

Créer un modèle de certificat Windows Server pour Catalyst Center

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Configurer](#)

[Dépannage](#)

Introduction

Ce document décrit les étapes pour créer un modèle de certificat sur un serveur Windows exécutant l'outil Autorité de certification (CA).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco Catalyst Center
- Un serveur Windows avec le rôle Autorité de certification installé et configuré
- Privilèges d'administrateur sur le serveur Windows
- Accès à la console de gestion des autorités de certification
- Connaissance de base des modèles de certificats et des demandes de signature de certificats (CSR)

Composants utilisés

Les informations contenues dans ce document sont basées sur Microsoft Windows Server 2022 Standard.

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

Informations générales

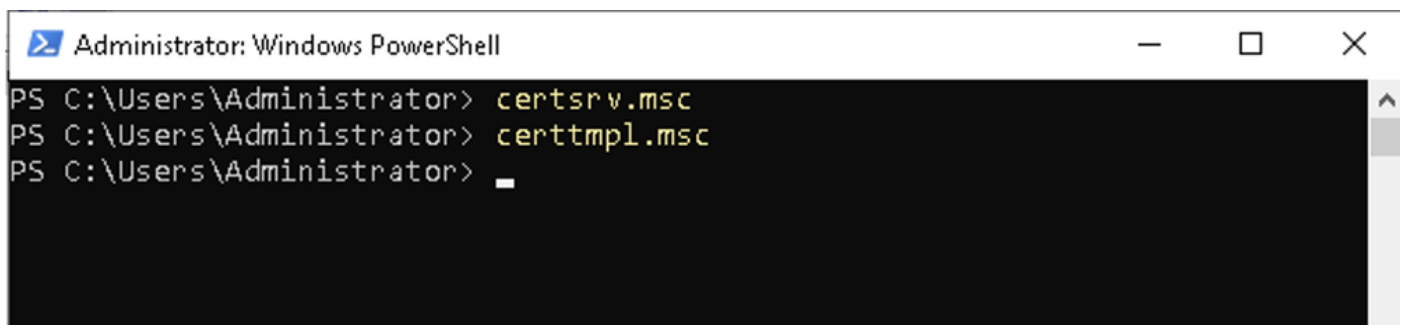
Ce modèle personnalisé résout le problème où les modèles d'autorité de certification par défaut suppriment l'authentification client des utilisations de clés étendues. Le modèle personnalisé peut signer la demande de signature de certificat (CSR) générée par Catalyst Center.

Configurer

Étapes de révision et de configuration des modèles de certificats sur Windows Server avec l'autorité de certification (AC).

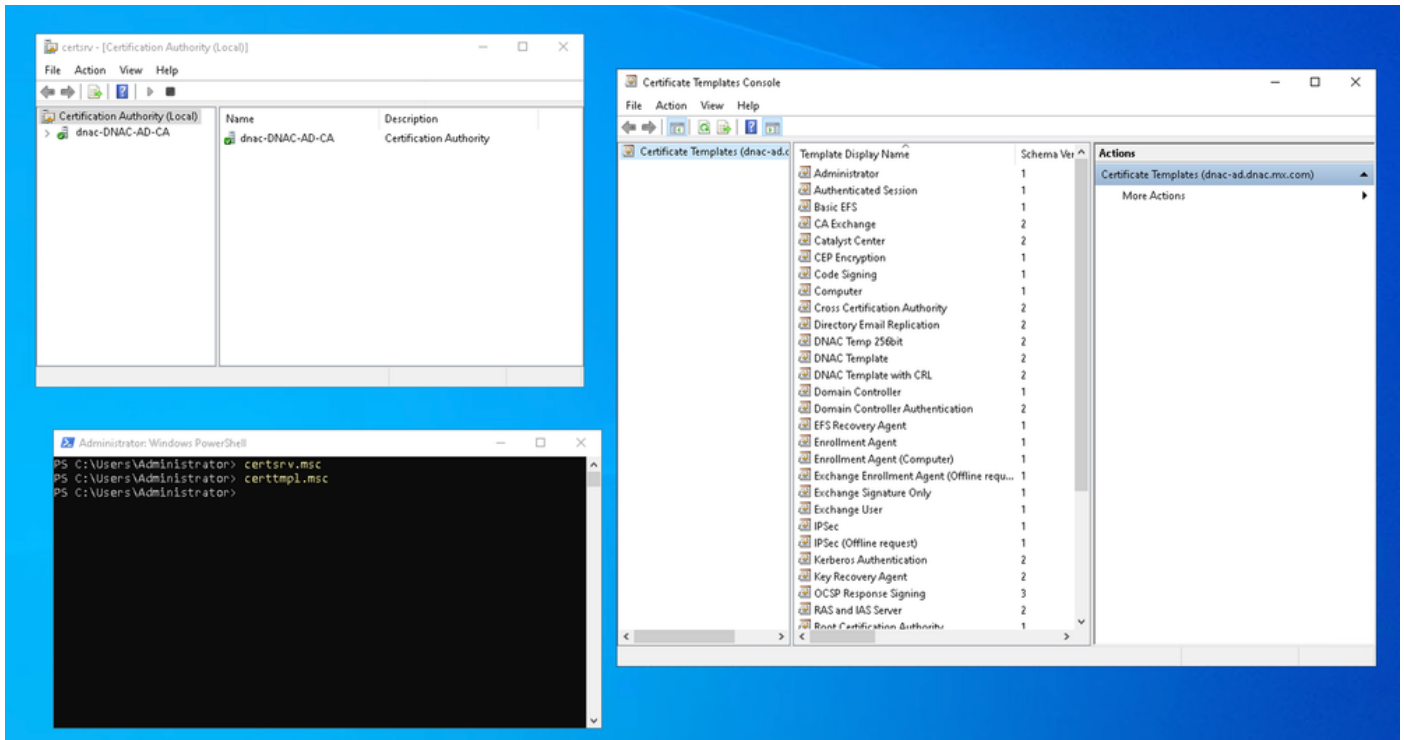
1. Connectez-vous au serveur Windows hébergeant l'autorité de certification à l'aide du Bureau à distance.
2. Ouvrez une session Command Prompt (CMD) ou PowerShell.
3. Lancez les consoles autorité de certification et modèle de certificat en exécutant :

