

UCCE 12.0(X)ローカル認証の設定

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[ステップ1: レジストリ権限の設定](#)

[ステップ2: フォルダ権限の設定](#)

[確認](#)

[トラブルシューティング](#)

概要

このドキュメントでは、Unified Contact Center Enterprise(CCE)コンポーネントの認可を管理するためにmicrosoft active directory(AD)の依存関係を削除するために必要な手順について説明します。

著者 : Cisco TAC エンジニア、Anuj Bhatia

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 Contact Center Enterprise
- Microsoft Active Directory

使用するコンポーネント

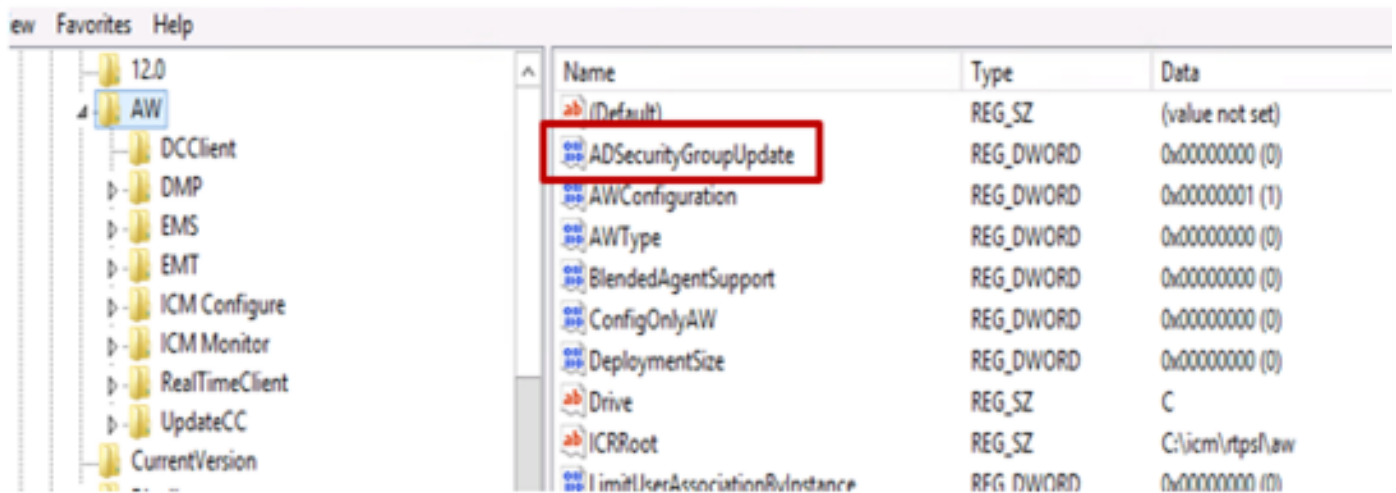
このドキュメントで使用されている情報は、UCCEソリューション12.0(1)バージョンに基づいています。

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、初期（デフォルト）設定の状態から起動しています。ネットワークが稼働中の場合は、すべてのステップの潜在的な影響を確実に理解してください。

背景説明

UCCE 12.Xリリースでは、ローカル管理サーバ(AW)上のローカルユーザグループに対してユーザ

メンバーシップ権限が付与されます。これにより、ユーザはActive Directory(AD)から認可を移動できます。これは、デフォルトで有効になっているレジストリADSecurityGroupUpdateによって制御され、セットアップおよび設定作業を実行するためのユーザアクセス権を制御するためにMicrosoft ADセキュリティグループを使用しないようにします。



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' entry is highlighted with a red box. The table below represents the data visible in the right pane.

