

Criar Modelo de Certificado do Windows Server para o Catalyst Center

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Troubleshooting](#)

Introdução

Este documento descreve as etapas para criar um modelo de certificado em um Windows Server executando a ferramenta Autoridade de Certificação (CA).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco Catalyst Center
- Um Windows Server com a função de autoridade de certificação instalada e configurada
- Privilégios de administrador no Windows Server
- Acesso ao Console de Gerenciamento de Autoridade de Certificação
- Conhecimento básico de modelos de certificado e CSR (Certificate Signing Requests, solicitações de assinatura de certificado)

Componentes Utilizados

As informações neste documento são baseadas no Microsoft Windows Server 2022 Standard.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

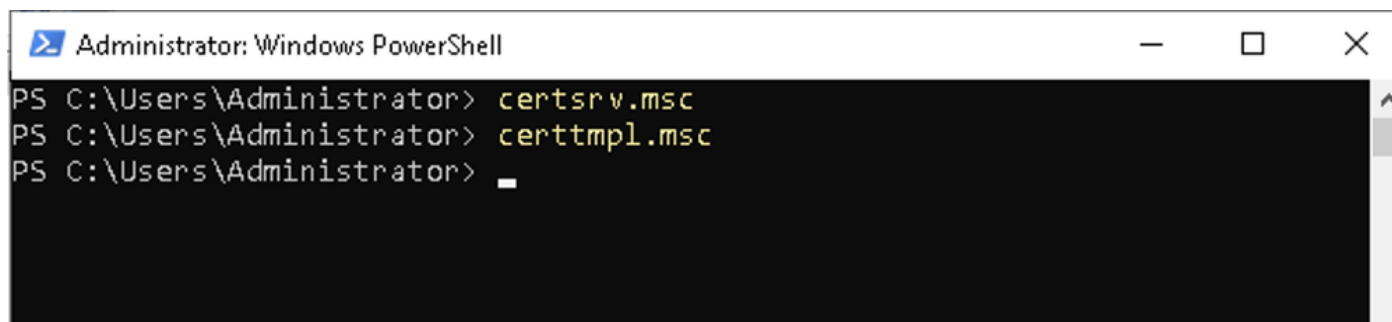
Este modelo personalizado resolve o problema em que os modelos de CA padrão removem a Autenticação de cliente dos Usos de chave estendida. O modelo personalizado pode assinar a CSR (Certificate Signing Request, Solicitação de assinatura de certificado) gerada pelo Catalyst Center.

Configurar

Etapas para revisar e configurar Modelos de Certificado no Windows Server com a Autoridade de Certificação (CA).

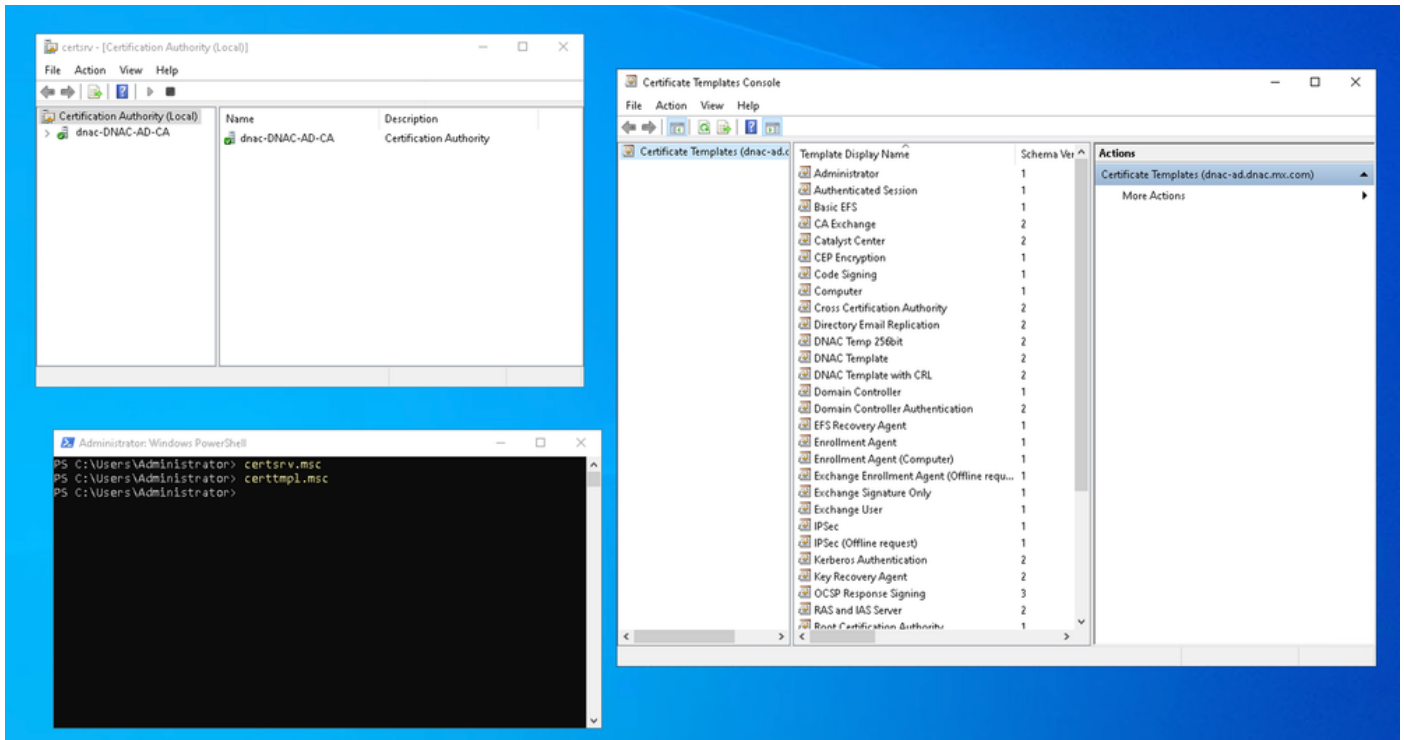
1. Faça login no Windows Server que hospeda a autoridade de certificação usando a Área de Trabalho Remota.
2. Abra uma sessão de prompt de comando (CMD) ou PowerShell.
3. Inicie os consoles certificate authority e certificate template executando:

certsrv.msc
certtmpl.msc



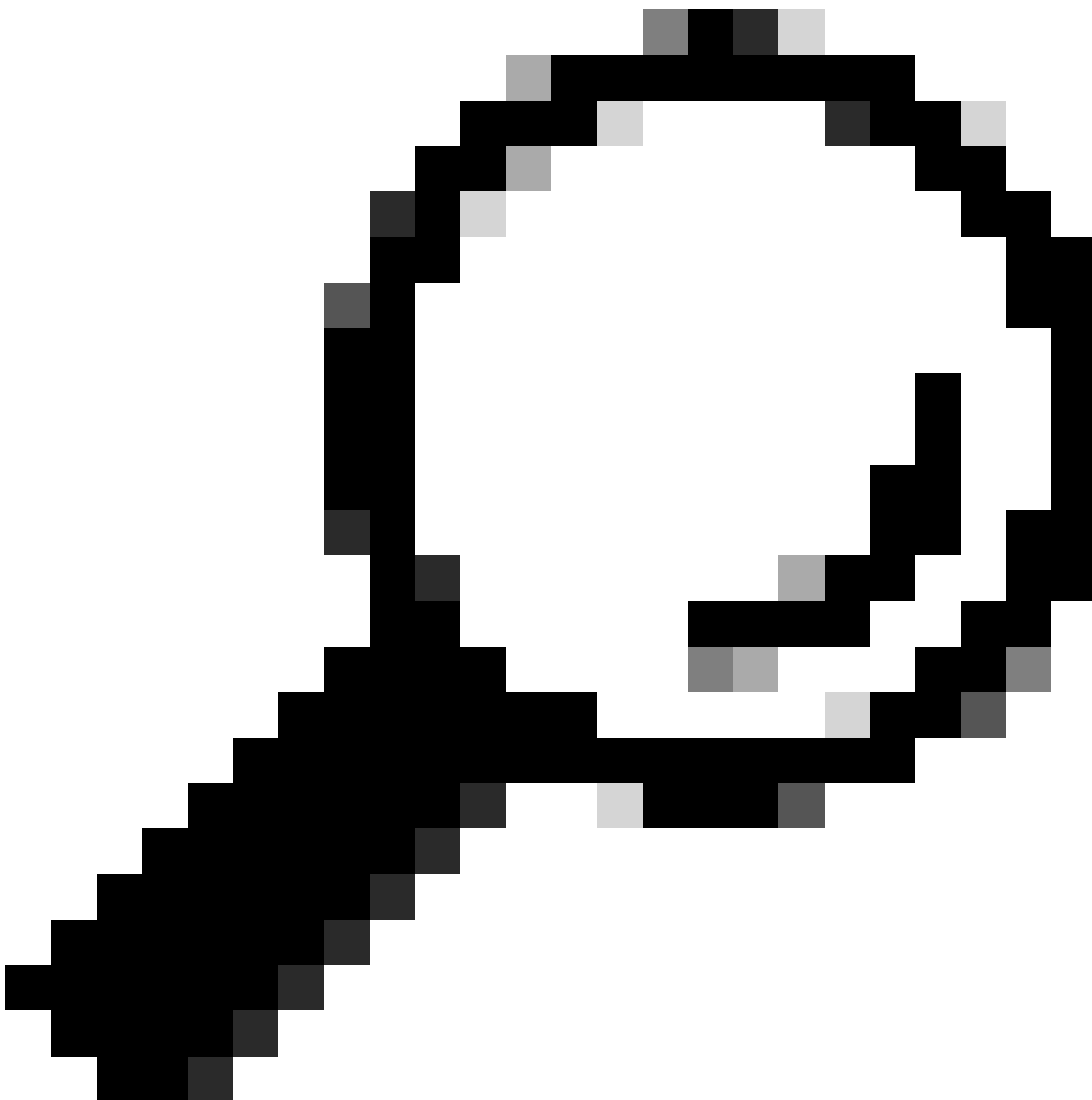
```
Administrator: Windows PowerShell
PS C:\Users\Administrator> certsrv.msc
PS C:\Users\Administrator> certtmpl.msc
PS C:\Users\Administrator> _
```

