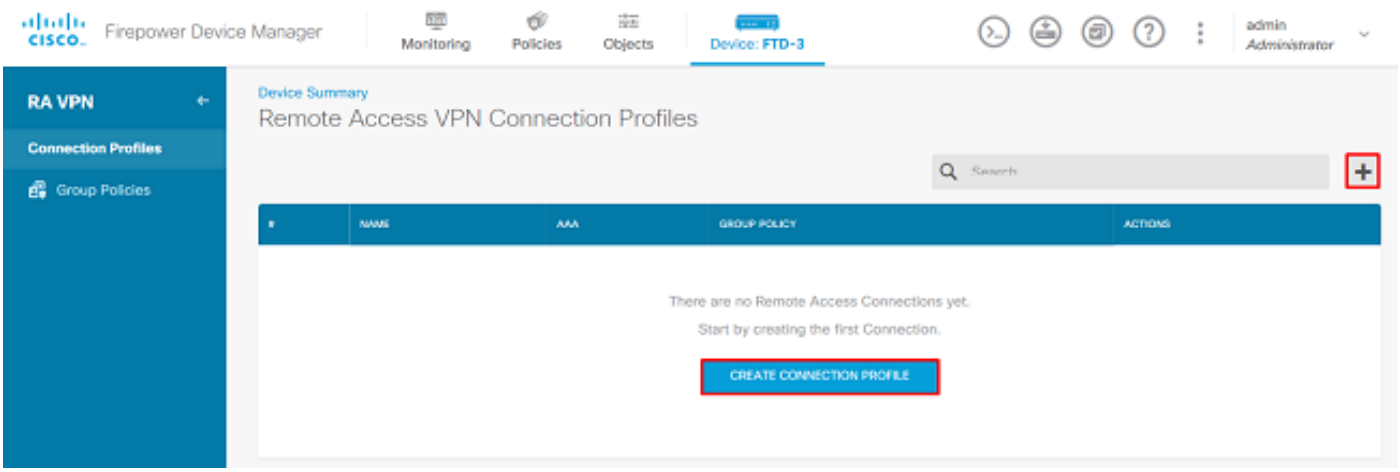
Configurer AnyConnect pour l'authentification AD

Pour utiliser la source d'identité AD configurée, elle doit être appliquée à la configuration AnyConnect.

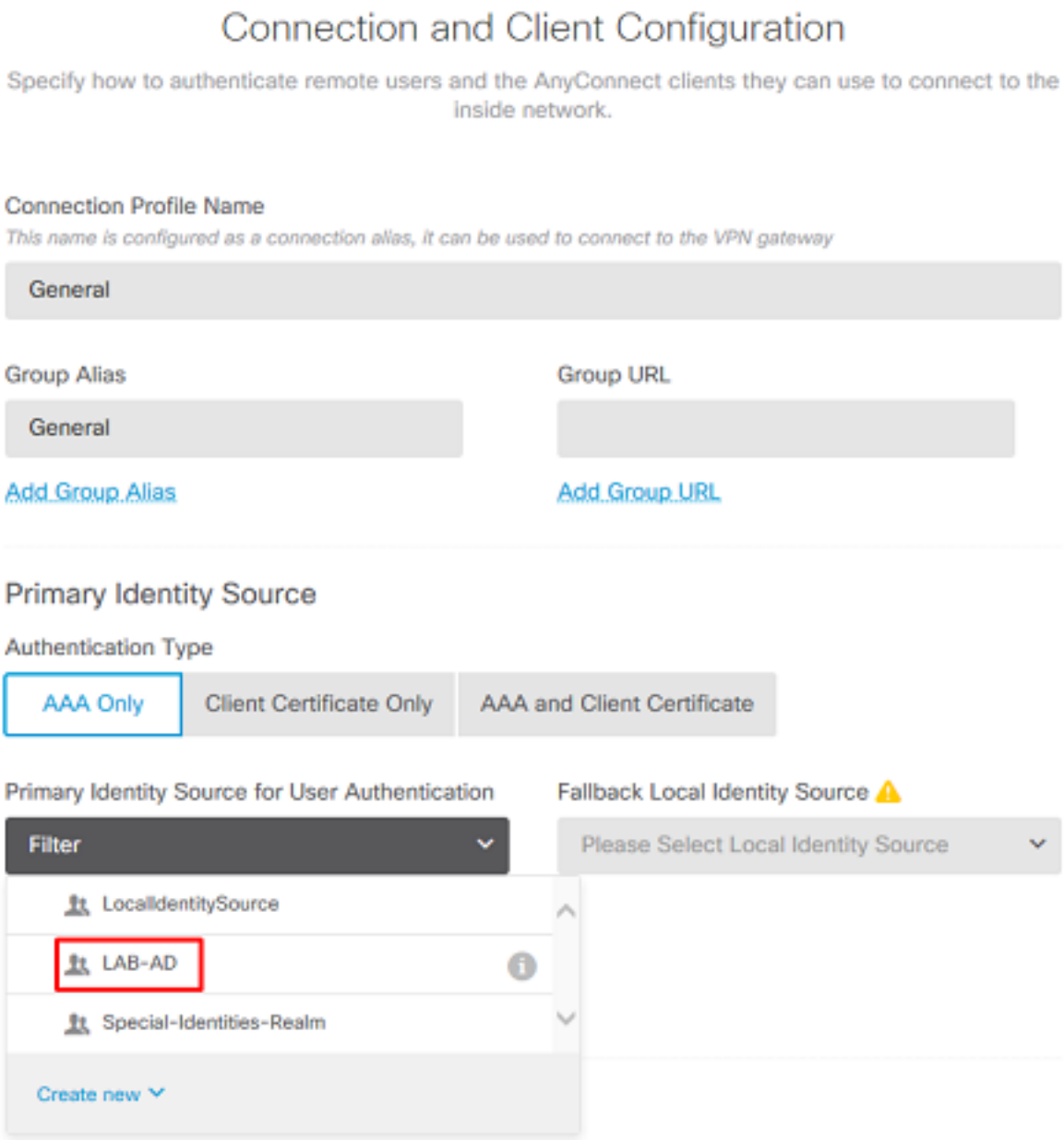
1. Accédez à **Device > Remote Access VPN** comme indiqué dans l'image.

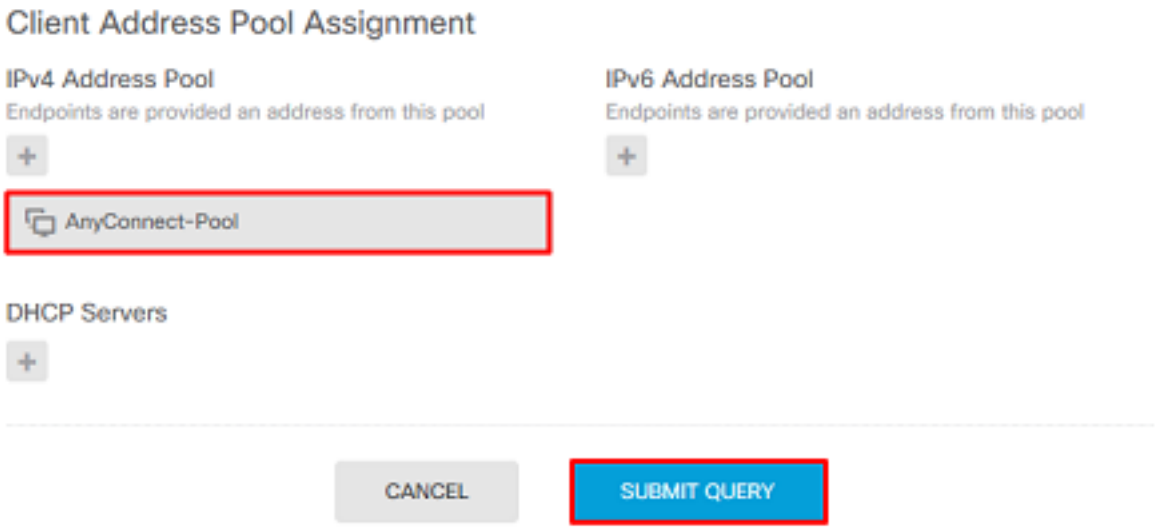


2. Cliquez sur le symbole **+** ou sur le bouton **Créer un profil de connexion** comme indiqué dans l'image.

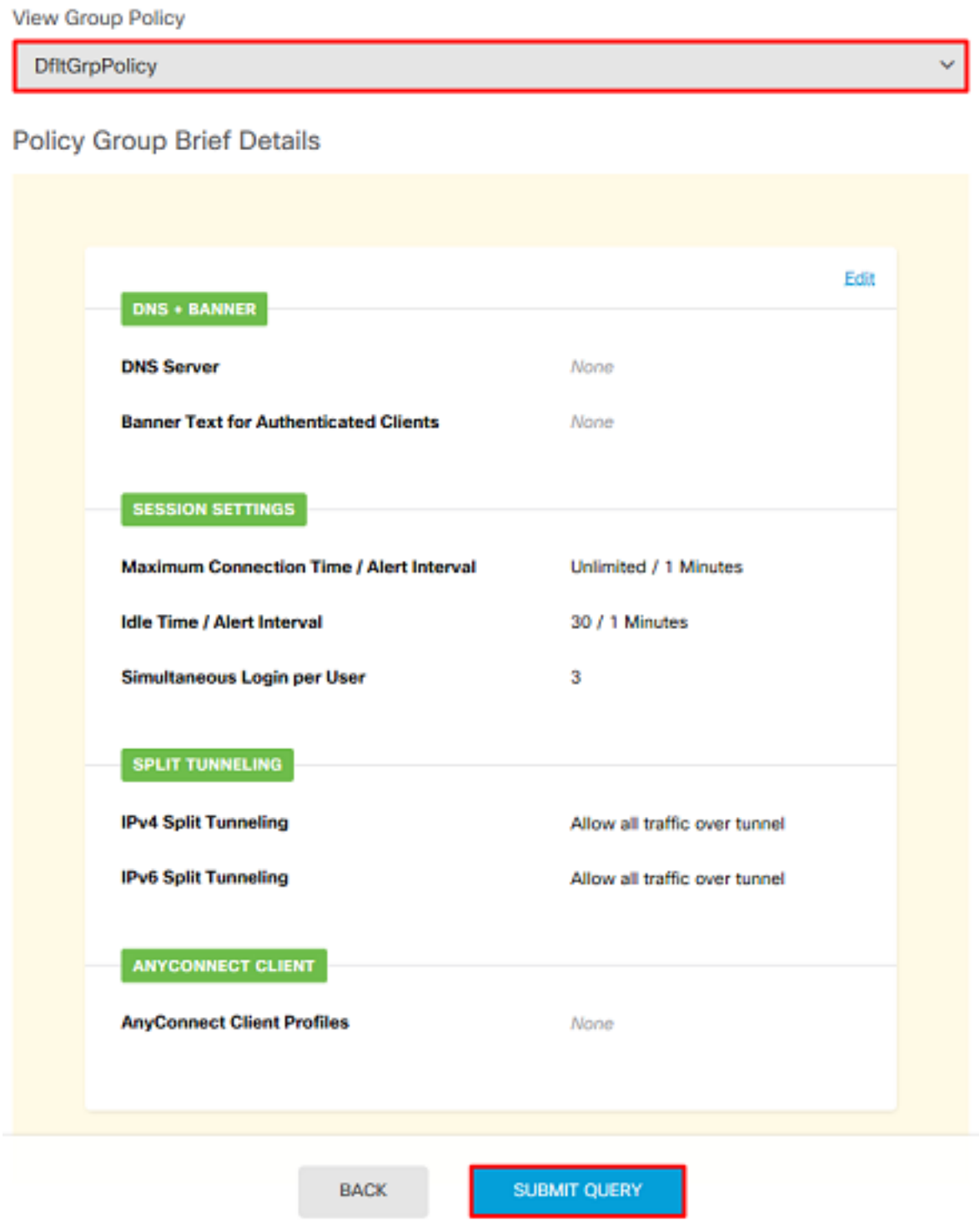


3. Dans la section Connection and Client Configuration, sélectionnez la source d'identité AD créée précédemment. Configurez les valeurs appropriées pour les autres sections, notamment le nom du profil de connexion et l'affectation du pool d'adresses client. Cliquez sur **Soumettre la requête** lorsque vous avez terminé.