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\rtps\law
LimitUserAssociationRvInstance	REG_DWORD	0x00000000 (0)

注：ビジネスが以前の動作を選択する場合は、ADSecurityGroupUpdateフラグを1に変更し、Active Directory(AD)に更新できます

認証をADから移動するには、各AWサーバマシンでUcceConfigグループに必要な権限を付与するワンタイムタスクが必要です。このドキュメントでは、CCE設定およびセットアップグループの一部としてドメインユーザをマッピングする例を示します。

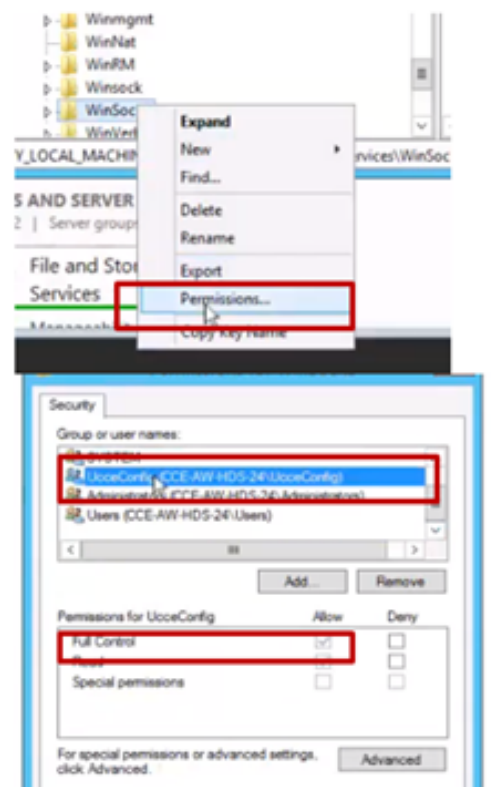
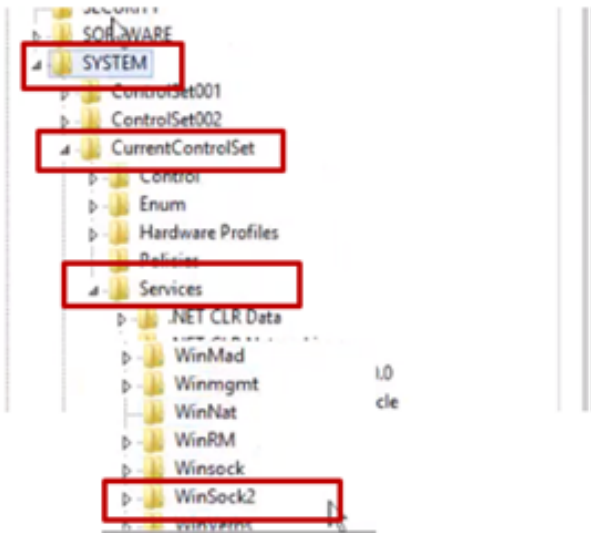
設定

ローカルAWサーバでUcceConfigグループの権限を付与するには、次の2つの手順を実行します。最初に、アクセス許可はレジストリレベルで提供され、2番目にフォルダレベルに渡されます。

ステップ1：レジストリ権限の設定

1. regedit.exeユーティリティを実行します。
2. HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\WinSock2を選択します。

