Konfigurieren der lokalen PCCE-Autorisierung

Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Hintergrundinformationen Konfigurieren Schritt 1: Konfigurieren Sie die Registrierungsberechtigungen. Schritt 2: Konfigurieren von Ordnerberechtigungen Schritt 3: Domänenbenutzerkonfiguration. Überprüfen Fehlerbehebung Zugehörige Informationen

Einführung

In diesem Dokument werden die Schritte beschrieben, die zum Entfernen der Abhängigkeit von Microsoft Active Directory (AD) erforderlich sind, um die Autorisierung lokal in PCCE-Komponenten (Package Contact Center Enterprise) zu verwalten.

Mitarbeiter: Meenakshi Sundaram, Ramiro Amaya und Anuj Bhatia, Cisco TAC Engineers.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Cisco Paket Contact Center Enterprise
- Microsoft Active Directory

Verwendete Komponenten

Die in diesem Dokument verwendeten Informationen basieren auf der PCCE 12.5(1)-Version.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen aller Schritte verstehen.

Hintergrundinformationen

Die PCCE 12.5-Version bietet Benutzerberechtigungen für lokale Benutzergruppen auf den Administration Servers (AW), wodurch Benutzer die Autorisierung aus Active Directory (AD) verschieben können. Dies wird von der Registrierung **ADSecurityGroupUpdate** gesteuert, die standardmäßig aktiviert ist. Dadurch wird die Verwendung von Microsoft AD Security Groups zur Kontrolle von Benutzerzugriffsrechten für Setup- und Konfigurationsaufgaben vermieden.

Hinweis: Die Unterstützung für die lokale Autorisierung wurde in Unified Contact Center Enterprise (UCCE) 12.0 eingeführt und wird jetzt von PCCE 12.5 unterstützt.

Registry Editor					
File Edit View Favorites Help)				
Registry Editor File Edit View Favorites Help 12.5	Ince Configuration ce tVersion utor ity tings nt ≡	Name (Default) ADSecurityGroupUpdate AWConfiguration AWType BlendedAgentSupport ConfigOnlyAW DeploymentSize Drive ICRRoot LimitUserAssociationByInstance ProductionMode UserListLocationButtonDisabled UserListSelectButtonDisabled VersionMajor VersionMinor	Type REG_SZ REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_SZ REG_SZ REG_SZ REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD	Data (value not set) 0x00000000 (0) 0x00000000 (1) 0x00000000 (0) 0x00000000 (0)	
> ODBC	_				
Policies RegisteredApplicat Numerine III	tions v				
Computer\HKEY_LOCAL_MACHINE\	Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\rpcce\AW				

Hinweis: Wenn für Unternehmen das vorherige Verhalten implementiert werden muss (AD-Autorisierung), kann das ADSecurityGroupUpdate-Flag in 1 geändert werden.

Konfigurieren

Um Berechtigungen für eine UcceConfig-Gruppe auf einem lokalen AW-Server zu erteilen, müssen zunächst Berechtigungen auf Registrierungsebene und dann auf Ordnerebene erteilt werden.

Schritt 1: Konfigurieren Sie die Registrierungsberechtigungen.

1. Führen Sie das Dienstprogramm regedit.exe aus.

2. Wählen Sie HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\WinSock2.

3. Wählen Sie unter Berechtigungen auf der Registerkarte Sicherheit die Gruppe **UCCEConfig** aus, und aktivieren Sie **die** Option **Vollzugriff zulassen**.



4. Wiederholen Sie die vorherigen Schritte, um der UCCEConfig-Gruppe für diese Registrierungen vollständige Kontrolle zu gewähren.

