Configurer l'autorisation locale PCCE

Contenu

Introduction

Ce document décrit les étapes nécessaires pour supprimer la dépendance de Microsoft Active Directory (AD) afin de gérer l'autorisation localement dans les composants du centre de contact de package Enterprise (PCCE).

Contribué par Meenakshi Sundaram, Ramiro Amaya et Anuj Bhatia, ingénieurs du TAC Cisco.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco Package Contact Center Enterprise
- Microsoft Active Directory

Components Used

Les informations utilisées dans le document sont basées sur la version PCCE 12.5(1).

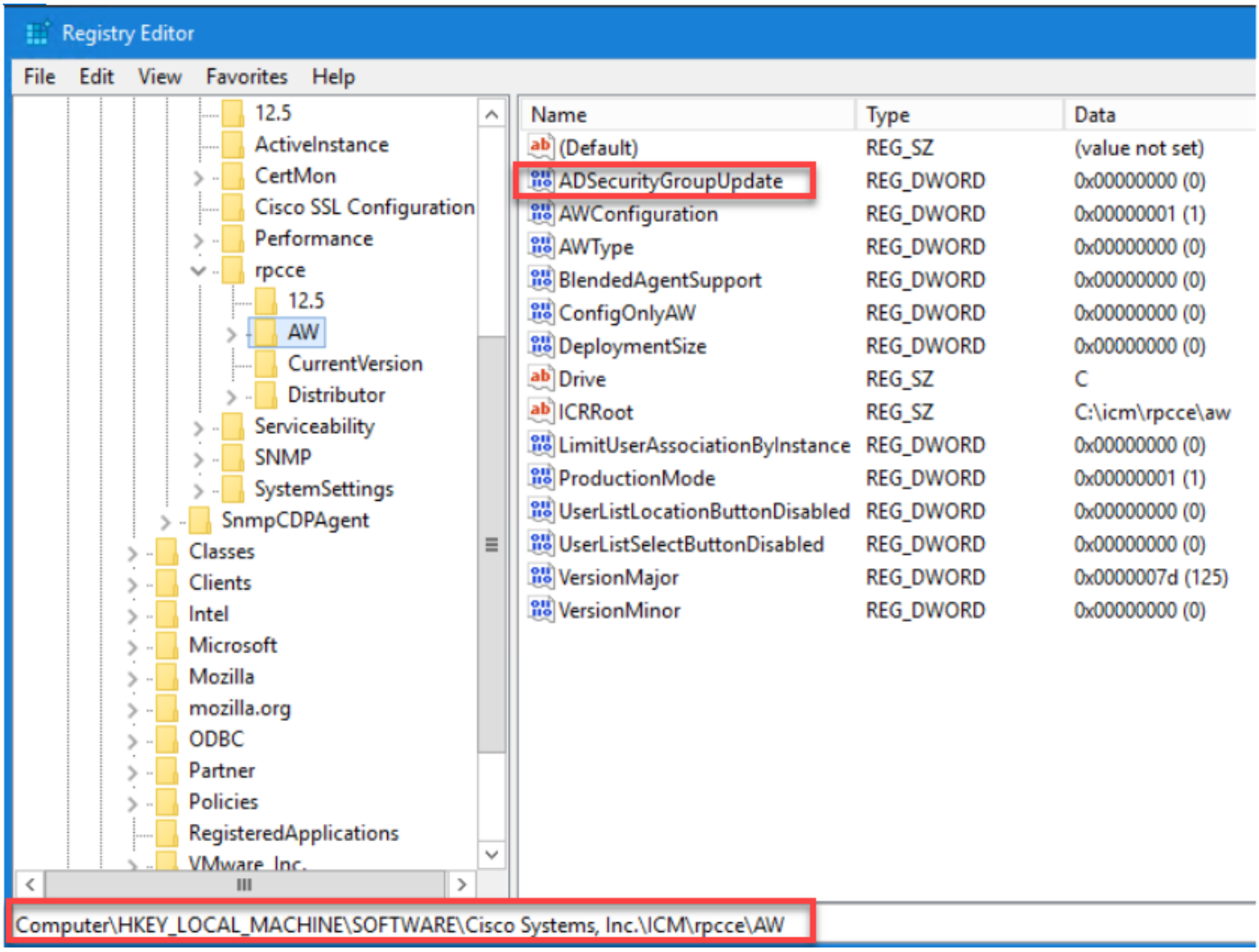
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est actif, assurez-vous de bien comprendre l'impact potentiel de n'importe quelle étape.

Informations générales

La version PCCE 12.5 fournit des privilèges utilisateur aux groupes d'utilisateurs locaux sur les

serveurs d'administration (AW), ce qui permet aux utilisateurs de déplacer l'autorisation hors d'Active Directory (AD). Ceci est contrôlé par le Registre **ADSecSecurityGroupUpdate** qui par défaut est activé et évite l'utilisation de groupes de sécurité Microsoft AD pour contrôler les droits d'accès des utilisateurs pour effectuer des tâches de configuration et de configuration.

> **Note**: La prise en charge de l'autorisation locale a commencé dans Unified Contact Center Enterprise (UCCE) 12.0 et est désormais prise en charge dans PCCE 12.5.



> **Note**: Si l'entreprise a besoin que le comportement antérieur soit implémenté (autorisation AD), l'indicateur ADSecSecurityGroupUpdate peut être changé en 1.

Configuration

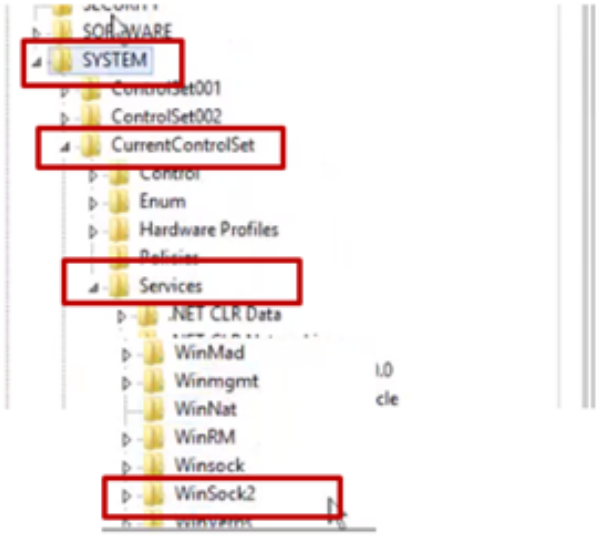
Pour octroyer des autorisations de groupe UcceConfig dans un serveur AW local, vous devez d'abord fournir des autorisations au niveau du Registre, puis au niveau du dossier.

