Configurer l'autorisation locale UCCE 12.0(X)

Contenu

Introduction Conditions préalables Conditions requises Components Used Informations générales Configuration Étape 1. Configurer les autorisations du Registre Étape 2. Configurer les autorisations de dossier Vérification Dépannage

Introduction

Ce document décrit les étapes nécessaires pour supprimer la dépendance de Microsoft Active Directory (AD) à gérer les autorisations dans les composants Unified Contact Center Enterprise (CCE).

Contribué par Anuj Bhatia, ingénieur TAC Cisco.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco Unified Contact Center Enterprise
- Microsoft Active Directory

Components Used

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est actif, assurez-vous de bien comprendre l'impact potentiel de n'importe quelle étape.

Informations générales

La version UCCE 12.X fournit des privilèges d'appartenance aux utilisateurs aux groupes d'utilisateurs locaux sur le serveur d'administration local (AW), ce qui permet aux utilisateurs de

déplacer l'autorisation hors d'Active Directory (AD). Ceci est contrôlé par le Registre **ADSecSecurityGroupUpdate** qui, par défaut, est activé et évite l'utilisation des groupes de sécurité Microsoft AD pour contrôler les droits d'accès des utilisateurs pour effectuer des tâches de configuration et de configuration.

	^	Name	Туре	Data
4 🍶 AW		2b (Default)	REG_SZ	(value not set)
DCClient		#ADSecurityGroupUpdate	REG_DWORD	0x00000000 (0)
þ- 🎍 DMP		#AWConfiguration	REG_DWORD	0x00000001 (1)
þ 🦂 EMS		# AWType	REG_DWORD	Ch00000000 (0)
p - 🕌 EMT		BlendedAgentSupport	REG_DWORD	Ch00000000 (0)
b - ICM Configure		ConfigOnlyAW	REG_DWORD	0x00000000 (0)
ICM Monitor		Contract Size	REG_DWORD	Cx00000000 (0)
b Keal limeClient		and Drive	REG_SZ	с
p - B Updatecc		A ICRRoot	REG_SZ	C:\icm\rtpsl\aw
Currentversion		I imitUserAssociationRvInstance	REG DWORD	0x0000000 (0)

Note: Si l'entreprise souhaite choisir le comportement antérieur, l'indicateur ADSecSecurityGroupUpdate peut être remplacé par 1 qui permet la mise à jour vers Active Directory (AD)

Pour déplacer l'autorisation hors d'AD, il faut effectuer une tâche unique sur chaque machine serveur AW pour accorder les autorisations requises pour le groupe UcceConfig. Ce document vise à présenter les étapes nécessaires à la configuration de ces autorisations, ainsi qu'un exemple de mappage d'un utilisateur de domaine dans le groupe Configuration et configuration CCE.

Configuration

Pour octroyer des autorisations de groupe UcceConfig au serveur AW local, il faut procéder en deux étapes : d'abord, les autorisations sont fournies au niveau du registre, puis transmises au niveau du dossier.

Étape 1. Configurer les autorisations du Registre

- 1. Exécutez l'utilitaire regedit.exe.
- 2. Sélectionnez HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\WinSock2.

3. Dans Autorisations sous l'onglet Sécurité, sélectionnez **UcceConfig** group et cochez **Autoriser** l'option **Contrôle total**.



Winmgmt WinNat b-WinRM b-Winseck		
WinSoc WinSoc WinVer LOCAL_MACHP AND SERVER Server group File and Stor Services	Expand New + Find Delete Rename Export Permissions	nices\WinSoc
Security Group or user nam References Refere	copy kky Hame Nes: CCE AW HDS-24 Uses Confer Encre AW HDS-24 Usen) BI	
Permissions for Un Full Control Record Special permiss	Add	Deny
For special permis click Advanced.	sions or advanced settings.	Advanced

5

4. Répétez les étapes précédentes pour accorder le contrôle total au groupe UcceConfig pour les registres

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

Étape 2. Configurer les autorisations de dossier

- 1. Dans l'Explorateur Windows, sélectionnez C:\icm and go to Properties.
- 2. Dans l'onglet Sécurité, sélectionnez UcceConfig et cochez Autoriser l'option Contrôle total.

lame	^			L	icm P	roperties	
CErts Cisco	Open Open in new window		1	General Sharing Object name: Group or user na St CREATOR St SYSTEM	Security R C:Vom mes: OWNER	revious Versions	Customize
P P P	Share with Restore previous versions Include in library Pin to Start	•		C UcceConfig C To change permi Permissions for U	issions, click E	WoosConfig) 11 Edministration 91. Alto	Edt
i v	Send to Cut Copy	•	'	Full control Modify Read & execut List folder cont	te tents	***	
	Create shortcut Delete Rename			Read Write For special permi click Advanced.	ssions or adva	nced settings.	Advanced
	Properties						

3. Cliquez sur OK pour enregistrer la modification.

4. Répétez les étapes précédentes pour accorder un contrôle total au groupe **UcceConfig** pour C:\Temp folder.

Lorsque la configuration préliminaire du jour 0 a été effectuée, examinez les étapes permettant de promouvoir un utilisateur de domaine pour qu'il dispose de droits de configuration et de configuration.

