

# 為Catalyst Center建立Windows Server證書模板

## 目錄

---

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[設定](#)

[疑難排解](#)

---

## 簡介

本文說明在運行證書頒發機構(CA)工具的Windows Server上建立證書模板的步驟。

## 必要條件

### 需求

思科建議您瞭解以下主題：

- Cisco Catalyst Center
- 安裝並配置具有證書頒發機構(CA)角色的Windows Server
- Windows Server上的管理員許可權
- 對證書頒發機構管理控制檯的訪問許可權
- 憑證範本和憑證簽名要求(CSR)的基本知識

### 採用元件

本文檔中的資訊基於Microsoft Windows Server 2022 Standard。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

## 背景資訊

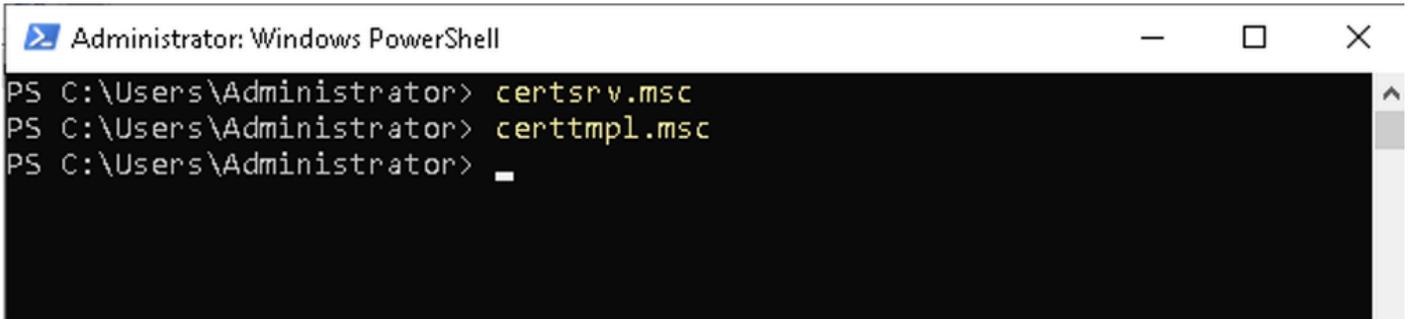
此自定義模板可解決預設CA模板從擴展金鑰用法中刪除客戶端身份驗證的問題。自定義模板能夠對由Catalyst Center生成的證書簽名請求(CSR)進行簽名。

## 設定

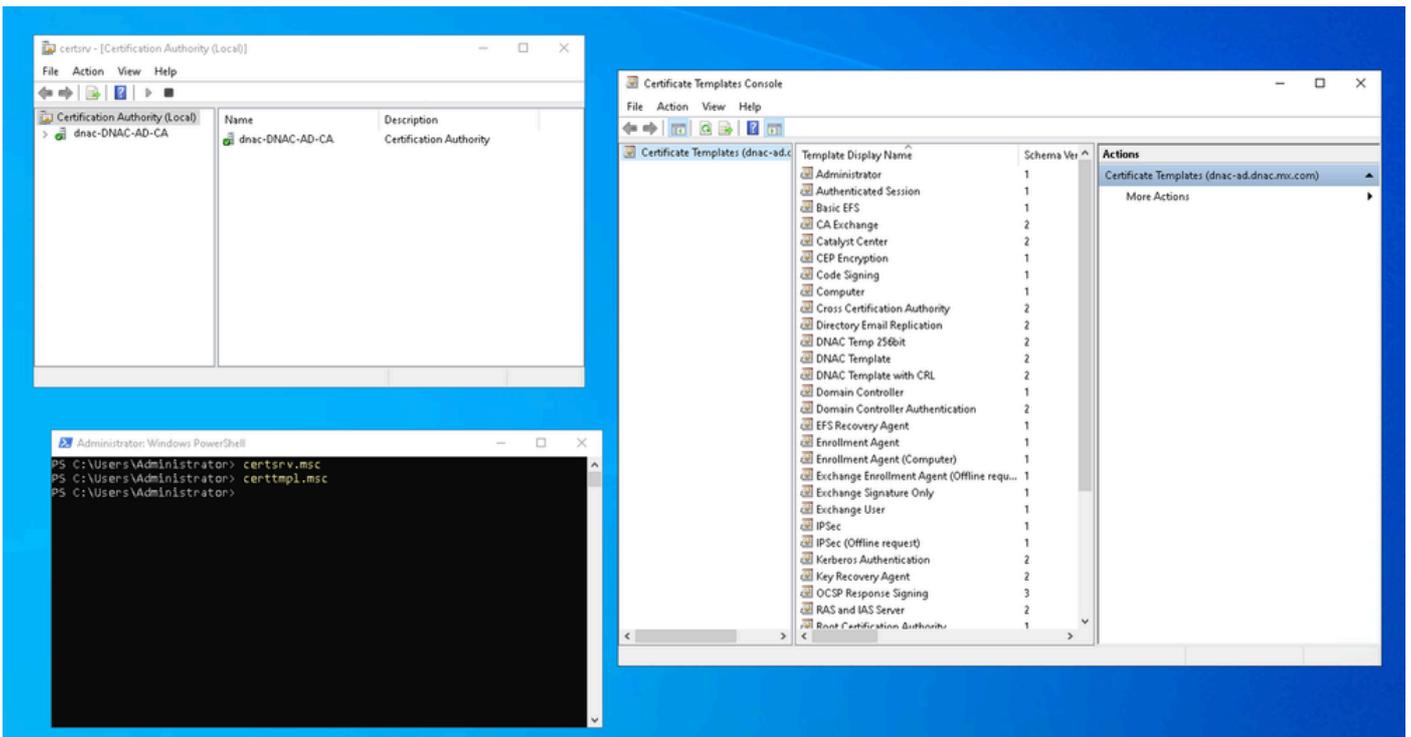
使用證書頒發機構(CA)在Windows Server上稽核和配置證書模板的步驟。