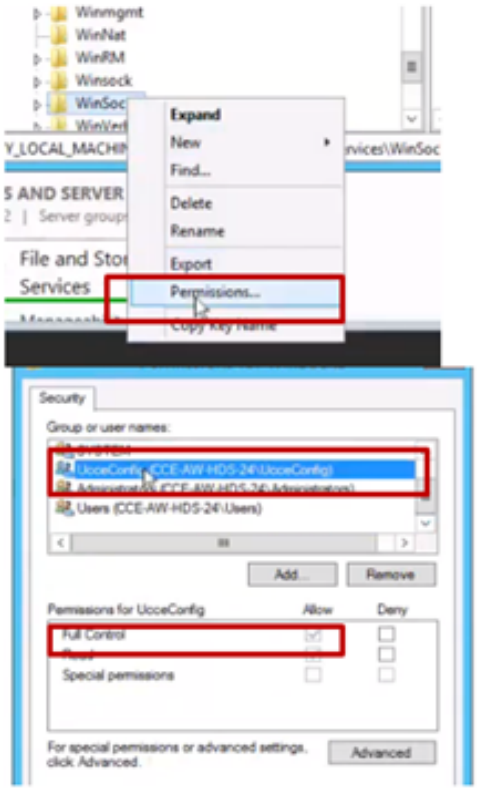
Étape 1. Configurez les autorisations du Registre.

1. Exécutez l'utilitaire regedit.exe.

2. Sélectionnez **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\WinSock2**.

3. Dans Autorisations sous l'onglet Sécurité, sélectionnez **UcceConfig** group et cochez **Autoriser l'**option **Contrôle total**.





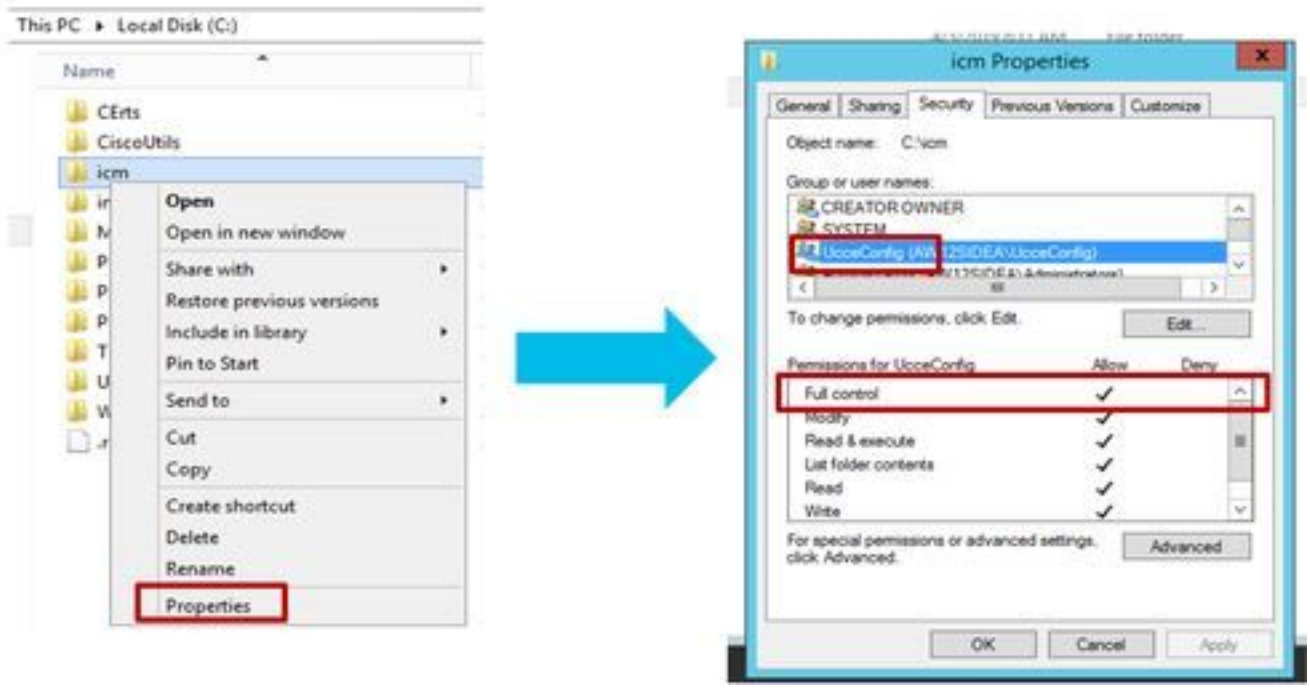
4. Répétez les étapes précédentes pour accorder un contrôle total au groupe UcceConfig pour ces registres.

- **Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, inc.\ICM**
- **Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Cisco Systems, inc.\ICM**

Étape 2. Configurez les autorisations de dossier.

1. Dans l'Explorateur Windows, accédez à <Répertoire installé ICM>:\icm et sélectionnez Propriétés.

2. Dans l'onglet Sécurité, sélectionnez **UcceConfig** et cochez **Autoriser l'**option **Contrôle total**.



3. Cliquez sur OK pour enregistrer les modifications.

4. Répétez les étapes précédentes pour accorder un contrôle total au groupe **UcceConfig** pour C:\Temp folder.

5. Dans SQL Management Studio, procédez comme suit :

a) Accédez à Security > Logins.