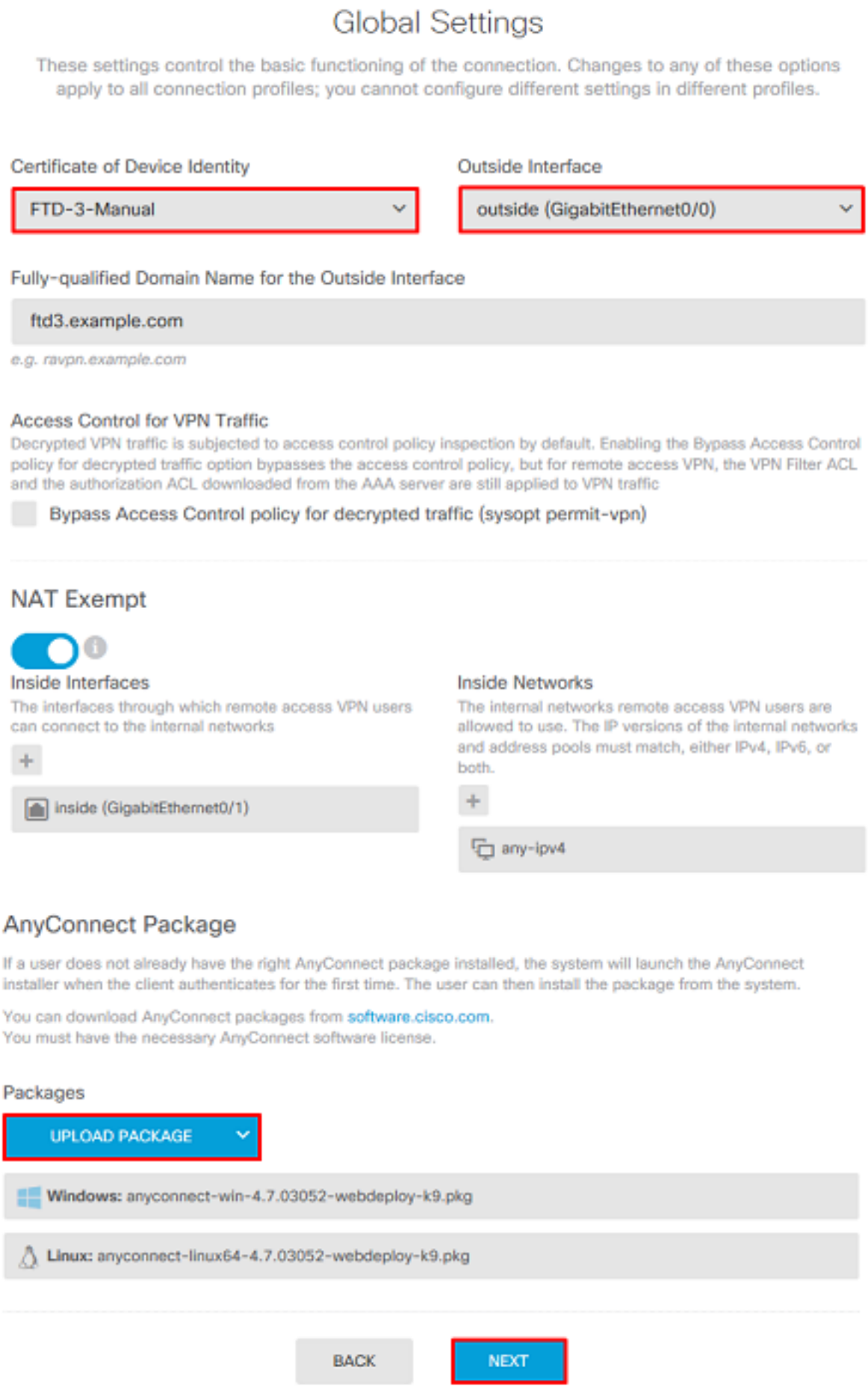




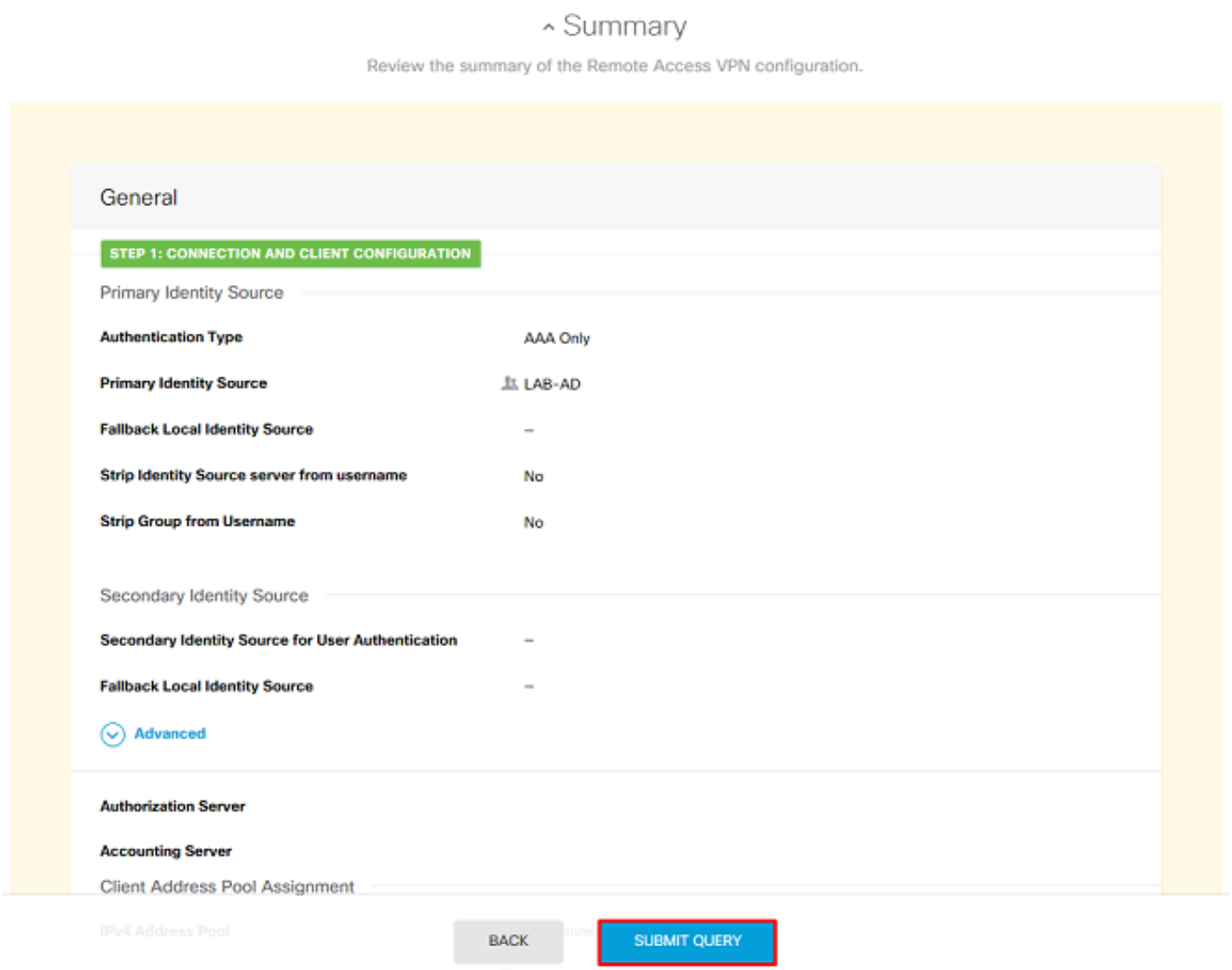
4. Dans la section Expérience utilisateur à distance, sélectionnez la stratégie de groupe appropriée. Par défaut, la **DfltGrpPolicy** sera utilisée ; cependant, il est possible d'en créer une autre.



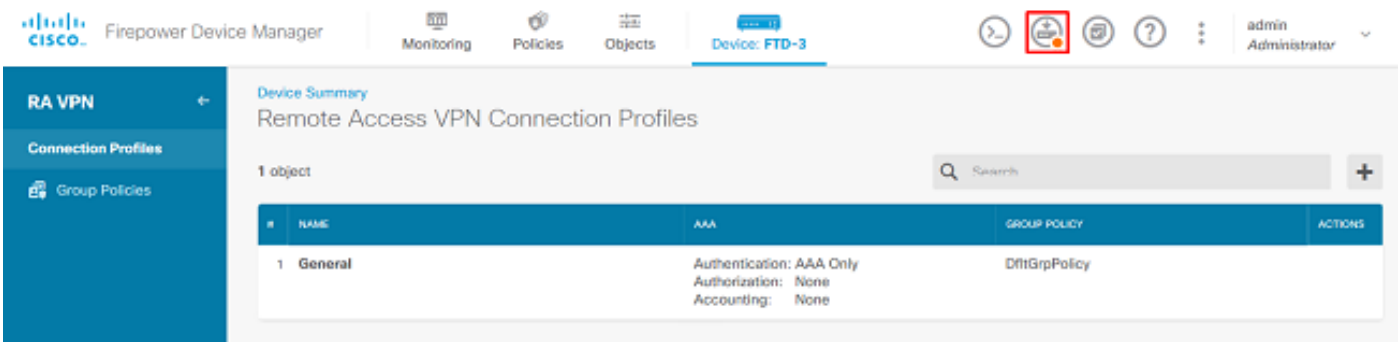
5. Dans la section Global Settings, spécifiez au minimum le certificat SSL, l'interface externe et les packages AnyConnect. Si aucun certificat n'a été créé précédemment, un certificat auto-signé par défaut (DefaultInternalCertificate) peut être sélectionné, mais un message de certificat de serveur non approuvé s'affiche. La stratégie de contrôle d'accès de contournement pour le trafic déchiffré (sysopt permit-vpn) doit être désactivée afin que les règles de stratégie d'accès aux identités des utilisateurs prennent effet ultérieurement. NAT Exempt peut également être configuré ici. Dans cette configuration, tout le trafic ipv4 provenant de l'interface interne qui se rend aux adresses IP du client AnyConnect est différent de la NAT. Pour les configurations plus complexes telles que l'épinglage externe à externe, des règles NAT supplémentaires devront être créées dans le cadre de la stratégie NAT. Les packages AnyConnect sont disponibles sur le site d'assistance Cisco : https://software.cisco.com/download/home. Une licence Plus ou Apex valide est requise pour télécharger le package AnyConnect.



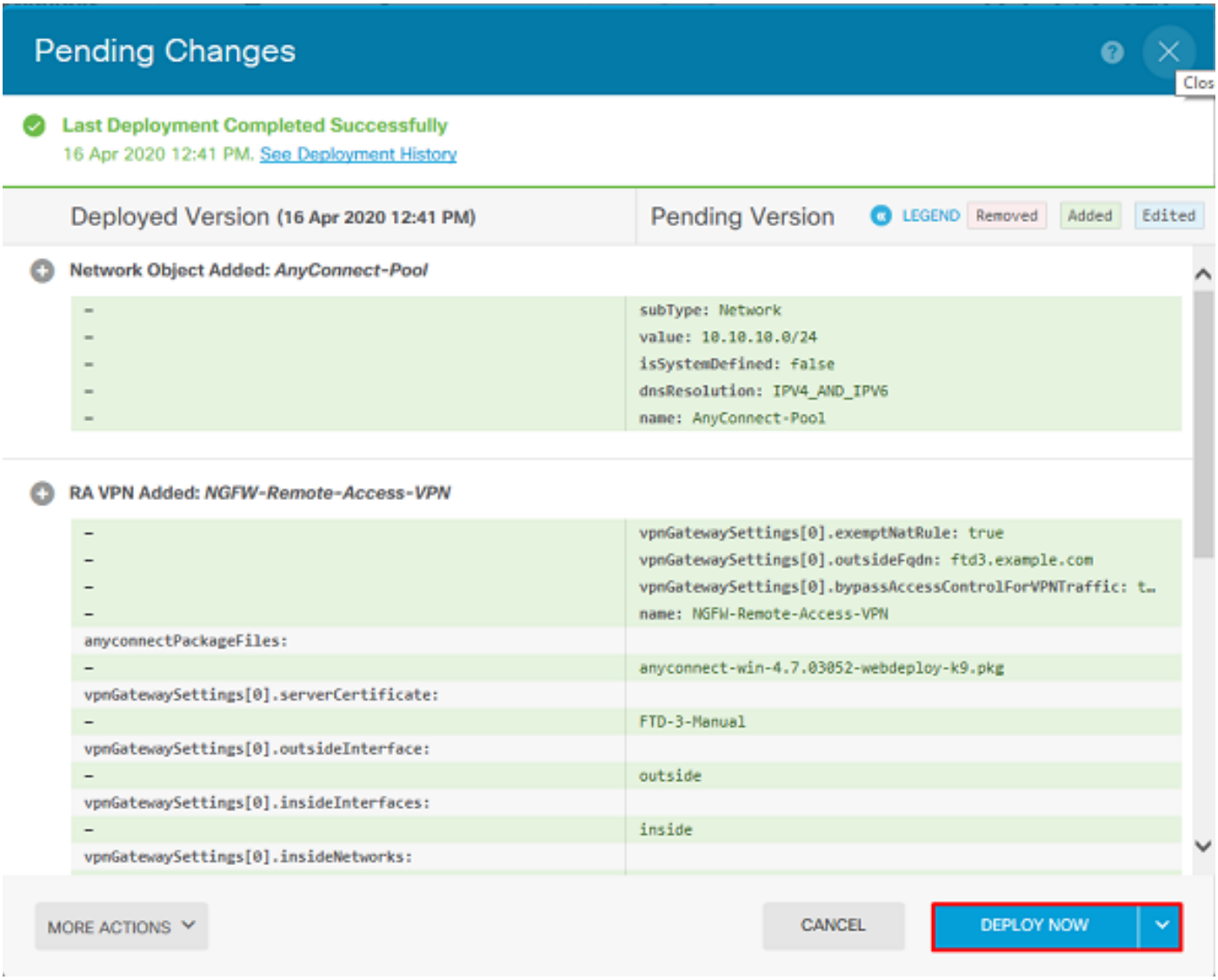
6. Dans la section Résumé, vérifiez que AnyConnect est configuré correctement, puis cliquez sur **Envoyer la requête**.



7. Cliquez sur le bouton **Modifications en attente** en haut à droite, comme illustré dans l'image.



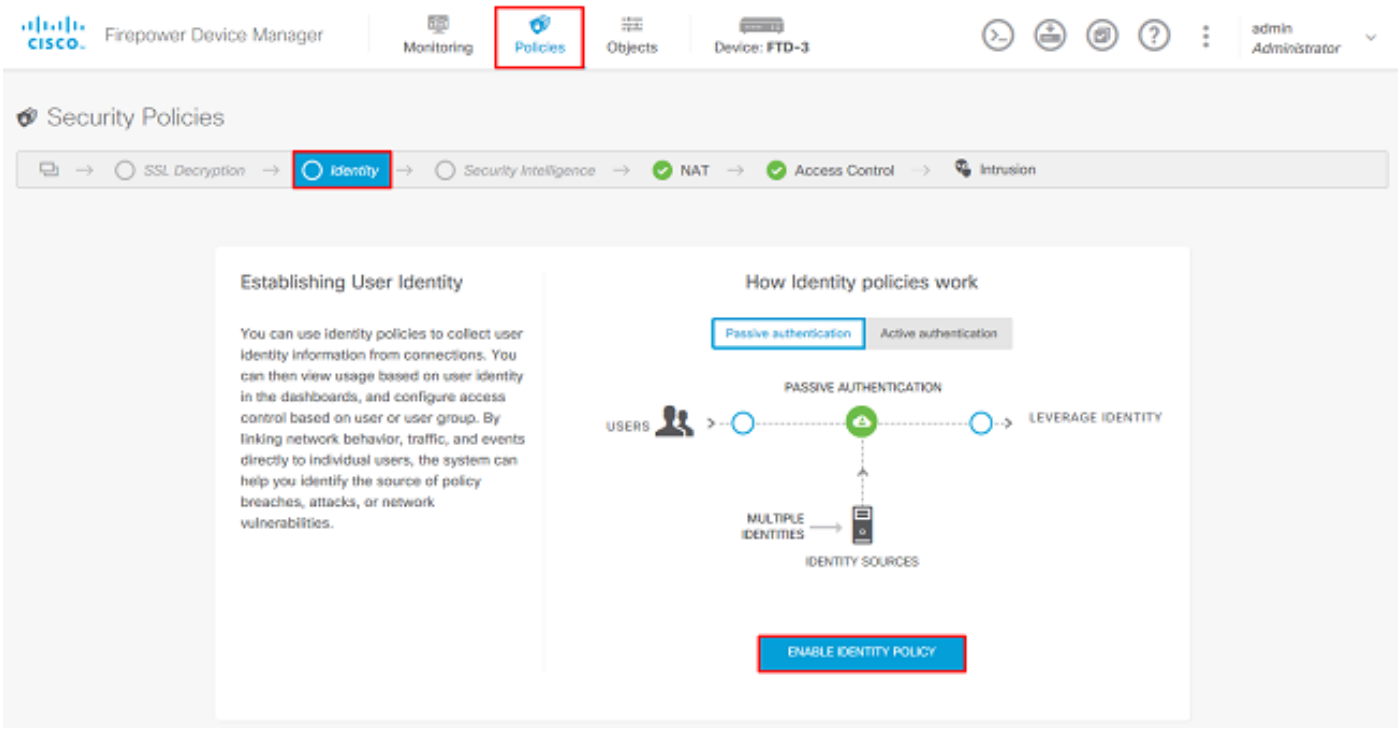
8. Cliquez sur **Déployer maintenant**.



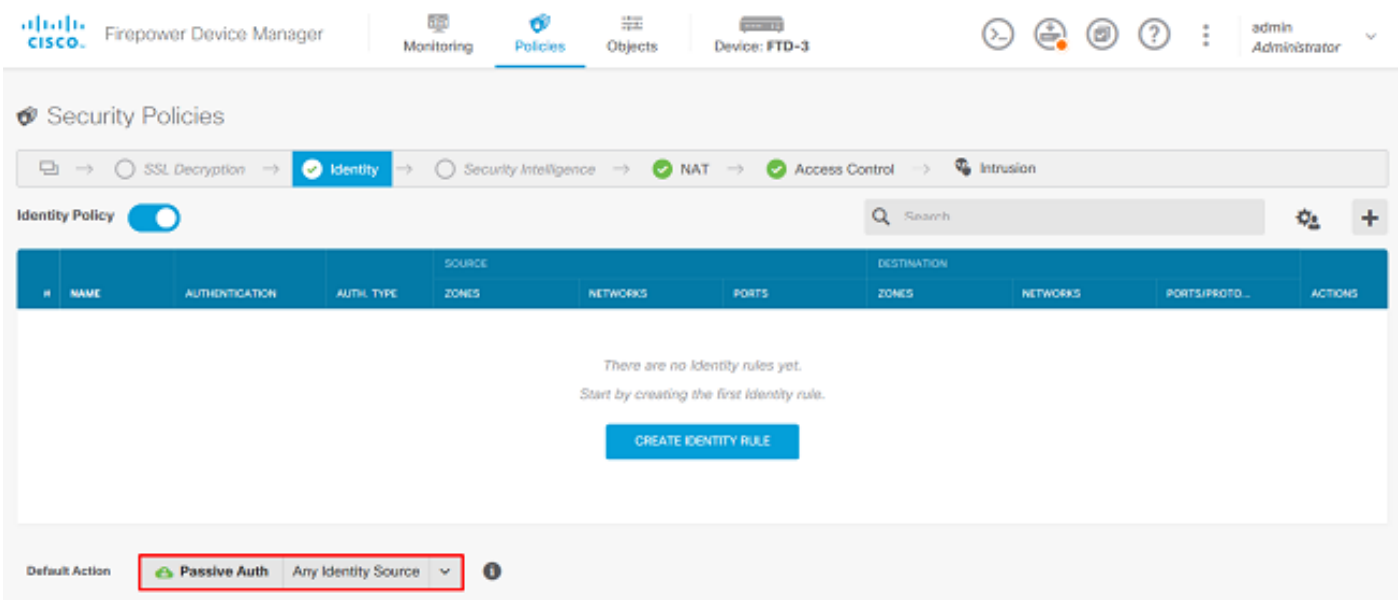
Activer la stratégie d'identité et configurer les stratégies de sécurité pour l'identité de l'utilisateur

Àce stade, les utilisateurs d'AnyConnect doivent être en mesure de se connecter correctement, mais peuvent ne pas pouvoir accéder à des ressources spécifiques. Cette étape active l'identité de l'utilisateur afin que seuls les utilisateurs des administrateurs AnyConnect puissent se connecter aux ressources internes à l'aide du protocole RDP et que seuls les utilisateurs du groupe Utilisateurs AnyConnect puissent se connecter aux ressources internes à l'aide du protocole HTTP.

