

Configurez l'autorisation locale UCCE 12.0(X)

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Informations générales](#)

[Configurer](#)

[Étape 1. Configurez les autorisations de registre](#)

[Étape 2. Configurez les autorisations de répertoire](#)

[Vérifier](#)

[Dépanner](#)

Introduction

Ce document décrit les étapes requises pour retirer la dépendance du répertoire actif de Microsoft (AD) pour gérer l'autorisation dans des composants d'Unified Contact Center Enterprise (CCE).

Contribué par Anuj Bhatia, ingénieur TAC Cisco.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco Unified Contact Center Enterprise
- Microsoft Active Directory

[Composants utilisés](#)

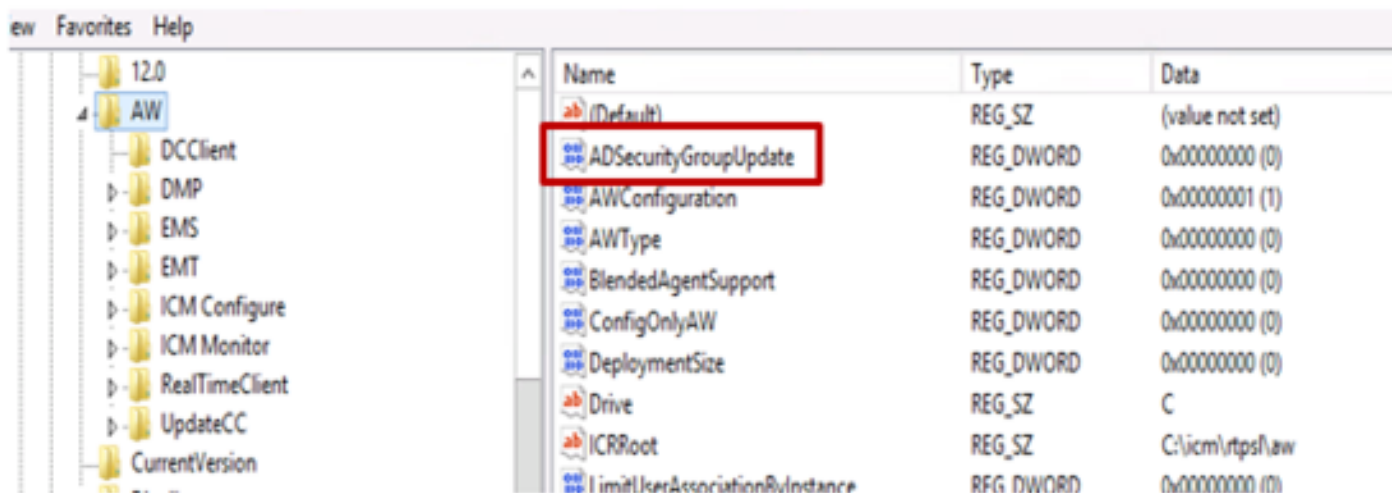
Les informations utilisées dans le document sont basées sur la version de la solution UCCE 12.0(1).

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 vivant, assurez-vous que vous comprenez l'impact potentiel de n'importe quelle étape.

[Informations générales](#)

La release UCCE 12.X fournit des privilèges d'adhésion d'utilisateur aux groupes d'utilisateur local sur le serveur de gestion local (aw), qui permet à des utilisateurs pour déplacer l'autorisation hors

du Répertoire actif (AD). Ceci est contrôlé par le registre **ADSecurityGroupUpdate** qui par le default est activé et évite l'utilisation des groupes de sécurité d'AD de Microsoft de contrôler des droits d'accès d'accès client d'effectuer des tâches d'installation et de configuration.



