CAPFオンラインCAによる自動証明書登録および更新の設定

内容

はじめに

このドキュメントでは、Cisco Unified Communications Manager(CUCM)のCertificate Authority Proxy Function(CAPF)オンライン機能を使用した自動証明書登録および更新について説明します。

著者：Cisco TAC エンジニア、Michael Mendoza

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco Unified Communications Manager
- X.509 証明書
- Windows Server
- Windows Active Directory(AD)
- Windowsインターネットインフォメーションサービス(IIS)
- NT（新しいテクノロジー）LAN Manager(NTLM)認証

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- CUCM バージョン 12.5.1.10000-22
- Windows Server 2012 R2
- IP Phone CP-8865/ファームウェア：SIP 12-1-1SR1-4および12-5-1SR2。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

このドキュメントでは、この機能の設定と、その他の調査に関連するリソースについて説明します。

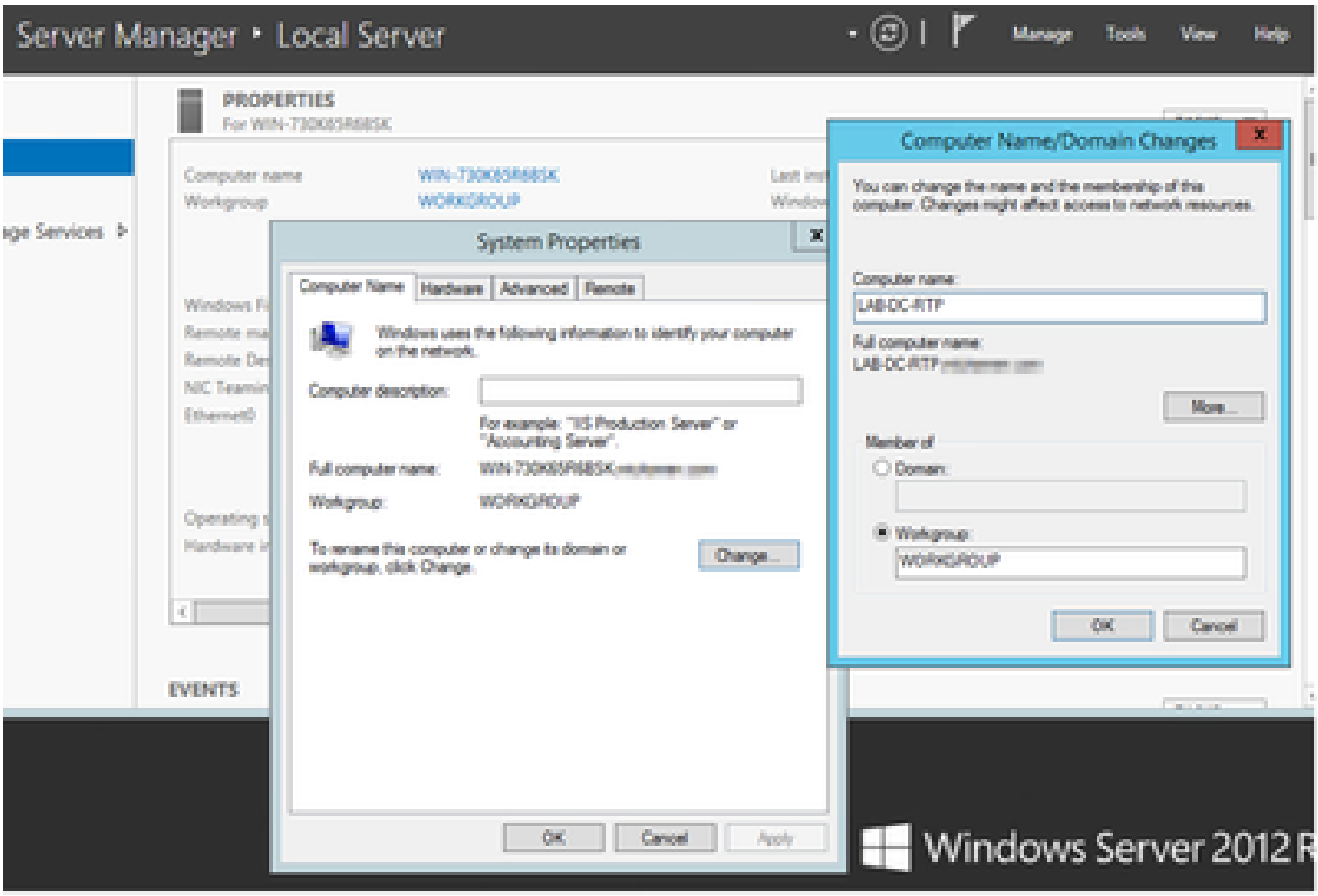
サーバの日付と時刻を確認する

サーバのルートCA（認証局）証明書およびそのサーバから発行された証明書の有効期間に影響を与えるため、Windowsサーバに正しい日付、時刻、およびタイムゾーンが設定されていることを確認します。

サーバーコンピューター名の更新

デフォルトでは、サーバのコンピュータ名にはWIN-730K65R6BSKなどのランダムな名前が付けられます。ADドメインサービスを有効にする前に最初に行う必要があるのは、インストールの最後までにサーバのコンピュータ名を、サーバのホスト名とルートCA発行者名が必要とする値に更新することです。それ以外の場合は、ADサービスのインストール後にこの設定を変更するために、追加の手順が大量に必要になります。

- Local Serverに移動し、コンピュータ名を選択してSystem Propertiesを開きます
- Changeボタンを選択し、新しいコンピュータ名を入力します。



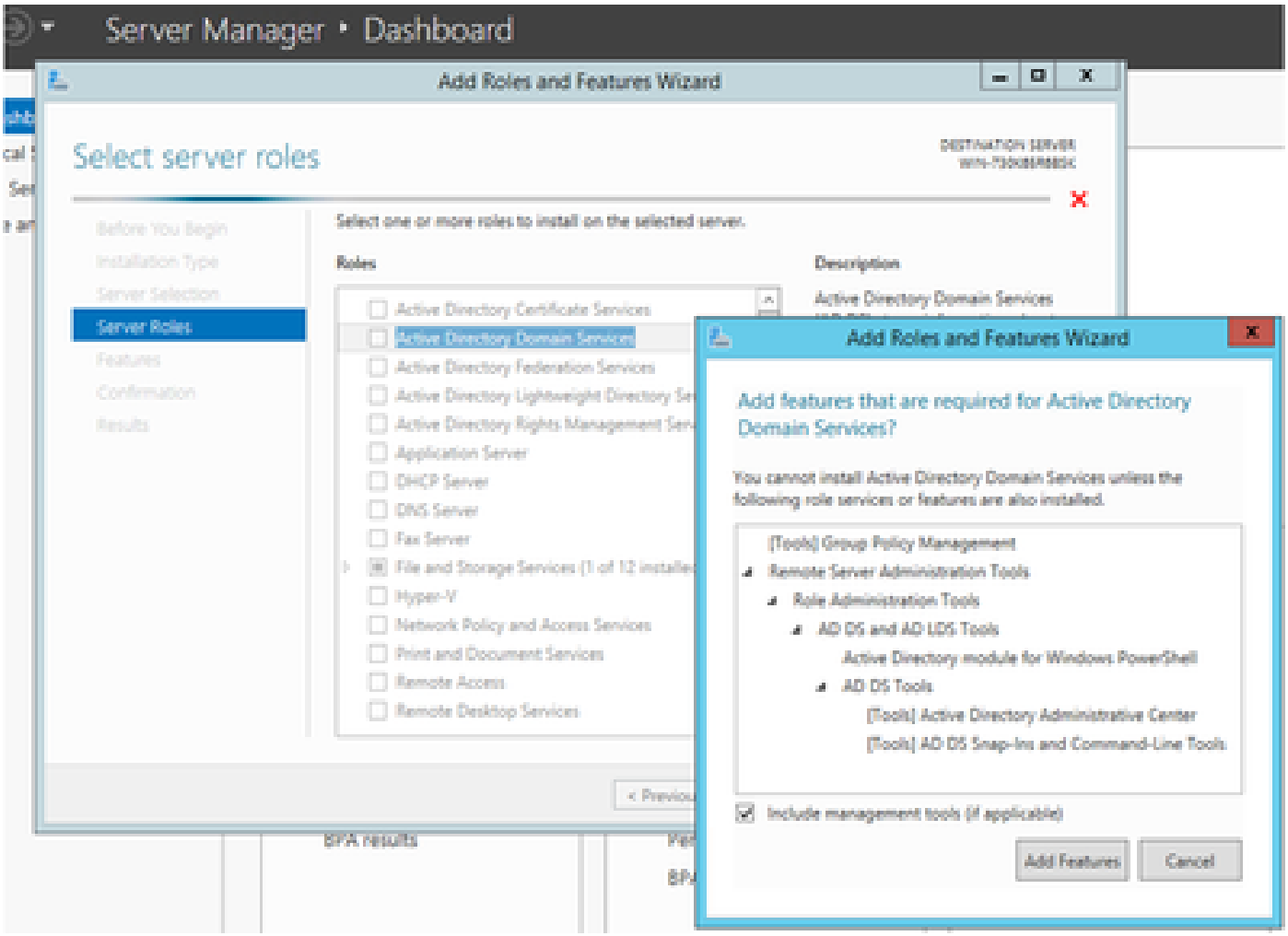
- 変更を適用するためにサーバを再起動します

設定

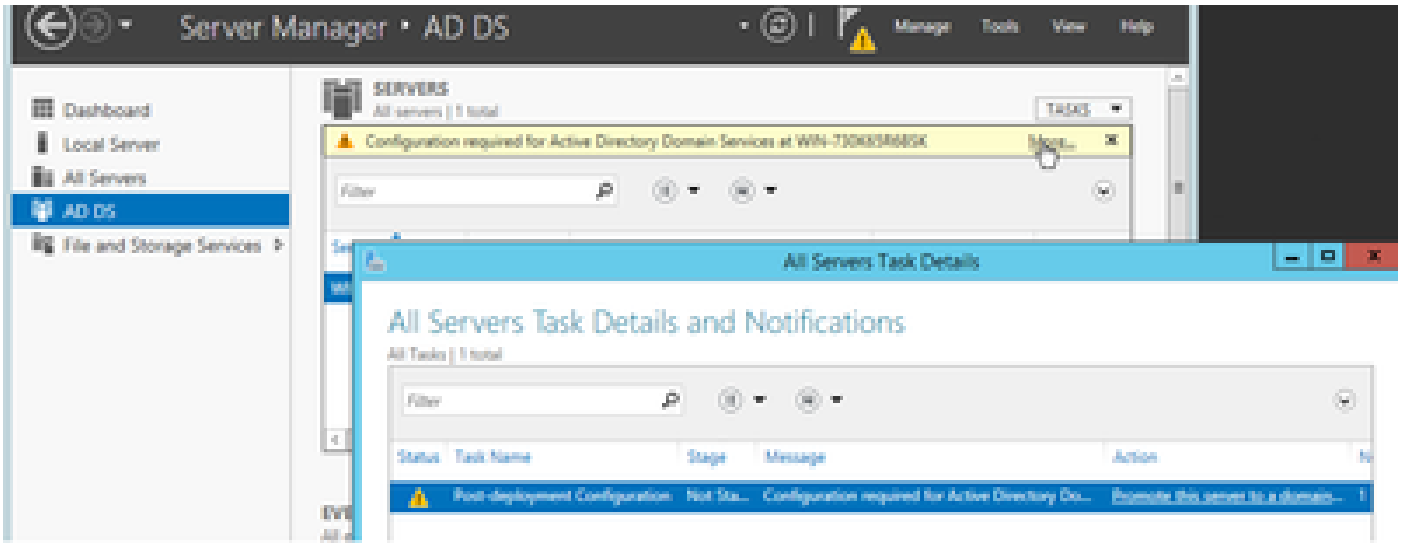
ADサービス、ユーザおよび証明書テンプレート

Active Directoryサービスの有効化と設定

- サーバマネージャで役割と機能の追加オプションを選択し、役割ベースまたは機能ベースのインストールを選択してプールからサーバを選択し（プールには1つのみ必要）、次にActive Directoryドメインサービスを選択します。

