

为Catalyst Center创建Windows Server证书模板

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[配置](#)

[故障排除](#)

简介

本文档介绍在运行证书颁发机构(CA)工具的Windows Server上创建证书模板的步骤。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科Catalyst中心
- 安装并配置了证书颁发机构(CA)角色的Windows Server
- Windows Server上的管理员权限
- 访问证书颁发机构管理控制台
- 证书模板和证书签名请求(CSR)的基本知识

使用的组件

本文档中的信息基于Microsoft Windows Server 2022 Standard。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

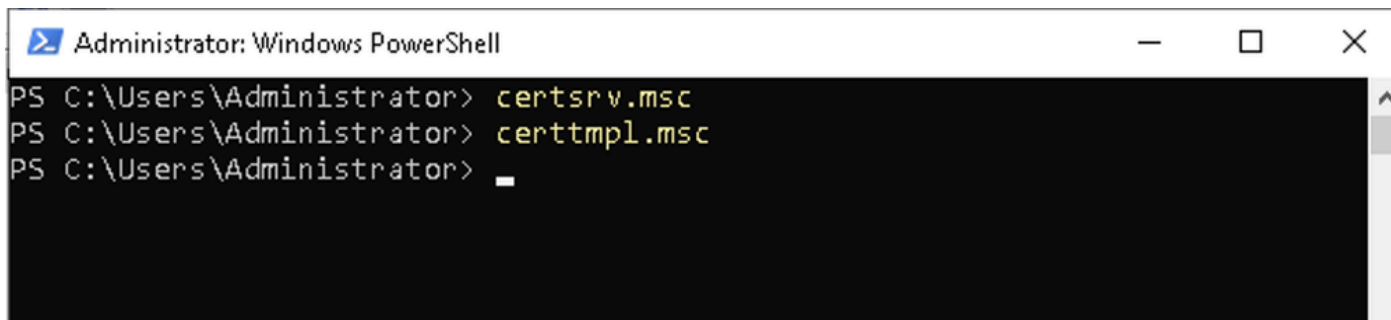
此自定义模板解决了默认CA模板从扩展密钥用法中删除客户端身份验证的问题。自定义模板能够对Catalyst Center生成的证书签名请求(CSR)进行签名。

配置

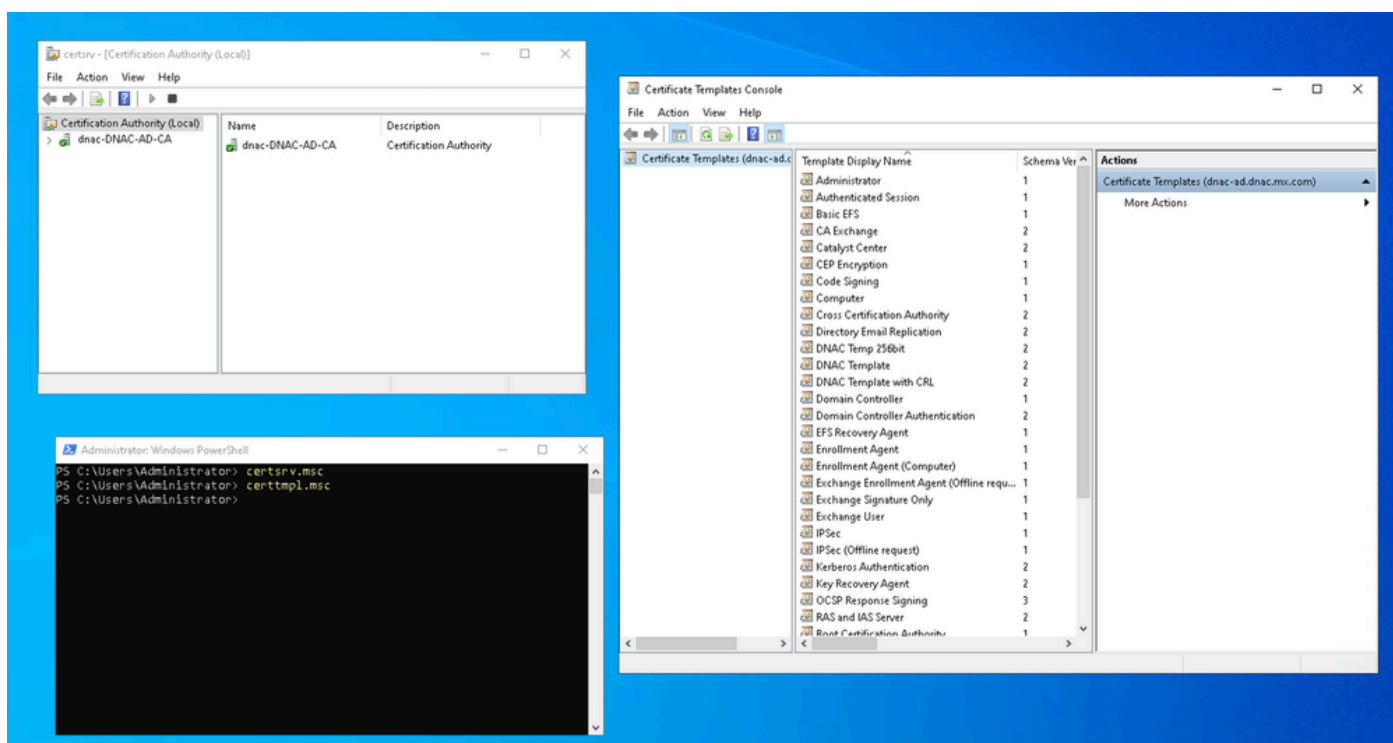
使用证书颁发机构(CA)在Windows Server上审核和配置证书模板的步骤。

