Configurez l'ouverture de session simple utilisant CUCM et AD FS 2.0 (Windows Server 2008 R2)

Contenu

Introduction

Ce document décrit comment configurer l'ouverture de session simple utilisant Cisco Unified Communications gèrent (CUCM) et des services de fédération de Répertoire actif (AD FS) 2.0 (Windows Server 2008 R2).

Contribué par Scott Kiewert, ingénieur TAC Cisco.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Gestionnaire de Cisco Unified Communications
- La connaissance de Basick d'ADFS 2.0

Afin d'activer SSO dans votre environnement de travaux pratiques, vous avez besoin de cette configuration

- Windows Server avec l'AD FS 2.0 installé
- CUCM avec le sync de LDAP configuré.
- **Un utilisateur final** avec le rôle de **superutilisateurs CCM standard** sélectionné.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Windows Server avec l'AD FS 2.0
- CUCM

Les informations internes de Cisco

Téléchargez et installez l'AD FS 2.0 sur vos Windows Server

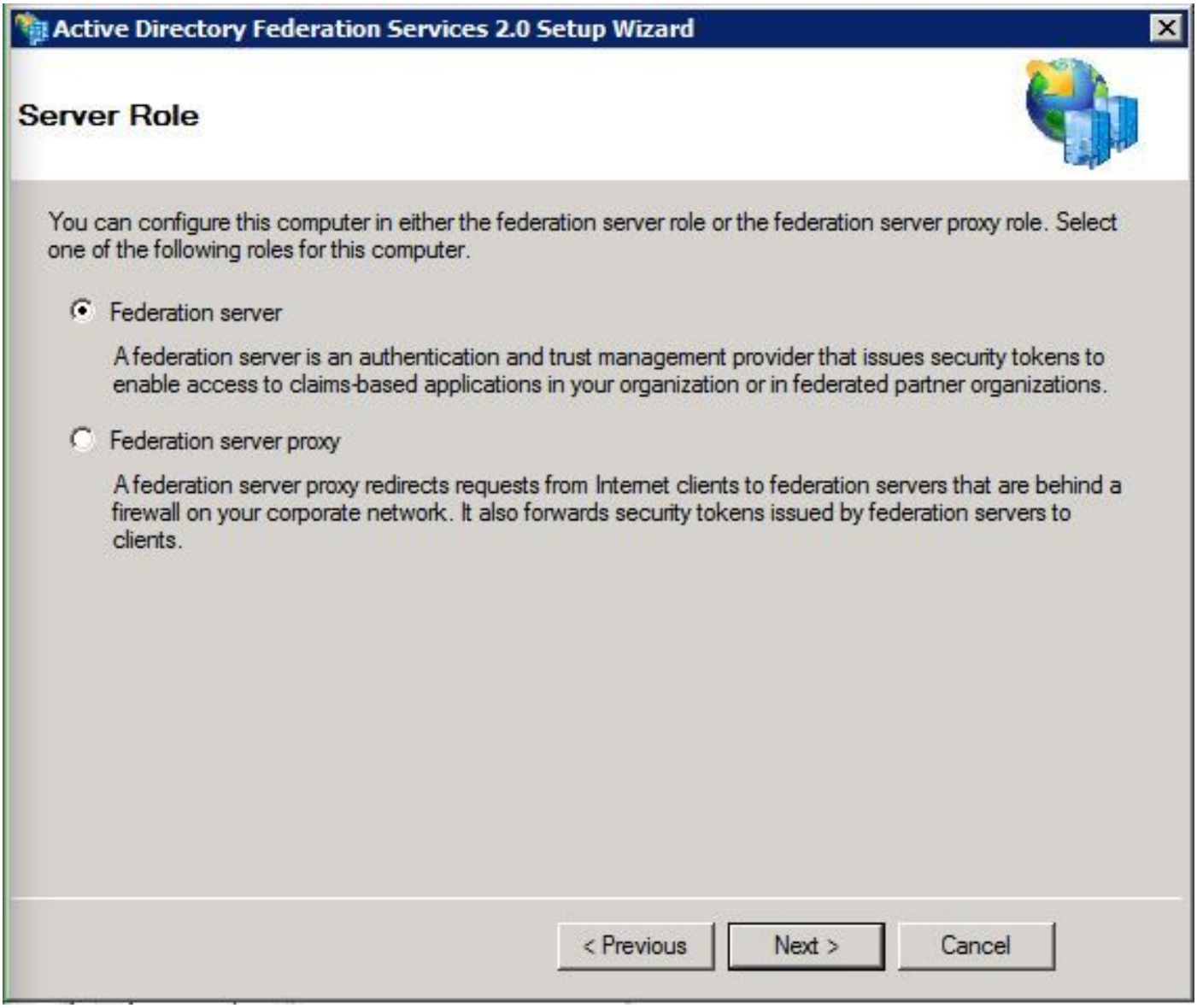
Étape 1. Naviguez vers https://www.microsoft.com/en-us/download/details.aspx?id=10909 et le clic continuent.

Étape 2. Dans la fenêtre contextuelle, veillez-vous pour sélectionner le téléchargement approprié basé sur vos Windows Server.

Étape 3. Déplacez le fichier téléchargé à vos Windows Server.

Étape 4. Procédez à l'installation :

Étape 5. Une fois incité, **serveur** choisi de **fédération** :



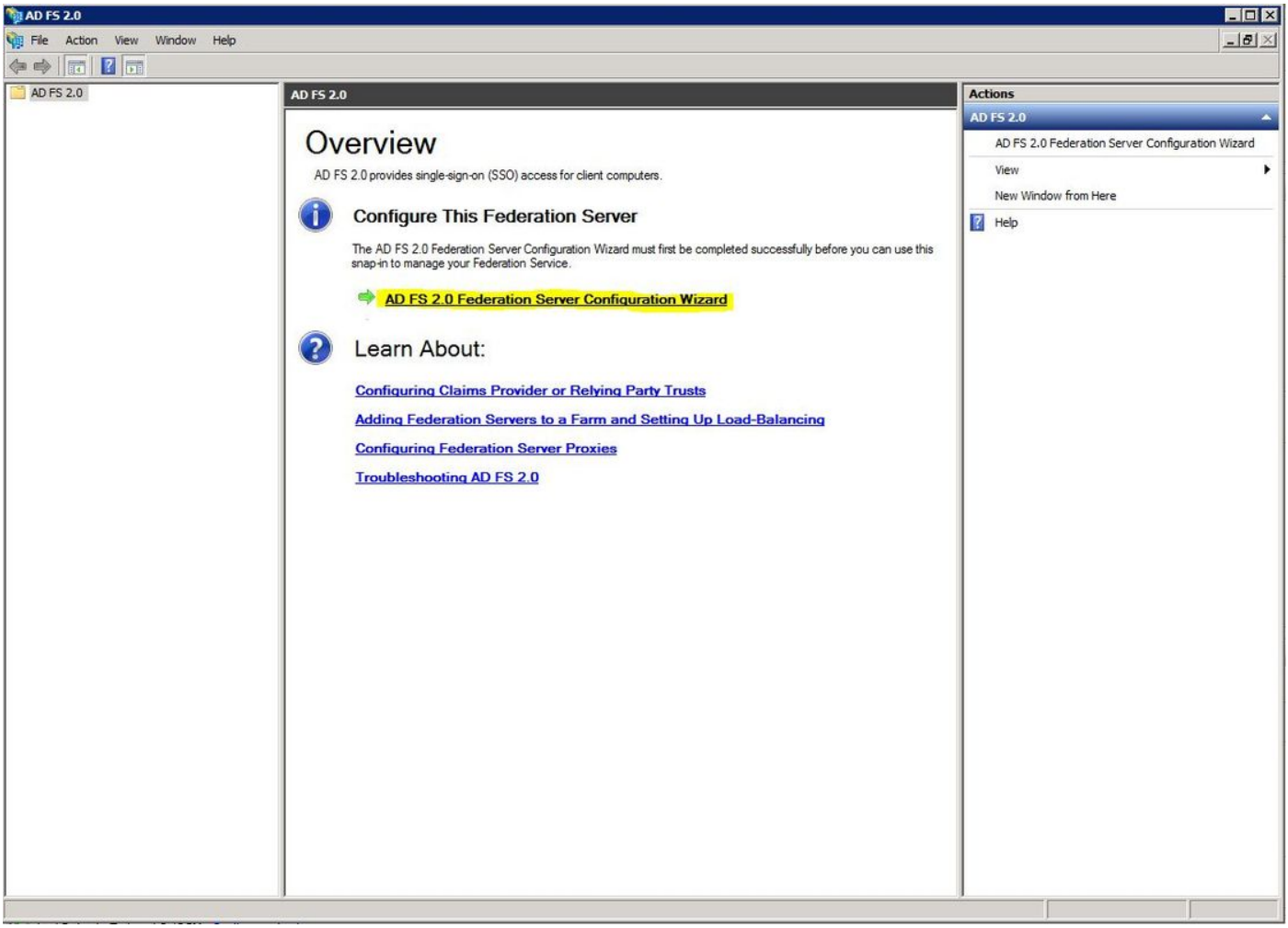
Étape 6. Quelques dépendances peuvent être installées automatiquement et vous êtes incité à cliquer sur Finish.