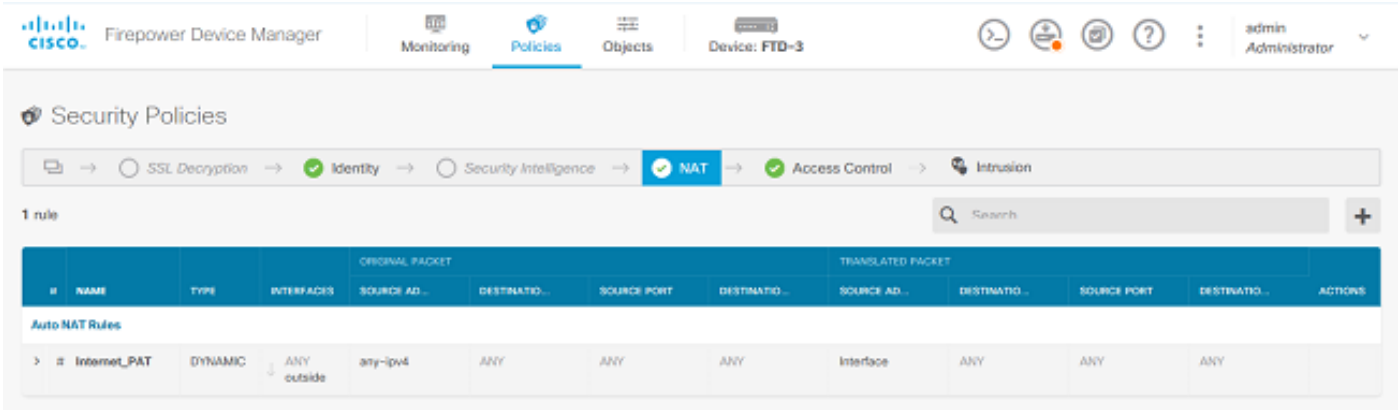
1. Accédez à **Politiques > Identité** et cliquez sur **Activer la stratégie d'identité**.



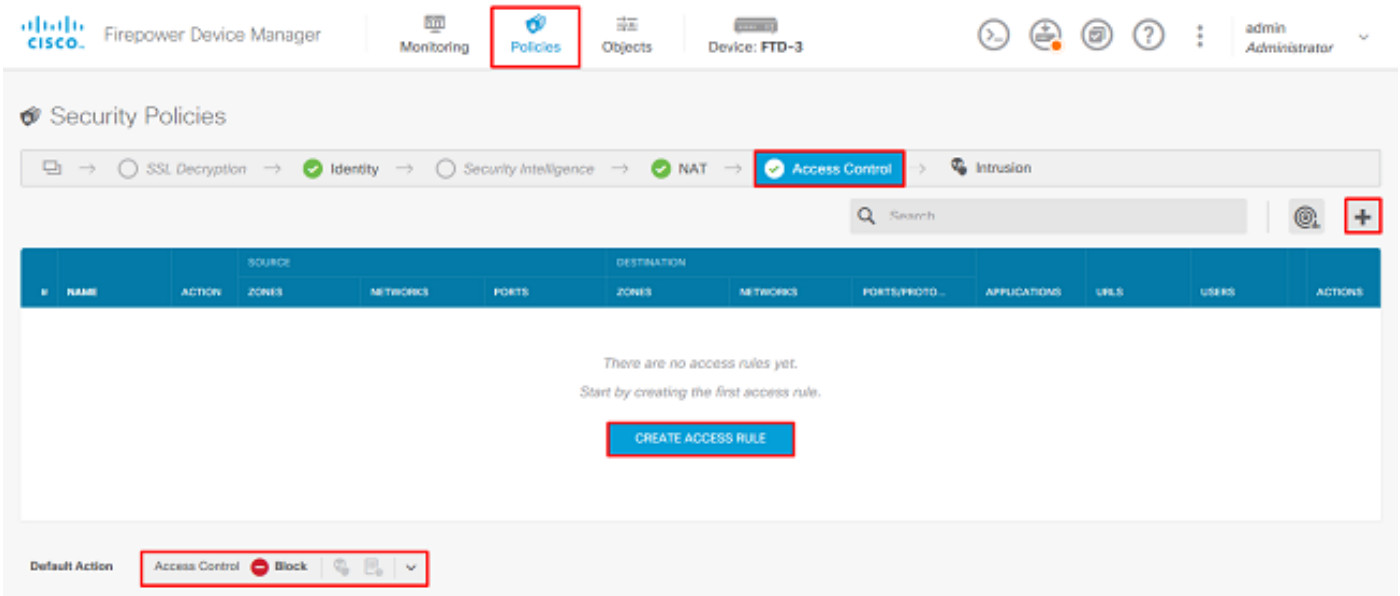
Pour cette configuration, aucune autre configuration n'est nécessaire et l'action par défaut est suffisante.



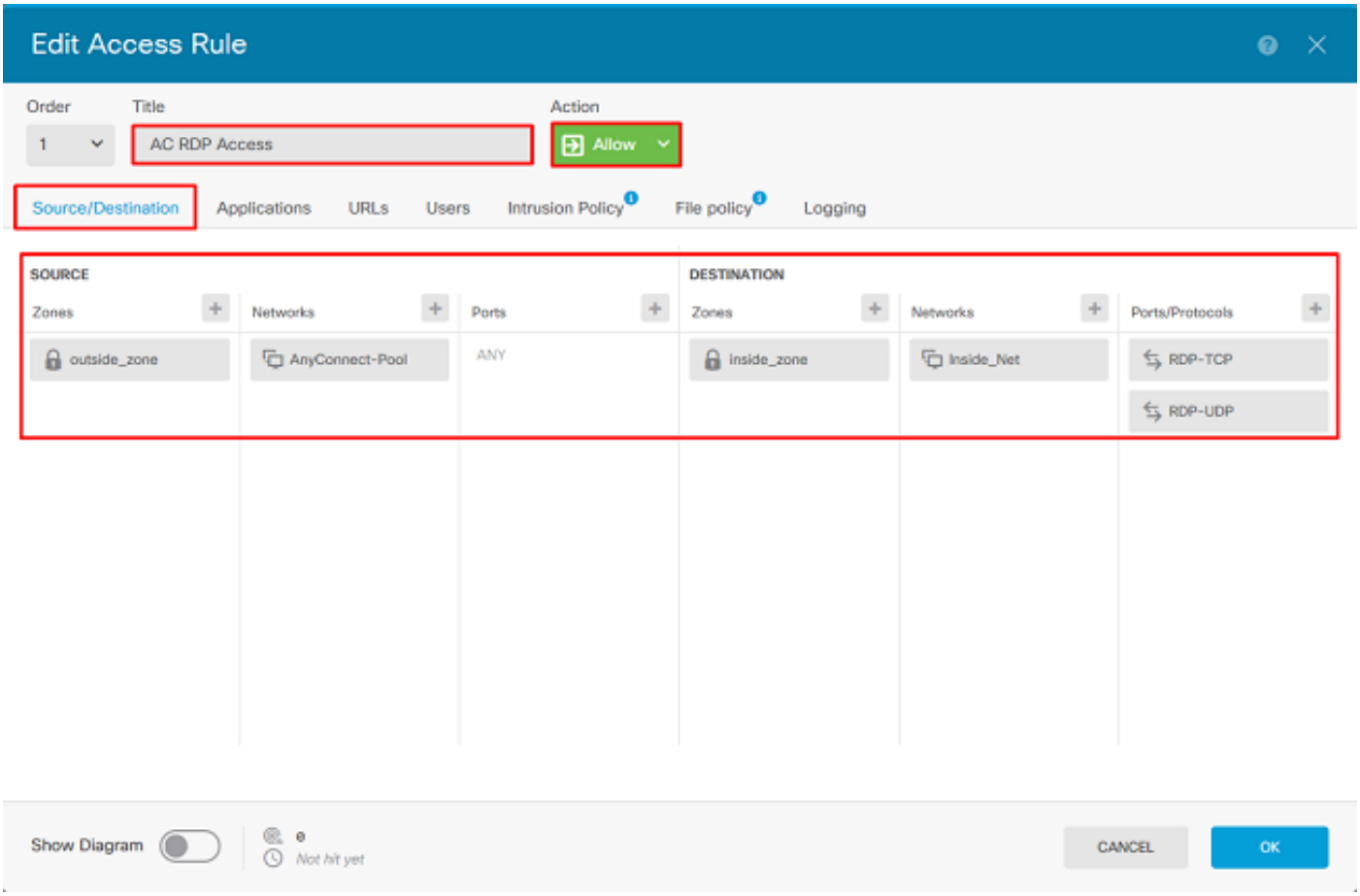
2. Accédez à **Policies > NAT** et assurez-vous que NAT est configuré correctement. Si l'exception NAT configurée dans les paramètres AnyConnect est suffisante, aucune configuration supplémentaire ne sera nécessaire ici.



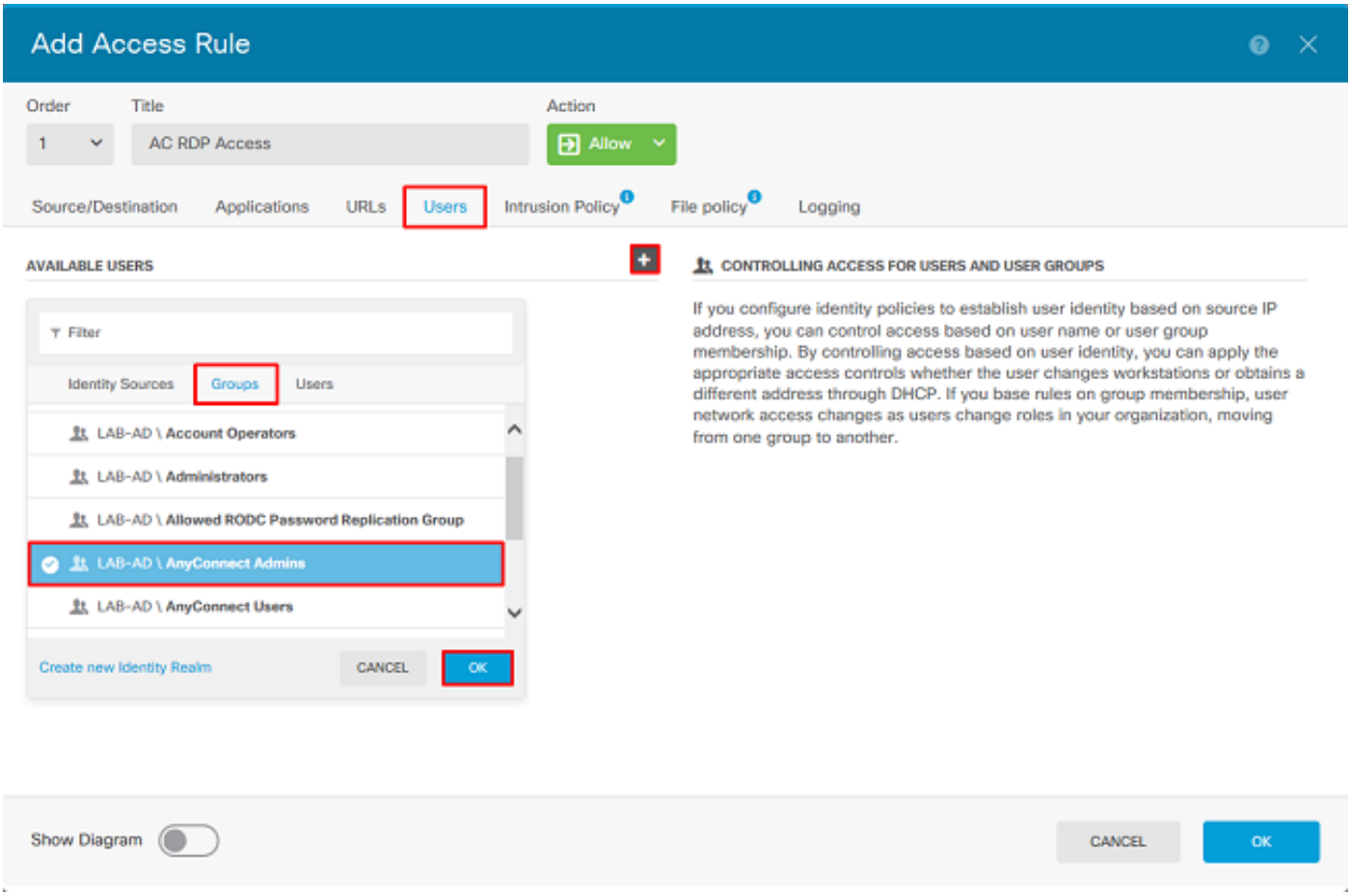
3. Accédez à **Politiques > Contrôle d'accès**. Dans cette section, l'action par défaut est définie sur Bloquer et aucune règle d'accès n'a été créée. Ainsi, une fois qu'un utilisateur AnyConnect se connecte, il ne pourra plus accéder à quoi que ce soit. Cliquez sur le symbole **+** ou sur Créer une règle d'accès pour ajouter une nouvelle règle.