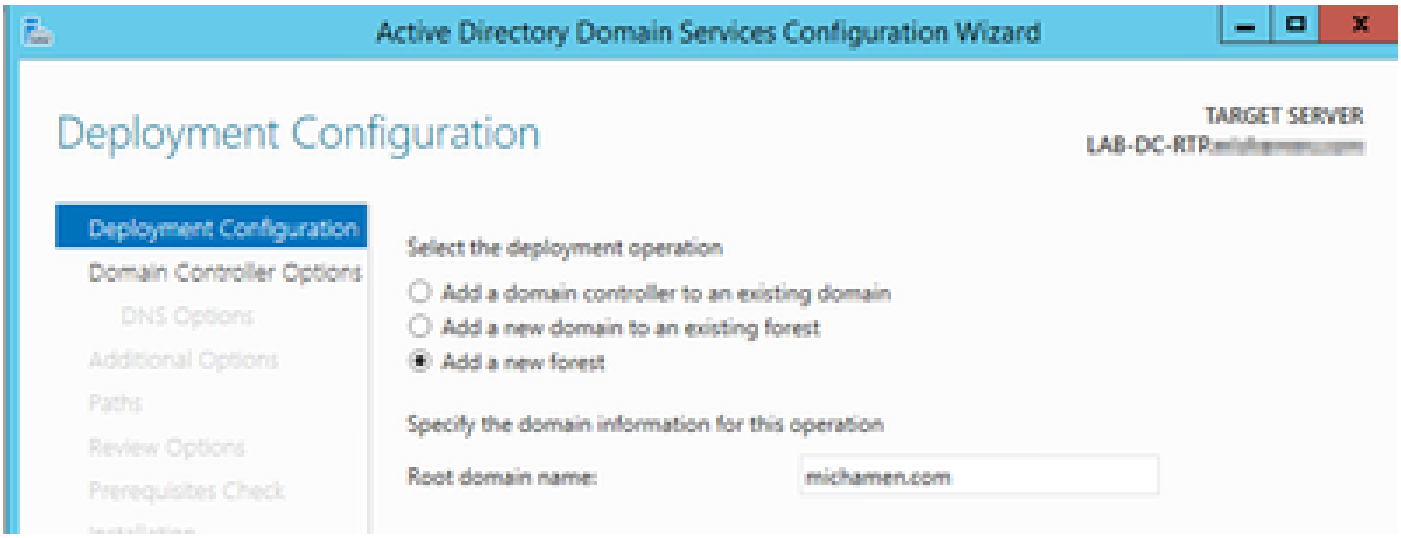


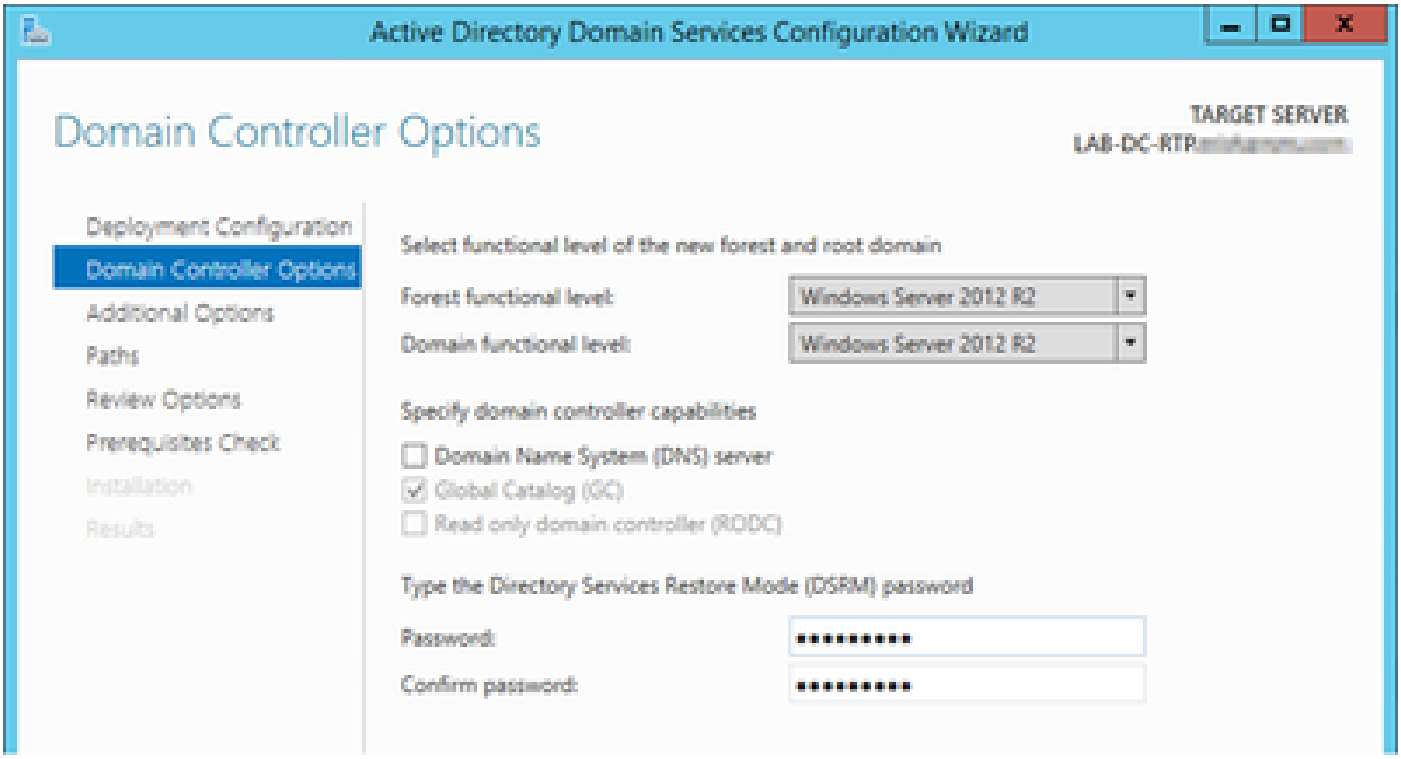
- Nextボタンを選択し、次にInstallを選択します。
- インストールが完了したら、Closeボタンをクリックします
- Server Manager > AD DSの下に、Active Directoryドメインサービスに必要な構成というタイトルの警告タブが表示されます。セットアップウィザードを起動するには、moreリンクを選択し、利用可能なアクションを選択します。



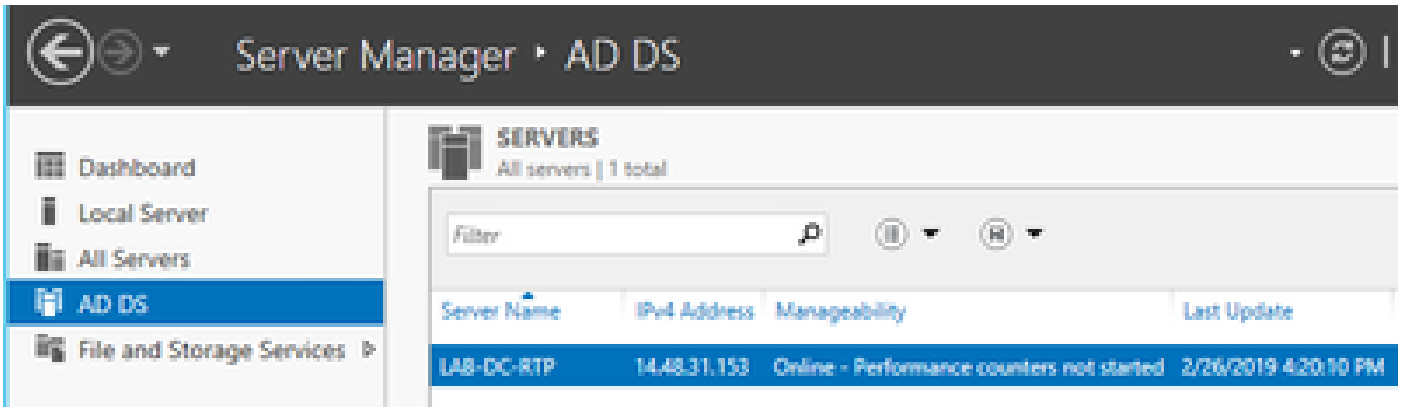
- ドメインセットアップウィザードの指示に従って、目的のルートドメイン名(この実習ではmichamen.comで使用)を持つ新しいフォレストを追加し、使用可能な場合はDNSボックス