Maintenant que vous avez l'AD FS 2.0 installé sur votre serveur, vous devez ajouter une certaine configuration.

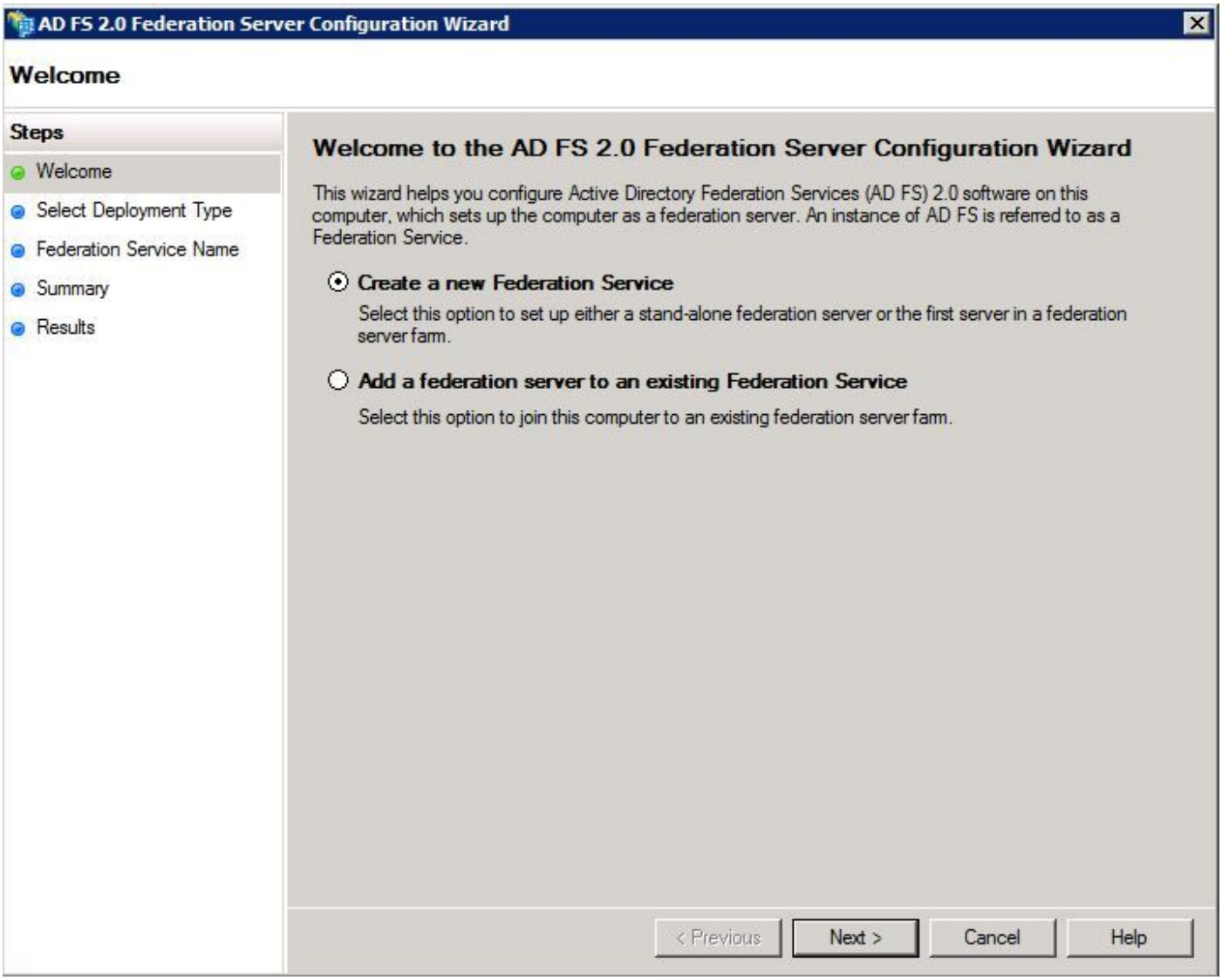
Configurez l'AD FS 2.0 sur vos Windows Server

Étape 1. La fenêtre FS 2.0 d'AD devrait s'être ouverte après que l'installer, cependant, vous pouvez le trouver en cliquant sur le **début** et en recherchant la Gestion FS 2.0 d'AD.

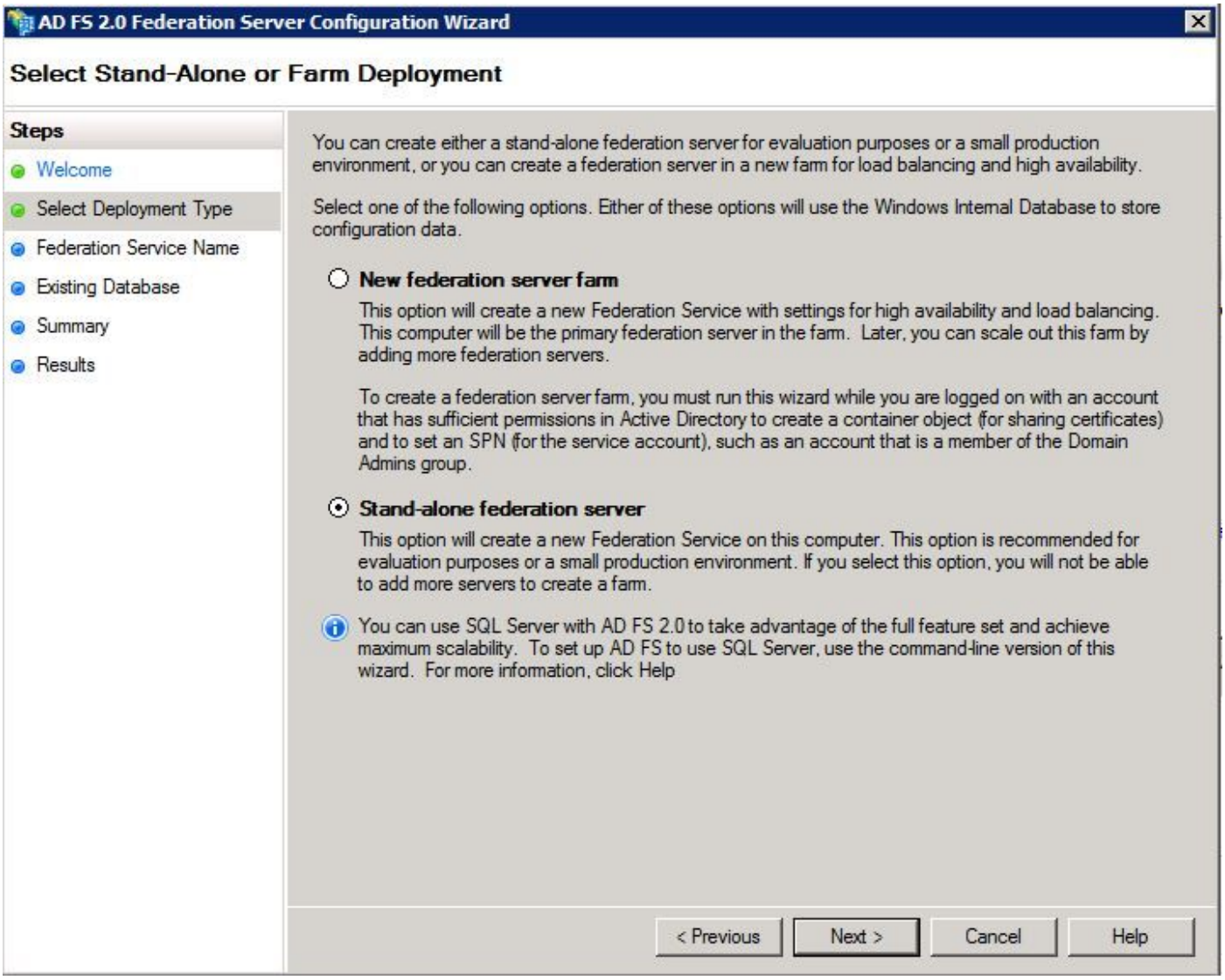
Étape 2. Une fois que vous avez la fenêtre FS d'AD ouverte, **assistant** choisi de **configuration du serveur de fédération FS 2.0 d'AD.**



