

Version 2.0 FS d'AD installée pour l'exemple de configuration SAML SSO

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Configurez](#)

[Métadonnées de fournisseur d'identité de version 2.0 FS d'AD de téléchargement \(IDP\)](#)

[Métadonnées de Collaboration Server de téléchargement \(fournisseur de services\)](#)

[CUCM IM et service de présence](#)

[Unity Connection](#)

[Ravitaillement de Collaboration de perfection de Cisco](#)

[Ajoutez CUCM comme confiance comptante d'interlocuteur](#)

[Ajoutez CUCM IM et présence comme confiance comptante d'interlocuteur](#)

[Ajoutez UCXN comme confiance comptante d'interlocuteur](#)

[Ajoutez le ravitaillement principal de Collaboration de Cisco comme confiance comptante d'interlocuteur](#)

[Vérifiez](#)

[Dépannez](#)

Introduction

Ce document décrit comment configurer la version 2.0 active de service de fédération de répertoire (AD FS) afin d'activer le langage de balisage d'assertion de Sécurité (SAML) choisissent Signe-sur (SSO) pour des Produits de Cisco Collaboration comme Cisco Unified Communications Manager (CUCM), le Cisco Unity Connection (UCXN), le CUCM IM et la présence, et la Collaboration principale de Cisco.

Conditions préalables

Conditions requises

La version 2.0 FS d'AD doit être installée et testée.

Attention : Ce guide d'installation est basé sur une installation de laboratoire et on assume que la version 2.0 FS d'AD est utilisée seulement pour SAML SSO avec des Produits de Cisco Collaboration. Au cas où il serait utilisé par d'autres applications critiques, puis la personnalisation nécessaire doit être faite selon la documentation Microsoft officielle.

[Composants utilisés](#)

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

- Version 2.0 FS d'AD
- Microsoft Internet Explorer 10
- Version 10.5 CUCM
- Cisco IM et version 10.5 de Presence Server
- Version 10.5 UCXN
- Ravitaillement 10.5 de Collaboration de perfection de Cisco

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Configurez

Métadonnées de fournisseur d'identité de version 2.0 FS d'AD de téléchargement (IDP)

Afin de télécharger des métadonnées d'IDP, exécutez ce lien sur vous navigateur : [https:// <FQDN d'ADFS>/FederationMetadata/2007-06/FederationMetadata.xml](https://<FQDN d'ADFS>/FederationMetadata/2007-06/FederationMetadata.xml).

Métadonnées de Collaboration Server de téléchargement (fournisseur de services)

CUCM IM et service de présence

Ouvrez un navigateur Web, log dans CUCM comme administrateur, et naviguez vers le **système > le SAML simples se connectent**.

Unity Connection

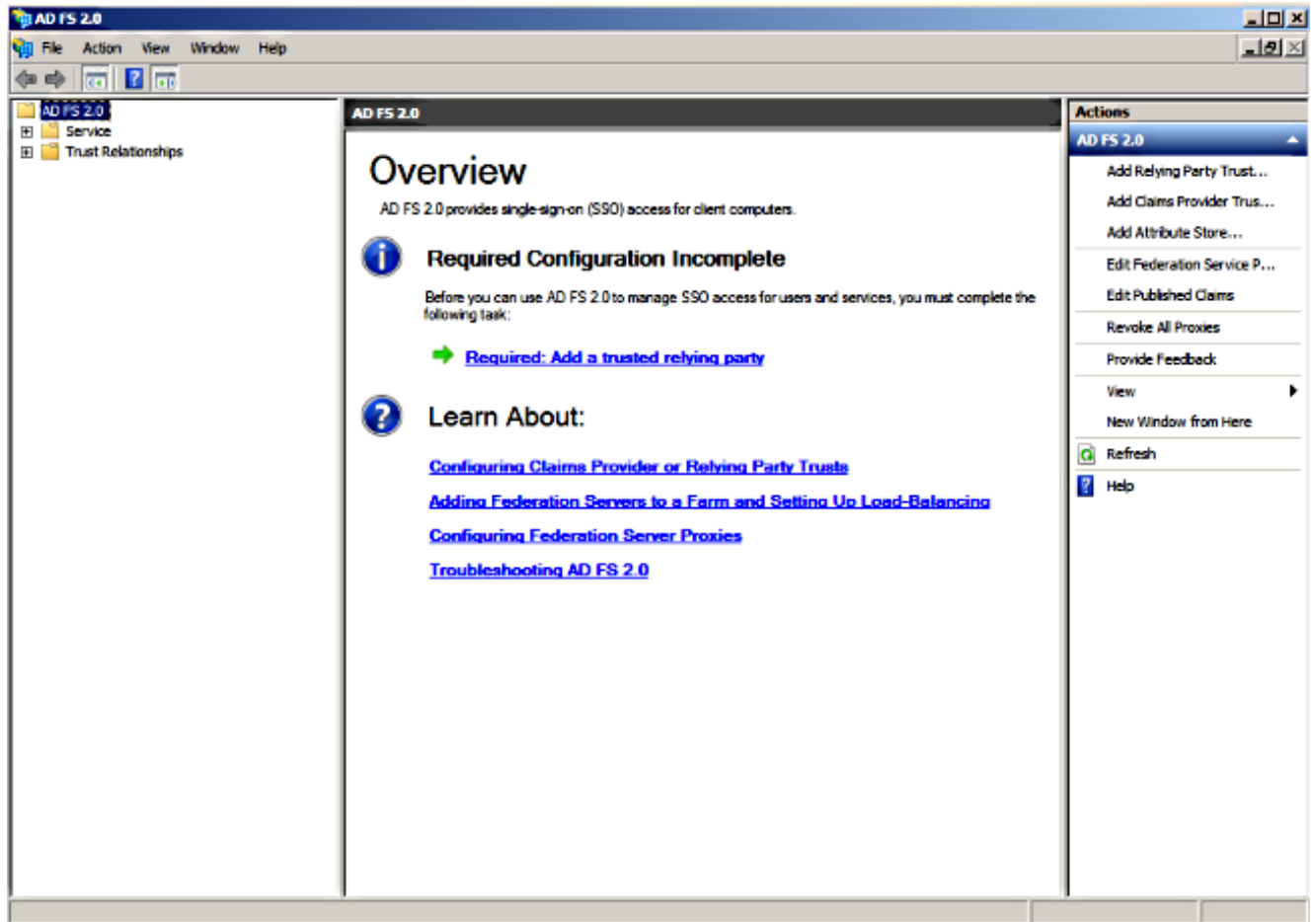
Ouvrez un navigateur Web, log dans UCXN comme administrateur, et naviguez vers des **paramètres système > le SAML simples se connectent**.

