Configura autorizzazione locale PCCE

Sommario

Introduzione

In questo documento viene descritto come rimuovere la dipendenza di Microsoft Active Directory (AD) per gestire localmente le autorizzazioni nei componenti di Package Contact Center Enterprise (PCCE).

Contributo di Meenakshi Sundaram, Ramiro Amaya e Anuj Bhatia, Cisco TAC Engineers.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Package Contact Center Enterprise
- Microsoft Active Directory

Componenti usati

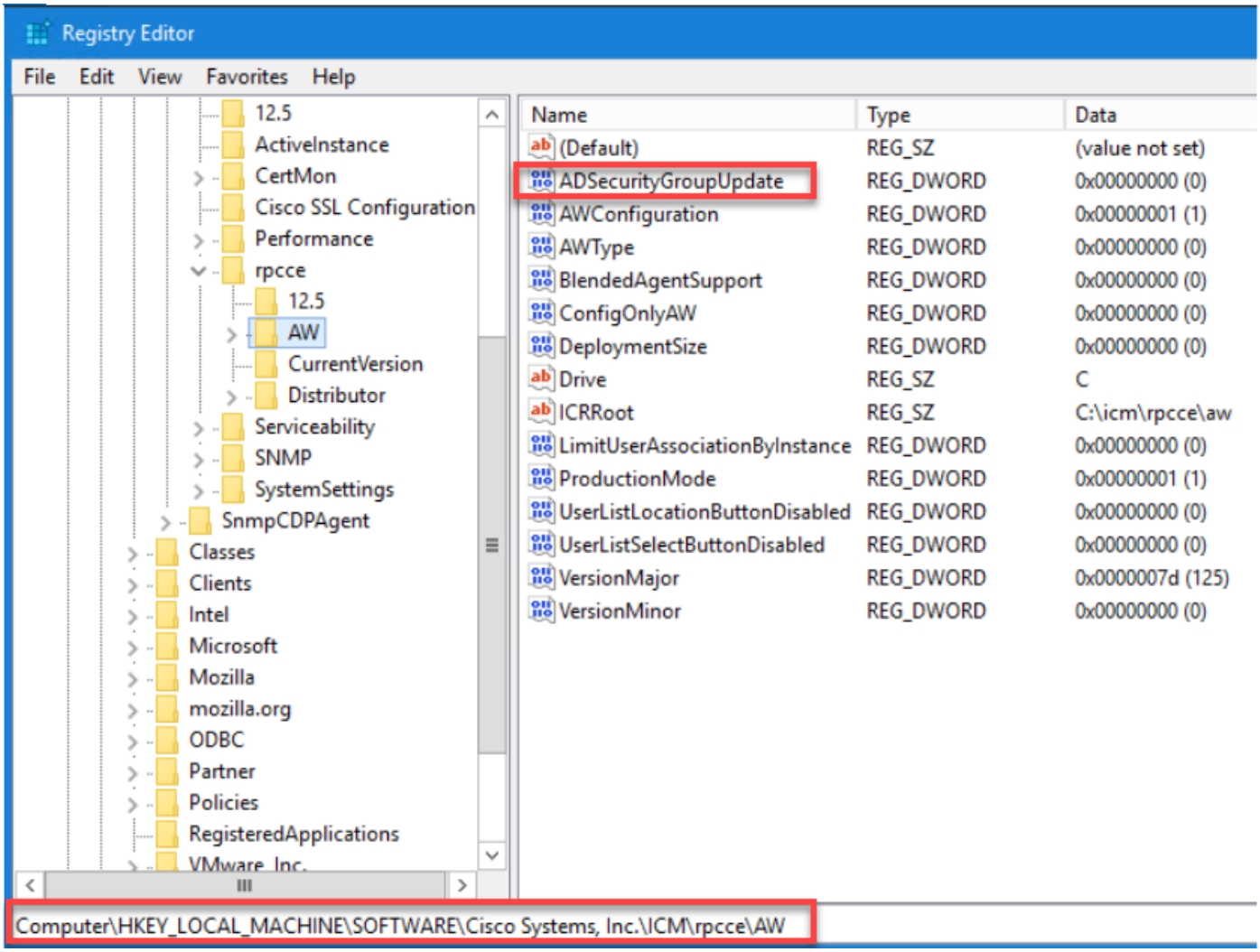
Le informazioni contenute nel documento si basano sulla versione PCCE 12.5(1).

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, verificare di aver compreso l'impatto potenziale di qualsiasi passaggio.

Premesse

La versione PCCE 12.5 fornisce i privilegi utente ai gruppi di utenti locali sui server di amministrazione (AW), che consentono agli utenti di spostare l'autorizzazione fuori da Active Directory (AD). Questa impostazione è controllata dal Registro di sistema **ADSecurityGroupUpdate** che, per impostazione predefinita, è abilitato ed evita l'utilizzo dei gruppi di sicurezza di Microsoft AD per controllare i diritti di accesso degli utenti per eseguire attività di installazione e configurazione.

> **Nota:** Il supporto per l'autorizzazione locale è stato avviato in Unified Contact Center Enterprise (UCCE) 12.0 ed è ora supportato in PCCE 12.5.



> **Nota:** Se è necessario implementare il comportamento precedente (autorizzazione AD), è possibile modificare il flag ADSecurityGroupUpdate in 1.

