

Windows Server-certificaatsjabloon voor Catalyst Center maken

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Problemen oplossen](#)

Inleiding

In dit document worden de stappen beschreven voor het maken van een certificaatsjabloon op een Windows-server waarop het hulpprogramma Certificaatautoriteit (CA) wordt uitgevoerd.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Catalyst Center
- Een Windows Server met de CA-rol (Certification Authority) geïnstalleerd en geconfigureerd
- Beheerdersrechten op de Windows Server
- Toegang tot de beheerconsole van de certificeringsinstantie
- Basiskennis van certificaatsjablonen en certificaatondertekeningsverzoeken (CSR)

Gebruikte componenten

De informatie in dit document is gebaseerd op Microsoft Windows Server 2022 Standard.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Deze aangepaste sjabloon lost het probleem op waarbij de standaard CA-sjablonen de

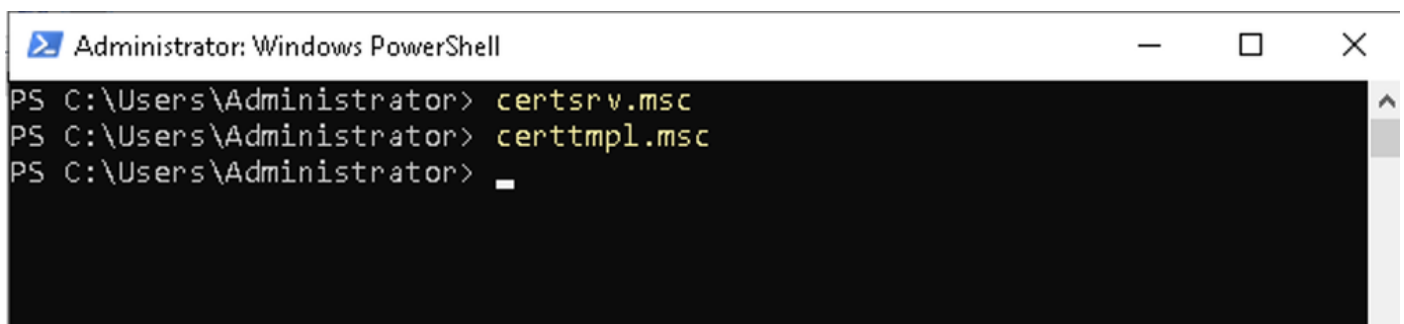
clientverificatie verwijderen uit Uitgebreid sleutelgebruik. De aangepaste sjabloon is in staat om het Certificate Signing Request (CSR) te ondertekenen dat is gegenereerd door Catalyst Center.

Configureren

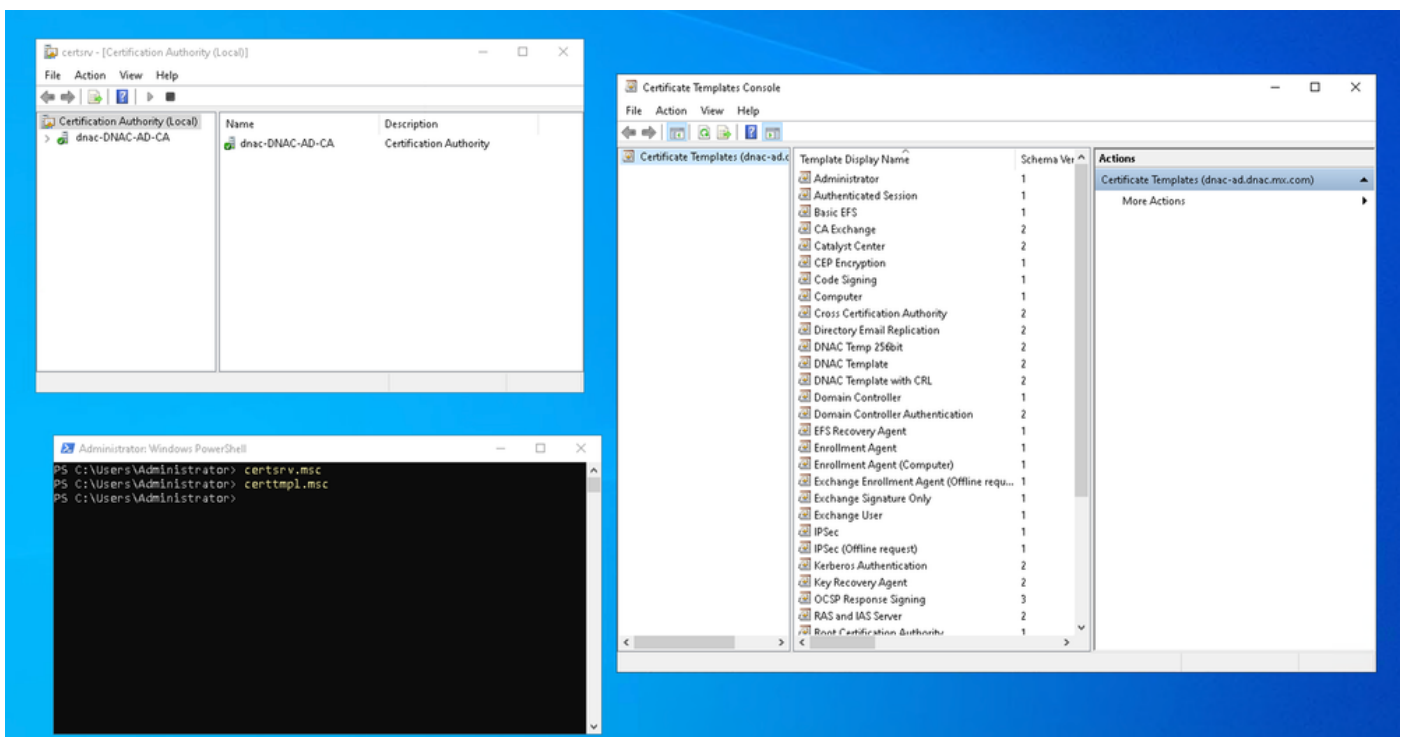
Stappen voor het controleren en configureren van certificaatsjablonen op Windows Server met de certificeringsinstantie.