The screenshot shows the Windows Registry Editor with the left pane displaying a tree view of folders including '12.0', 'AW', 'DCClient', 'DMP', 'EMS', 'EMT', 'ICM Configure', 'ICM Monitor', 'RealTimeClient', 'UpdateCC', and 'CurrentVersion'. The right pane shows a list of registry values with columns for Name, Type, and Data. The 'ADSecurityGroupUpdate' value is highlighted with a red box. Its details are as follows:

Name	Type	Data
(Default)	REG_SZ	(value not set)
ADSecurityGroupUpdate	REG_DWORD	0x00000000 (0)
AWConfiguration	REG_DWORD	0x00000001 (1)
AWType	REG_DWORD	0x00000000 (0)
BlendedAgentSupport	REG_DWORD	0x00000000 (0)
ConfigOnlyAW	REG_DWORD	0x00000000 (0)
DeploymentSize	REG_DWORD	0x00000000 (0)
Drive	REG_SZ	C
ICRRoot	REG_SZ	C:\icm\rtpsf\aw
LimitUserAssociationInstance	REG_DWORD	0x00000000 (0)

Remarque: Si l'entreprise souhaite choisir le comportement antérieur, l'indicateur d'ADSecurityGroupUpdate peut être changé à 1 qui permet mis à jour au Répertoire actif (AD)

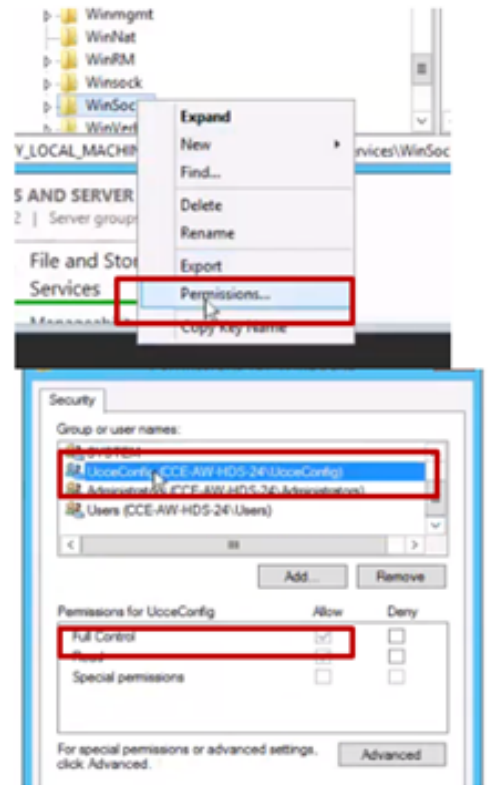
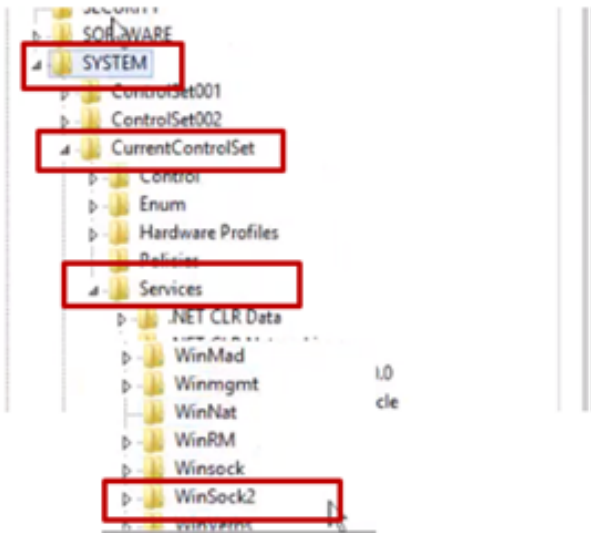
Pour déplacer l'autorisation hors de l'AD exige une tâche une fois sur chaque ordinateur hôte aw d'accorder les autorisations exigées pour que les objectifs de groupe d'UcceConfig et de ce document présentent les étapes requises pour configurer ces l'autorisation avec un exemple de la façon tracer un utilisateur de domaine comme une partie de groupe de configuration et d'installation CCE.

Configurer

Au groupe de Grant UcceConfig les autorisations dans le serveur local aw est un processus en deux étapes : d'abord, des autorisations sont fournies au niveau de registre, et en second lieu, transmis au niveau de répertoire.