certsrv.msc
certtmpl.msc



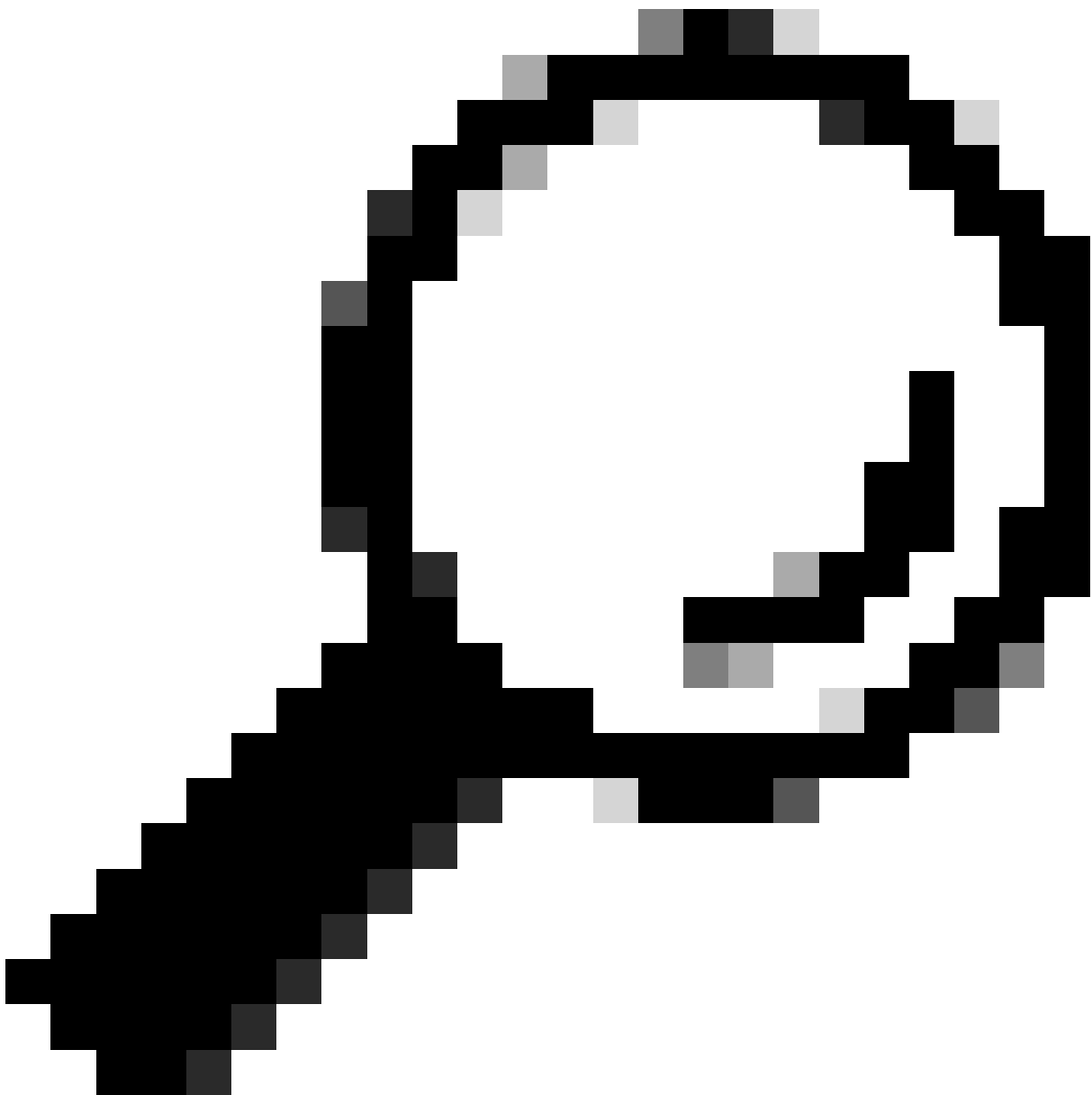
```
Administrator: Windows PowerShell
PS C:\Users\Administrator> certsrv.msc
PS C:\Users\Administrator> certtmpl.msc
PS C:\Users\Administrator> _
```