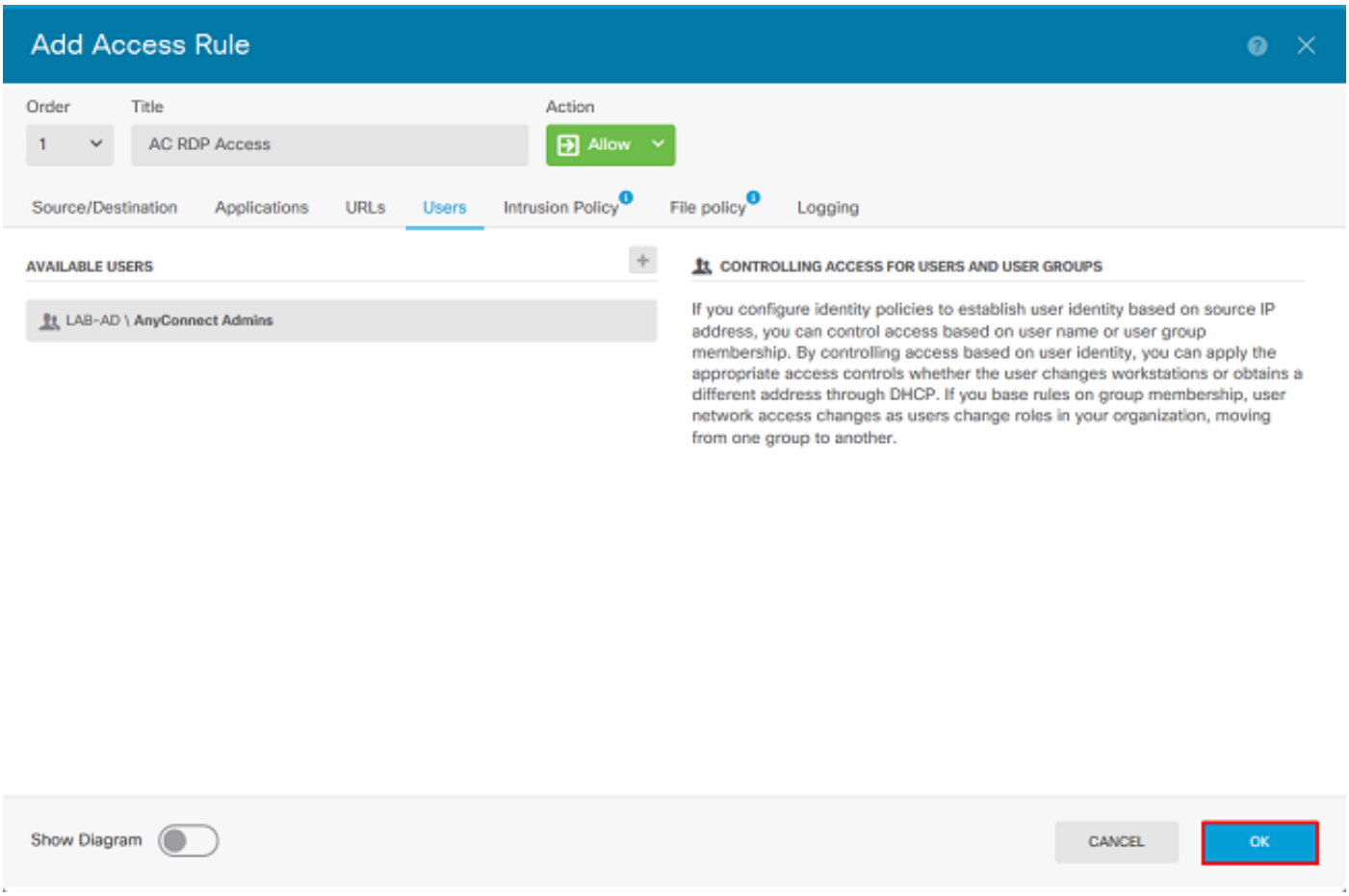
4. Remplissez les champs avec les valeurs appropriées. Dans cette configuration, les utilisateurs du groupe Admins AnyConnect doivent disposer d'un accès RDP au serveur Windows du réseau interne. Pour la source, la zone est configurée comme zone_externe, qui est l'interface externe à laquelle les utilisateurs d'AnyConnect se connecteront et le réseau est configuré en tant qu'objet AnyConnect-Pool configuré précédemment pour attribuer des adresses IP aux clients AnyConnect. Pour l'identité de l'utilisateur dans FDM, la source doit être la zone et le réseau à partir desquels l'utilisateur initiera la connexion. Pour la destination, la zone est configurée en tant que zone interne qui est l'interface interne de Windows Server, le réseau est configuré en tant qu'objet Inside_Net qui est un objet définissant le sous-réseau dans lequel se trouve Windows Server et les ports/protocoles sont définis sur deux objets de port personnalisés pour permettre l'accès RDP sur TCP 3389 et UDP 3389.



Dans la section Utilisateurs, le groupe Admins AnyConnect sera ajouté afin que les utilisateurs autres que ce groupe puissent accéder au RDP sur Windows Server. Cliquez sur le symbole **+**, sur l'onglet Groupes, sur le groupe approprié, puis sur **OK**. Notez que les utilisateurs individuels et la source d'identité peuvent également être sélectionnés.

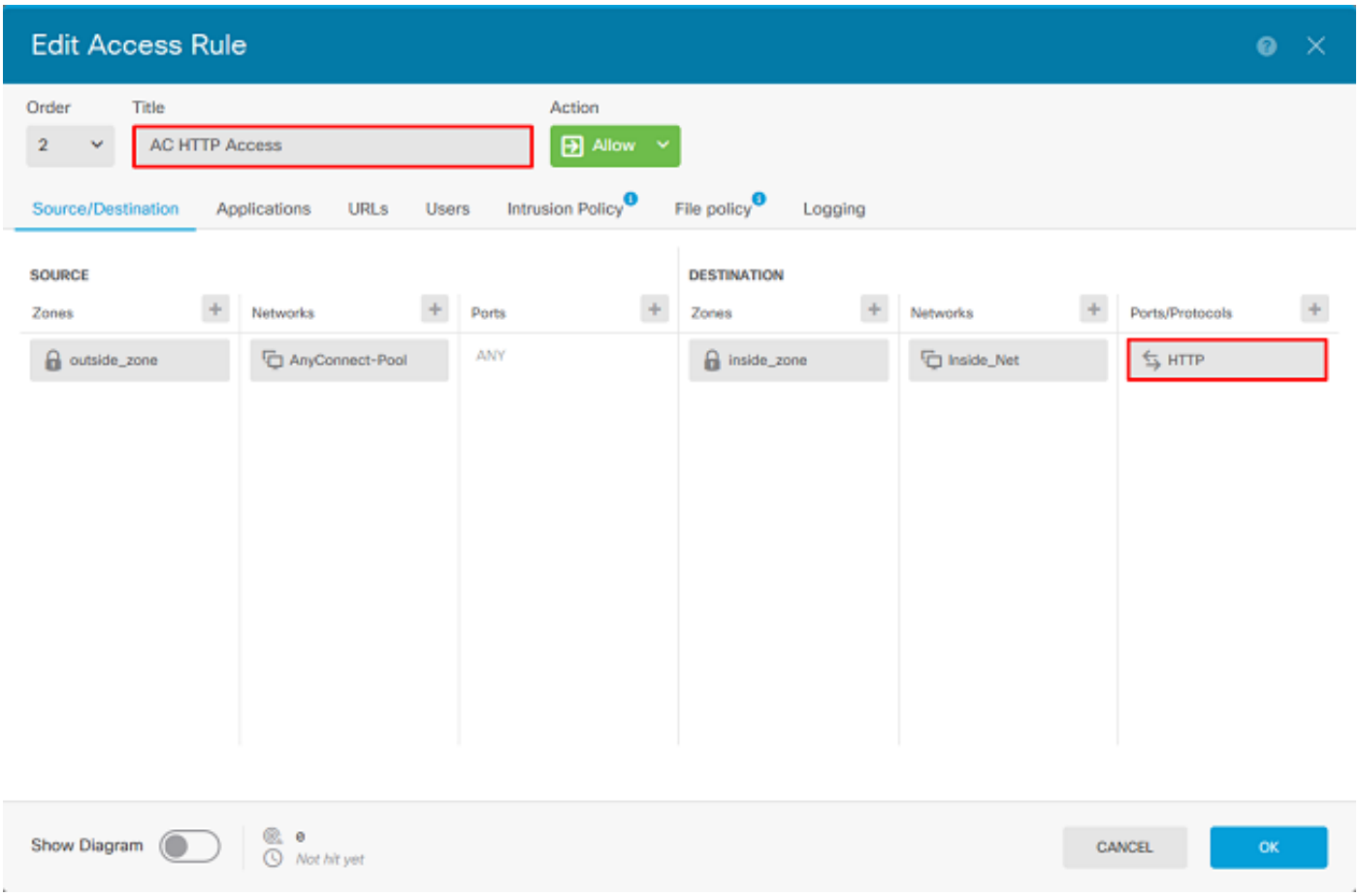


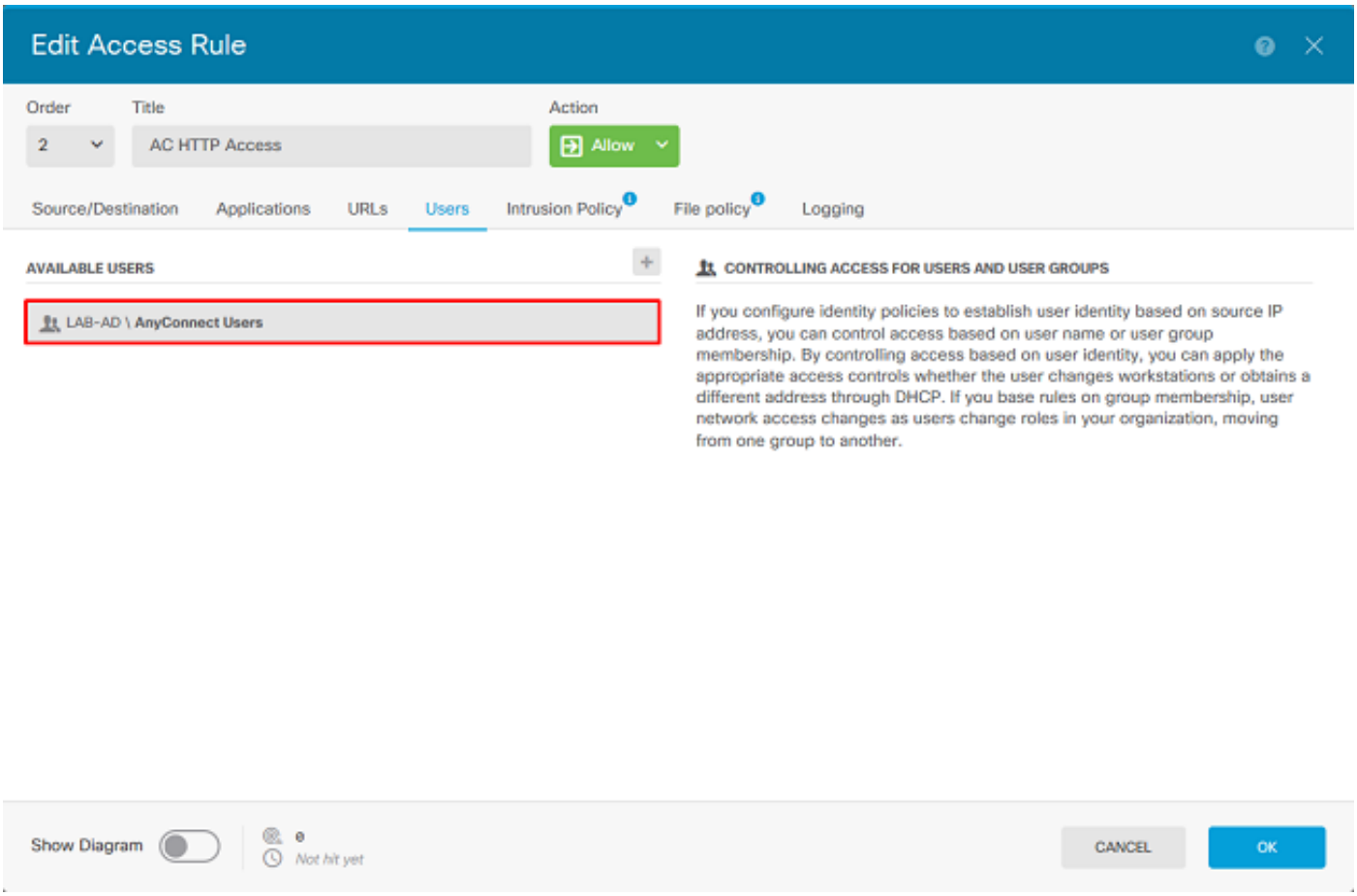
Une fois les options appropriées sélectionnées, cliquez sur **OK**.



5. Créez davantage de règles d'accès si nécessaire. Dans cette configuration, une autre règle

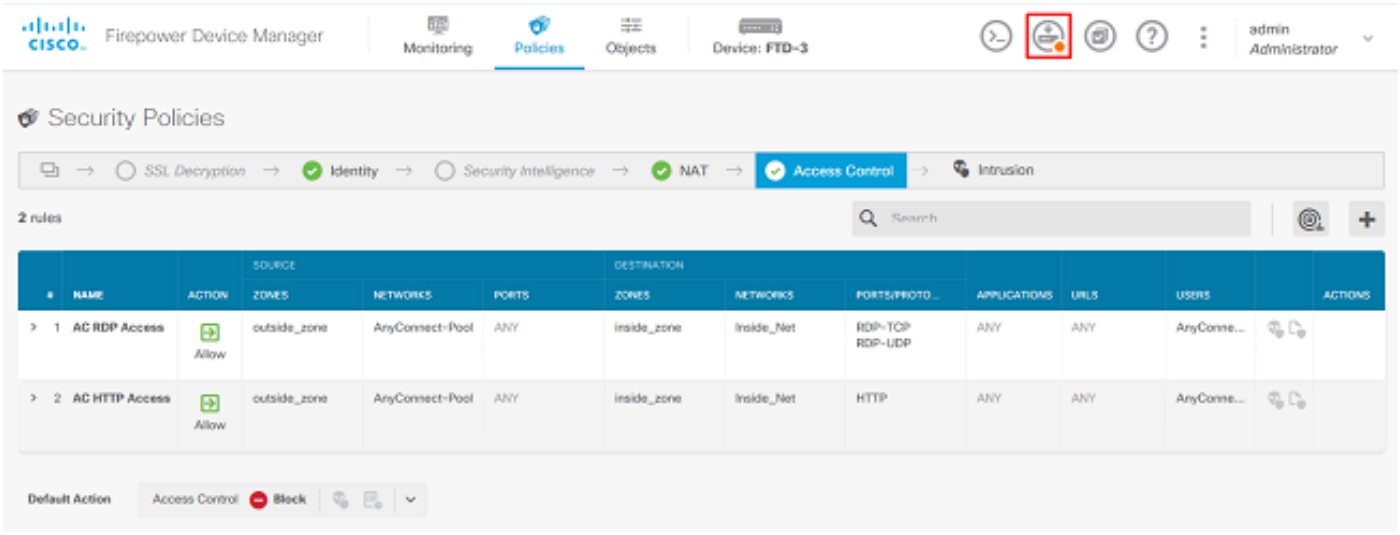
d'accès est créée pour autoriser les utilisateurs du groupe AnyConnect Users à accéder au serveur Windows via HTTP.



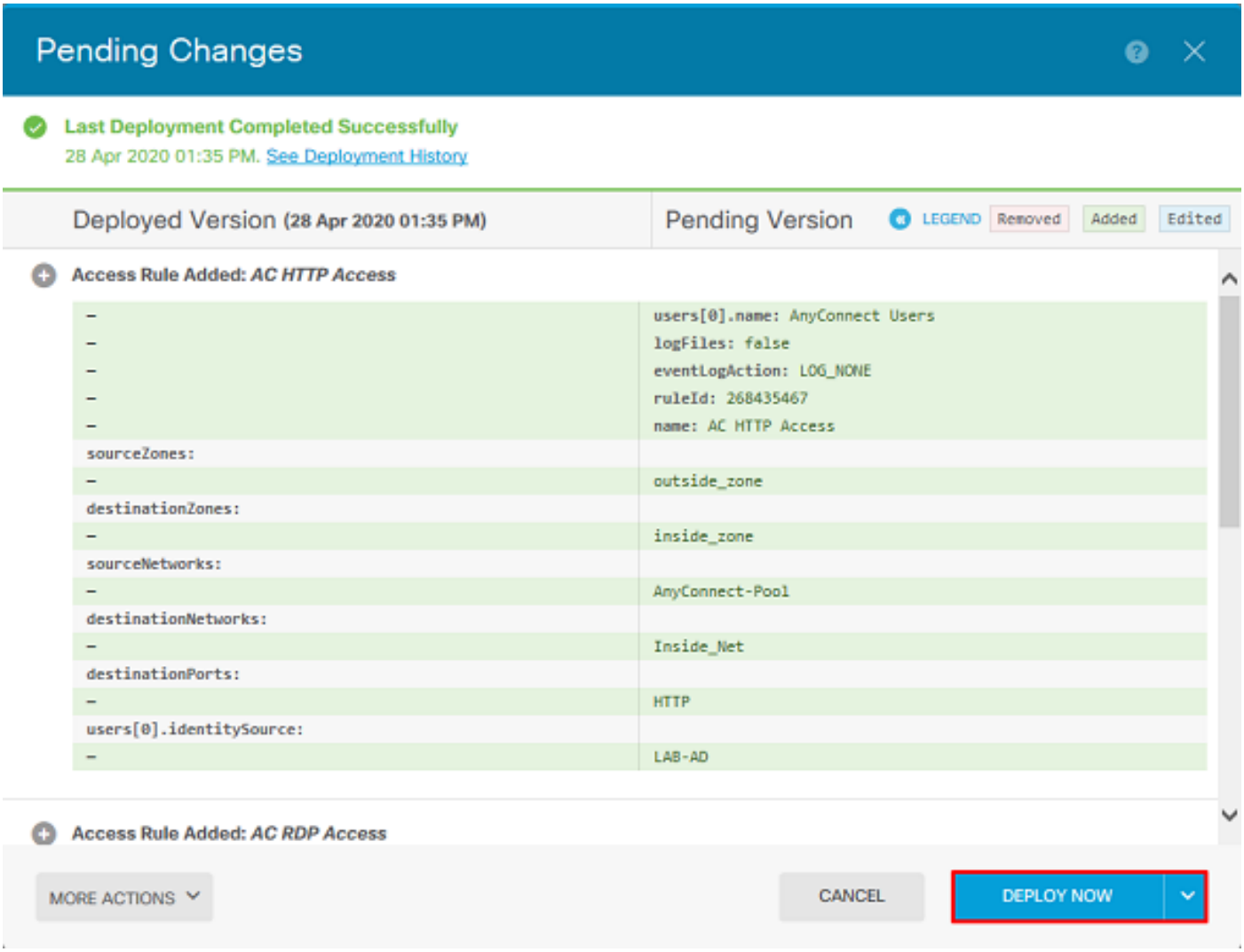


6. Vérifiez la configuration de la règle d'accès, puis cliquez sur le bouton **Modifications en attente**

en haut à droite, comme illustré dans l'image.



