

配置UCCE 12.0(X)本地授權

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[設定](#)

[步驟1.配置登錄檔許可權](#)

[步驟2.配置資料夾許可權](#)

[驗證](#)

[疑難排解](#)

簡介

本文檔介紹在Unified Contact Center Enterprise(CCE)元件中移除對microsoft active directory(AD)的依賴關係以管理授權所需的步驟。

作者：Anuj Bhatia，思科TAC工程師。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco Unified Contact Center Enterprise
- Microsoft Active Directory

採用元件

本文檔中使用的資訊基於UCCE解決方案12.0(1)版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何步驟可能造成的影響。

背景資訊

UCCE 12.X版本為本地Administration Server(AW)上的本地使用者組提供使用者成員許可權，允許使用者將授權移出Active Directory(AD)。這由預設情況下啟用的登錄檔ADSecurityGroupUpdate控制，並避免使用Microsoft AD安全組控制使用者訪問許可權以執行設定和配置任務。

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
LimitUserAssociationByInstance	REG_DWORD	0x00000000 (0)

附註： 如果企業希望選擇先前行為，ADSecurityGroupUpdate標誌可更改為1，以允許更新到Active Directory(AD)

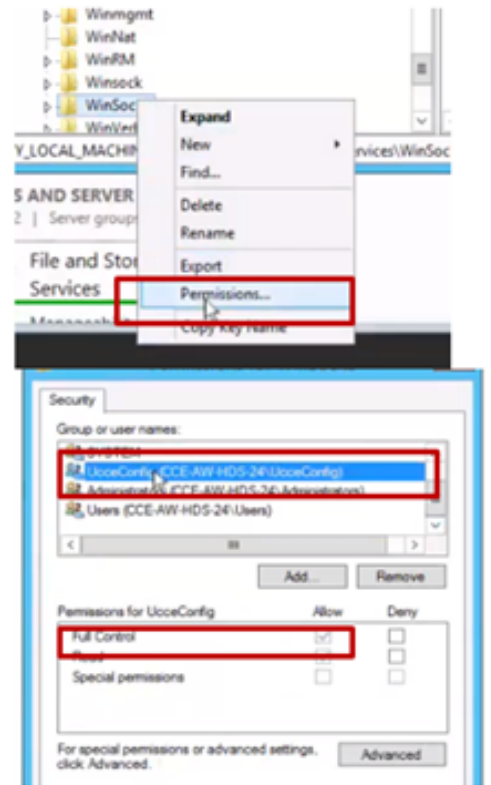
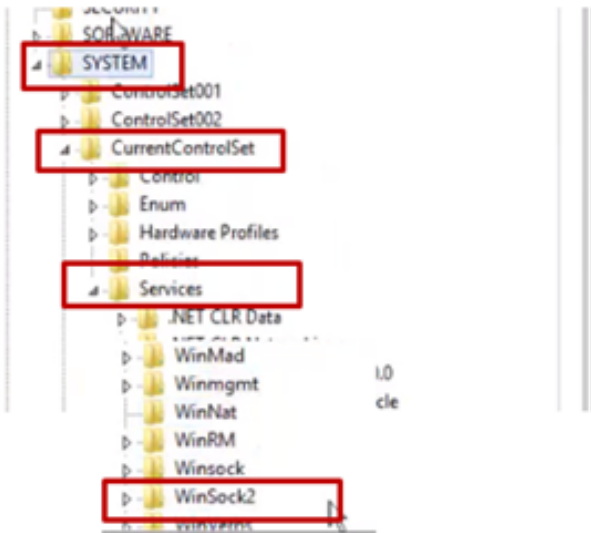
要將授權移出AD，需要在每台AW伺服器電腦上執行一次任務以授予UcceConfig組所需的許可權，本文檔旨在展示配置這些許可權所需的步驟，以及如何將域使用者對映為CCE配置和設定組的一部分。

設定

在本地AW伺服器中授予UcceConfig組許可權是一個兩步過程：第一，在登錄檔級別提供許可權，第二，傳遞到資料夾級別。

步驟1.配置登錄檔許可權

1. 運行regedit.exe實用程式。
2. 選擇HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\WinSock2。
3. 在「安全」頁籤下的「許可權」中，選擇「UcceConfig」組，然後選中「允許完全控制」選項。