Ravitaillement de Collaboration de perfection de Cisco

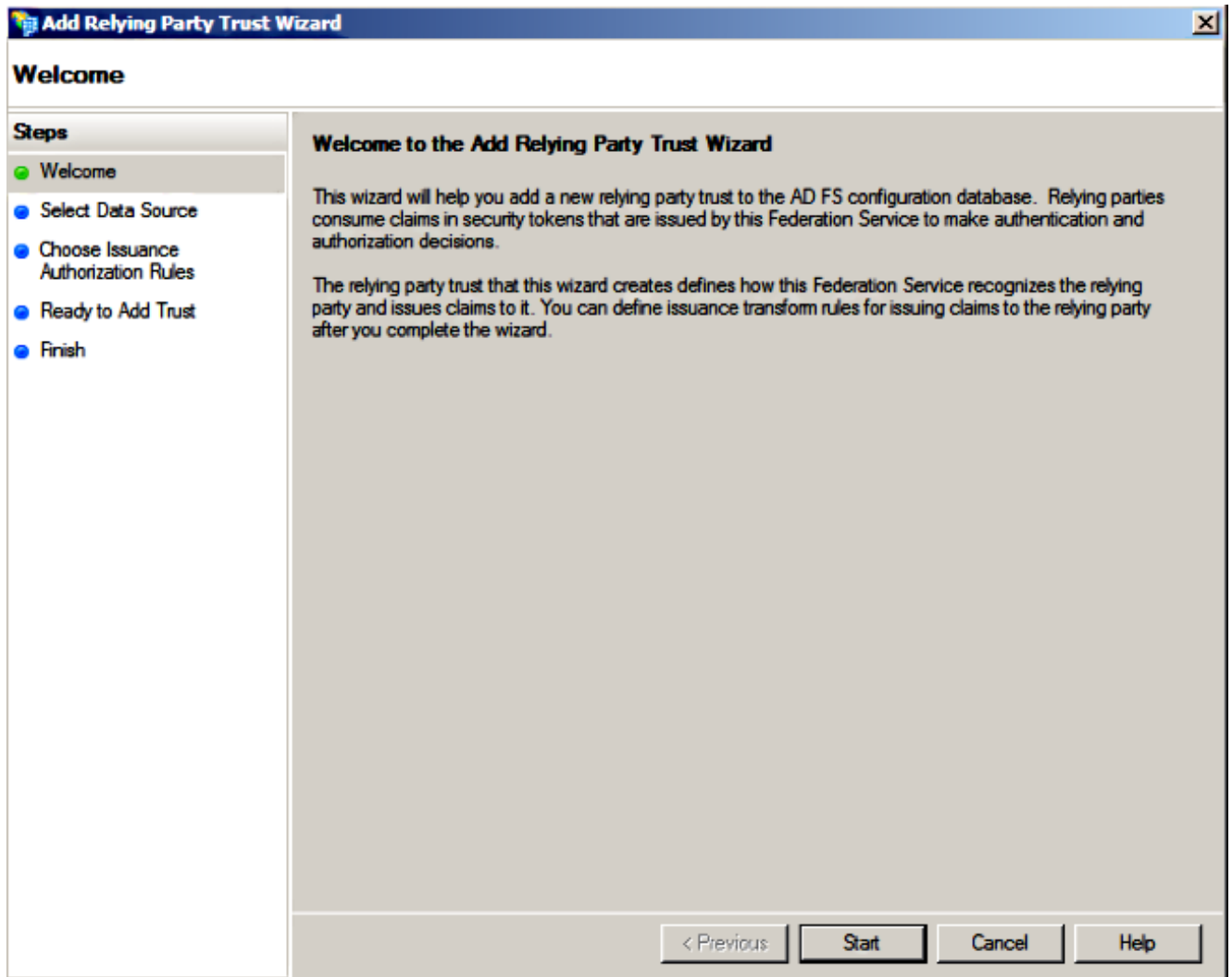
Ouvrez un navigateur Web, log dans l'assurance principale de Collaboration comme globaladmin, et naviguez vers la **gestion > le système installés > simple se connectent**.

Ajoutez CUCM comme confiance comptante d'interlocuteur

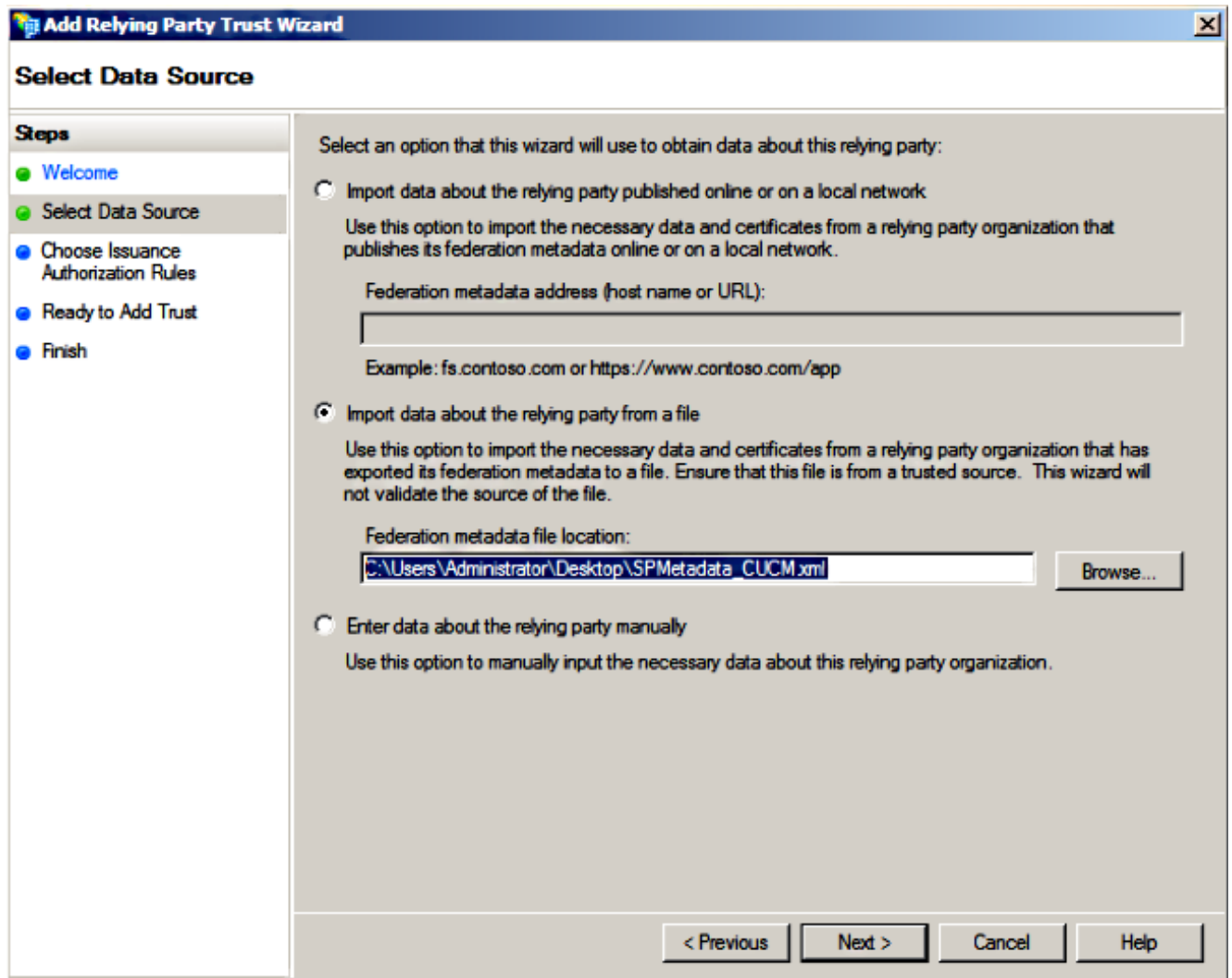
1. Connectez-vous dans le serveur FS d'AD et lancez la version 2.0 FS d'AD du menu de **programmes de Microsoft Windows**.
2. Choisi **ajoutez la confiance comptante d'interlocuteur**.