7. Vérifiez les modifications, puis cliquez sur **Déployer maintenant**.



Vérification

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Configuration finale

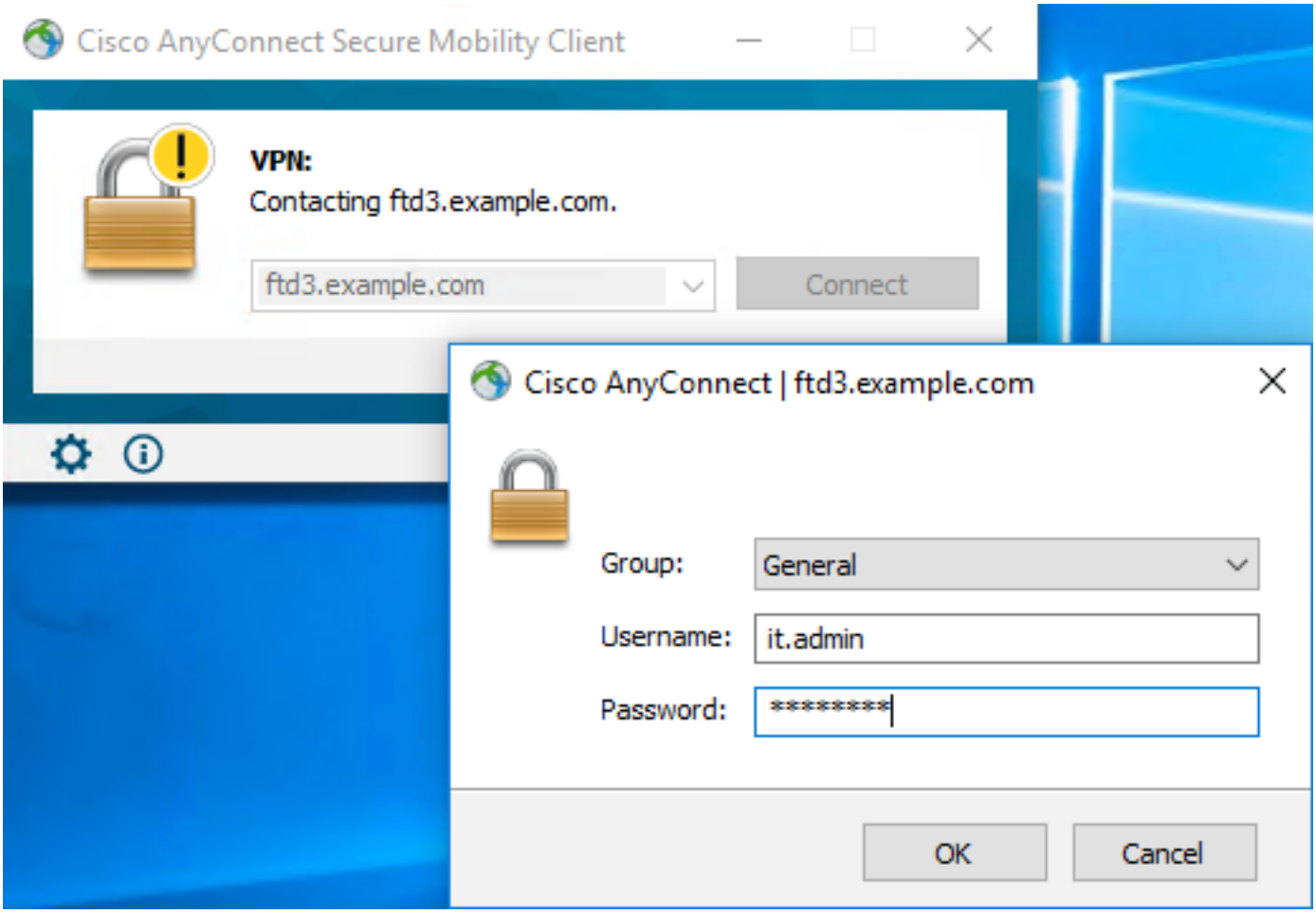
Configuration AAA

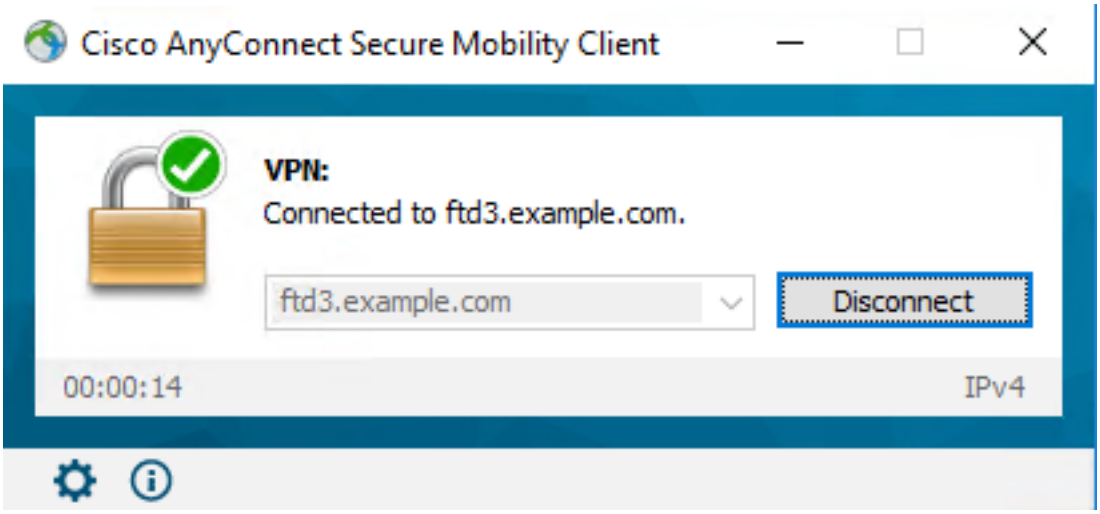
```
show running-configuration aaa-server
aaa-server LAB-AD protocol ldap realm-id 7 aaa-server LAB-AD host win2016.example.com server-
port 389 ldap-base-dn DC=example,DC=com ldap-scope subtree ldap-login-password ***** ldap-login-
dn ftd.admin@example.com server-type auto-detect
```

Configurer AnyConnect

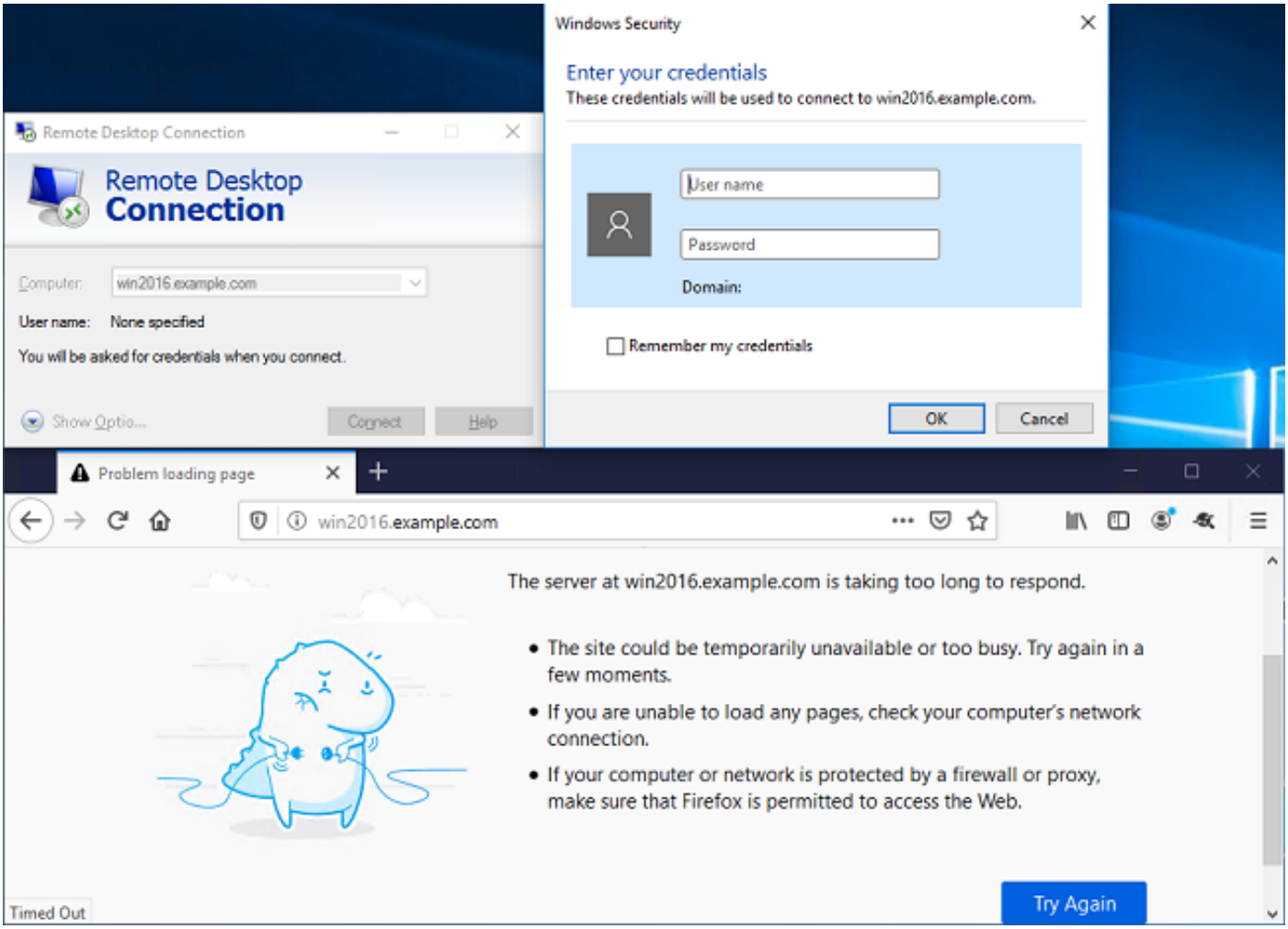
```
> show running-config webvpn
webvpn
 enable outside
 http-headers
  hsts-server
   enable
   max-age 31536000
   include-sub-domains
   no preload
  hsts-client
   enable
  x-content-type-options
  x-xss-protection
  content-security-policy
 anyconnect image disk0:/anyconnpkgs/anyconnect-linux64-4.7.03052-webdeploy-k9.pkg 1
 anyconnect image disk0:/anyconnpkgs/anyconnect-win-4.7.03052-webdeploy-k9.pkg 2
 anyconnect enable
 tunnel-group-list enable
 cache
  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-tunnel-protocol ssl-client
 split-tunnel-policy tunnelspecified
 split-tunnel-network-list value DfltGrpPolicy|splitAcl
 webvpn
  anyconnect ssl dtls none

> show running-config ssl
ssl trust-point FTD-3-Manual outside
```

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

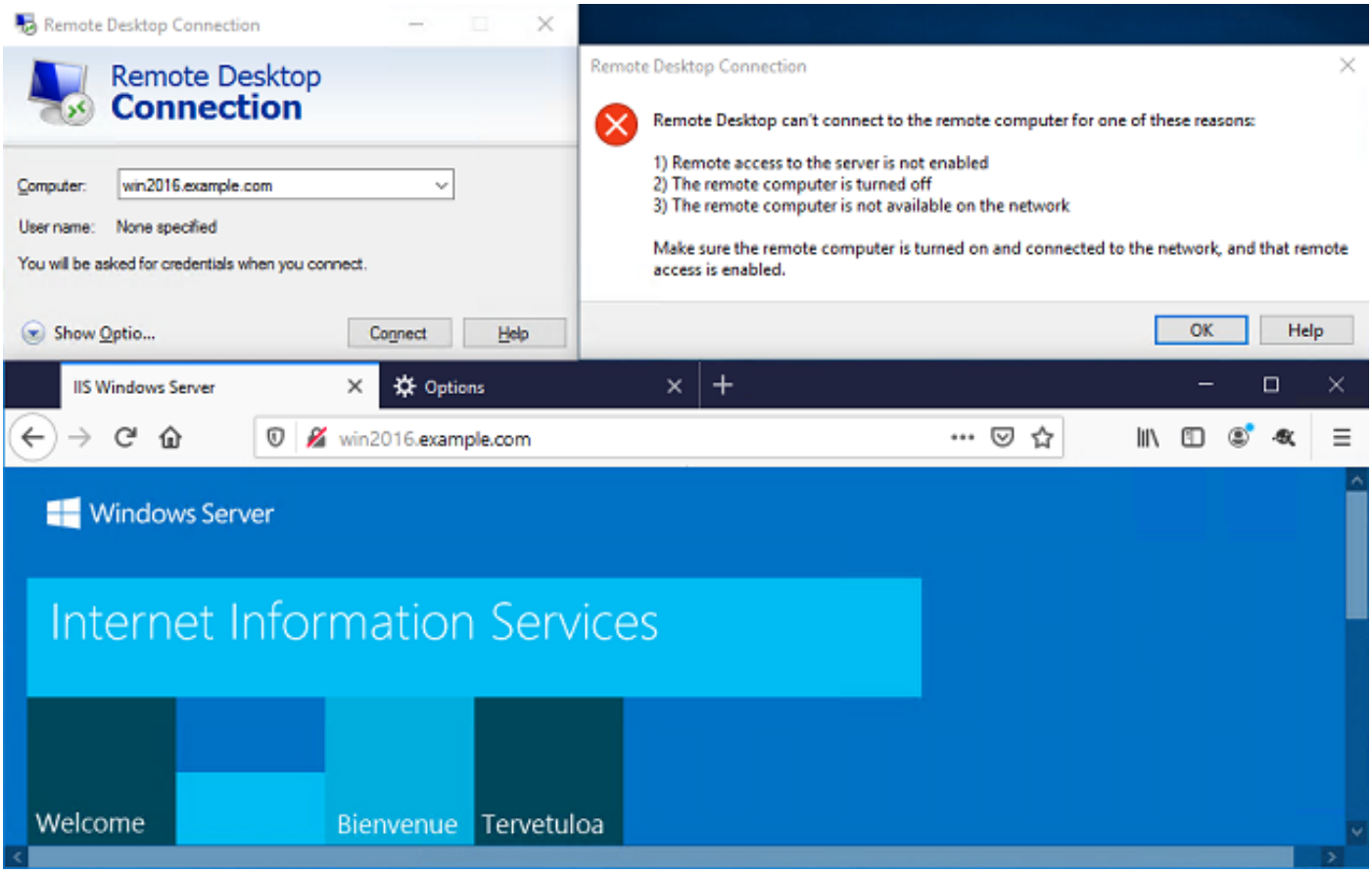




L'administrateur informatique de l'utilisateur fait partie du groupe Admins AnyConnect qui dispose d'un accès RDP à Windows Server, mais n'a pas accès au protocole HTTP. L'ouverture d'une session RDP et Firefox sur ce serveur vérifie que cet utilisateur ne peut accéder au serveur que via RDP.