Configurazione

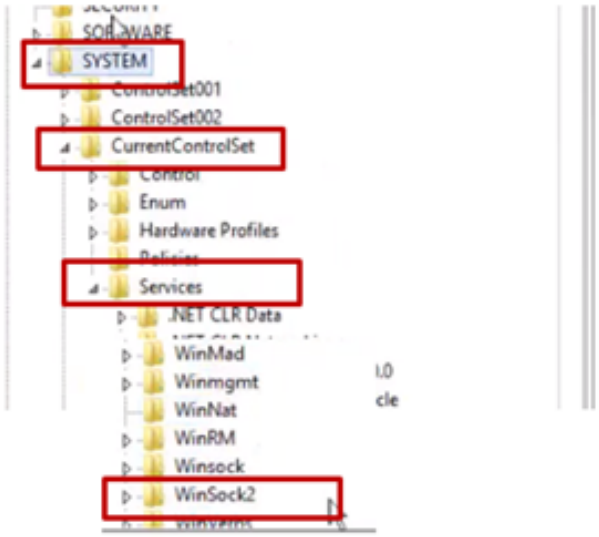
Per concedere le autorizzazioni di gruppo UcceConfig in un server AW locale, è necessario innanzitutto fornire le autorizzazioni a livello del Registro di sistema e quindi a livello della cartella.

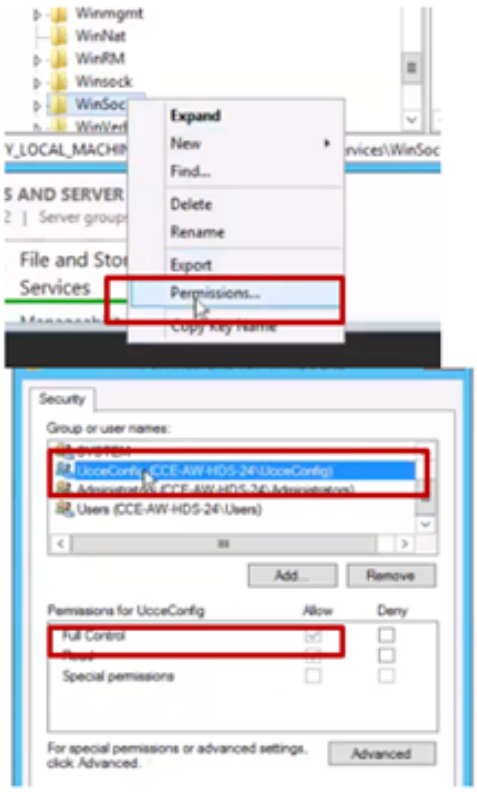
Passaggio 1. Configurare le autorizzazioni del Registro di sistema.

1. Eseguire l'utilità regedit.exe.

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

3. In Autorizzazioni nella scheda Protezione selezionare il gruppo **UcceConfig** e selezionare **Allow for the Full Control** option.





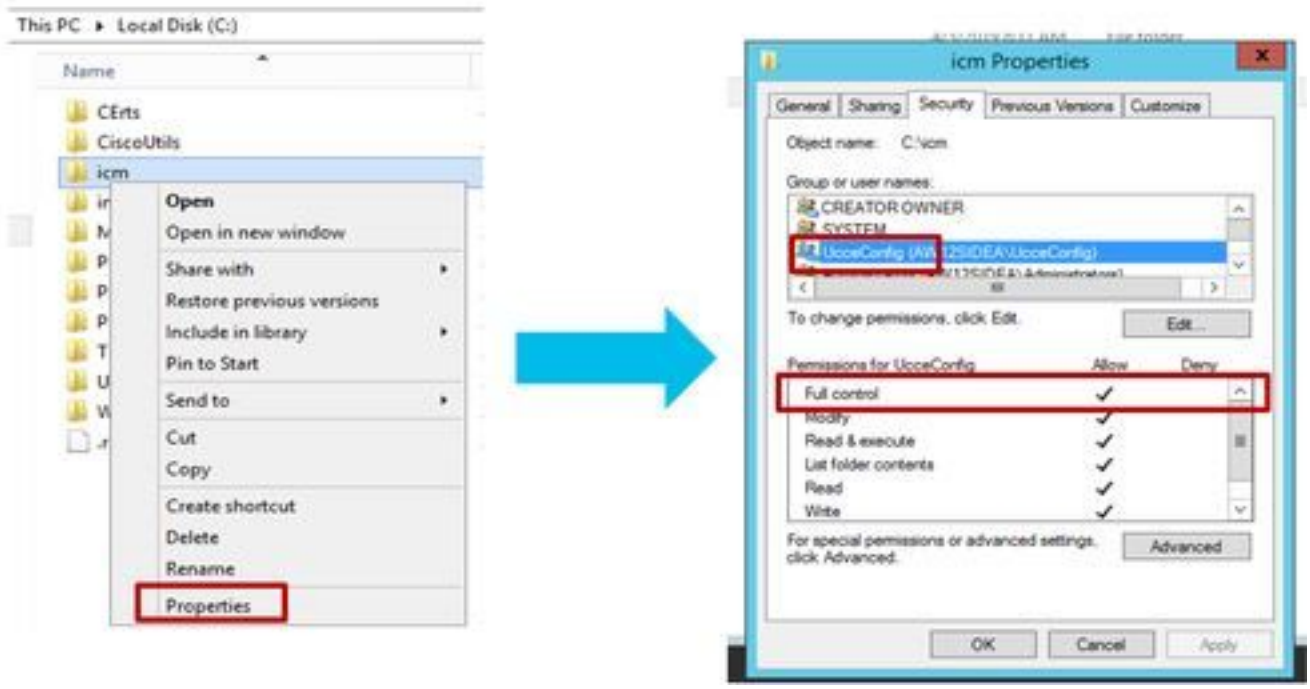
4. Ripetere i passaggi precedenti per concedere al gruppo UcceConfig il controllo completo di questi registri.

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

Passaggio 2. Configurare Le Autorizzazioni Della Cartella.