Administration Commandes Powershell



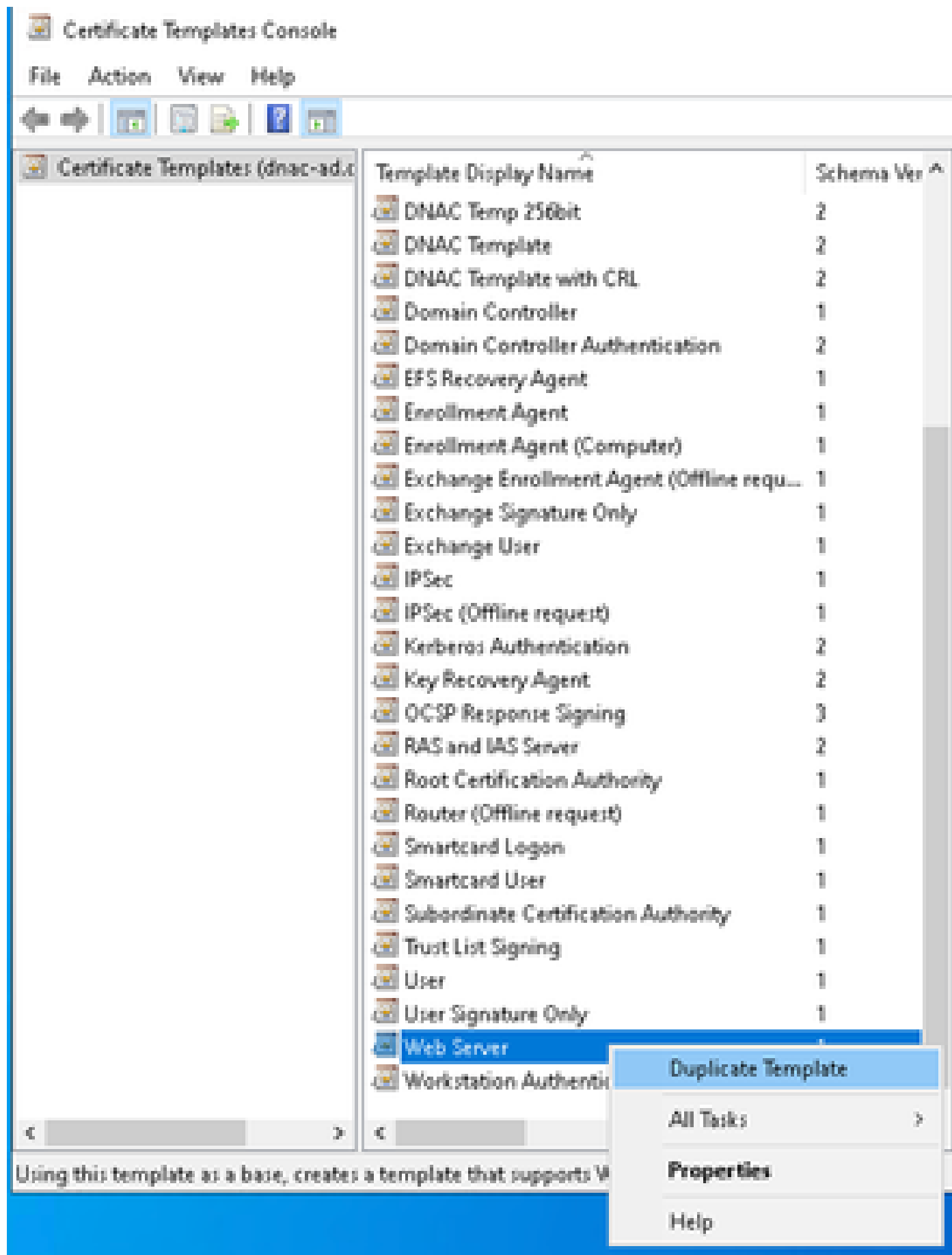
Exemple de Windows Server

4. Dans la console des modèles de certificats, localisez le modèle à cloner pour créer un nouveau modèle personnalisable.



Conseil : Utilisez le modèle de serveur Web, car il inclut déjà tous les paramètres requis pour le certificat Catalyst Center.