Si vous êtes connecté à un utilisateur de test qui fait partie du groupe Utilisateurs AnyConnect disposant d'un accès HTTP mais non RDP, vous pouvez vérifier que les règles de stratégie de contrôle d'accès prennent effet.



Dépannage

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Déboguages

Ce débogage peut être exécuté dans l'interface CLI de diagnostic afin de dépanner les problèmes liés à l'authentification LDAP : **debug ldap 255**.

Afin de dépanner les problèmes de stratégie de contrôle d'accès d'identité utilisateur, le **système prend en charge firewall-engine-debug** peut être exécuté en clish afin de déterminer pourquoi le trafic est autorisé ou bloqué de manière inattendue.

Débogues LDAP de travail

```
[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 la 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 :

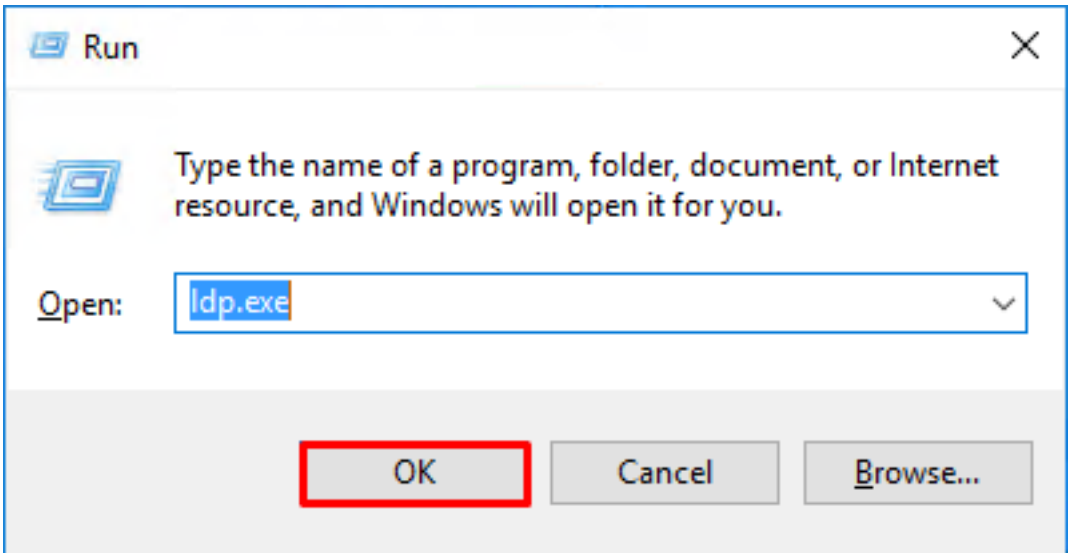
- Vérifiez le routage et assurez-vous que le serveur LDAP reçoit une réponse du FTD.
- Si LDAPS ou STARTTLS est utilisé, assurez-vous que le certificat d'autorité de certification racine correct est approuvé afin que la connexion SSL puisse s'effectuer correctement.
- Vérifiez que l'adresse IP et le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

DN de connexion et/ou mot de passe de liaison incorrects

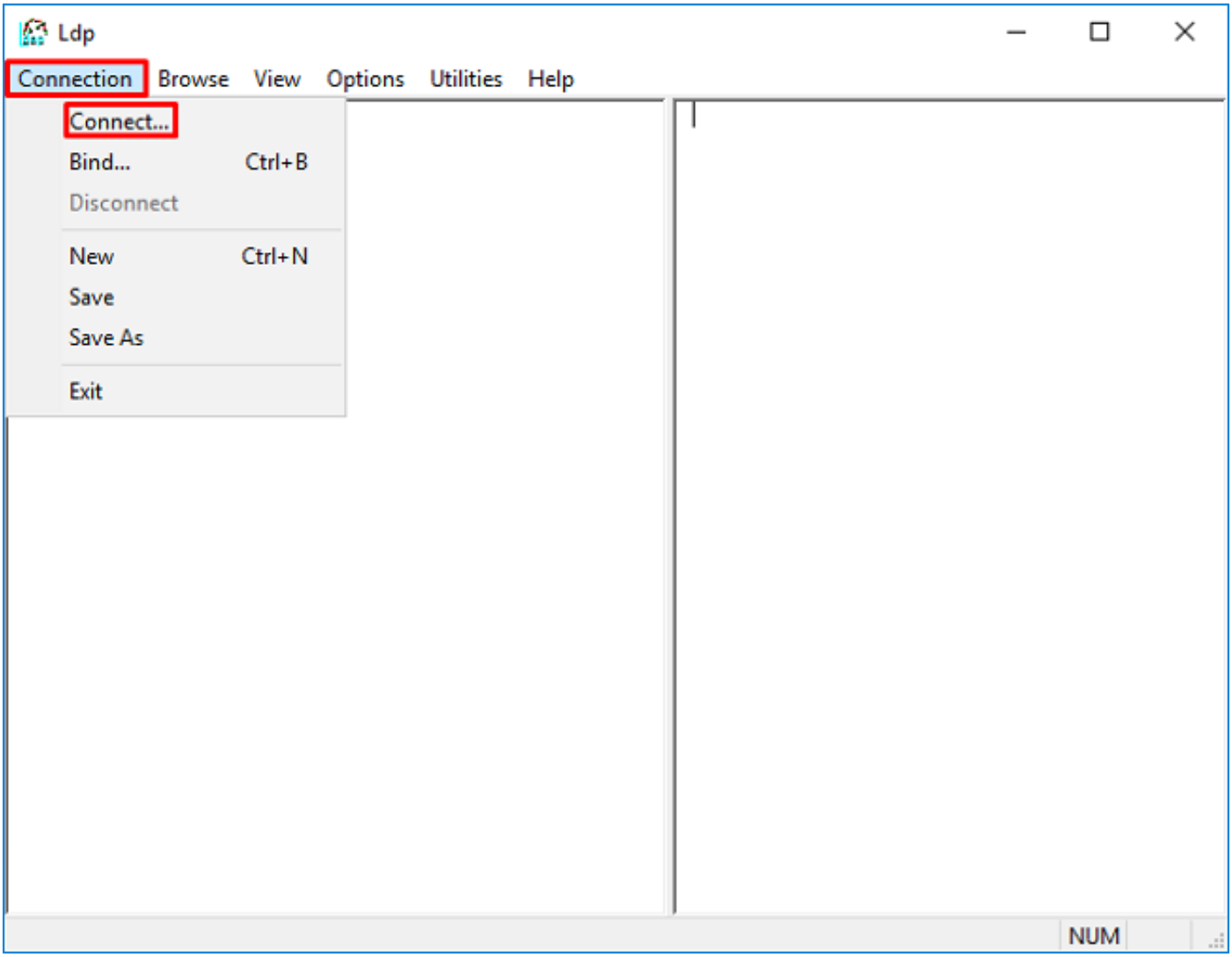
```
[-2147483615] Session Start
[-2147483615] New request Session, context 0x00007f9e65ccdc40, reqType = Authentication
[-2147483615] Fiber started
[-2147483615] Creating LDAP context with uri=ldap://192.168.1.1:389
[-2147483615] Connect to LDAP server: ldap://192.168.1.1:389, status = Successful
[-2147483615] 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 DN de connexion et le mot de passe de connexion sont configurés correctement. Ceci peut être vérifié sur le serveur AD avec **ldp.exe**. Afin de vérifier qu'un compte peut se lier correctement à l'utilisation de ldp, naviguez à travers ces étapes :

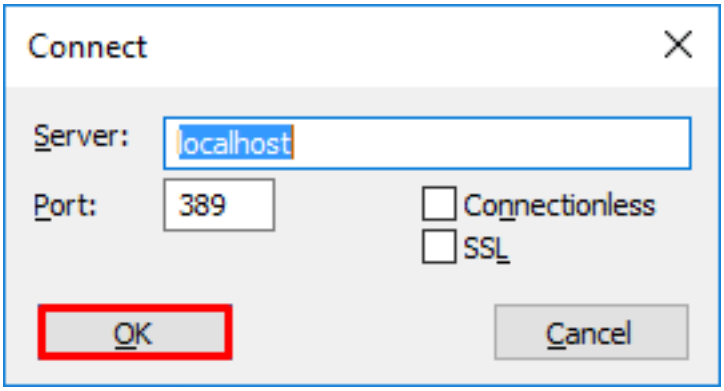
1. Sur le serveur AD, appuyez sur **Win+R** et recherchez **ldp.exe**.



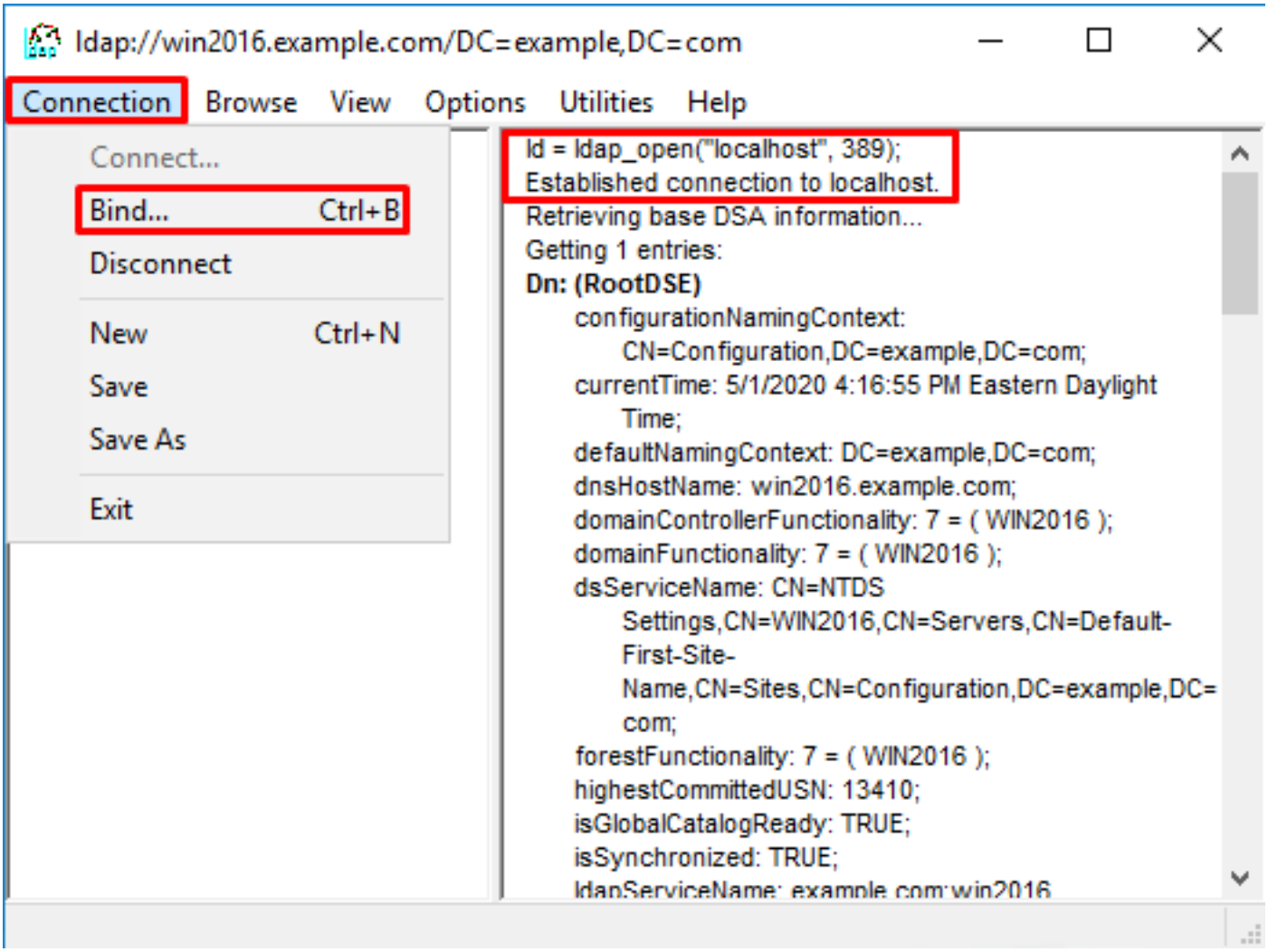
2. Cliquez sur **Connexion > Connexion...** comme le montre l'image.



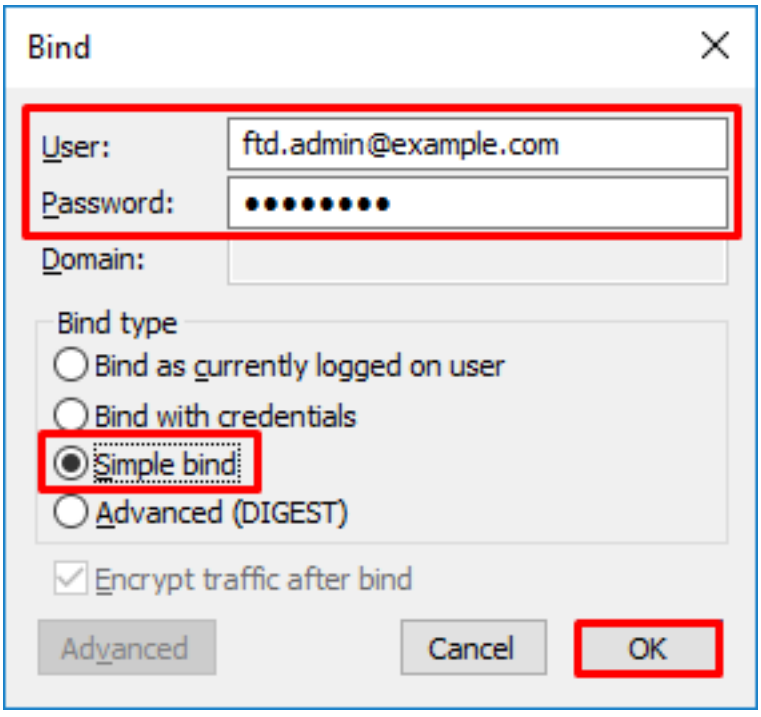
3. Spécifiez localhost pour le serveur et le port approprié, puis cliquez sur **OK**.