1. In Esplora risorse, passare a <ICM Installed Directory>:\icm e selezionare Proprietà.

2. Nella scheda Security, selezionare **UcceConfig** e selezionare **Allow for the Full Control** option.



3. Selezionare OK per salvare le modifiche.

4. Ripetere i passaggi precedenti per concedere il controllo completo al gruppo **UcceConfig** per la cartella C:\Temp.

5. In SQL Management Studio eseguire le operazioni seguenti:

a) Selezionare Sicurezza > Accessi.

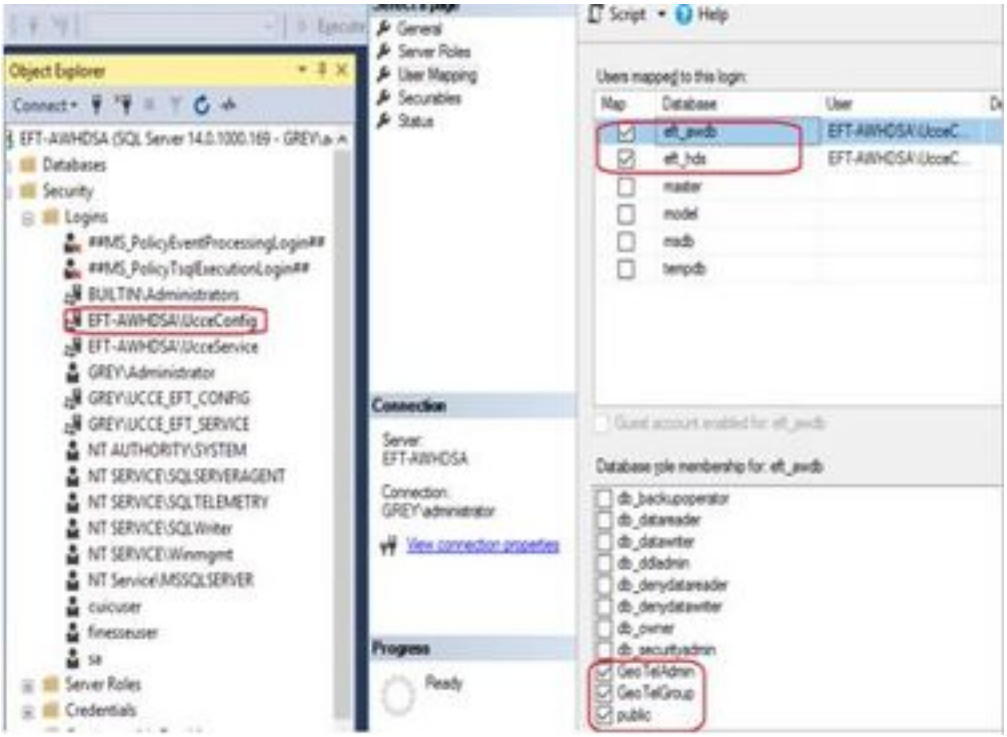
b) Individuare <Nome computer>\UcceConfig.

c) Fare clic con il pulsante destro del mouse e selezionare Proprietà.

d) Navigare in Mapping utente e selezionare il database AWDB.

e) Selezionare le caselle di controllo GeoTelAdmin, GeoTelGroup e public.

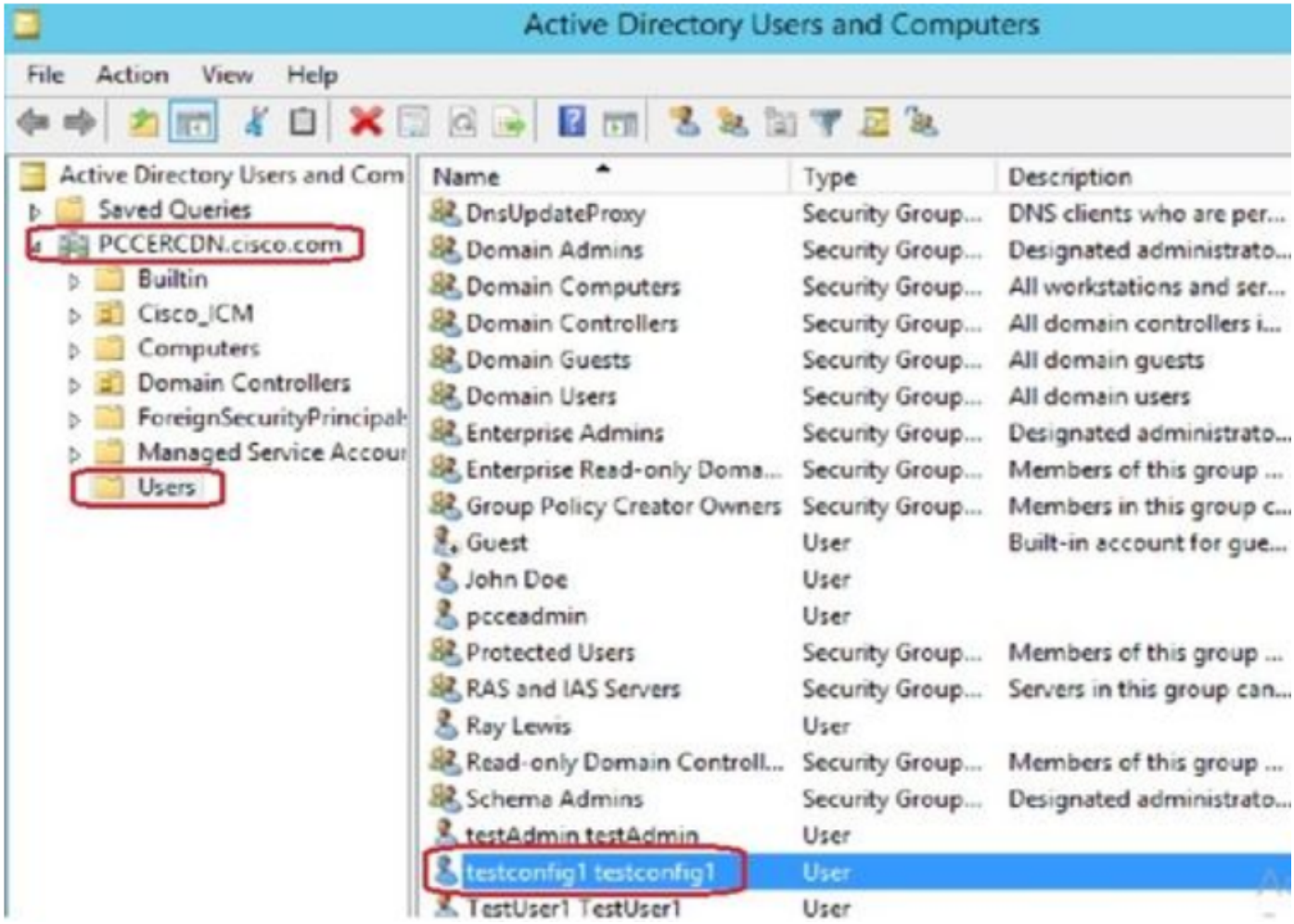
f) Ripetere la fase d) per il database dei dati storici (HDS).