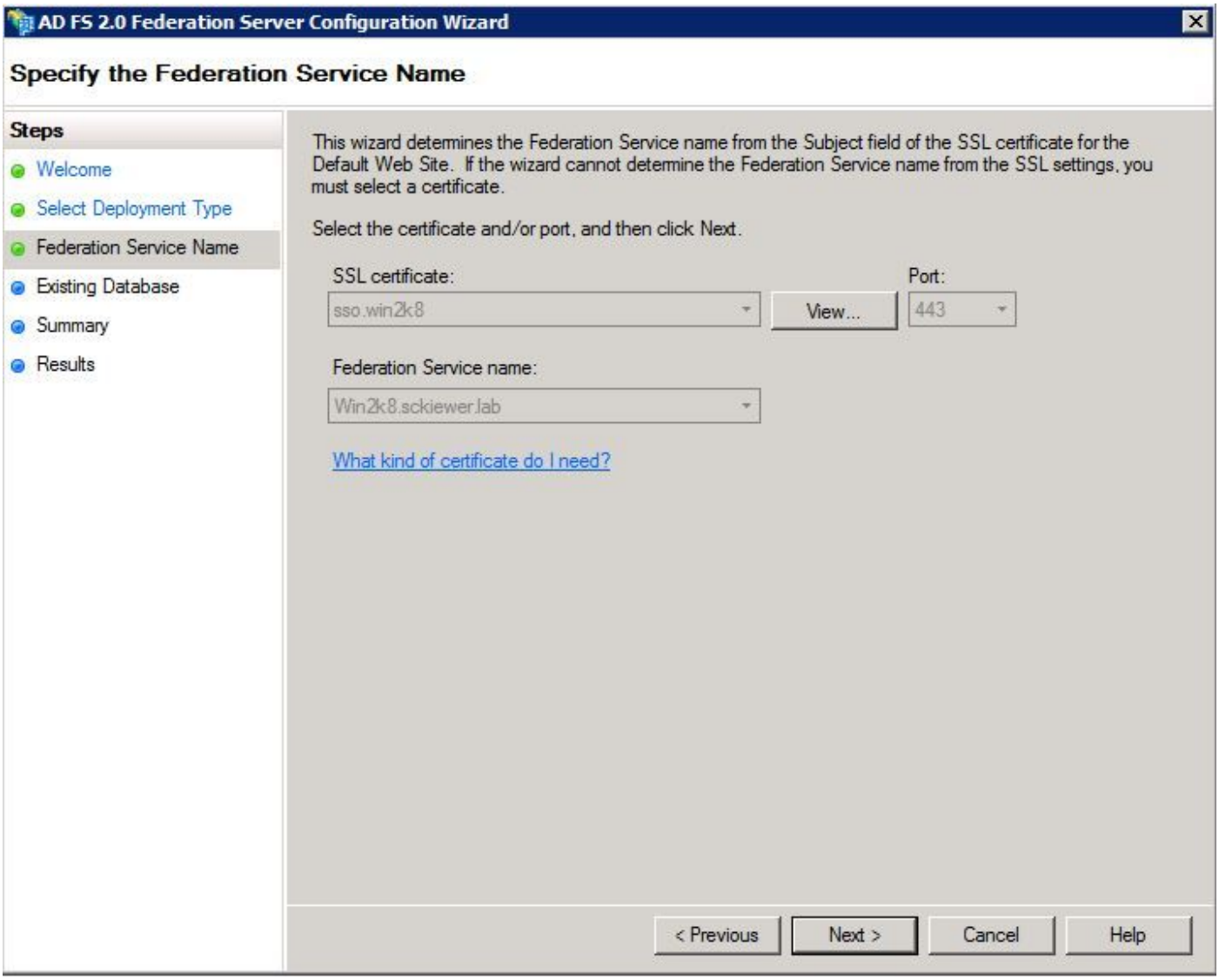
Étape 3. Ensuite, le clic **créent un nouveau service de fédération.**



Étape 4. Pour un environnement de travaux pratiques, le **serveur autonome de fédération** est suffisant.



Étape 5. Ensuite, vous êtes invité à sélectionner un certificat que les utilisations de serveur. Ceci si l'automatique le remplit tant que le serveur a un certificat déjà.



Étape 6. Si vous avez une base de données existante FS d'AD sur le serveur, vous devez l'enlever pour continuer.

Étape 7. En conclusion, vous êtes sur un écran récapitulatif où vous pouvez juste cliquer sur Next.

Importez les métadonnées d'IDP à CUCM/à téléchargement les métadonnées CUCM

Étape 1. Téléchargez les métadonnées de votre serveur FS d'AD en naviguant vers l'URL suivant : https://hostname/federationmetadata/2007-06/federationmetadata.xml

Étape 2. Naviguez vers la **gestion de Cisco Unified CM** > le **système** > l'**ouverture de session simple SAML**

Étape 3. **Enable SAML SSO de** clic

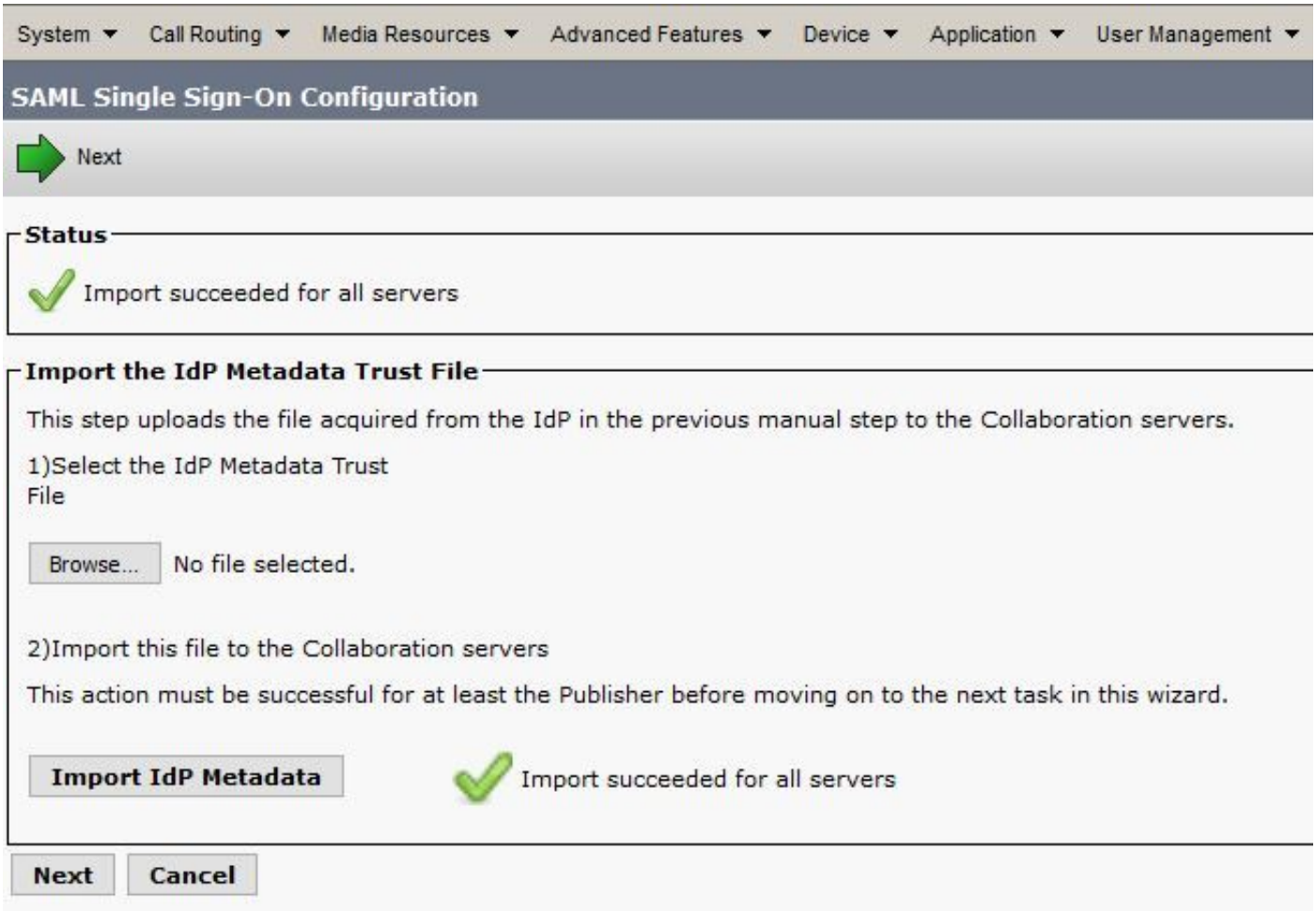
Étape 4. Vous pouvez recevoir un avertissement au sujet des connexions de serveur Web devant être remis à l'état initial, simplement hit **continuez**