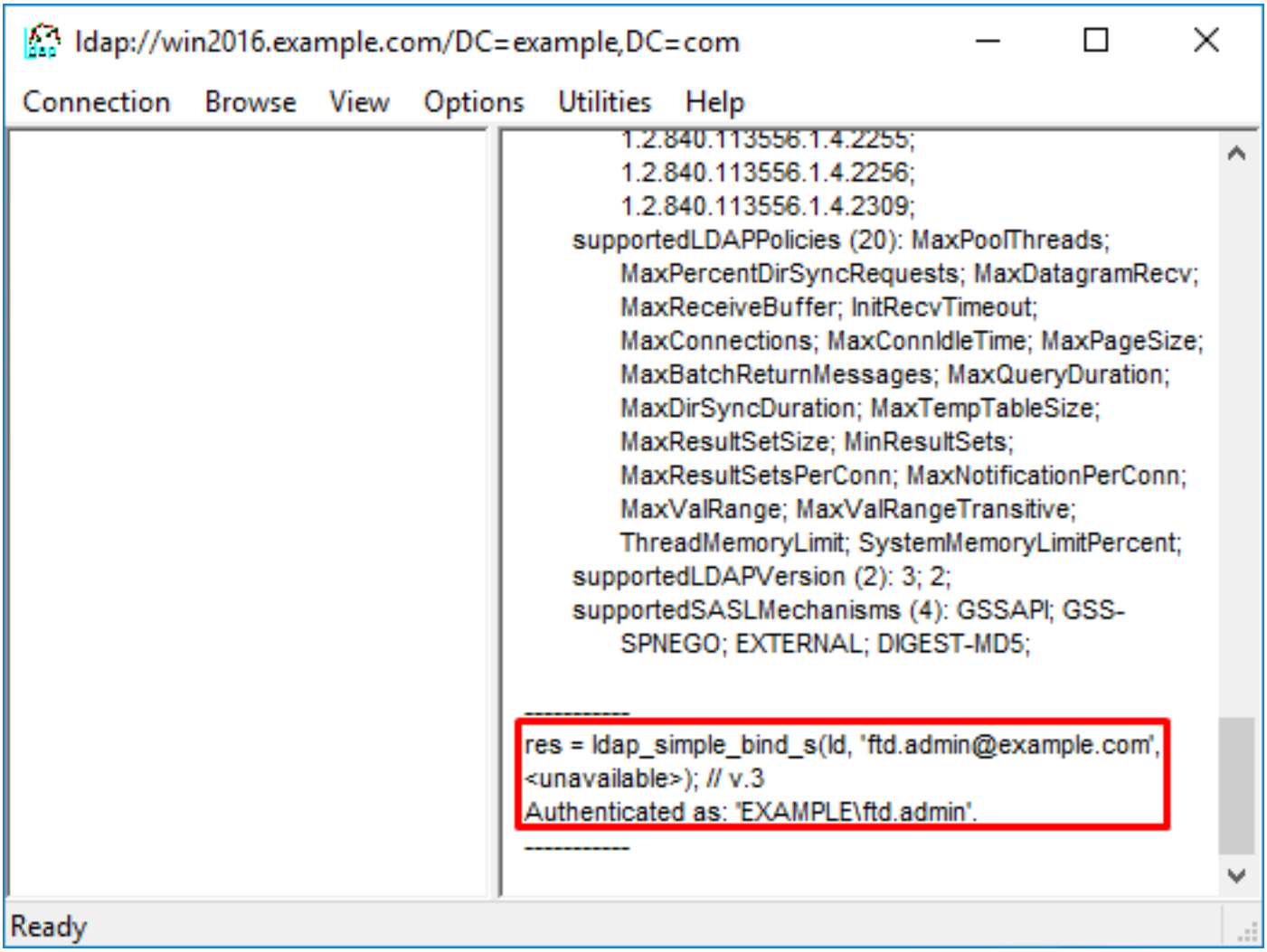
4. La colonne de droite affiche le texte qui indique une connexion réussie. Cliquez sur **Connexion > Lier...** comme le montre l'image.



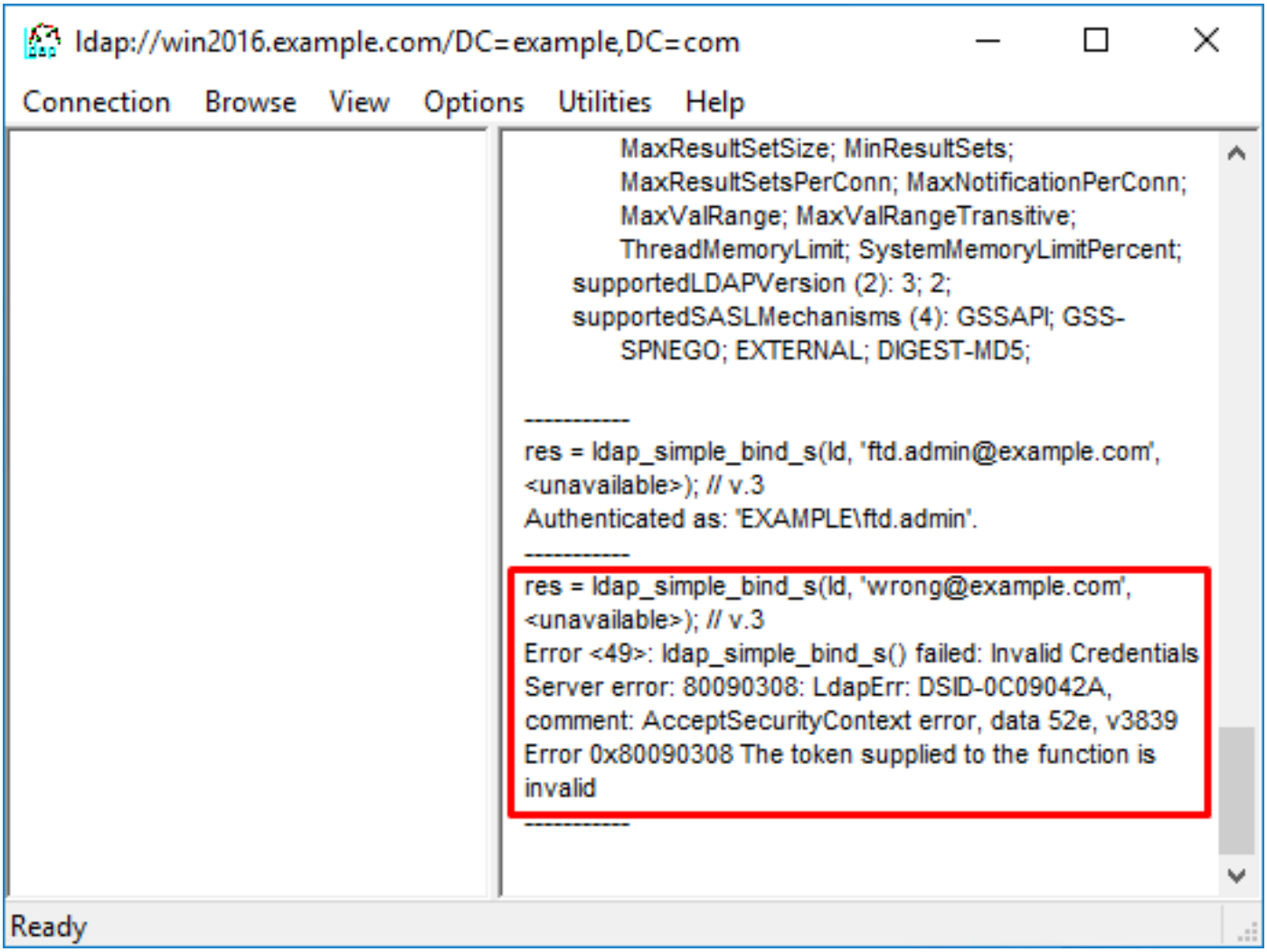
5. Sélectionnez **Liaison simple**, puis spécifiez le nom d'utilisateur et le mot de passe du compte d'annuaire. Click OK.



Avec une liaison réussie, ldp affiche Authenticated en tant que **DOMAIN\username**.



Si vous tentez une liaison avec un nom d'utilisateur ou un mot de passe non valide, cela entraînera un échec comme celui-ci.