1. 使用远程桌面登录到托管CA的Windows Server。
2. 打开命令提示符(CMD)或PowerShell会话。
3. 通过运行以下命令启动证书颁发机构和证书模板控制台：

certsrv.msc
certtmpl.msc

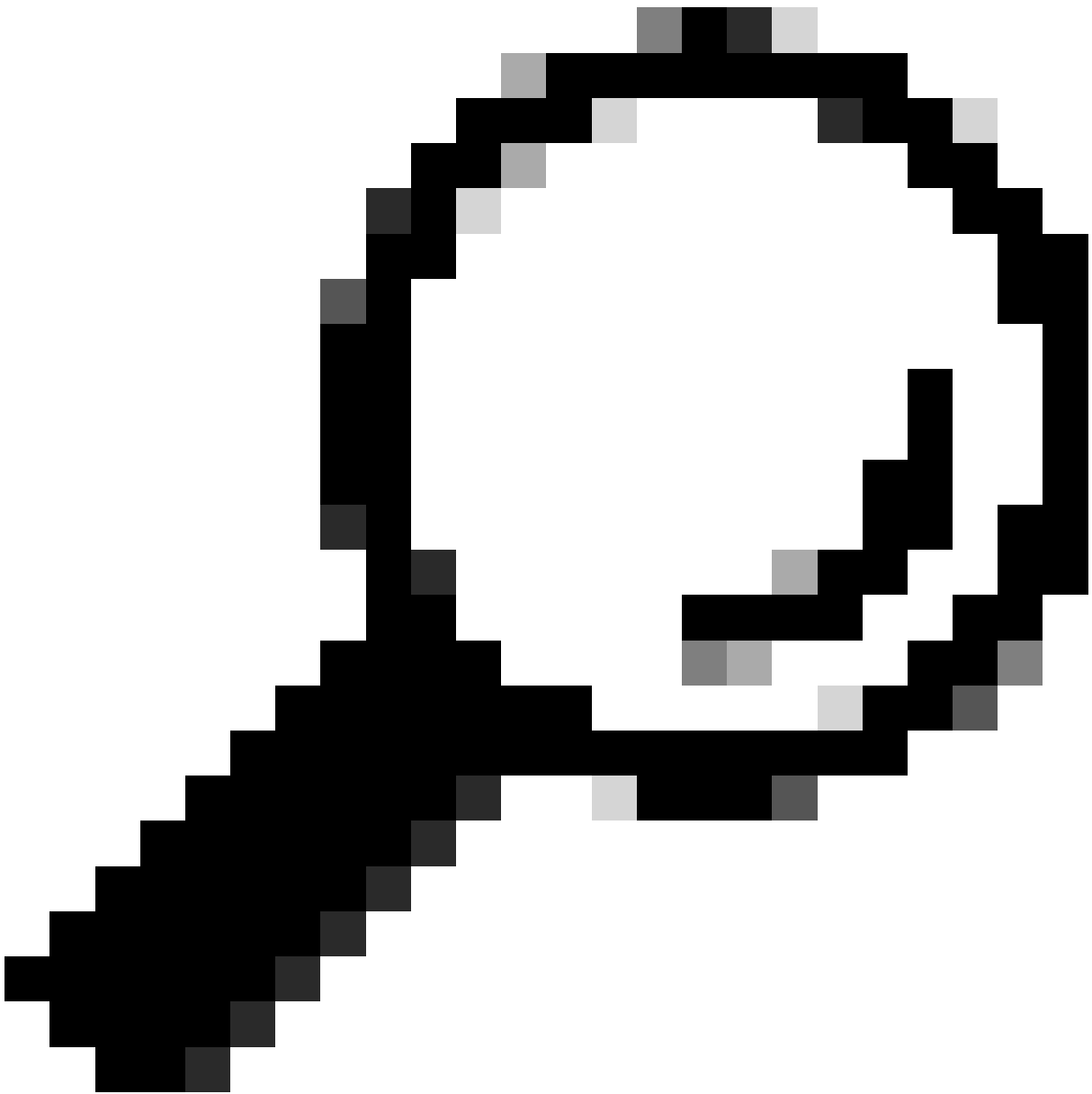


管理Powershell命令



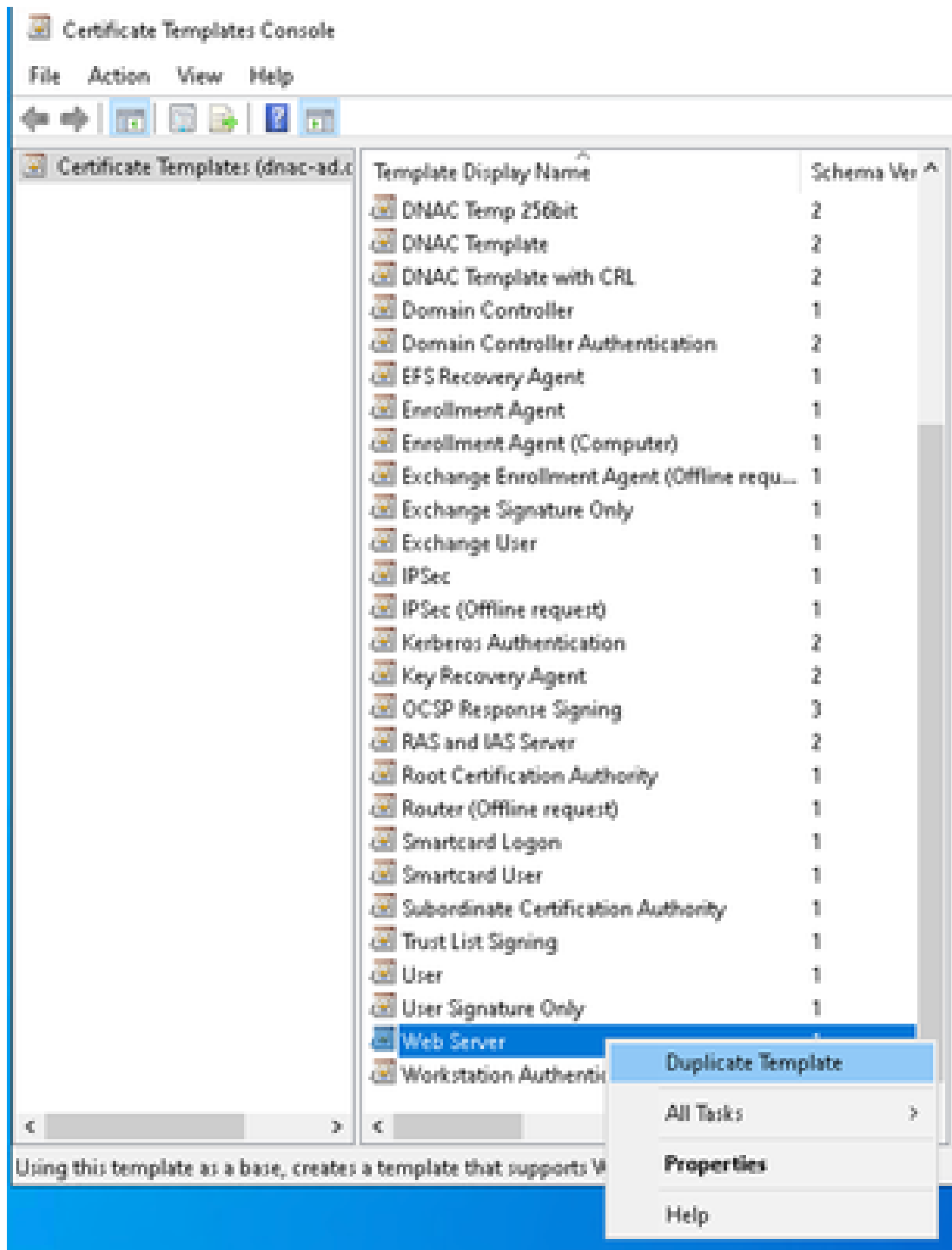
Windows Server示例

- 4.在证书模板控制台中，找到要克隆的模板，以创建新的可自定义模板。



提示：使用Web服务器模板，因为它已包含Catalyst Center证书的所有必需参数。

-
- 示例：右键单击web服务器并选择复制模板。



复制模板

5.新模板已打开，请根据所需特征对其进行修改。

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Superseded Templates			Extensions		Security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.按如下方式修改新模板：

6.1常规选项卡。

- 输入模板名称（例如，Catalyst Center模板）。
- 定义有效期(默认：2年)。

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Superseded Templates			Extensions		Security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

