Configurer la gestion des mots de passe à l'aide de LDAP pour RA VPN sur FTD géré par FMC

Table des matières

Introduction

Ce document décrit la configuration de la gestion des mots de passe à l'aide de LDAP pour les clients AnyConnect se connectant à Cisco Firepower Threat Défense (FTD).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissances de base de la configuration VPN d'accès à distance (VPN) sur FMC
- Connaissances de base de la configuration du serveur LDAP sur FMC
- Connaissances de base d'Active Directory

Composants utilisés

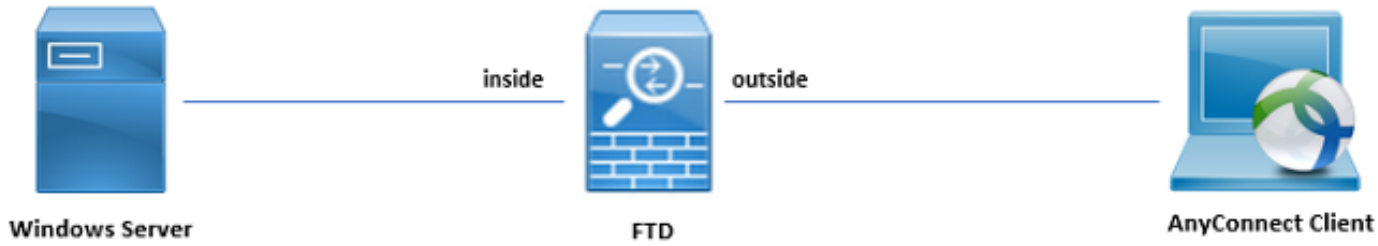
Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Serveur Microsoft 2012 R2
- FMCv 7.3.0
- FTDv exécutant 7.3.0

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

Diagramme et scénario du réseau



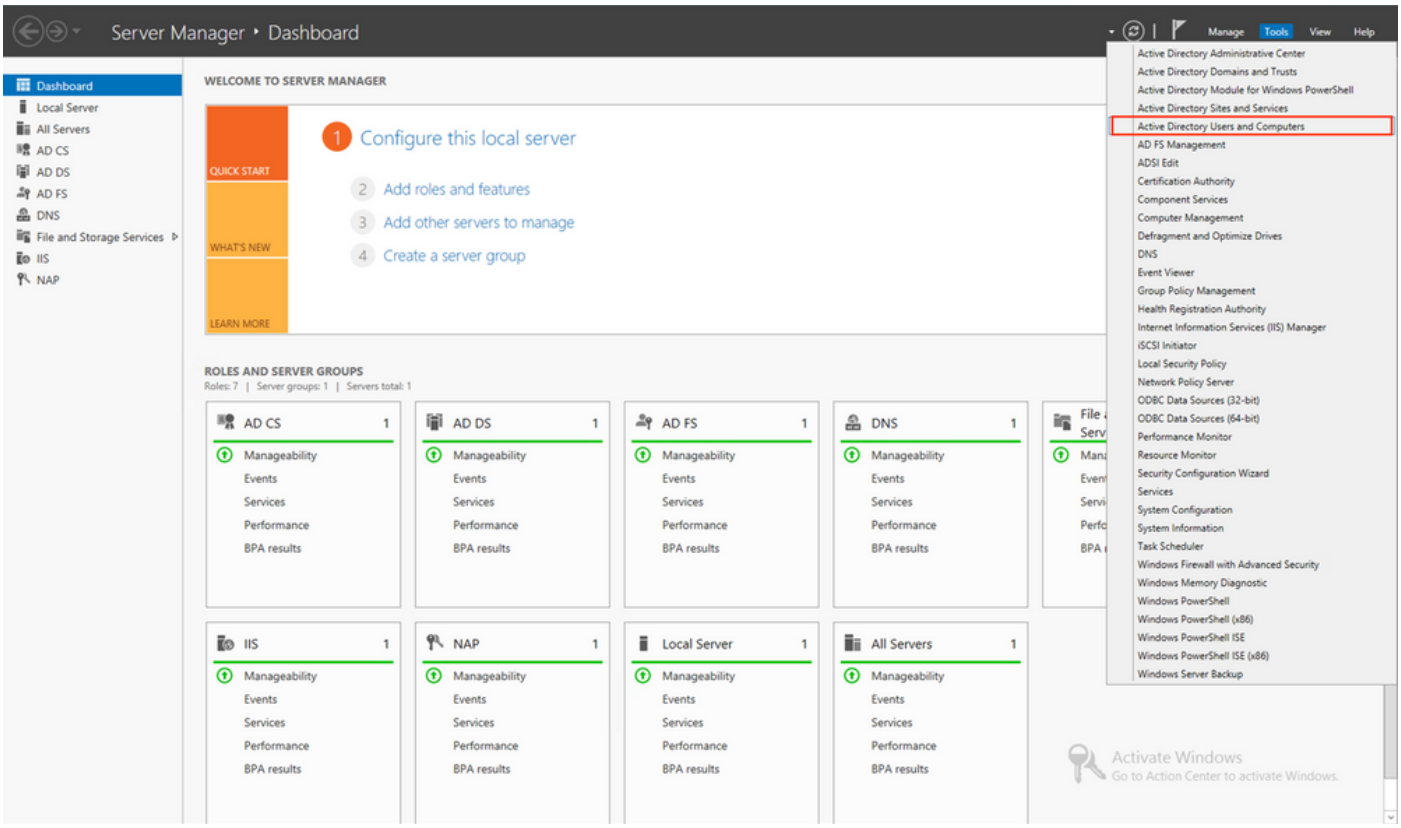
Le serveur Windows est préconfiguré avec ADDS et ADCS afin de tester le processus de gestion des mots de passe utilisateur. Dans ce guide de configuration, ces comptes utilisateur sont créés.

Comptes utilisateurs:

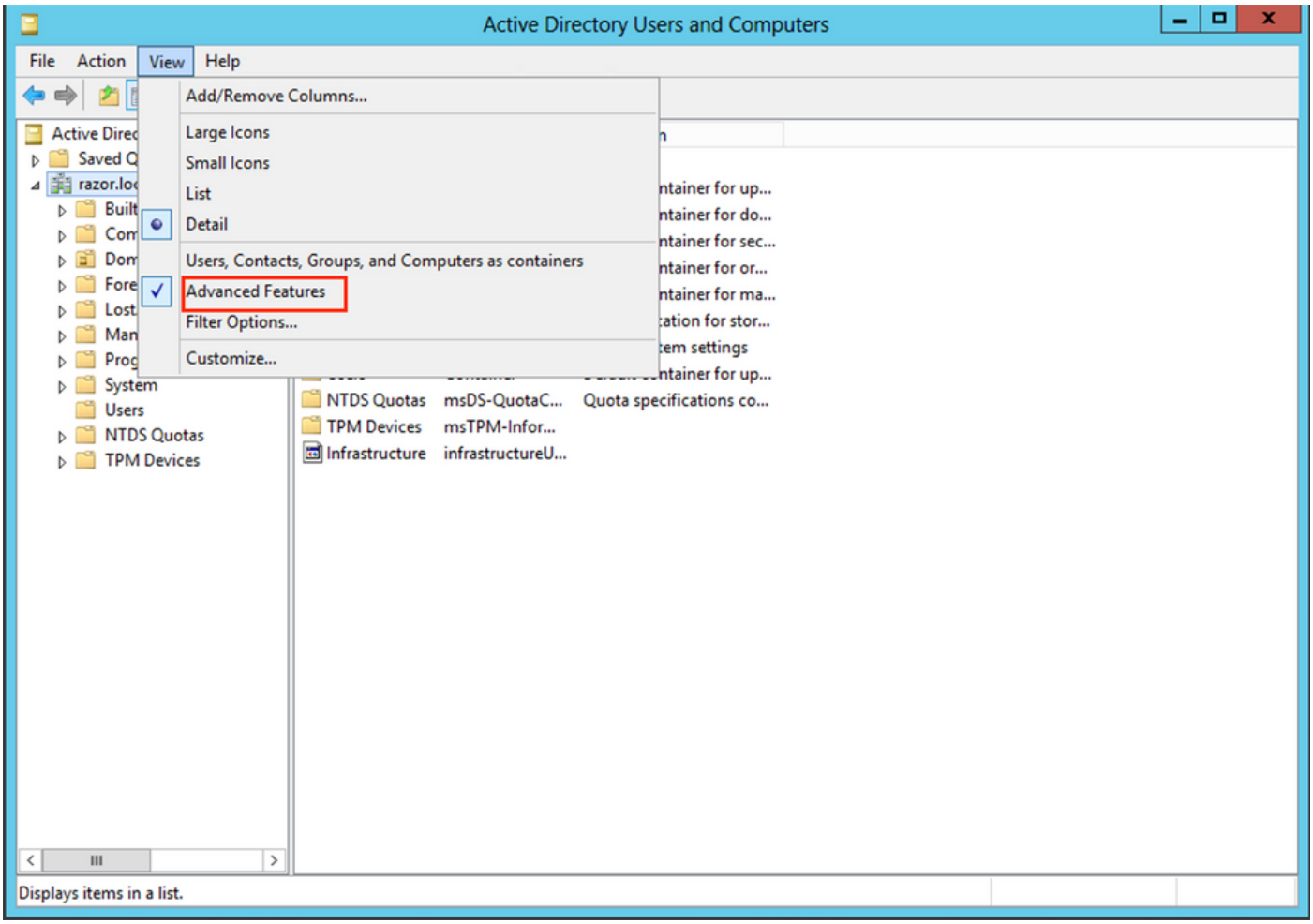
- Administrateur : il est utilisé comme compte d'annuaire afin de permettre au FTD de se lier au serveur Active Directory.
- admin : compte d'administrateur de test utilisé pour démontrer l'identité de l'utilisateur.

Déterminer le DN de base LDAP et le DN de groupe

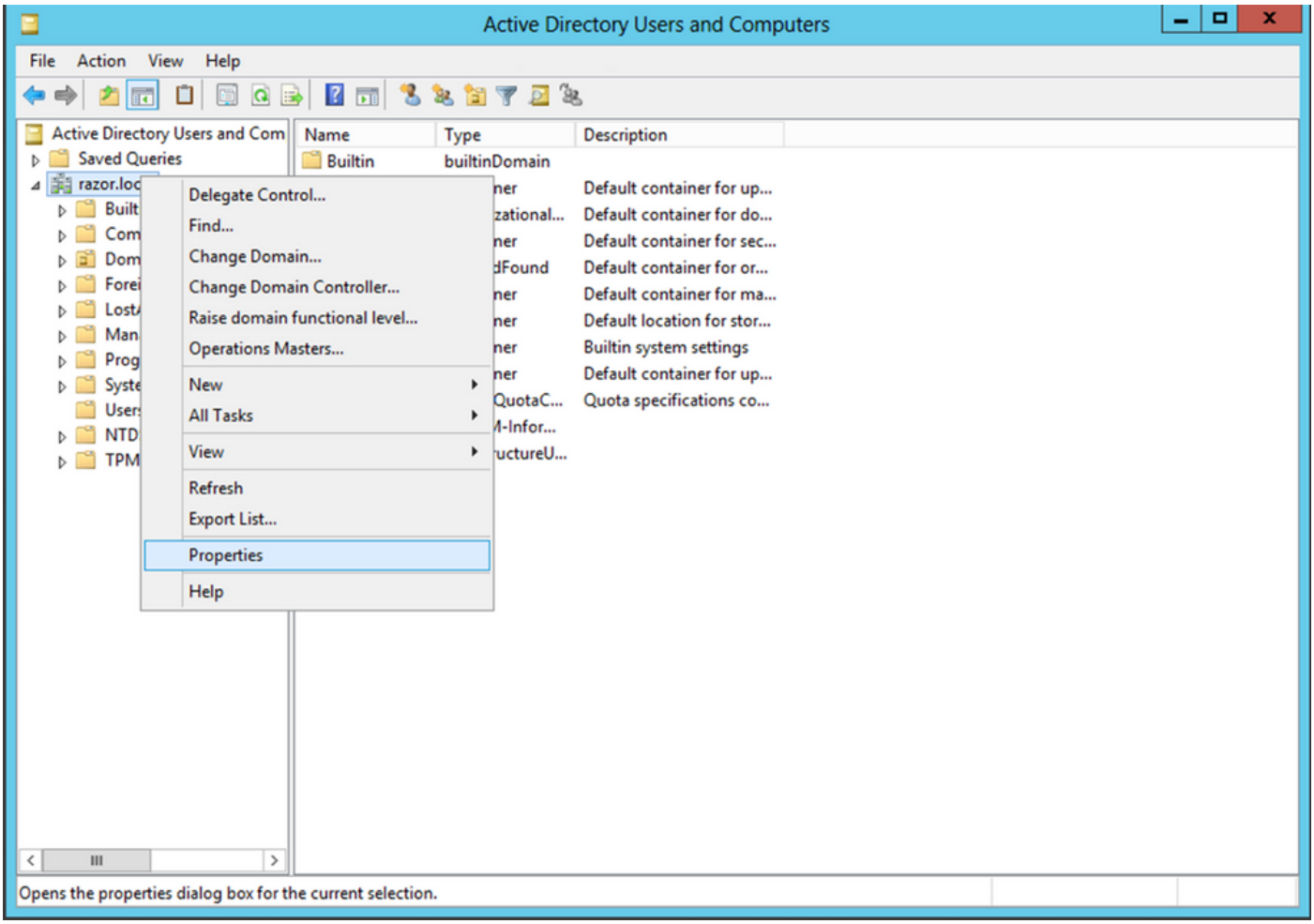
1. Open (ouvert) Active Directory Users and Computers via le tableau de bord du Gestionnaire de serveur.



2. Ouvrez le View Option sur le panneau supérieur et activez l'option Advanced Features, comme l'illustre l'image :



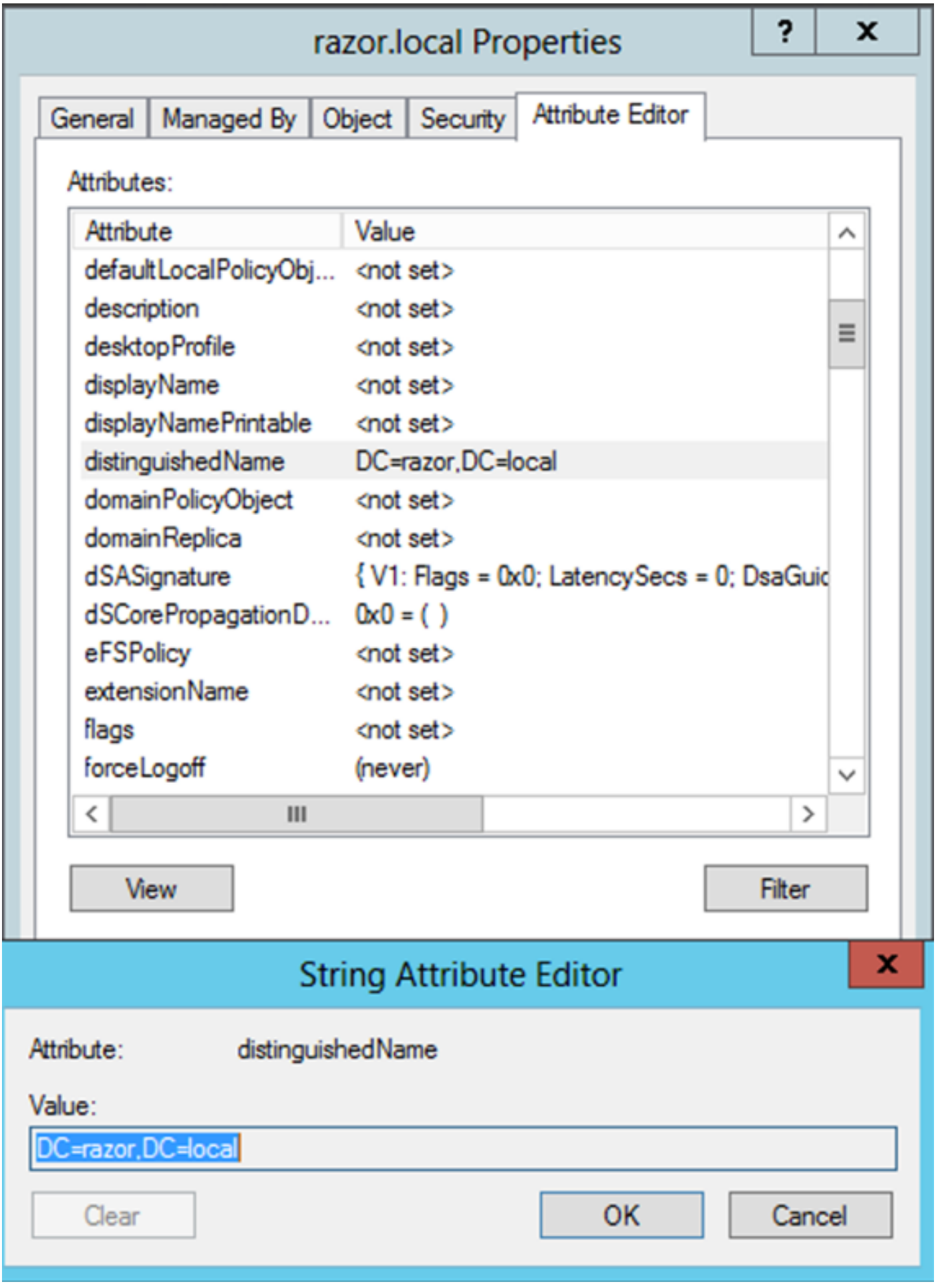
3. Cela permet d'afficher des propriétés supplémentaires sous les objets Active Directory. Par exemple, afin de trouver le DN pour la racine razor.local, clic droit razor.local, puis choisissez Properties, comme le montre cette image :



4. Sous Properties, sélectionnez la commande Attribute Editor s'affiche. Rechercher distinguishedName sous Attributs, puis cliquez sur View, comme l'illustre l'image.