Administração Comandos do Powershell



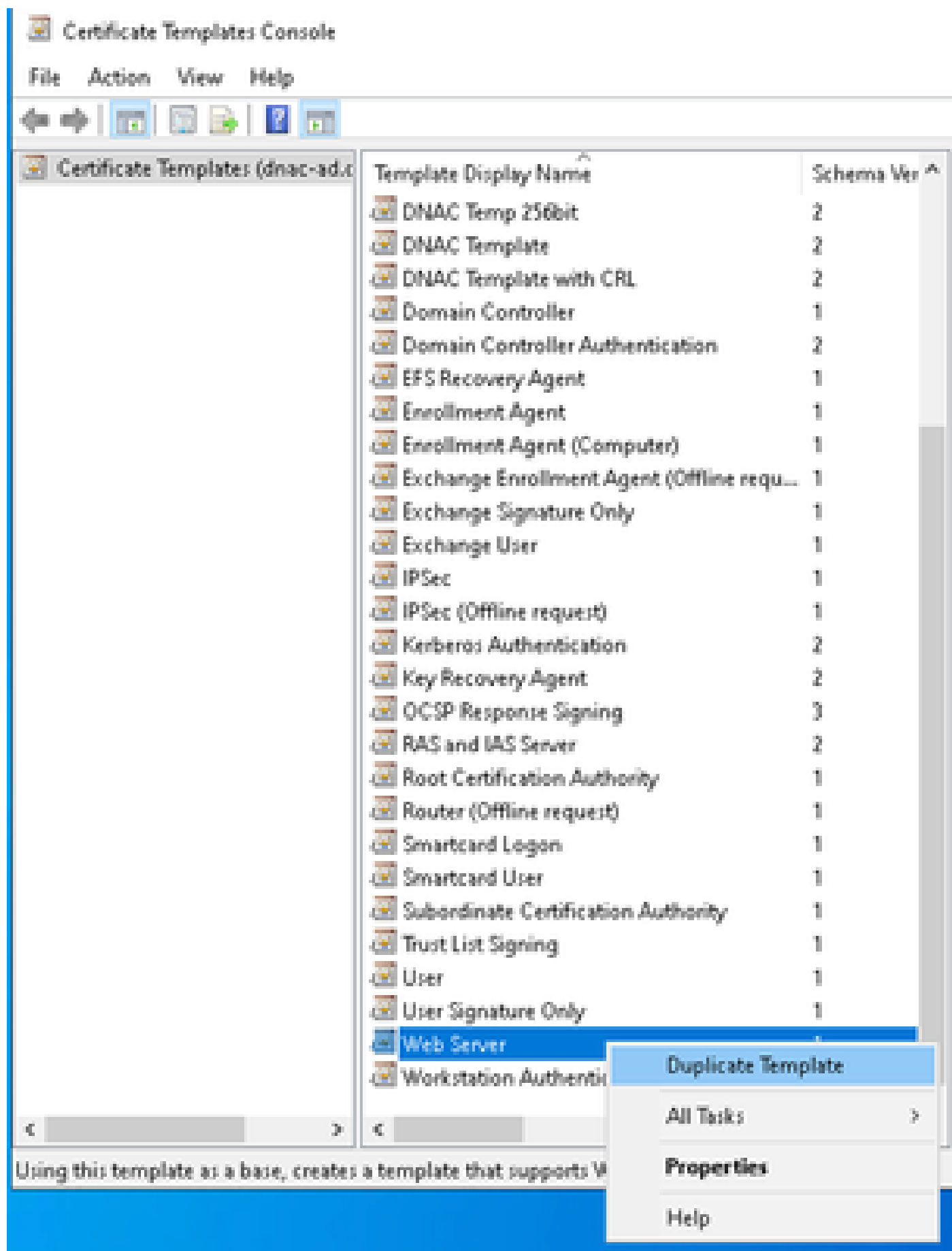
Exemplo do Windows Server

4. No Console de Modelo de Certificado, localize o modelo a ser clonado para criar um novo modelo personalizável.



Tip: Use o modelo de Servidor Web já que ele já inclui todos os parâmetros necessários para o certificado do Catalyst Center.