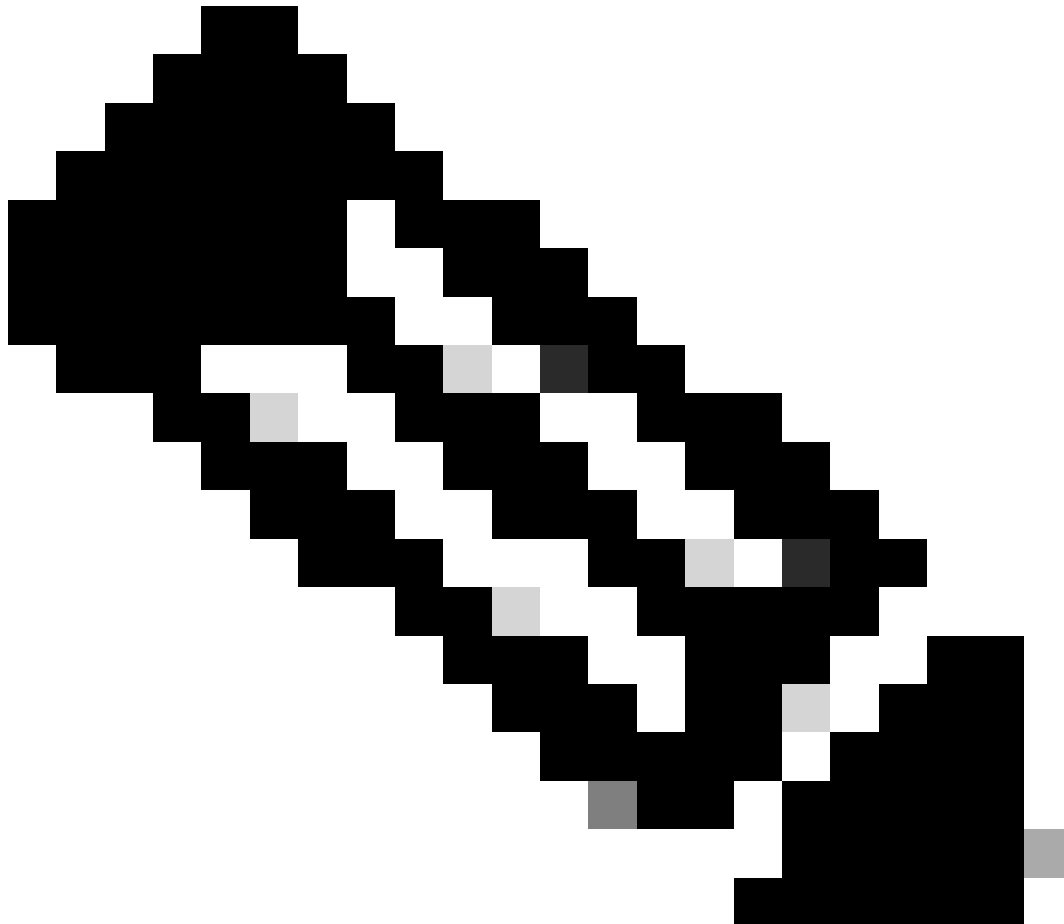
Apply

Help

模板名称

6.2扩展选项卡。

- 导航到应用策略，然后单击编辑。



注意：在此选项卡中，确认模板包括Catalyst Center证书所需的强制性密钥使用扩展，例如keyEncipherment和digitalSignature。这些内容已存在于用作基础的默认Web服务器模板中。

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

- 单击add，找到client authentication，然后单击ok将其包含在内。

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

添加应用策略

- 确认模板显示Client Authentication以及默认用法。

Edit Application Policies Extension



An application policy defines how a certificate can be used.

Application policies:

Client Authentication
Server Authentication

Add...

Edit...