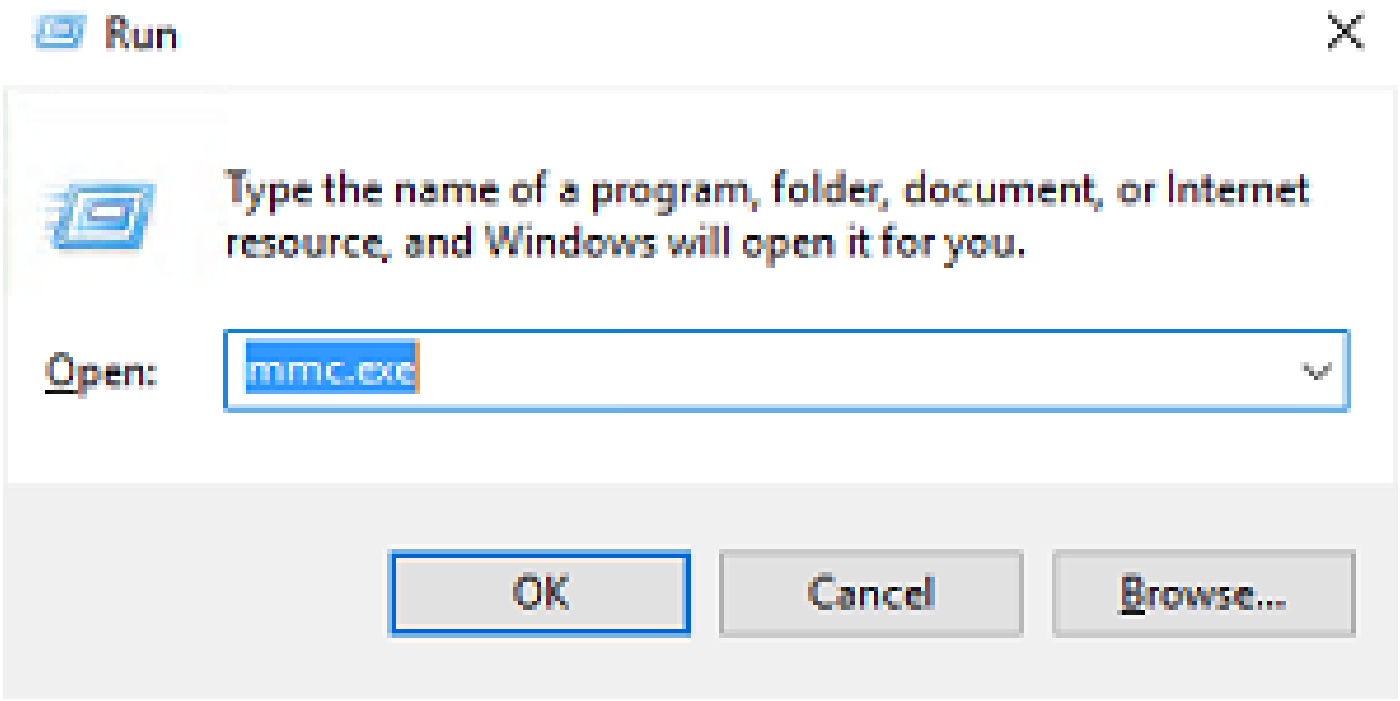
Une nouvelle fenêtre s'ouvre, dans laquelle le nom distinctif (DN) peut être copié et collé dans FMC ultérieurement.

Dans cet exemple, le DN racine est DC=razor, DC=local. Copiez la valeur et enregistrez-la pour plus tard. Cliquer OK afin de quitter la fenêtre Éditeur d'attributs de chaîne et cliquez sur OK afin de quitter les Propriétés.

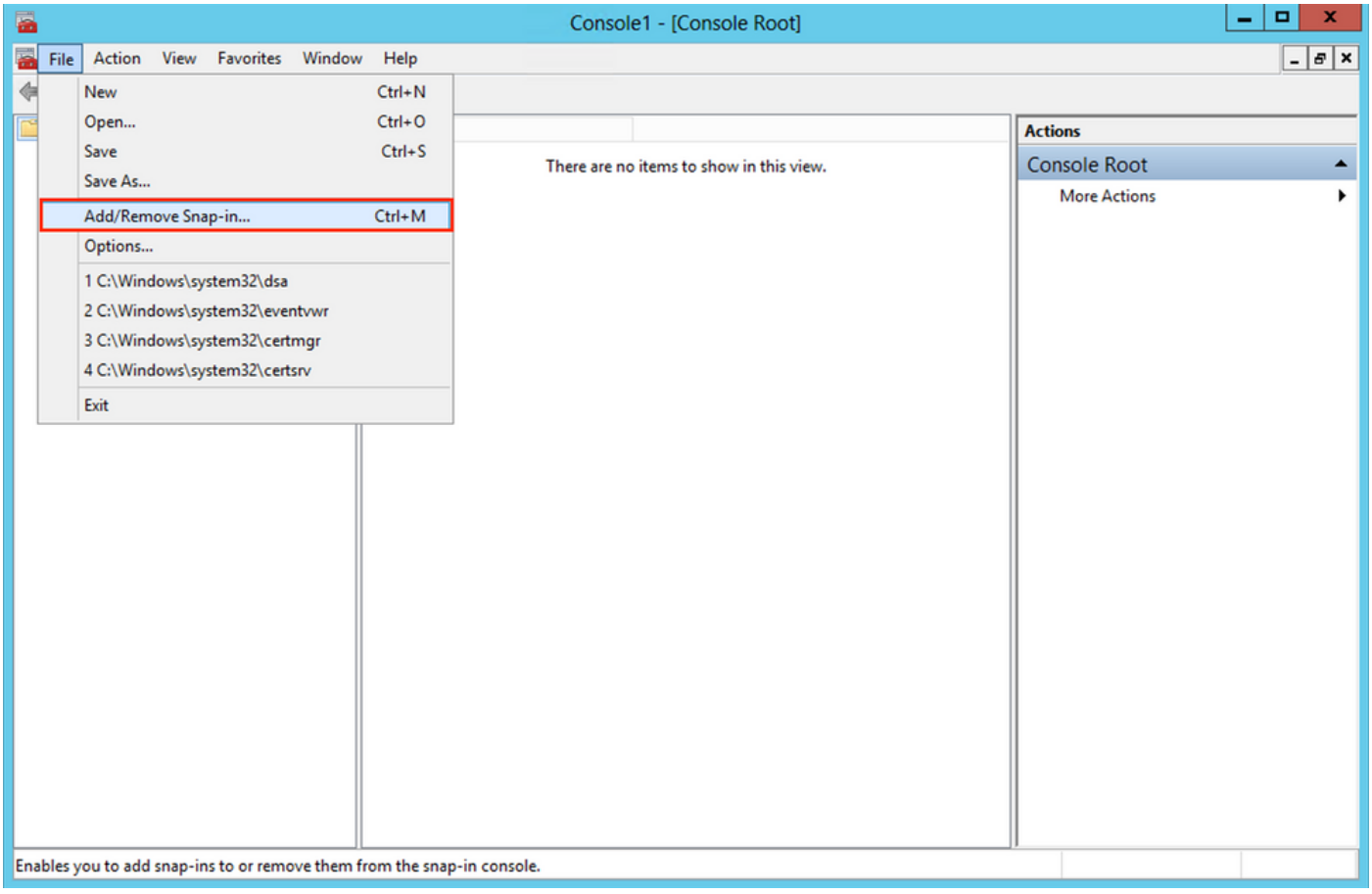

razor.local Properties
General
Managed By
Object
Security
Attribute Editor
Attributes:
Attribute
Value
defaultLocalPolicyObj...
<not set>
description
<not set>
desktopProfile
<not set>
displayName
<not set>
displayNamePrintable
<not set>
distinguishedName
DC=razor,DC=local
domainPolicyObject
<not set>
domainReplica
<not set>
dSASignature
{ V1: Flags = 0x0; LatencySecs = 0; DsaGuic
dSCorePropagationD...
0x0 = ( )
eFSPolicy
<not set>
extensionName
<not set>
flags
<not set>
forceLogoff
(never)
View
Filter
String Attribute Editor
Attribute:
distinguishedName
Value:
DC=razor,DC=local
Clear
OK
Cancel

Copier la racine du certificat SSL LDAPS

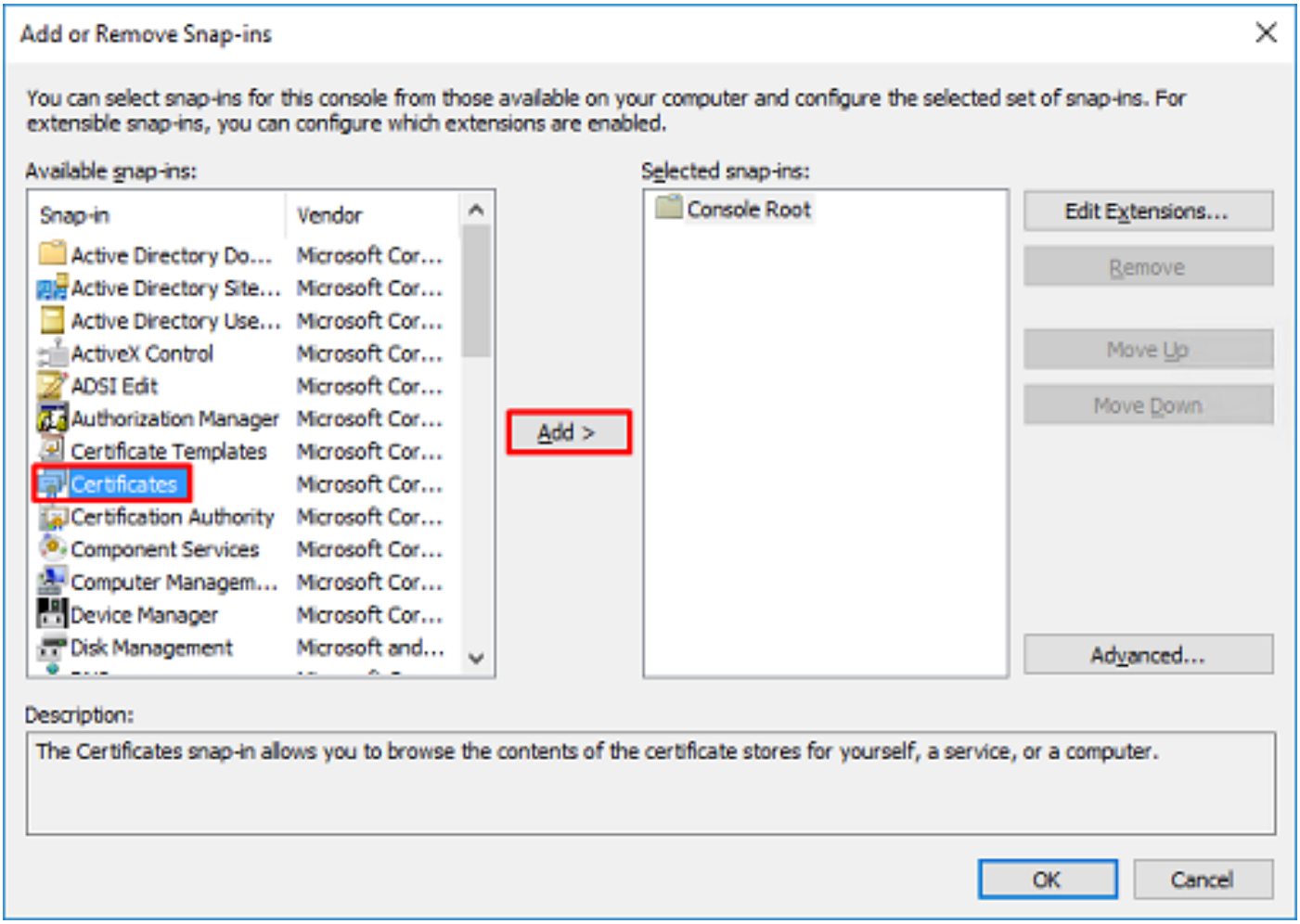
1. Presse Win+R et entrez mmc.exe, puis cliquez sur OK, comme le montre cette image.



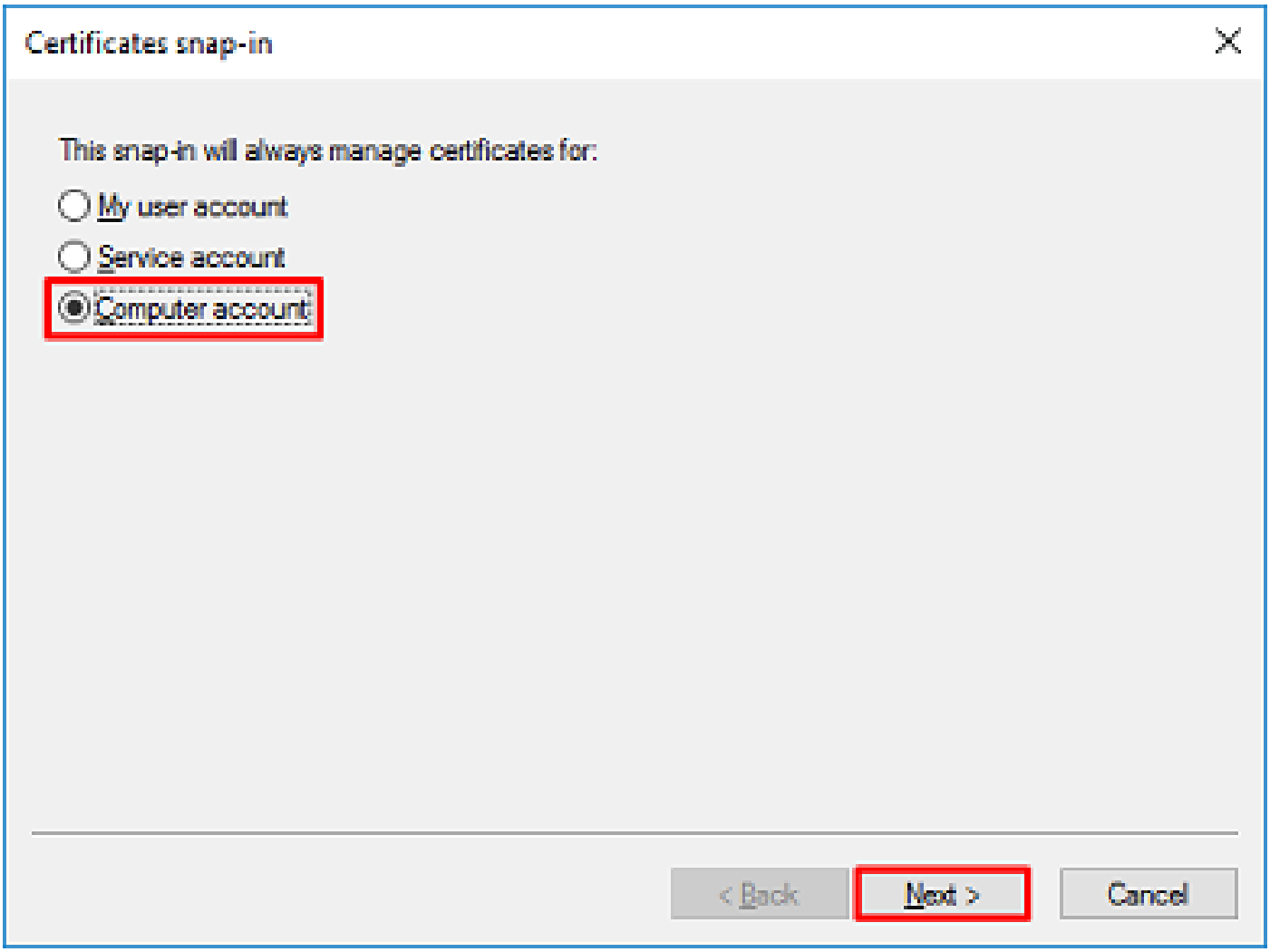
2. Naviguez jusqu'à File > Add/Remove Snap-in..., comme le montre cette image :