を選択します。 [セキュリティ]タブの[権限]で、[UcceConfig]グループを選択し、[フルコントロール]オプションの[許可]をオンにします。

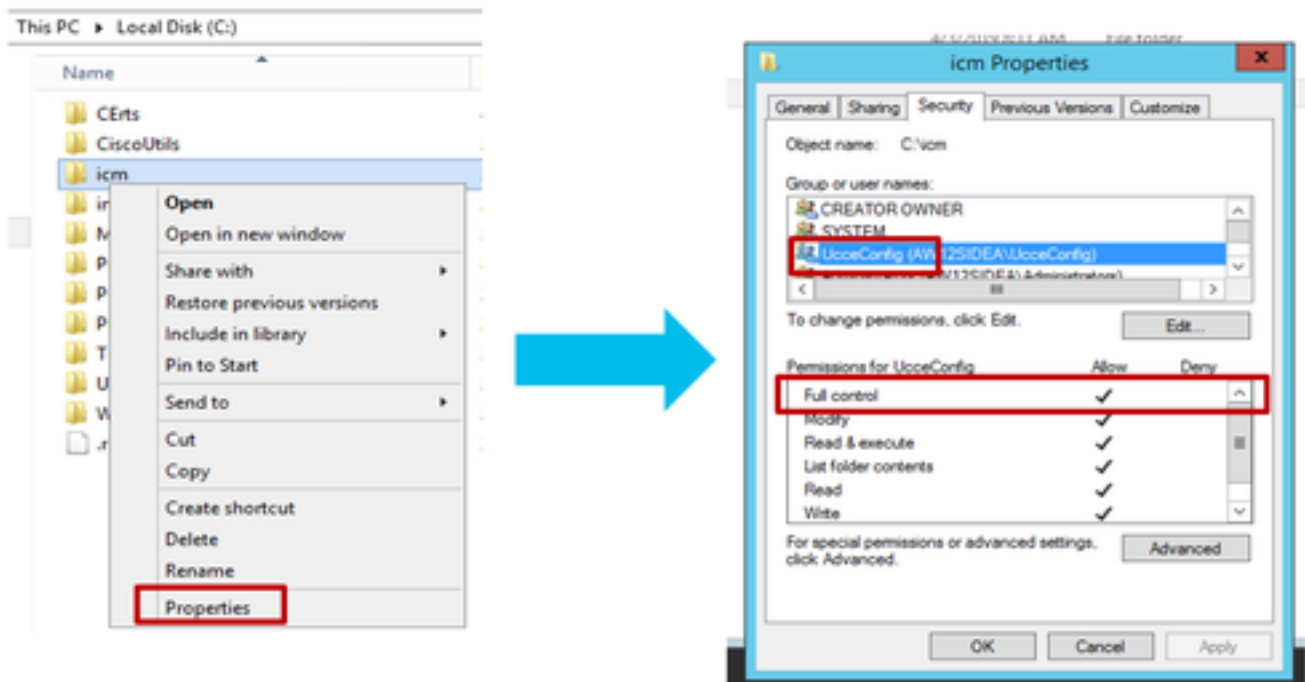


4. レジストリのUcceConfigグループにフルコントロールを付与するには、前の手順を繰り返します

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

ステップ2：フォルダ権限の設定

1. Windowsエクスプローラで、C:\icm and go to Propertiesを選択します。
2. [Security]タブで[UcceConfig]を選択し、[Full Control]オプションの[Allow]をオンにします。