1. Meld u aan bij de Windows Server waarop de CA wordt gehost met Extern bureaublad.
2. Open een opdrachtprompt (CMD) of PowerShell-sessie.
3. Start de consoles van de certificeringsinstantie en de certificaatsjabloon door:

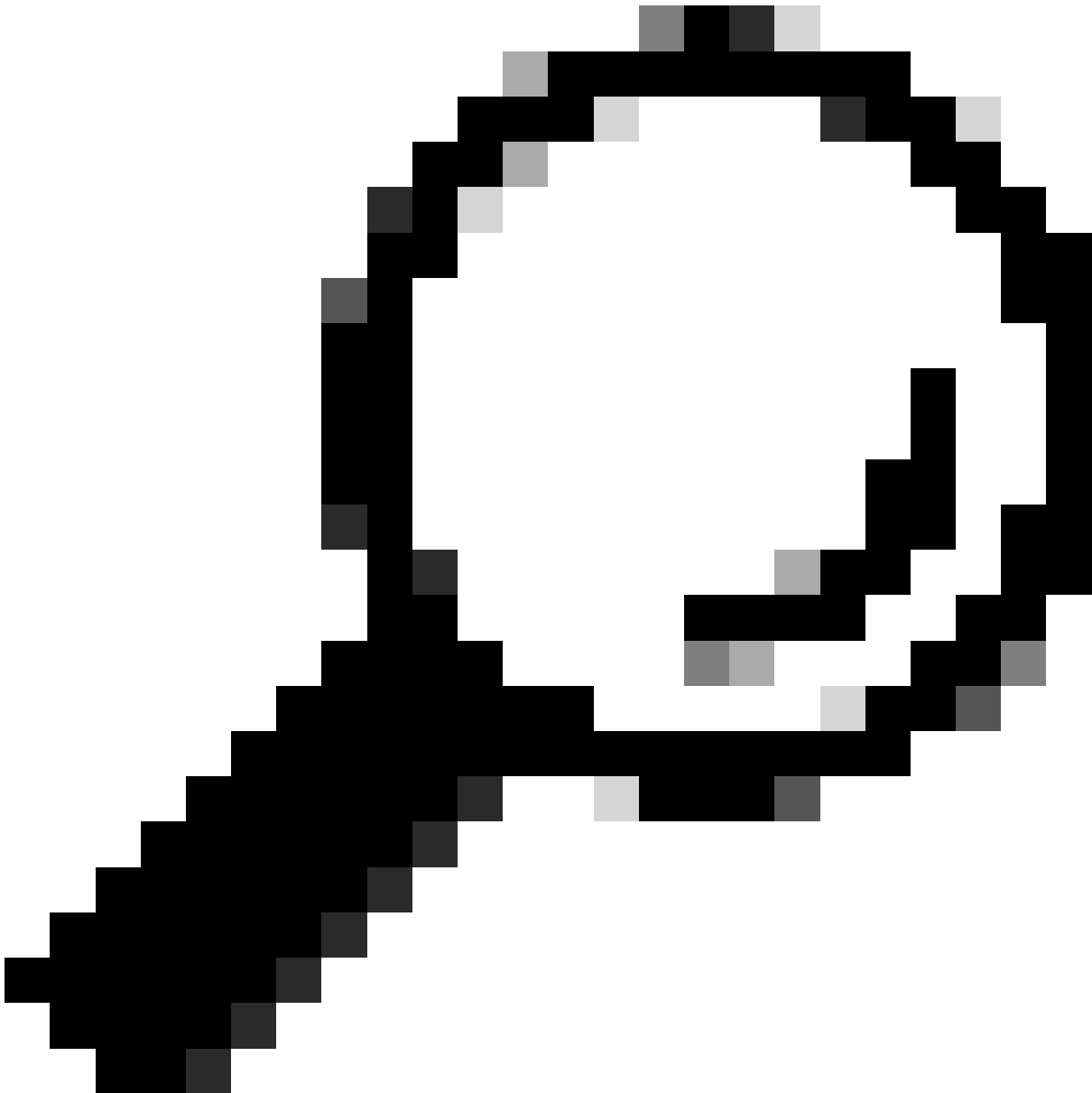
certsrv.msc
certtmpl.msc



Beheer PowerShell-opdrachten

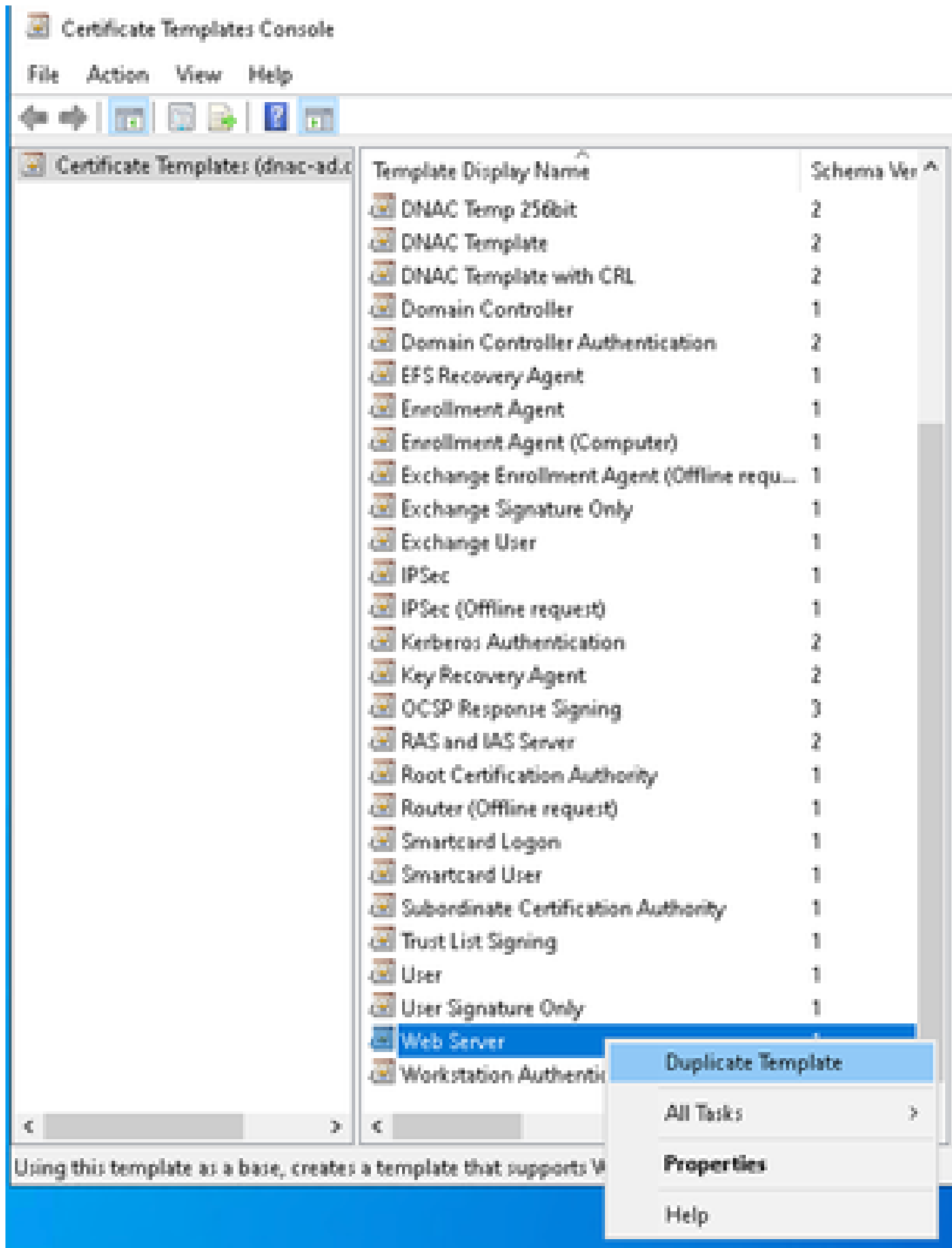


4. Zoek in de certificaatsjabloonconsole de sjabloon die moet worden gekloond om een nieuwe aanpasbare sjabloon te maken.



Tip: gebruik de webserverjabloon omdat deze al alle vereiste parameters voor het Catalyst Center-certificaat bevat.

- Voorbeeld: klik met de rechtermuisknop op de webserver en selecteer Sjabloon dupliceren.



Template dupliceren

5. Als een nieuwe template is geopend, wijzigt u deze met de vereiste kenmerken.

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. Wijzig de nieuwe template als volgt:

6.1 Tabblad Algemeen.

- Geef een naam op voor de template (bijvoorbeeld Catalyst Center Template).
- Bepaal de geldigheidsduur (standaard: 2 jaar).