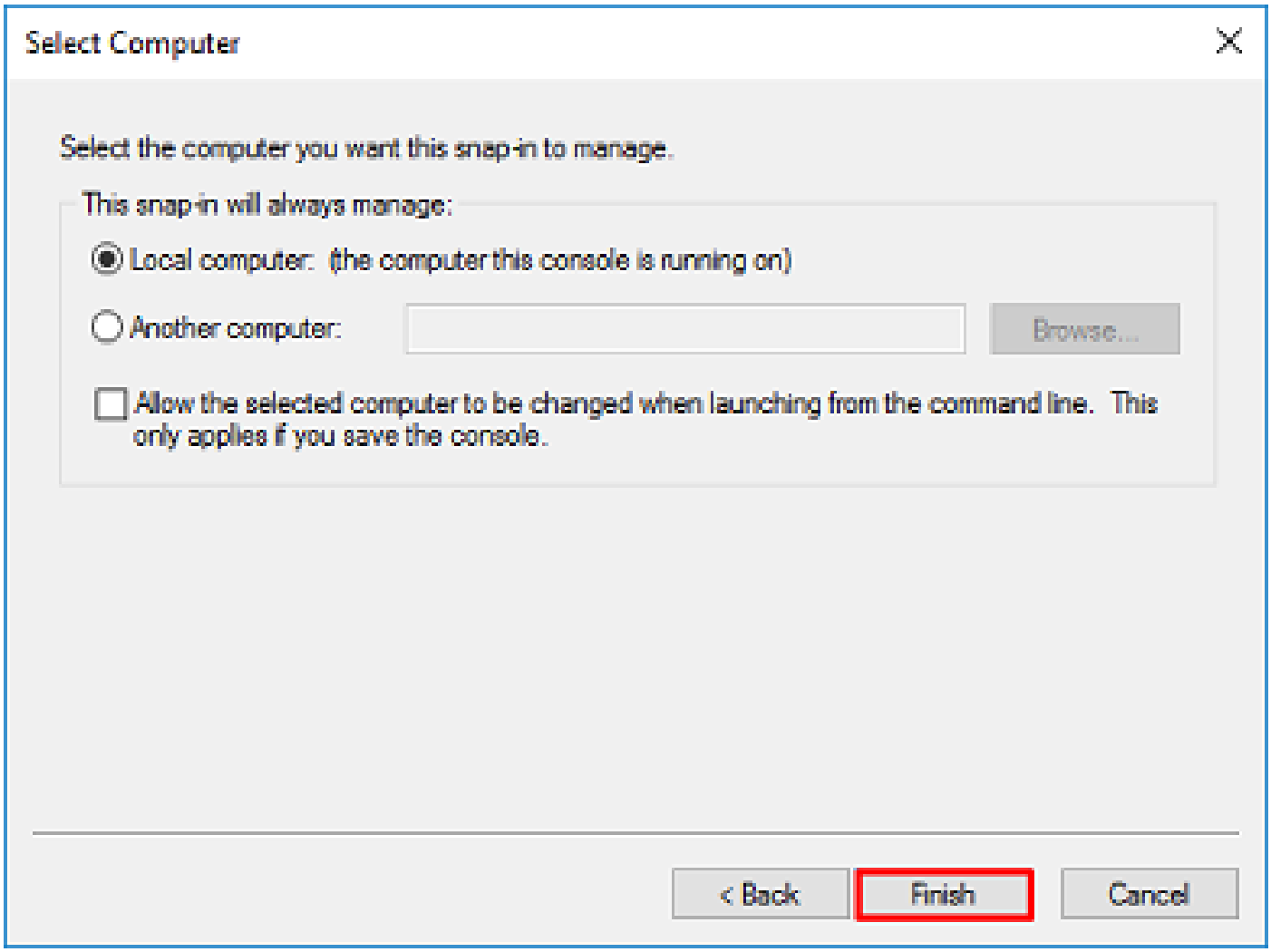
3. Sous Composants logiciels enfichables disponibles, sélectionnez Certificates puis cliquez sur Add, comme le montre cette image :



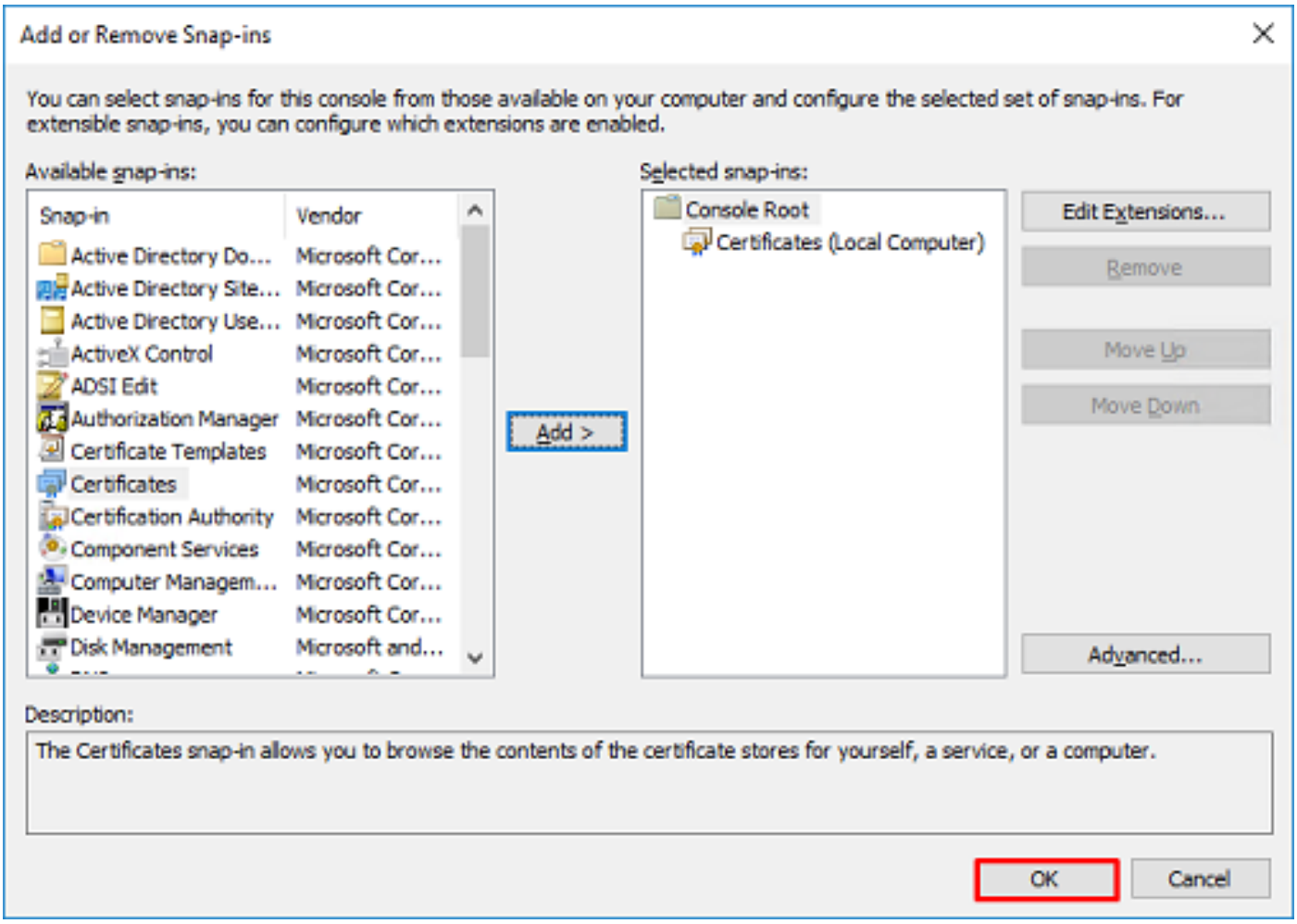
4. Choisir Computer account puis cliquez sur Next, comme le montre cette image :



Comme indiqué ici, cliquez sur Finish.



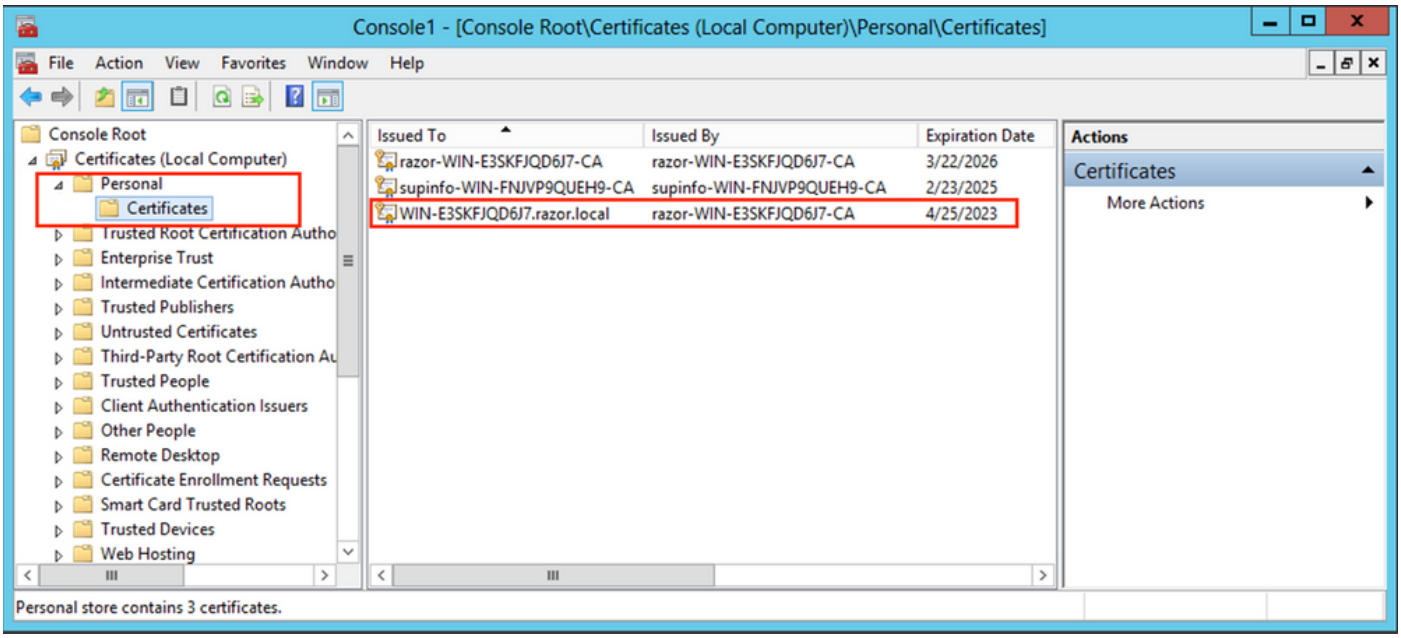
5. Maintenant, cliquez sur OK, comme le montre cette image.



6. Développez le Personal , puis cliquez sur Certificates. Le certificat utilisé par les LDAP doit être délivré au nom de domaine complet (FQDN) du serveur Windows. Sur ce serveur, trois certificats sont répertoriés :

- Un certificat CA a été délivré à et par razor-WIN-E3SKFJQD6J7-CA.
- Un certificat CA délivré à et par supinfo-WIN-FNJVP9QUEH9-CA.
- Un certificat d'identité a été délivré à WIN-E3SKFJQD6J7.razor.local par razor-WIN-E3SKFJQD6J7-CA.

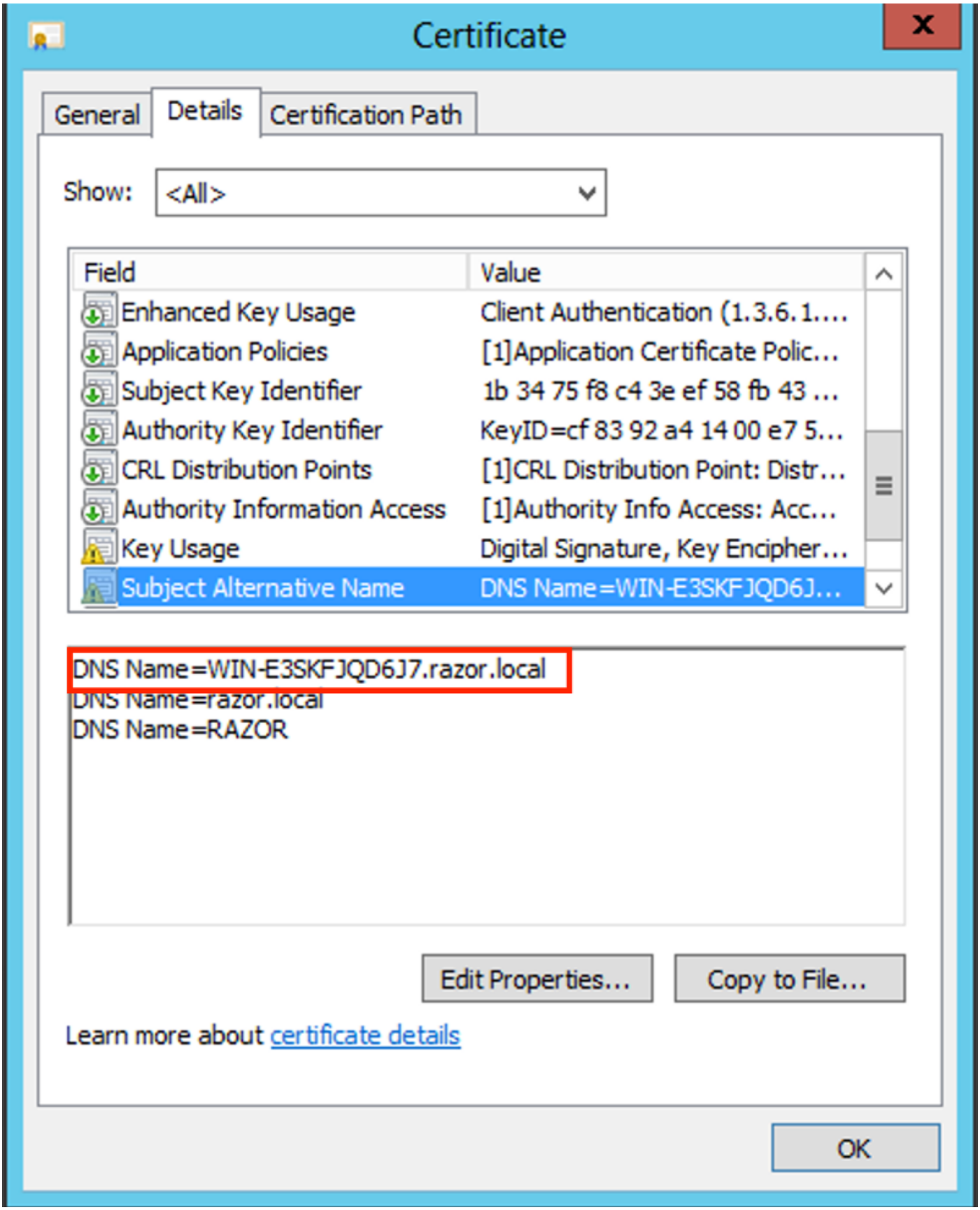
Dans ce guide de configuration, le nom de domaine complet est WIN-E3SKFJQD6J7.razor.local Les deux premiers certificats ne sont donc pas valides pour être utilisés comme certificat SSL LDAP. Le certificat d'identité délivré à WIN-E3SKFJQD6J7.razor.local est un certificat qui a été émis automatiquement par le service AC de Windows Server. Double-cliquez sur le certificat afin de vérifier les détails.