Étape 5. Ensuite, CUCM vous instruit télécharger le fichier de métadonnées de votre IDP. Dans ce scénario, votre serveur FS d'AD est l'IDP, et nous avons téléchargé les métadonnées dans l'**étape 1** ci-dessus, ainsi cliquez sur Next.

Étape 6. Vous êtes invité à importer le fichier.

Étape 7. Le clic **parcourent >** sélectionnent le .xml de l'**étape 1 >** des **métadonnées d'IDP d'importation de** clic.

Étape 8. Vous devriez recevoir un message que l'importation était réussie :



Étape 9. Cliquez sur Next

Étape 10. Maintenant que vous avez les métadonnées d'IDP importées dans CUCM, vous devez importer les métadonnées de CUCM dans votre IDP.

Étape 11. Cliquez sur Download le **fichier de métadonnées de confiance**

Étape 12. Cliquez sur Next

Étape 13. Déplacez le fichier .zip qui a été téléchargé dans l'**étape 12 à** vos Windows Server et extrayez le contenu à un répertoire.

Importez CUCM Metatdata au serveur FS 2.0 d'AD et créez les règles de demande

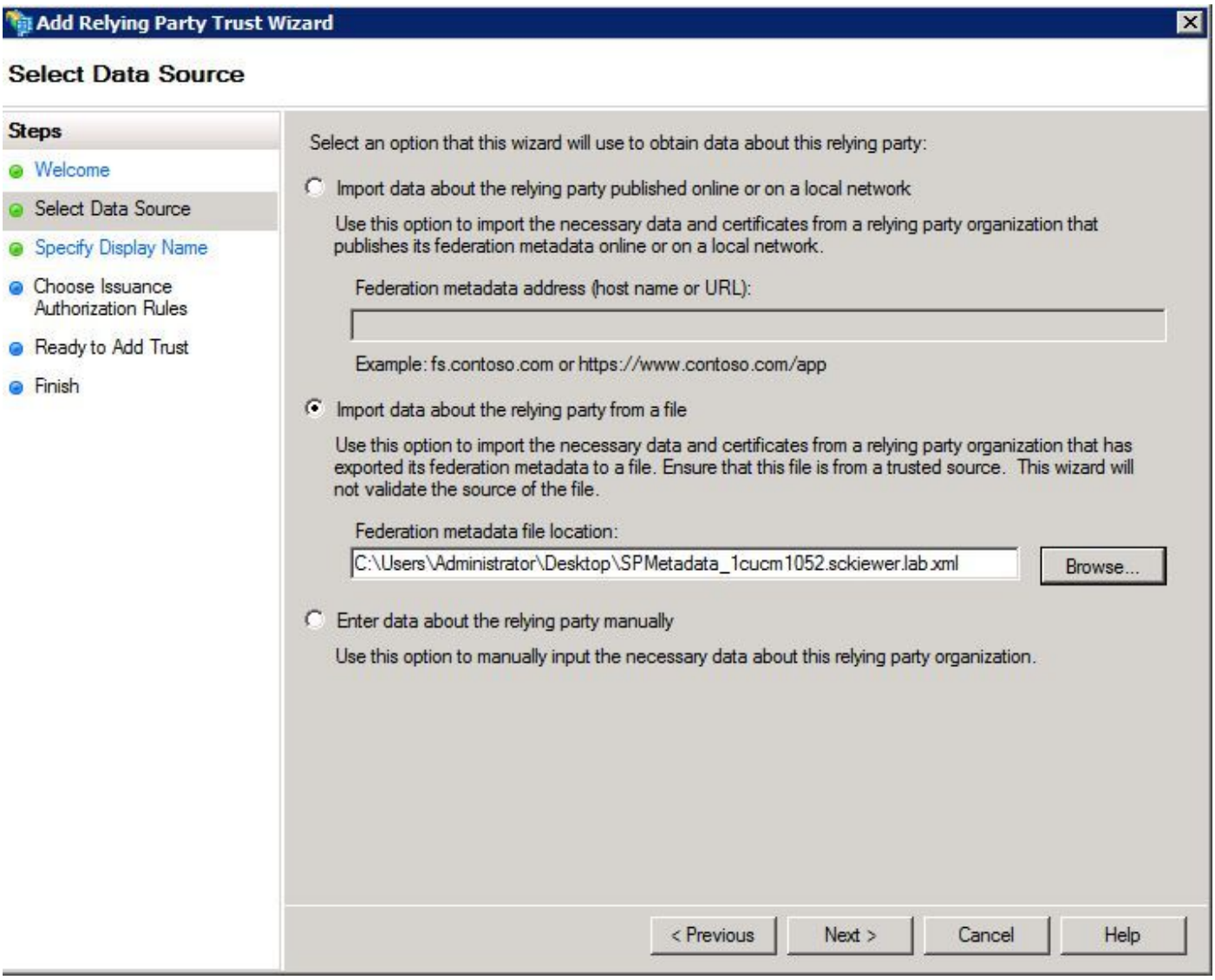
Étape 1. En ce moment, retournez à votre serveur FS d'AD et ouvrez la fenêtre de Gestion FS 2.0 d'AD en cliquant sur le **début** et en recherchant la **Gestion FS 2.0 d'AD.**

Étape 2. Clic **requis : Ajoutez un interlocuteur comptant de confiance** (note : si vous ne voyez pas ceci, vous pouvez devoir fermer la fenêtre et ouvert elle sauvegardent. Cette option ne révélera pas si la fenêtre a resté ouvert puisque l'**assistant de serveur de fédération** terminé).

Étape 3. Une fois que vous avez l'**assistant comptant de confiance d'interlocuteur d'ajouter** ouvert, cliquez sur le **début**.

Étape 4. Ici, vous devez importer les fichiers .xml que vous avez extraits dans l'**étape 13**, ainsi des **données** choisies d'**importation au sujet de l'interlocuteur comptant à partir d'un fichier** et parcourez au répertoire contenant les fichiers, sélectionnez le .xml pour votre éditeur.

Remarque: Suivez les mêmes étapes ci-dessus pour n'importe quel serveur unifié de Collaboration que vous voulez utiliser SSO en fonction.