3. Début de clic.



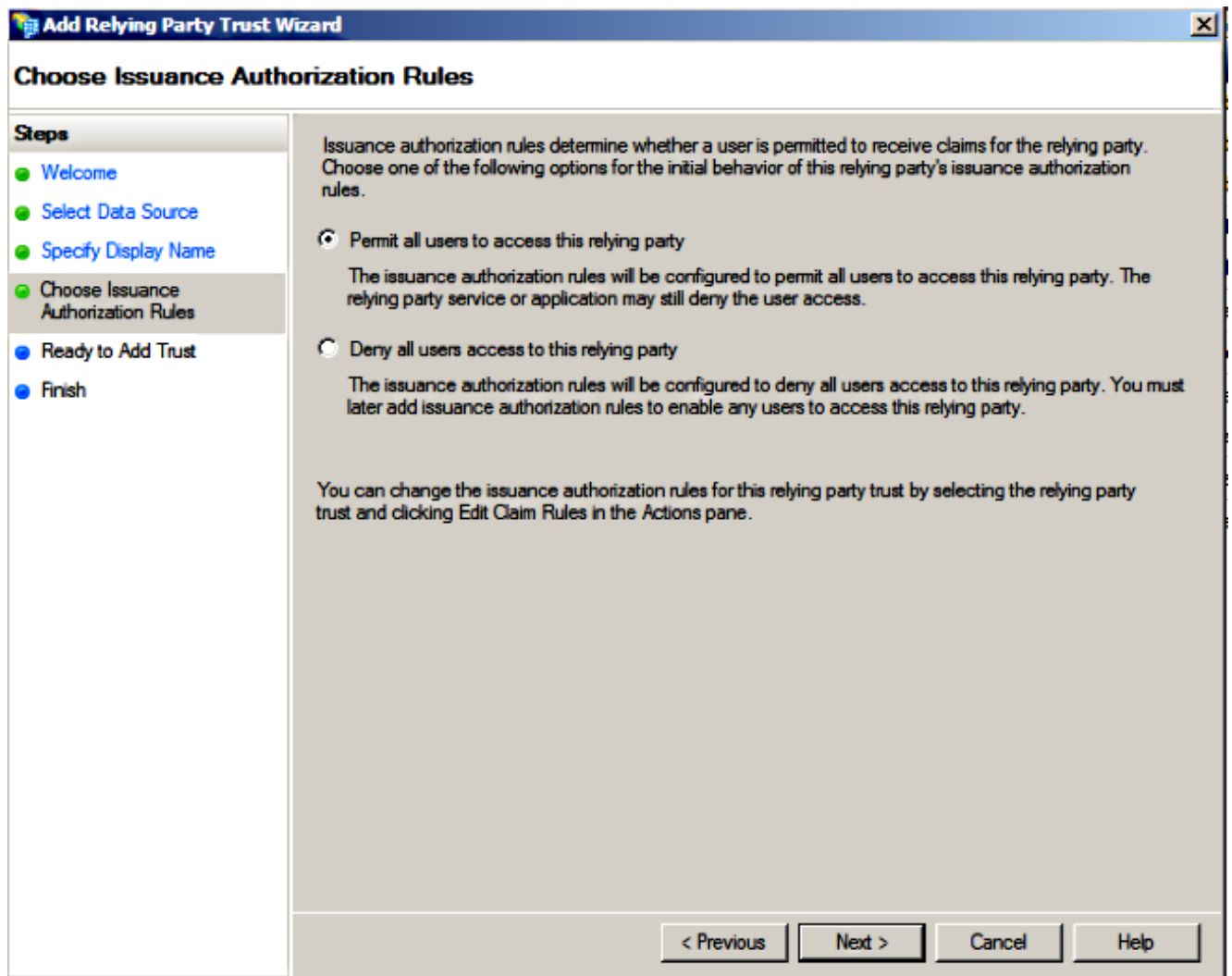
4. Sélectionnez les **données d'importation au sujet de l'interlocuteur comptant d'une option de fichier**, choisissez les **métadonnées SPMetadata_CUCM.xml** classent que vous avez téléchargé de CUCM plus tôt, et cliquent sur Next.



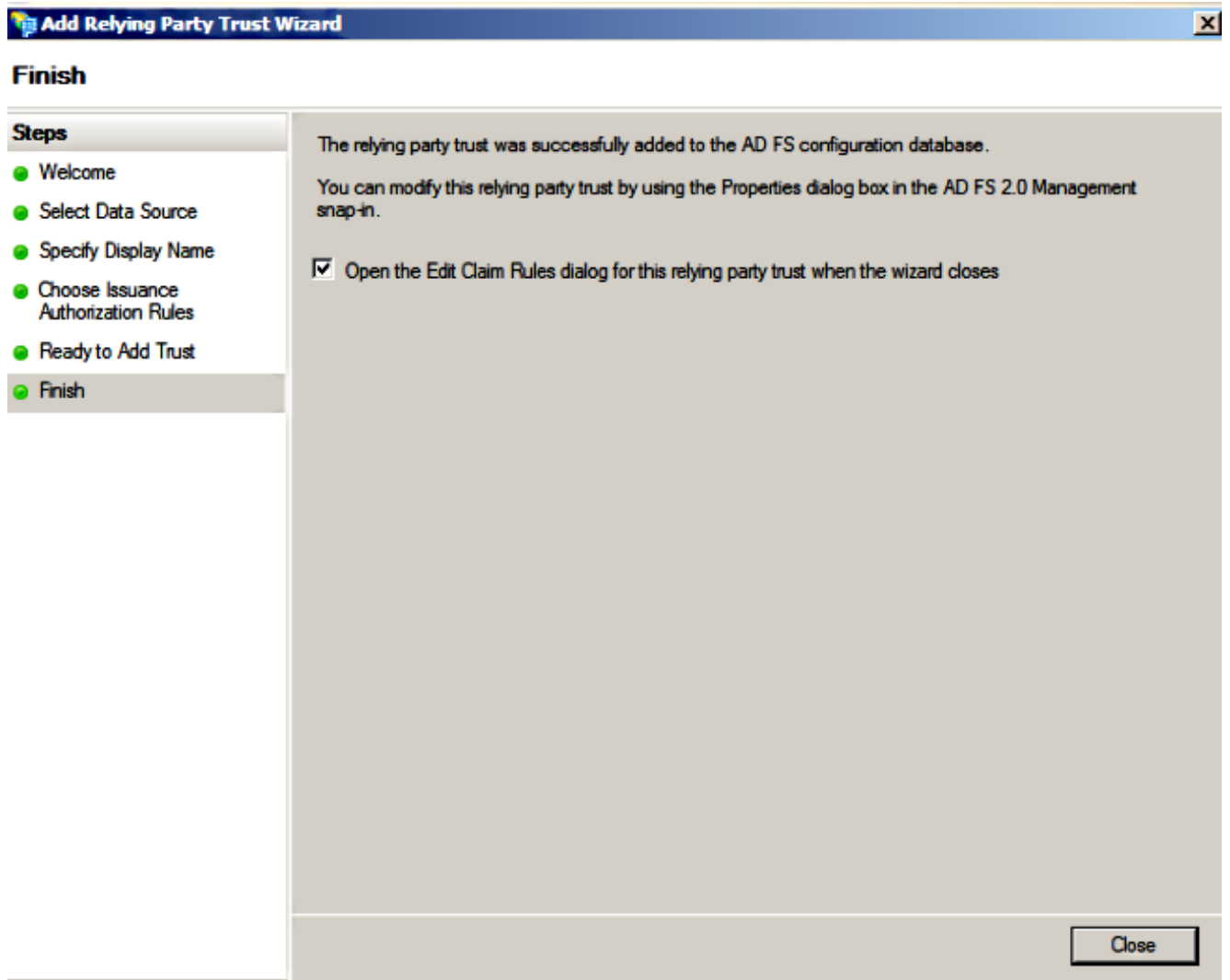
5. Écrivez le nom d'affichage et cliquez sur Next.

The screenshot shows a Windows-style dialog box titled "Add Relying Party Trust Wizard". The main title bar is blue with a close button (X) on the right. Below the title bar, the text "Specify Display Name" is displayed in a bold font. On the left side, there is a "Steps" pane with a list of steps: "Welcome", "Select Data Source", "Specify Display Name" (which is highlighted with a grey background), "Choose Issuance Authorization Rules", "Ready to Add Trust", and "Finish". The main area of the dialog contains the instruction "Type the display name and any optional notes for this relying party." Below this instruction, there is a text box labeled "Display name:" containing the text "CUCM". Below the text box is a larger text area labeled "Notes:" containing the text "Adding CUCM as Relaying Party to ADFS". At the bottom of the dialog, there are four buttons: "< Previous", "Next >", "Cancel", and "Help".