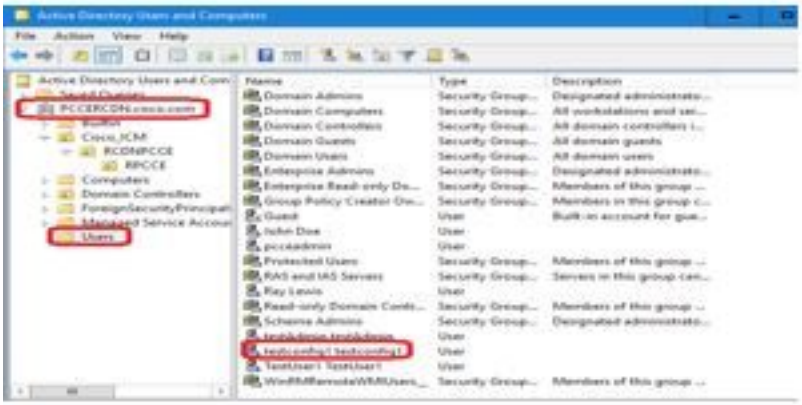


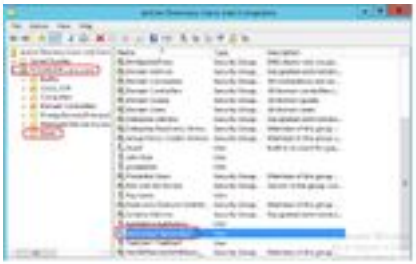
Una volta completata la configurazione preliminare, seguire la procedura descritta di seguito per promuovere un utente di dominio in modo da disporre dei diritti di configurazione e configurazione.

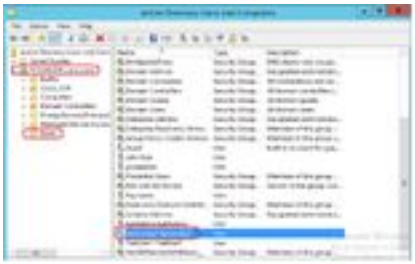
Passaggio 3. Configurazione utente del dominio.