Remove

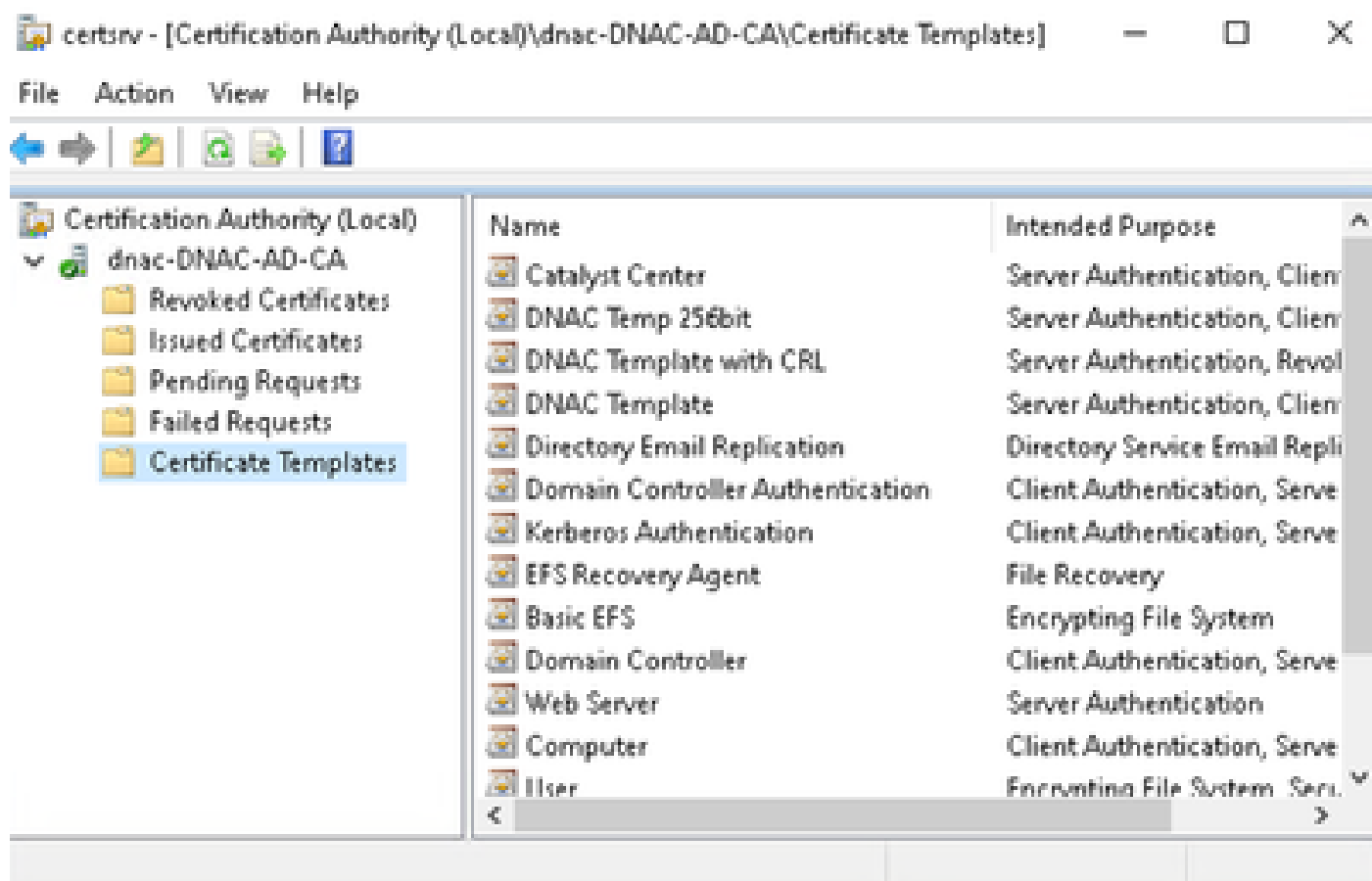
☐ Make this extension critical

OK

Cancel

7.单击apply，然后单击ok。

8.在Certificate Authority控制台中，展开CA树，然后选择certificate templates文件夹。



CA树证书模板

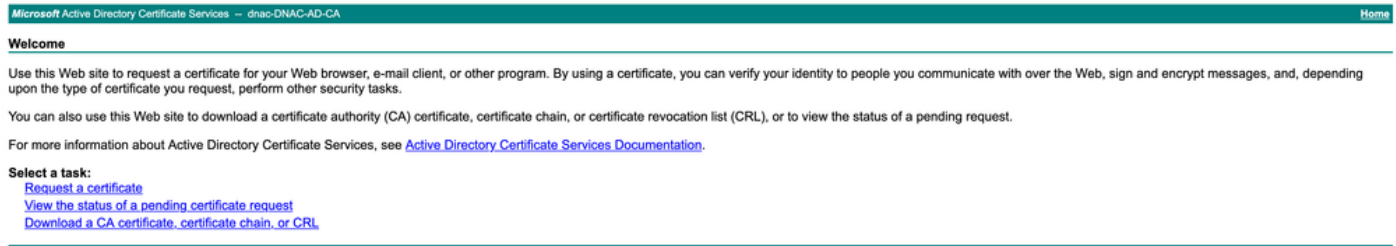
9.右键单击certificate templates文件夹并选择：

New > Certificate Template to Issue.