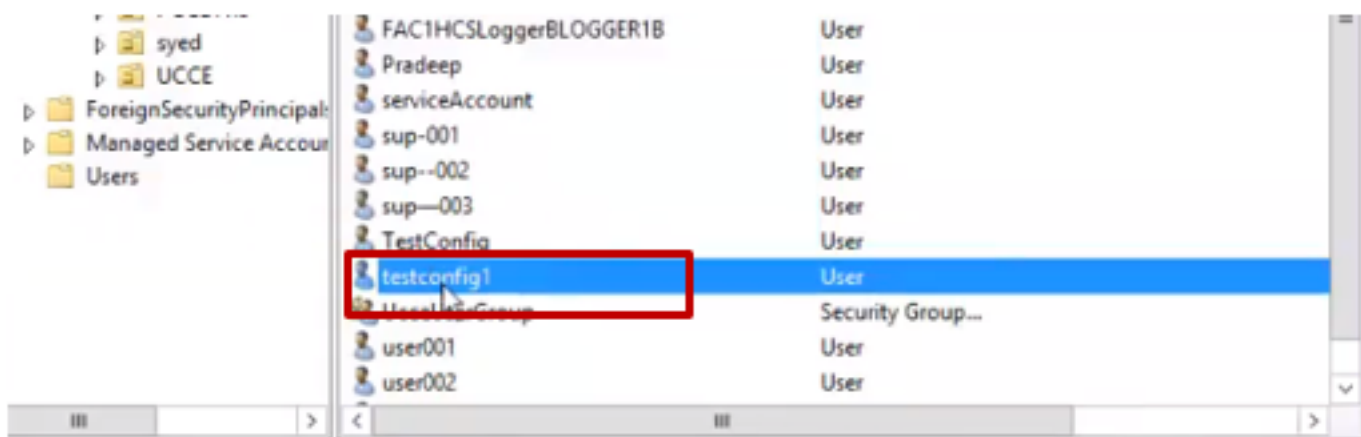
3. 「OK」を選択して変更を保存します。

4.上記の手順を繰り返して、C:\Temp folderのUcceConfigグループに完全な制御を付与します。

Day 0の事前構成が完了したら、ドメインユーザに構成とセットアップの権限を昇格させる手順を確認します。

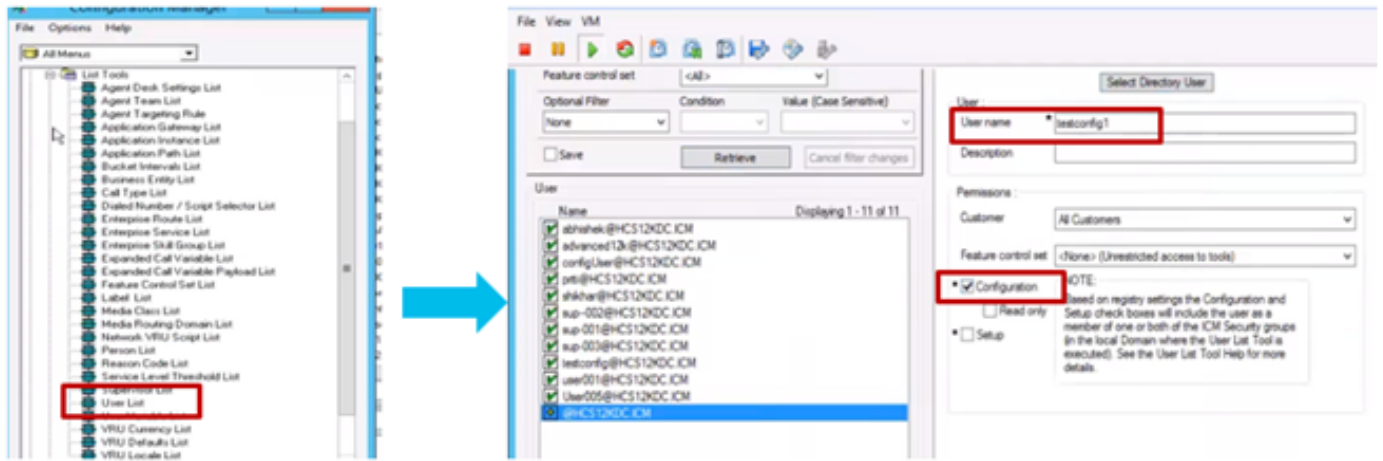
ステップ3：ドメインユーザの設定

1. ADでドメインユーザを作成します。この演習testconfig1ユーザが作成されました。

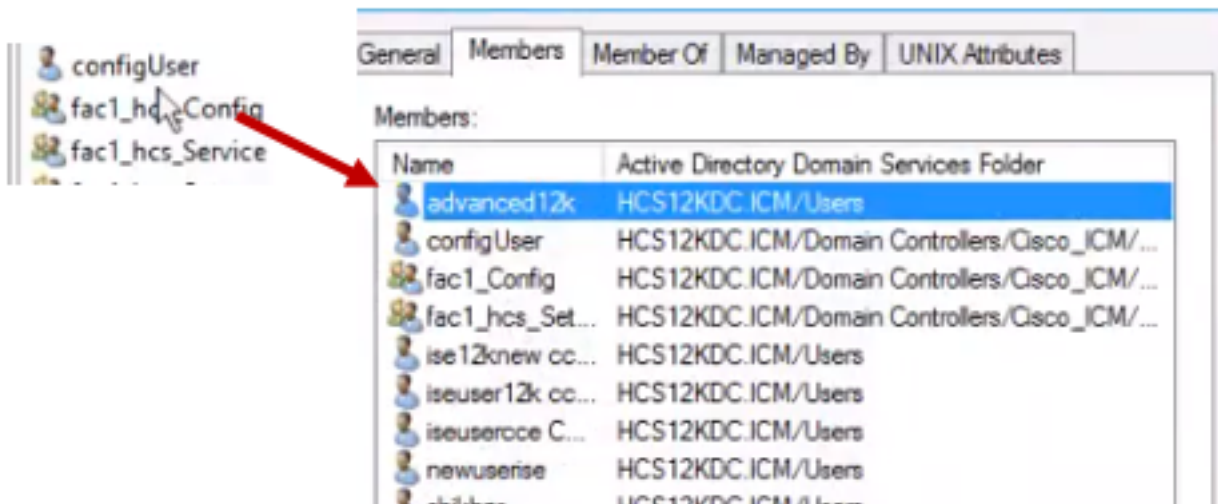