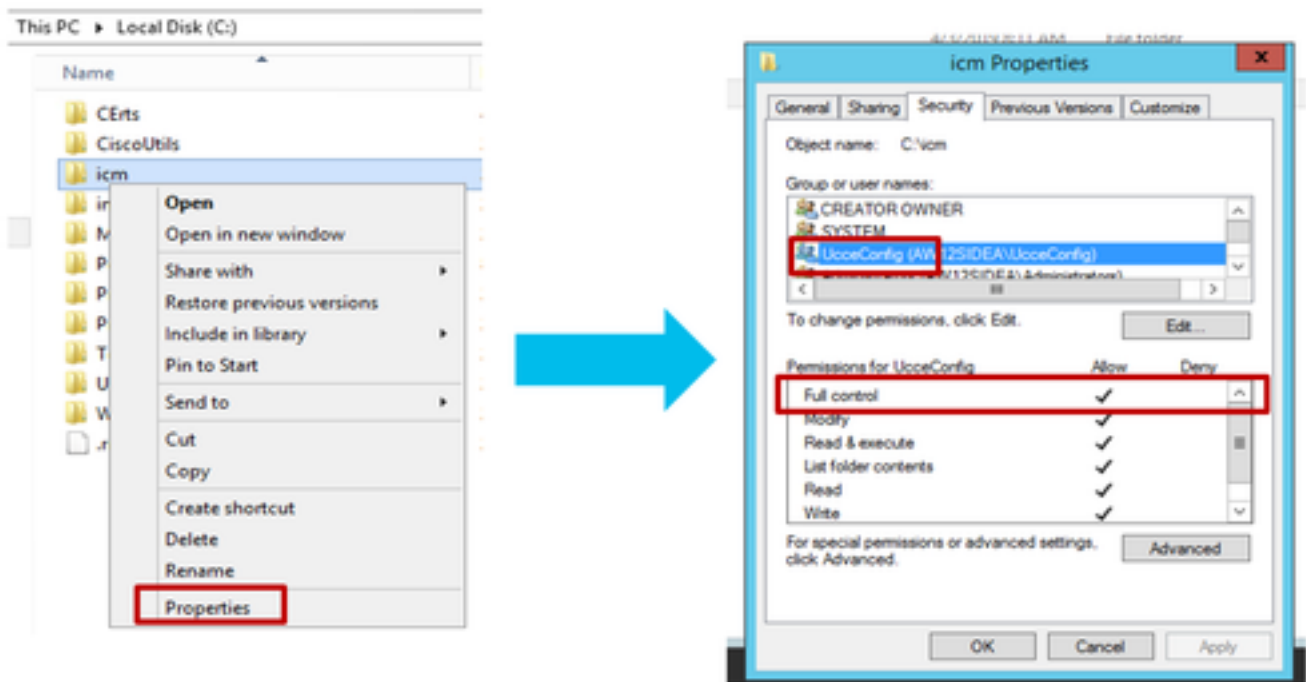
4. 重複上述步驟，為註冊機構將「完全控制」授予UcceConfig組

- Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, inc.\ICM
- Computer\HKEY_LOCAL_MACHINE\SOFTWAREWow6432Node\Cisco Systems, inc.\ICM