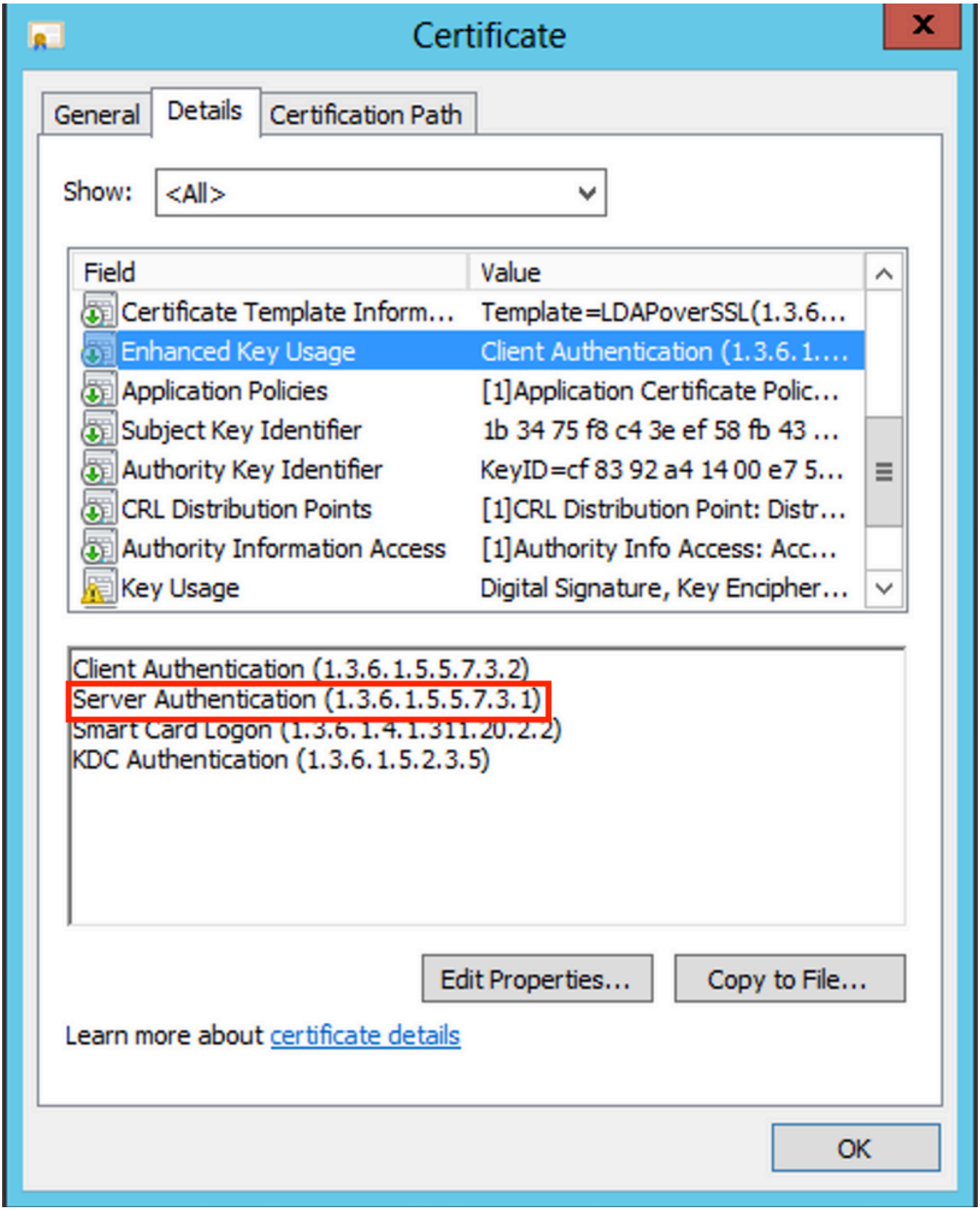
7. Pour être utilisé comme certificat SSL LDAP, le certificat doit répondre aux exigences suivantes :

- Le nom commun ou le nom secondaire de l'objet DNS correspond au nom de domaine complet de Windows Server.
- Le certificat dispose de l'authentification serveur dans le champ Enhanced Key Usage.

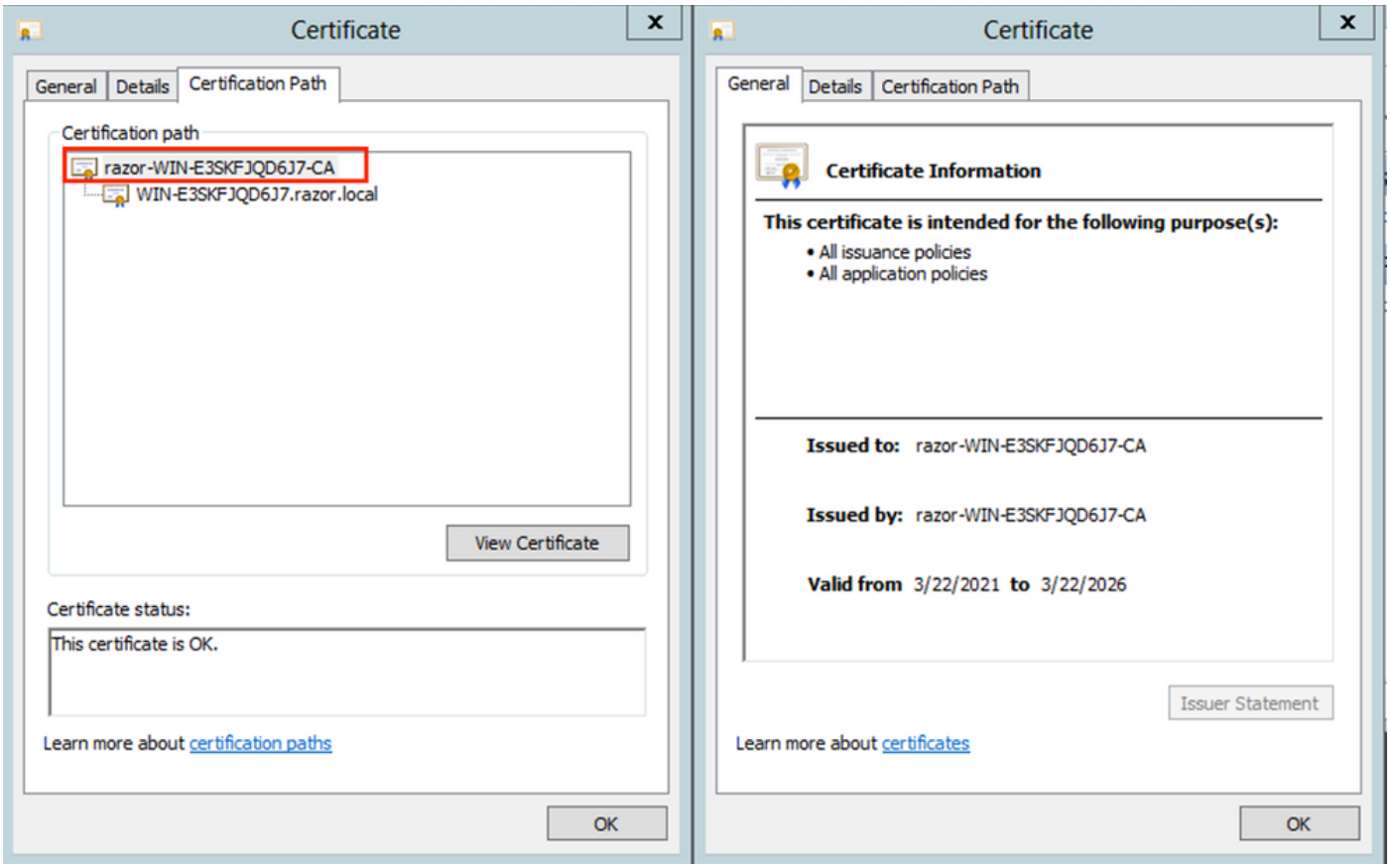
Sous la Details pour le certificat, sélectionnez Subject Alternative Name, où le nom de domaine complet WIN-E3SKFJQD6J7.razor.local est présent.



Sous Enhanced Key Usage, Server Authentication est présent.

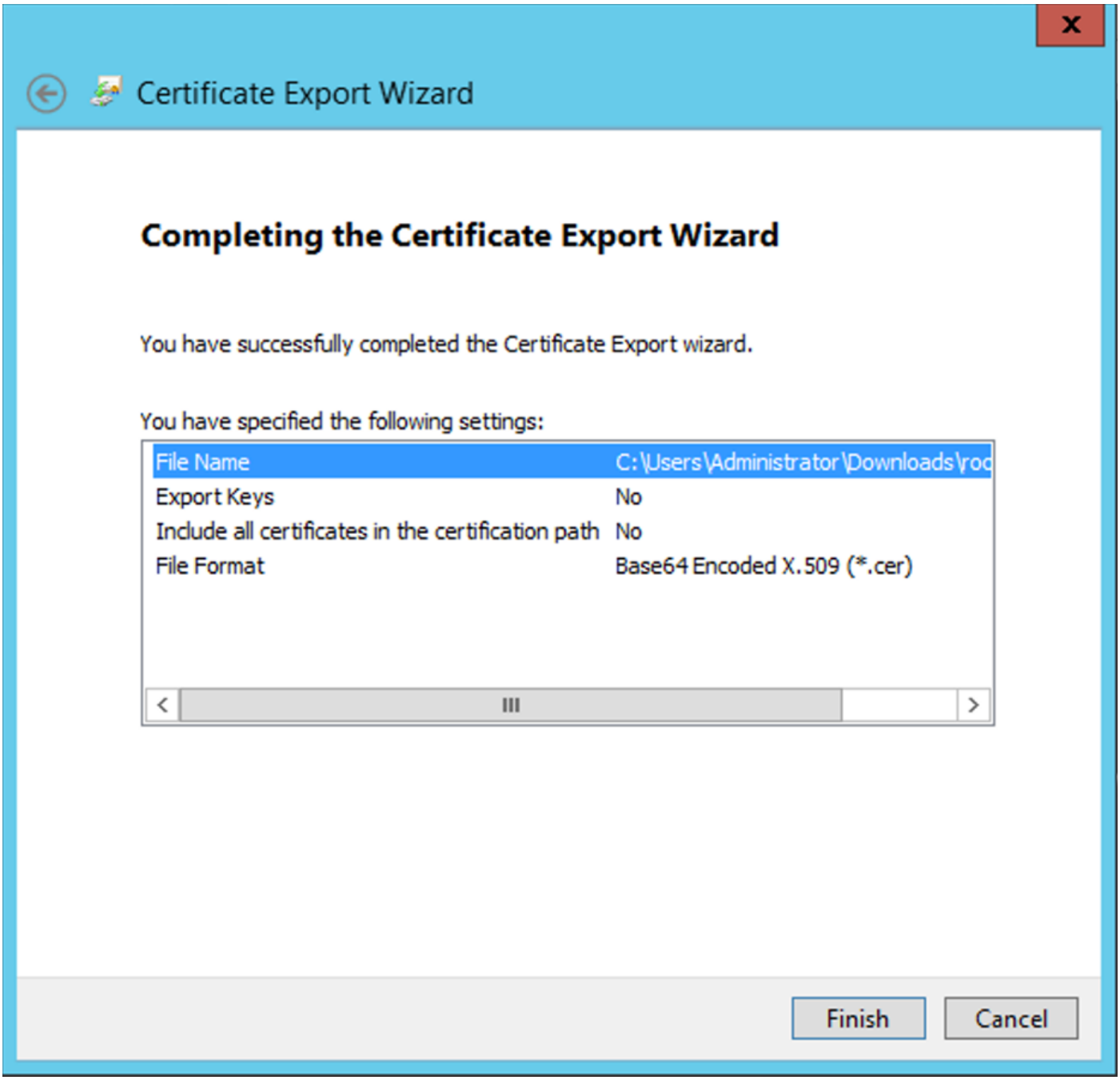


8. Une fois que cela est confirmé, sous la rubrique Certification Path , choisissez le certificat de niveau supérieur qui est le certificat d'autorité de certification racine, puis cliquez sur View Certificate. Les détails du certificat pour le certificat de l'autorité de certification racine s'ouvrent comme indiqué dans l'image :



9. Sous la Details du certificat CA racine, cliquez sur Copy to File et naviguez à travers leCertificate Export Wizard qui exporte la CA racine au format PEM.

Choisir Base-64 encoded X.509 comme format de fichier.



10. Ouvrez le certificat d'autorité de certification racine stocké à l'emplacement sélectionné sur la machine à l'aide d'un bloc-notes ou d'un autre éditeur de texte.

Affiche le certificat de format PEM. Enregistrez ceci pour plus tard.

```
-----BEGIN CERTIFICATE-----
MIIDfTCCAmWgAwIBAgIQV4ymxtI3BJ9JHnDL+luYazANBgkqhkiG9w0BAQUFADBRMRUwEwYKCZImiZPyLGQBGRYFbG9jYWwxFTATBgo
vcjEhMB8GA1UEAxMYcmF6b3ItV0lOLUUzU0tGSlFENko3LUNBMB4XDTIxMDMyMjE0MzMxNVoXDTI2MDMyMjE0NDMxNVowUTEVMBMGCg
BWxvY2FsMRUwEwYKCZImiZPyLGQBGRYFcmF6b3IxITAfBgNVBAMTGHJhem9yLVdJTi1FM1NLRkpRRDZKNy1DQTCCASIwDQYJKoZIhvc
CCAQoCggEBAL803nQ6xPpazjj+HBZYc+8fV++RXCG+cUnblxwtXOB2G4UxZ3LRrWznjXaSO2Rc3qVw4lnOAziGs4ZMNM1X8UWeKuwi8
9dkncZaGtQ1cPmqcnCWunfTsaENKbgoKi4eXjpwwUSbEYwU3OaiiI/tp422ydy3Kgl7Iqt1s4XqpZmTezykWra7dUyXfkuESk6lEOAV
CSkTQTRXYryy8dJrWjAF/n6A3VnS/l7Uhujlx4CD2OBkfQy6p5HpGxdc4GMTTnDzUL46ot6imeBXPHF0IJehh+tZk3bxpoxTDXECAwE
DAgGGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0OBBYEFM+DkqQUAOdY379NnViaMIJAVTZ1MBAGCSsGAQQBgjcVAQQDAgEAMA0GCSqGSI
AA4IBAQCiSm5U7U6Y7zXdx+dleJdOQmGgKayAAuYAD+MWNwC4NzFD8Yr7BnO6f/VnF6VGYPXa+Dvs7VLZewMNkp3i+VQpkBCKdhAV6q
4sMZffbVrGlRz7twWY36J5G5vhNUhzZ1N2OLw6wtHg2SO8XlvpTS5fAnyCZgSK3VPKfXnn1HLp7UH5/SWN2JbPL15r+wCW84b8nrylb
GuDsepY7/u2uWfy/vpTJigeok2DH6HFfOET3sE+7rsIAY+ofOkWW5gNwQ4hOwv4Goqj+YQRAXXi2OZyltHR1dfUUbwVENSFQtDnFA7X
```

```
-----END CERTIFICATE-----
```

En cas d'installation de plusieurs certificats dans le magasin de l'ordinateur local sur le serveur LDAP (facultatif)

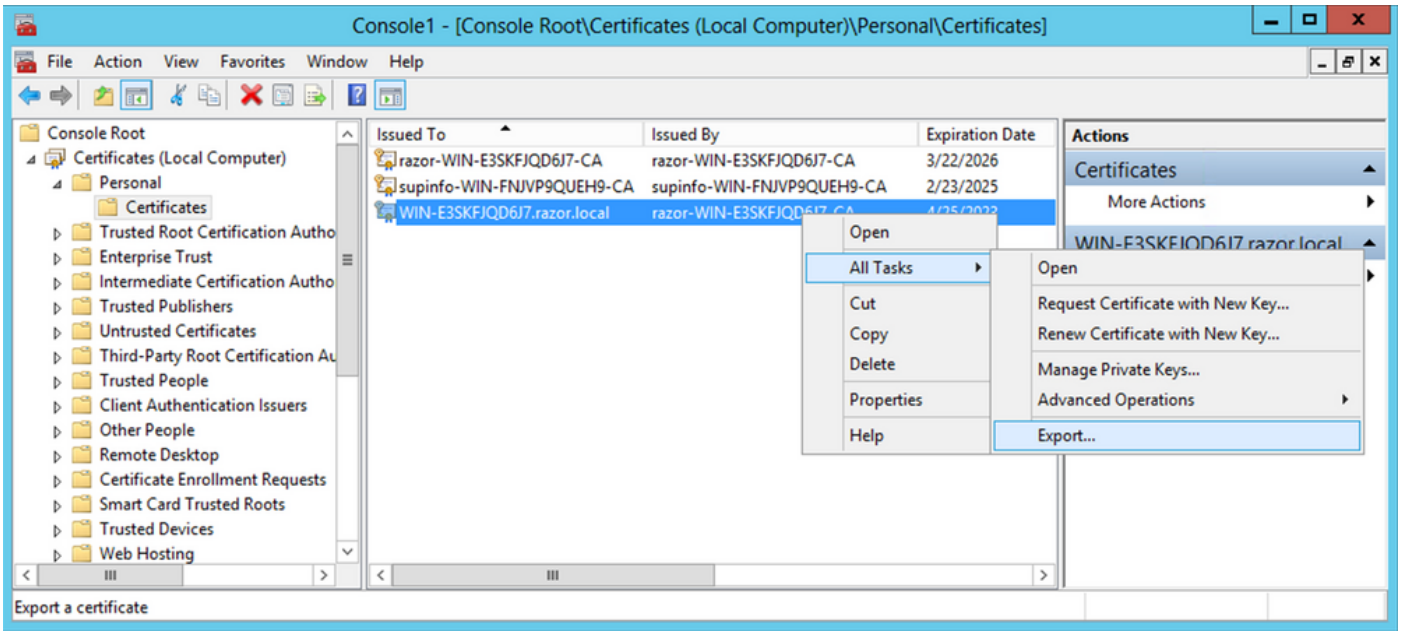
1. Dans une situation de certificats d’identité multiples qui peuvent être utilisés par LDAPS et lorsqu’il y a une incertitude quant à savoir lequel est utilisé, ou lorsqu’il n’y a pas d’accès au serveur LDAPS, il est toujours possible d’extraire l’autorité de certification racine d’une capture de paquets effectuée sur le FTD.