Étape 1. Configurez les autorisations de registre

1. Exécutez l'utilitaire de regedit.exe.
2. HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\WinSock2 choisi.
3. Dans les autorisations sous le groupe et le contrôle choisis d'UcceConfig d'onglet de Sécurité tenez compte de l'option de plein contrôle.



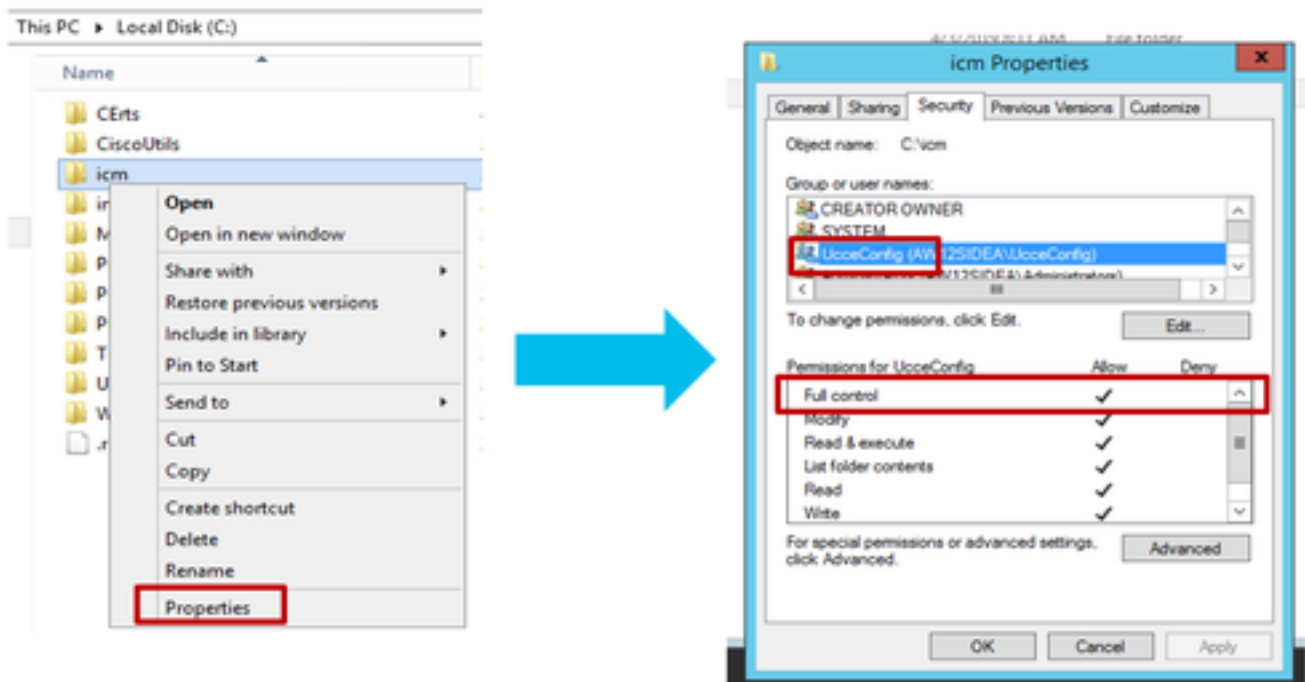
4. Répétez les étapes précédentes pour accorder le plein contrôle au groupe d'UcceConfig pour des registres

- Ordinateur \ HKEY_LOCAL_MACHINE \ LOGICIEL \ Cisco Systems, inc. \ missile aux performances améliorées
- Systèmes Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Cisco, inc. \ missile aux performances améliorées