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

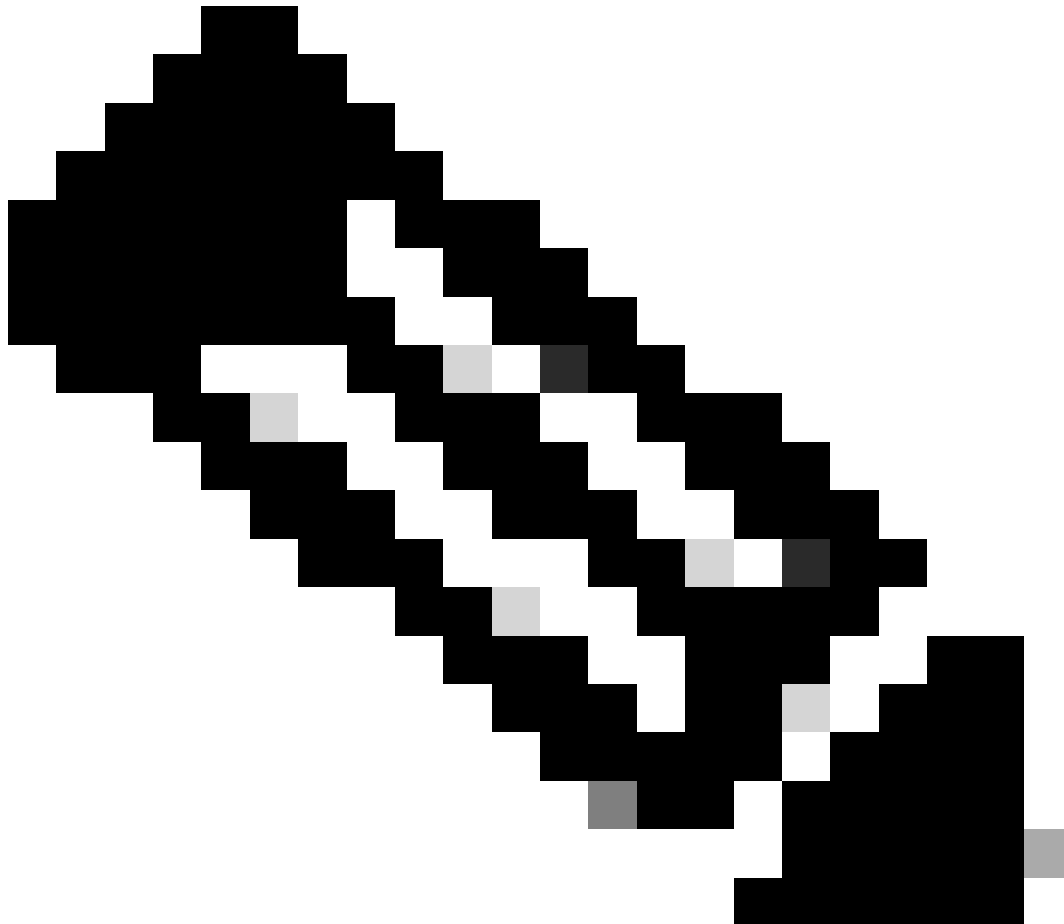
Cancel

Apply

Help

6.2 Tabblad Extensies.

- Navigeer naar toepassingsbeleid en klik op bewerken.
-



Opmerking: Bevestig op dit tabblad dat de sjabloon de verplichte Key Usage-extensies bevat die vereist zijn voor het Catalyst Center-certificaat, zoals keyEncryption en digitalSignature. Deze zijn al aanwezig in de standaard webserver sjabloon die als basis wordt gebruikt.

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

- Klik op toevoegen, zoek clientverificatie en klik op OK om deze toe te voegen.

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

Toepassingsbeleid toevoegen

- Bevestig dat de sjabloon de clientverificatie en de standaardtoepassingen toont.

Edit Application Policies Extension



An application policy defines how a certificate can be used.

Application policies:

Client Authentication
Server Authentication

Add...

Edit...