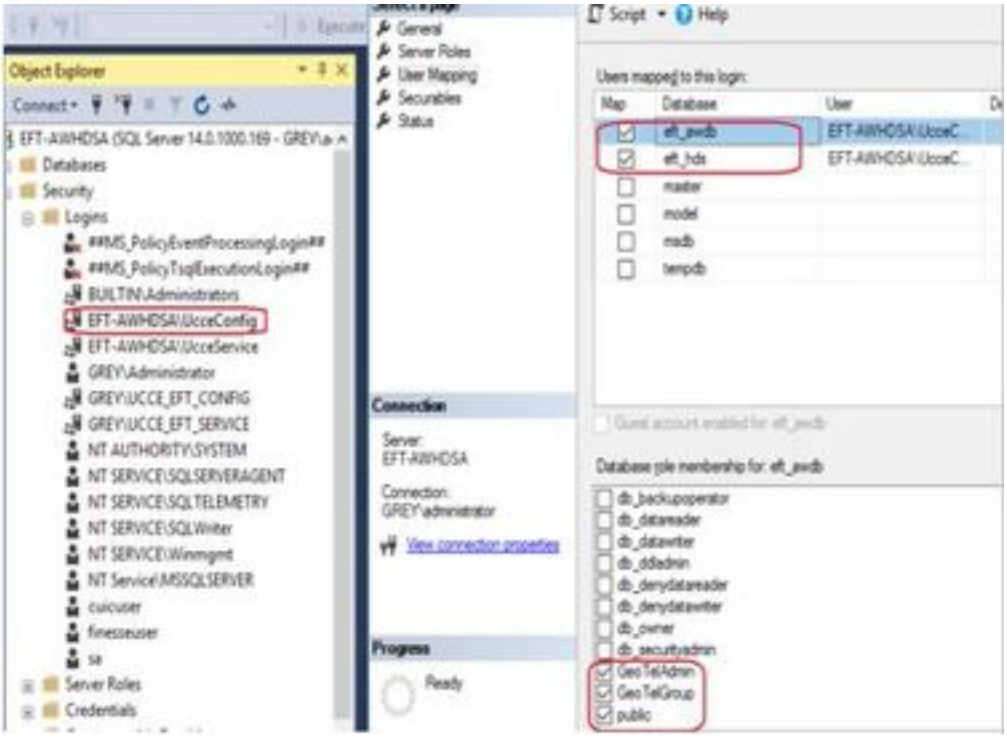
b) Recherchez <Nom de la machine>\UcceConfig.

c) Cliquez avec le bouton droit de la souris et sélectionnez propriétés.

d) Naviguez dans Mappages utilisateur et sélectionnez la base de données AWDB.

e) Cochez les cases GeoTelAdmin, GeoTelGroup et public.

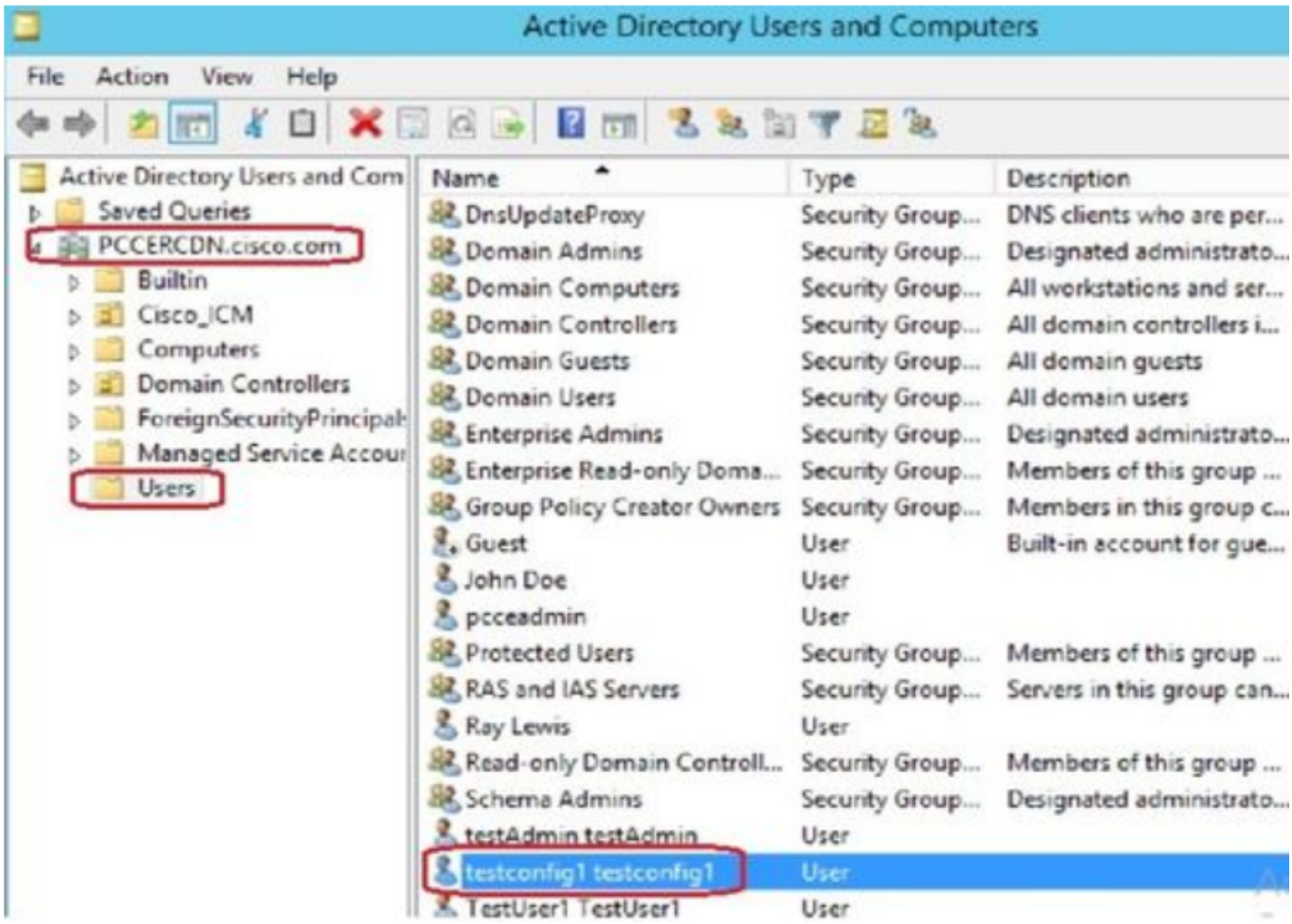
f) Répétez l'étape d) pour la base de données des données historiques (HDS).