Étape 5. Cliquez sur Next

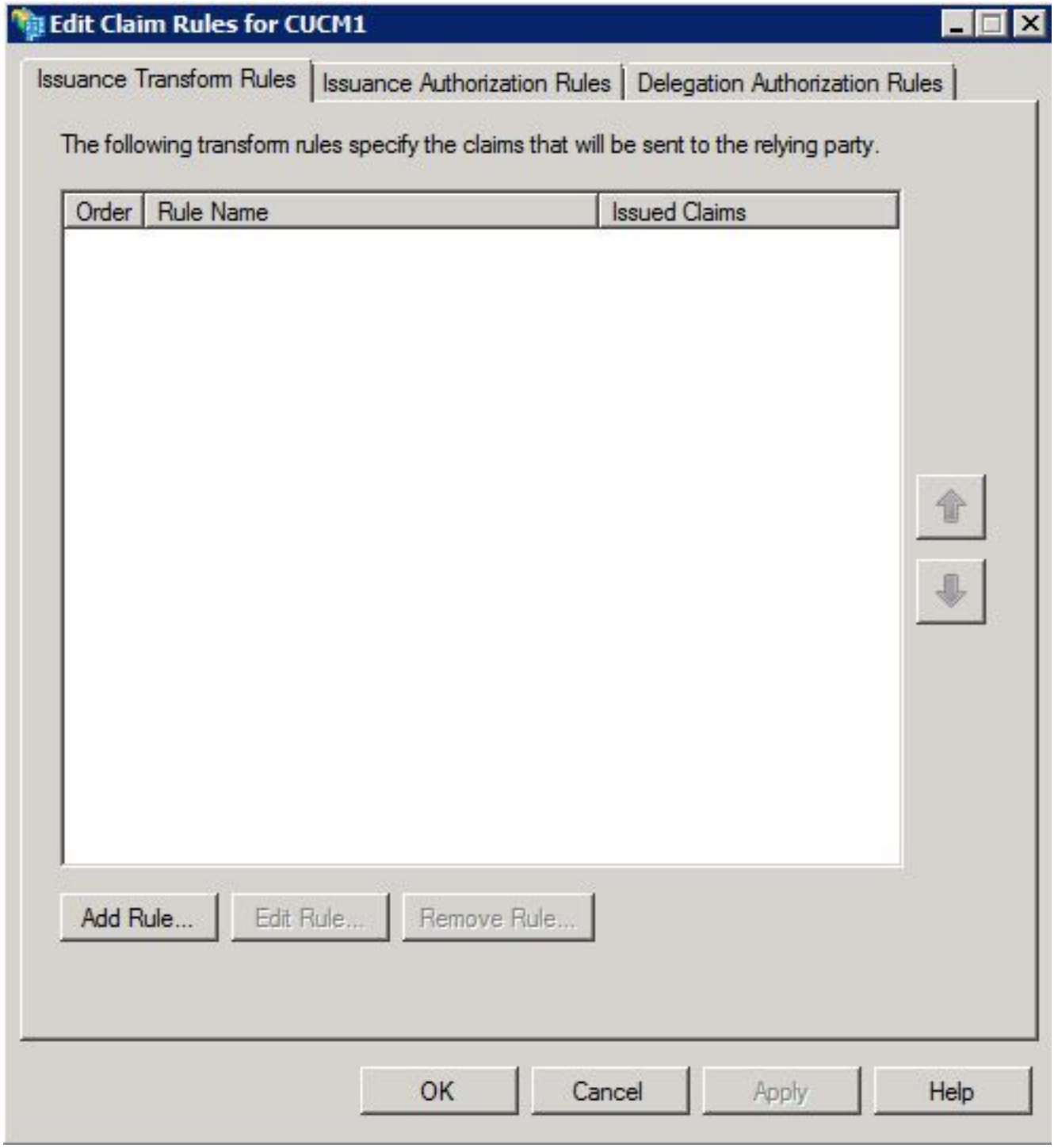
Étape 6. Éditez le **nom d'affichage** à celui que vous voudriez alors cliquiez sur Next.

Étape 7. **Autorisation** choisie **tous les utilisateurs d'accéder à cet interlocuteur comptant** et de cliquer sur Next

Étape 8. Cliquez sur Next une fois de plus

Étape 9. Sur cet écran, veillez-vous pour avoir **ouvert le dialogue de règles de demande d'éditer pour cette confiance comptante d'interlocuteur quand l'assistant se ferme** vérifié, alors cliquent sur **étroitement**

Étape 10. Vous devriez maintenant être amené à une fenêtre qui ressemble à ceci :



Étape 11. Dans cette fenêtre, cliquez sur Add la **règle**.

Étape 12. Pour le **modèle de règle de demande**, choisi **envoyez les attributs de LDAP comme demandes** et cliquez sur Next.

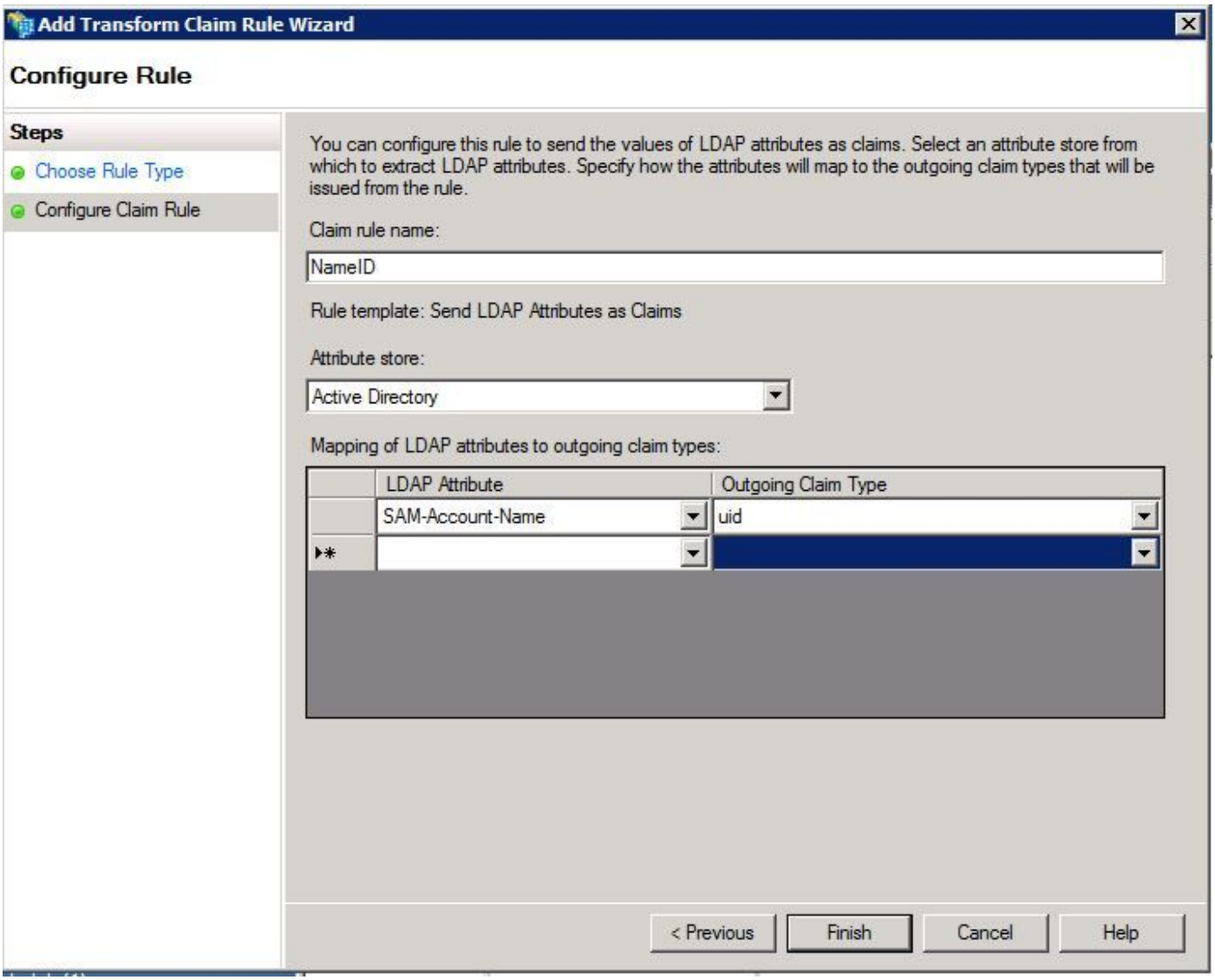
Étape 13. Sur la page suivante, entrez dans **NameID** pour le **nom de règle de demande**

Étape 14. **Répertoire actif** choisi pour la **mémoire d'attribut**

Étape 15. **Sam-Compte-nom** choisi pour l'**attribut de LDAP**

Étape 16. Entrez dans l'**uid** pour le **type sortant de demande**

Remarque: **l'uid** n'est pas une option qui autofill ou révéler dans la liste déroulante



Étape 17. Cliquez sur Finish

Étape 18. Vous devriez maintenant voir votre règle, cependant, nous devrons ajouter une autre règle ainsi cliquez sur Add la **règle** de nouveau.