のチェックマークを外して、DSRMパスワード(この実習ではC1sc0123!で使用)を定義します。



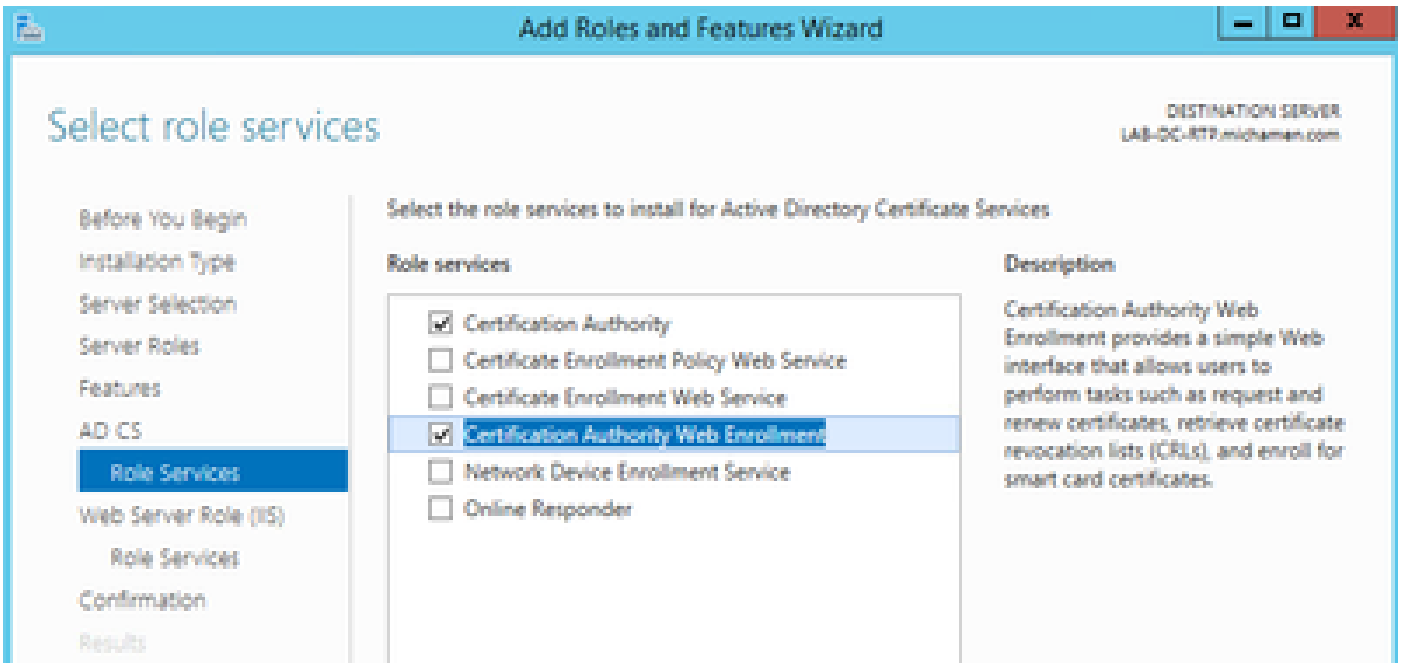


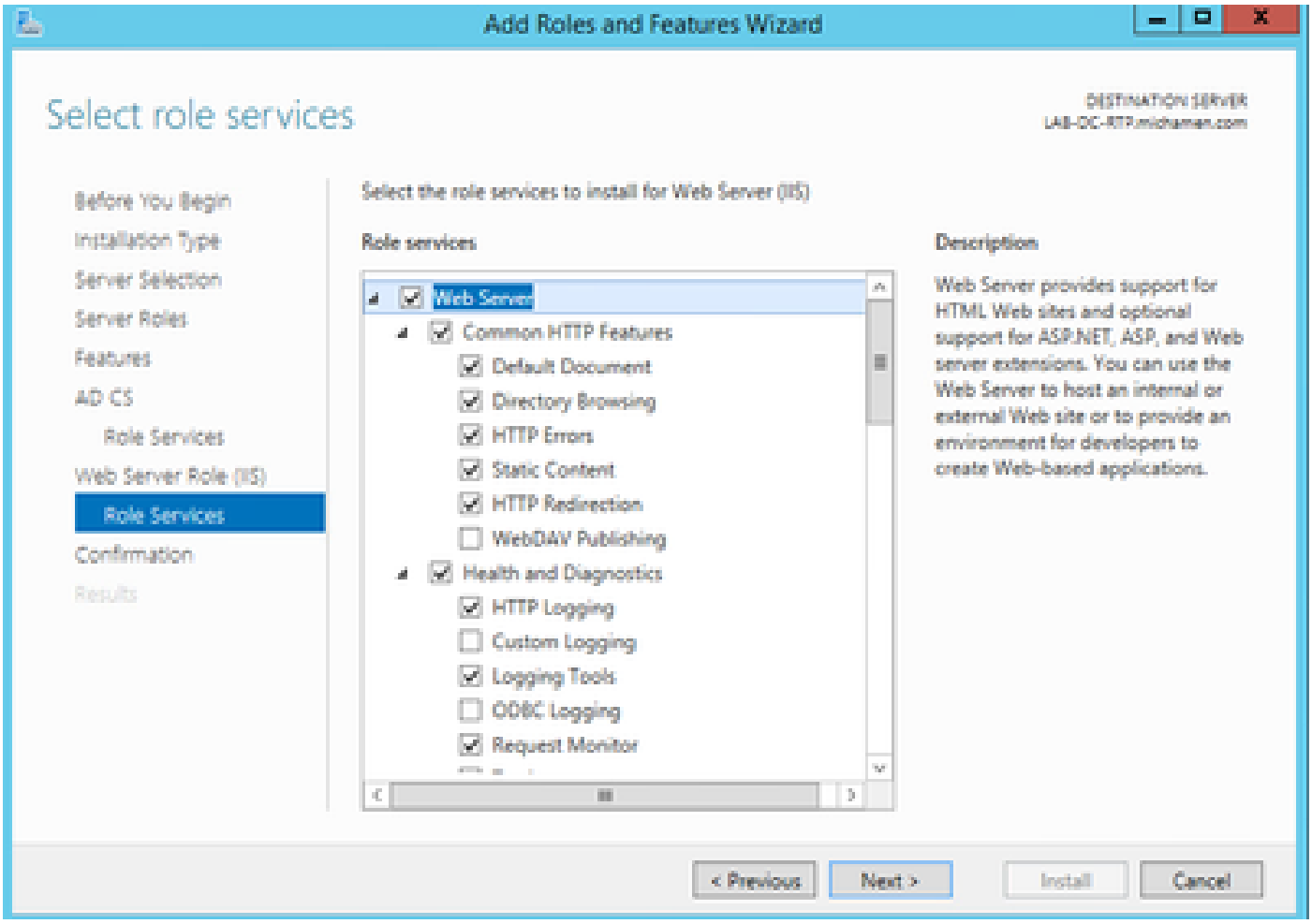
- NetBIOSドメイン名を指定する必要があります（この実習ではMICHAMEN1を使用）。
- ウィザードに従って操作を完了します。その後、サーバがリブートしてインストールが完了します。
- 次に口グインするときに、新しいドメイン名を指定する必要があります。 例：MICHAMEN1\Administrator



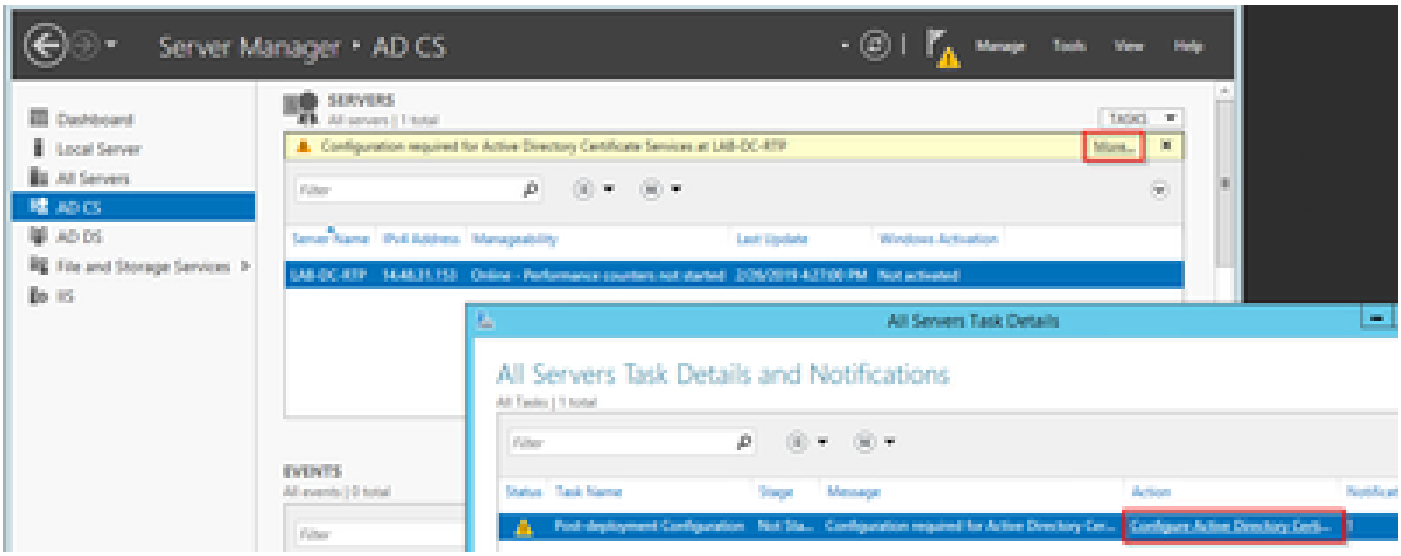
証明書サービスの有効化と設定

- サーバーマネージャーで、[役割と機能の追加]を選択します
- [Active Directory証明書サービス]を選択し、プロンプトに従って必要な機能を追加します（このラボで有効にされた役割サービスから、使用可能なすべての機能が選択されています）
- 役割サービスの場合は、証明機関Web登録を確認してください



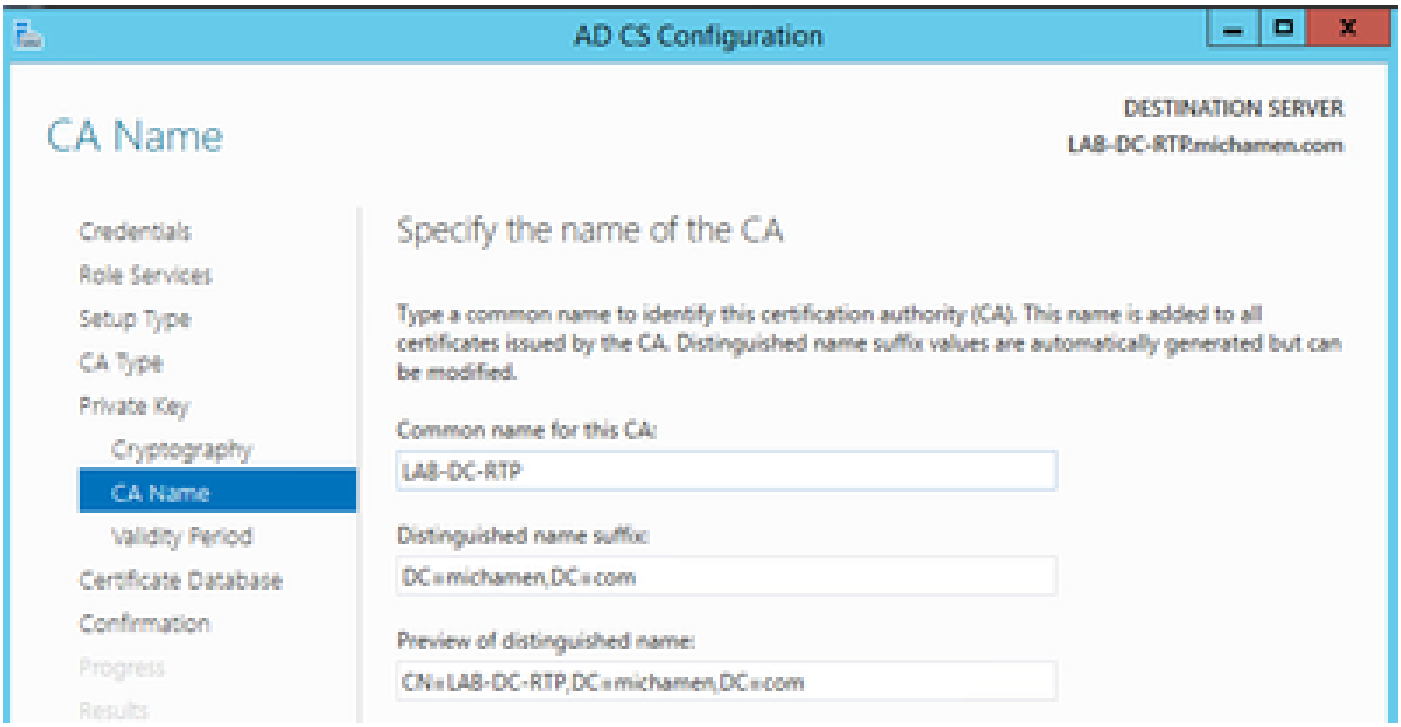


- サーバーマネージャー>AD DSの下に、[Active Directory証明書サービスに必要な構成]というタイトルの警告タブが表示されている必要があります。詳細リンクを選択し、利用可能なアクションを選択してください。



- AD-CS Post Install Configurationウィザードで、次の手順に従います。
- 証明機関と証明機関Web登録ロールを選択します
- 次のオプションでエンタープライズCAを選択します。
- ルートCA
- 新しい秘密キーを作成する

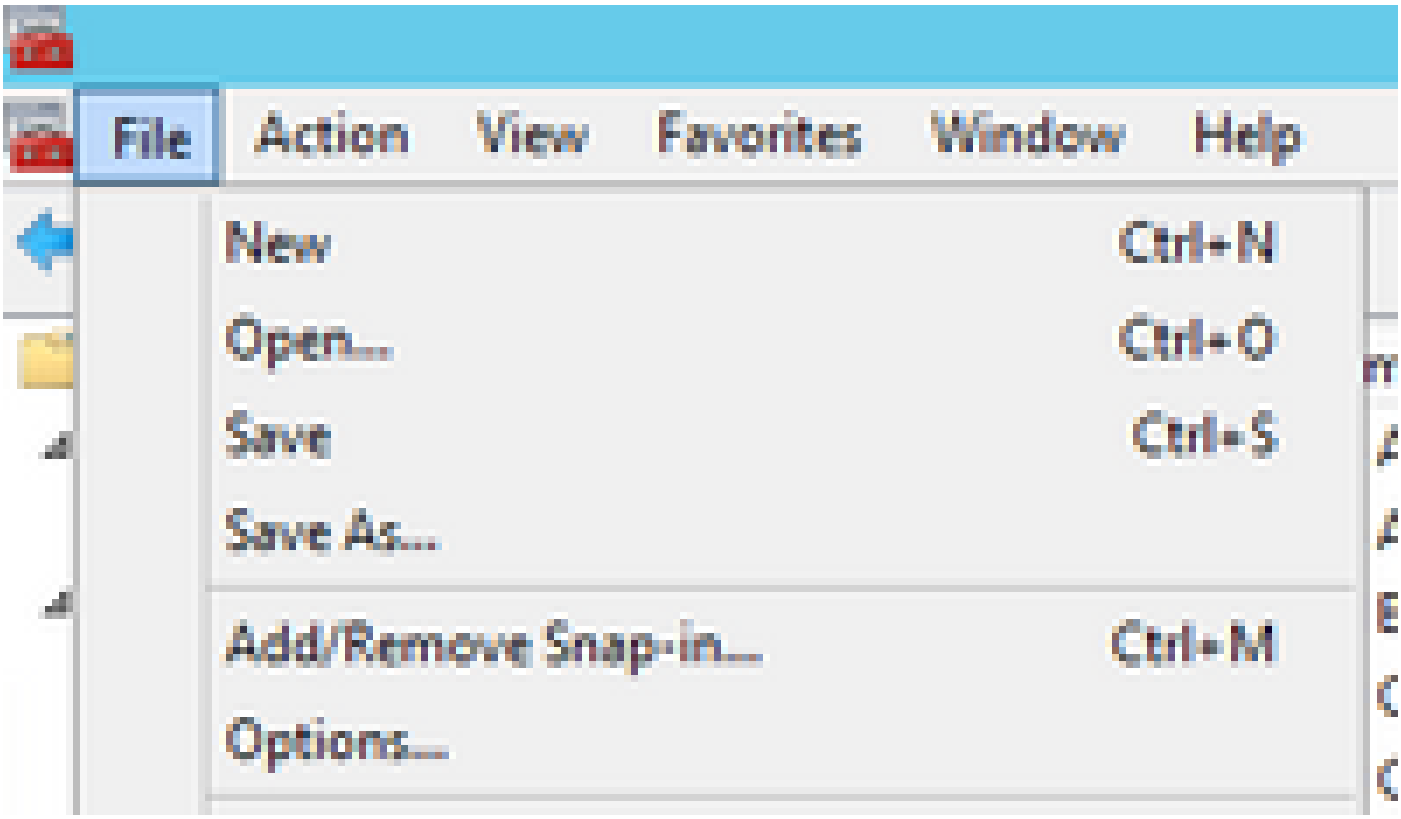
- 秘密キーを使用する – SHA1（既定の設定）
- CAの共通名を設定します（サーバのホスト名と一致する必要があります）。