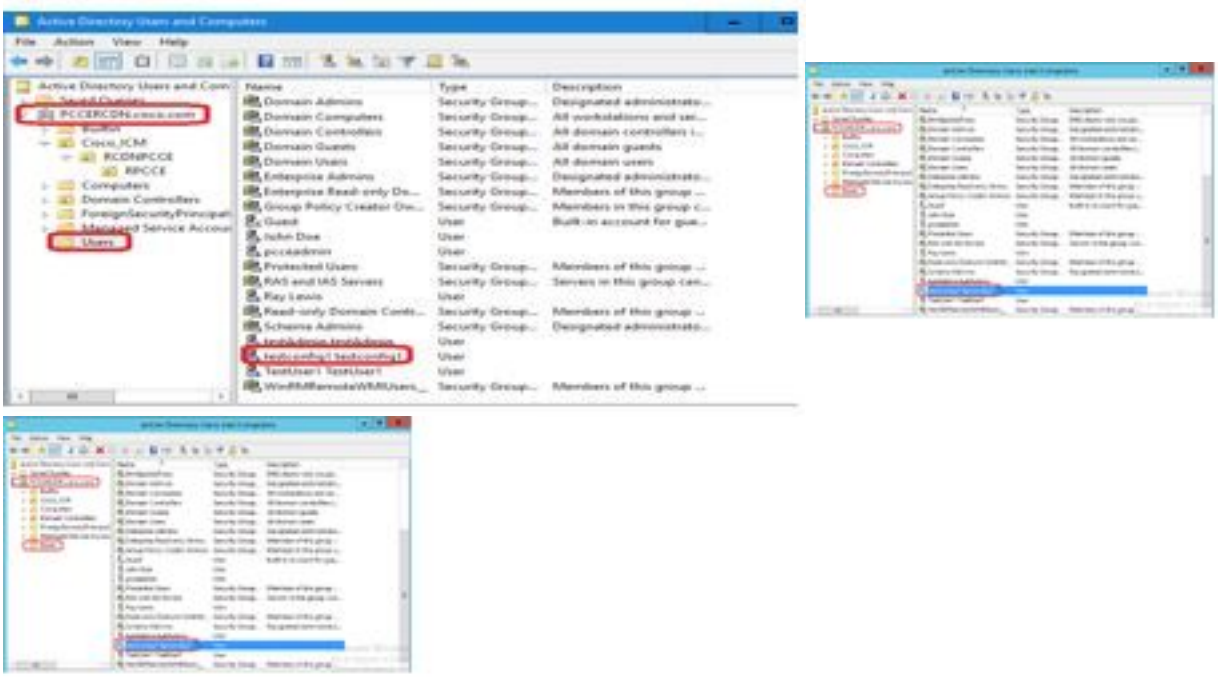


Lorsque la configuration préliminaire a été effectuée, suivez les étapes de promotion d'un utilisateur de domaine afin d'avoir des droits de configuration et de configuration.

Étape 3. Configuration de l'utilisateur du domaine.

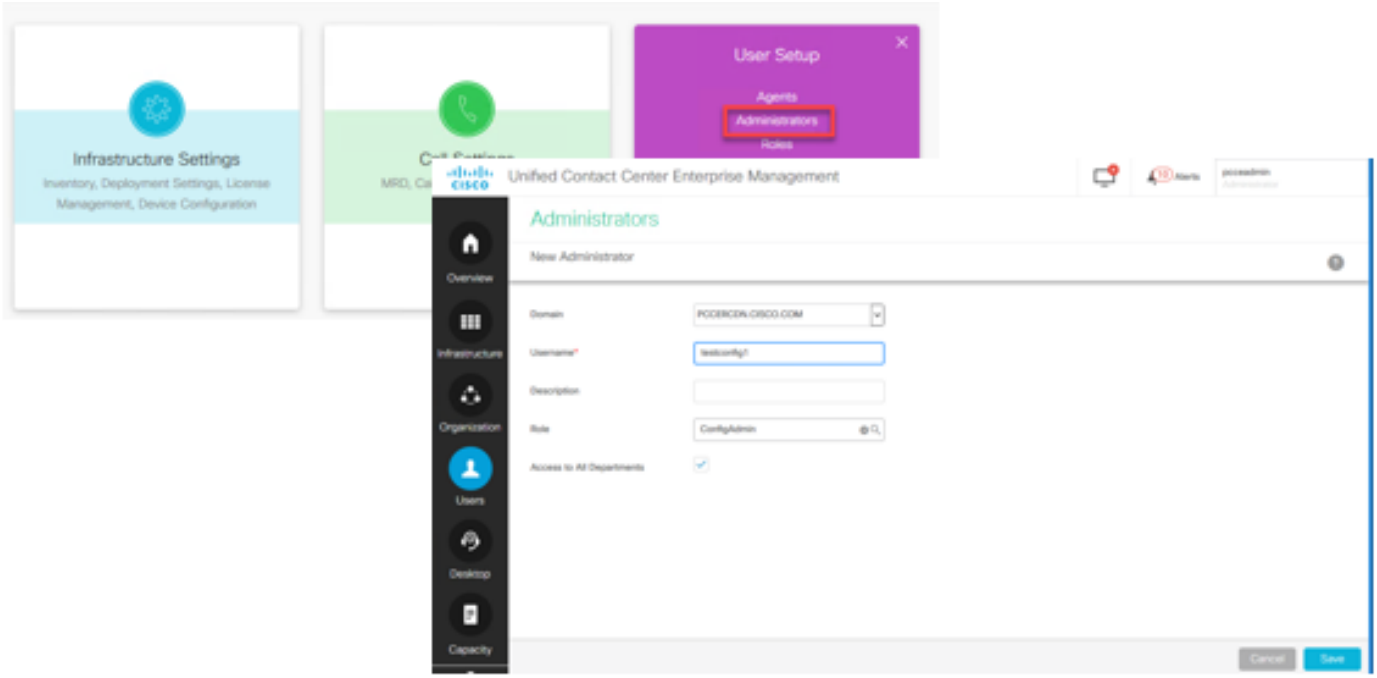
1. Créez un utilisateur de domaine dans AD. Pour cet exercice, l'utilisateur testconfig1 a été créé.