2. Dans le cas où vous avez plusieurs certificats valides pour l'authentification du serveur dans le magasin de certificats de l'ordinateur local du serveur LDAP (tel que le contrôleur de domaine AD DS), il peut être remarqué qu'un certificat différent est utilisé pour les communications LDAP. La meilleure solution à ce problème consiste à supprimer tous les certificats inutiles du magasin de certificats de l'ordinateur local et à n'avoir qu'un seul certificat valide pour l'authentification du serveur.

Toutefois, s'il existe une raison légitime pour laquelle vous avez besoin de deux certificats ou plus et que vous disposez au moins d'un serveur LDAP Windows Server 2008, le magasin de certificats des services de domaine Active Directory (NTDS\Personal) peut être utilisé pour les communications LDAP.

Ces étapes montrent comment exporter un certificat compatible LDAPS d'un magasin de certificats d'ordinateur local de contrôleur de domaine vers le magasin de certificats de service des services de domaine Active Directory (NTDS\Personal).

- Accédez à la console MMC sur le serveur Active Directory, sélectionnez Fichier, puis cliquez sur Add/Remove Snap-in.
- Cliquer Certificates puis cliquez sur Add.
- Dans la Certificates snap-in, choisissez Computer account puis cliquez sur Next.
- Dans Select Computer, choisissez Local Computer, cliquez sur OK, puis cliquez sur Finish. Dans Add or Remove Snap-ins, cliquez sur OK.
- Dans la console des certificats d'un ordinateur qui contient un certificat utilisé pour l'authentification du serveur, cliquez avec le bouton droit sur le certificate, cliquez sur All Tasks, puis cliquez sur Export.



- Exporter le certificat dans le pfx dans les sections suivantes. Référez-vous à cet article pour savoir comment exporter un certificat dans le pfx format à partir de MMC :

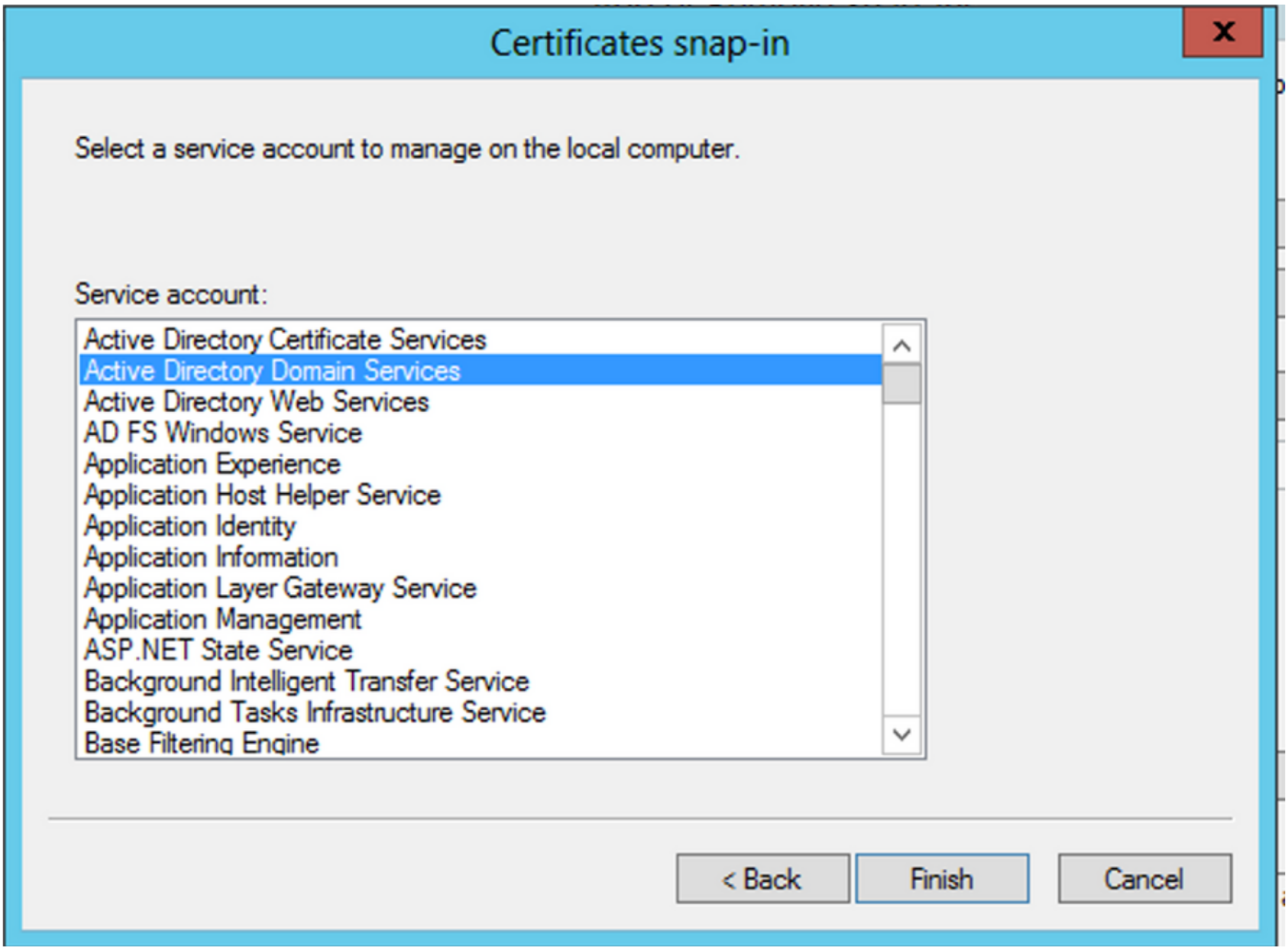
https://www.cisco.com/c/en/us/support/docs/security/web-security-appliance/118339-technote-wsa-00.html.

- Une fois l'exportation du certificat terminée, accédez à Add/Remove Snap-in activé MMC console. Cliquer Certificates puis cliquez sur Add.

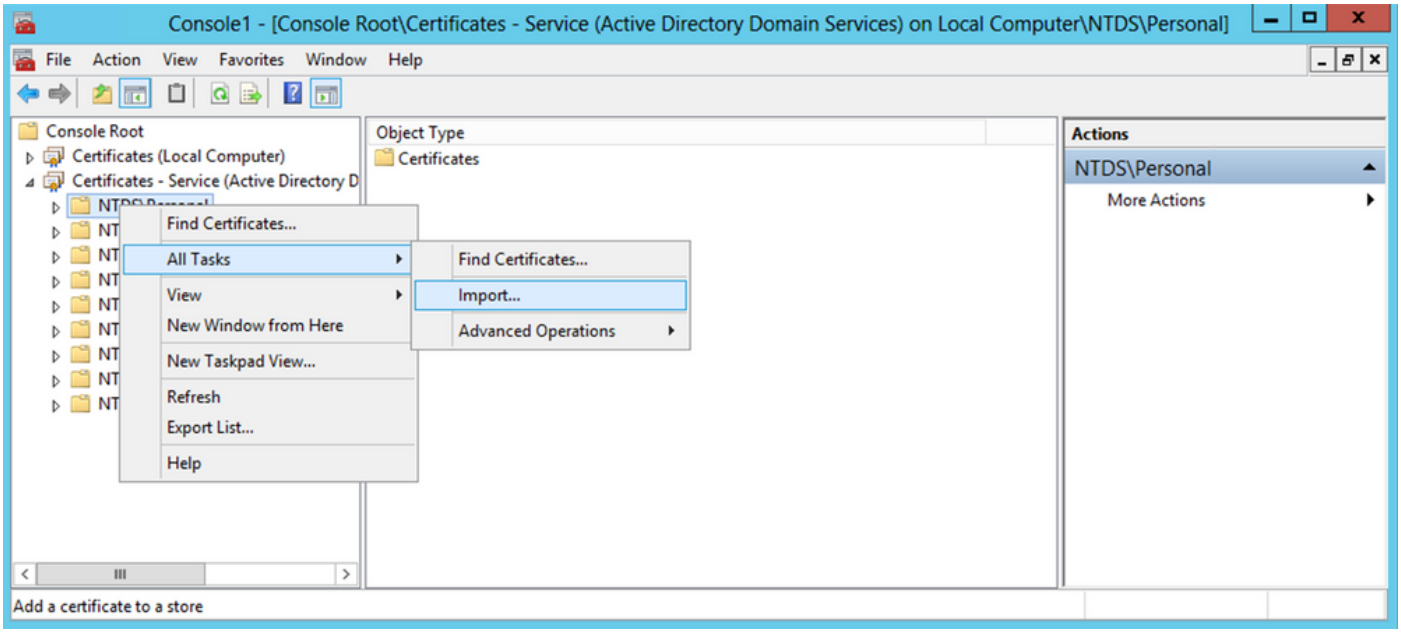
- Choisir Service account puis cliquez sur Next.

- Dans la Select Computer , choisissez Local Computer et cliquez sur Next.

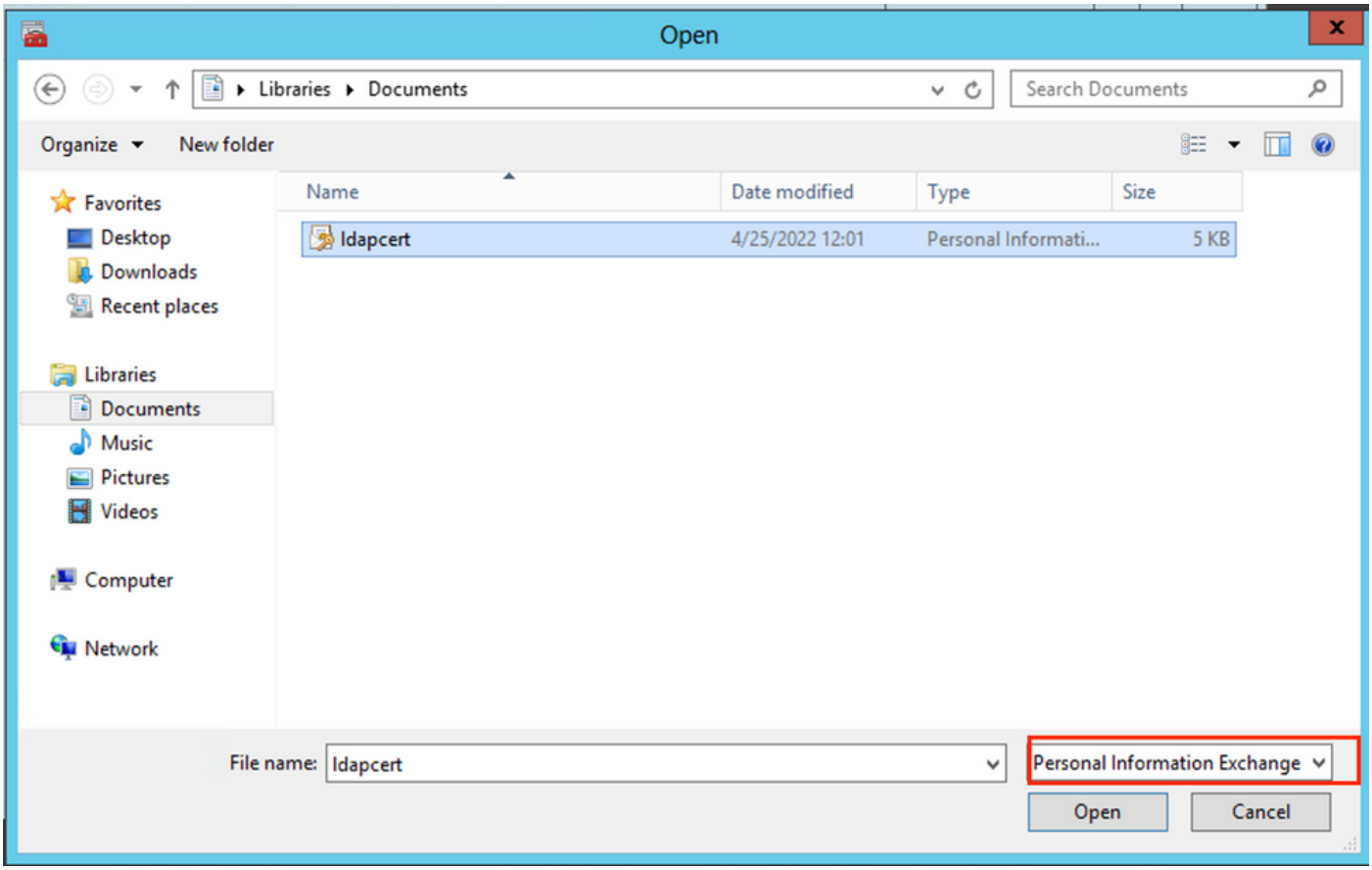
- Choisir Active Directory Domain Services puis cliquez sur Finish.



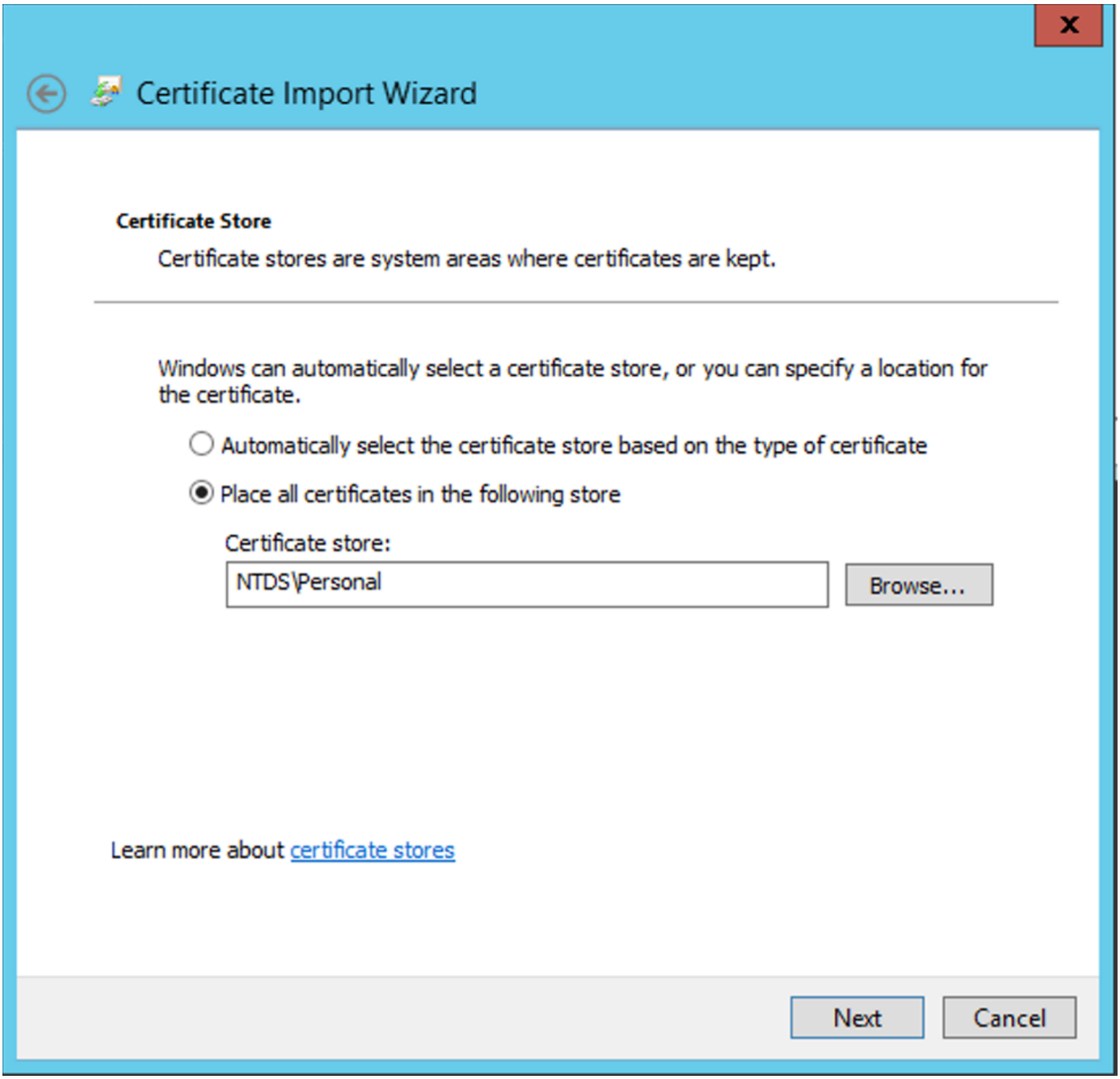
- Sur la page Add/Remove Snap-ins , cliquez sur OK.
- Accroissement Certificates - Services (Active Directory Domain Services) puis cliquez sur NTDS\Personal.
- Cliquer avec le bouton droit NTDS\Personal, cliquez sur All Tasks, puis cliquez sur Import.