Étape 3 : Configuration de l'utilisateur du domaine

1. Créez un utilisateur de domaine dans Active Directory, pour cet utilisateur Excercise testconfig1 a été créé.

 ▷ □ ○ ○ ○ Manag ○ <	syed UCCE SecurityPrincipal: ed Service Accour		FAC1HCSLoggerBLOGGER1B Pradeep serviceAccount sup-001 sup002 sup003 TestConfig testconfig user001 user002		User User User User User User User Security Group User User User		<
	>	<		ш		>	

2. Connectez-vous au serveur AW à l'aide d'un admin de domaine ou d'un compte d'administrateur local.

3. Dans le gestionnaire de configuration via l'outil Liste d'utilisateurs, ajoutez l'utilisateur et cochez l'option **de configuration**.

File Options Help	Fie Vew VM	
Compared Team Line Compared Team Lin	Peakure cardinal set calls v Optional Filter Candition Yake (Case Senative) Name v v v Servet Retrieve Cancel filter changes User Name Displaying 1 - 11 of 11 Intra-self-HCS120DC.ICM ManufHCS120DC.ICM Intersection-BerCS120DC.ICM ManufHCS120DC.ICM	Select Dexctory User User name * testcorfig1 Description

Avant la version 12.0, cette modification aurait mis à jour les groupes de sécurité Config dans le domaine sous une unité d'organisation (OU) d'instance, mais avec la version 12.0, le comportement par défaut est qu'elle n'ajoute pas cet utilisateur au groupe AD. Comme l'illustre l'image, il n'y a aucune mise à jour de cet utilisateur dans le groupe de sécurité de configuration ICM du domaine.

Config	Members				
ce	Name		Active Dir	ectory Domain S	Services Folder
	📕 👗 adva	nced12k	HCS12KE	C.ICM/Users	
	💄 confi	gUser	HCS12KD	C.ICM/Domain	Controllers/Cisco_ICM/.
	Stac1	Config	HCS12KD	C.ICM/Domain	Controllers/Cisco_ICM/.
	Stac1	hcs_Set.	HCS12KD	C.ICM/Domain	Controllers/Cisco_ICM/.
	👗 ise 12	knew cc.	HCS12KD	C.ICM/Users	
	🙎 iseus	er12k cc.	HCS12KE	C.ICM/Users	
	🙎 iseus	eroce C	HCS12KE	C.ICM/Users	
	🙎 new.	serise	HCS12KD	C.ICM/Users	
	2 .L.1.L		UCC10VD	CHALLER.	

4. Dans le serveur AW sous **Gestion de l'ordinateur > Utilisateurs et groupes locaux > Groupes**, sélectionnez UcceConfig et ajoutez l'utilisateur testconfig1 à celui-ci.



5. Déconnectez-vous de l'ordinateur et connectez-vous avec les identifiants de l'utilisateur testconfig1. Comme cet utilisateur dispose de droits de configuration, il pourra exécuter des outils de configuration CCE tels que Configuration Manager, Script ou Internet Script Editor.

6. Cependant, si l'utilisateur tente d'exécuter une tâche nécessitant des droits de configuration, il échoue.

Cet exemple illustre la configuration de test config1 user change device gateway (pg) et le système restreint la modification par un message d'avertissement.

		Explorer	>
Periph <u> </u>	0	The Peripheral data required for the proper operation of this explorer is not present in the system, or not accessible. The PG explorer is used to create this data.	

7. Si l'entreprise exige que cet utilisateur dispose de droits de configuration et de configuration, vous devez vous assurer que l'utilisateur est ajouté au groupe d'administrateurs locaux du serveur AW.

8. Afin d'atteindre, connectez-vous au serveur AW avec le compte de droits d'administration du domaine ou local et via **la gestion de l'ordinateur > Utilisateurs et groupes locaux > groupes** sélectionnez Groupes et dans Administrateurs ajoutez l'utilisateur à l'utilisateur.



9. Dans l'outil de liste Configuration Manager via User, sélectionnez l'utilisateur et activez l'option de configuration.

ł			User List		
Select filter data			Abributes		
Customer Feature control set	(Ab)	* *	Domain name	BORA.COM Select Directory User	v
Optional Filter	Condition	Value (Case Sensitive)	User :		
None v	~	×	User name *	lestconfig1	
Seve	Retrieve	Cancel filter changes	Description		
User			Permissions :		
Name Name anubhat2@bora.com		Displaying 1 - 2 of 2	Customer	All Customens	¥
testconfig1@BORA.CO	М		Feature control set	<none> (Unrestricted access to tools)</none>	¥
			■ Configuration	NOTE:	
			Read only	Based on registry settings the Configuration and Setup check boxes will include the user as a member of one or both of the ICM Society on the	
			 Setup 	to the local Degris where the Line List Teal is	

10. L'utilisateur peut désormais accéder à toutes les ressources de l'application CCE sur ce serveur AW et apporter les modifications souhaitées.

Vérification

La procédure de vérification fait en fait partie du processus de configuration.

Dépannage

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