Étape 19. Choisi **envoyez les demandes utilisant une règle faite sur commande**

Étape 20. Écrivez un **nom de règle de demande** (ceci peut être quelque chose)

Étape 21. Dans le domaine de **règle faite sur commande**, collez le texte suivant :

c : [== « http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"] de type

question de => (type = « http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier", émetteur = c.Issuer, OriginalIssuer = c.OriginalIssuer, valeur = c.Value, ValueType = c.ValueType, Properties

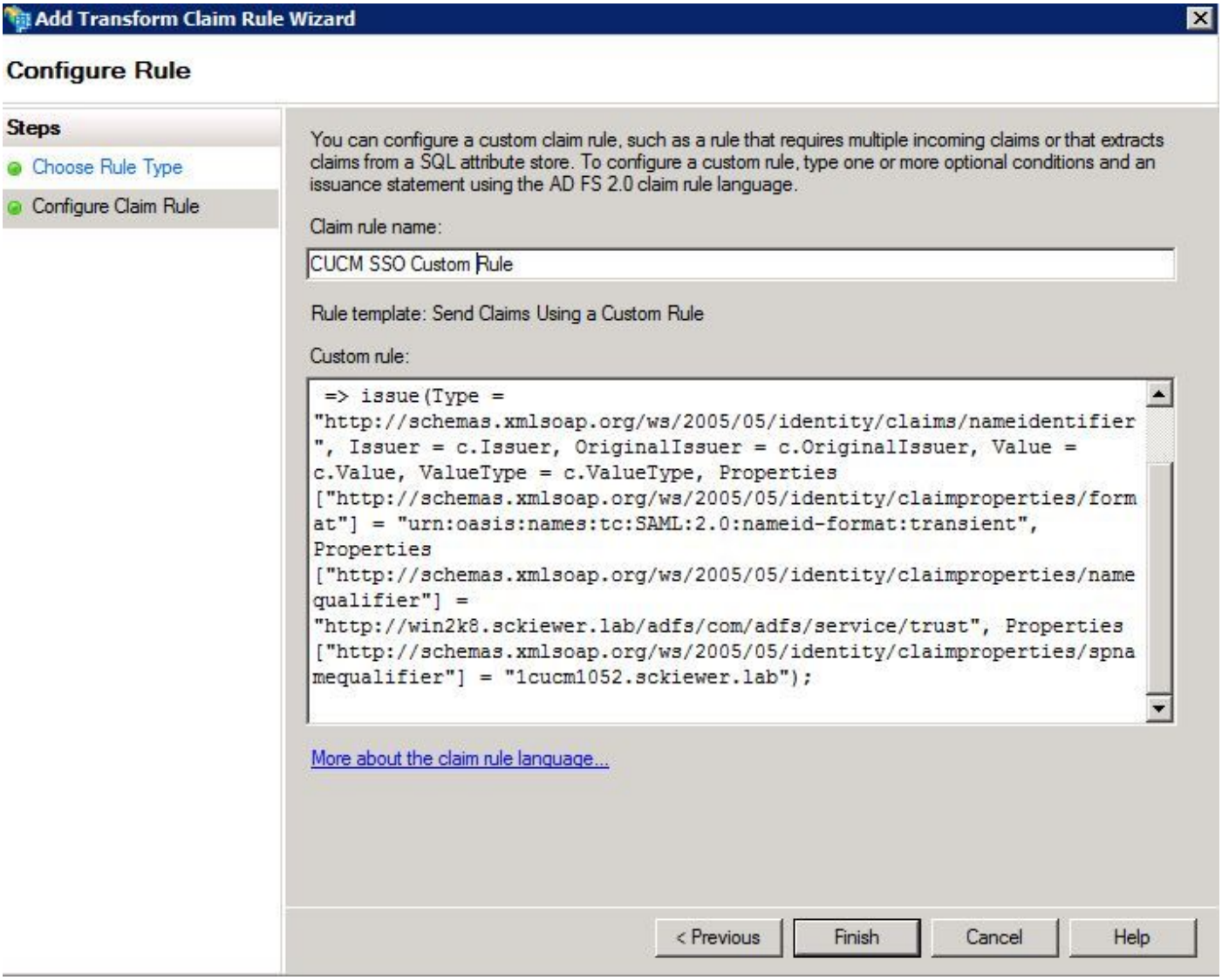
[« http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] = "urn:oasis:names:tc:SAML:2.0:nameid-format:transient",

Properties [« http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/namequalifier"] = « http:// <AD_FS_SERVICE_NAME>

/adfs/com/adfs/service/trust », Properties [« http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"] = « <CUCM_FQDN>") ;

Étape 22. Veillez-vous pour modifier les deux blocs bleus des textes avec les valeurs appropriées.

Remarque: Si vous n'êtes pas sûr au sujet du **nom de service FS d'AD**, allez aux commentaires de ce document apprendre comment idendtify le **nom de service FS d'AD.**



Étape 23. Cliquez sur Finish

Étape 24. Cliquez sur OK

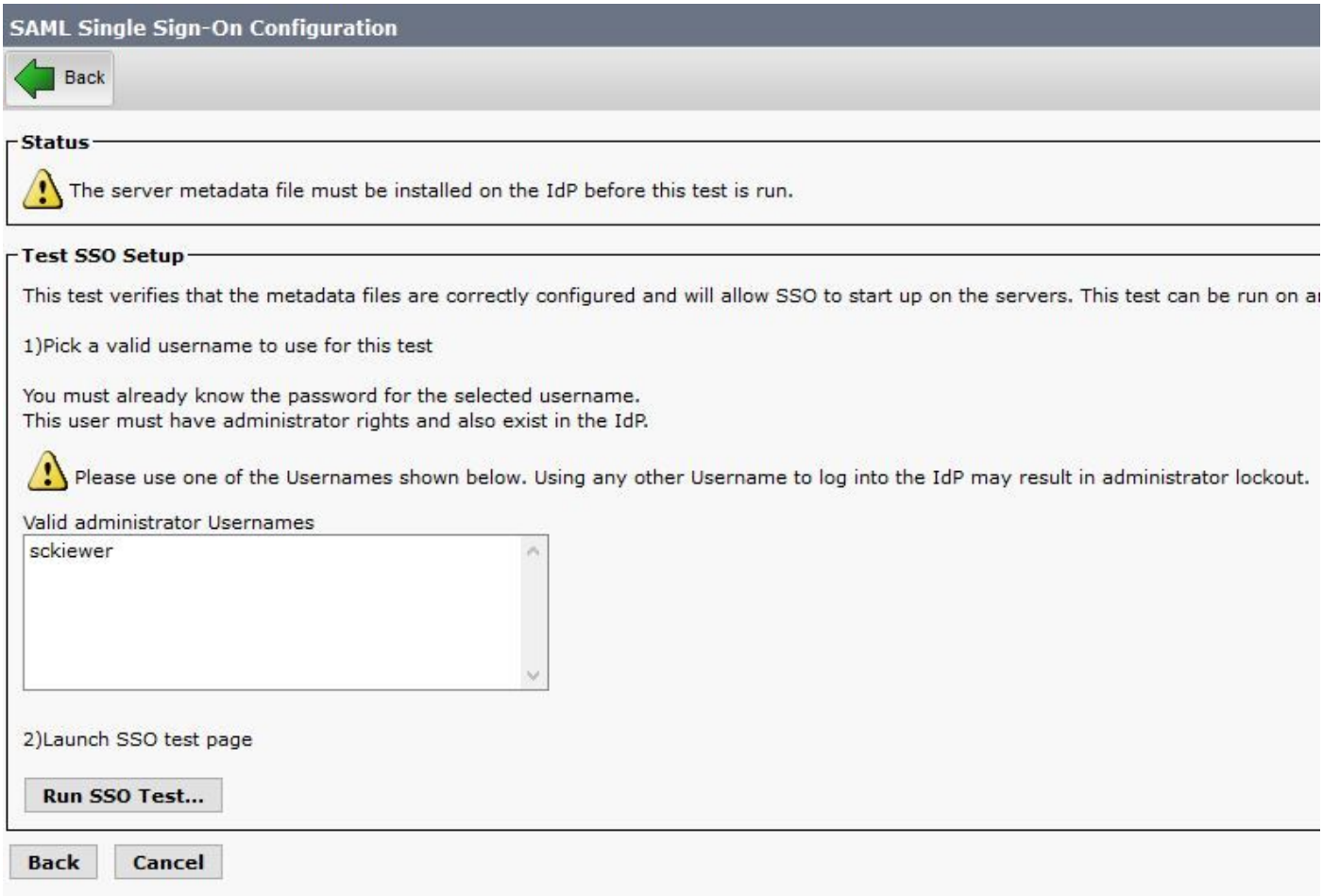
Remarque: Les règles de demande sont nécessaires pour n'importe quel serveur unifié de

Collaboration que vous voulez utiliser SSO en fonction.

