Configurez les enregistrements de SIP pour authentifier et autoriser sur une base par utilisateur (MRA) pour CUCM 11.5

Contenu

Introduction

Ce document décrit le comportement amélioré dans Cisco Unified Communications Manager (CUCM) qui fournit une couche supplémentaire d'authentification d'ID utilisateur dans les messages de REGISTRE de Protocole SIP (Session Initiation Protocol) contre la méthode d'authentification en cours seulement à l'autoroute.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Gestion et configuration CUCM
- SIP Portocol
- Autoroute du serveur de communication vidéo (VCS)

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco Unified Communications Manager 11.5 et plus tard
- Autoroute du serveur de communication vidéo (VCS)

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est vivant, assurez-vous que

vous comprenez l'impact potentiel de n'importe quelle commande.

Informations générales

Dans le passé, l'enregistrement de périphérique par l'autoroute du serveur de communication vidéo (VCS) fonctionne quand le périphérique envoie le nom d'utilisateur et mot de passe par l'intermédiaire du Protocole HTTP (Hypertext Transfer Protocol). L'autoroute alors authentifie le nom d'utilisateur et permet au périphérique pour se poursuivre par l'enregistrement vers CUCM sans davantage de vérification.

Le nouveau comportement est que maintenant CUCM vérifie le message de REGISTRE de SIP et s'assure que l'ID utilisateur a l'association appropriée au périphérique. Par cette caractéristique l'ID utilisateur devrait autoriser avant qu'il s'enregistre dans le CUCM ; , fournit donc le prochain niveau de protection contre le périphérique de réseau externe/inconnu. Ceci s'assure que le REGISTRE de SIP est autorisé, c.-à-d. seulement un périphérique valide associé avec l'utilisateur valide devrait s'enregistrer. S'il n'y a aucune association d'ID utilisateur aux anomalies d'enregistrement de périphérique puis avec le code de 401 réponses.

Historique de fond

- CSCuu97283
- ID CVE-2015-6410 CVE

Limites

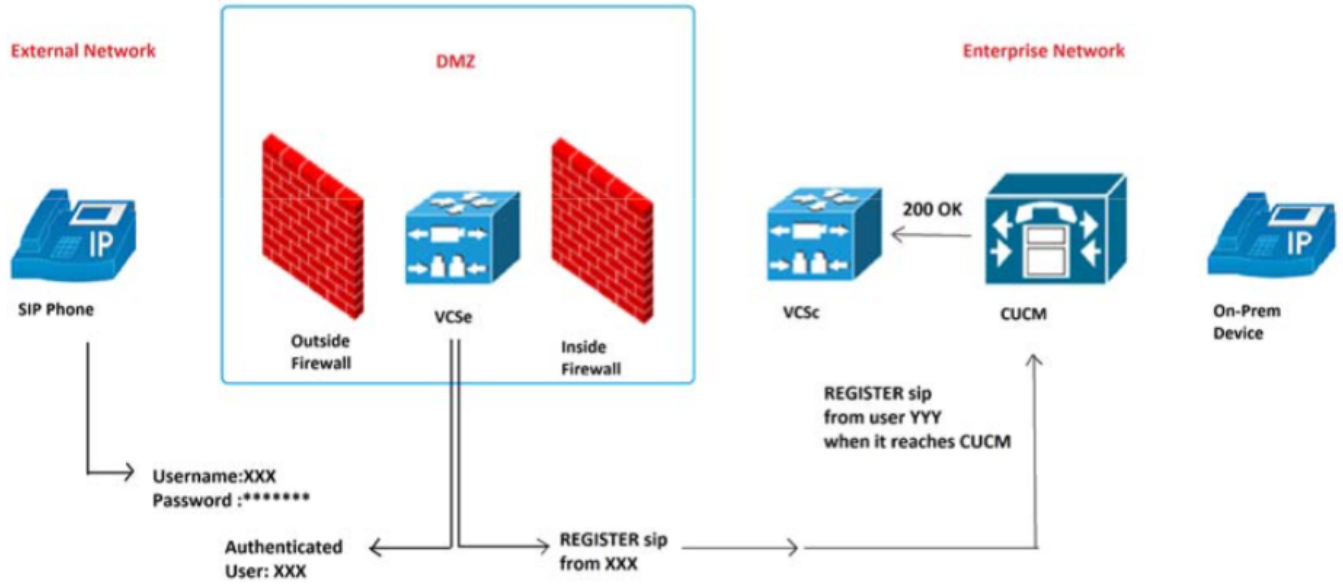
- Seulement téléphones SIP d'affects
- Les enregistrements de Sur-site sont inchangés