-
- Exemple : cliquez avec le bouton droit sur le serveur web et sélectionnez modèle dupliqué.



Modèle dupliqué

5. Un nouveau modèle est ouvert, modifiez-le avec les caractéristiques requises.

Properties of New Template



Subject Name		Server		Issuance Requirements	
Superseded Templates			Extensions		Security
Compatibility	General	Request Handling	Cryptography	Key Attestation	

The template options available are based on the earliest operating system versions set in Compatibility Settings.

☒ Show resulting changes

Compatibility Settings

Certification Authority

Windows Server 2003



Certificate recipient

Windows XP / Server 2003



These settings may not prevent earlier operating systems from using this template.

OK

Cancel

Apply

Help

6. Modifiez le nouveau modèle comme suit :

6.1 Onglet Général

- Entrez un nom de modèle (par exemple, Modèle Catalyst Center).
- Définissez la période de validité (par défaut : 2 ans).

Properties of New Template



Subject Name		Server		Issuance Requirements	
Superseded Templates			Extensions		Security
Compatibility	General	Request Handling	Cryptography	Key Attestation	

Template display name:

Template name:

Validity period:

 years

Renewal period:

 weeks ☐ Publish certificate in Active Directory☐ Do not automatically reenroll if a duplicate certificate exists in Active Directory

OK

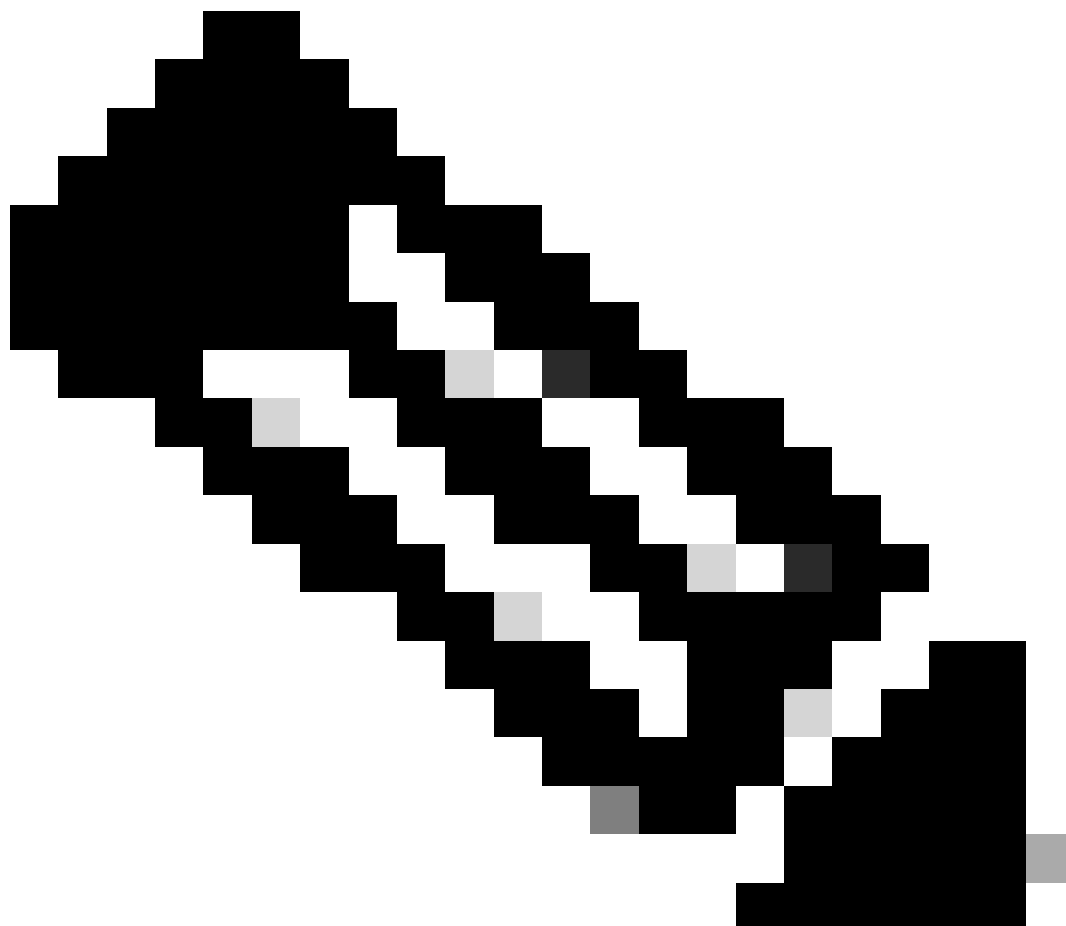
Cancel

Apply

Help

6.2 Onglet Postes

- Accédez à politiques d'application et cliquez sur modifier.
-



Remarque : Dans cet onglet, vérifiez que le modèle inclut les extensions d'utilisation de clé obligatoires requises par le certificat Catalyst Center, telles que keyEncipherment et digitalSignature. Elles sont déjà présentes dans le modèle de serveur Web par défaut utilisé comme base.