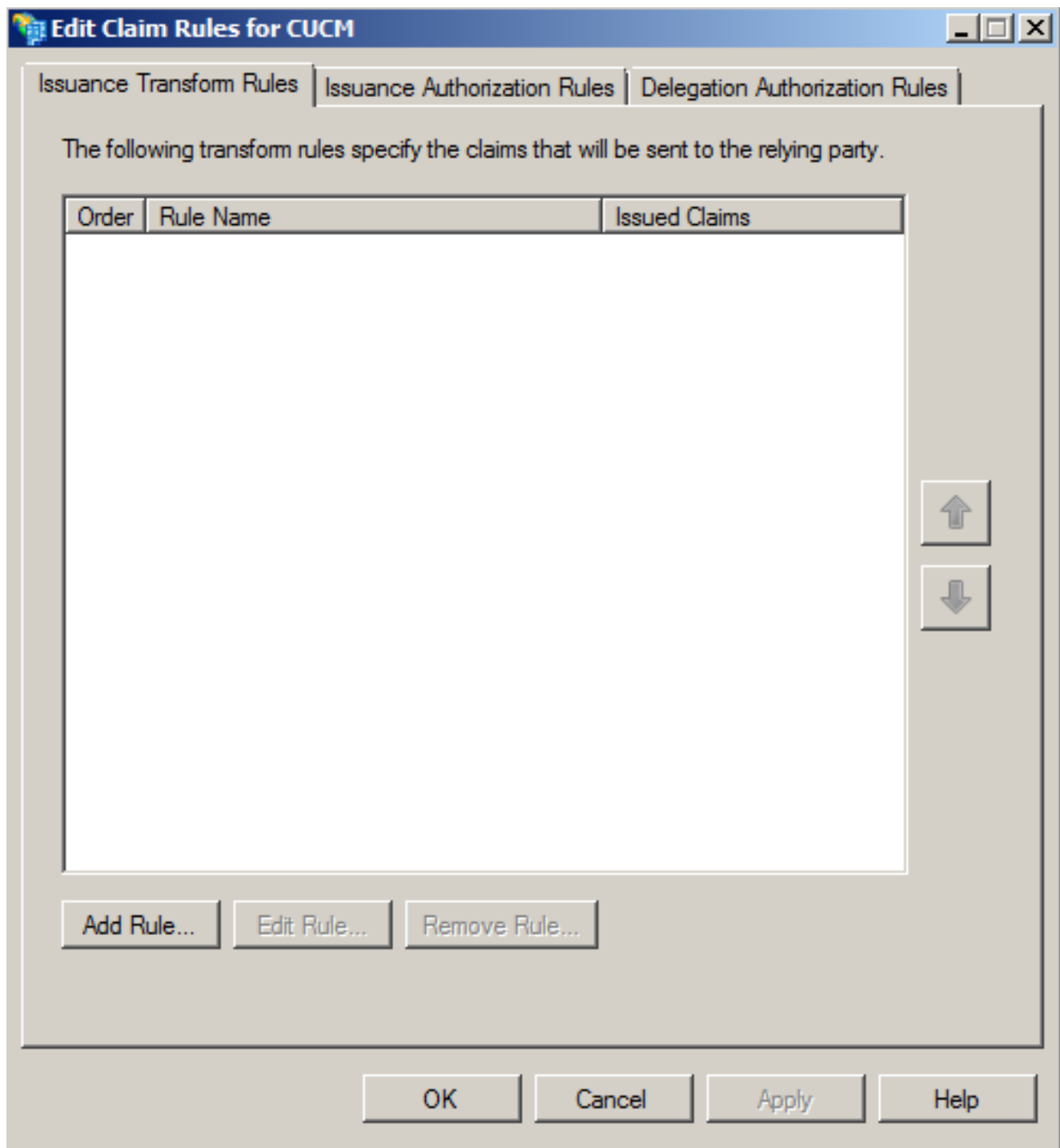
6. Choisissez l'autorisation tous les utilisateurs d'accéder à cet interlocuteur comptant et de cliquer sur Next.



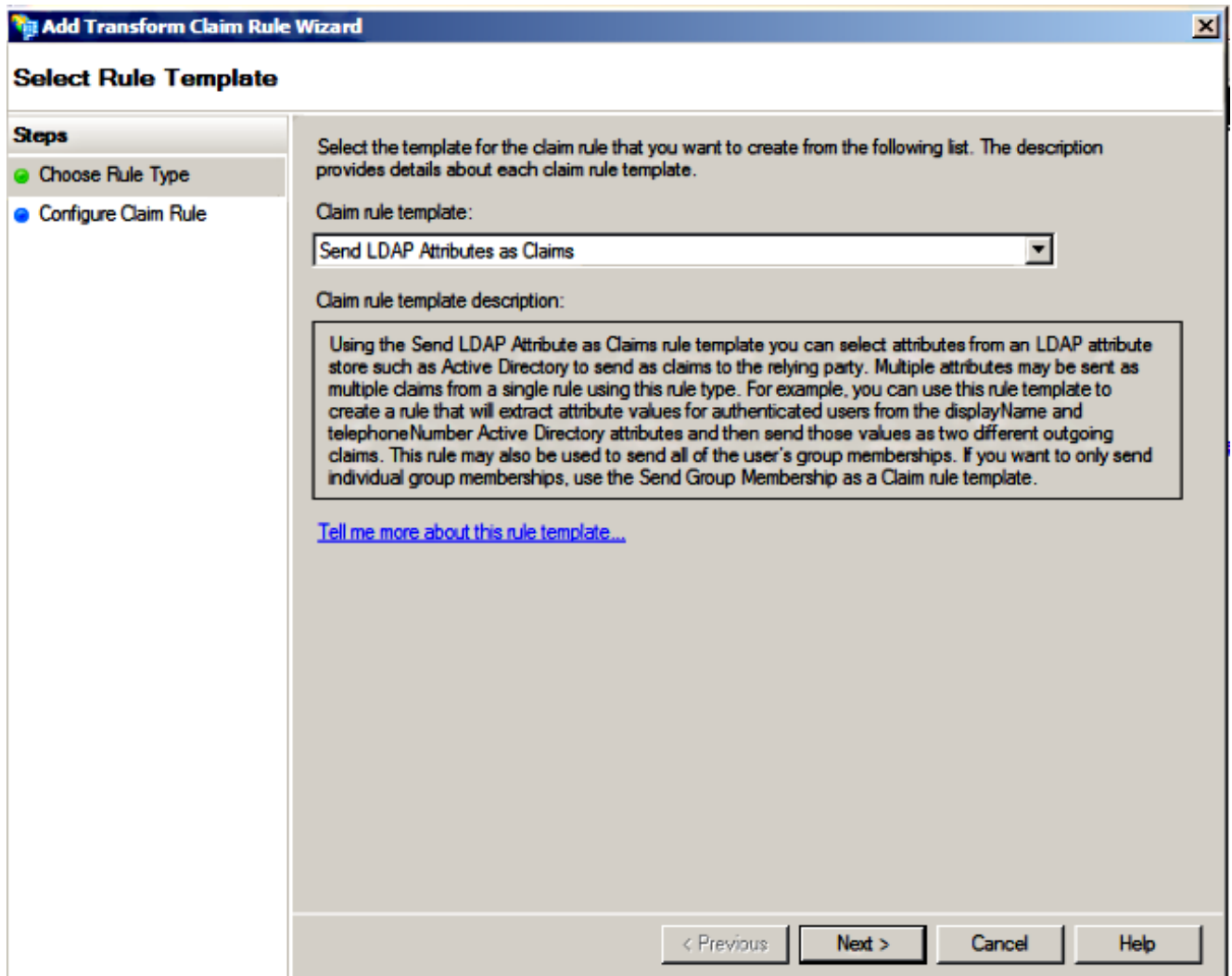
7. Choisissez les règles de demande d'édition de dialogue pour la confiance comptable d'interlocuteur de thé quand l'assistant se ferme et cliquez sur **étroitement**.