1. Creare un utente di dominio in Active Directory. Per questo esercizio è stato creato l'utente testconfig1.



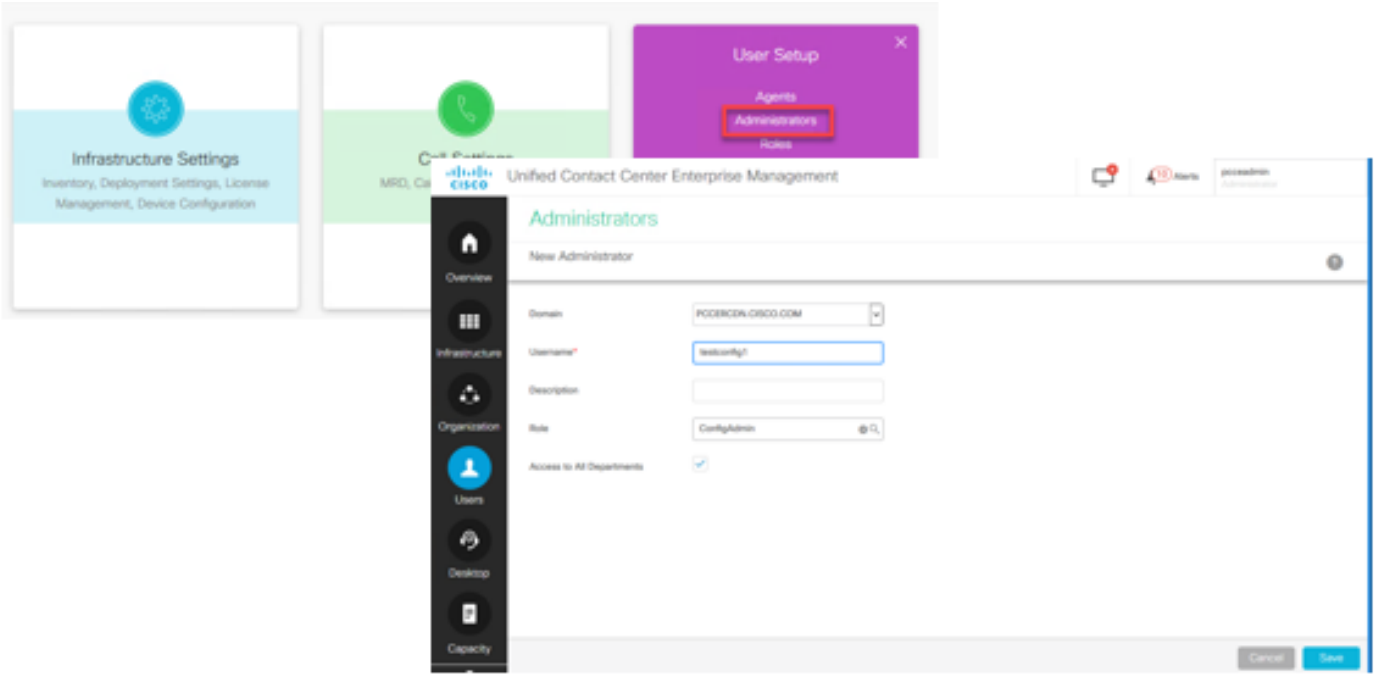




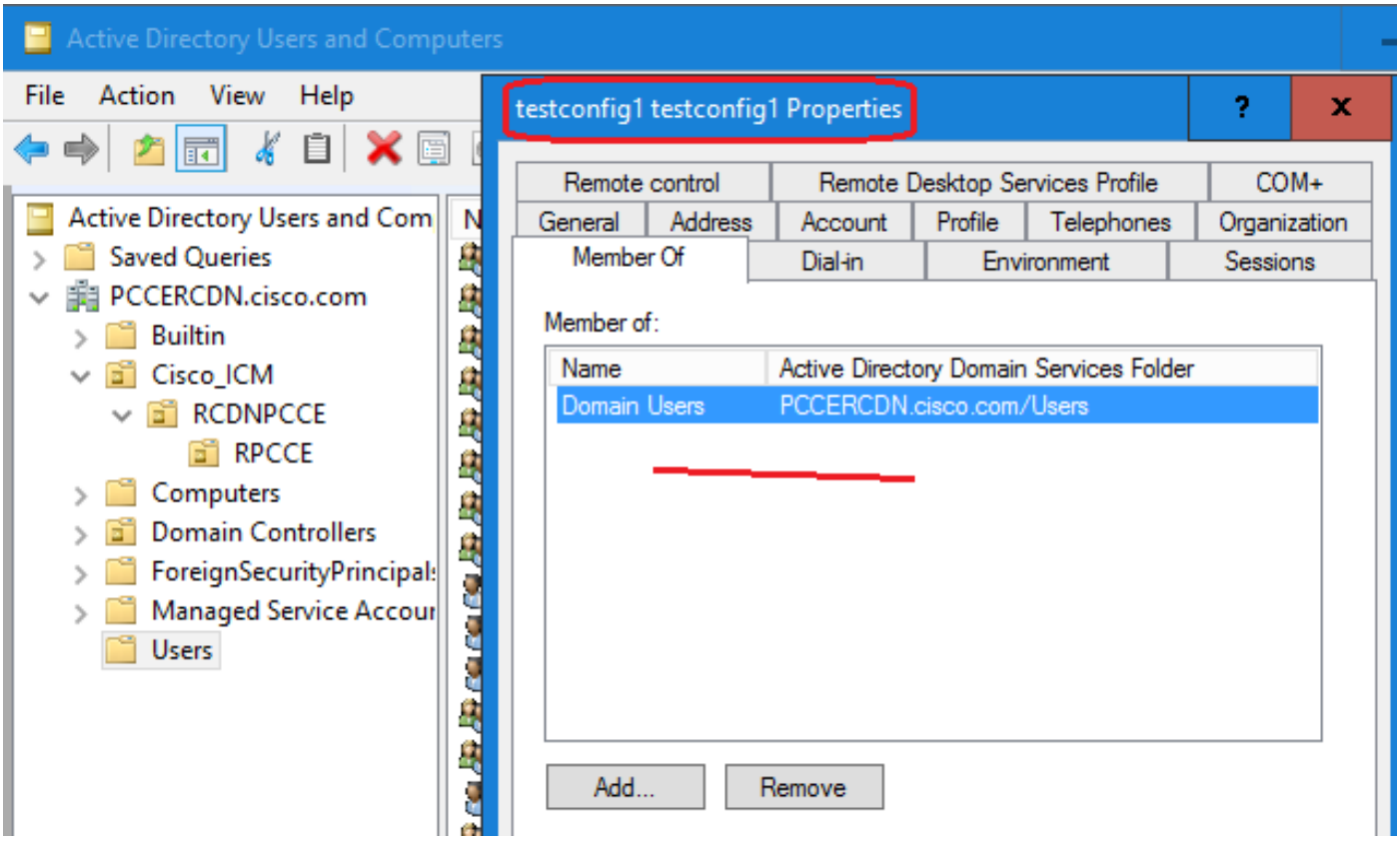


2. Accedere al server AW con un account di amministratore di dominio o di amministratore locale.

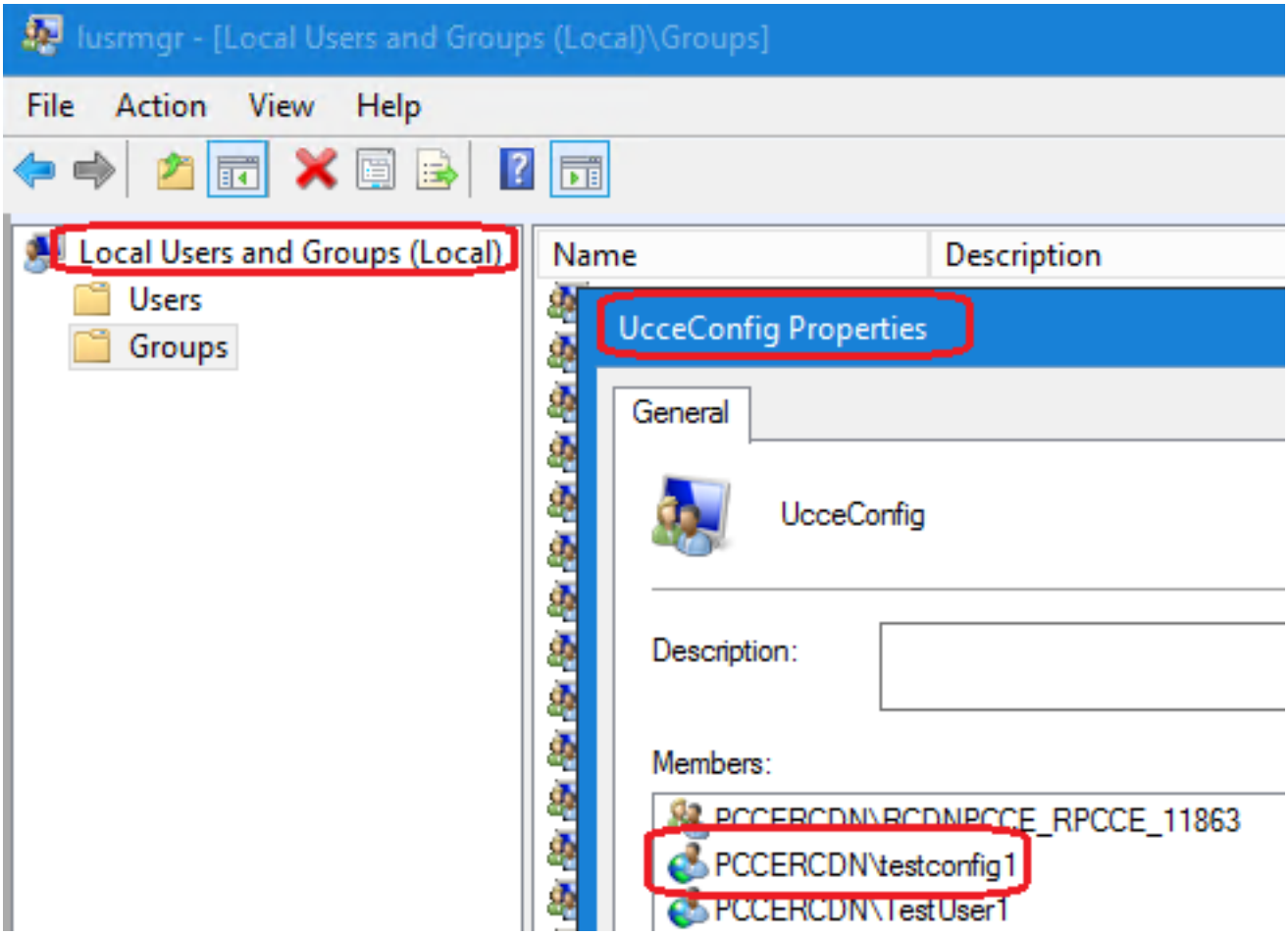
3. Aprire l'amministratore CCE sul AW. Passare alla scheda Impostazione utente e selezionare Amministratori. Aggiungere l'utente e selezionare il ruolo **ConfigAdmin**.



Nelle versioni precedenti alla 12.5 di PCCE questa modifica avrebbe aggiornato i gruppi di sicurezza Config nel dominio in un'unità organizzativa di istanza (OU, Organizational Unit), ma con la versione 12.5 per impostazione predefinita non è possibile aggiungere l'utente al gruppo AD. Come mostrato nell'immagine, non è presente alcun aggiornamento di questo utente nel gruppo di sicurezza della configurazione ICM del dominio.



4. Nel server AW in **Gestione computer > Utenti e gruppi locali > Gruppi** selezionare UcceConfig e aggiungere l'utente testconfig1.