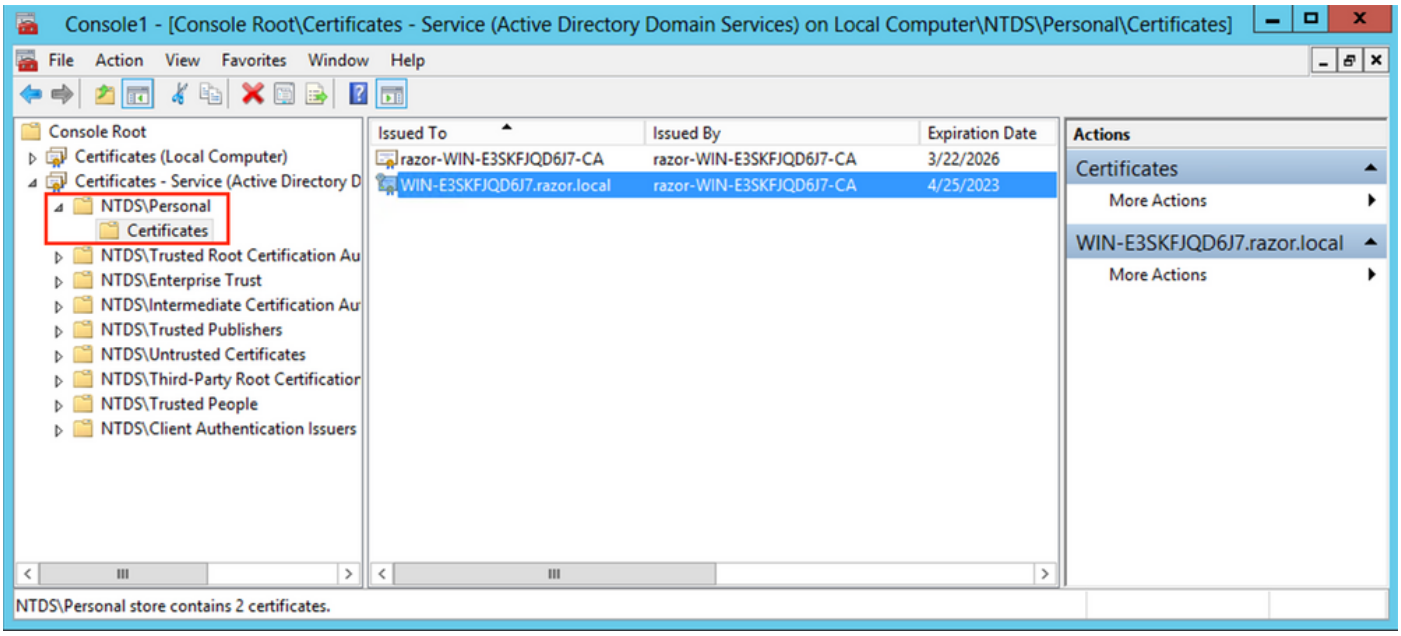
- Sur la page Certificate Import Wizard écran de bienvenue, cliquez sur Next.
- Dans l'écran Fichier à importer, cliquez sur Browseet localisez le fichier de certificat que vous avez exporté précédemment.
- Dans l'écran Ouvrir, vérifiez que l'échange d'informations personnelles (*pfx,*.p12) est sélectionné comme type de fichier, puis parcourez le système de fichiers pour localiser le certificat que vous avez exporté précédemment. Cliquez ensuite sur ce certificat.



- Cliquer Open puis cliquez sur Next.
- Dans l'écran Mot de passe, entrez le mot de passe que vous avez défini pour le fichier, puis cliquez sur Next.
- Sur la page Magasin de certificats, assurez-vous que l'option Placer tous les certificats est sélectionnée et lisez Magasin de certificats : NTDS\Personal puis cliquez sur Next.



- Sur la page Certificate Import Wizard écran de fin, cliquez sur Finish. Un message s'affiche pour indiquer que l'importation a réussi. Cliquer OK. Le certificat a été importé sous le magasin de certificats : NTDS\Personal.



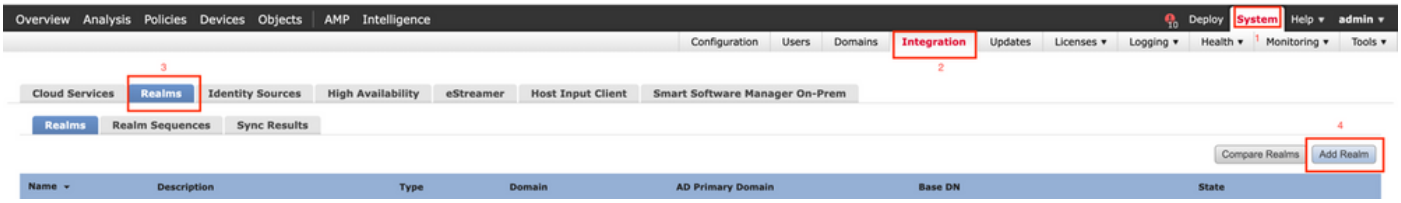
Configurations FMC

Vérifier les licences

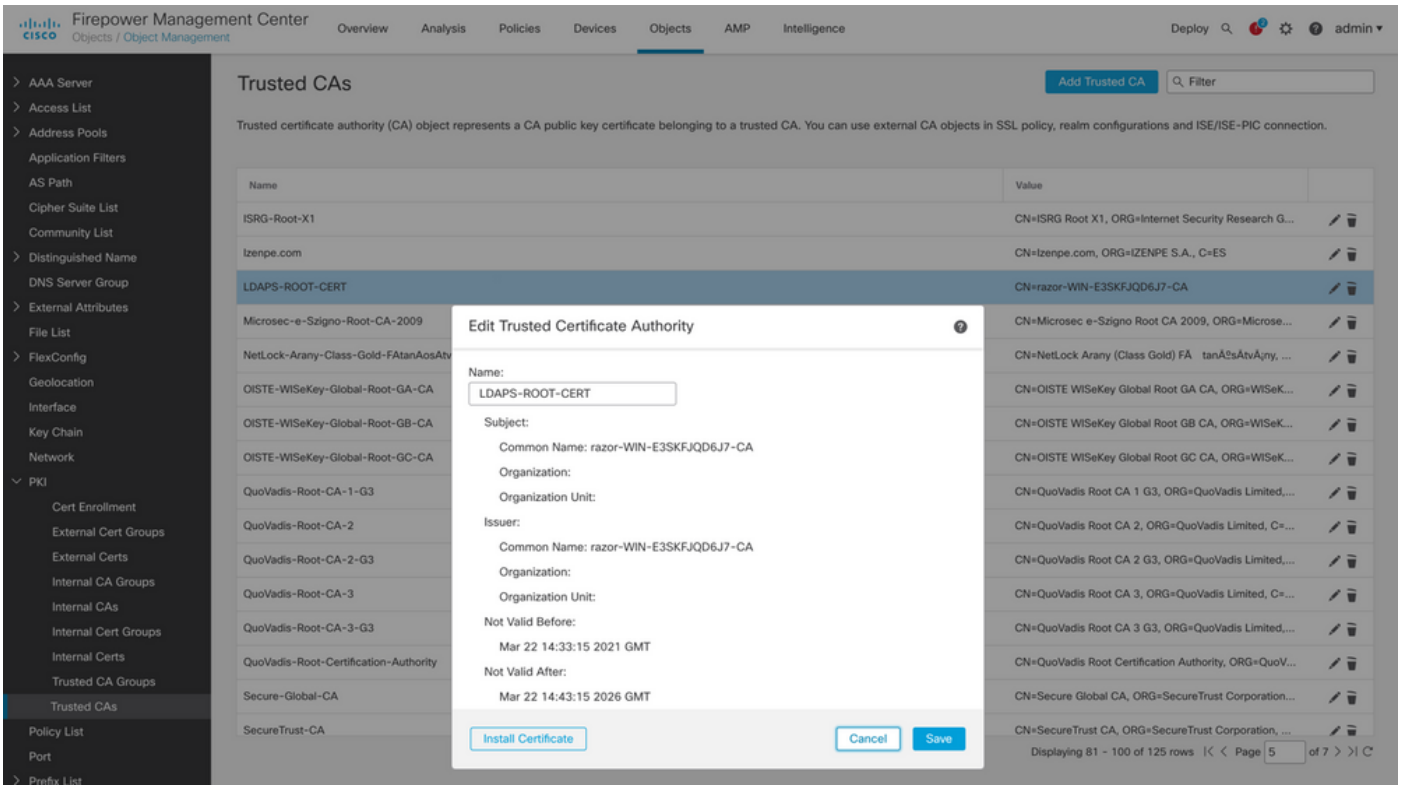
Pour déployer la configuration AnyConnect, le FTD doit être enregistré auprès du serveur de licences Smart et une licence Plus, Apex ou VPN Only valide doit être appliquée au périphérique.

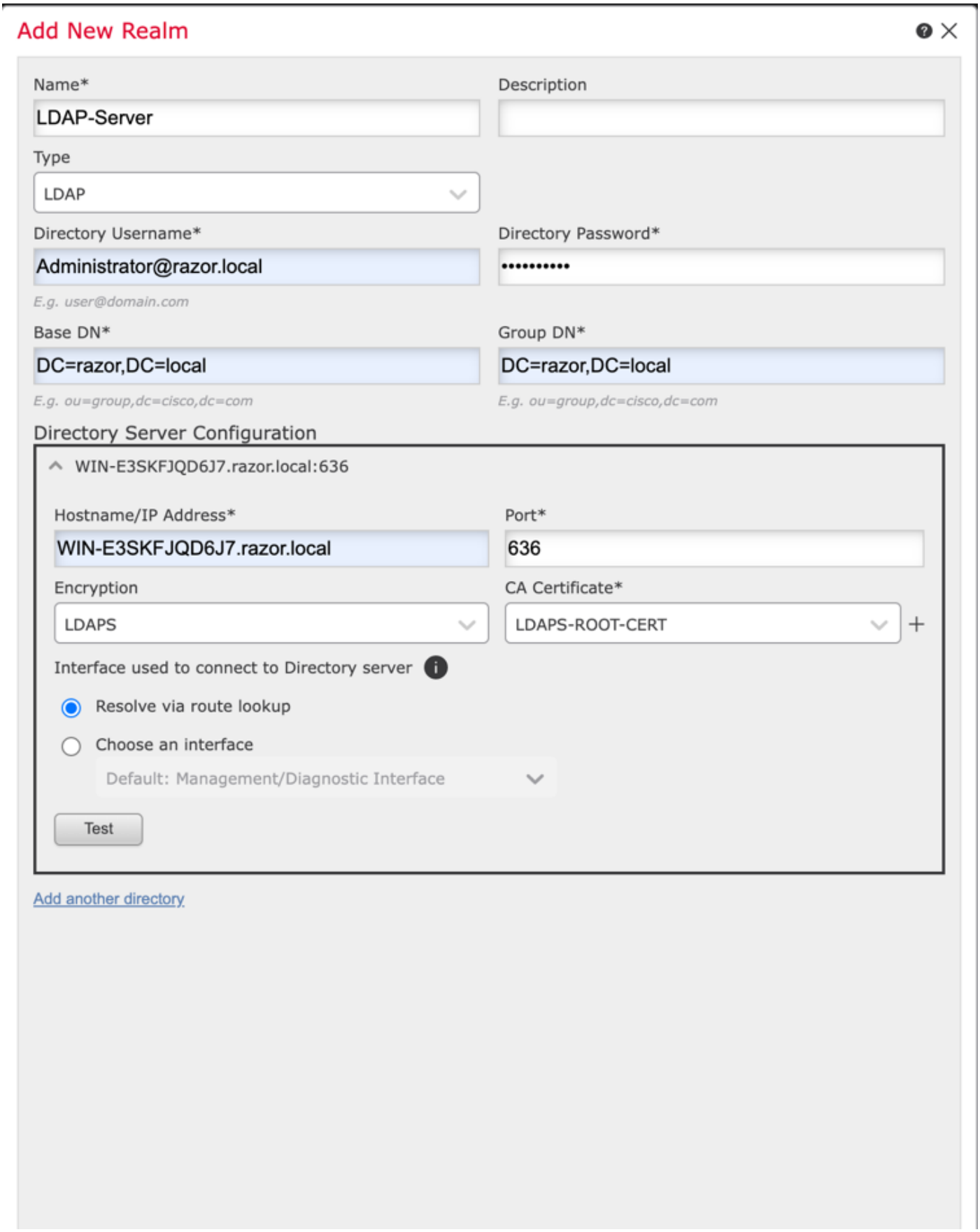
Configurer le domaine

1. Naviguez jusqu'à System > Integration. Naviguez jusqu'à Realms, puis cliquez sur Add Realm, comme le montre cette image :



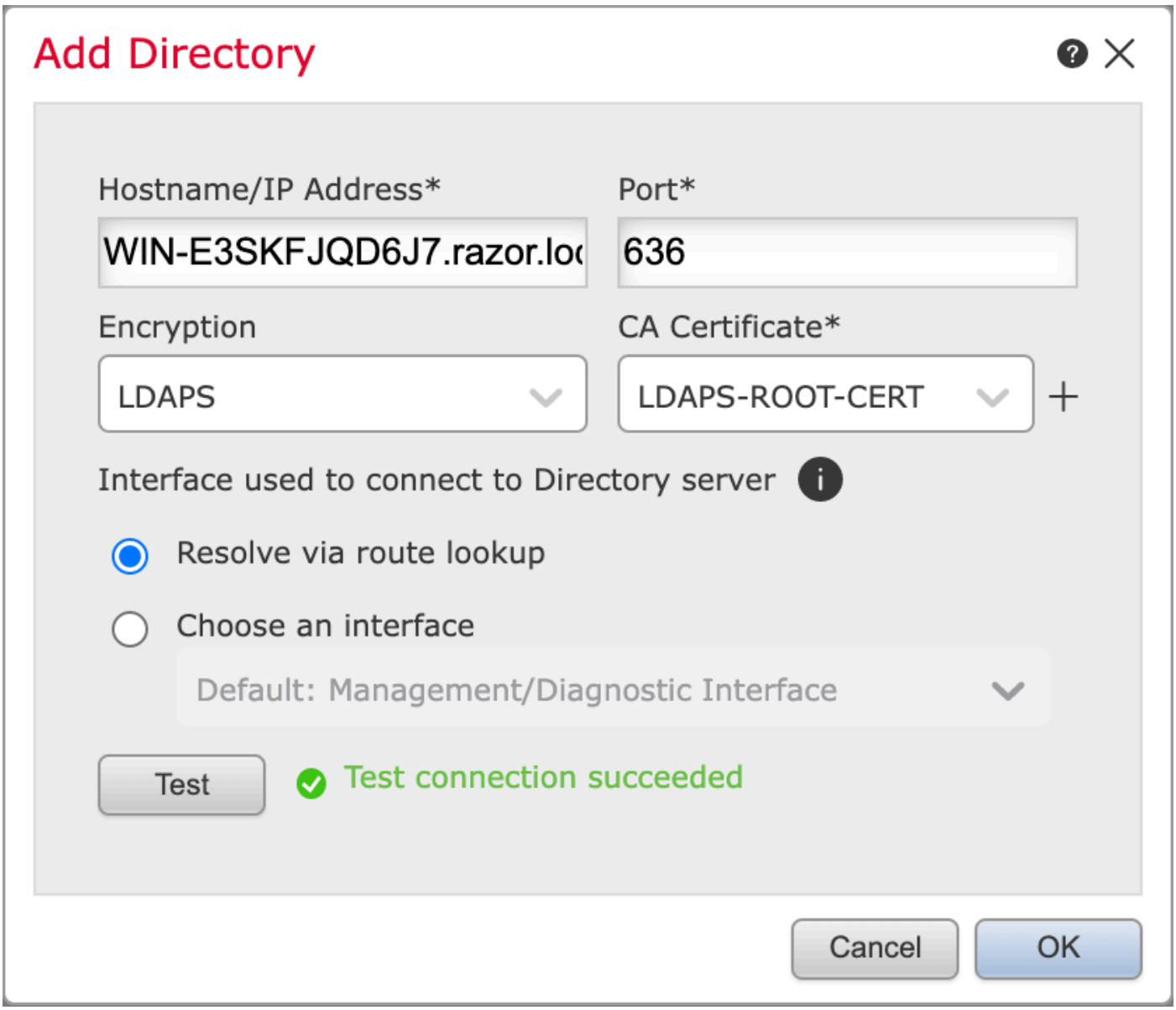
2. Remplissez les champs affichés en fonction des informations collectées à partir du serveur Microsoft pour les LDAP. Avant cela, importez le certificat d'autorité de certification racine qui a signé le certificat de service LDAP sur le serveur Windows sous Objects > PKI > Trusted CAs > Add Trusted CA, car il est référencé dans la sectionDirectory Server Configuration du royaume. Une fois terminé, cliquez sur OK.