8. Cliquez sur Add la règle.



9. Cliquez sur Next avec le positionnement par défaut de modèle de règle de demande **pour envoyer des attributs de LDAP comme demandes.**



10. Dans configurez la règle, écrivez le nom de règle de demande, **Répertoire actif** choisi pendant que la mémoire d'attribut, configurent l'**attribut de LDAP** et le **type sortant de demande** suivant les indications de cette image, et cliquez sur Finish.

Note:

- L'attribut de Protocole LDAP (Lightweight Directory Access Protocol) devrait apparier l'attribut de sync de répertoire sur CUCM.
- le « uid » devrait être en minuscules.

Add Transform Claim Rule Wizard

Configure Rule

Steps

- Choose Rule Type
- Configure Claim Rule

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name:
Name ID

Rule template: Send LDAP Attributes as Claims

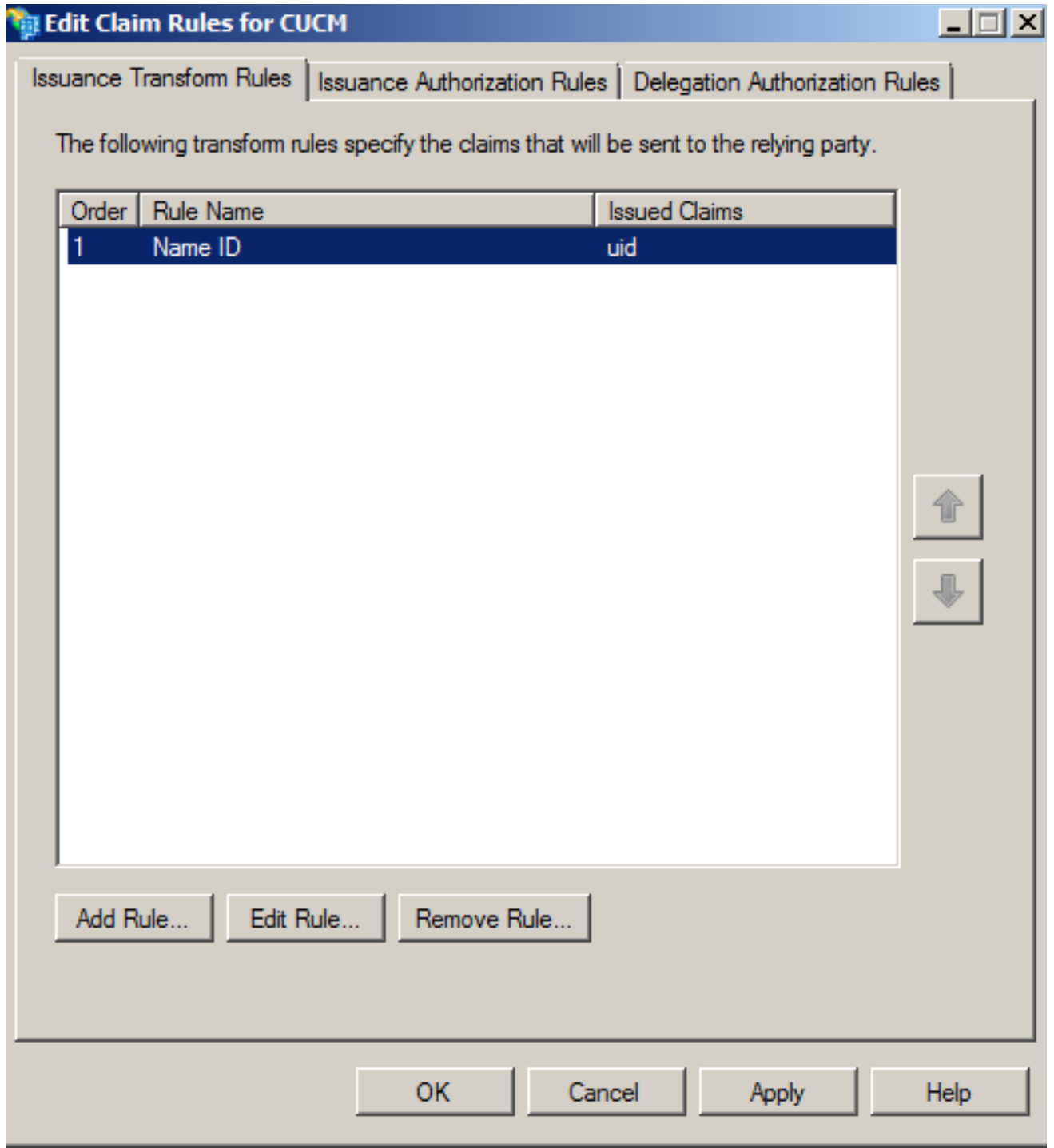
Attribute store:
Active Directory

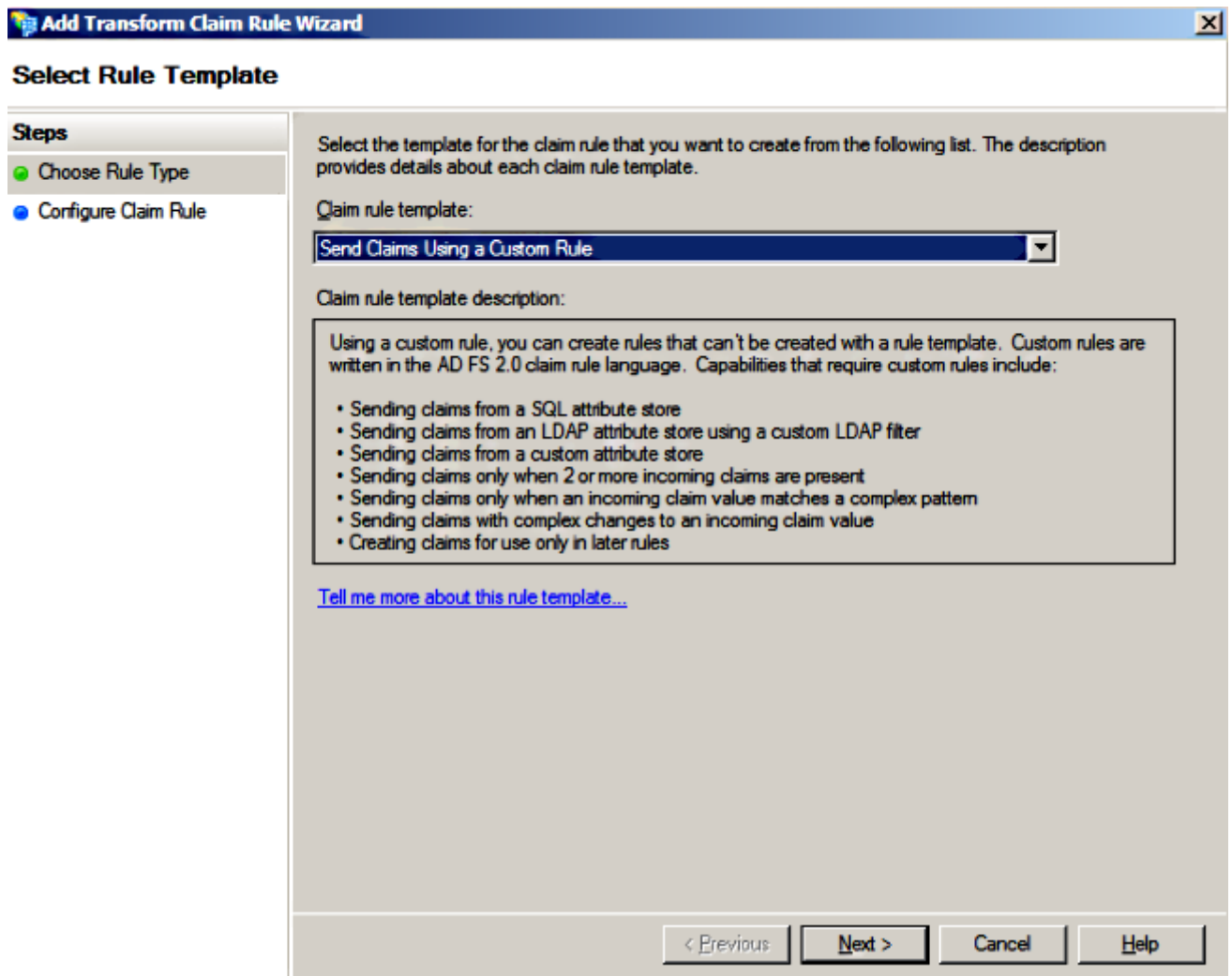
Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute	Outgoing Claim Type
▶	SAM-Account-Name	uid
*		