Étape 2. Configurez les autorisations de répertoire

1. Dans l'Explorateur Windows, C:\icm choisi et vont à Properties.

2. Dans l'onglet Sécurité, UcceConfig choisi et contrôle tiennent compte de l'option de plein contrôle.



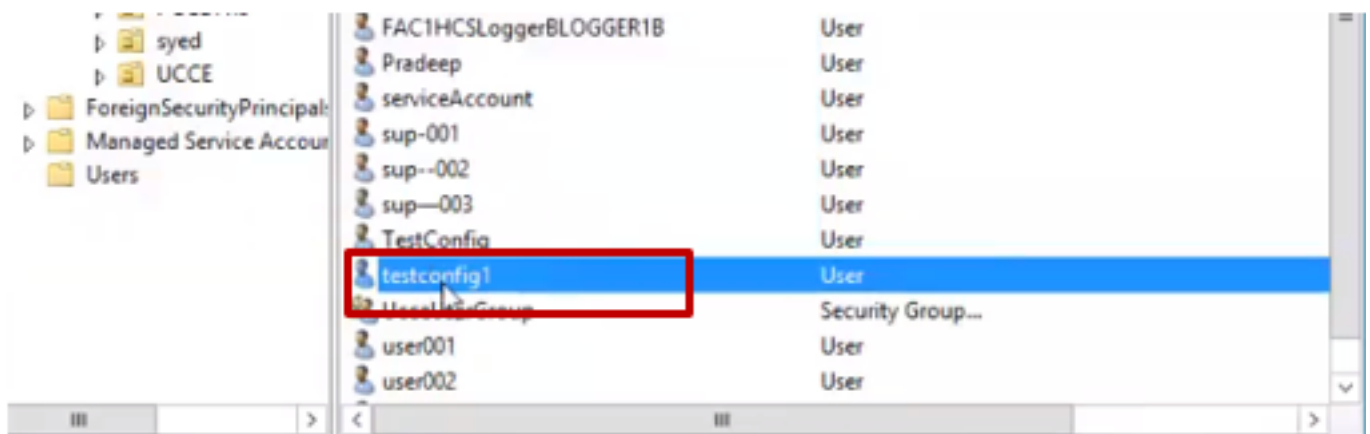
3. OK choisi pour sauvegarder la modification.

4. Répétez les étapes précédentes pour accorder le plein contrôle au groupe d'UcceConfig pour le répertoire de C:\Temp.

Car la configuration préliminaire du jour 0 a été réalisée, regardez les étapes sur la façon dont vous pouvez promouvoir un utilisateur de domaine pour avoir des droits de configuration et d'installation.

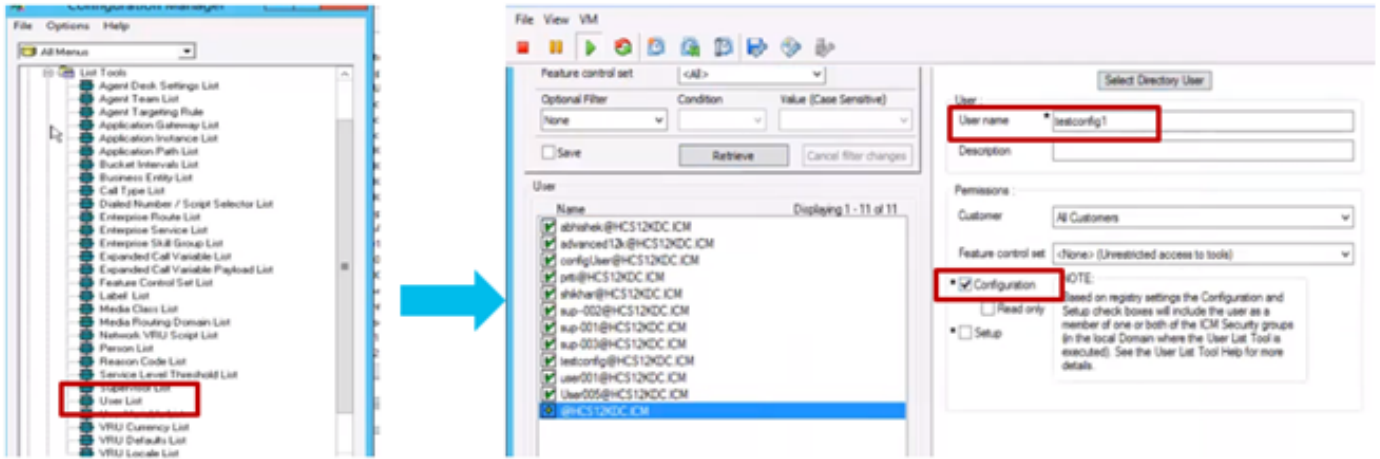
Étape 3 : Configuration utilisateur de domaine