Remove

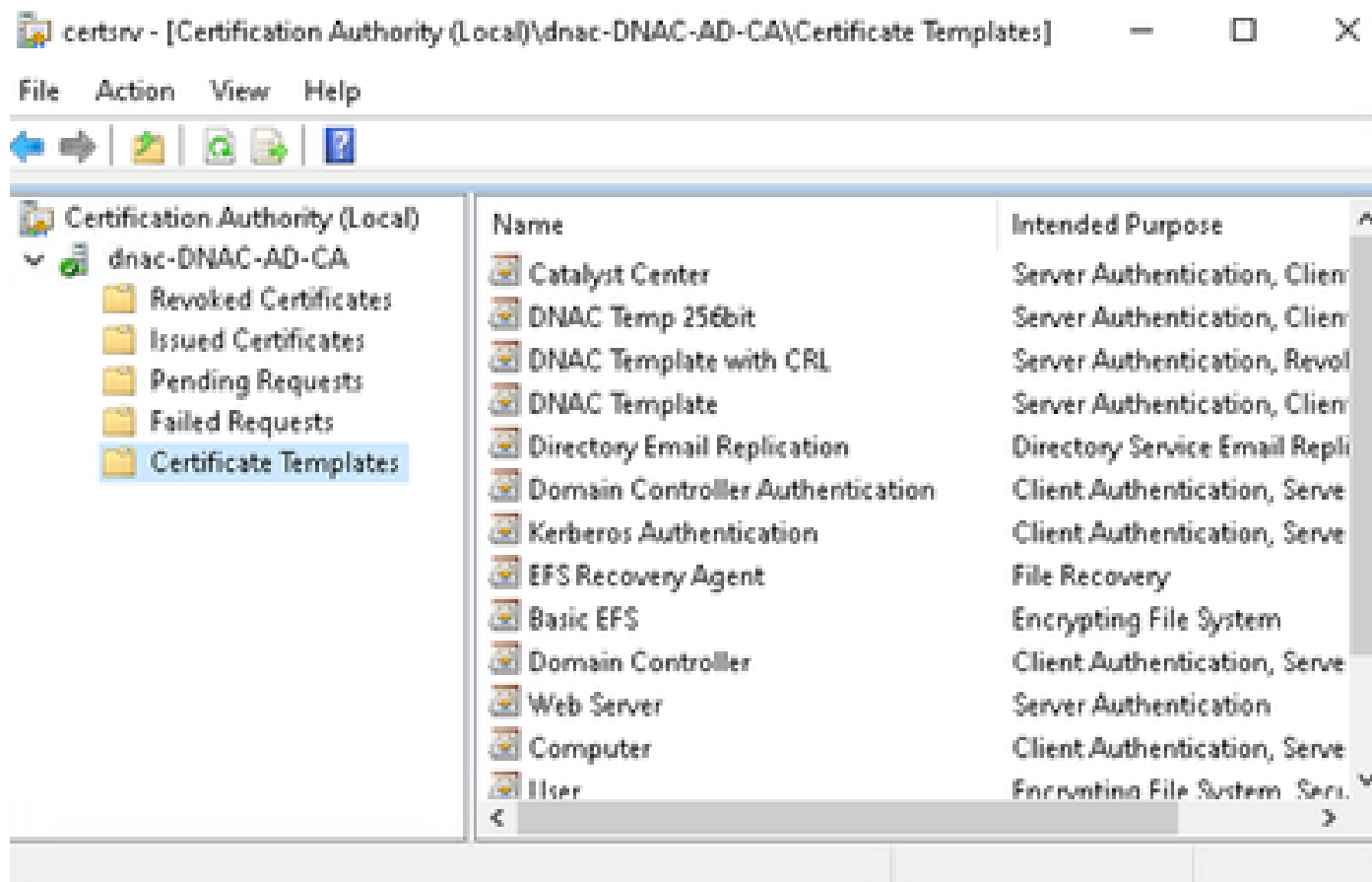
☐ Make this extension critical

OK

Cancel

7. Klik op Toepassen en vervolgens op OK.