< Previous Finish Cancel Help

11. Cliquez sur Add la règle, choisie **envoyez les demandes utilisant une règle faite sur commande** pendant que le modèle de règle de demande, et cliquez sur Next.

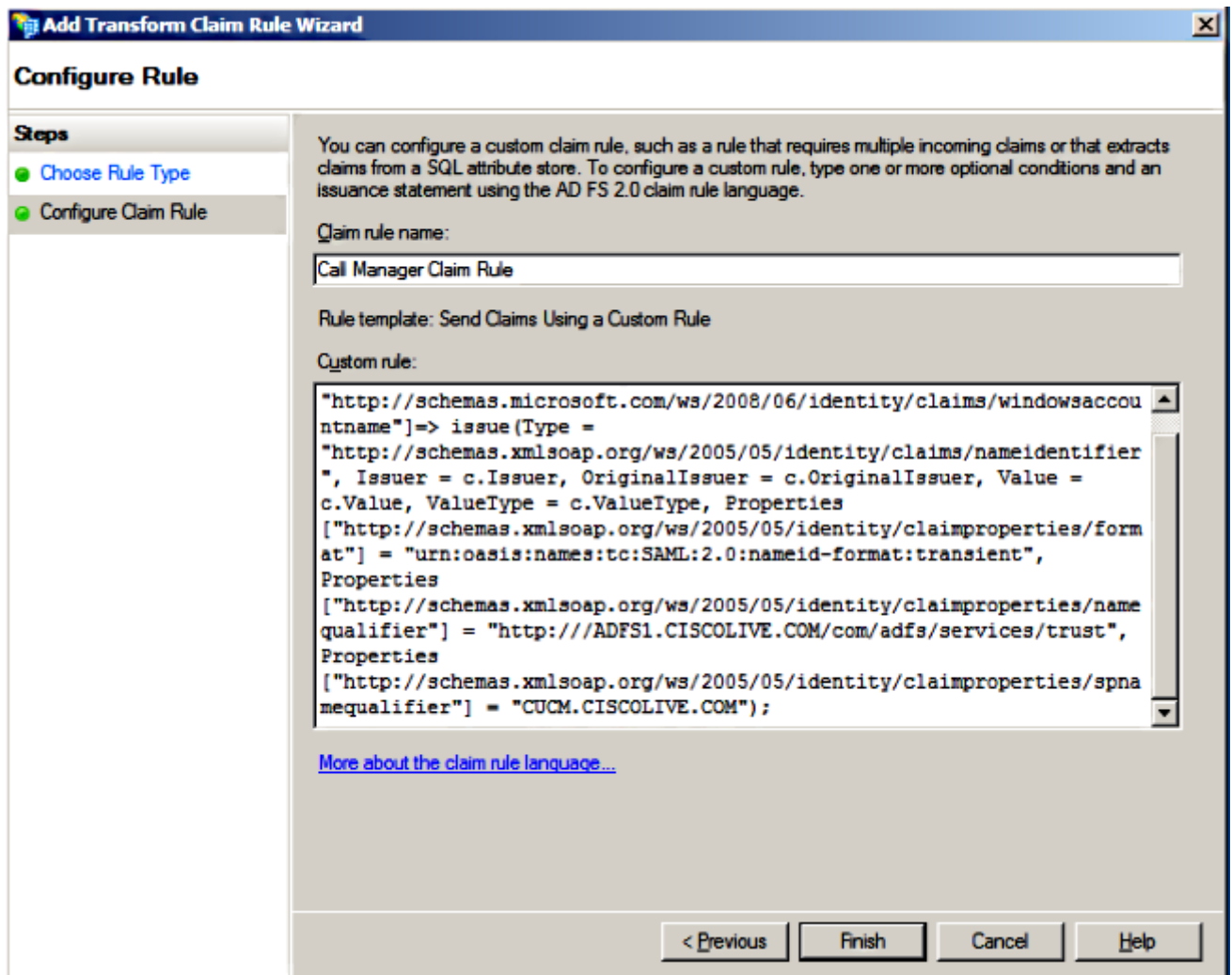




12. Écrivez un nom pour le nom de règle de demande et copiez cette syntaxe dans l'espace donné selon la règle faite sur commande :

```
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"]=>
issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier",
Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = 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://<FQDN of ADFS>/com/adfs/services/trust",
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier
"] = "<FQDN of CUCM>");
```

(NOTE : Si vous copiez et collez le texte de ces exemples, rendez-vous compte que du logiciel de traitement substituera les guillemets ASCII (") avec les versions d'UNICODE ("). Les versions d'UNICODE entraîneront la règle de demande d'échouer.)



Note:

- Le nom de domaine complet CUCM et ADFS (FQDN) prepopulated avec le laboratoire CUCM et l'AD FS dans cet exemple et doit être modifié pour appairer votre environnement.
- le FQDN de CUCM/ADFS distinguent les majuscules et minuscules et doivent appairer avec les fichiers de métadonnées.