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

Schritt 2: Konfigurieren von Ordnerberechtigungen

1. Navigieren Sie in Windows Explorer zu <ICM Installed Directory>:\icm, und wählen Sie Eigenschaften aus.

2. Wählen Sie auf der Registerkarte Sicherheit die Option **UCCEConfig** aus, und aktivieren Sie **die Option Vollzugriff zulassen**.

me		icm Properties
CErts CiscoUtils		General Sharing Security Previous Versions Custom Object name: C.Nom
icm ir Open N Open in new window		Group or user names.
P Share with P Restore previous versions Include in library P Pin to Start	•	C C C C
V Send to		Ful control
r Cut Copy		Read & execute
Create shortcut		Wite 2
Delete Rename		For special permissions or advanced settings. Adve click Advanced.

3. Klicken Sie auf OK, um die Änderungen zu speichern.

4. Wiederholen Sie die vorherigen Schritte, um der **UCCEConfig-**Gruppe für C:\Temp folder volle Kontrolle zu gewähren.

- 5. Gehen Sie in SQL Management Studio wie folgt vor:
- a) Navigieren Sie zu Sicherheit > Anmeldungen.
- b) Suchen Sie <Gerätename>\UCCEConfig.
- c) Klicken Sie mit der rechten Maustaste, und wählen Sie Eigenschaften aus.
- d) Navigieren Sie zu Benutzerzuordnungen, und wählen Sie die AWDB-Datenbank aus.
 - e) Aktivieren Sie die Kontrollkästchen GeoTelAdmin, GeoTelGroup und public.
- f) Schritt d) für die HDS-Datenbank wiederholen.



Nachdem eine vorläufige Konfiguration erreicht wurde, befolgen Sie die Schritte, wie Sie einen Domänenbenutzer bewerben können, um Konfigurations- und Einrichtungsrechte zu erhalten.

Schritt 3: Domänenbenutzerkonfiguration.

1. Erstellen Sie einen Domänenbenutzer in AD. Für diesen exakten Testconfig1-Benutzer wurde erstellt.

	Active Directory Users and Computers						
File Action View Help							
🗢 🔿 🙍 🚮 🖬 🗶 🕻	1 @ 🕞 🛛 🗂 🔧 🖹	7 2 2					
Active Directory Users and Com Saved Queries PCCERCDN.cisco.com Builtin Cisco_ICM Computers Domain Controllers ForeignSecurityPrincipale Managed Service Accourtion Users	Name Name DonsUpdateProxy Domain Admins Domain Computers Domain Controllers Domain Guests Domain Guests Domain Users Enterprise Read-only Doma Group Policy Creator Owners Group Policy Creator Owners John Doe poceadmin Protected Users RAS and IAS Servers Ray Lewis Read-only Domain Controll Schema Admins LestAdmin testAdmin	Type Security Group Security Group Security Group Security Group Security Group Security Group Security Group Security Group User User User Security Group Security Group Security Group Security Group User	Description DNS clients who are per Designated administrato All workstations and ser All domain controllers i All domain guests All domain users Designated administrato Members of this group Built-in account for gue Members of this group Servers in this group can Members of this group Servers in this group can				
	TestUser1 TestUser1	User	A				