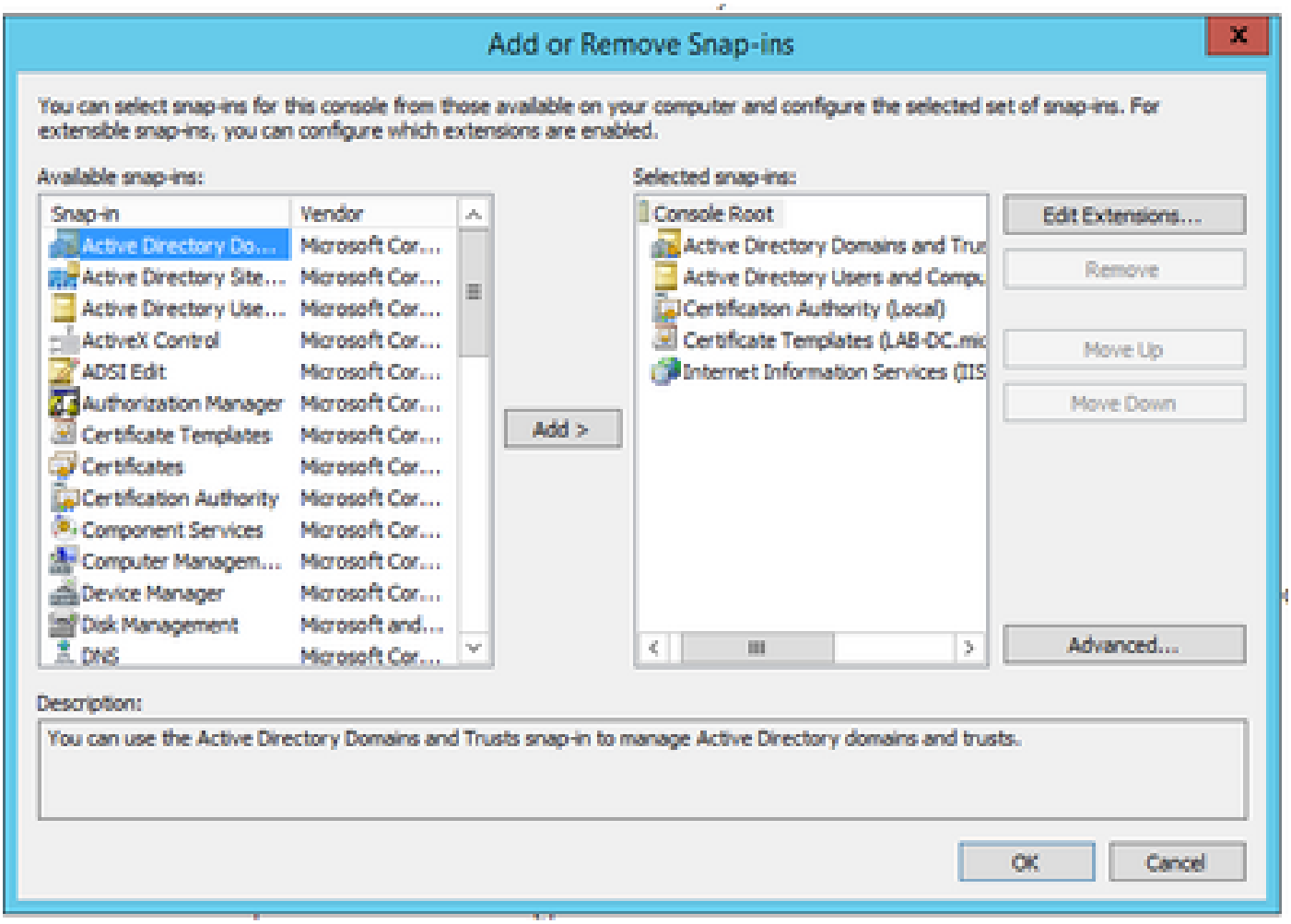


- 有効期間を5年間（必要に応じて以上）に設定する
- ウィザードの残りの部分でNextボタンを選択します

CiscoRA用の証明書テンプレートの作成

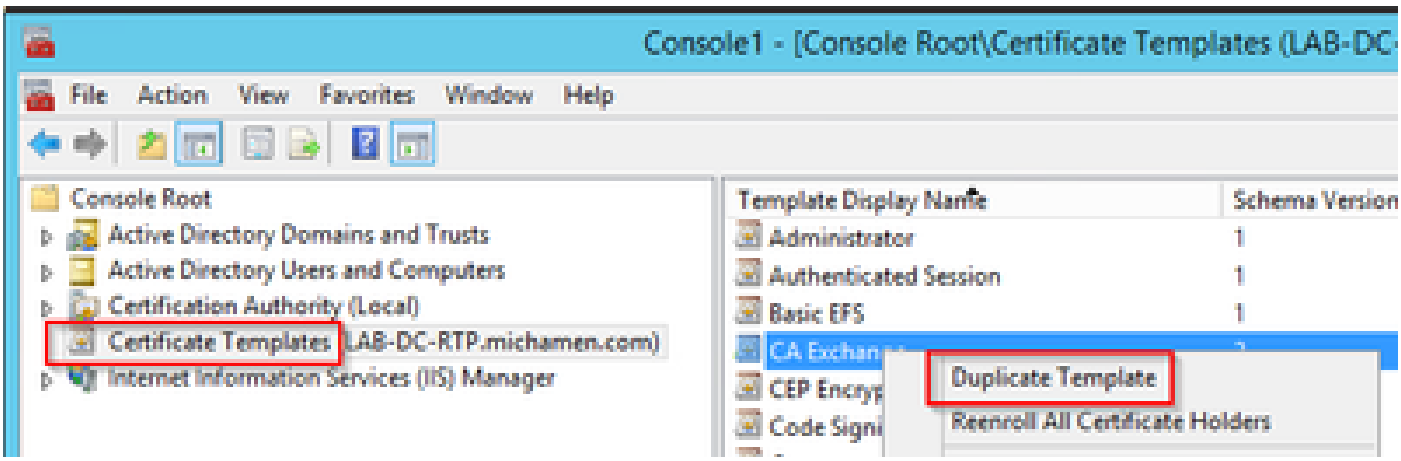
- MMCを開きます。Windowsのスタートロゴを選択し、Runからmmcと入力します
- MMCウィンドウを開き、フォロースナップイン（設定の別の場所で使用）を追加して、OKを選択します。



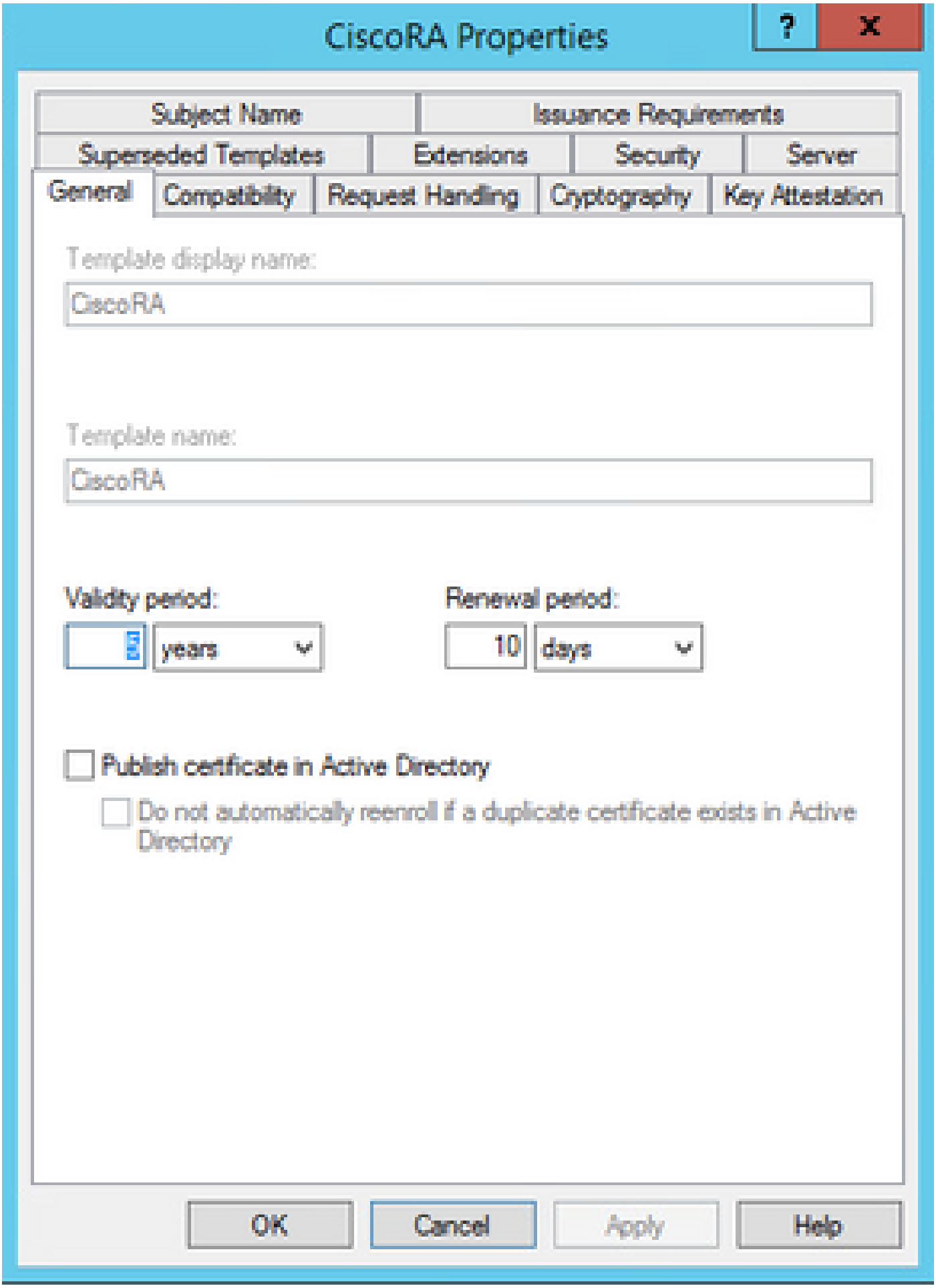


- File > Saveの順に選択し、このコンソールセッションをデスクトップに保存して、簡単に再アクセスできるようにします

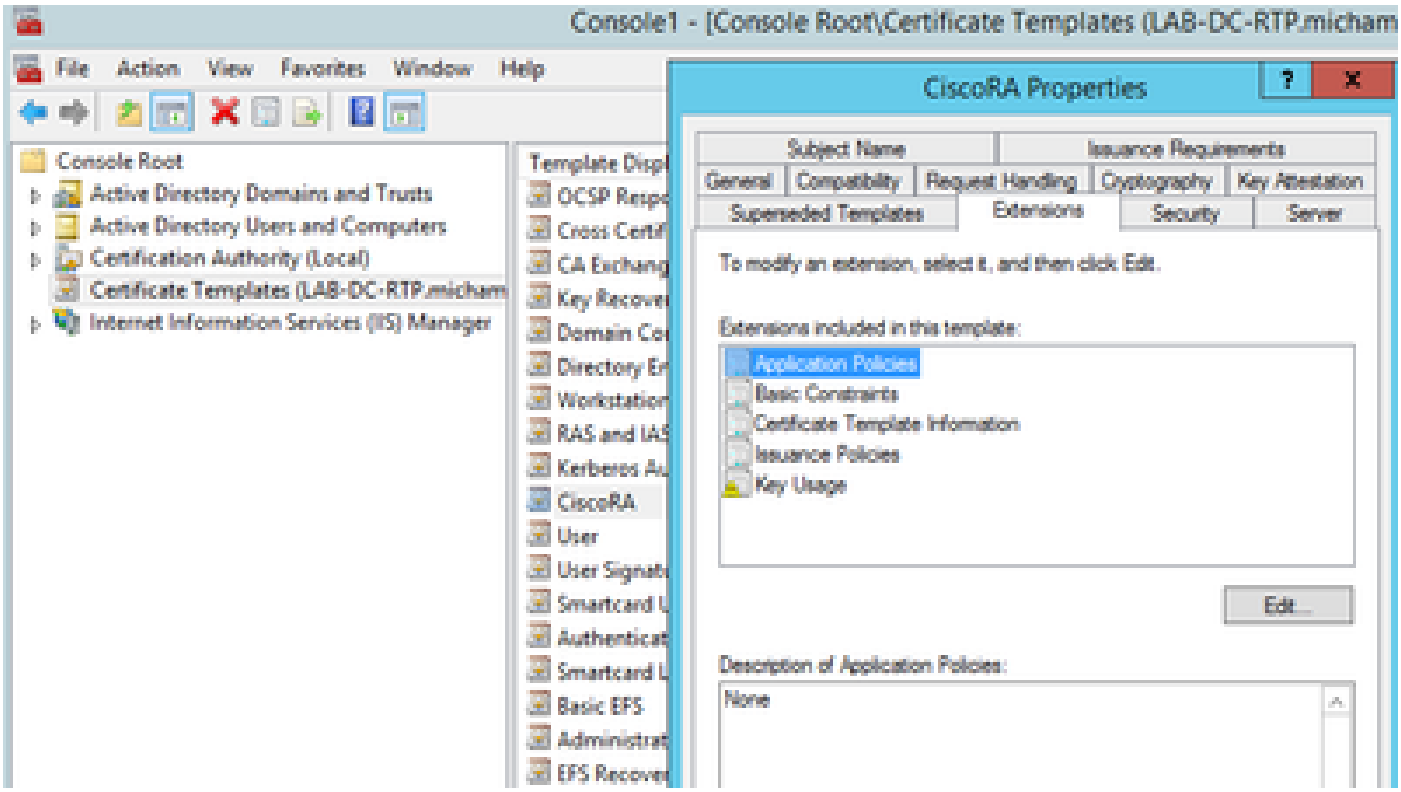
- スナップインから、[Certificate Templates]を選択します
- テンプレート(可能であれば「ルート認証局」テンプレート)を作成または複製し、CiscoRAという名前を付けます