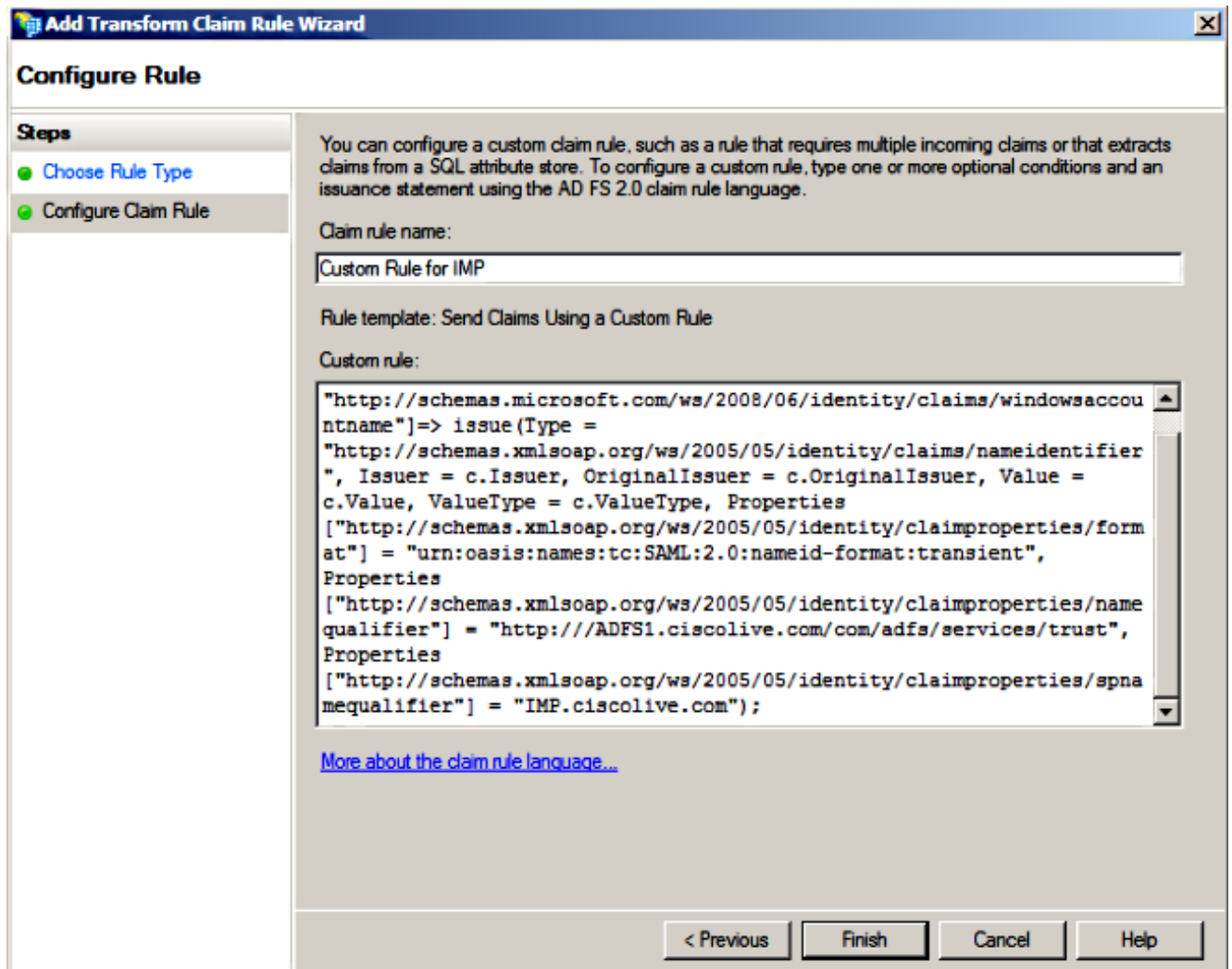
13. Cliquez sur **Finish** (Terminer).
14. Cliquez sur Apply et puis **APPROUVEZ**.
15. Redémarrez le service de version 2.0 FS d'AD de **Services.msc**.

Ajoutez CUCM IM et présence comme confiance comptante d'interlocuteur

1. Répétez les étapes 1 11 comme décrit pour **Add CUCM comme confiance comptante d'interlocuteur** et passez à l'étape 2.
2. Écrivez un nom pour le nom de règle de demande et copiez cette syntaxe dans l'espace donné selon la règle faite sur commande :

```
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"]=> issue (Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier", Issuer
```

```
= c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = 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://<FQDN of ADFS>/com/adfs/services/trust",
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"
] = "<FQDN of IMP>");
```



Notez qu'IM et FQDN FS de présence et d'AD prepopulated avec le laboratoire IM et la présence et l'AD FS dans cet exemple et doivent être modifiés pour apparier votre environnement.

3. Cliquez sur **Finish** (Terminer).
4. Cliquez sur Apply et puis **APPROUVEZ**.
5. Redémarrez le service de version 2.0 FS d'AD de **Services.msc**.

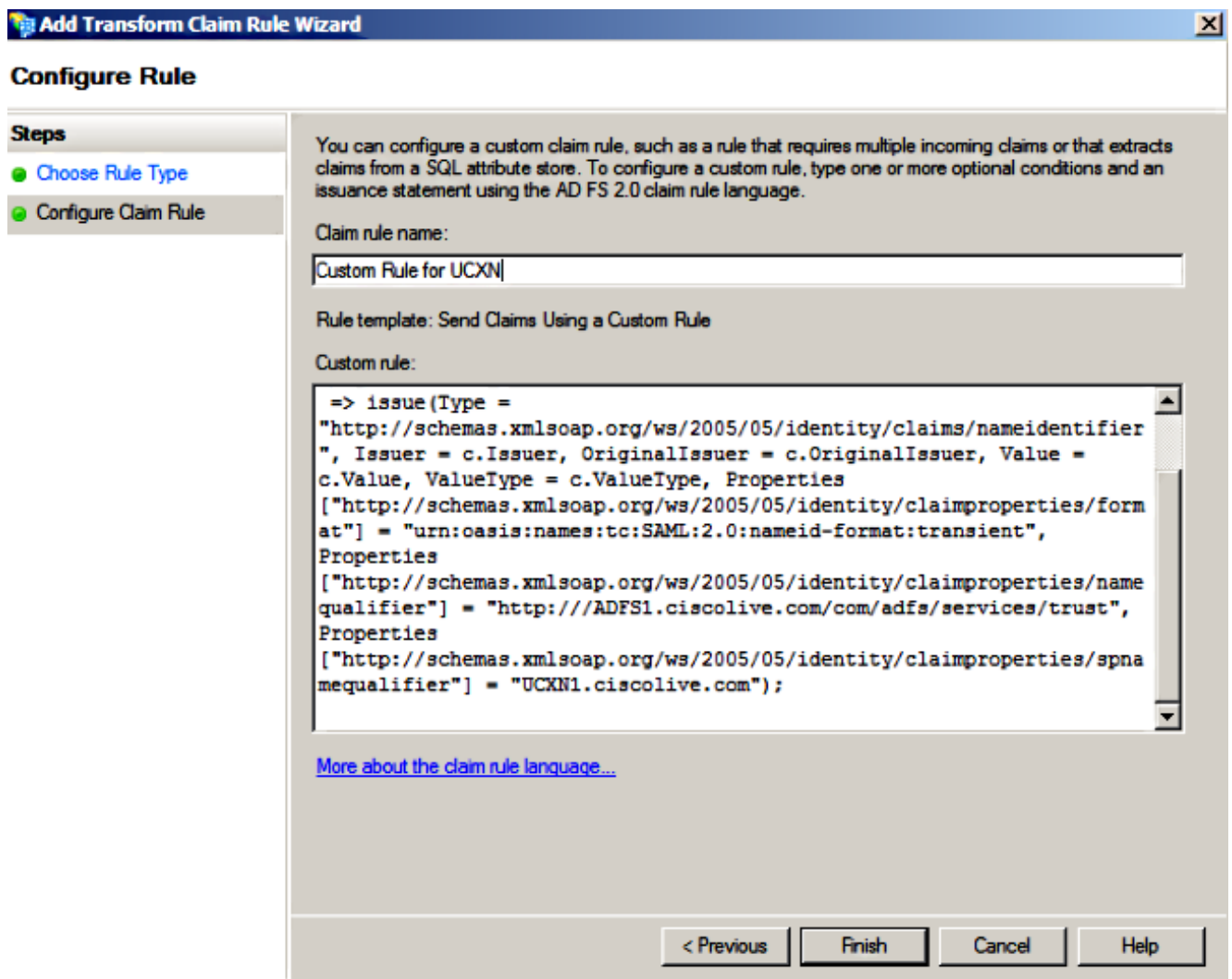
Ajoutez UCXN comme confiance comptante d'interlocuteur

1. Répétez les étapes 1 12 comme décrit pour **Add CUCM** comme confiance comptante

d'interlocuteur et passez à l'étape 2.

2. Écrivez un nom pour le nom de règle de demande et copiez cette syntaxe dans l'espace donné selon la règle faite sur commande :

```
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"]=>
issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier", Issuer =
c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = 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://<FQDN of ADFS>/com/adfs/services/trust",
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"
] = "<FQDN of UCXN>");
```



Notez qu'UCXN et FQDN FS d'AD prepopulated avec le laboratoire UCXN et ADFS dans cet exemple et doivent être modifiés pour apparier votre environnement.