Firepower Management Center
Objects / Object Management
Overview
Analysis
Policies
Devices
Objects
AMP
Intelligence
Deploy
admin
AAA Server
Access List
Address Pools
Application Filters
AS Path
Cipher Suite List
Community List
Distinguished Name
DNS Server Group
External Attributes
File List
FlexConfig
Geolocation
Interface
Key Chain
Network
PKI
Cert Enrollment
External Cert Groups
External Certs
Internal CA Groups
Internal CAs
Internal Cert Groups
Internal Certs
Trusted CA Groups
Trusted CAs
Policy List
Port
Trusted CAs
Add Trusted CA
Filter
Trusted certificate authority (CA) object represents a CA public key certificate belonging to a trusted CA. You can use external CA objects in SSL policy, realm configurations and ISE/ISE-PIC connection.
Name
Value
ISRG-Root-X1
CN=ISRG Root X1, ORG=Internet Security Research G...
Izenpe.com
CN=Izenpe.com, ORG=IZENPE S.A., C=ES
LDAPS-ROOT-CERT
CN=razor-WIN-E3SKFJQD6J7-CA
Microsec-e-Szigno-Root-CA-2009
CN=Microsec e-Szigno Root CA 2009, ORG=Microse...
NetLock-Arany-Class-Gold-FAtanAosAtv
CN=NetLock Arany (Class Gold) FÁ tanÚsÁtvÁny, ...
OISTE-WISeKey-Global-Root-GA-CA
CN=OISTE WISeKey Global Root GA CA, ORG=WISeK...
OISTE-WISeKey-Global-Root-GB-CA
CN=OISTE WISeKey Global Root GB CA, ORG=WISeK...
OISTE-WISeKey-Global-Root-GC-CA
CN=OISTE WISeKey Global Root GC CA, ORG=WISeK...
QuoVadis-Root-CA-1-G3
CN=QuoVadis Root CA 1 G3, ORG=QuoVadis Limited,...
QuoVadis-Root-CA-2
CN=QuoVadis Root CA 2, ORG=QuoVadis Limited, C=...
QuoVadis-Root-CA-2-G3
CN=QuoVadis Root CA 2 G3, ORG=QuoVadis Limited,...
QuoVadis-Root-CA-3
CN=QuoVadis Root CA 3, ORG=QuoVadis Limited, C=...
QuoVadis-Root-CA-3-G3
CN=QuoVadis Root CA 3 G3, ORG=QuoVadis Limited,...
QuoVadis-Root-Certification-Authority
CN=QuoVadis Root Certification Authority, ORG=QuoV...
Secure-Global-CA
CN=Secure Global CA, ORG=SecureTrust Corporation...
SecureTrust-CA
CN=SecureTrust CA, ORG=SecureTrust Corporation, ...
Displaying 81 - 100 of 125 rows
Page 5 of 7
Edit Trusted Certificate Authority
Name:
LDAPS-ROOT-CERT
Subject:
Common Name: razor-WIN-E3SKFJQD6J7-CA
Organization:
Organization Unit:
Issuer:
Common Name: razor-WIN-E3SKFJQD6J7-CA
Organization:
Organization Unit:
Not Valid Before:
Mar 22 14:33:15 2021 GMT
Not Valid After:
Mar 22 14:43:15 2026 GMT
Install Certificate
Cancel
Save

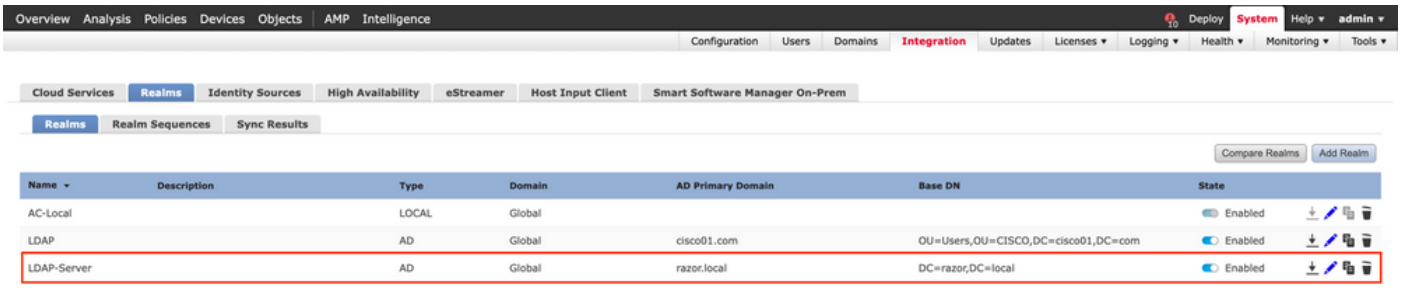


3. Cliquer Test afin de s'assurer que FMC peut se lier correctement avec le nom d'utilisateur et le mot de passe du répertoire fournis à l'étape précédente. Puisque ces tests sont initiés à partir du FMC et non par l'intermédiaire d'une des interfaces routables configurées sur le FTD (comme l'intérieur, l'extérieur, dmz), une connexion réussie (ou échouée) ne garantit

pas le même résultat pour l'authentification AnyConnect puisque les demandes d'authentification LDAP AnyConnect sont initiées à partir de l'une des interfaces routables FTD.



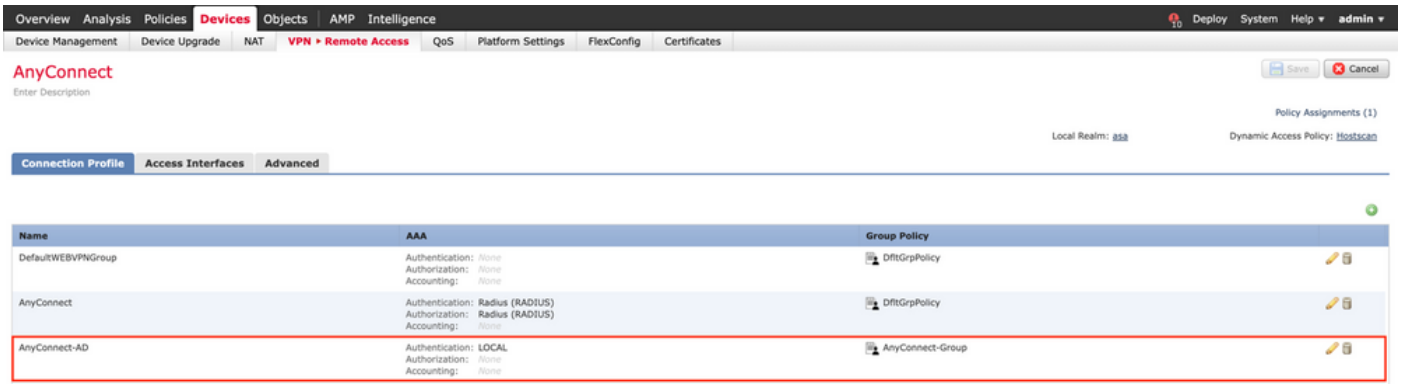
4. Activez le nouveau domaine.



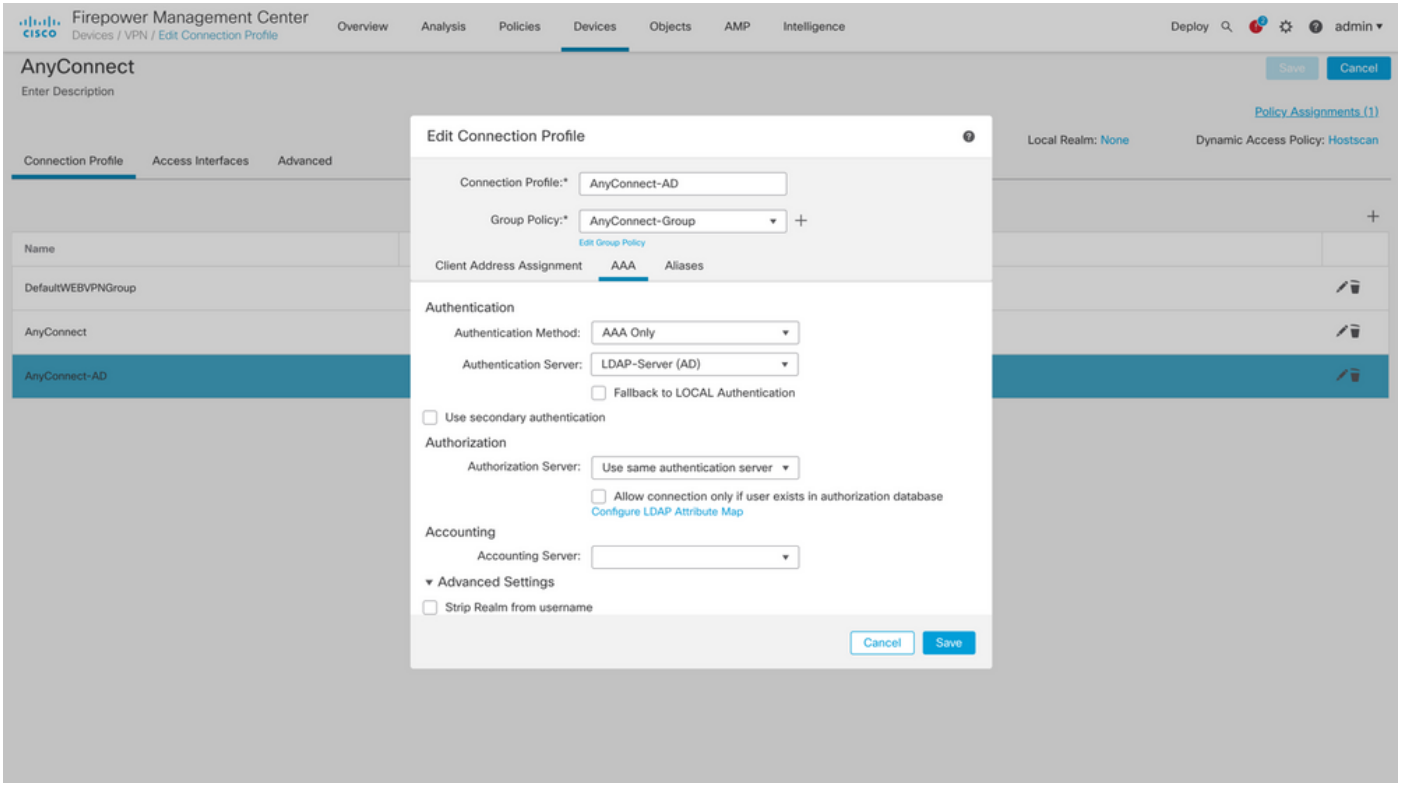
Configurer AnyConnect pour la gestion des mots de passe

1. Choisissez le profil de connexion existant ou créez-en un nouveau, s'il s'agit d'une configuration initiale d'AnyConnect. Ici, un profil de connexion existant nommé «

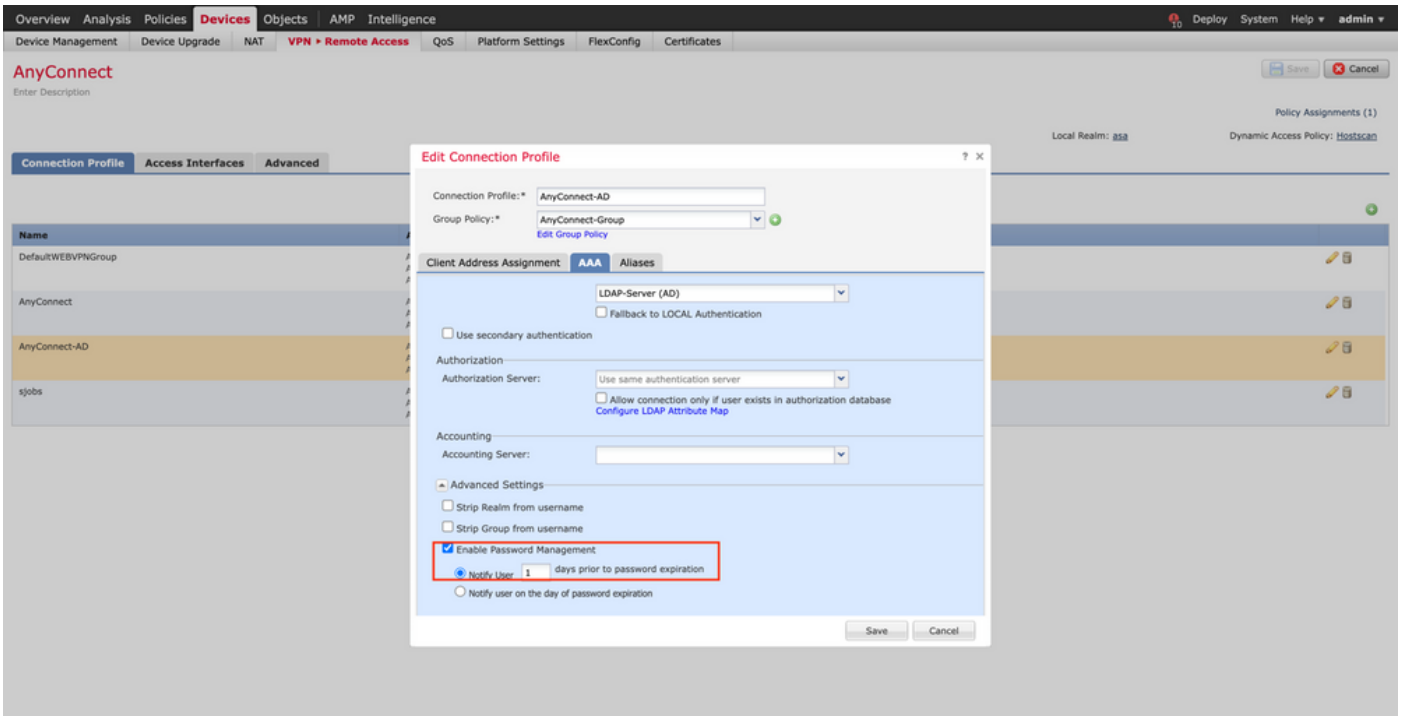
AnyConnect-AD » mappé avec l'authentification locale est utilisé.



2. Modifiez le profil Connection et mappez le nouveau serveur LDAP configuré aux étapes précédentes, sous les paramètres AAA du profil Connection. Une fois terminé, cliquez sur Save dans l'angle supérieur droit.



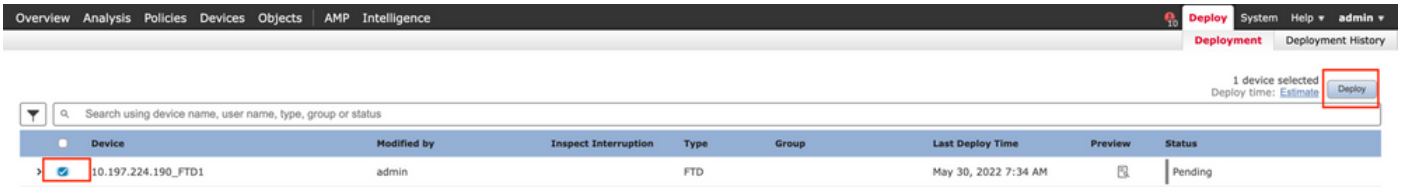
3. Activez la gestion des mots de passe sous AAA > Advanced Settings et enregistrez la configuration.



Déploiement

1. Une fois la configuration terminée, cliquez sur le boutonDeploy en haut à droite.

2. Cochez la case en regard de la configuration FTD qui lui est appliquée, puis cliquez sur Deploy, comme le montre cette image :



Configuration finale

Il s'agit de la configuration affichée dans l'interface de ligne de commande du FTD après le déploiement réussi.