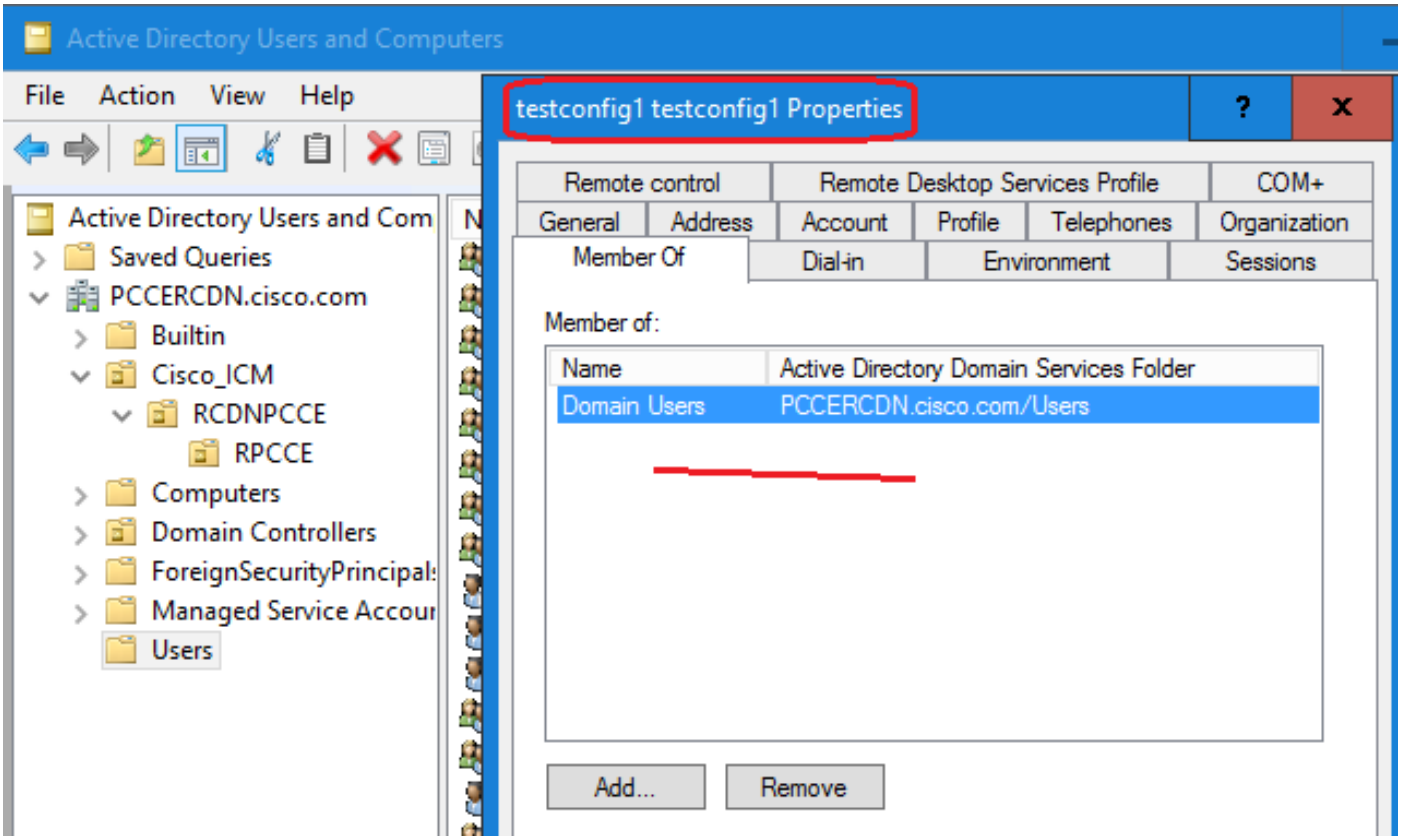


2. Connectez-vous au serveur AW avec un compte d'administrateur de domaine ou d'administrateur local.

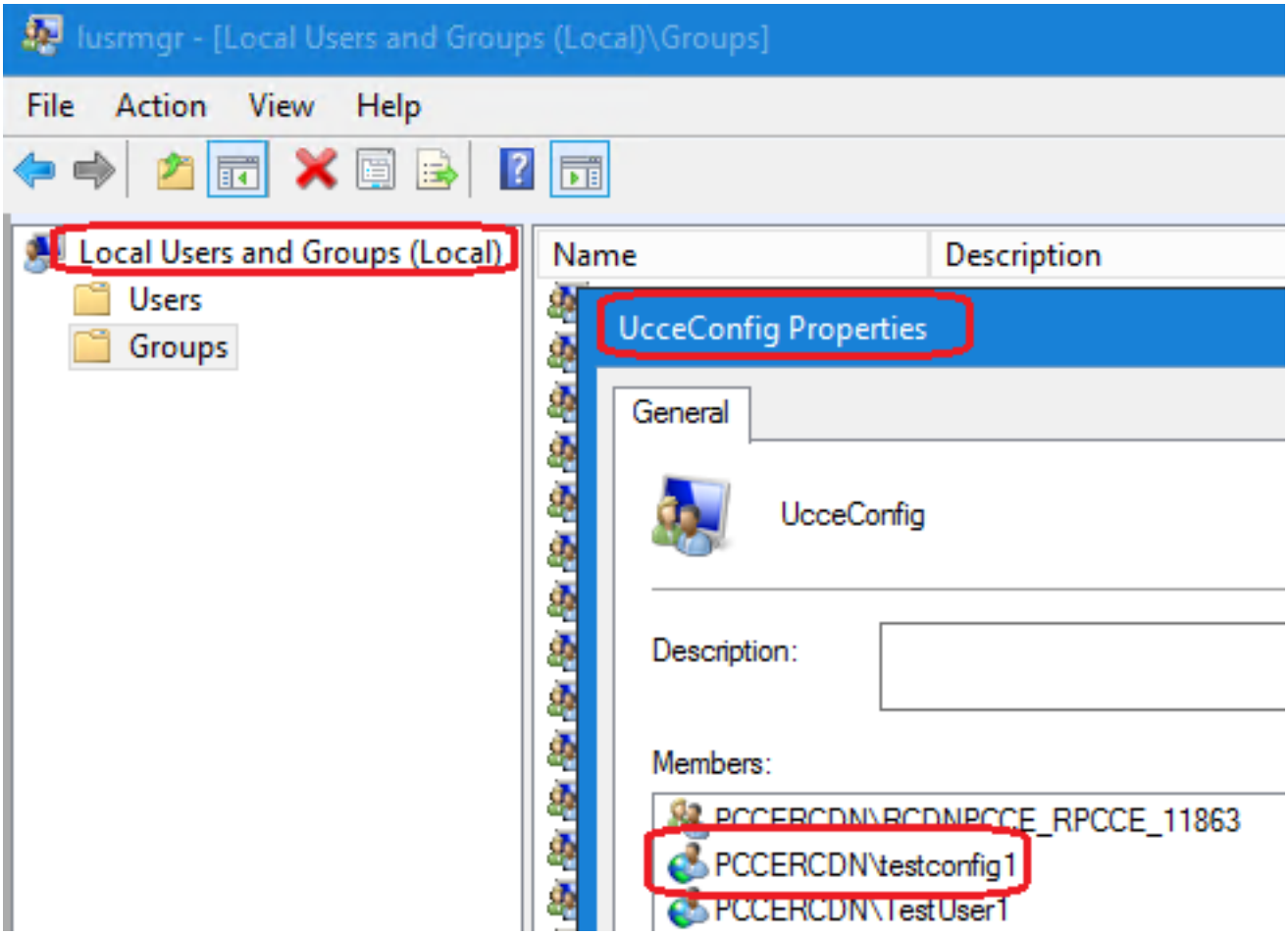
3. Ouvrez l'administrateur CCE sur l'AW. Accédez à la carte User Setup, puis sélectionnez Administrators. Ajoutez l'utilisateur et sélectionnez le rôle **ConfigAdmin**.