3. Cliquez sur **Finish** (Terminer).
4. Cliquez sur Apply et puis **APPROUVEZ**.

5. Redémarrez le service de version 2.0 FS d'AD de **Services.msc**.

Ajoutez le ravitaillement principal de Collaboration de Cisco comme confiance comptante d'interlocuteur

1. Répétez les étapes 1 12 comme décrit pour **Add CUCM comme confiance comptante d'interlocuteur** et passez à l'étape 2.
2. Écrivez un nom pour le nom de règle de demande et copiez cette syntaxe dans l'espace donné selon la règle faite sur commande :

```
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"]=>
issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier", Issuer =
c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = 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://<FQDN of ADFS>/com/adfs/services/trust",
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"
] = "<FQDN of PCP>");
```

Add Transform Claim Rule Wizard

Configure Rule

Steps

- Choose Rule Type
- Configure Claim Rule

You can configure a custom claim rule, such as a rule that requires multiple incoming claims or that extracts claims from a SQL attribute store. To configure a custom rule, type one or more optional conditions and an issuance statement using the AD FS 2.0 claim rule language.

Claim rule name:
Custom Rule for PCP

Rule template: Send Claims Using a Custom Rule

Custom rule:

```
ntname"]
=> issue (Type =
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier
", Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value =
c.Value, ValueType = c.ValueType, Properties
["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/form
at"] = "urn:oasis:names:tc:SAML:2.0:nameid-format:transient",
Properties
["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/name
qualifier"] = "http://ADFS1.ciscolive.com/com/adfs/services/trust",
Properties
["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spna
mequalifier"] = "PCP.ciscolive.com");
```

[More about the claim rule language...](#)

< Previous Finish Cancel Help

Notez que le FQDN FS de ravitaillement et d'AD de perfection prepopulated avec le

ravitaillement de Collaboration de perfection de laboratoire (PCP) et l'AD FS de cet exemple et doit être modifié pour appairer votre environnement.

3. Cliquez sur **Finish** (Terminer).
4. Cliquez sur Apply et puis **APPROUVEZ**.
5. Redémarrez le service de version 2.0 FS d'AD de **Services.msc**.

Une fois que vous installez la version 2.0 FS d'AD, poursuivez pour activer SAML SSO sur des Produits de Cisco Collaboration.

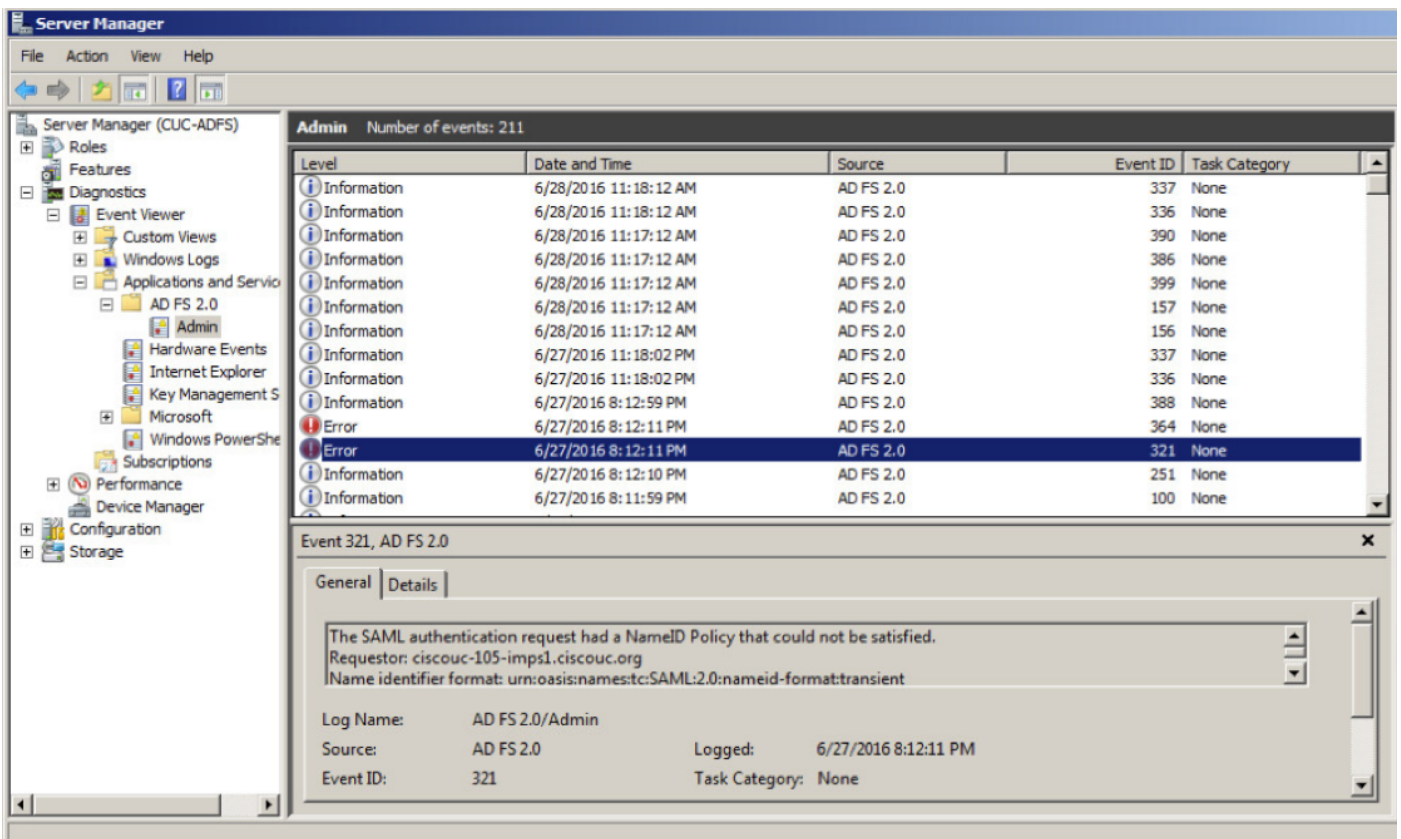
Vérifiez

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannez

L'AD FS se connecte des données diagnostiques au journal d'événements de système. Du gestionnaire du serveur sur le serveur FS d'AD ouvrez les **diagnostics - > visualisateur d'événements - > des applications et des services - > l'AD FS 2.0 - > admin**

Recherchez les erreurs connectées pour l'activité FS d'AD



Server Manager (CUC-ADFS)

Admin Number of events: 211

Level	Date and Time	Source	Event ID	Task Category
Information	6/28/2016 11:18:12 AM	AD FS 2.0	337	None
Information	6/28/2016 11:18:12 AM	AD FS 2.0	336	None
Information	6/28/2016 11:17:12 AM	AD FS 2.0	390	None
Information	6/28/2016 11:17:12 AM	AD FS 2.0	386	None
Information	6/28/2016 11:17:12 AM	AD FS 2.0	399	None
Information	6/28/2016 11:17:12 AM	AD FS 2.0	157	None
Information	6/28/2016 11:17:12 AM	AD FS 2.0	156	None
Information	6/27/2016 11:18:02 PM	AD FS 2.0	337	None
Information	6/27/2016 11:18:02 PM	AD FS 2.0	336	None
Information	6/27/2016 8:12:59 PM	AD FS 2.0	388	None
Error	6/27/2016 8:12:11 PM	AD FS 2.0	364	None
Error	6/27/2016 8:12:11 PM	AD FS 2.0	321	None
Information	6/27/2016 8:12:10 PM	AD FS 2.0	251	None
Information	6/27/2016 8:11:59 PM	AD FS 2.0	100	None

Event 321, AD FS 2.0

General Details

The SAML authentication request had a NameID Policy that could not be satisfied.
Requestor: ciscouc-105-imps1.ciscouc.org
Name identifier format: urn:oasis:names:tc:SAML:2.0:nameid-format:transient

Log Name: AD FS 2.0/Admin
Source: AD FS 2.0
Event ID: 321

Logged: 6/27/2016 8:12:11 PM
Task Category: None