Properties of New Template



Subject Name

Server

Issuance Requirements

Compatibility

General

Request Handling

Cryptography

Key Attestation

Superseded Templates

Extensions

Security

To modify an extension, select it, and then click **Edit**.

Extensions included in this template:

-  Application Policies
-  Basic Constraints
-  Certificate Template Information
-  Issuance Policies
-  Key Usage

Edit...

Description of Application Policies:

Server Authentication

OK

Cancel

Apply

Help

- Cliquez sur add, localisez client authentication, et cliquez sur ok pour l'inclure.

Edit Application Policies Extension



An application policy defines how a certificate can be used.

Application policies:

Server Authentication

Add...

Edit...

Remove

☐ Make this extension critical

OK

Cancel

Add Application Policy



An application policy (called enhanced key usage in Windows 2000) defines how a certificate can be used. Select the application policy required for valid signatures of certificates issued by this template.

Application policies:

Any Purpose
Attestation Identity Key Certificate
Certificate Request Agent
Client Authentication
Code Signing
CTL Usage
Digital Rights
Directory Service Email Replication
Disallowed List
Document Encryption
Document Signing
Domain Name System (DNS) Server Trust
Dynamic Code Generator

New...

OK

Cancel

Ajouter une stratégie d'application

- Vérifiez que le modèle affiche l'authentification client avec les utilisations par défaut.

Edit Application Policies Extension



An application policy defines how a certificate can be used.

Application policies:

Client Authentication
Server Authentication

Add...

Edit...