-
- Exemplo: clique com o botão direito do mouse no servidor web e selecione modelo duplicado.



Modelo Duplicado

5. Um novo modelo é aberto, modifique-o com as características necessárias.

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. Modifique o novo modelo da seguinte maneira:

6.1 Guia Geral.

- Insira um nome de modelo (por exemplo, Modelo do Catalyst Center).
- Defina o período de validade (padrão: 2 anos).

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

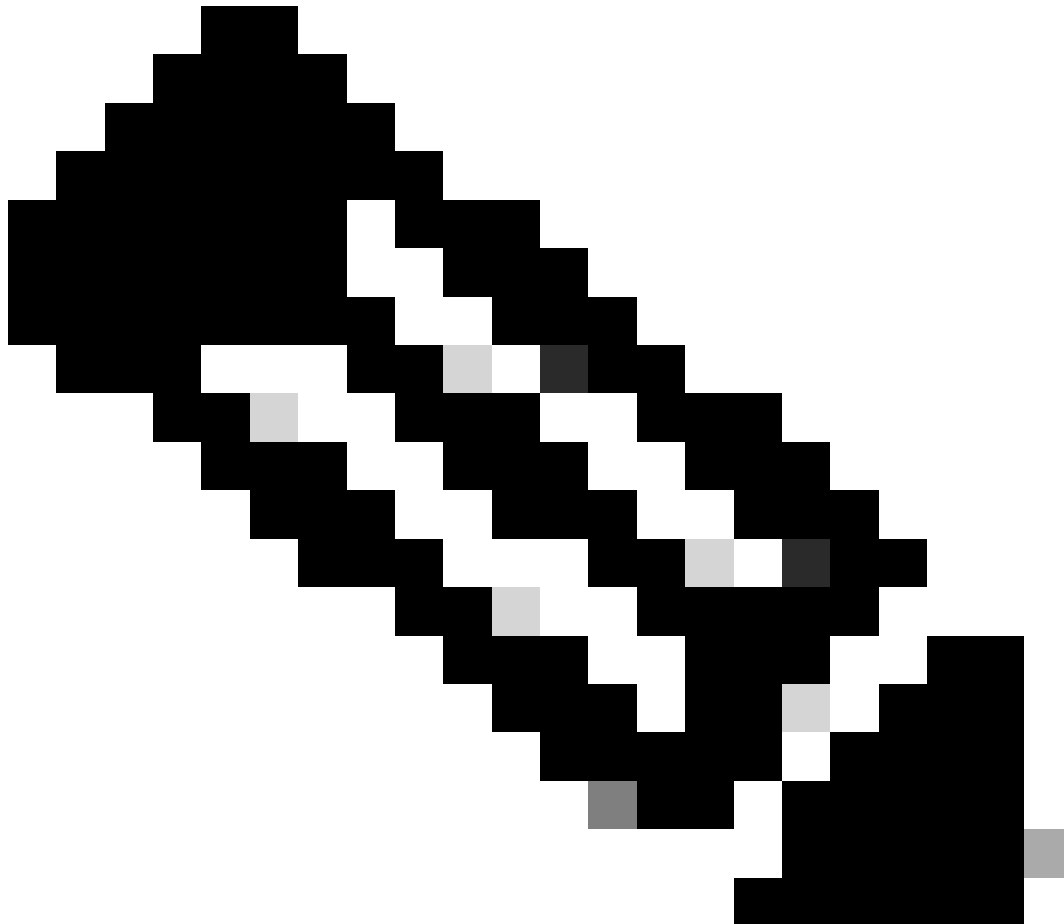
Cancel

Apply

Help

6.2 Aba Extensions (Extensões).

- Navegue até políticas de aplicativos e clique em editar.
-



Note: Nesta guia, confirme se o modelo inclui as extensões obrigatórias de Uso de Chave exigidas pelo certificado do Catalyst Center, como keyEncipherment e digitalSignature. Eles já estão presentes no modelo de servidor Web padrão usado como 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

- Clique em adicionar, localize autenticação de cliente e clique em ok para incluí-la.

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

Adicionar Política de Aplicativo

- Confirme se o modelo mostra Autenticação de cliente junto com os usos padrão.

Edit Application Policies Extension



An application policy defines how a certificate can be used.

Application policies:

Client Authentication
Server Authentication

Add...

Edit...