Finissez d'activer SSO sur CUCM et exécutez le test SSO

Étape 1. Maintenant que le serveur FS d'AD est saturé, vous pouvez retourner à CUCM.

Étape 2. Vous devriez s'asseoir sur une page qui ressemble à ceci :



Étape 3. Avancez et sélectionnez votre utilisateur final qui fait sélectionner le rôle de **superutilisateurs CCM standard** et cliquez sur Run le **test SSO…**

Étape 4. Une fenêtre contextuelle devrait apparaître qui peut prendre environ 30 secondes pour charger, mais par la suite vous devriez être présenté avec un défi pour ouvrir une session.

Étape 5. Entrez le mot de passe que vous avez configuré sur le serveur LDAP pour l'utilisateur sélectionné et vous devriez alors voir :

Étape 6. **La fin de** clic sur la fenêtre contextuelle et **terminent** alors.

SSO est maintenant configuré dans votre laboratoire.

Dépannage

Placez les logs SSO pour mettre au point

Pour placer SSO les logs pour vous mettre au point doivent exécuter cette commande dans le CLI du CUCM : **placez le niveau de samltrace mettent au point**

Les logs SSO peuvent être téléchargés de RTMT. Le nom du positionnement de log est **Cisco SSO**.

Trouver le nom de service de fédération

Vous pouvez confirmer le nom de service de fédération en cliquant sur le **début** et en recherchant et en ouvrant la **Gestion FS 2.0 d'AD**.

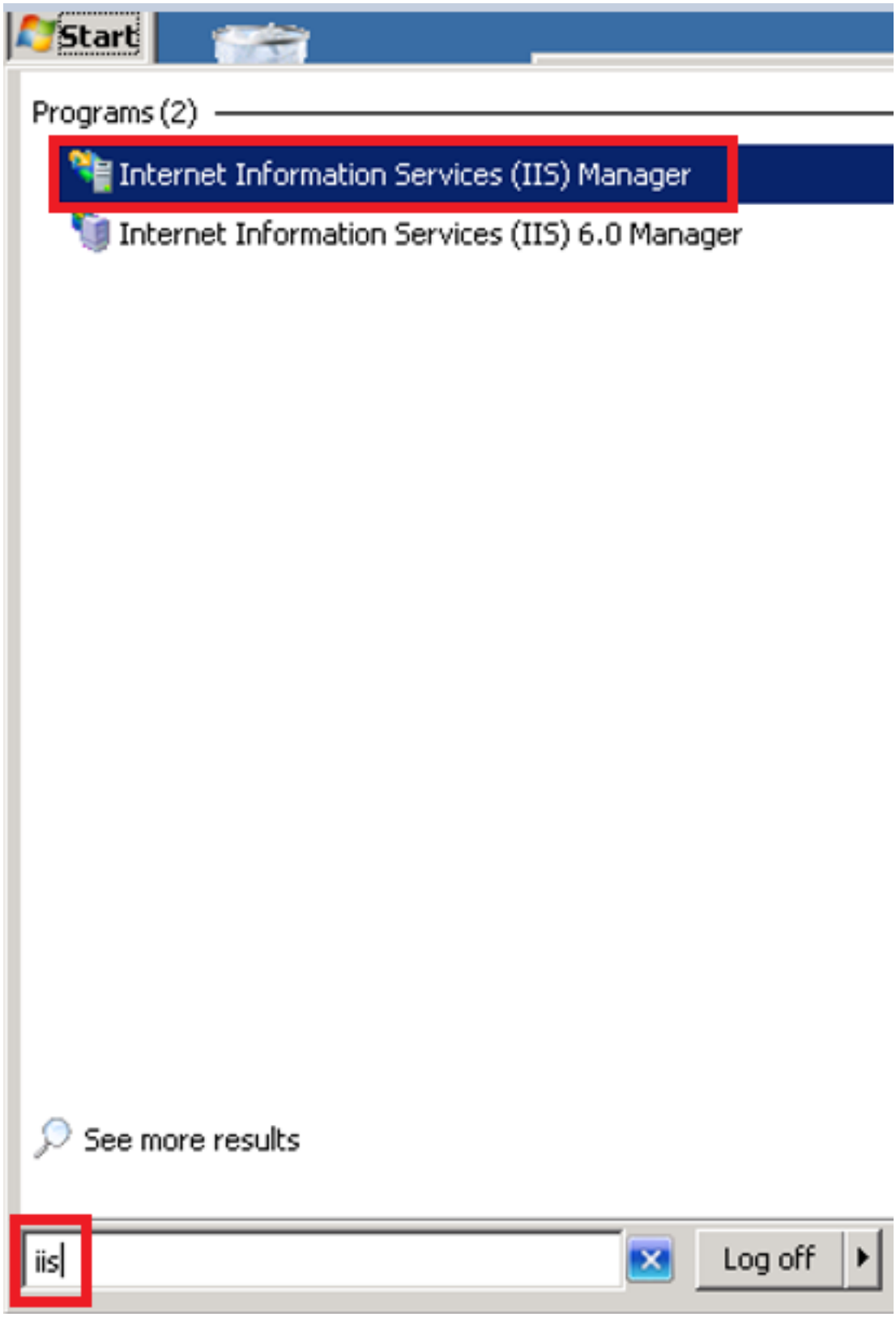
• Cliquez sur éditent en fonction le **service Properties de fédération…**
• Tandis que sur l'onglet Général recherchez le **nom de service de fédération**

Certificat Dotless quand Specifing le nom de service de fédération

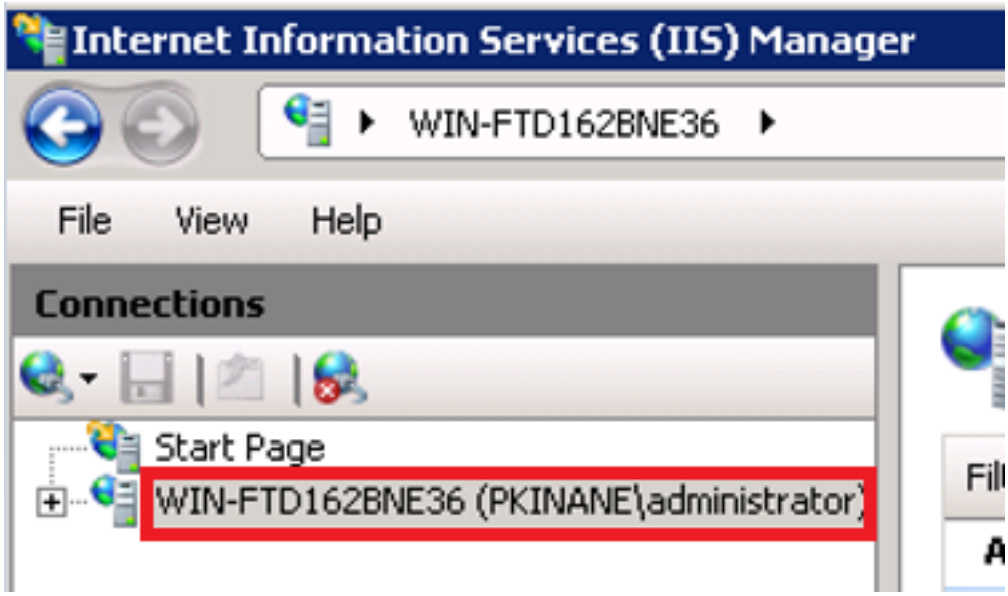
Si vous recevez le message d'erreur suivant tout en allant par l'assistant de configuration FS d'AD, vous devrez créer un nouveau certificat.