步驟2. 配置資料夾許可權

1. 在Windows資源管理器中，選擇C:\icm並轉到「屬性」。

2. 在「安全」頁籤中，選擇UcceConfig，並選中Allow for the Full Control選項。



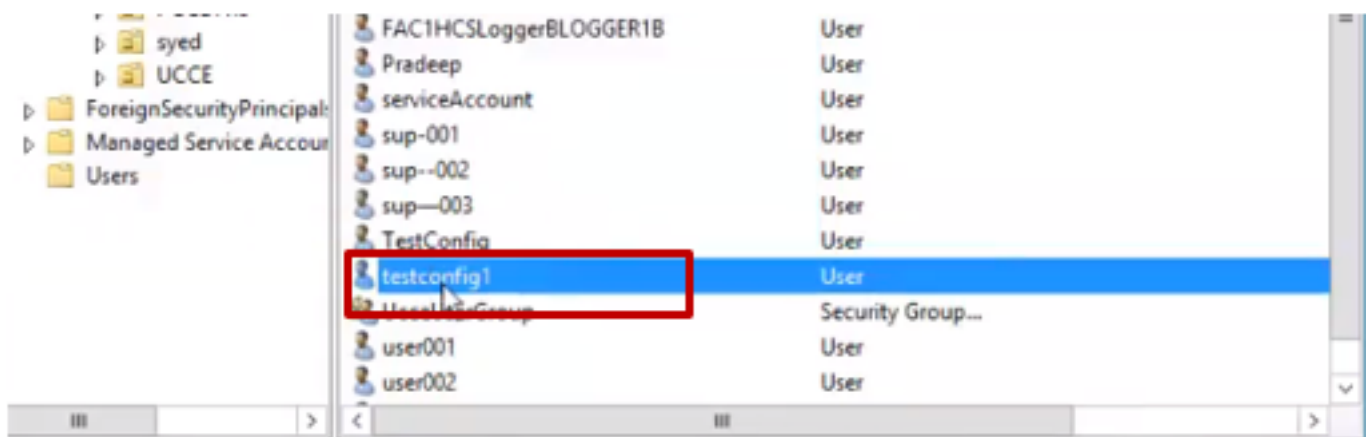
3.選擇「確定」儲存更改。

4.重複上述步驟，對C:\Temp資料夾的UcceConfig組授予完全控制。

第0天初步配置完成後，請檢視如何提升域使用者擁有配置和設定許可權的步驟。

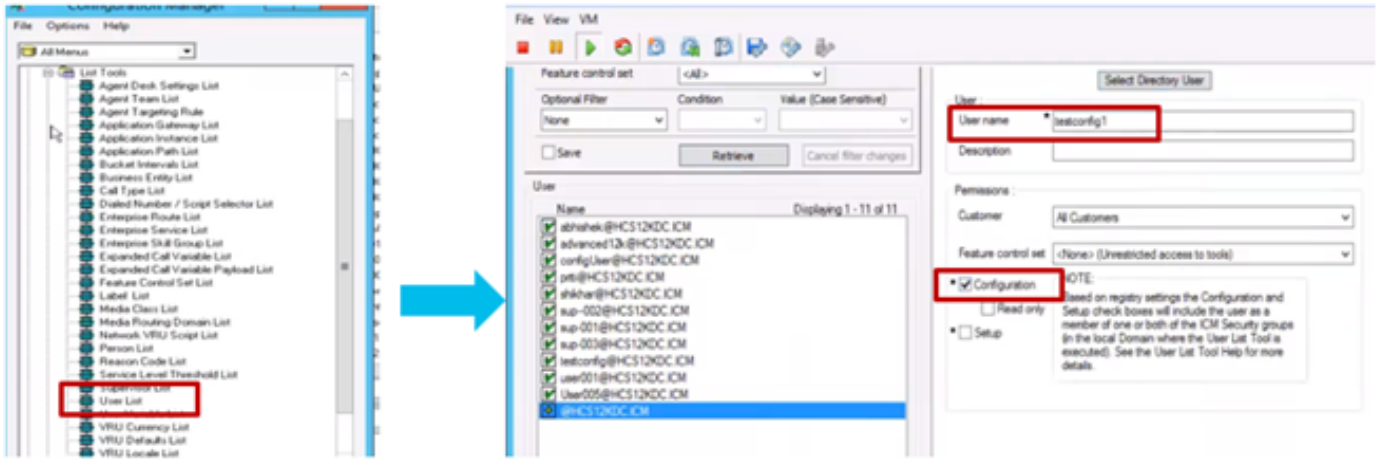
步驟3:域使用者配置