Remove

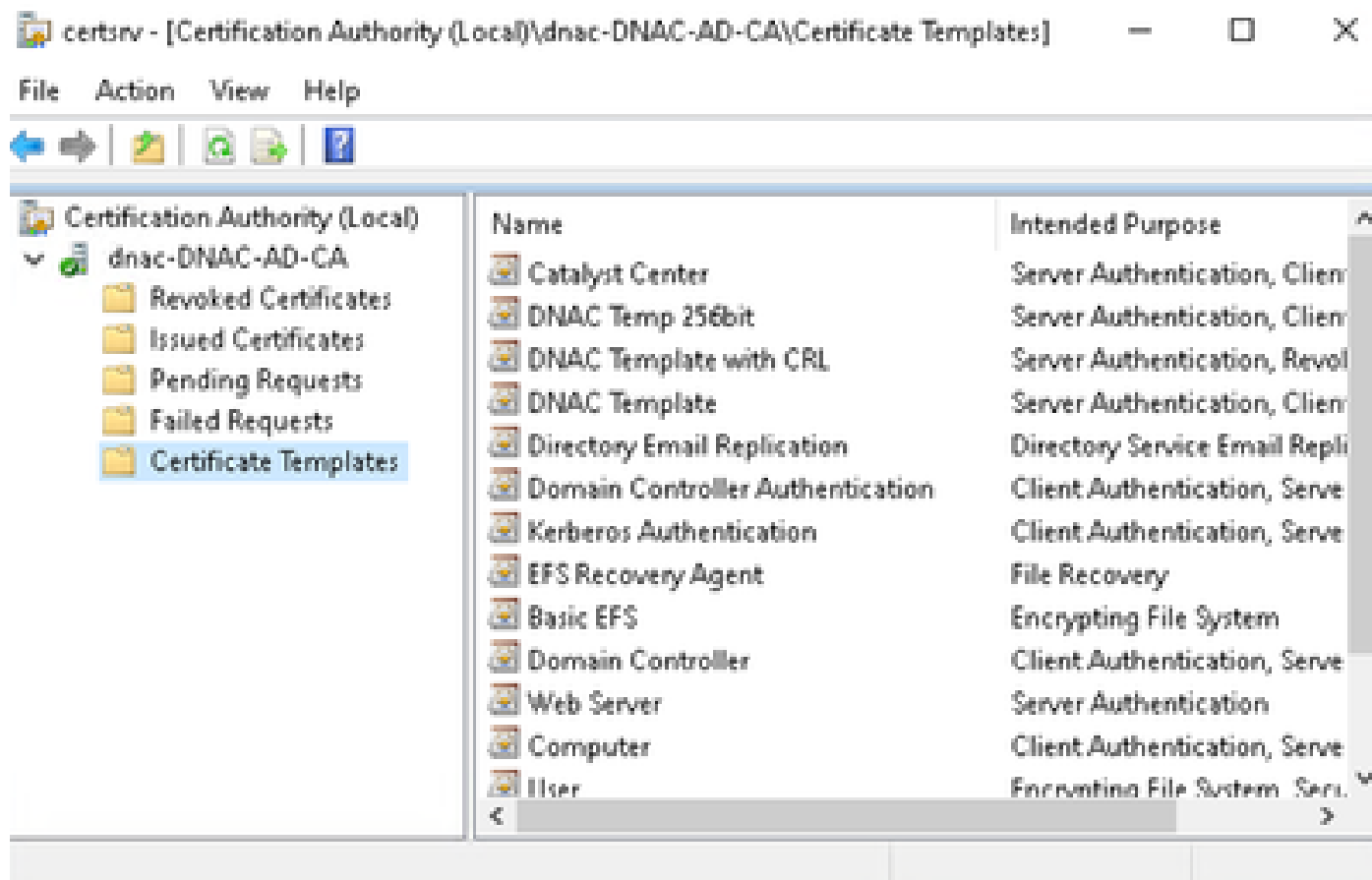
☐ Make this extension critical

OK

Cancel

7. Cliquez sur Apply, puis sur ok.

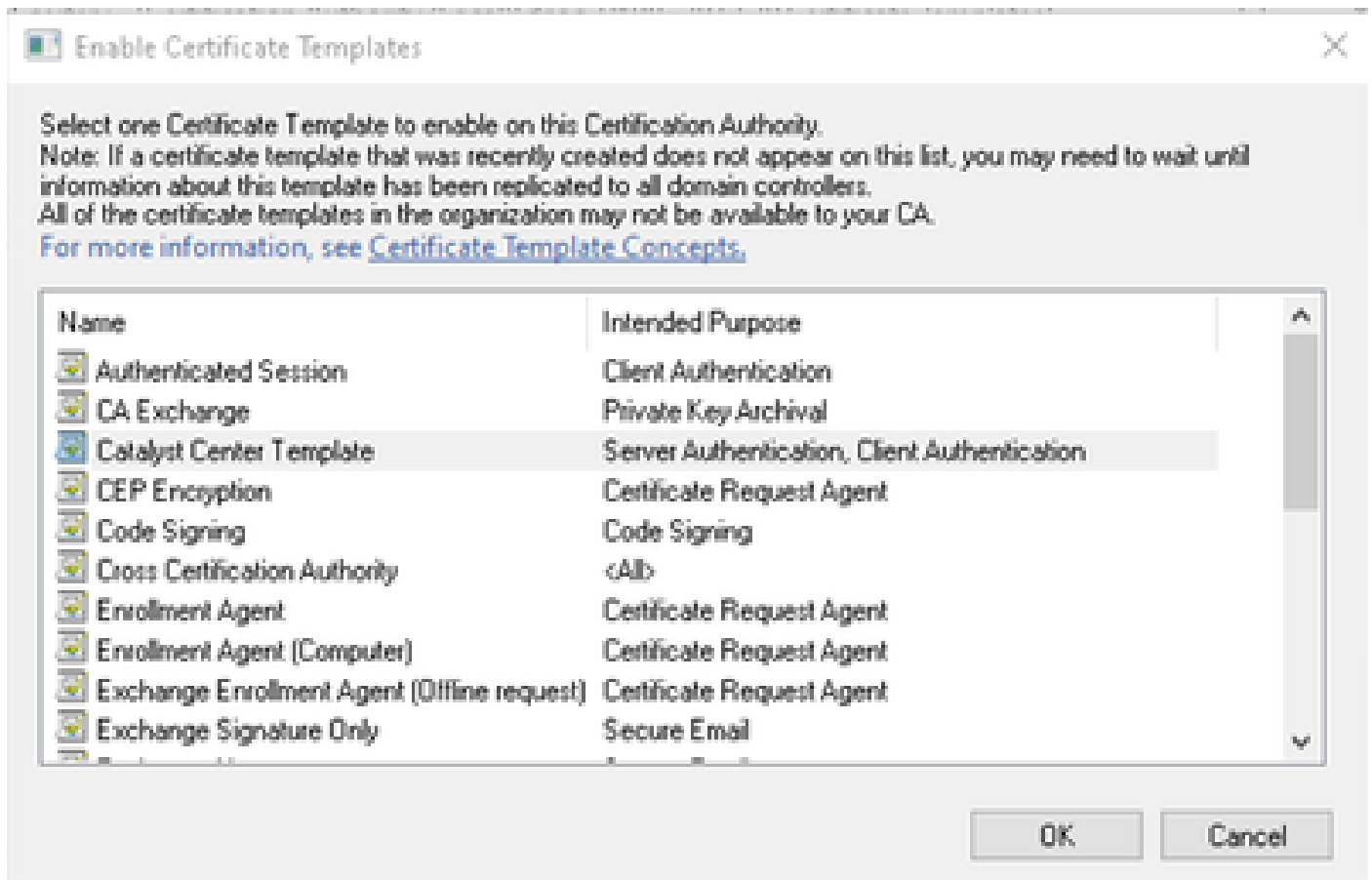
8. Dans la console Certificate Authority, développez l'arborescence CA et sélectionnez le dossier certificate templates.