1. 使用遠端桌面登錄到託管CA的Windows Server。
2. 開啟命令提示符(CMD)或powerShell會話。
3. 通過運行以下命令啟動證書頒發機構和證書模板控制檯：

certsrv.msc  
certtmpl.msc

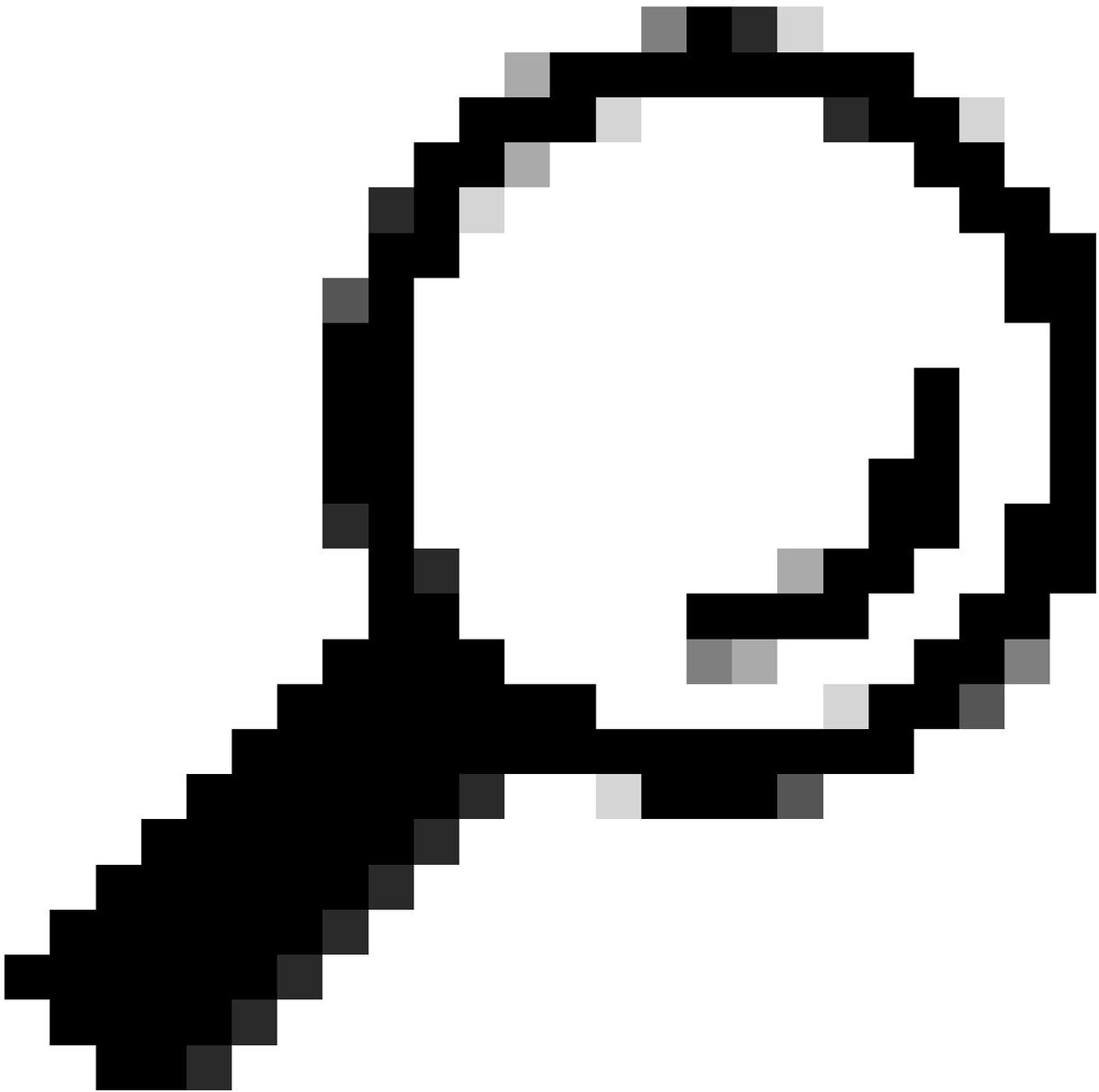


管理Powershell命令



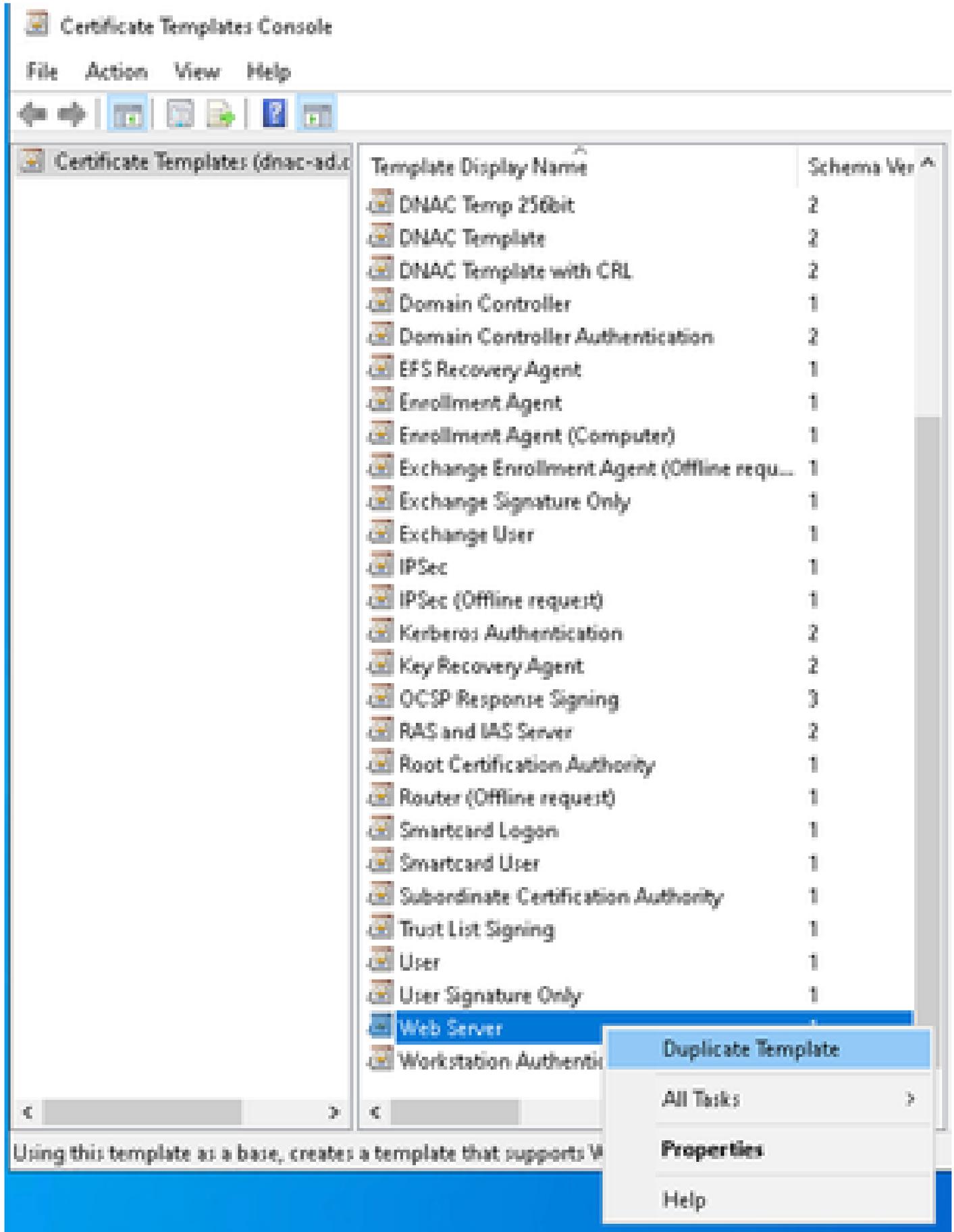
Windows Server示例

4. 在證書模板控制檯中，找到要克隆的模板，以建立新的可自定義模板。



提示：使用Web伺服器模板，因為它已包含Catalyst Center證書的所有必需引數。

- 
- 範例：按一下右鍵web server，然後選擇duplicate template。



複製模板

5. 開啟新模板，使用所需特徵對其進行修改。

## 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Superseded Templates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