1.在AD中建立域使用者，此練習的testconfig1使用者已建立。

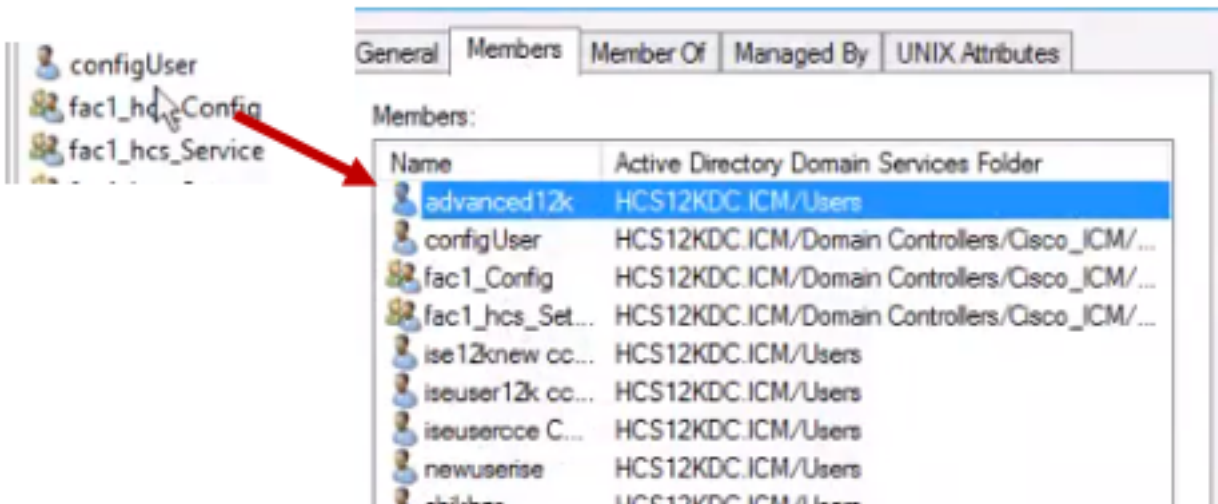


2.使用域adim或本地管理員帳戶登入到AW伺服器。

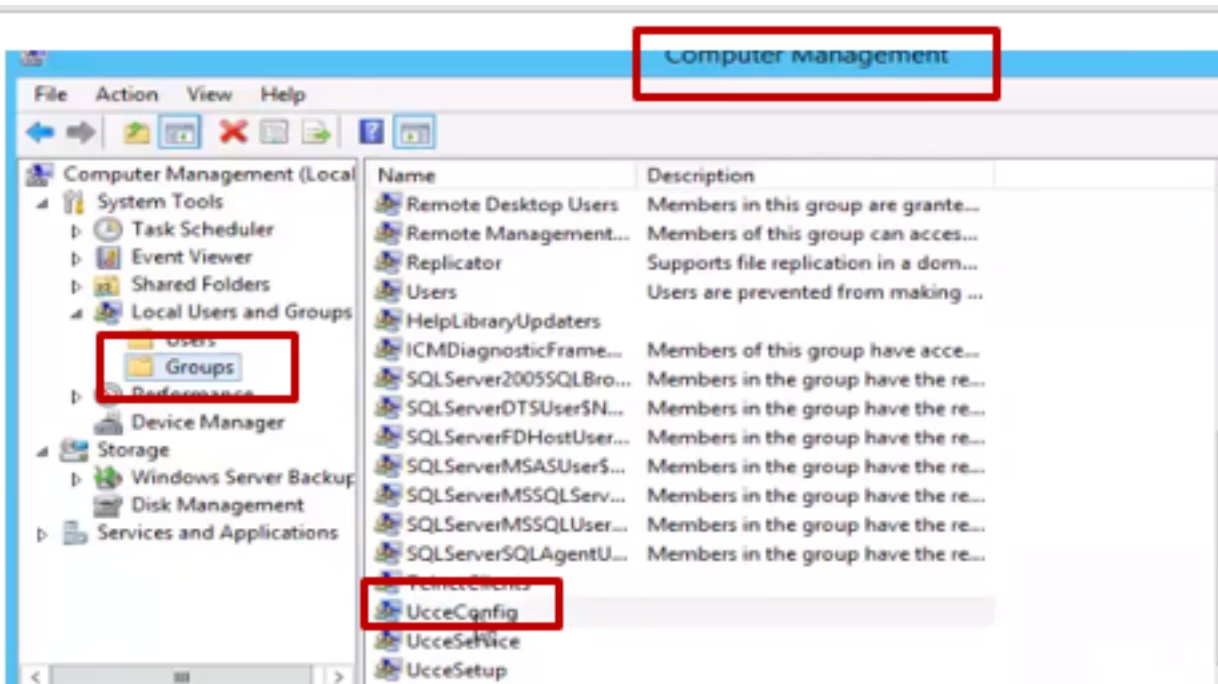
3.在configuration manager中，通過使用者清單工具新增使用者並選中configuration選項。



在12.0版本之前，此更改會更新例項組織單元(OU)下的域中的配置安全組，但使用12.0時，預設行為是不會將該使用者新增到AD組。如圖所示，在域ICM配置安全組中沒有此使用者的更新。