1. Créez un utilisateur de domaine dans l'AD, parce que cet utilisateur de l'exercice testconfig1 avait été créé.

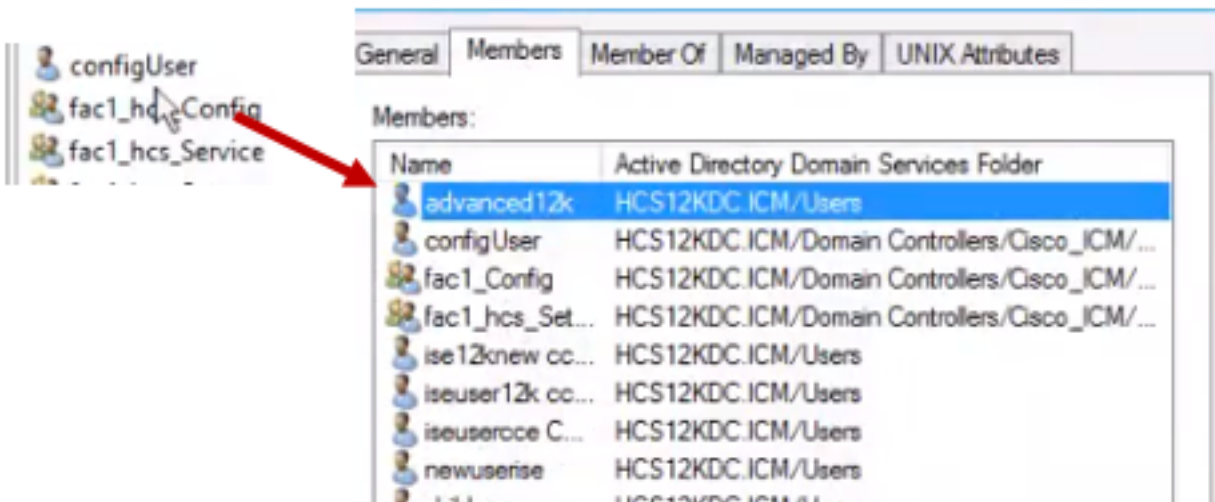


2. Procédure de connexion dans le serveur aw avec un compte d'admin d'adim ou de gens du pays de domaine.

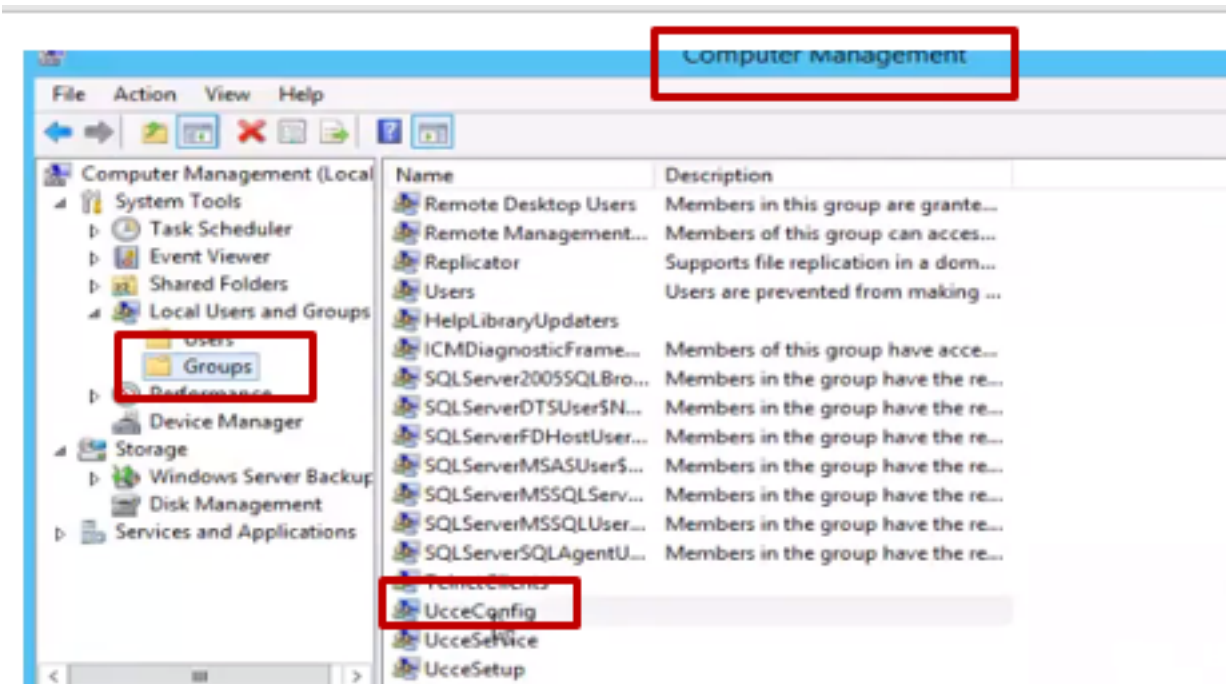
3. Dans le gestionnaire de configuration par l'outil de liste des utilisateurs ajoutez l'utilisateur et vérifiez l'option de **configuration**.



Avant la version 12.0 cette modification aurait mis à jour les groupes de sécurité de