2.ドメインadimまたはローカル管理者アカウントでAWサーバにログインします。

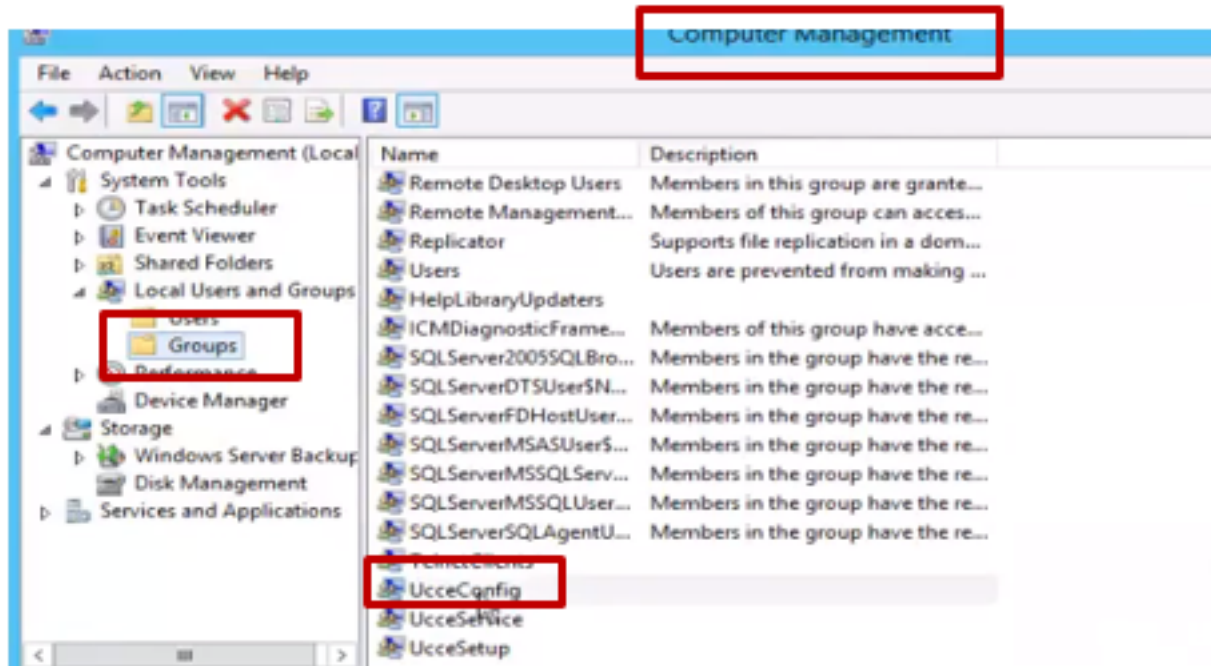
3.ユーザーリストツールを使用して構成マネージャーでユーザーを追加し、構成オプションを確認してください。



12.0より前のバージョンでは、この変更により、インスタンスOrganizational Unit(OU)の下のドメインのConfigセキュリティグループが更新されましたが、12.0では、デフォルトの動作では、そのユーザがADグループに追加されません。図に示すように、ドメインのICM Configセキュリティグループにこのユーザの更新はありません。