Active Deservoy Hears and Core Particle Deservoy Hears and Core Hears Deservoy Core Accore Deres	Plante B. Dornaan Ademan B. Dornaan Ademan Dornaan Camputers Dornaan Camputers Dornaan Gueens Dornaan Sueens Dornaan Su	Type Type Becarity Consp. Decority Consp. Secority Consp. Secority Consp. Secority Consp. Secority Consp. Const. Const. Const. Const. Decority Consp. Secority Consp. Secority Consp. Secority Consp. Secority Consp. Secority Consp. Secority Consp.	Creatingsteen Designated administration. All vonhalableres and sen All vonhalableres and sen All demain guards All demains vormiller (All demains vormiller) Mandess vormiller (Mandess vormiller) Mandess för blev genop c Budt en anzmand for gen Mandess of blev genop c Budt en anzmand for gen	Control of the second sec	$\begin{array}{c} \begin{array}{c} \\ \\ \end{array} \\ \\ \end{array} \\ \\ \end{array} \\ \\ \end{array} \\ \\ \begin{array}{c} \\ \\ \\ \end{array} \\ \\ \end{array} \\ \\ \end{array} \\ \\ \begin{array}{c} \\ \\ \\ \end{array} \\ \\ \end{array} \\ \\ \end{array} \\ \\ \begin{array}{c} \\ \\ \\ \\ \end{array} \\ \\ \end{array} \\ \\ \begin{array}{c} \\ \\ \\ \\ \\ \end{array} \\ \\ \end{array} \\ \\ \begin{array}{c} \\ \\ \\ \\ \\ \end{array} \\ \\ \end{array} \\ \\ \begin{array}{c} \\ \\ \\ \\ \\ \\ \\ \end{array} \\ \\ \end{array} \\ \\ \begin{array}{c} \\ \\ \\ \\ \\ \\ \\ \end{array} \\ \\ \end{array} \\ \\ \begin{array}{c} \\ \\ \\ \\ \\ \\ \\ \\ \end{array} \\ \\ \end{array} \\ \\ \begin{array}{c} \\ \\ \\ \\ \\ \\ \\ \\ \end{array} \\ \\ \end{array} \\ \\ \begin{array}{c} \\ \\ \\ \\ \\ \\ \\ \\ \end{array} \\ \\ \end{array} \\ \\ \begin{array}{c} \\ \\ \\ \\ \\ \\ \\ \\ \\ \end{array} \\ \\ \end{array} \\ \\ \begin{array}{c} \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \end{array} \\ \\ \end{array} \\ \\ \begin{array}{c} \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\$	
1 0		User User Viter Tercority Onicop	Merden of this program			

2. Melden Sie sich mit einem Domänenadmin- oder lokalen

Administratorkonto beim AW-Server an.

3. Öffnen Sie den CCE-Administrator auf dem AW. Navigieren Sie zur Benutzer-Setup-Karte, und wählen Sie Administratoren aus. Fügen Sie den Benutzer hinzu, und wählen Sie die Rolle **ConfigAdmin aus**.

0	ß	User Setup × Agents Administrators Roles	
Intrastructure Settings Inventory, Deployment Settings, License	MRD, Cal CISCO Unified Contact Ce	nter Enterprise Management	C Allana Mana
Management, Device Configuration	Administrato	ß	
	New Administrator		٥
	iii Consti	PODERCEN-CRECK.COM	
	Infrastructure Chemistre"	Teleficioning 7	
	Conception (
	Organization Bale	ConfigAdmin @ Q,	
	Access to Al Department		
	(P) Desires		
	Capacity		Careet See

Vor der Version 12.5 von PCCE hätte diese Änderung die Config Security Groups in der Domäne unter einer Instanz Organizational Unit (OU) aktualisiert. Mit 12.5 ist das Standardverhalten jedoch nicht, diesen Benutzer der AD-Gruppe hinzuzufügen. Wie im Bild gezeigt, gibt es in der Sicherheitsgruppe "ICM Config" der Domäne keine Aktualisierung dieses Benutzers.

Active Directory Users and Computers	5						
File Action View Help	testconfig1	testconfig	1 Properties			? X	
🗢 🔿 🙇 📰 🤞 📋 🗙 🗒 [Remote	control	Remote D	esktop Se	rvices Profile	COM+	1
Active Directory Users and Com N	General	Address	Account	Profile	Telephones	Organization	
> 📔 Saved Queries 🛛 🛔	Membe	r Of	Dial-in	Env	ironment	Sessions	1
✓ jii PCCERCDN.cisco.com A provide the second s	Member of	f:					1
Cisco ICM	Name		Active Directo	ory Domain	Services Folde	r	
V 🗊 RCDNPCCE	Domain	Users	PCCERCDN.	cisco.com/	/Users		
📓 RPCCE							
> 📫 Computers 🛛 🙀							
> 🛅 Domain Controllers 🛛 🙀							
> 📔 ForeignSecurityPrincipal:							
> 🦳 Managed Service Accour 🍟							
📔 Users							
	Add.	F	lemove				

4. Wählen Sie im AW-Server unter **Computerverwaltung > Lokale Benutzer und Gruppen > Gruppen** die Option UCCEConfig aus, und fügen Sie testconfig1-Benutzer hinzu.