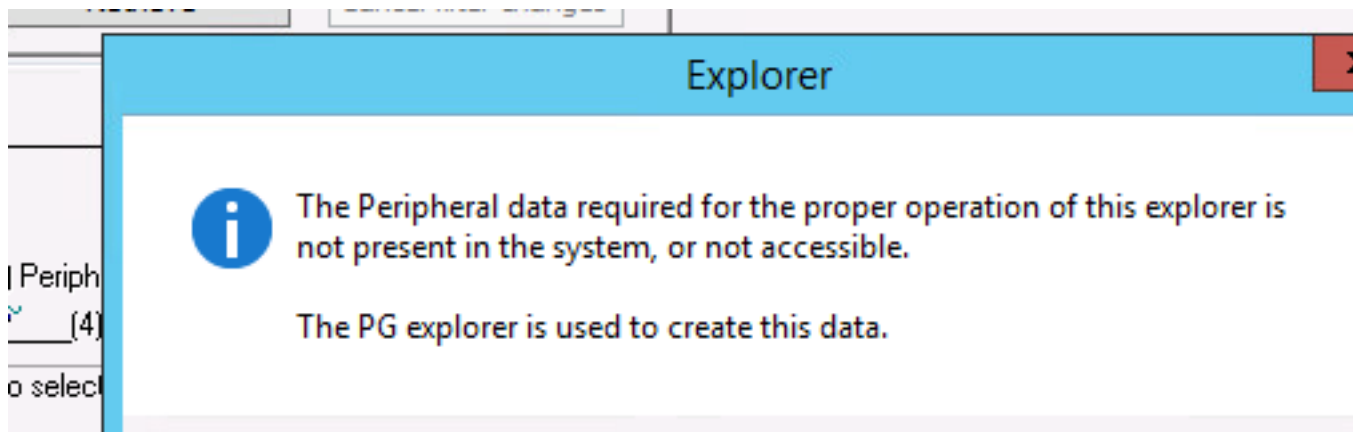
4.在AW伺服器中的computer management > Local Users and Groups > Groups下，選擇UcceConfig並將testconfig1使用者新增到其中。



5.從電腦註銷，然後使用testconfig1使用者的憑據登入。由於此使用者具有配置許可權，因此它將能夠運行CCE配置工具，如Configuration Manager、指令碼或Internet指令碼編輯器。