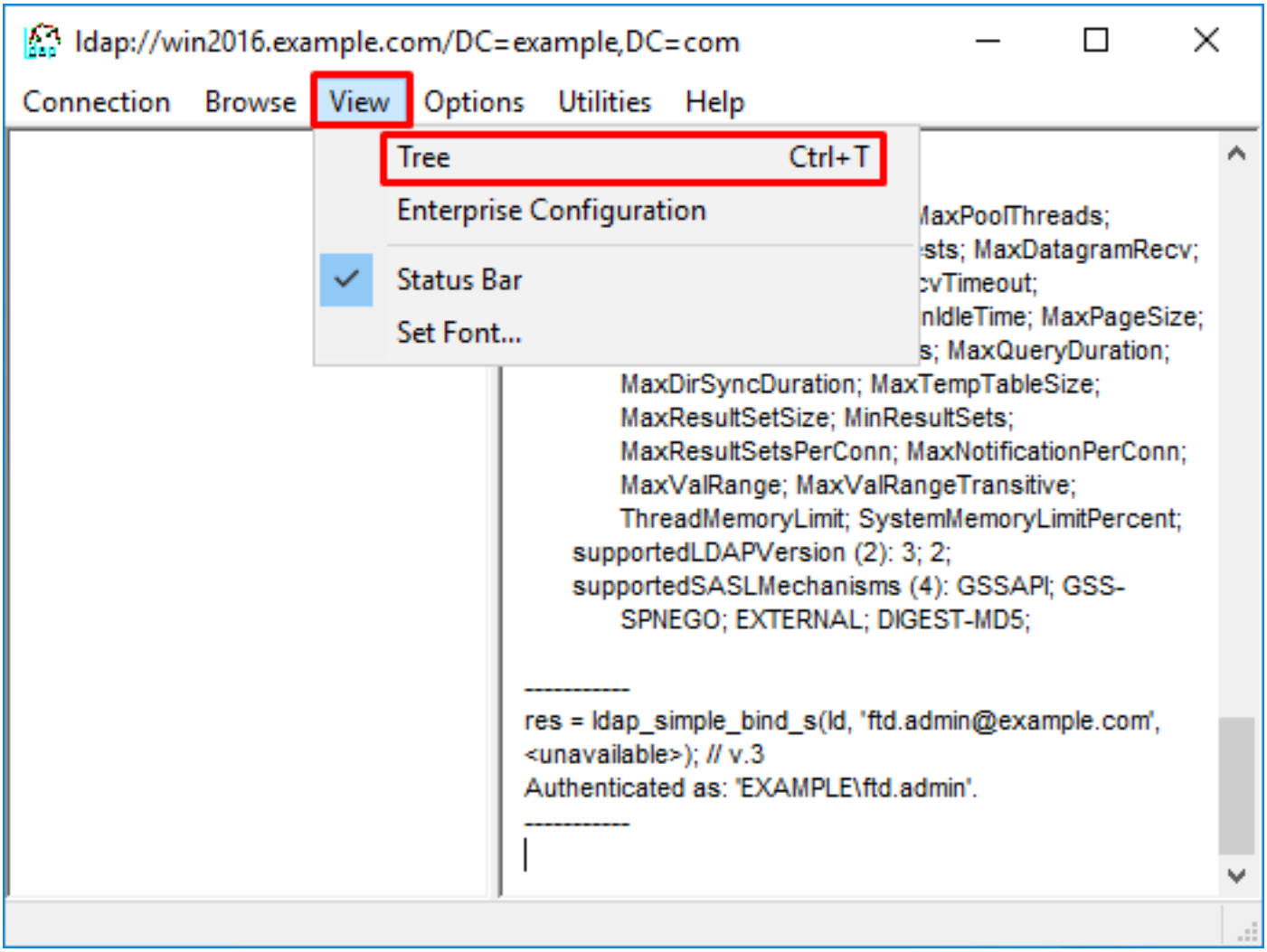


Serveur LDAP introuvable Nom d'utilisateur

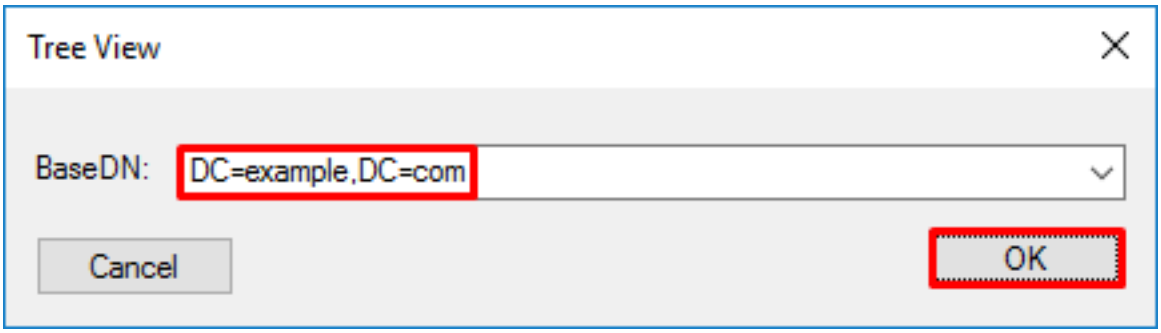
```
[-2147483612] Session Start
[-2147483612] New request Session, context 0x00007f9e65ccdc40, reqType = Authentication
[-2147483612] Fiber started
[-2147483612] Creating LDAP context with uri=ldap://192.168.1.1:389
[-2147483612] Connect to LDAP server: ldap://192.168.1.1:389, status = Successful
[-2147483612]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

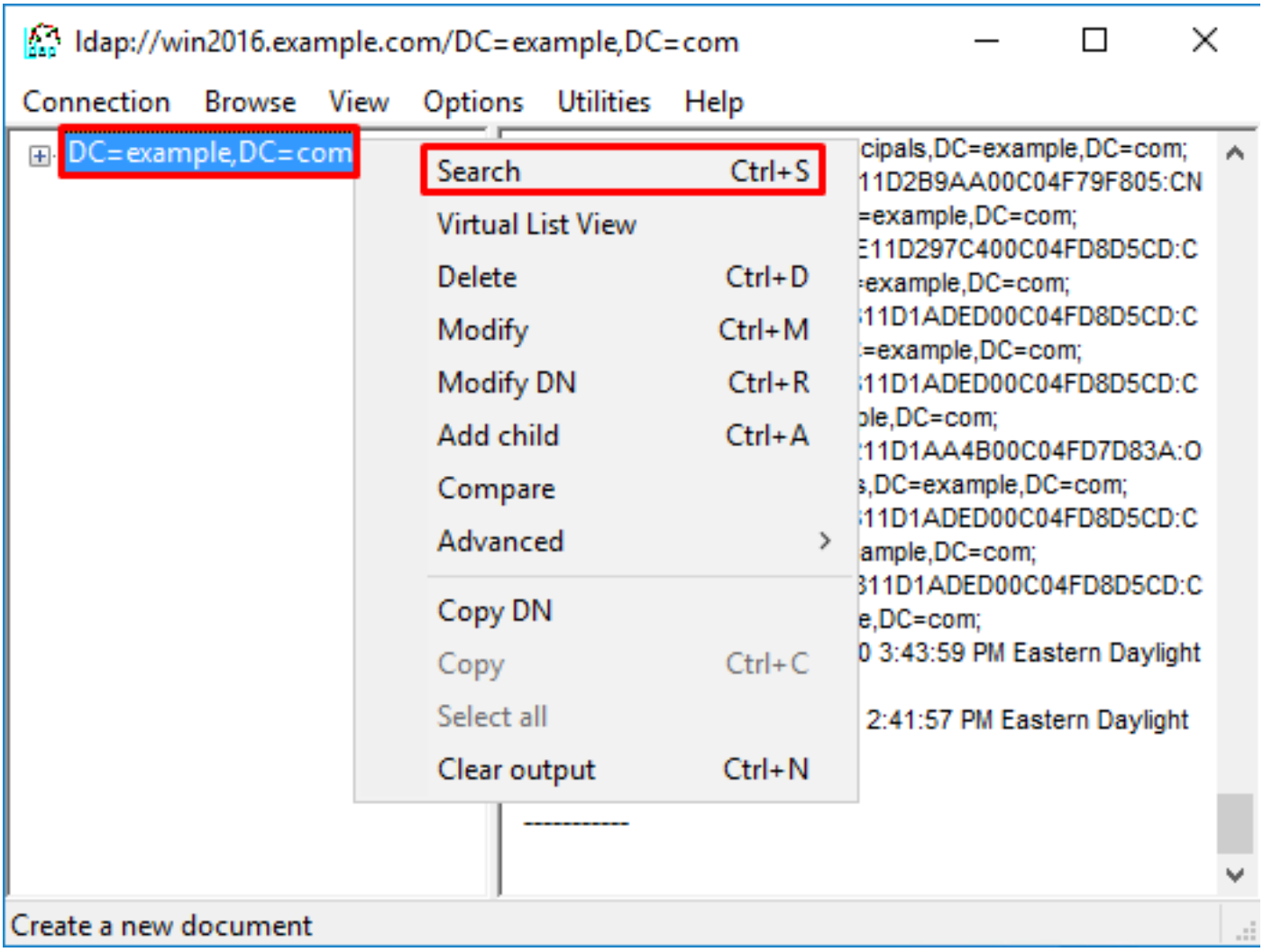
1. Une fois la liaison établie, accédez à **Affichage > Arborescence** comme indiqué dans l'image.



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

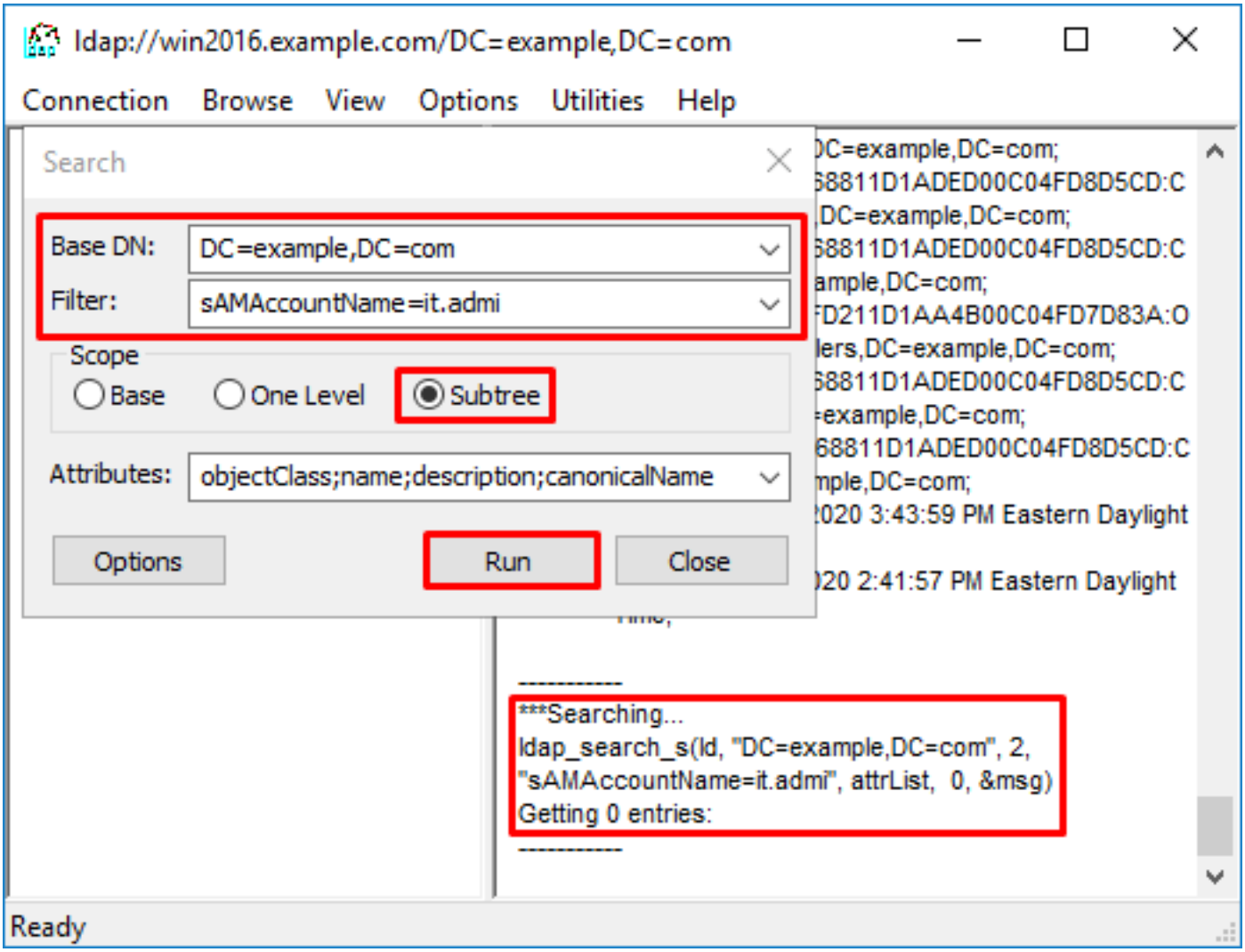


3. Cliquez avec le bouton droit sur le DN de base, puis cliquez sur Rechercher comme indiqué dans l'image.



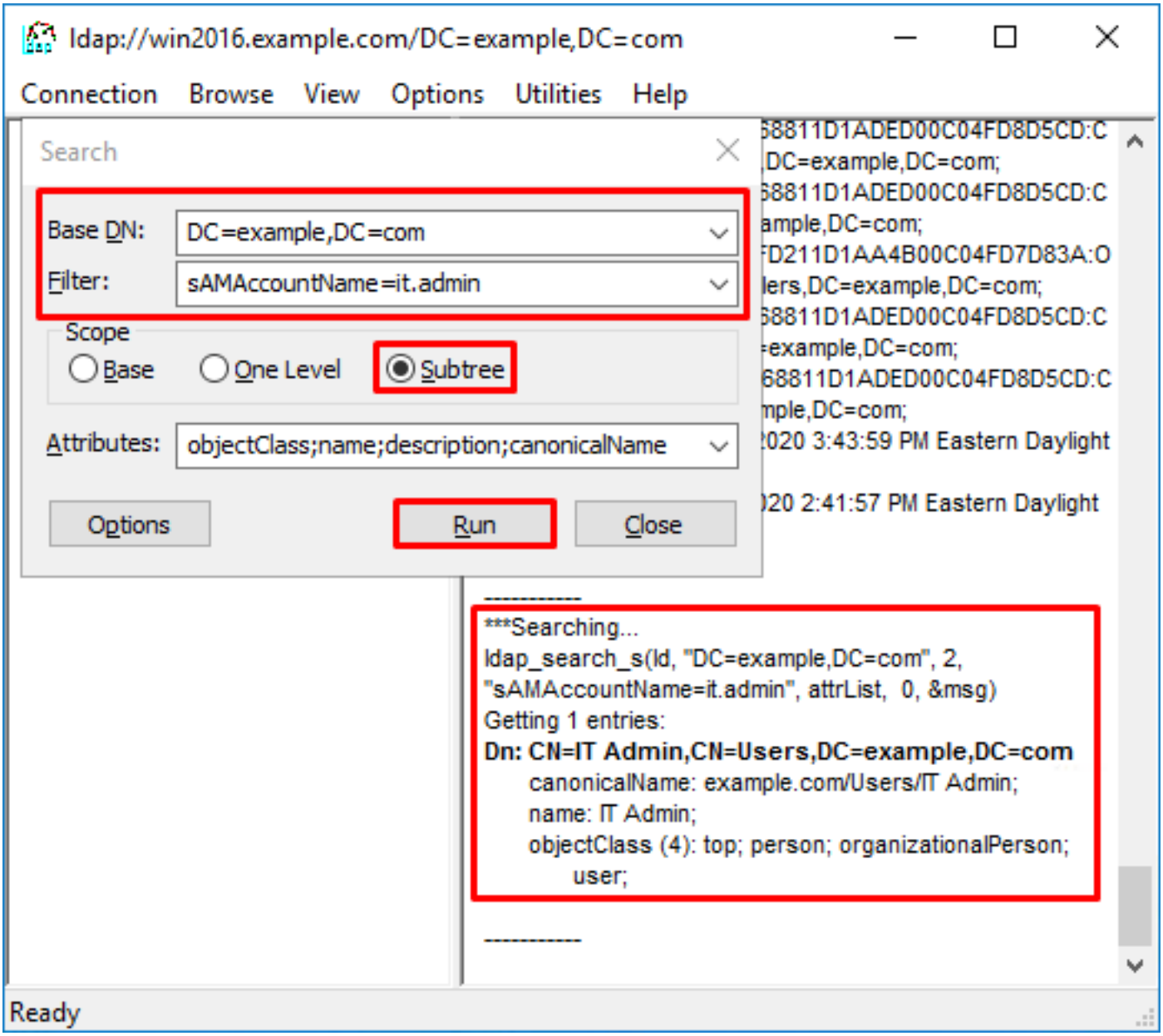
4. Spécifiez les mêmes valeurs de base DB, de filtre et d'étendue que celles indiquées dans les débogages. Dans cet exemple, voici :

- DN de base : dc=exemple,dc=com
- Filtre : samaccountname=it.admi
- Champ d'application : SOUS-ARBRE



ldp trouve 0 entrée car il n'y a pas de compte utilisateur avec **samaccountname=it.admi** sous le DN de base dc=example,dc=com.

Une nouvelle tentative avec le **nom_compte=it.admin** correct montre un résultat différent. ldp trouve 1 entrée sous le DN de base dc=exemple, dc=com et imprime le DN de cet 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 de l'utilisateur est configuré correctement et qu'il n'a pas expiré. Tout comme le DN de connexion, le FTD établit une liaison avec AD avec les informations d'identification de l'utilisateur. Cette liaison peut également être effectuée dans ldp afin de vérifier que la distance administrative est capable de reconnaître les mêmes informations d'identification de nom d'utilisateur et de mot de passe. Les étapes de ldp sont affichées dans la section **Liaison du nom de connexion et/ou du mot de passe incorrect**. En outre, les journaux de l'Observateur d'événements du serveur Microsoft peuvent être examinés pour une raison potentielle.

Test AAA

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

Voici une capture qui montre le trafic LDAP bidirectionnel :

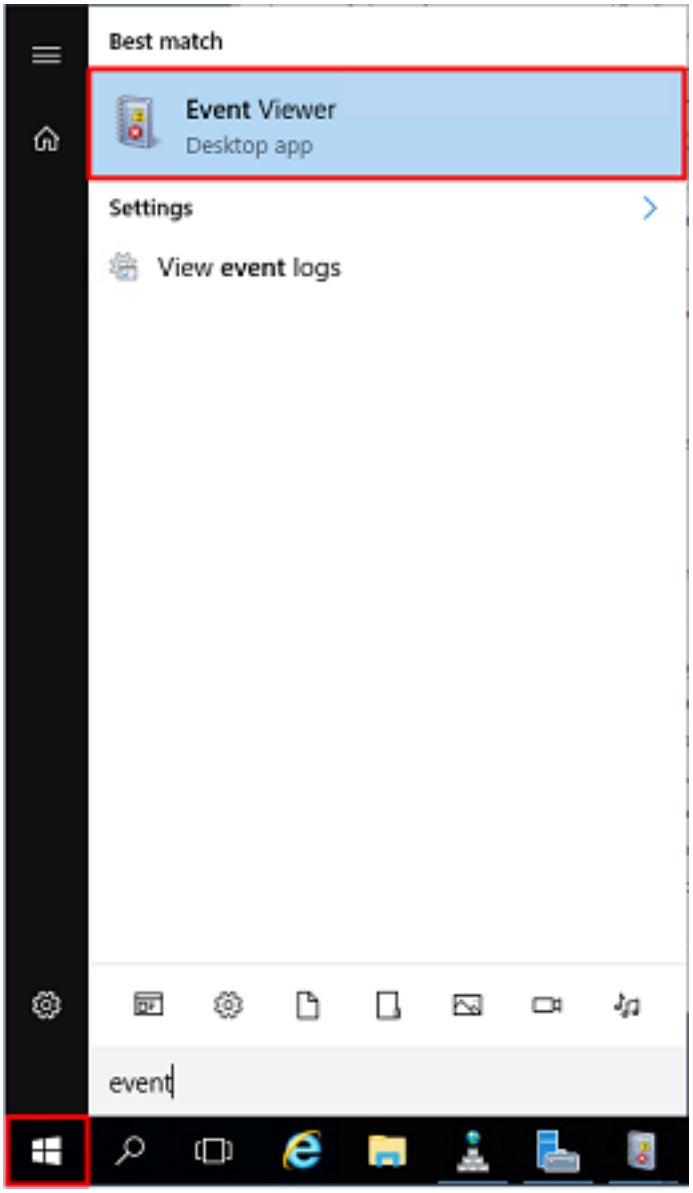
```
> show route 192.168.1.1

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
```

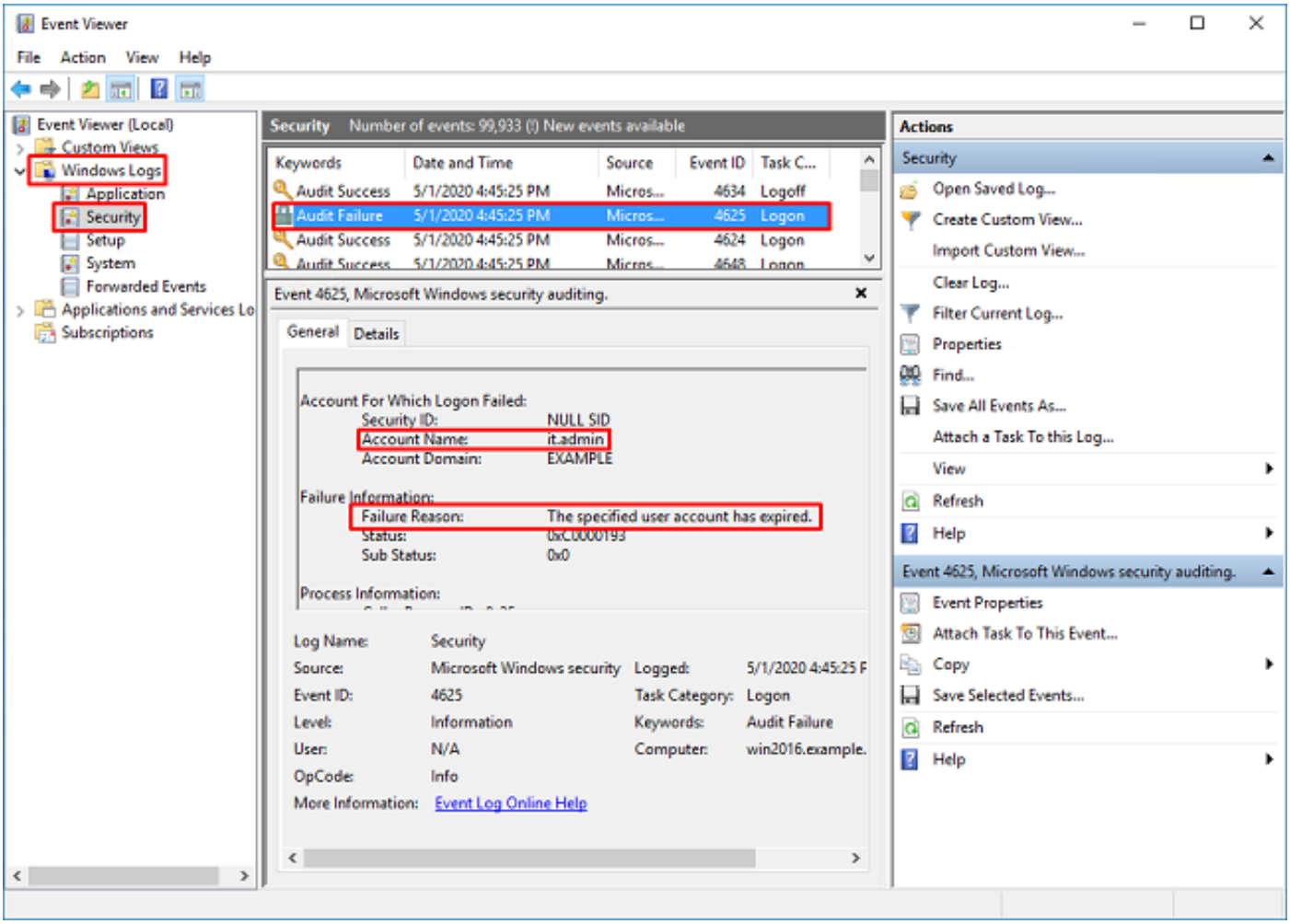
Journaux de l'Observateur d'événements Windows Server

Les journaux de l'Observateur d'événements sur la van du serveur AD fournissent des informations plus détaillées sur les raisons d'une défaillance.

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



2. Développez **Journaux Windows** et cliquez sur **Sécurité**. Recherchez **Échec de l'audit** avec le nom de compte de l'utilisateur et vérifiez les informations d'échec comme indiqué dans l'image.



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