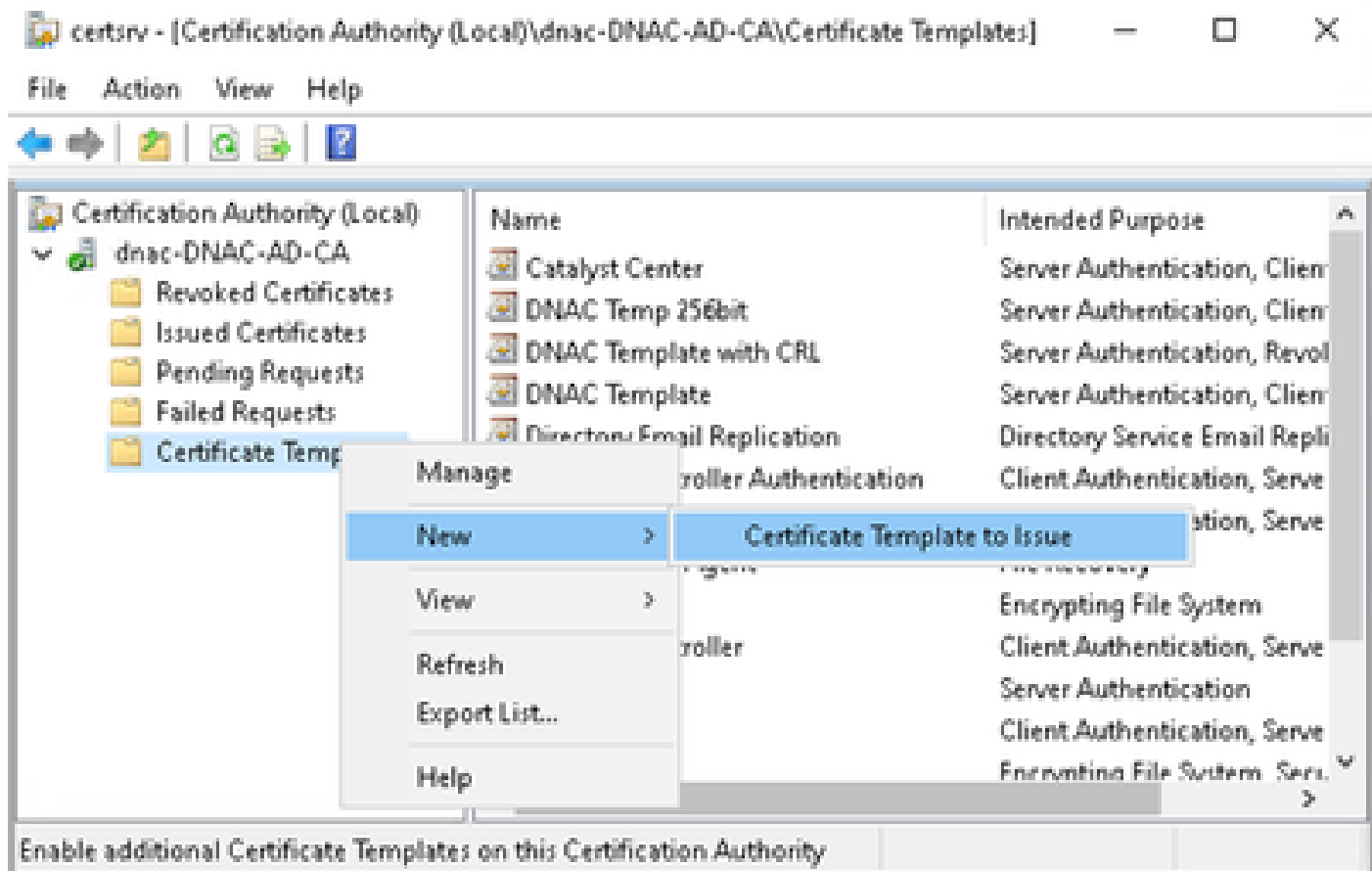
8. Vouw in de console Certificaatautoriteit de CA-structuur uit en selecteer de map Certificaatsjablonen.