config dans le domaine sous une unité organisationnelle d'exemple (OU), mais avec 12.0 le comportement par défaut est qu'il n'ajoute pas cet utilisateur au groupe d'AD. Suivant les indications de l'image, il n'y a aucune mise à jour de cet utilisateur au groupe de sécurité de config améliorées de domaine.



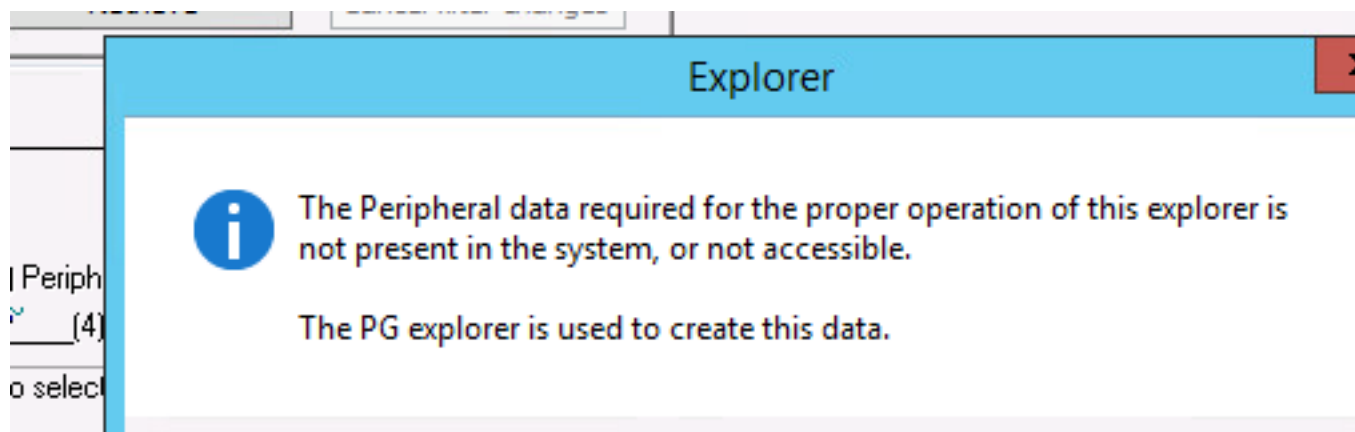
4. Dans le serveur aw sous la **gestion de l'ordinateur > les utilisateurs locaux et des groupes > des groupes** sélectionnez UcceConfig et ajoutez l'utilisateur testconfig1 dans lui.