Avant la version 12.5 de PCCE, cette modification aurait mis à jour les groupes de sécurité Config dans le domaine sous une unité d'organisation (OU) d'instance, mais avec la version 12.5, le comportement par défaut est de ne pas ajouter cet utilisateur au groupe AD. Comme l'illustre l'image, il n'y a aucune mise à jour de cet utilisateur dans le groupe de sécurité de configuration ICM du domaine.



4. Dans le serveur AW sous **Gestion de l'ordinateur > Utilisateurs et groupes locaux > Groupes**, sélectionnez UcceConfig et ajoutez l'utilisateur testconfig1 à celui-ci.

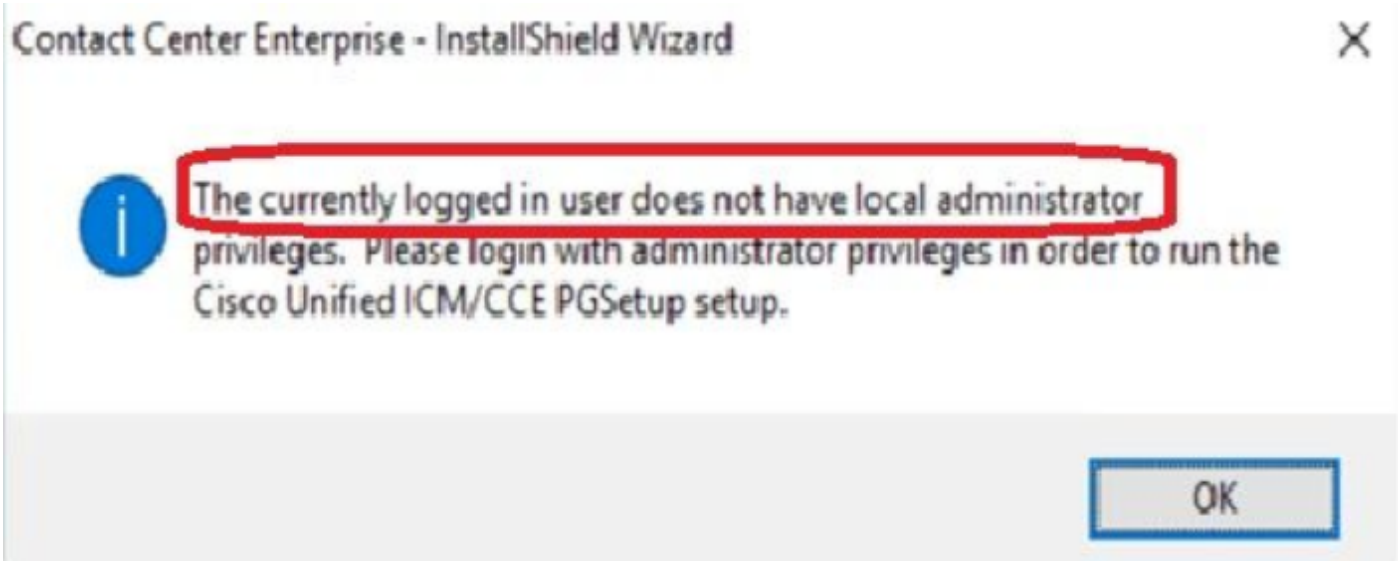


5. Déconnectez-vous de l'ordinateur et connectez-vous avec les informations d'identification de l'utilisateur testconfig1. Comme cet utilisateur dispose de droits de configuration, il peut exécuter