模板所需特徵

6.按如下方式修改新模板：

6.1 「常規」頁籤。

- 輸入模板名稱（例如Catalyst Center模板）。
- 定義有效期(預設值：2年)。



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

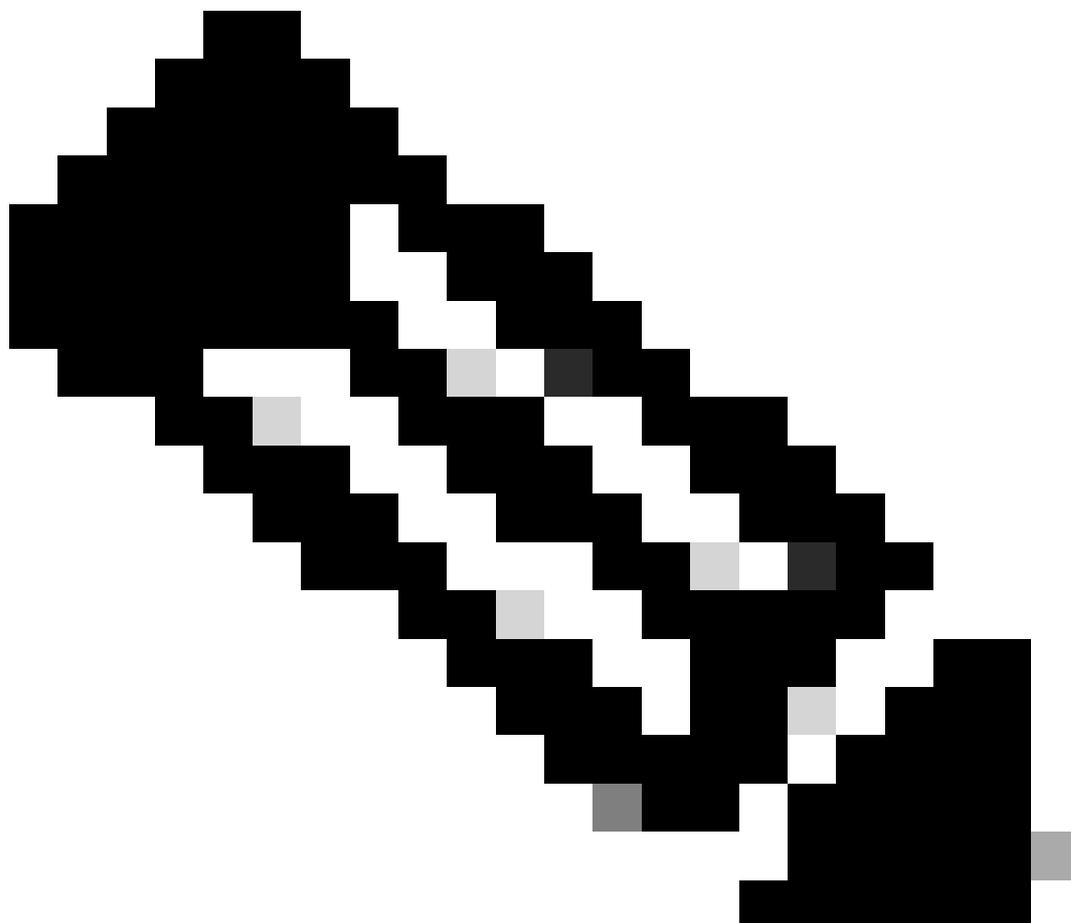
Publish certificate in Active Directory

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

模板名稱

## 6.2 擴展頁籤。

- 導航到應用程式策略，然後按一下edit。
- 



附註：在此頁籤中，確認模板包括Catalyst Center證書所需的強制性金鑰使用擴展，例如keyEncipherment和digitalSignature。它們已存在於用作基礎的預設Web伺服器模板中。

---

# 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**

- 按一下add，找到client authentication，然後按一下ok以包含它。

## 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:

A list box containing the following application policies:

- Any Purpose
- Attestation Identity Key Certificate
- Certificate Request Agent
- Client Authentication** (highlighted)
- 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

新增應用程式策略

- 確認模板顯示Client Authentication以及預設用法。

## Edit Application Policies Extension



An application policy defines how a certificate can be used.

Application policies:

Client Authentication  
Server Authentication

Add...

Edit...