Remove

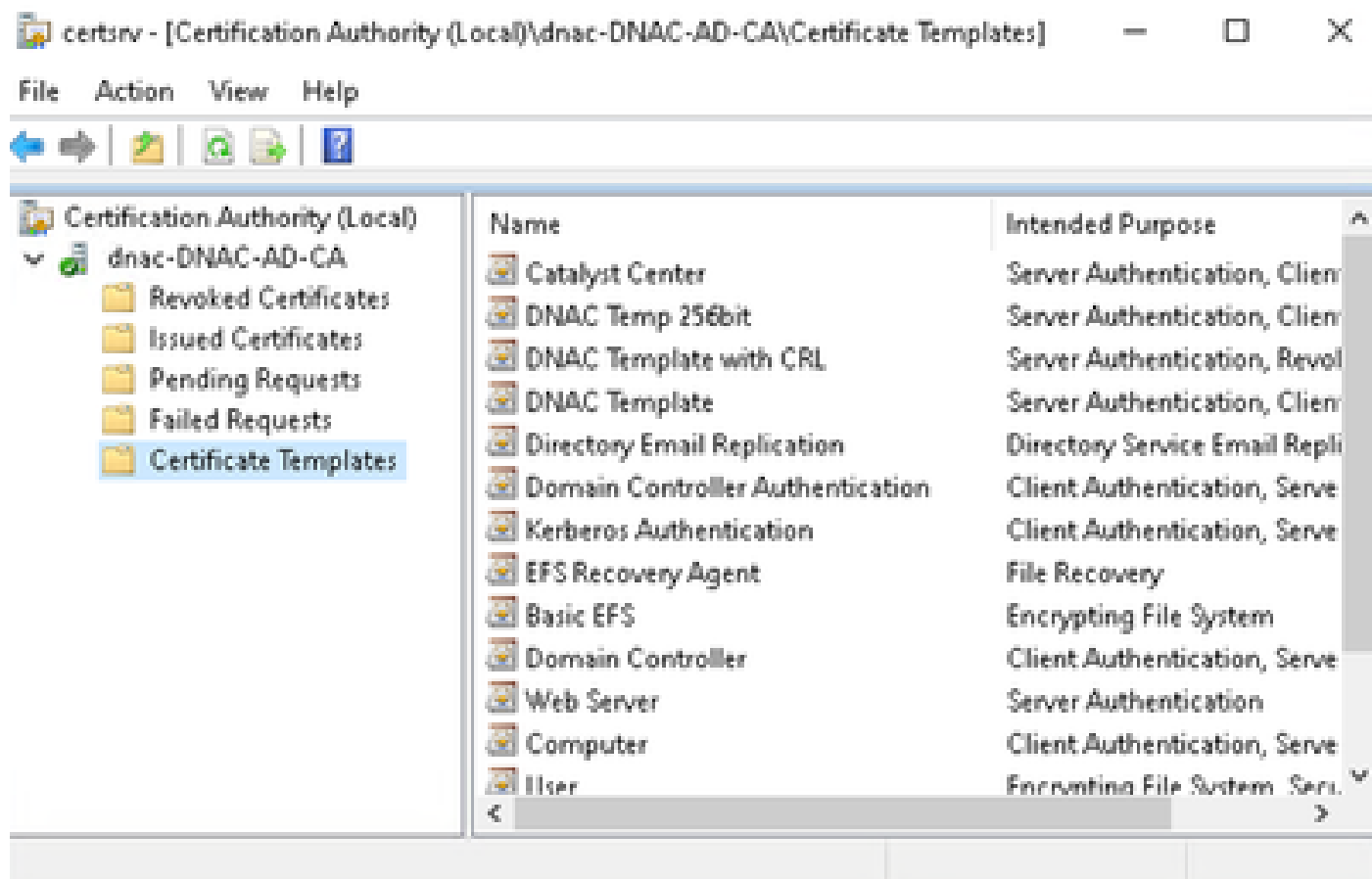
☐ Make this extension critical

OK

Cancel

7. Clique em aplicar e em ok.