11.模板现在显示在CA的证书模板列表下。

12.打开浏览器并导航至：

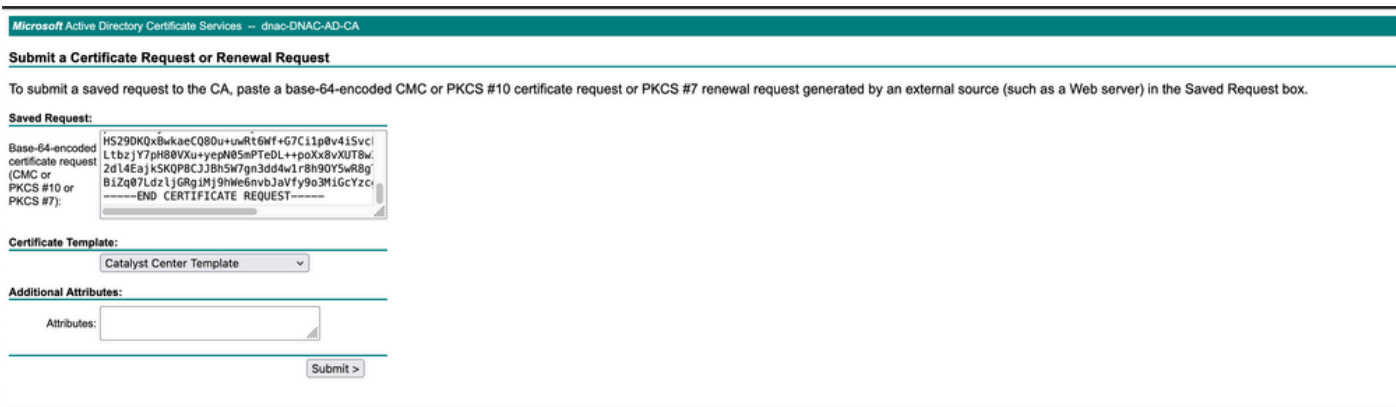
http://localhost/certsrv/



登录页面http://localhost/certsrv/

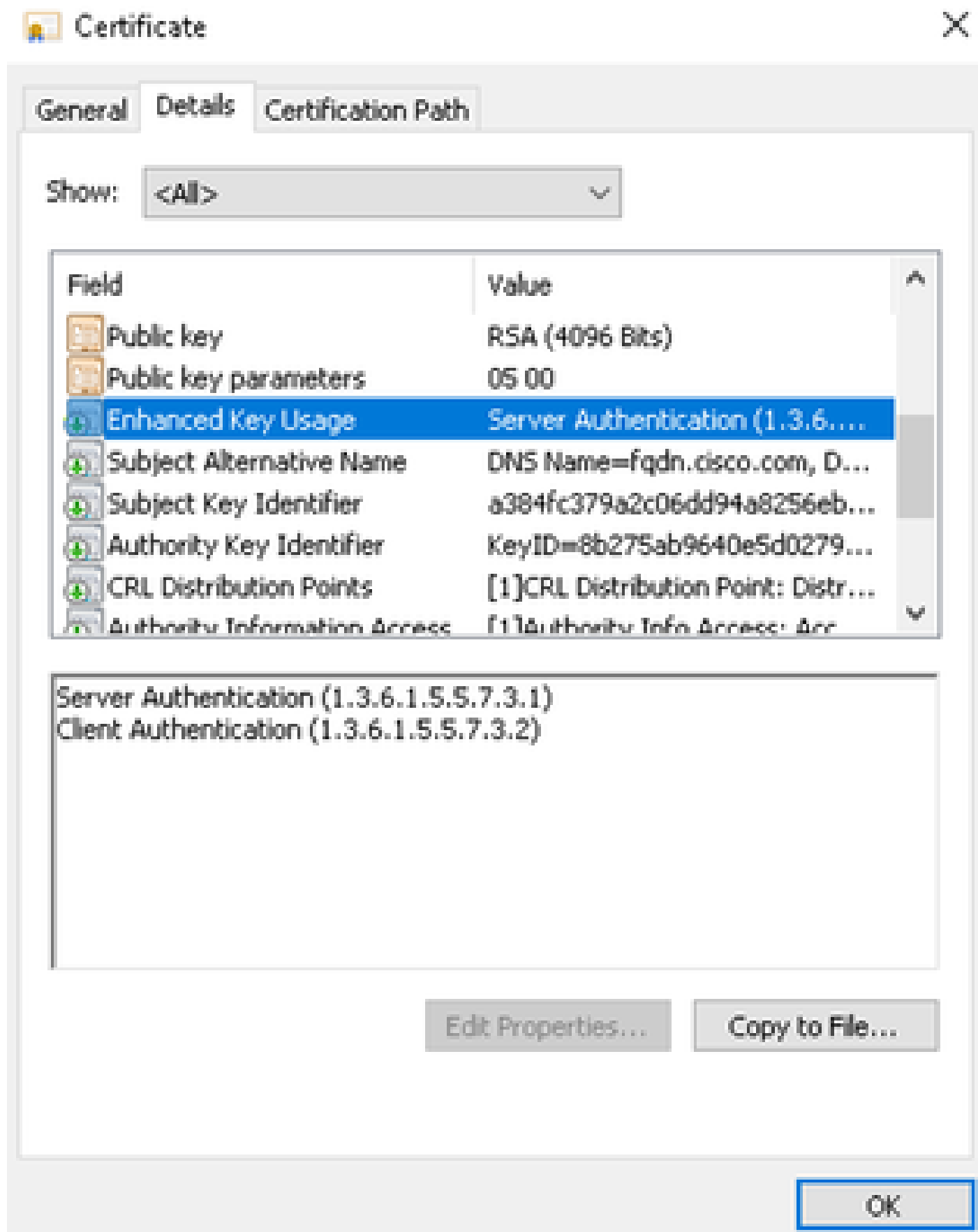
13.选择请求证书，然后选择高级证书请求，以验证新模板是否可用。

14.在此页上，提交CSR并选择新创建的模板以生成签名证书。



申请证书

13.证书是使用正确的扩展名生成的，如示例所示。



证书示例

故障排除

如果在签署CSR时遇到错误，请查看Windows Server日志，了解更多详细信息：

Error:



故障排除错误

1.通过运行以下命令打开事件查看器：

`eventvwr.msc`

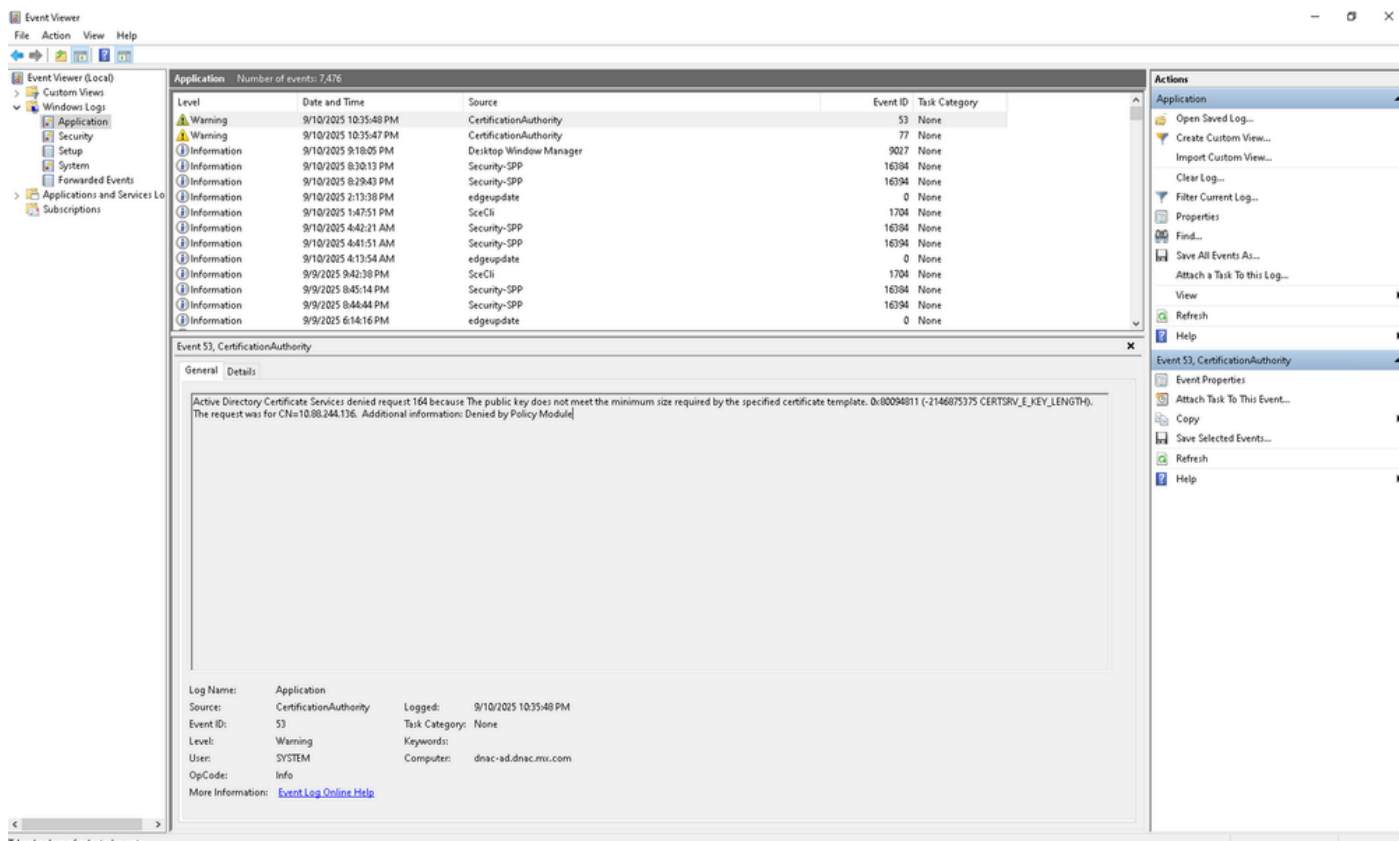
2.定位至事件查看器> Windows日志>应用程序。

3. 在以下情况下过滤或搜索事件：

1. 来源= CertificationAuthority
2. 事件ID = 53、54、55或类似事件（表示请求已发出、被拒绝或处于待处理状态）。
3. 事件消息包含有关拒绝原因的详细信息（如果适用）。

4.使用Find选项(右键单击Application > Find...)并按以下搜索方式：

- certsrv
- 请求ID(如果已知，例如164)



Windows Server日志故障排除

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。