5. Déconnexion de l'ordinateur et procédure de connexion avec les credentials de l'utilisateur testconfig1. Comme cet utilisateur a la configuration le redresse pourra exécuter des outils de configuration CCE tels que la Configuration Manager, le script ou le scripteur d'Internet.

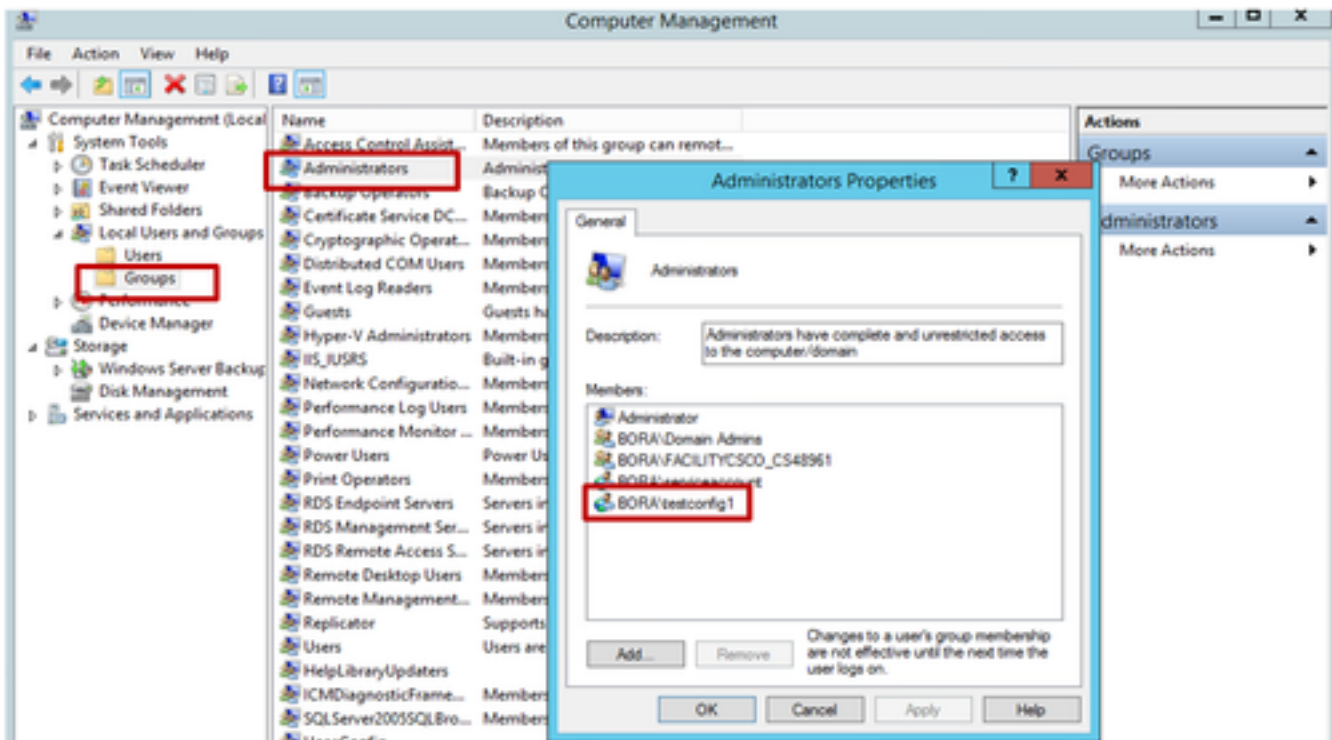
6. Cependant, si les essais d'utilisateur pour exécuter n'importe quelle tâche qui exigent d'installer redresse il échoue.