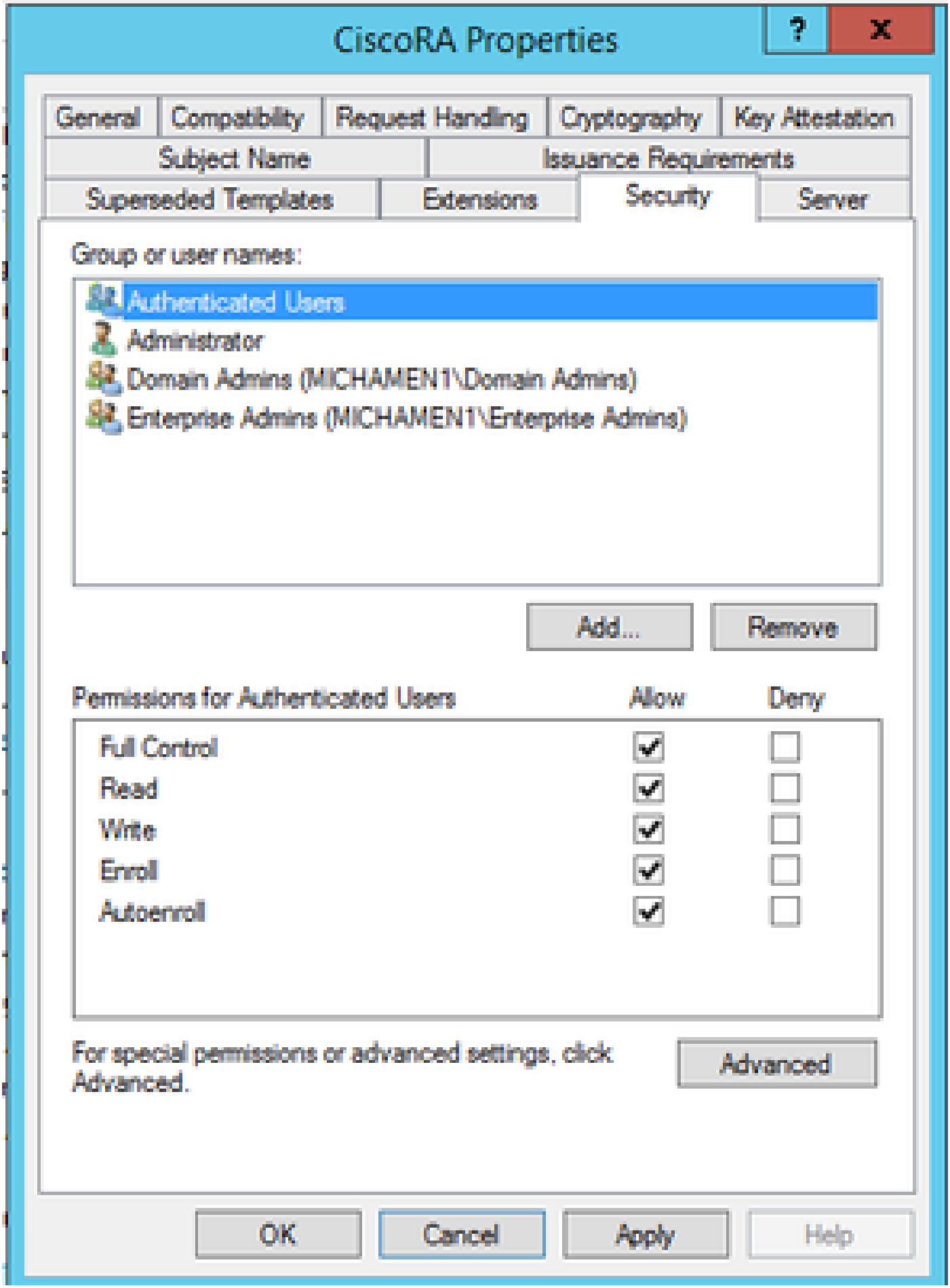
- テンプレートを変更します。その上で右クリックして、Propertiesを選択します
- Generalタブを選択し、有効期間を20年（または必要に応じて他の値）に設定します。このタブで、テンプレートの「表示名」と「名前」の値が一致していることを確認します


CiscoRA Properties
Subject Name
Issuance Requirements
Superseded Templates
Extensions
Security
Server
General
Compatibility
Request Handling
Cryptography
Key Attestation
Template display name:
CiscoRA
Template name:
CiscoRA
Validity period:
years
Renewal period:
10
days
Publish certificate in Active Directory
Do not automatically reenroll if a duplicate certificate exists in Active Directory
OK
Cancel
Apply
Help

- Extensionsタブを選択し、Application Policiesを強調表示してから、Editを選択します

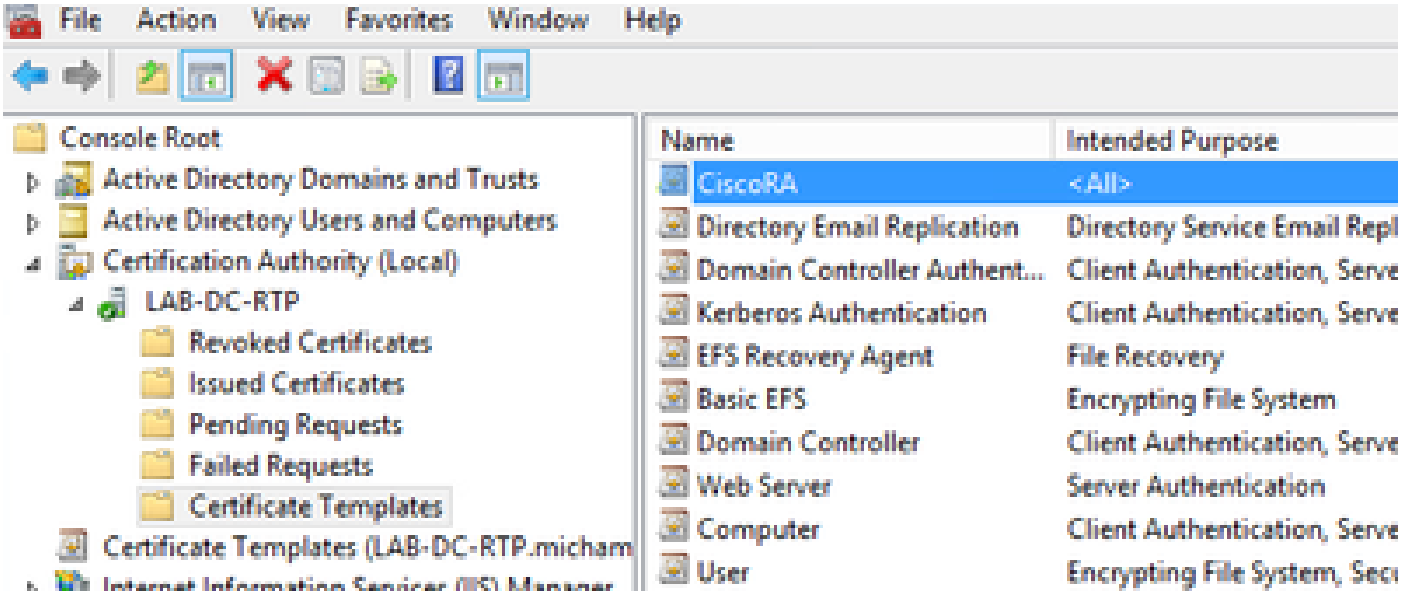


- 表示されるウィンドウに表示されているポリシーをすべて削除します
- Subject Nameタブを選択し、Supply in Requestオプションボタンを選択します
- Securityタブを選択し、表示されているすべてのグループ/ユーザ名に対してすべての権限を付与します



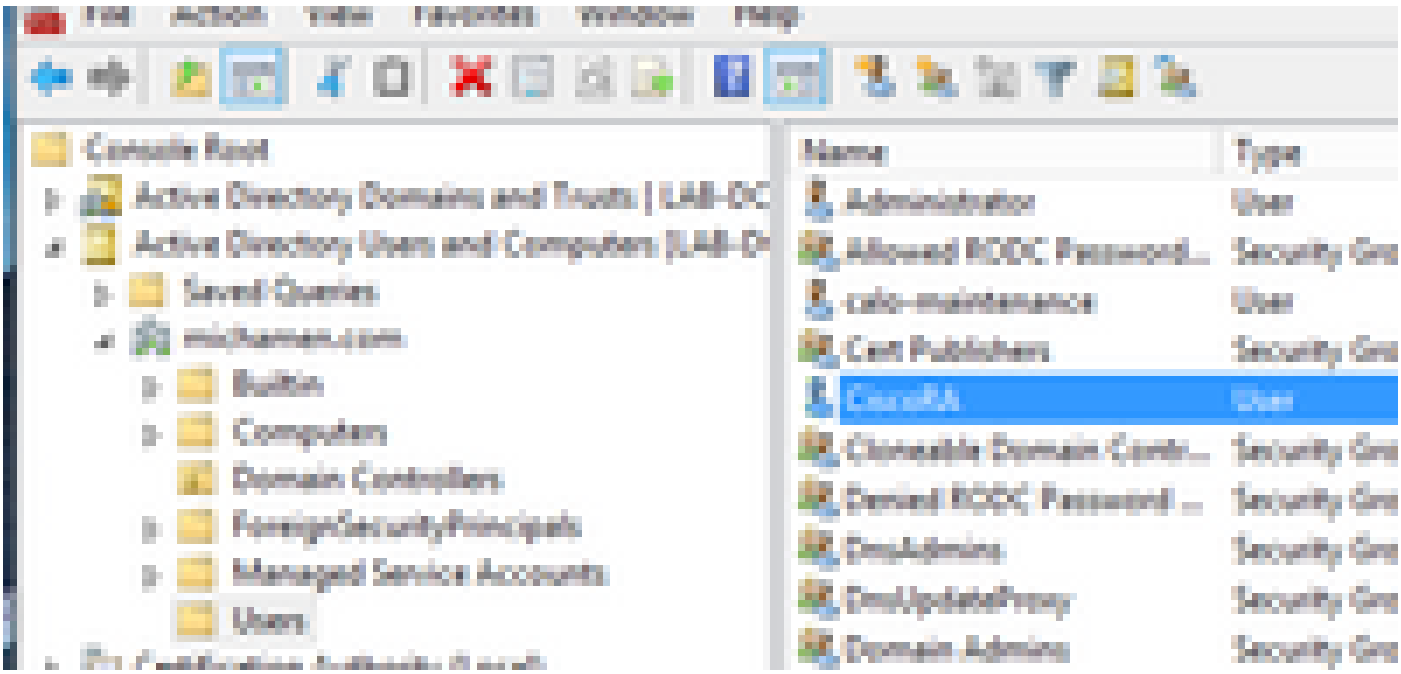
証明書テンプレートを発行に使用できるようにする

- MMCスナップインでCertification Authorityを選択し、フォルダツリーを展開してCertificate Templatesフォルダを見つけます
- 名前と使用目的を含むフレームの空白を右クリックします
- 発行するNewおよびCertificate Templateを選択します
- 新しく作成および編集したCiscoRAテンプレートを選択します