Remove

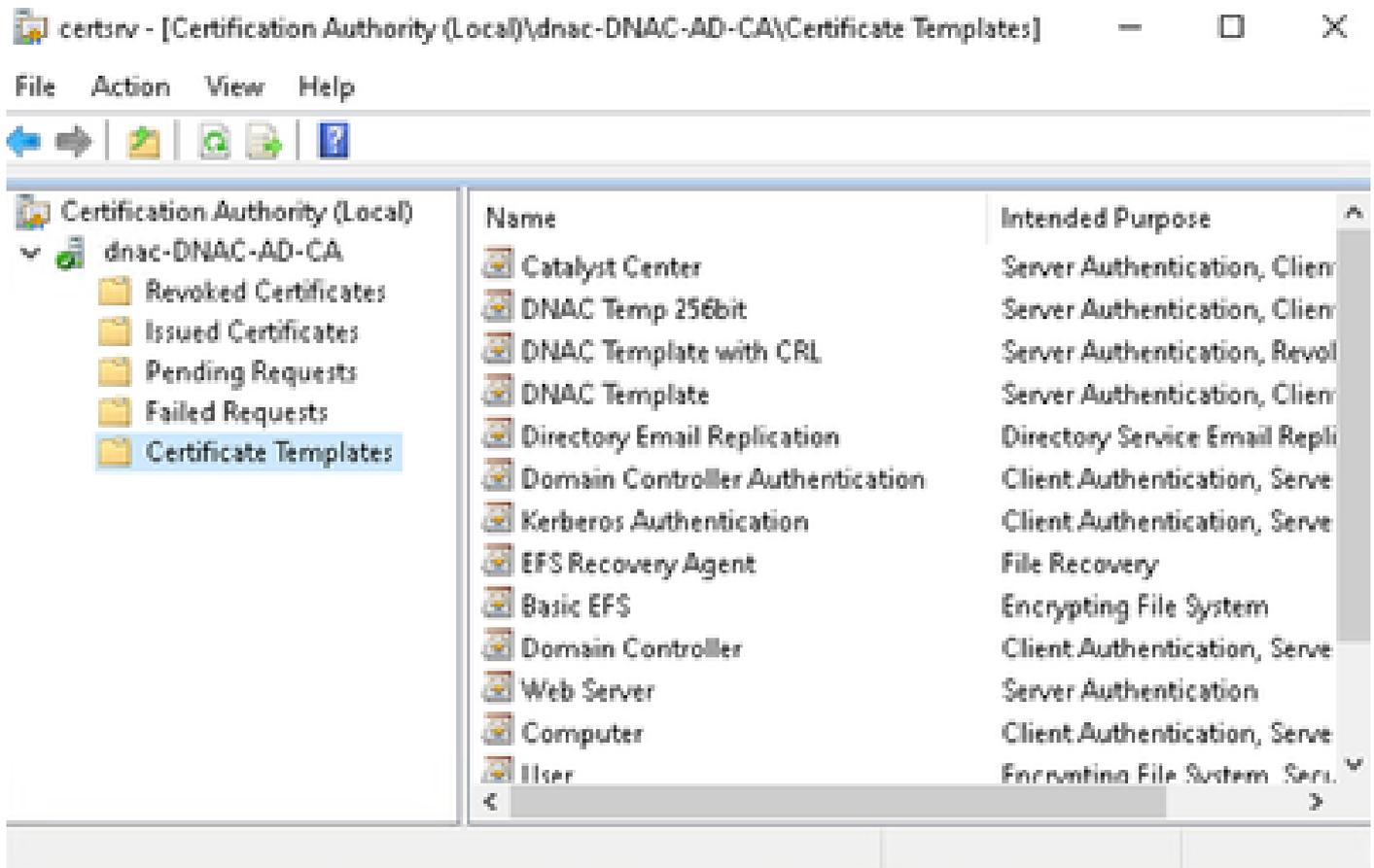
Make this extension critical

OK

Cancel

7.按一下apply，然後按一下ok。