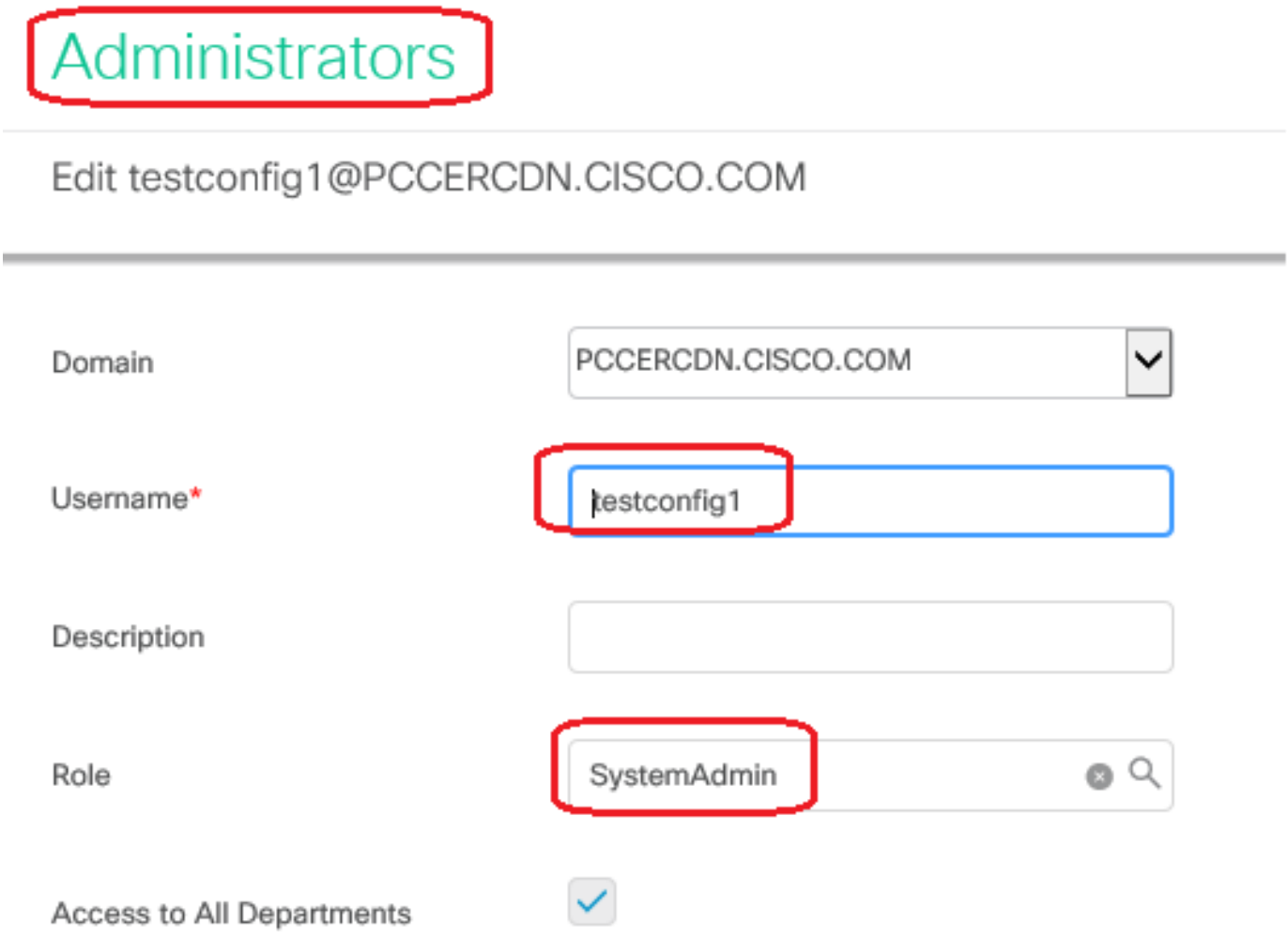
des outils de configuration CCE tels que CCE Admin, Script ou Internet Script Editor.

6. Cependant, si l'utilisateur tente d'exécuter une tâche qui nécessite des droits de configuration, elle échoue. Cet utilisateur n'a pas accès à toutes les ressources d'administration CCE ou aux outils de configuration.

Comme le montre l'image, l'utilisateur testconfig1 dans le déploiement PCCE 4K tente d'exécuter la configuration de la passerelle d'accès aux périphériques (PG) et le système limite la modification par un message d'avertissement.



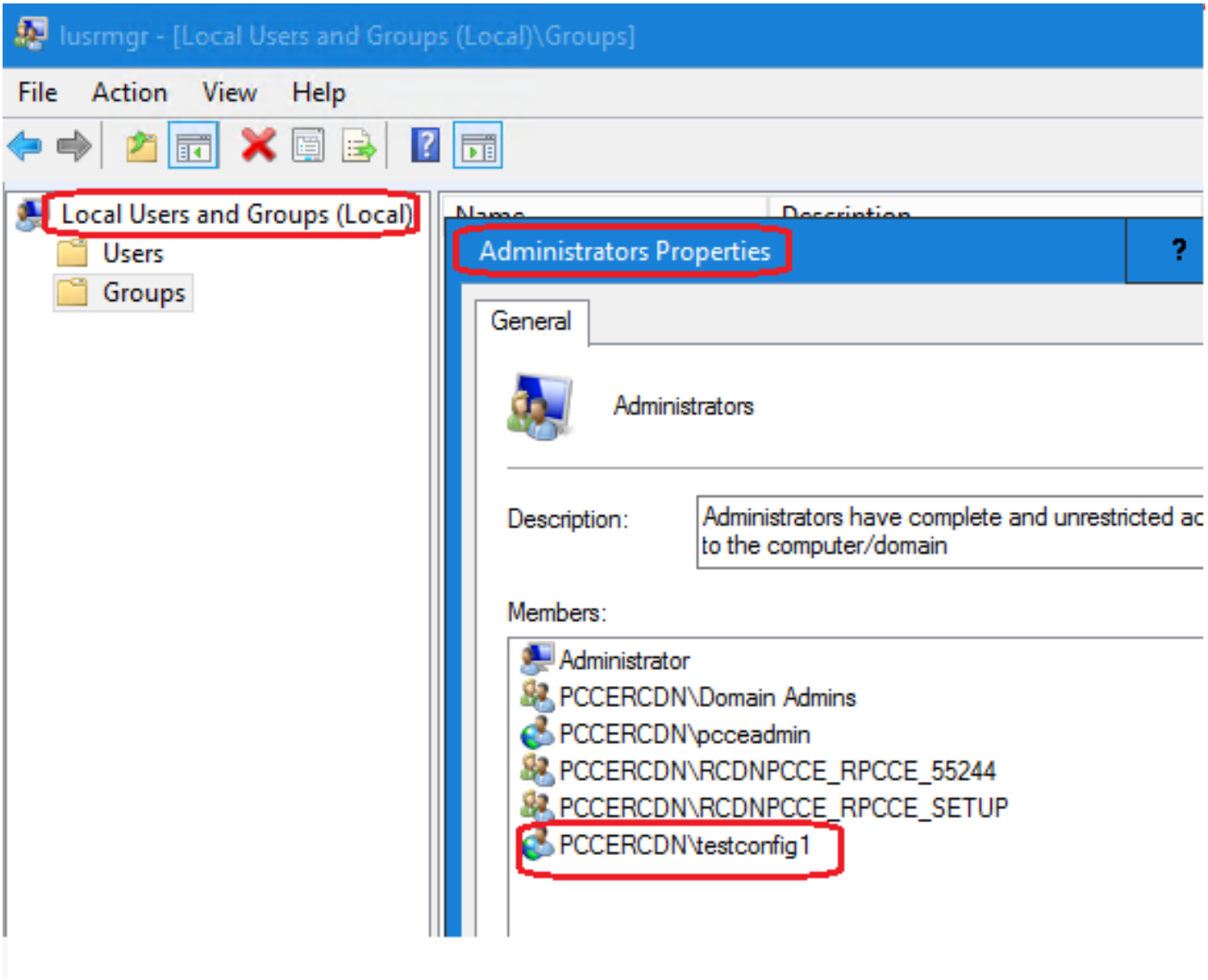
7. Si l'entreprise exige que cet utilisateur dispose de droits de configuration et de configuration, vous devez vous assurer que le rôle utilisateur est changé en SystemAdmin dans CCEAdmin.