Active Directory CiscoRAアカウントの作成

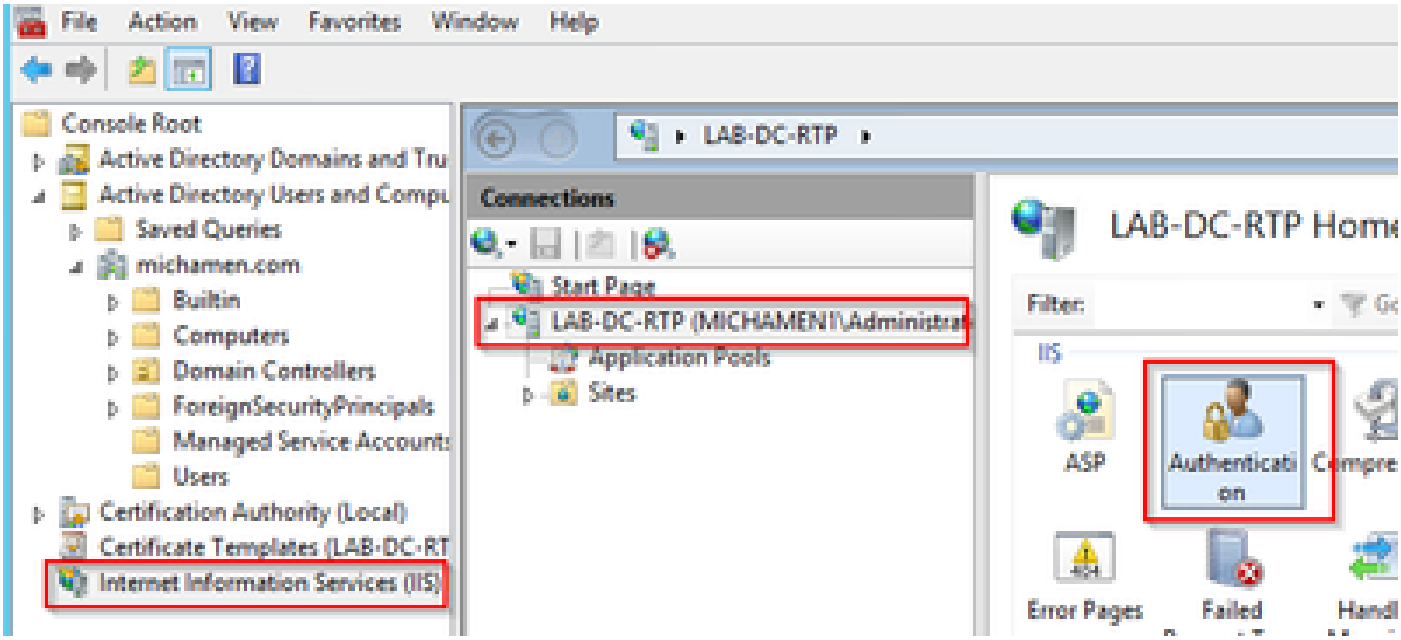
- MMCスナップインに移動し、Active Directory Users and Computersを選択します。
- 左端のペインのツリーでUsersフォルダを選択します
- 名前、タイプ、説明を含むフレームの空白スペースを右クリックします
- NewとUserを選択します。
- ユーザ名とパスワードを使用してCiscoRAアカウントを作成し(この実習ではciscora/Cisco123を使用)、画面にパスワードが表示されたら[Password never expires]チェックボックスをオンにします



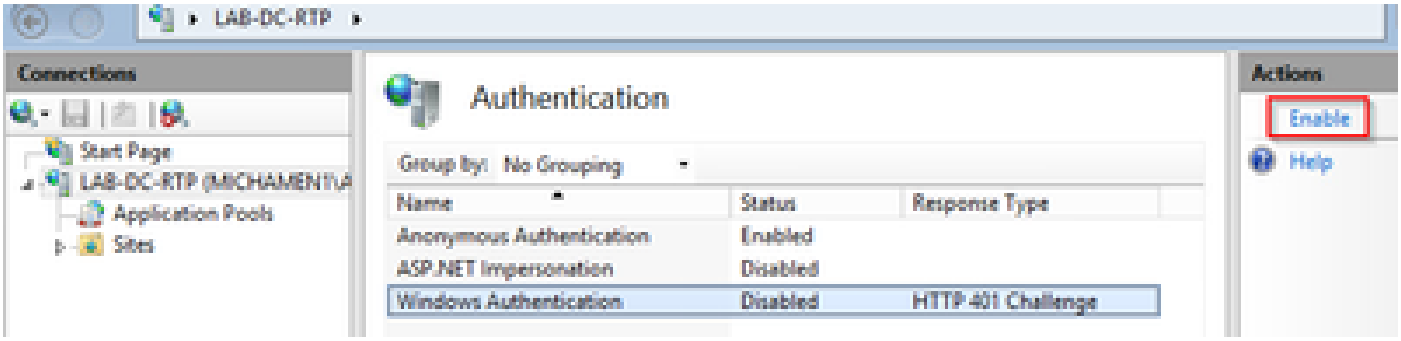
IIS 認証とSSLバインディングの設定

[Enable] NTLM [Authentication]

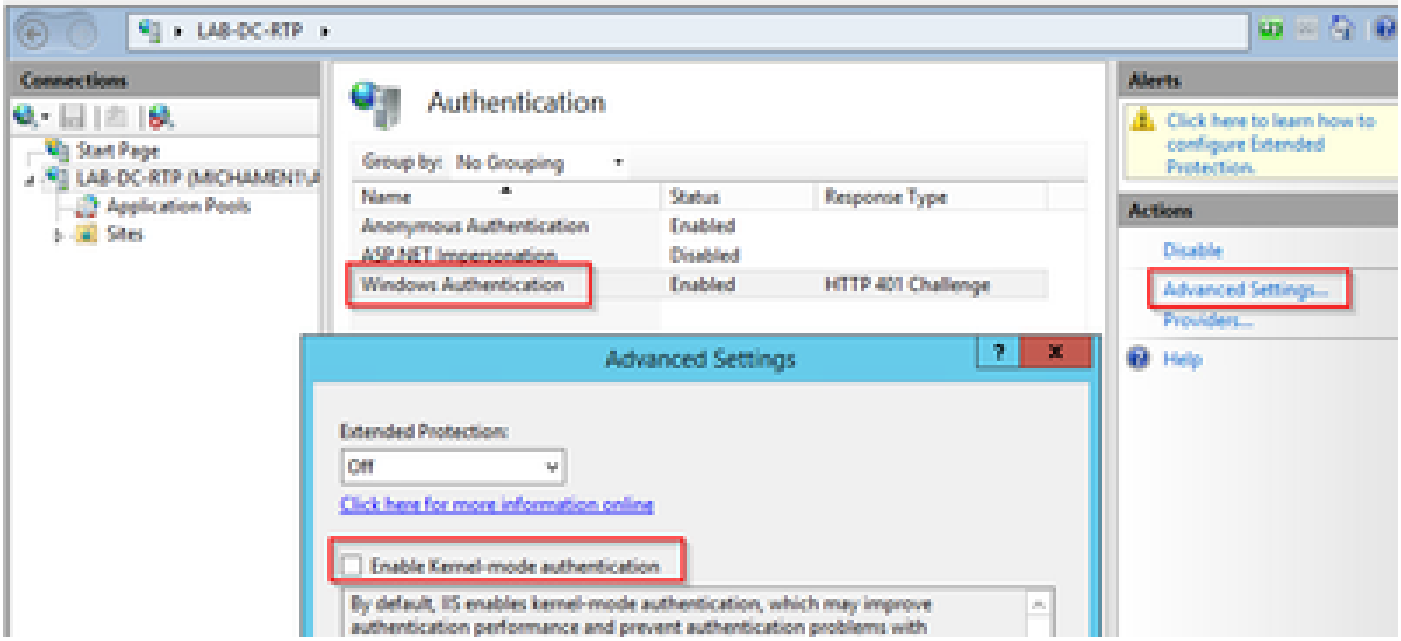
- MMCスナップインに移動し、インターネットインフォメーションサービス(IIS)マネージャスナップインでサーバー名を選択します
- 次のフレームに機能リストが表示されます。Authentication機能アイコンをダブルクリックします



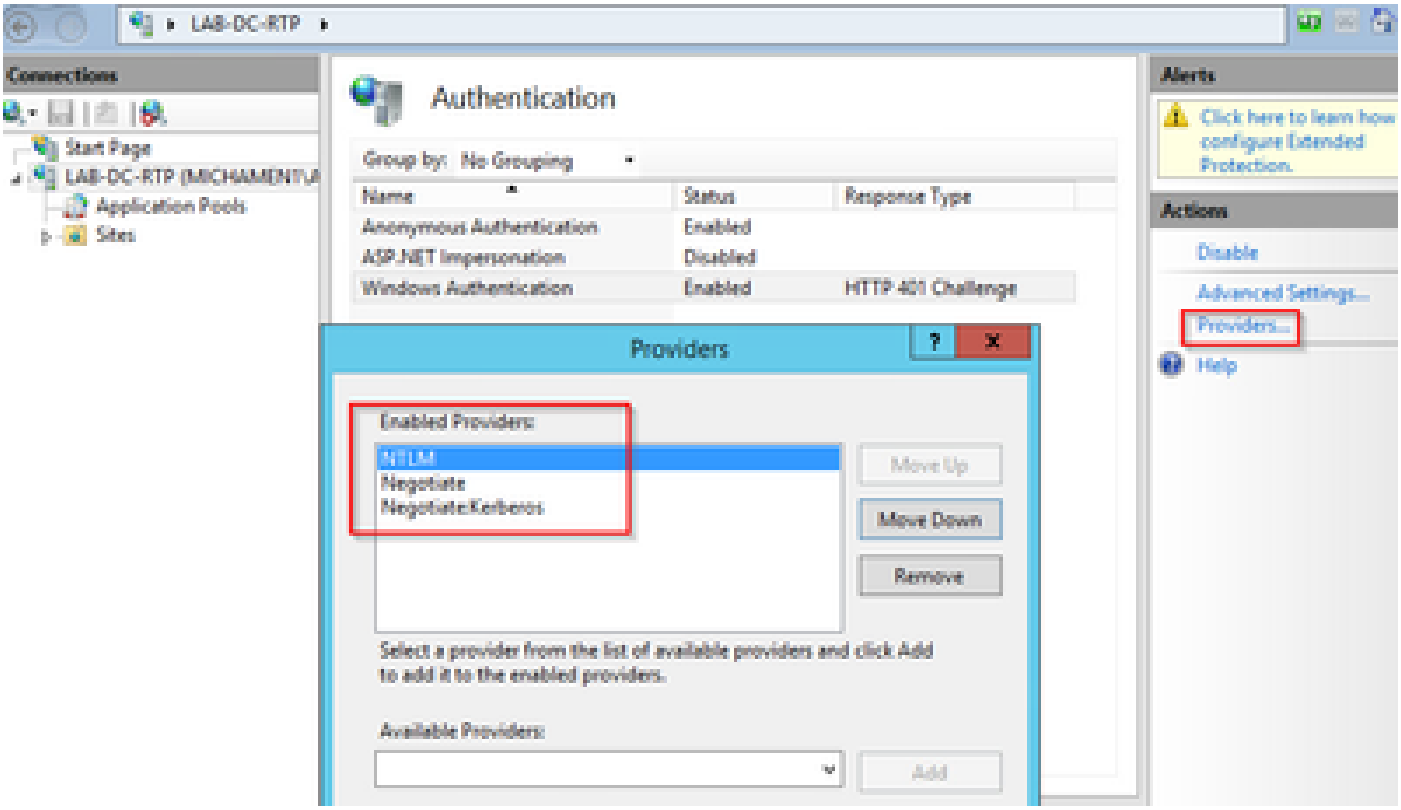
- Windows Authenticationを強調表示して、Actionsフレーム（右ペイン）からEnableオプションを選択します



- 操作ペインにAdvanced Settingsオプションが表示されます。これを選択してEnable Kernel-mode authenticationのチェックマークを外します。