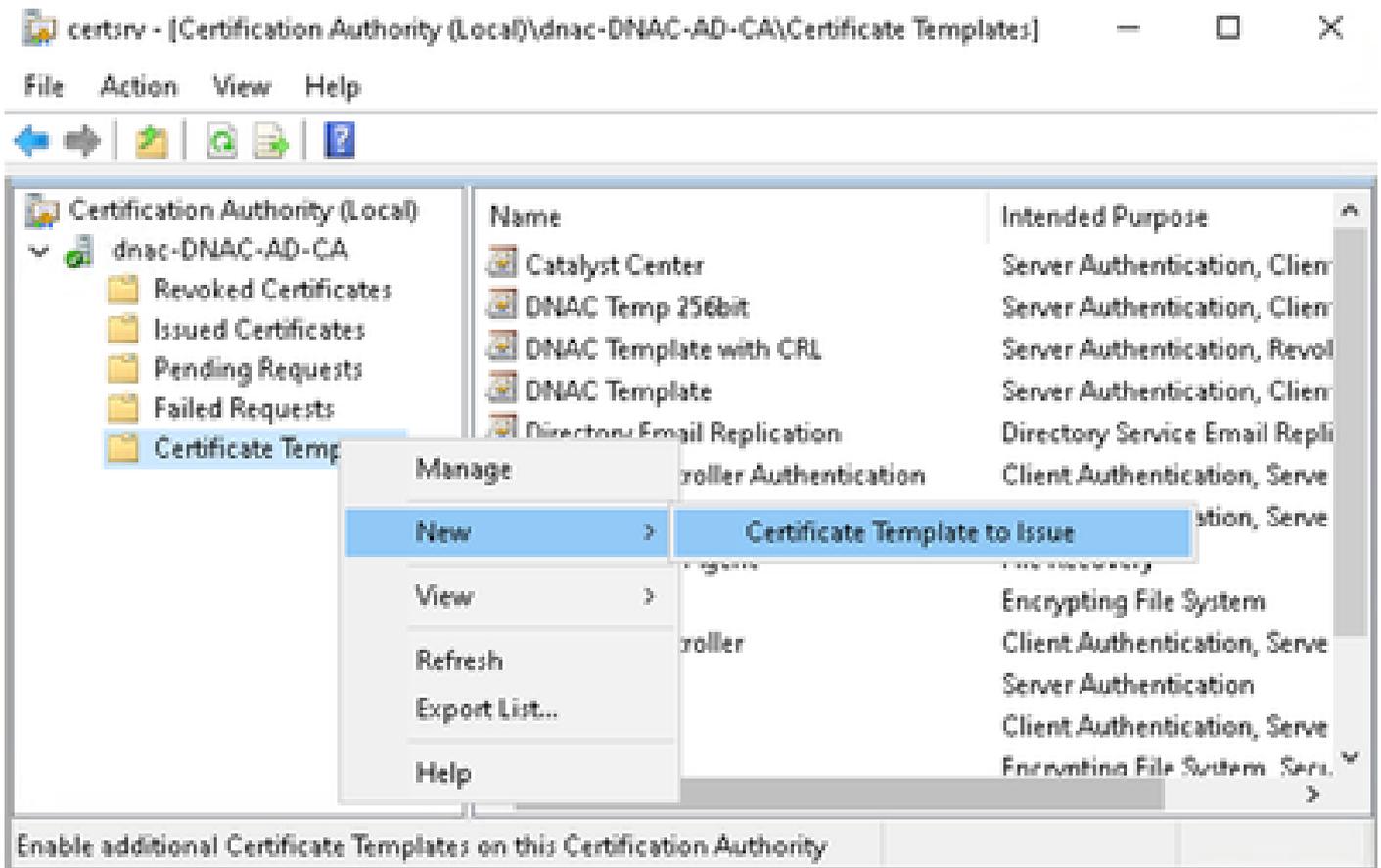
8.在Certificate Authority控制檯中，展開CA樹，然後選擇certificate templates資料夾。