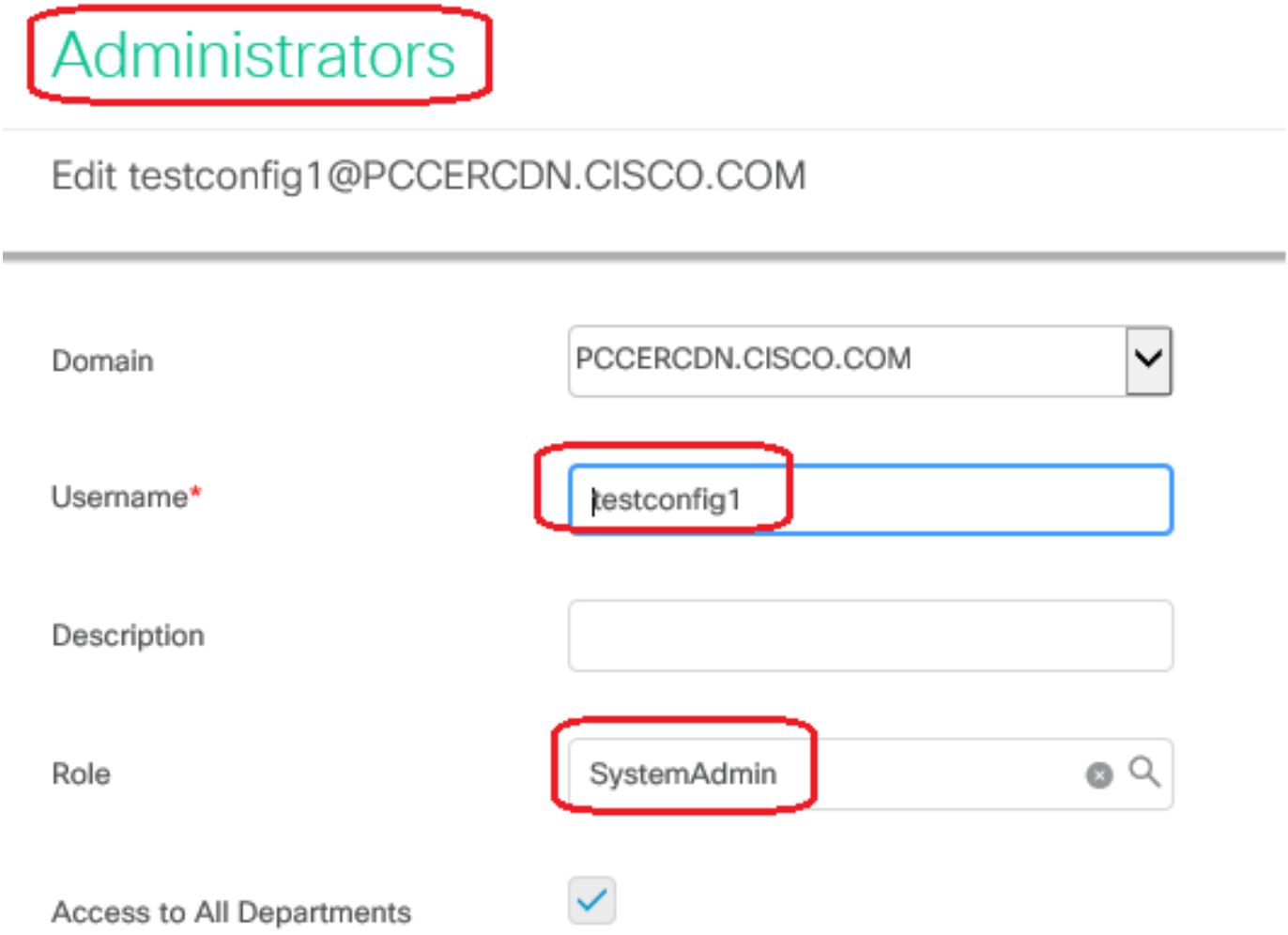


5. Uscire dal computer e accedere con le credenziali dell'utente testconfig1. Poiché l'utente dispone dei diritti di configurazione, è in grado di eseguire gli strumenti di configurazione CCE, quali CCE Admin, Script o Internet Script Editor.

6. Tuttavia, se l'utente tenta di eseguire un task che richiede diritti di impostazione, l'operazione non riesce. Questo utente non ha accesso a tutte le risorse di amministrazione CCE o agli strumenti di installazione.

Come mostrato nell'immagine, l'utente testconfig1 nella distribuzione PCCE 4K tenta di eseguire la configurazione di Peripheral Gateway (PG) e il sistema limita la modifica con un messaggio di avviso.

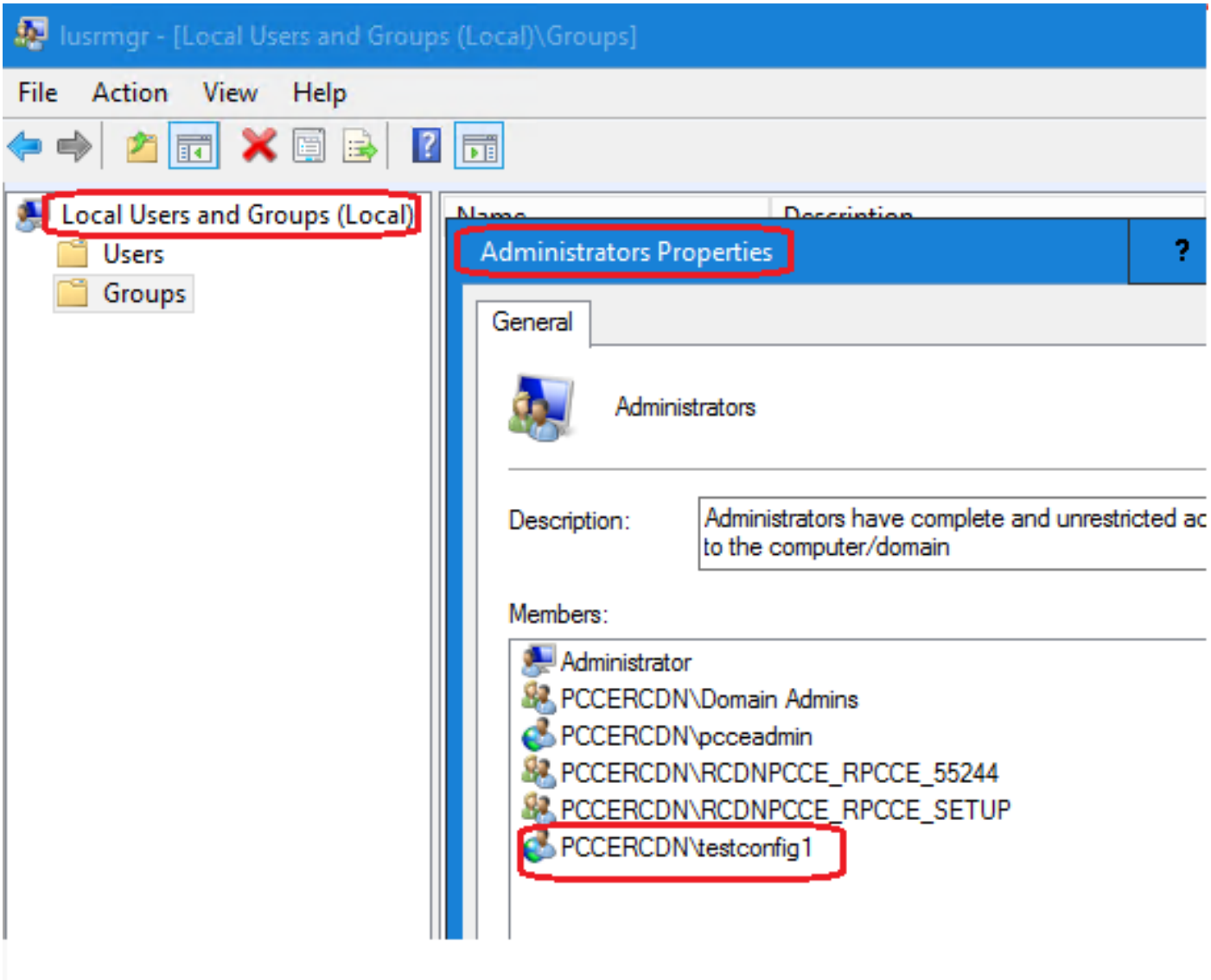
7. Se le attività aziendali richiedono che l'utente disponga dei diritti di impostazione insieme alla configurazione, è necessario assicurarsi che il ruolo utente venga modificato in SystemAdmin in CCEAdmin.