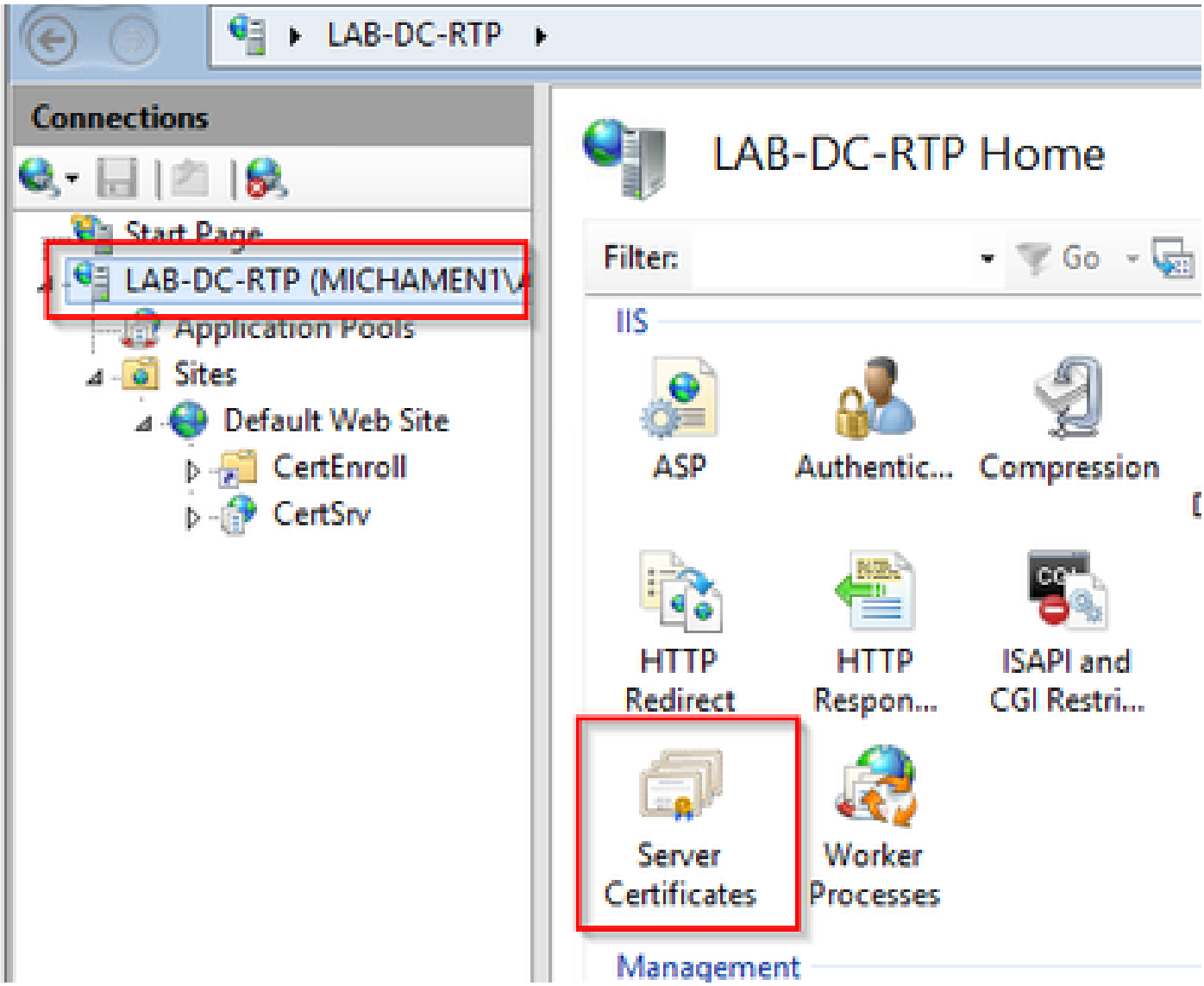
- Providersを選択し、NTMLを順に配置してからNegotiateを選択します。



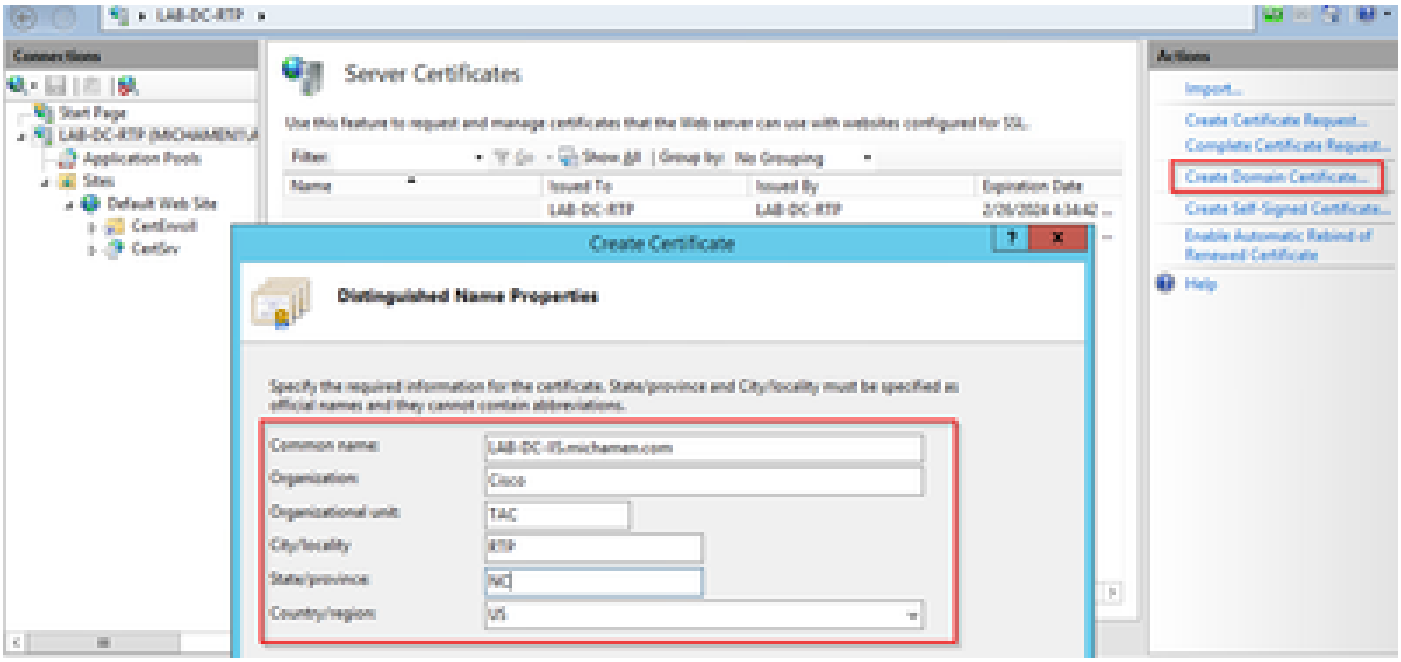
WebサーバのID証明書の生成

Webサーバの証明書が自己署名の場合、CiscoRAは接続できないため、まだケースが存在しない場合は、CAによって署名されたWebサービスのID証明書の証明書を生成する必要があります。

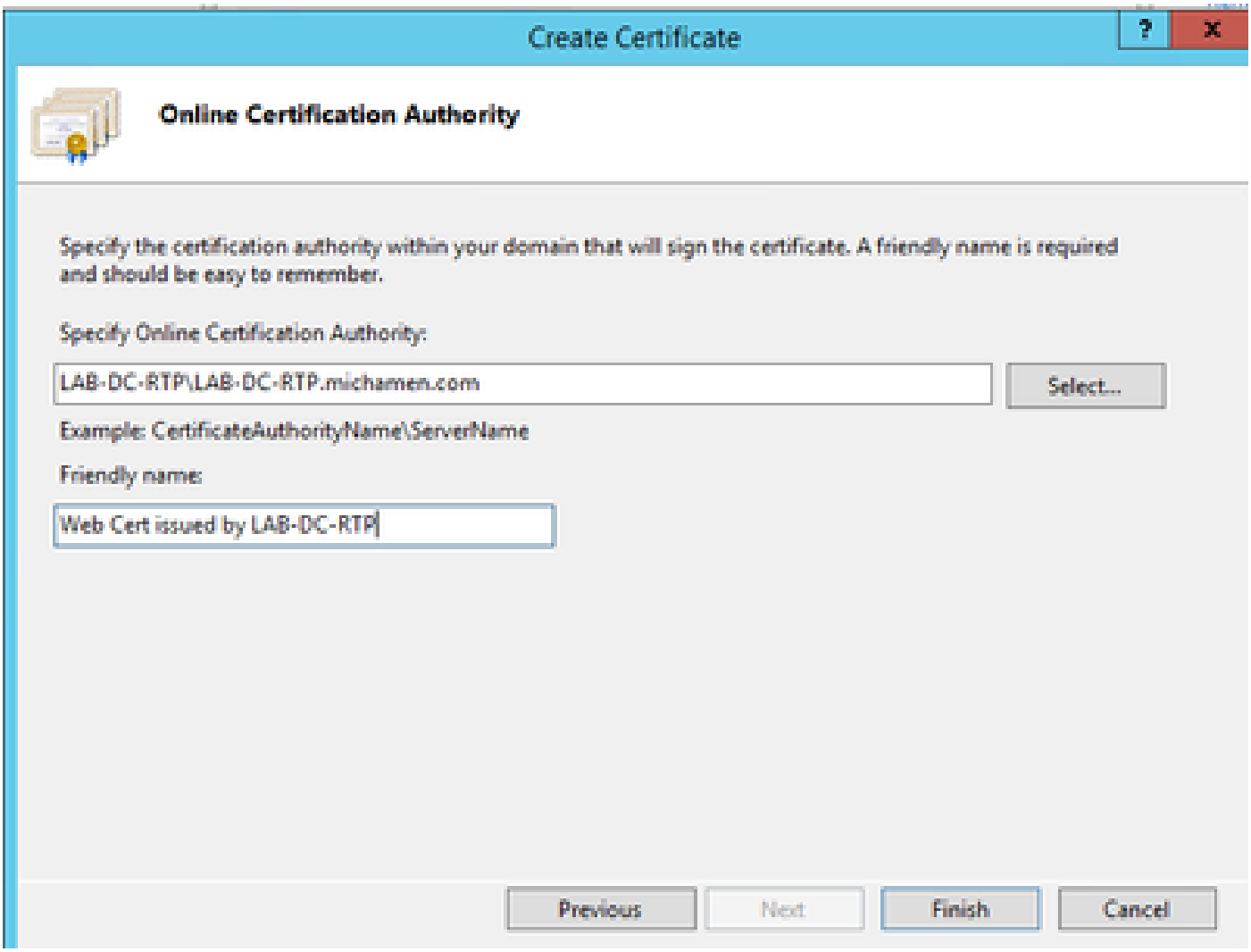
- IISスナップインからWebサーバを選択し、Server Certificates機能アイコンをダブルクリックします。



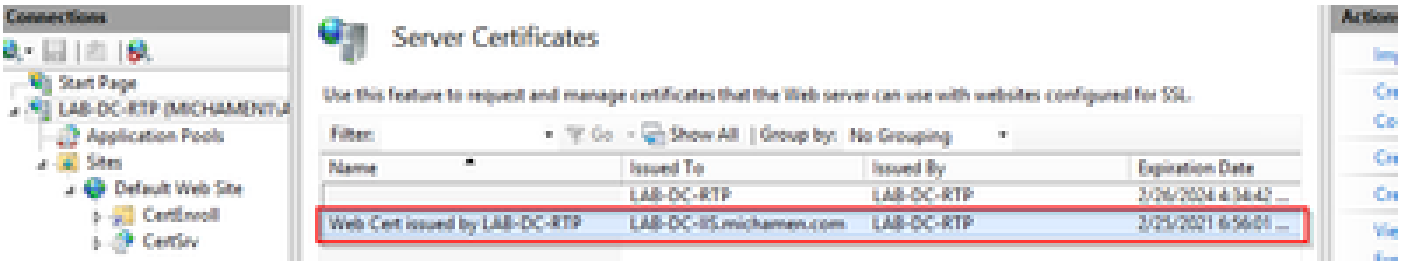
- デフォルトでは、1つの証明書（自己署名ルートCA証明書）が表示されます。この証明書は、「アクション」メニューから「ドメイン証明書の作成」オプションを選択します。新しい証明書を作成するために、設定ウィザードで値を入力します。共通名が解決可能なFQDN（完全修飾ドメイン名）であることを確認し、Nextを選択します。