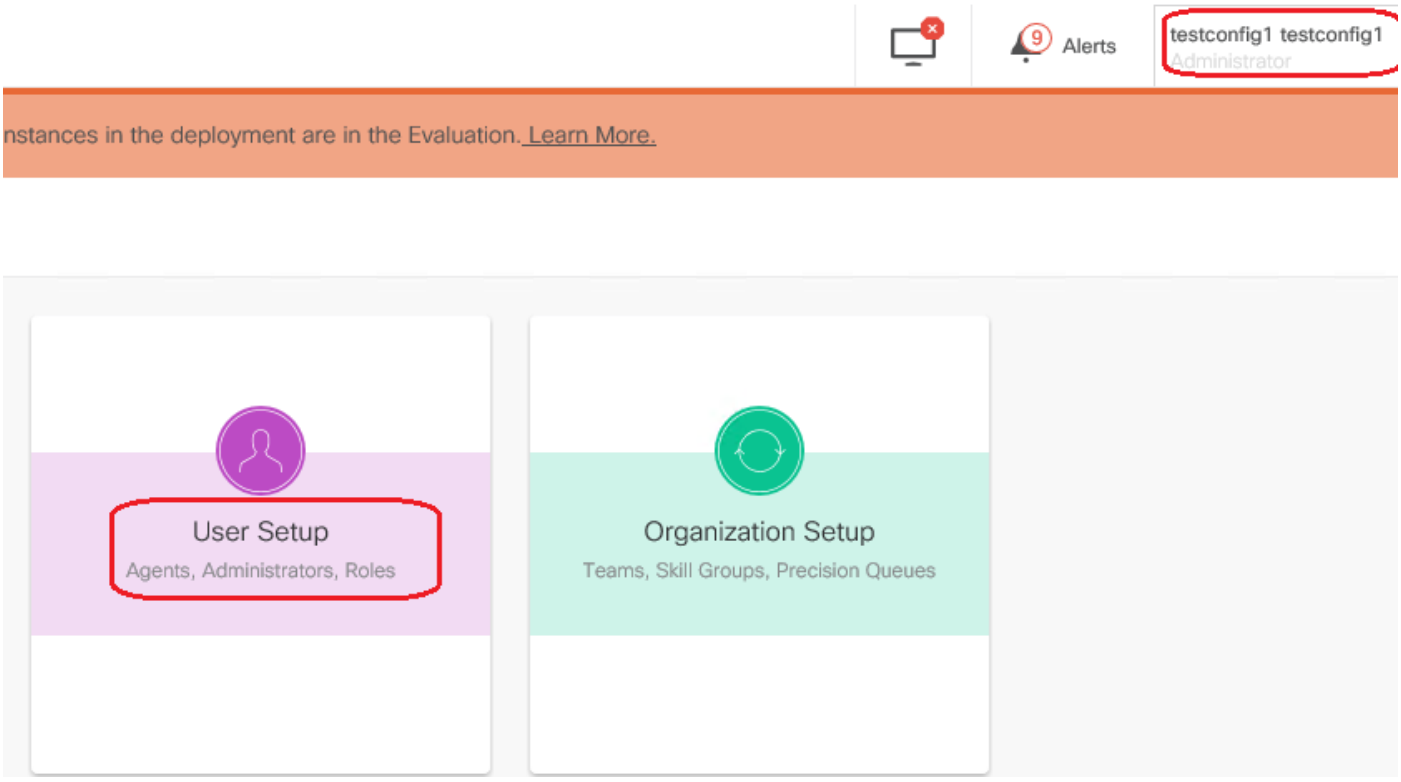
Le rôle utilisateur a été mis à jour en tant que 1 (SystemAdmin) dans la base de données :

	UserRole	UserGroupID	CustomerDefinitionID	UserGroupName	UserGroupType	Description	ServiceProvider	ReadOnly	FeatureSetID
1	0	1	NULL	DBO	U	The ICM System Administrator	Y	N	NULL
2	0	5000	NULL	PCCERCDN\RLEWIS	U	NULL	N	N	NULL
3	1	5002	NULL	PCCERCDN\TESTCONFIG1	U	NULL	N	N	5000
4	2	5001	NULL	PCCERCDN\TESTUSER1	U	NULL	N	N	5001

8. Connectez-vous au serveur AW avec le compte de droits d'administration du domaine ou local et via **la gestion de l'ordinateur > Utilisateurs et groupes locaux > groupes** sélectionnez Groupes et dans Administrateurs ajoutez l'utilisateur à l'utilisateur.



10. L'utilisateur peut désormais accéder à toutes les ressources de l'application CCE sur ce serveur AW et apporter les modifications souhaitées.



Vérification

La procédure de vérification fait en fait partie du processus de configuration.

Dépannage

Aucune étape spécifique n'est actuellement disponible pour dépanner cette configuration.

Informations connexes

Guide d'administration PCCE

Support et documentation techniques - Cisco Systems