« Le certificat sélectionné ne peut pas être utilisé pour déterminer le nom de service de fédération parce que le certificat sélectionné a un nom du sujet (court-nommé) dotless (par exemple, fabrikam). Sélectionnez un autre certificat sans nom du sujet (court-nommé) dotless (par exemple, fs.fabrikam.com), et puis l'essayez de nouveau. »

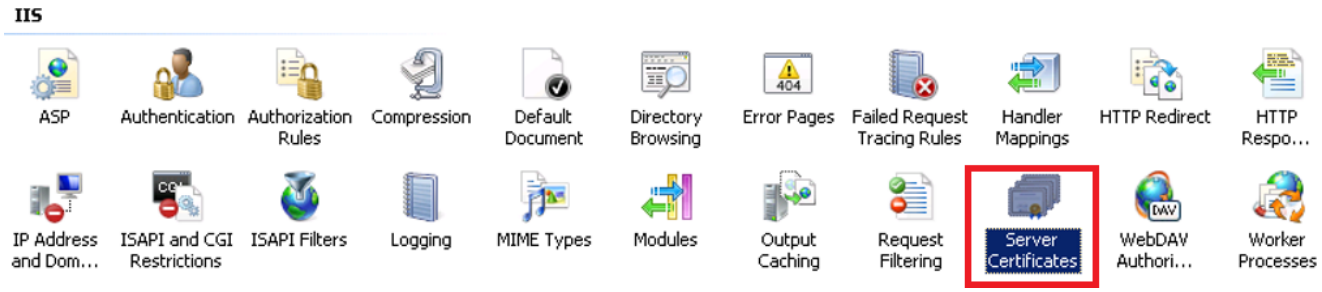
Cliquez sur le début et recherchez les iis puis ouvrez le gestionnaire de l'Internet Information Services (IIS)



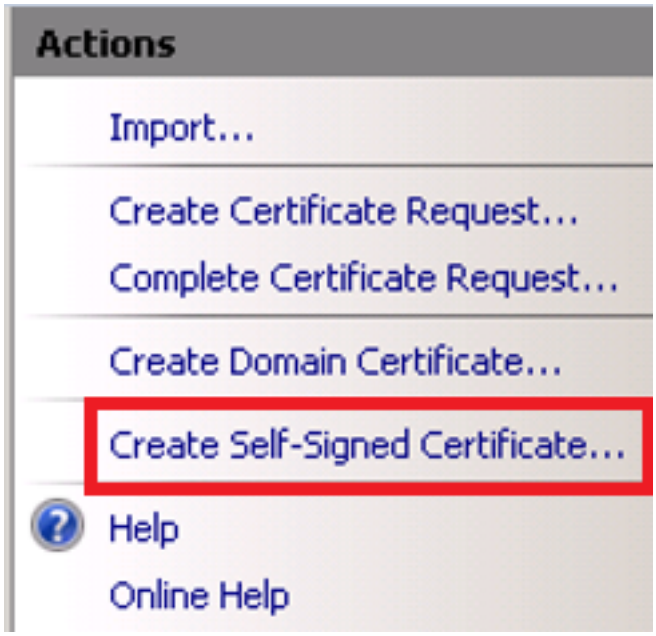
Cliquez sur en fonction votre nom de serveur



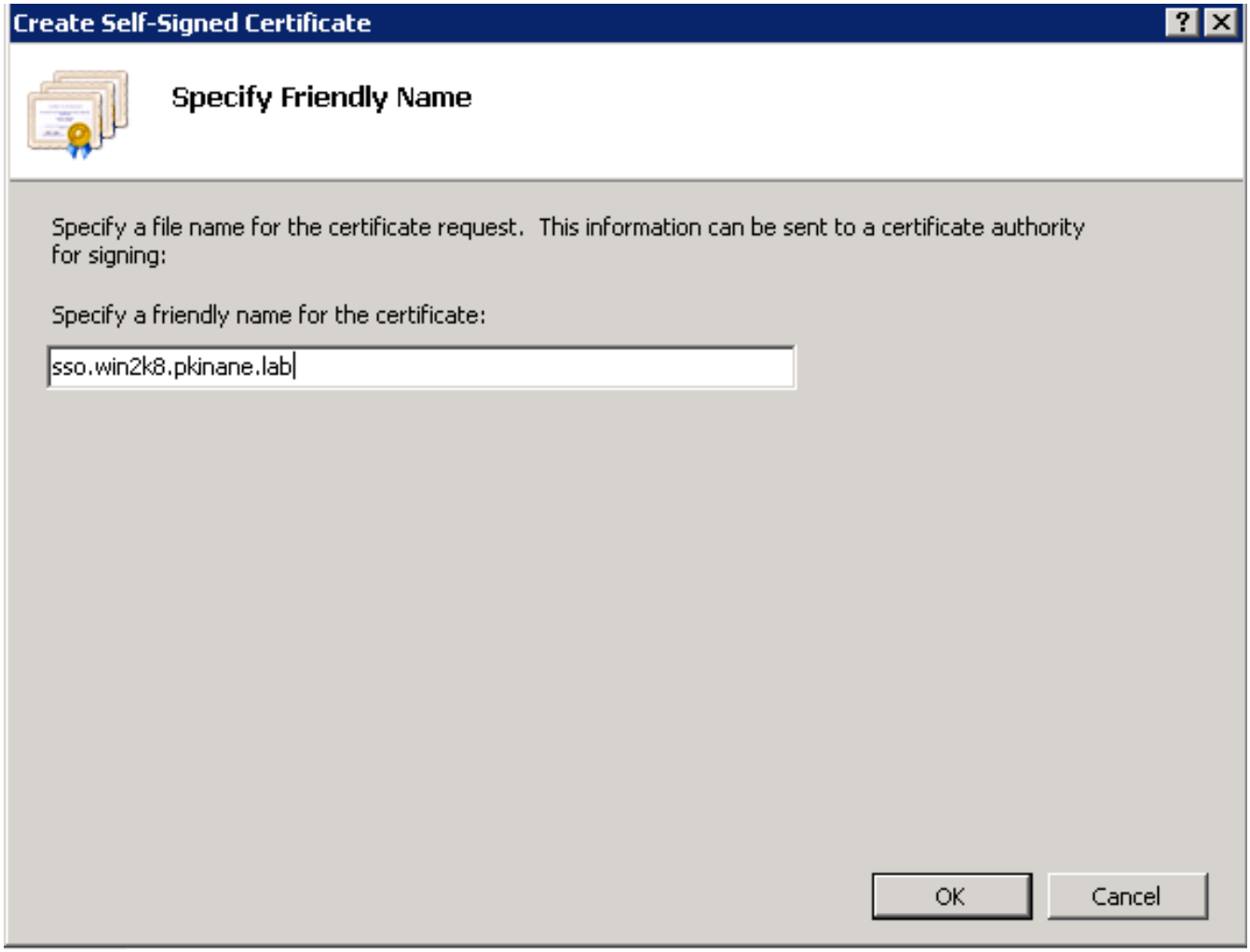
Cliquez sur en fonction les Certificats de serveur



Cliquez sur créent en fonction le certificat Auto-signé



Écrivez le nom que vous voulez pour le pseudonyme de votre certificat



Le temps est hors de sync entre les serveurs CUCM et d'IDP

Si vous recevez l'erreur répertoriée ci-dessous en essayant d'exécuter le test SSO de CUCM, vous pouvez devoir configurer les Windows Server pour utiliser les mêmes serveurs de NTP que le CUCM. Le processus pour faire ceci est couvert dans les commentaires de.

« Réponse non valide SAML. Ceci peut sont provoqué par quand le temps est hors de sync entre Cisco Unified Communications Manager et les serveurs d'IDP. Veuillez vérifier la configuration de NTP sur les deux serveurs. Exécutez « l'état de ntp d'utils » du CLI pour vérifier cet état sur Cisco Unified Communications Manager. »

Une fois que les Windows Server ont les serveurs de NTP vous ont spécifié devraient obtenir les métadonnées de l'IDP de nouveau et les télécharger au CUCM. Alors allez directement au test SSO et voyez si vous obtenez toujours la même erreur.