Configuration AAA

<#root>

```
> show running-config aaa-server
```

```
aaa-server LDAP-Server protocol ldap
```

```
                                                    <------ aaa-server group configured for LDAPs

 max-failed-attempts 4
 realm-id 8
aaa-server LDAP-Server host WIN-E3SKFJQD6J7.razor.local
                          <-------- LDAPs Server to which the queries are sent

 server-port 636
 ldap-base-dn DC=razor,DC=local
 ldap-group-base-dn DC=razor,DC=local
 ldap-scope subtree
 ldap-naming-attribute sAMAccountName
 ldap-login-password *****
 ldap-login-dn *****@razor.local
 ldap-over-ssl enable
 server-type microsoft
```

Configuration AnyConnect

<#root>

```
> show running-config webvpn

webvpn
 enable Outside
 anyconnect image disk0:/csm/anyconnect-win-4.10.01075-webdeploy-k9.pkg 1 regex "Windows"
 anyconnect profiles FTD-Client-Prof disk0:/csm/ftd.xml
 anyconnect enable
 tunnel-group-list enable
 cache
  no disable
error-recovery disable
```

```
> show running-config tunnel-group

tunnel-group AnyConnect-AD type remote-access
tunnel-group AnyConnect-AD general-attributes
 address-pool Pool-1
authentication-server-group LDAP-Server                                    <-------- LDAPs Serve

 default-group-policy AnyConnect-Group
 password-management password-expire-in-days 1                          <-------- Password-management

tunnel-group AnyConnect-AD webvpn-attributes
 group-alias Dev enable


> show running-config group-policy AnyConnect-Group

group-policy
AnyConnect-Group
 internal
<--------- Group-Policy configuration that is mapped once the user is authenticated

group-policy AnyConnect-Group attributes
 vpn-simultaneous-logins 3
 vpn-idle-timeout 35791394
 vpn-idle-timeout alert-interval 1
 vpn-session-timeout none
 vpn-session-timeout alert-interval 1
 vpn-filter none
vpn-tunnel-protocol ikev2 ssl-client                                       <-------- Protocol

 split-tunnel-policy tunnelspecified
```

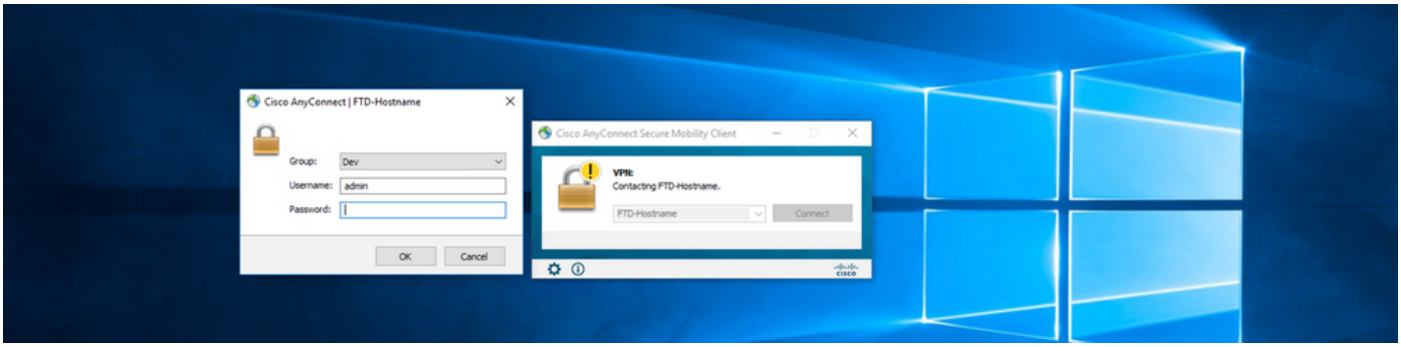
```
 split-tunnel-network-list value Remote-Access-Allow
 default-domain none
 split-dns none
 split-tunnel-all-dns disable
 client-bypass-protocol disable
 vlan none
 address-pools none
 webvpn
  anyconnect ssl dtls enable
  anyconnect mtu 1406
  anyconnect firewall-rule client-interface public none
  anyconnect firewall-rule client-interface private none
  anyconnect ssl keepalive 20
  anyconnect ssl rekey time none
  anyconnect ssl rekey method none
  anyconnect dpd-interval client 30
  anyconnect dpd-interval gateway 30
  anyconnect ssl compression none
  anyconnect dtls compression none
  anyconnect modules value none
  anyconnect profiles value FTD-Client-Prof type user
  anyconnect ask none default anyconnect
  anyconnect ssl df-bit-ignore disable
```

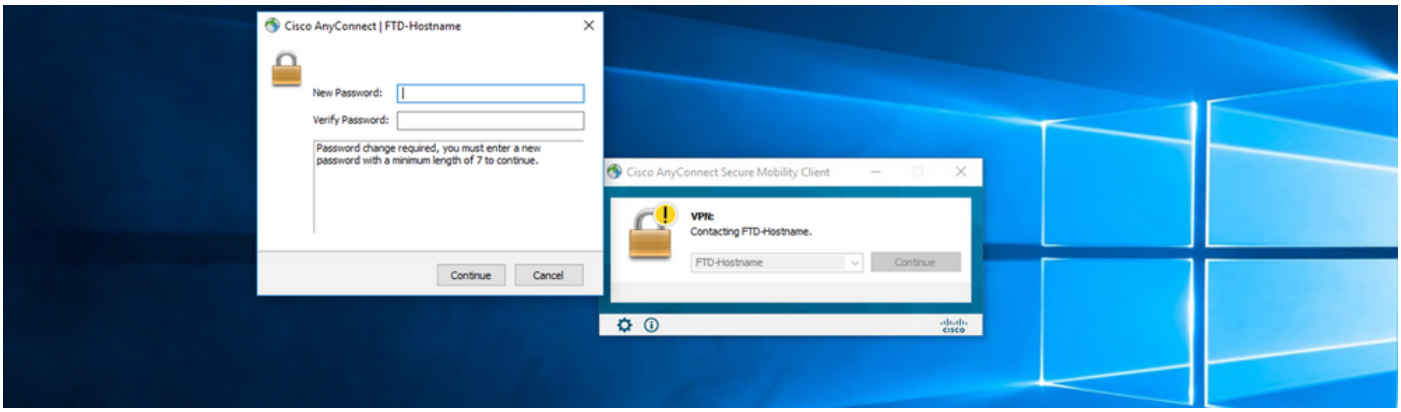
```
> show running-config ssl

ssl trust-point ID-New-Cert Outside
  <-------- FTD ID-cert trustpoint name mapped to the outside interface on which AnyConnect Connections
```

Vérification

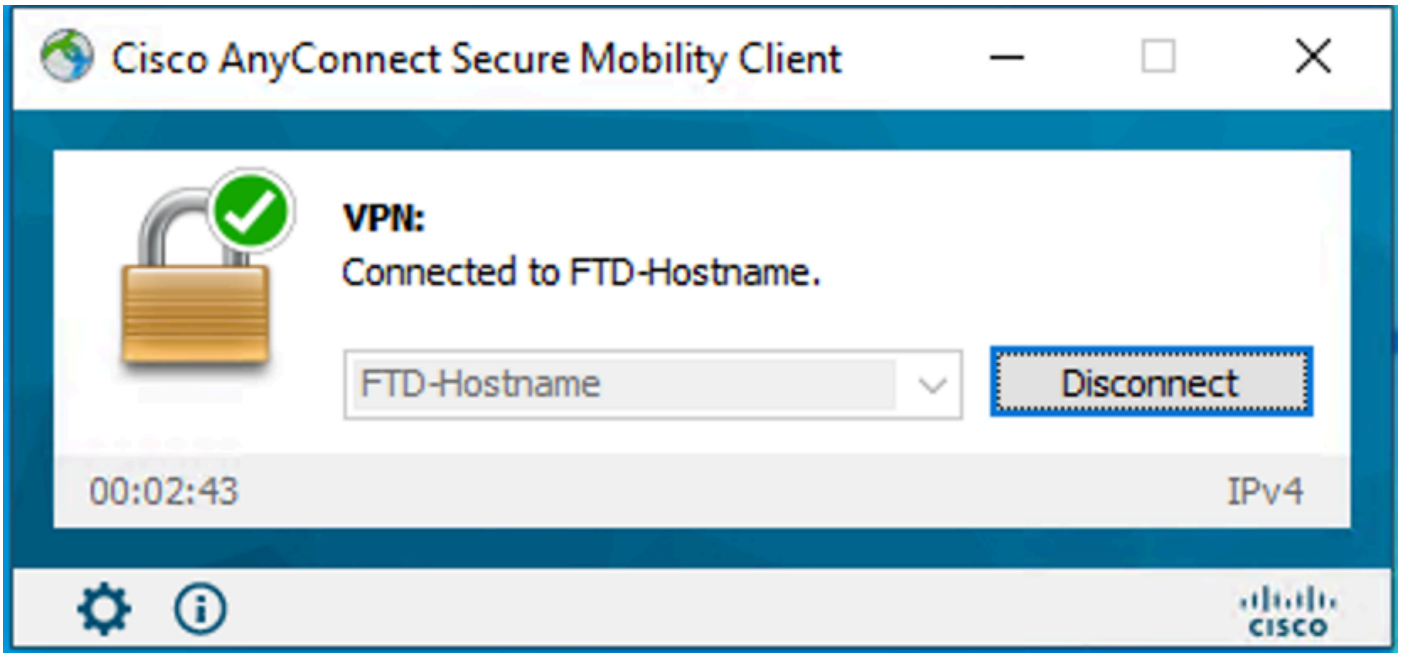
Connexion à AnyConnect et vérification du processus de gestion des mots de passe pour la connexion utilisateur

1. Établissez une connexion au profil de connexion concerné. Une fois qu'il a été déterminé lors de la connexion initiale que le mot de passe doit être modifié puisque le mot de passe précédent a été rejeté par le serveur Microsoft au moment de son expiration, l'utilisateur est invité à modifier le mot de passe.





2. Une fois que l'utilisateur a entré le nouveau mot de passe de connexion, la connexion est établie avec succès.



3. Vérifiez la connexion utilisateur sur l'interface de ligne de commande FTD :

<#root>

```
FTD_2# sh vpn-sessiondb anyconnect


Session Type: AnyConnect


Username     : admin
               Index        : 7
<------- Username, IP address assigned information of the client


Assigned IP  : 10.1.x.x
             Public IP    : 10.106.xx.xx
Protocol     :
AnyConnect-Parent SSL-Tunnel DTLS-Tunnel


License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES-GCM-256  DTLS-Tunnel: (1)AES-GCM-256
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA384  DTLS-Tunnel: (1)SHA384
```

```
Bytes Tx     : 16316                 Bytes Rx     : 2109

Group Policy : AnyConnect-Group      Tunnel Group : AnyConnect-AD

Login Time   : 13:22:24 UTC Mon Apr 25 2022

Duration     : 0h:00m:51s

Inactivity   : 0h:00m:00s

VLAN Mapping : N/A                   VLAN         : none

Audt Sess ID : 0ac5e0fa000070006266a090

Security Grp : none                  Tunnel Zone  : 0
```

Dépannage

Déboguages

Ce débogage peut être exécuté dans la CLI de diagnostic afin de dépanner les problèmes liés à la gestion des mots de passe : debug ldap 255.

Débogages de gestion des mots de passe

<#root>

```
[24] Session Start

[24] New request Session, context 0x0000148f3c271830, reqType = Authentication

[24] Fiber started

[24] Creating LDAP context with uri=ldaps://10.106.71.234:636

[24] Connect to LDAP server: ldaps://10.106.71.234:636, status = Successful

[24] supportedLDAPVersion: value = 3

[24] supportedLDAPVersion: value = 2

[24] Binding as *****@razor.local

[24] Performing Simple authentication for *****@razor.local to 10.106.71.234

[24] LDAP Search:
```

Base DN = [DC=razor,DC=local]

Filter = [sAMAccountName=admin]

Scope   = [SUBTREE]

[24] User DN = [CN=admin,CN=Users,DC=razor,DC=local]

[24] Talking to Active Directory server 10.106.71.234

[24] Reading password policy for admin, dn:CN=admin,CN=Users,DC=razor,DC=local

[24] Read bad password count 3

[24] Binding as admin

[24] Performing Simple authentication for admin to 10.106.71.234

[24] Simple authentication for admin returned code (49) Invalid credentials

[24] Message (admin): 80090308: LdapErr: DSID-0C0903C5, comment: AcceptSecurityContext error, data 773,

[24] Checking password policy

[24] New password is required for admin

[24] Fiber exit Tx=622 bytes Rx=2771 bytes, status=-1

[24] Session End

[25] Session Start

[25] New request Session, context 0x0000148f3c271830, reqType = Modify Password

[25] Fiber started

[25] Creating LDAP context with uri=ldaps://10.106.71.234:636

[25] Connect to LDAP server: ldaps://10.106.71.234:636, status = Successful

[25] supportedLDAPVersion: value = 3

[25] supportedLDAPVersion: value = 2

[25] Binding as *****@razor.local

[25] Performing Simple authentication for *****@razor.local to 10.106.71.234

[25] LDAP Search:

Base DN = [DC=razor,DC=local]

Filter = [sAMAccountName=admin]

Scope = [SUBTREE]

[25] User DN = [CN=admin,CN=Users,DC=razor,DC=local]

[25] Talking to Active Directory server 10.106.71.234

[25] Reading password policy for admin, dn:CN=admin,CN=Users,DC=razor,DC=local

[25] Read bad password count 3

[25] Change Password for admin successfully converted old password to unicode

[25] Change Password for admin successfully converted new password to unicode

[25] Password for admin successfully changed

[25] Retrieved User Attributes:

[25] objectClass: value = top

[25] objectClass: value = person

[25] objectClass: value = organizationalPerson

[25] objectClass: value = user

[25] cn: value = admin

[25] givenName: value = admin

[25] distinguishedName: value = CN=admin,CN=Users,DC=razor,DC=local

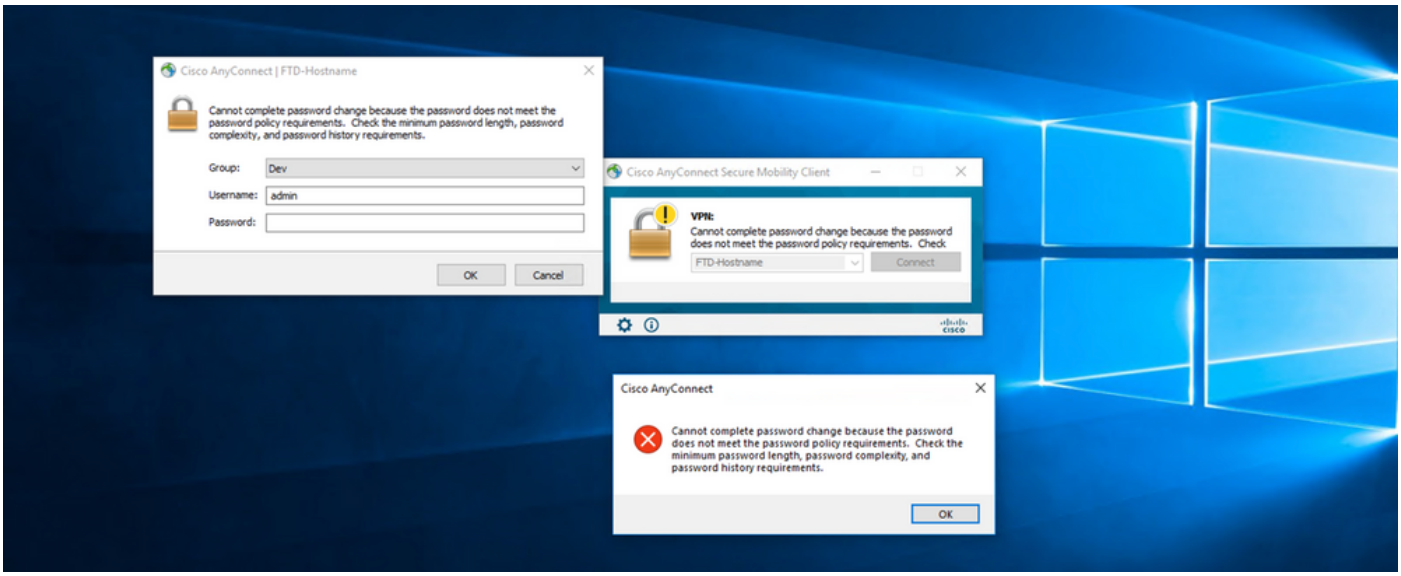
[25] instanceType: value = 4

[25] whenCreated: value = 20201029053516.0Z

```
[25]   whenChanged: value = 20220426032127.0Z
[25]   displayName: value = admin
[25]   uSNCreated: value = 16710
[25]   uSNChanged: value = 98431
[25]   name: value = admin
[25]   objectGUID: value = ..0.].LH.....9.4
[25]   userAccountControl: value = 512
[25]   badPwdCount: value = 3
[25]   codePage: value = 0
[25]   countryCode: value = 0
[25]   badPasswordTime: value = 132610388348662803
[25]   lastLogoff: value = 0
[25]   lastLogon: value = 132484577284881837
[25]   pwdLastSet: value = 0
[25]   primaryGroupID: value = 513
[25]   objectSid: value = ................7Z|....RQ...
[25]   accountExpires: value = 9223372036854775807
[25]   logonCount: value = 0
[25]   sAMAccountName: value = admin
[25]   sAMAccountType: value = 805306368
[25]   userPrincipalName: value = ******@razor.local
[25]   objectCategory: value = CN=Person,CN=Schema,CN=Configuration,DC=razor,DC=local
[25]   dSCorePropagationData: value = 20220425125800.0Z
[25]   dSCorePropagationData: value = 20201029053516.0Z
[25]   dSCorePropagationData: value = 16010101000000.0Z
[25]   lastLogonTimestamp: value = 132953506361126701
[25]   msDS-SupportedEncryptionTypes: value = 0
[25]   uid: value = ******@razor.local
[25] Fiber exit Tx=714 bytes Rx=2683 bytes, status=1
[25] Session End
```

Erreurs courantes rencontrées lors de la gestion des mots de passe

En général, si la stratégie de mot de passe définie par Microsoft Server n'est pas respectée pendant que l'utilisateur fournit le nouveau mot de passe, la connexion se termine avec l'erreur « Le mot de passe ne répond pas aux exigences de la stratégie de mot de passe ». Par conséquent, assurez-vous que le nouveau mot de passe respecte la stratégie définie par Microsoft Server pour les LDAP.



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.