- 発行者にするルートCAの証明書を選択し、Finishを選択します。

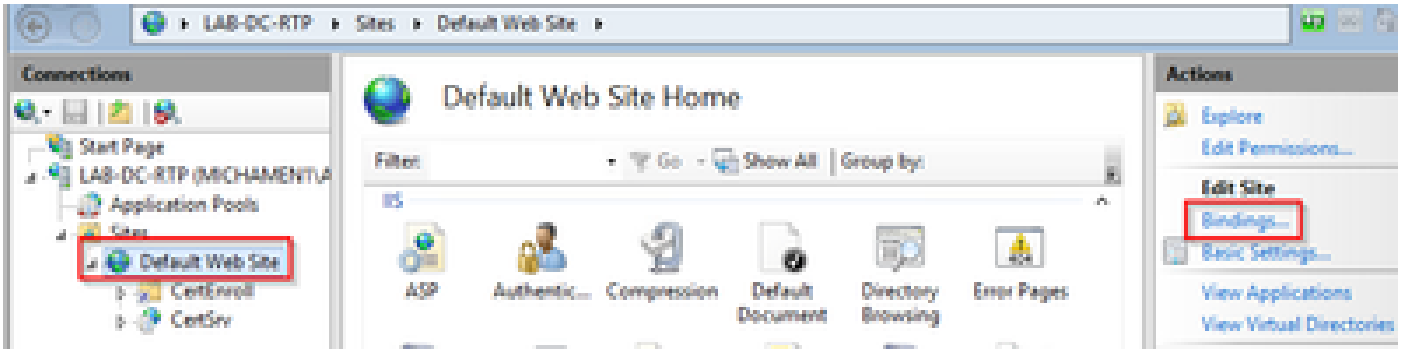


- CA証明書とWebサーバのID証明書の両方が表示されます。

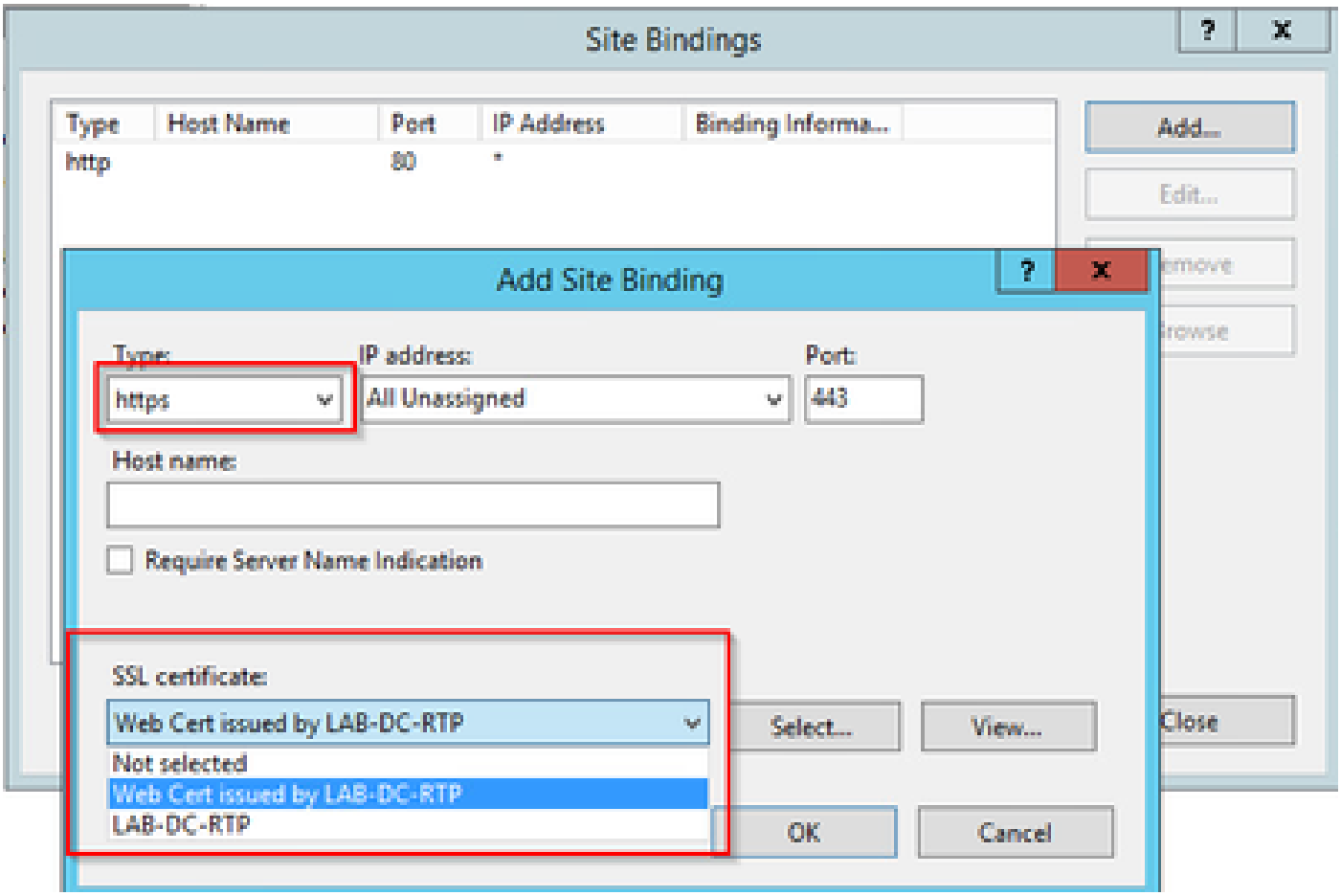


WebサーバのSSLバインディング

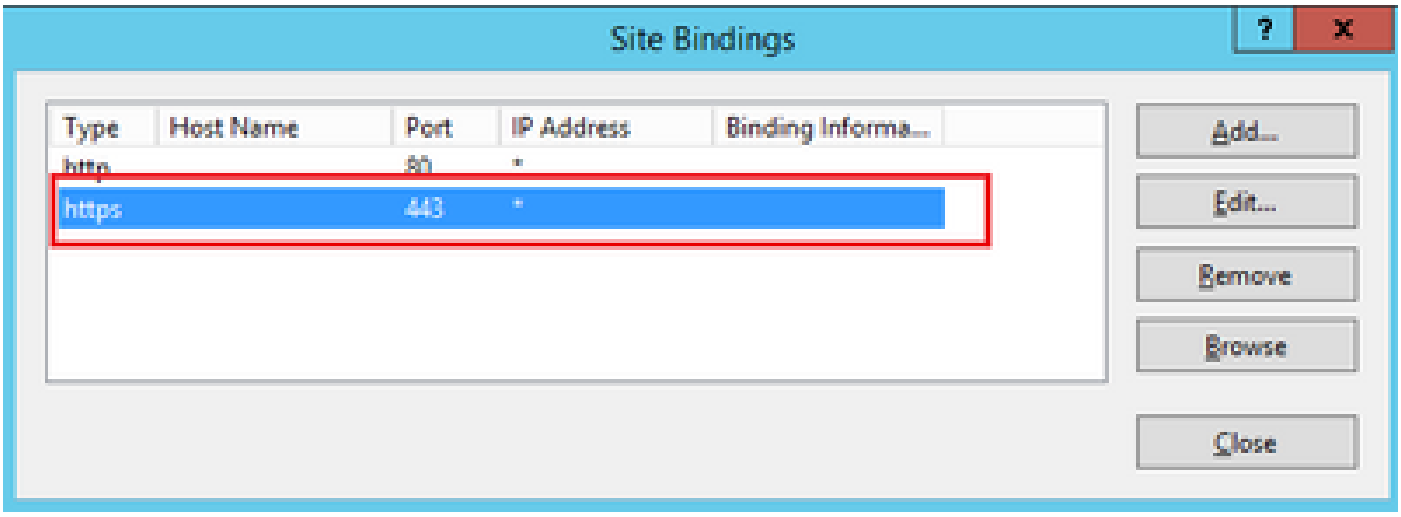
- ツリービューでサイトを選択し（デフォルトのWebサイトを使用するか、特定のサイトにより細かく設定できます）、操作ペインからBindingsを選択します。表示されるバインディング工ディタを使用して、Webサイトのバインディングを作成、編集、および削除できます。Addを選択して、新しいSSLバインディングをサイトに追加します。

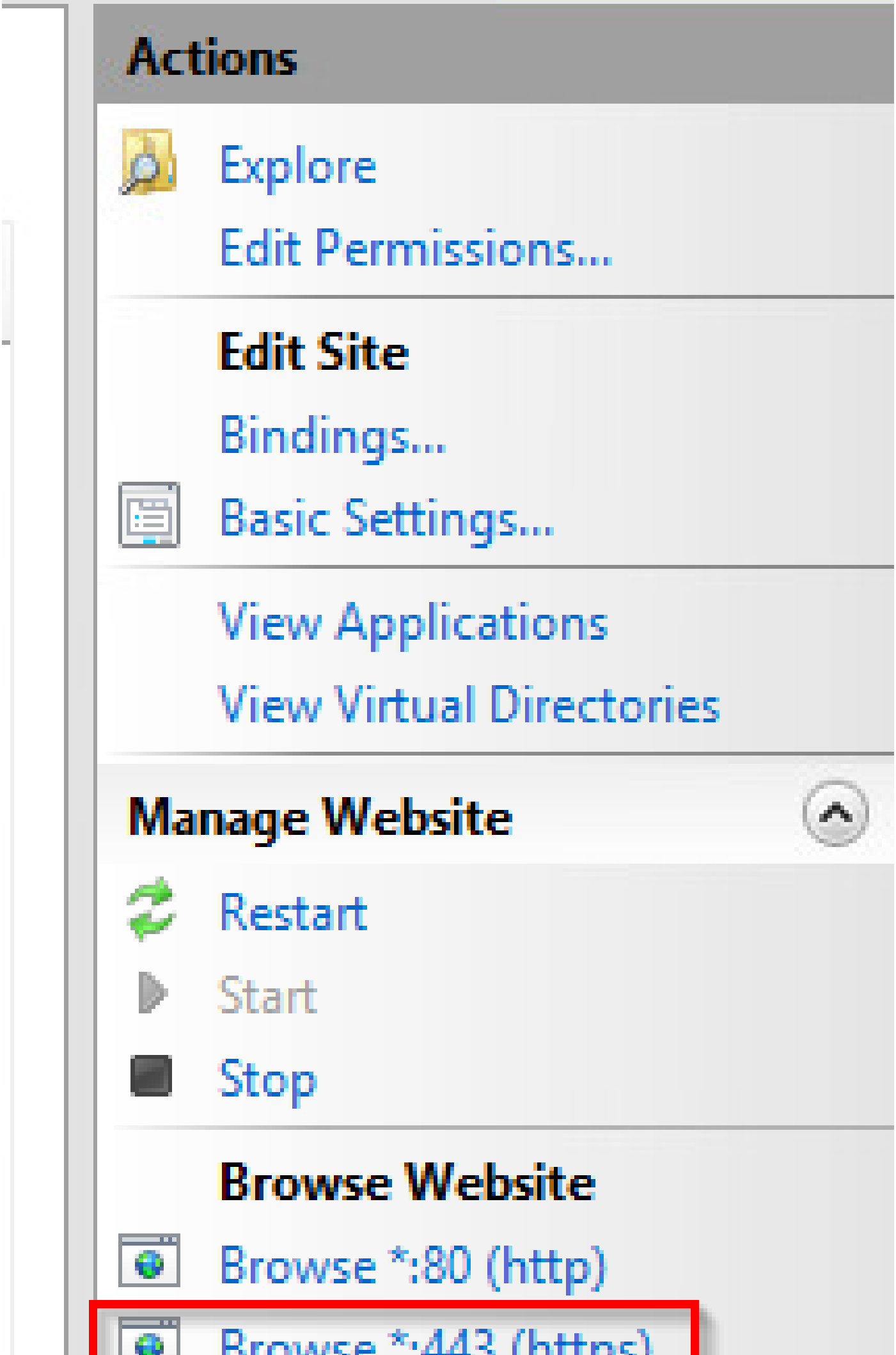


- 新しいバインディングのデフォルト設定は、ポート80でHTTPに設定されています。Typeドロップダウンリストからhttpsを選択します。SSL Certificateドロップダウンリストから、前のセクションで作成した自己署名証明書を選択し、OKを選択します。



- これでサイトに新しいSSLバインディングが作成されました。残りの処理は、メニューからBrowse *:443 (https)オプションを選択してSSLバインディングが機能することを確認し、デフォルトのIIS WebページでHTTPSが使用されていることを確認するだけです。




Actions
Explore
Edit Permissions...
Edit Site
Bindings...
Basic Settings...
View Applications
View Virtual Directories
Manage Website
Restart
Start
Stop
Browse Website
Browse *:80 (http)
Browse *:443 (https)

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。