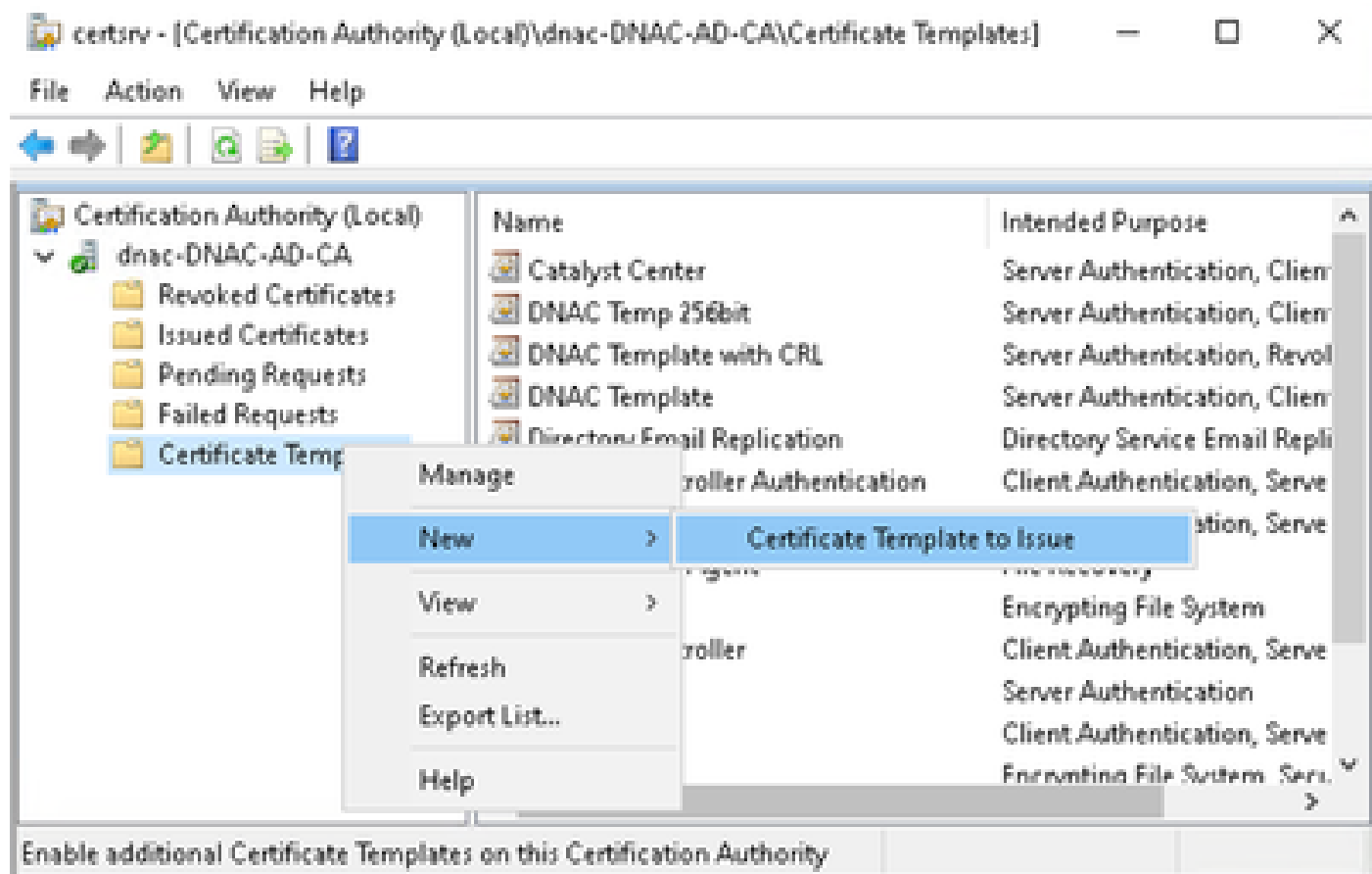
8. No console Certificate Authority, expanda a árvore CA e selecione a pasta certificate templates.