💀 lusrmgr - [Local Users and Groups (Local)\Groups]					
File Action View Help					
← ⇒ 2	?				
Local Users and Groups (Local)	Name Description				
Users Groups	UcceConfig Properties				
	General				
	UcceConfig				
	Description:				
	Members: A PCCERCDN\RCDNPCCE_RPCCE_11863 A PCCERCDN\testconfig1 A PCCERCDN\testUser1				

5. Melden Sie sich vom Computer ab, und melden Sie sich mit den Anmeldeinformationen des Benutzers testconfig1 an. Da dieser Benutzer über Konfigurationsrechte verfügt, kann er CCE-Konfigurationstools wie CCE Admin, Script oder Internet Script Editor ausführen.

6. Wenn der Benutzer jedoch versucht, eine Aufgabe auszuführen, die Setup-Rechte erfordert, schlägt er fehl. Dieser Benutzer hat keinen Zugriff auf alle CCE-Administrator-Ressourcen oder - Setup-Tools.

Wie im Bild gezeigt, versucht der Benutzer testconfig1 in der PCCE 4K-Bereitstellung, die Konfiguration des Peripheral Gateway (PG) auszuführen, und das System schränkt die Änderung durch eine Warnmeldung ein.



7. Wenn dieser Benutzer für eine Geschäftstätigkeit neben der Konfiguration über Setup-Rechte verfügen muss, müssen Sie sicherstellen, dass die Benutzerrolle in CCEAdmin in SystemAdmin geändert wird.

					-
		1 - A.	- -		
	min	IST	at	nrs	
7 MG		100	au	010	
					_

Edit testconfig1@PCCERCDN.CISCO.COM

Domain	PCCERCDN.CISCO.COM
Username*	testconfig1
Description	
Role	SystemAdmin 💿 🔍
Access to All Departments	

Die Benutzerrolle wurde in der Datenbank als 1 (SystemAdmin) aktualisiert:

	UserRole	UserGroupID	CustomerDefinitionID	UserGroupName	UserGroup Type	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

 Melden Sie sich beim AW-Server mit dem Domänenkonto oder dem lokalen Administratorberechtigungskonto an, und über Computerverwaltung > Lokale Benutzer und Gruppen > Gruppen wählen Sie Gruppen aus, und fügen Sie den Benutzer unter "Administratoren" dem Benutzer hinzu.

not stronger - [Local Users and Group	os (Local)\Groups]
File Action View Help	
🗢 🔿 📶 🔀 📑 🚺	
Local Users and Groups (Local)	Name Description Administrators Properties ? General Administrators Description: Administrators have complete and unrestricted actor to the computer/domain Members: Administrator Administrator PCCERCDN\Domain Admins PCCERCDN\pcceadmin PCCERCDN\RCDNPCCE_RPCCE_55244 PCCERCDN\RCDNPCCE_RPCCE_SETUP PCCERCDN\testconfig1

10. Der Benutzer kann nun auf alle Ressourcen der CCE-Anwendung in diesem AW-Server zugreifen und die gewünschten Änderungen vornehmen.





Überprüfen

Die Überprüfung ist Teil des Konfigurationsprozesses.

Fehlerbehebung

Es sind derzeit keine spezifischen Schritte zur Fehlerbehebung für diese Konfiguration verfügbar.

Zugehörige Informationen

PCCE-Administrationsleitfaden

Technischer Support und Dokumentation - Cisco Systems