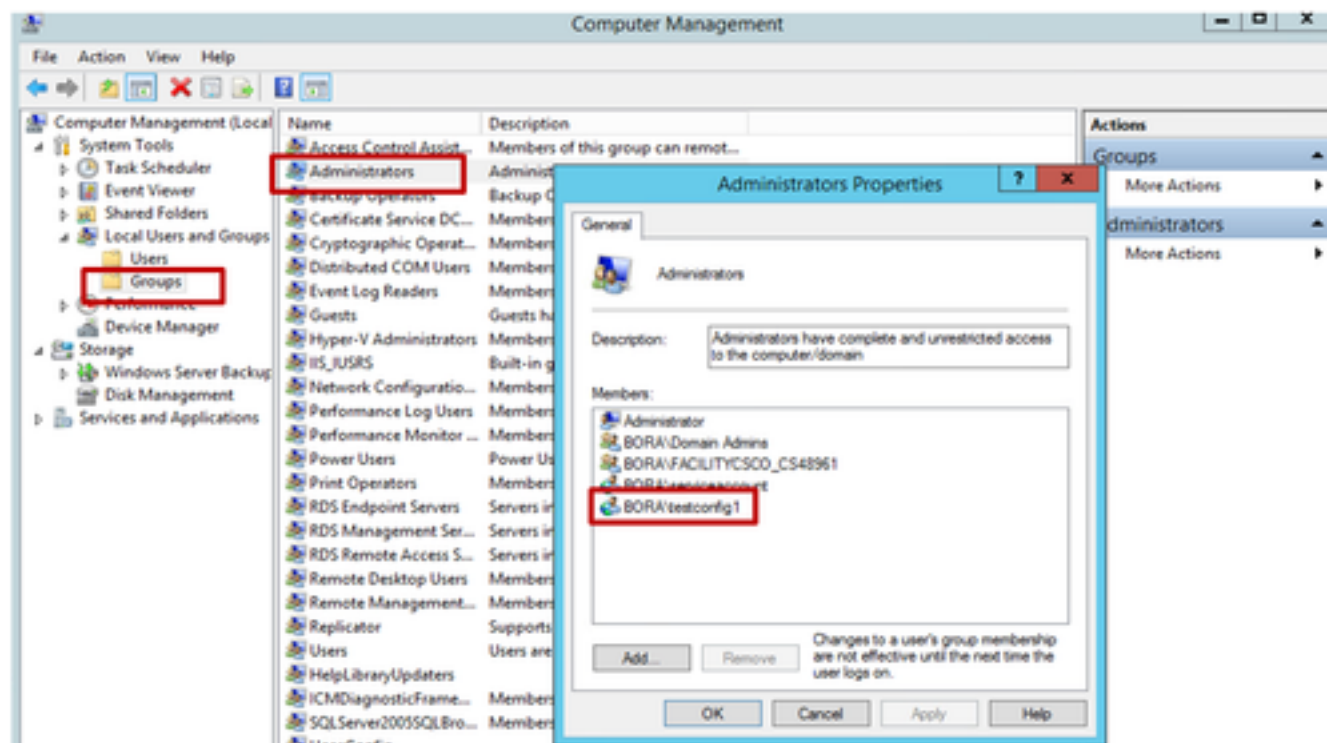
6.但是，如果使用者嘗試執行任何需要設定許可權的任務，則失敗。

此示例展示testconfig1使用者更改外圍裝置網關(pg)配置，並且系統使用警告消息限制更改。

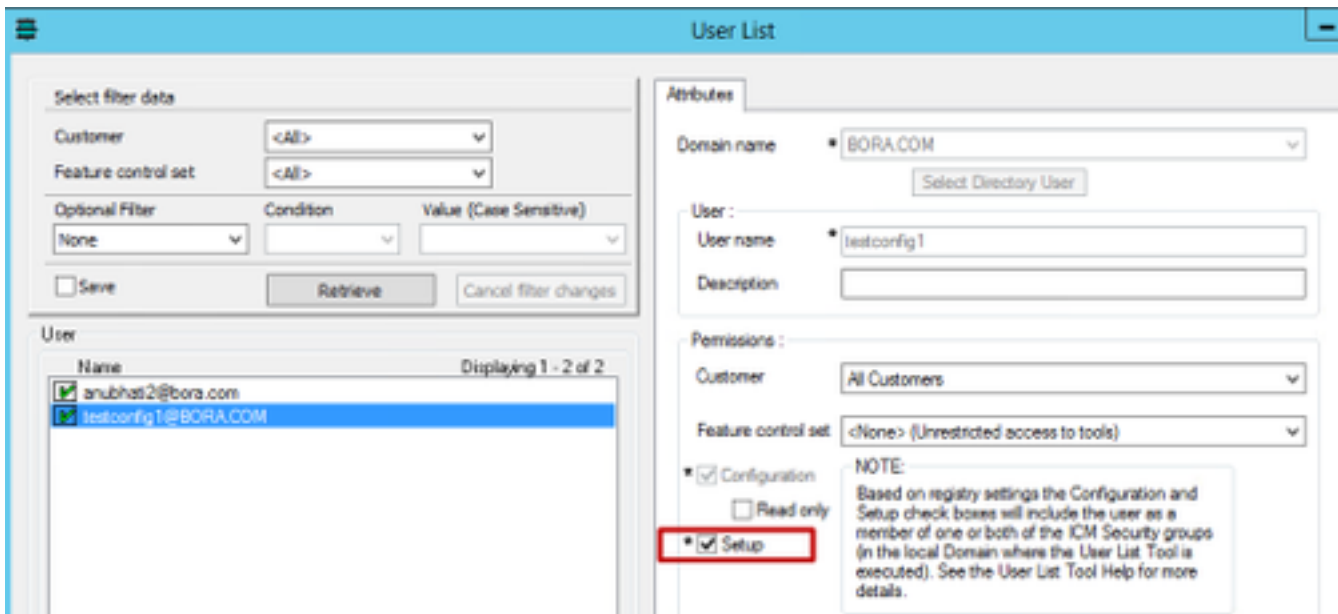


7.如果企業要求此使用者具有設定許可權以及config，則必須確保將該使用者新增到AW伺服器本地管理員組中。

8.若要實現，請使用域或本地管理員許可權帳戶登入AW伺服器，然後通過**computer management > Local Users and Groups > groups**選擇Groups，然後在Administrators中將使用者新增到該使用者。



9.在Configuration manager中，通過使用者清單工具選擇使用者並選中設定選項。



10.使用者現在能夠訪問該AW伺服器中CCE應用程式的所有資源並進行所需的更改。

驗證

驗證過程實際上是配置過程的一部分。

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。