Modelos de Certificado de Árvore de Autoridades de Certificação

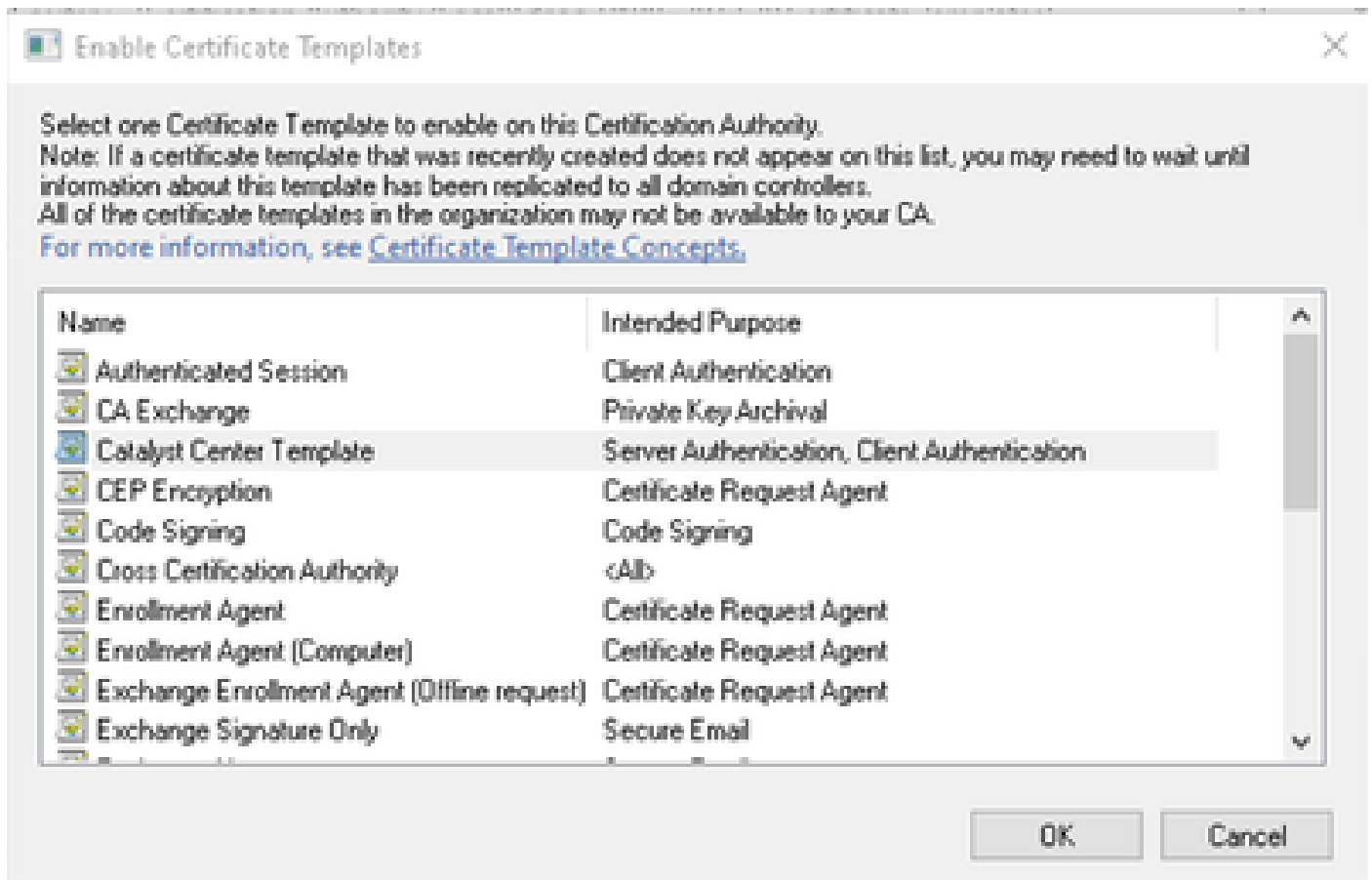
9. Clique com o botão direito do mouse na pasta modelos de certificado e selecione:

Novo > Modelo de certificado a emitir.



Novo modelo de certificado a emitir

10. Na nova janela, selecione o modelo recém-criado (por exemplo, Modelo do Catalyst Center) e clique em ok.

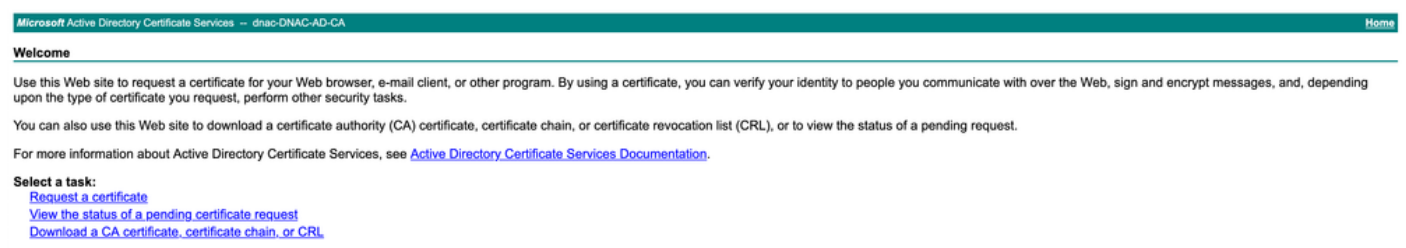


Modelo do Catalyst Center

11. O modelo agora aparece na lista Modelos de Certificado na CA.

12. Abra um navegador e navegue até:

<http://localhost/certsrv/>



Página de login <http://localhost/certsrv/>

13. Selecione solicitar um certificado, depois solicitação de certificado avançada, para verificar se o novo modelo está disponível.