CA Tree-certificaatsjablonen

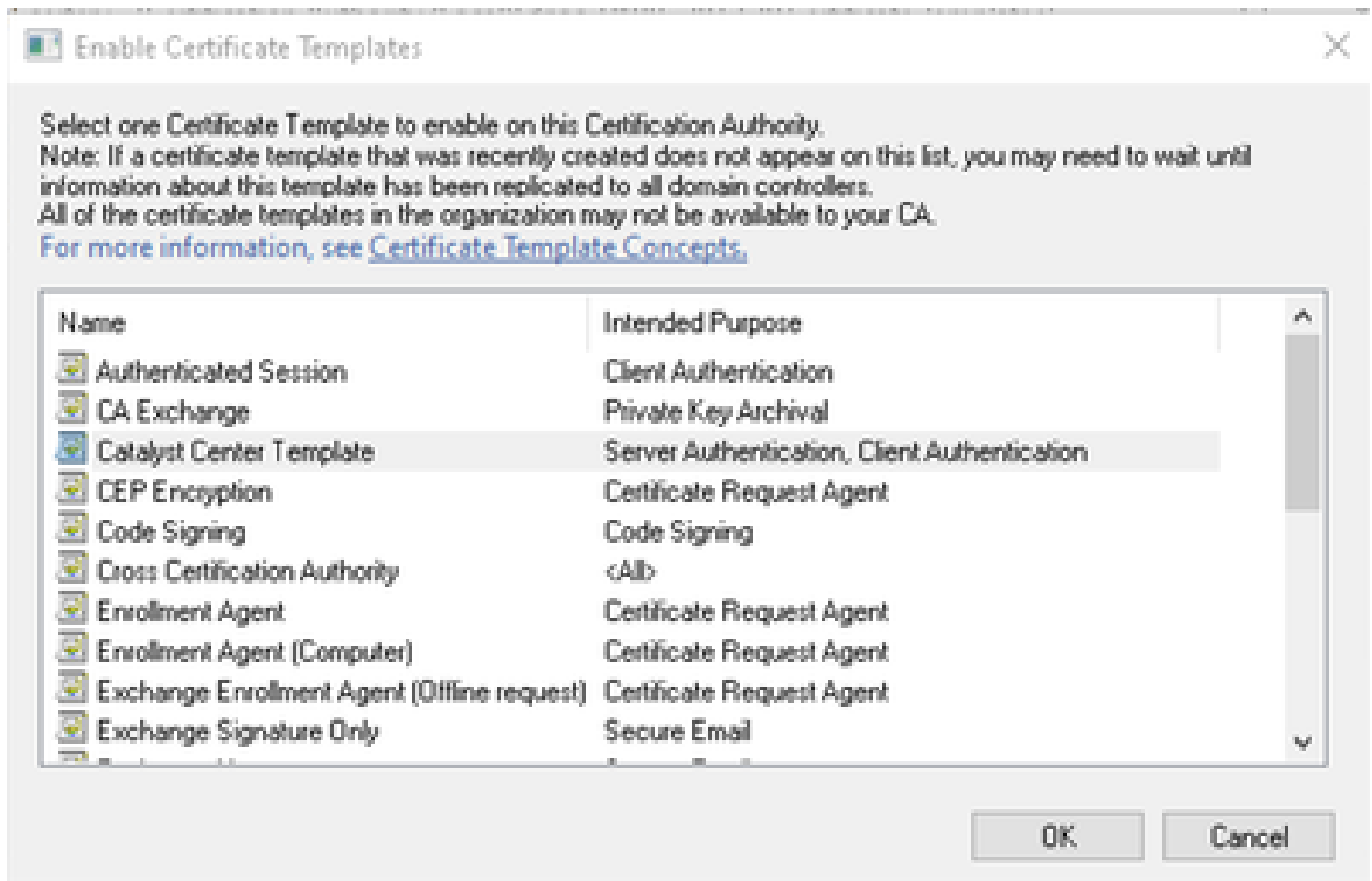
9. Klik met de rechtermuisknop op de map certificaatsjablonen en selecteer:

Nieuw > Te verstrekken certificaatsjabloon.