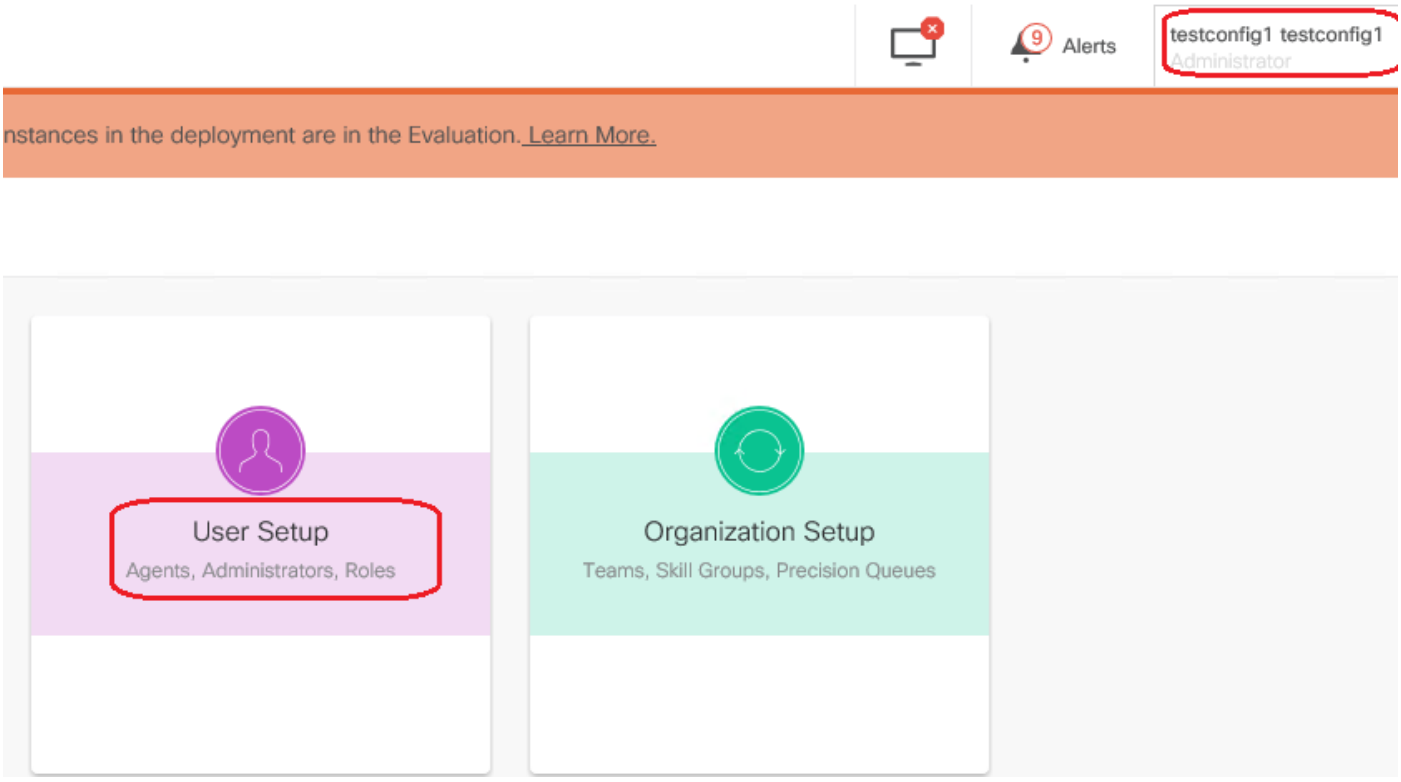
Il ruolo utente è stato aggiornato come 1 (SystemAdmin) nel database:

	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. Accedere al server AW con l'account dei diritti di amministratore di dominio o locale e tramite **gestione computer > Utenti e gruppi locali > gruppi** selezionare Gruppi e in Amministratori aggiungere l'utente all'utente.



10. L'utente è ora in grado di accedere a tutte le risorse dell'applicazione CCE in quel server AW e apportare le modifiche desiderate.



Verifica

La procedura di verifica fa effettivamente parte del processo di configurazione.

Risoluzione dei problemi

Non sono attualmente disponibili procedure specifiche per la risoluzione dei problemi relativi a questa configurazione.

Informazioni correlate

Guida all'amministrazione di PCCE

Documentazione e supporto tecnico – Cisco Systems