14. Nesta página, submeta o CSR e selecione o modelo recém-criado para gerar o certificado assinado.

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+G7Ci1p0v415vc|
LtbzjY7pH80VXu+yePN85mPTeDL++poXx8vXUT8w|
2d14EajkSKQP8CJJh5W7gn3dd4w1r8h90Y5wR8g|
B1Zq07Ldz1jGRgJMj9hWe6nvnvJaVfy9o3M1GcYzc|
-----END CERTIFICATE REQUEST-----
```

Certificate Template:

Catalyst Center Template

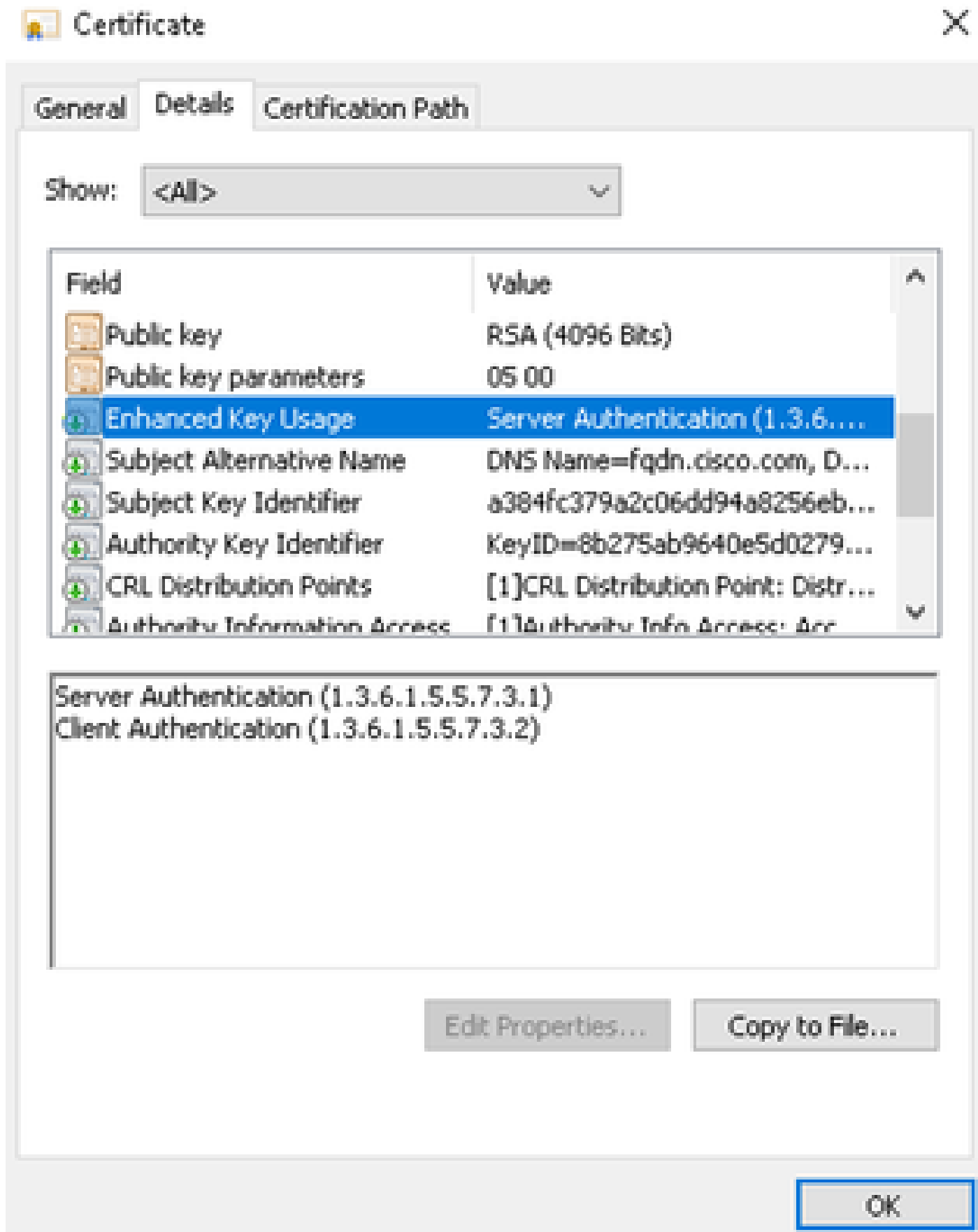
Additional Attributes:

Attributes:

Submit >

Solicitar um certificado

13. O certificado é gerado com as extensões corretas, conforme mostrado no exemplo.



Exemplo de certificado

Troubleshooting

Se você encontrar erros ao assinar o CSR, examine os logs do Windows Server para obter mais detalhes:

Erro:



Solucionar erros

1. Abra o visualizador de eventos executando:

`eventvwr.msc`

2. Navegue até Visualizador de Eventos > Logs do Windows > Aplicativo.

3. Filtrar ou pesquisar eventos onde:

1. Origem = Autoridade de Certificação

2. ID do evento = 53, 54, 55 ou similar (indicam que uma solicitação foi emitida, negada ou está pendente).

3. A mensagem de evento contém detalhes sobre o motivo da recusa (se aplicável).

4. Use a opção Find (clique com o botão direito do mouse em Application > Find...) e pesquise por:

- `certsrv`
- ID da solicitação (se conhecido, por exemplo, 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

Solucionar Problemas de Logs do Windows Server

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.