Modèles de certificats de l'arborescence CA

9. Cliquez avec le bouton droit sur le dossier modèles de certificat et sélectionnez :

Nouveau > Modèle de certificat à émettre.

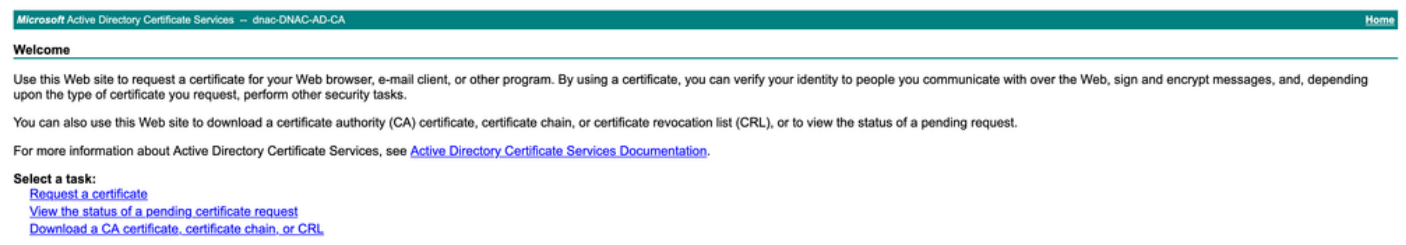


Modèle Catalyst Center

11. Le modèle apparaît maintenant sous la liste Modèles de certificats dans l'autorité de certification.

12. Ouvrez un navigateur et accédez à :

<http://localhost/certsrv/>



Page de connexion <http://localhost/certsrv/>

13. Sélectionnez Demander un certificat, puis Demande de certificat avancée, pour vérifier que le nouveau modèle est disponible.

14. Sur cette page, envoyez le CSR et sélectionnez le modèle nouvellement créé pour générer le certificat signé.

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded
certificate request
(CMC or
PKCS #10 or
PKCS #7):

```
HS29DKQx8wkaeC080u+uwRt6Wf+G7Ci1p0v4i5vc|
LtbzjY7pH80VXu+yepN85mPTeDL++poXx8vXUT8w|
2d14EajkSKQP8CJJh5W7gn3dd4w1r8h90Y5wR8g|
B1Zq07Ldz1jGRgJMj9hWe6nvnvJaVfy9o3M1GcYzc|
-----END CERTIFICATE REQUEST-----
```

Certificate Template:

Catalyst Center Template ▾

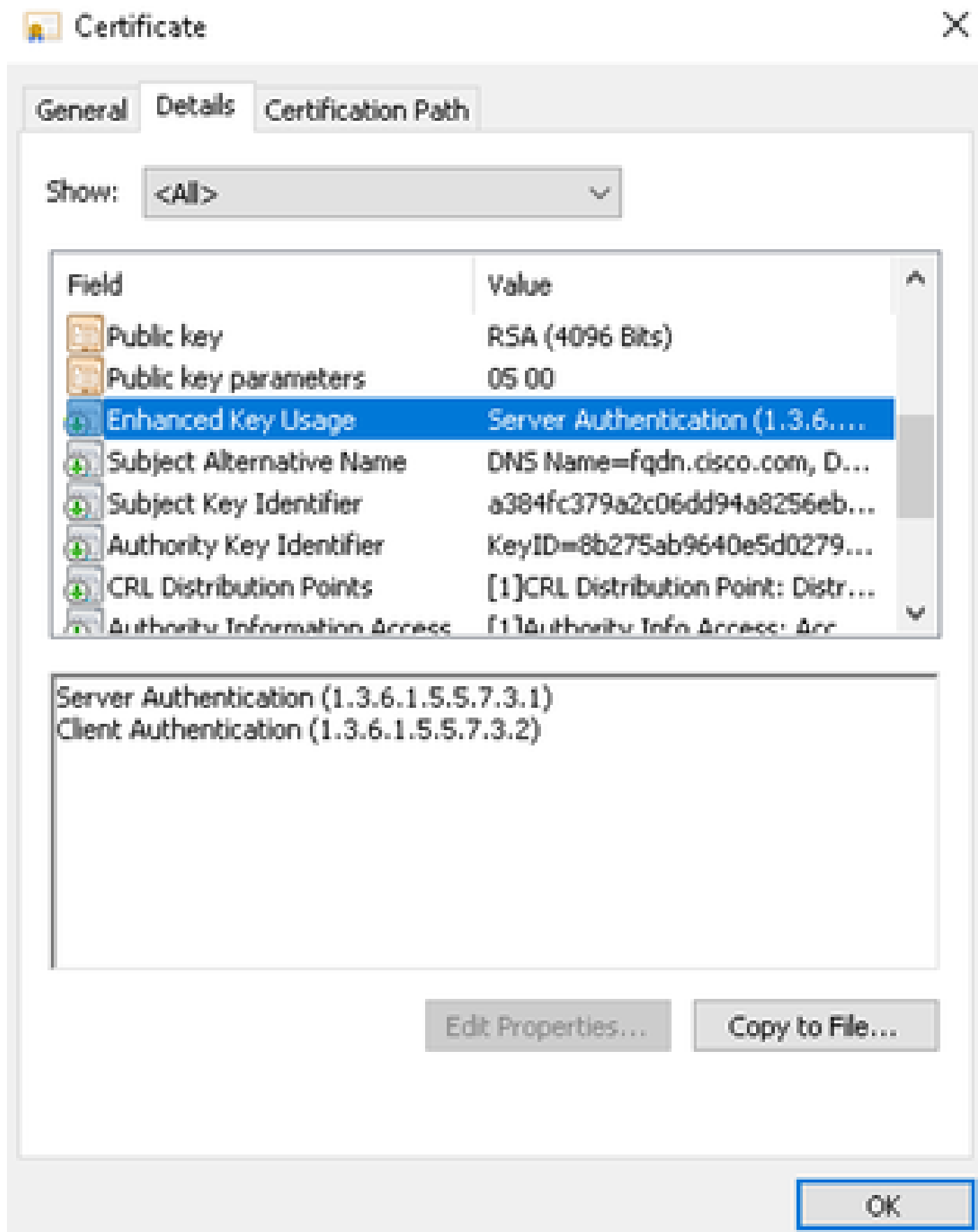
Additional Attributes:

Attributes:

Submit >

Demander un certificat

13. Le certificat est généré avec les extensions correctes, comme indiqué dans l'exemple.



Exemple de certificat

Dépannage

Si vous rencontrez des erreurs lors de la signature du CSR, consultez les journaux Windows Server pour plus de détails :

Erreur :



Dépannage des erreurs

1. Ouvrez la visionneuse d'événements en exécutant :

eventvwr.msc

2. Accédez à Observateur d'événements > Journaux Windows > Application.

3. Filtrer ou rechercher des événements où :

1. Source = Autorité de certification

2. ID d'événement = 53, 54, 55, ou similaire (cela indique qu'une demande a été émise, refusée ou est en attente).

3. Le message d'événement contient des détails sur la raison du refus (le cas échéant).

4. Utilisez l'option Rechercher (clic droit sur Application > Rechercher...) et effectuez une recherche par :

- certsrv
- ID de la demande (s'il est connu, par exemple, 164)

Event Viewer

File Action View Help

Event Viewer (Local)

- Custom Views
- Windows Logs
 - Application
 - Security
 - Setup
 - System
 - Forwarded Events
- Applications and Services Logs
 - Subscriptions

Level	Date and Time	Source	Event ID	Task Category
Warning	9/10/2025 10:35:48 PM	CertificationAuthority	53	None
Warning	9/10/2025 10:35:47 PM	CertificationAuthority	77	None
Information	9/10/2025 9:18:05 PM	Desktop Window Manager	9027	None
Information	9/10/2025 8:30:13 PM	Security-SPP	16394	None
Information	9/10/2025 8:29:43 PM	Security-SPP	16394	None
Information	9/10/2025 2:13:38 PM	edgeupdate	0	None
Information	9/10/2025 1:47:51 PM	SecCli	1704	None
Information	9/10/2025 4:42:21 AM	Security-SPP	16394	None
Information	9/10/2025 4:41:51 AM	Security-SPP	16394	None
Information	9/10/2025 4:13:54 AM	edgeupdate	0	None
Information	9/9/2025 9:42:38 PM	SecCli	1704	None
Information	9/9/2025 8:45:14 PM	Security-SPP	16394	None
Information	9/9/2025 8:44:44 PM	Security-SPP	16394	None
Information	9/9/2025 6:14:16 PM	edgeupdate	0	None

Event 53, CertificationAuthority

General Details

Active Directory Certificate Services denied request 164 because The public key does not meet the minimum size required by the specified certificate template. 0x00094811 (-2146875375 CERTSRV_E_KEY_LENGTH). The request was for CN=10.88.244.116. Additional information: Denied by Policy Module

Log Name: Application
Source: CertificationAuthority
Event ID: 53
Level: Warning
User: SYSTEM
OpCode: Info
More Information: [EventLog Online Help](#)

Logged: 9/10/2025 10:35:48 PM
Task Category: None
Keywords:
Computer: dnac-ad.dnac.msi.com

Actions

- Application
- Open Saved Log...
- Create Custom View...
- Import Custom View...
- Clear Log...
- Filter Current Log...
- Properties
- Find...
- Save All Events As...
- Attach a Task To this Log...
- View
- Refresh
- Help

Event 53, CertificationAuthority

- Event Properties
- Attach Task To This Event...
- Copy
- Save Selected Events...
- Refresh
- Help

Dépannage des journaux Windows Server

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.