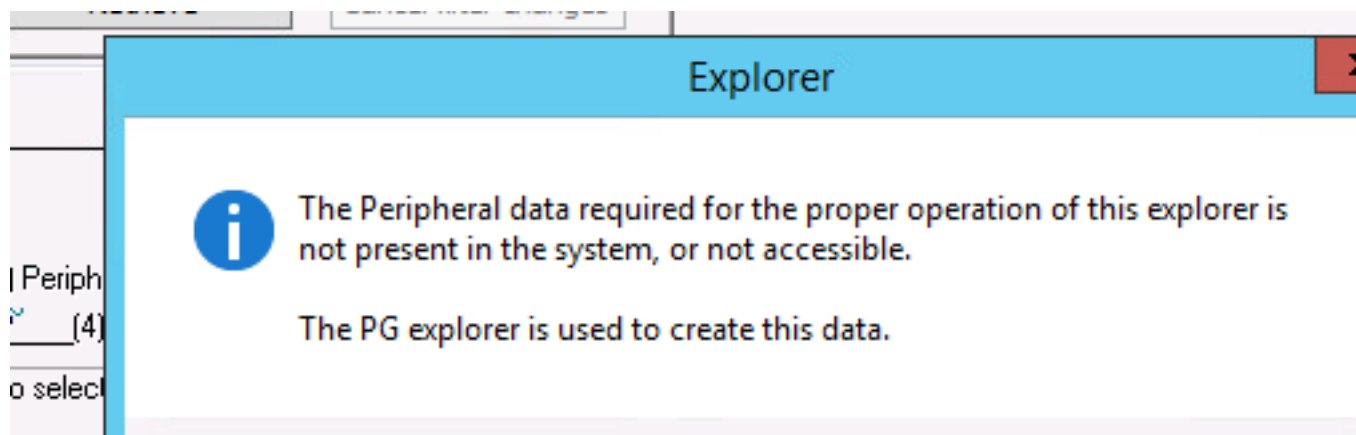
4. AWサーバの[Computer Management] > [Local Users and Groups] > [Groups]で[UcceConfig]を選択し、testconfig1ユーザを追加します。



5. マシンからログアウトし、testconfig1ユーザのクレデンシャルでログインします。このユーザは設定権限を持っているため、Configuration Manager、スクリプト、またはInternet Script EditorなどのCCE設定ツールを実行できます。

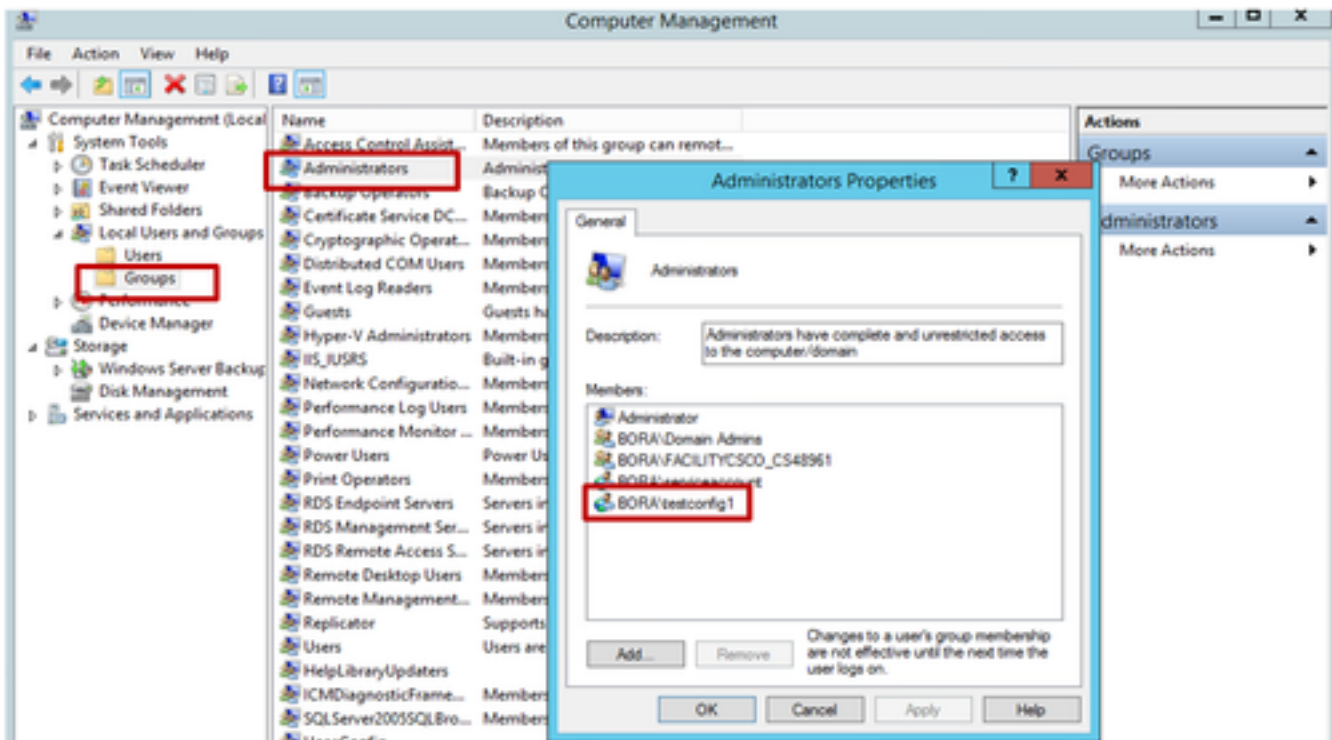
6. ただし、ユーザがセットアップ権限を必要とするタスクを実行しようとする、失敗します。