CA樹憑證模板

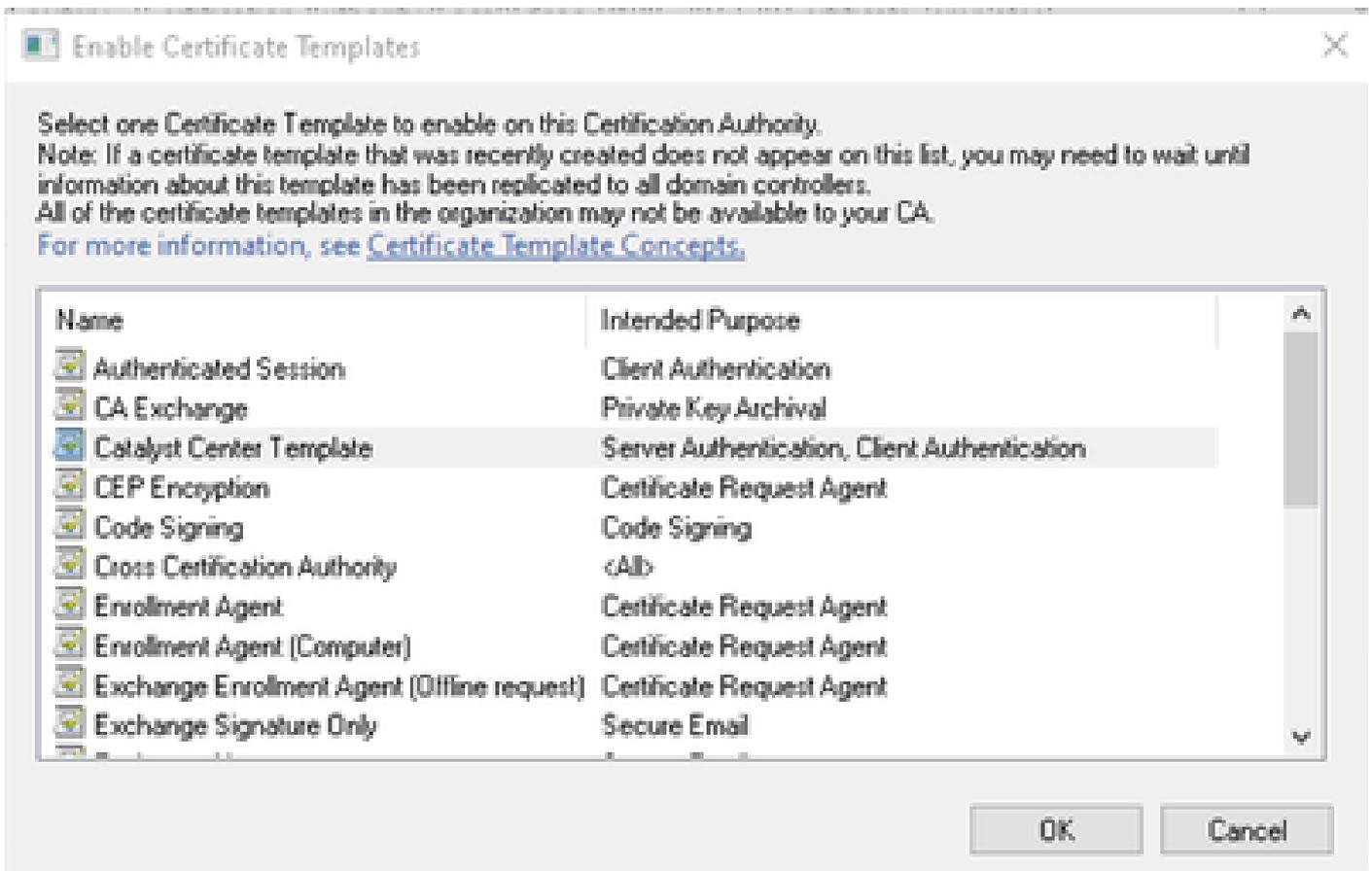
9.按一下右鍵證書模板資料夾，然後選擇：

新建>要頒發的證書模板.



要頒發的新證書模板

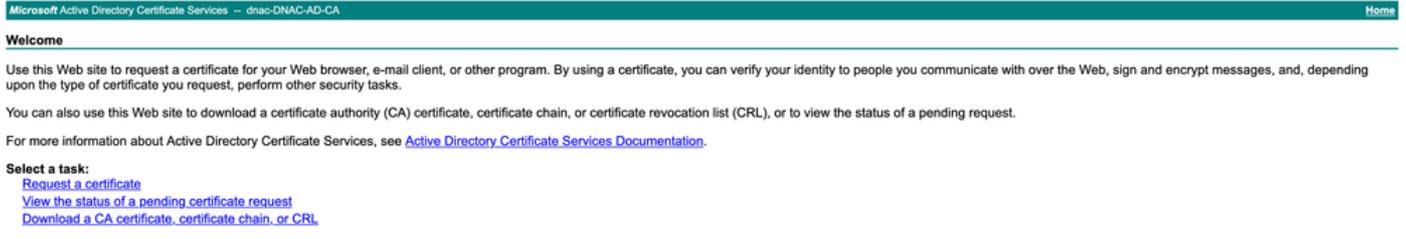
10. 在新視窗中，選擇新創建的模板（例如Catalyst Center模板），然後按一下ok。



11. 模板現在顯示在CA的Certificate Templates清單下。

12. 開啟瀏覽器，然後導航至：

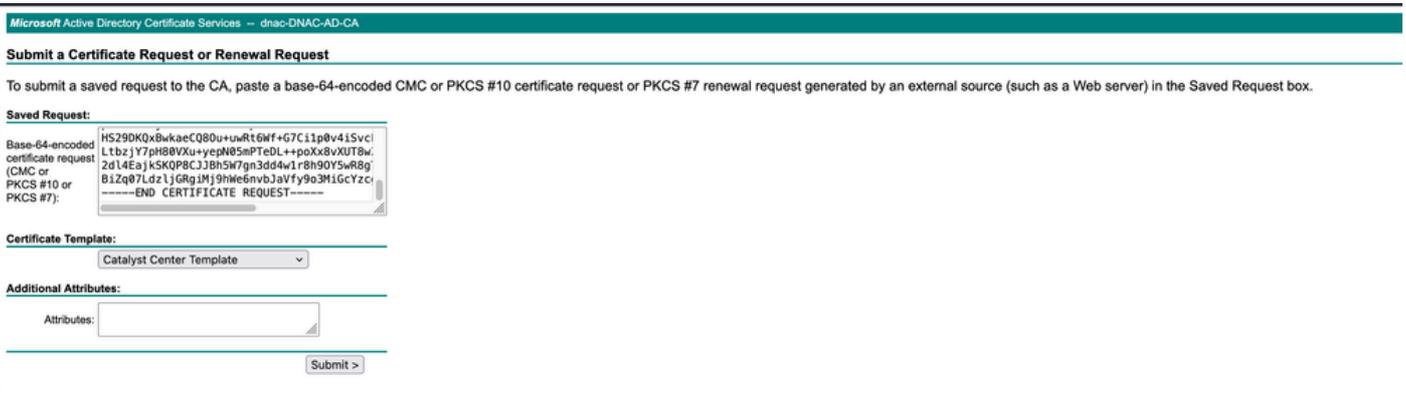
http://localhost/certsrv/



登入頁面http://localhost/certsrv/

13. 依次選擇請求證書和高級證書請求，以驗證新模板是否可用。

14. 在此頁面上，提交CSR並選擇新建的模板以生成簽名證書。



請求證書

13. 憑證是使用正確的擴展生成的，如示例所示。

General Details Certification Path

Show: &lt;All&gt;