Cet exemple présente l'utilisateur testconfig1 changeant la configuration de passerelle d'accès aux périphériques (page) et le système limite la modification avec un message d'avertissement.

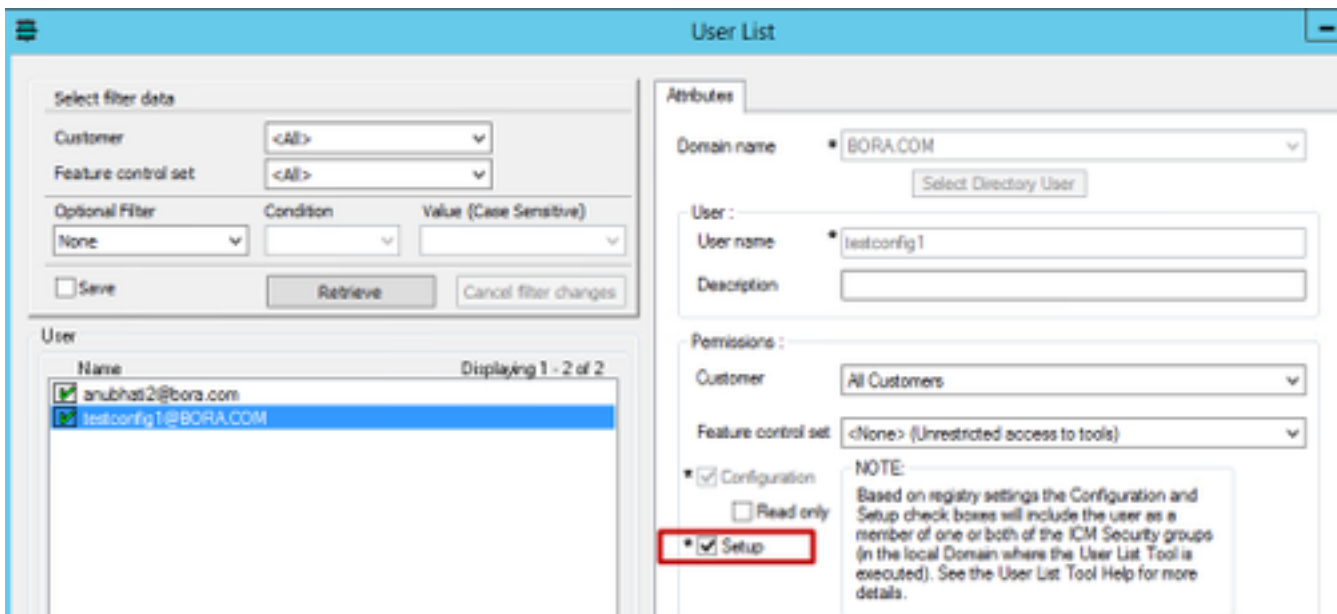


7. Si l'entreprise exige de cet utilisateur d'avoir des droits installés avec le config, alors vous doit s'assurer que l'utilisateur est ajouté au groupe d'admin de server local aw.

8. Afin de réaliser, ouvrez une session au serveur aw avec le domaine ou les droites d'admin de gens du pays rendent compte et par l'intermédiaire de la **gestion de l'ordinateur > des utilisateurs locaux et des groupes > des groupes** sélectionnez les groupes et dans les administrateurs ajoutez l'utilisateur à l'utilisateur.



9. Dans le gestionnaire de configuration par l'outil de liste des utilisateurs sélectionnez l'utilisateur et vérifiez l'option de configuration.



10. L'utilisateur peut maintenant accéder à toutes les ressources d'application CCE dans ce serveur aw et apporter les modifications désirées.

Vérifiez

La procédure de vérification est réellement une partie du processus de configuration.

Dépanner

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.