次の例は、testconfig1ユーザがペリフェラルゲートウェイ(pg)の設定を変更し、システムが変更を警告メッセージで制限していることを示しています。

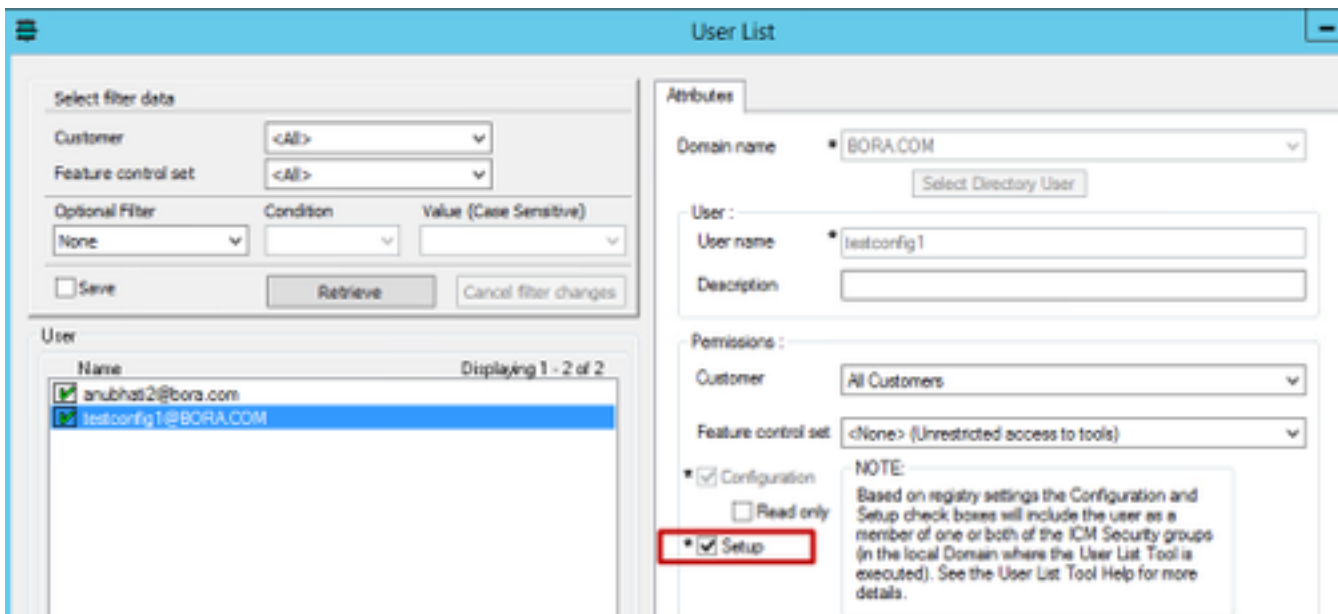


7. ビジネスでこのユーザに設定権限と設定が必要な場合は、ユーザがAWサーバのローカル管理者グループに追加されていることを確認する必要があります。

8. アクティブにするには、ドメインまたはローカル管理者権限アカウントでAWサーバにログインし、[computer management] > [Local Users and Groups] > [groups]を選択し、[Administrators]でユーザをユーザに追加します。



9. Configuration ManagerでUser listツールを使用してユーザを選択し、セットアップオプションをオンにします。



10.これで、ユーザはそのAWサーバ内のCCEアプリケーションのすべてのリソースにアクセスし、必要な変更を行うことができます。

確認

検証手順は、実際には設定プロセスの一部です。

トラブルシューティング

現在、この設定に関する特定のトラブルシューティング情報はありません。