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

憑證範例

疑難排解

如果在對CSR進行簽名時遇到錯誤，請檢視Windows Server日誌以瞭解更多詳細資訊：

錯誤：



疑難排解

1.通過運行以開啟事件檢視器：

eventvwr.msc

2.定位至「事件檢視器」>「Windows日誌」>「應用程式」。

3. 在以下情況下過濾或搜尋事件：

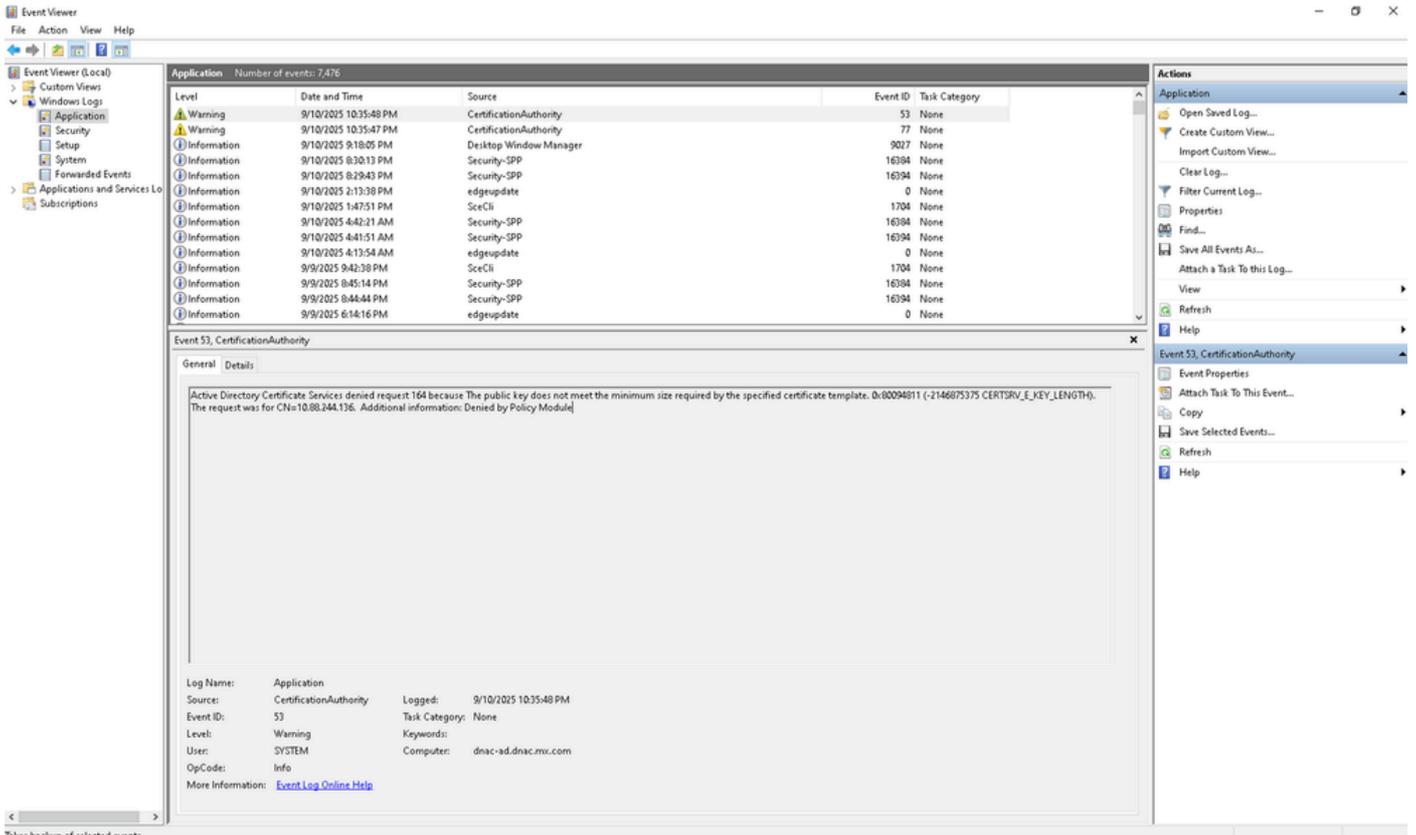
1. 來源= CertificationAuthority

2. 事件ID = 53、54、55或類似事件（這些事件表示請求已發出、被拒絕或處於掛起狀態）。

3. 事件消息包含有關拒絕原因的詳細資訊（如果適用）。

4.使用Find選項(按一下右鍵Application > Find...)，然後按以下方式搜尋：

- certsrv
- 請求ID(如果知道，例如164)



排除Windows Server日誌故障

## 關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。