Nieuw certificaatsjabloon voor uitgifte

10. Selecteer in het nieuwe venster de nieuw gemaakte sjabloon (bijvoorbeeld de sjabloon Catalyst Center) en klik op OK.

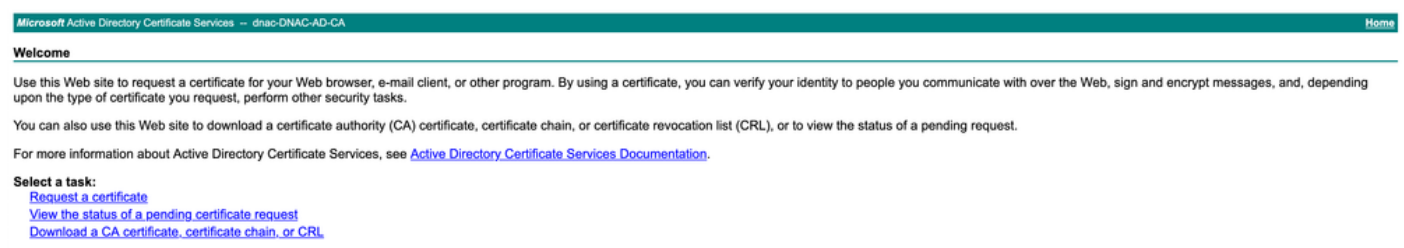


Catalyst Center-sjabloon

11. De sjabloon wordt nu weergegeven onder de lijst Certificaatsjablonen in de CA.

12. Open een browser en ga naar:

<http://localhost/certsrv/>



Inlogpagina <http://localhost/certsrv/>

13. Selecteer Certificaat aanvragen en vervolgens Geavanceerd Certificaat aanvragen om te controleren of de nieuwe sjabloon beschikbaar is.

14. Op deze pagina dient u de CSR in en selecteert u de nieuw gemaakte sjabloon om het ondertekende certificaat te genereren.

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|
2d14Ea|kSKQP8CJJh5W7gn3dd4w1r8h90Y5wR8g|
B1Zq07Ldz1jGRgJMj9hWe6nvnvJaVfy9o3M1GcYzc|
-----END CERTIFICATE REQUEST-----
```

Certificate Template:

Catalyst Center Template

Additional Attributes:

Attributes:

Submit >

Vraag een certificaat aan

13. Het certificaat wordt gegenereerd met de juiste extensies, zoals weergegeven in het voorbeeld.

General Details Certification Path

Show:

<All>

Field	Value
Public key	RSA (4096 Bits)
Public key parameters	05 00
Enhanced Key Usage	Server Authentication (1.3.6.1.5.5.7.3.1)
Subject Alternative Name	DNS Name=fqdn.cisco.com, D...
Subject Key Identifier	a384fc379a2c06dd94a8256eb...
Authority Key Identifier	KeyID=8b275ab9640e5d0279...
CRL Distribution Points	[1]CRL Distribution Point: Distr...
Authority Information Access	[1]Authority Info Access: Acc...

Server Authentication (1.3.6.1.5.5.7.3.1)

Client Authentication (1.3.6.1.5.5.7.3.2)

Edit Properties...

Copy to File...

OK

Als u fouten tegenkomt tijdens het ondertekenen van de CSR, raadpleegt u de Windows Server-logs voor meer informatie:

Fout:



Fout bij probleemoplossing

1. Open de gebeurtenisviewer door:

eventvwr.msc

2. Navigeer naar Event Viewer > Windows-logs > Toepassing.

3. Filteren of zoeken naar gebeurtenissen waarbij:

1. Bron = certificeringsinstantie
2. Gebeurtenis-ID = 53, 54, 55, of iets dergelijks (deze geven aan dat een verzoek is afgegeven, geweigerd of in behandeling is).
3. Het eventbericht bevat details over de reden voor de weigering (indien van toepassing).

4. Gebruik de optie Zoeken (rechtsklik op Toepassing > Zoeken...) en zoek op:

- certsrv
- ID aanvragen (indien bekend, bijvoorbeeld 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

Problemen met Windows Server-logboeken oplossen

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.