Configurez

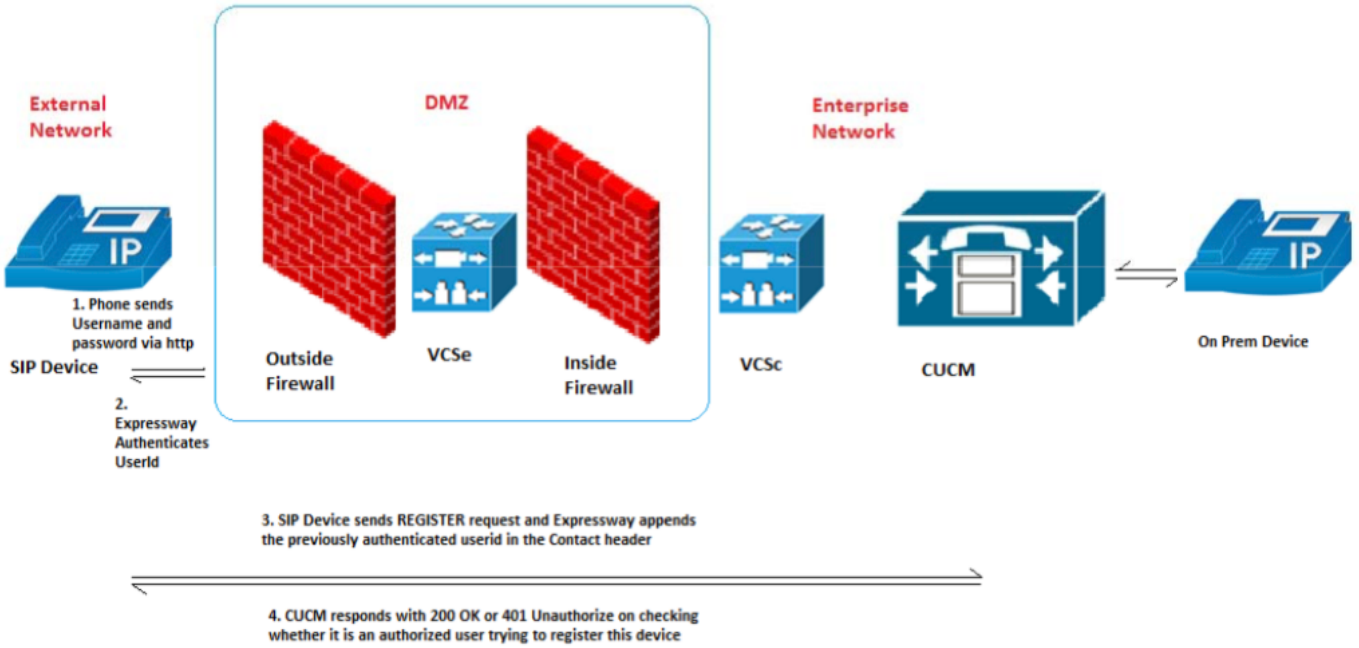
Diagramme du réseau

Composants utilisés (vieux contre. Nouvelle architecture)

Vieille image de comportement :



Nouvelle image de comportement :



Configurations

Nouveau paramètre de service pour basculer cette caractéristique "Marche/Arrêt" : **Système > paramètres de service > *serveur* > Cisco CallManager > autorisation d'enregistrement de SIP activée**

Valeurs :

- Vrai - (par défaut)
- Faux

L'association correcte d'ID utilisateur au périphérique correct détermine si l'enregistrement de SIP

autorise ou des anomalies.

La demande de processus d'autorisation d'enregistrement suit ces scénarios :

Scénario 1. Si l'ID utilisateur n'est pas présent dans le message de REGISTRE qu'il devrait autorise et l'OK 200 est envoyé.

Remarque: Ceci s'assure sur-prem l'Interopérabilité et la compatibilité ascendante avec des versions plus anciennes d'autoroute.

Scénario 2. Si l'ID utilisateur est présent dans le message de REGISTRE puis…

- SI l'ID utilisateur apparie le champ de propriétaire-id en page de configuration de téléphone CUCM, ALORS autorisez et envoyez l'OK 200
- SI l'ID utilisateur apparie l'association d'ID utilisateur avec le périphérique dans la page de configuration d'utilisateur final CUCM, ALORS autorisez et envoyez l'OK 200
- SI le champ de propriétaire-id est vide et association de périphérique à l'utilisateur final n'existe pas, ALORS autorisez et envoyez l'OK 200
- AUTREMENT SI aucune correspondance, ALORS N'ÉCHOUENT et envoient 401 non autorisés

Scénario 3. Si le message de REGISTRE contient plus d'un ID utilisateur de différentes valeurs, ALORS L'ÉCHOUER et envoient 401 non autorisés.

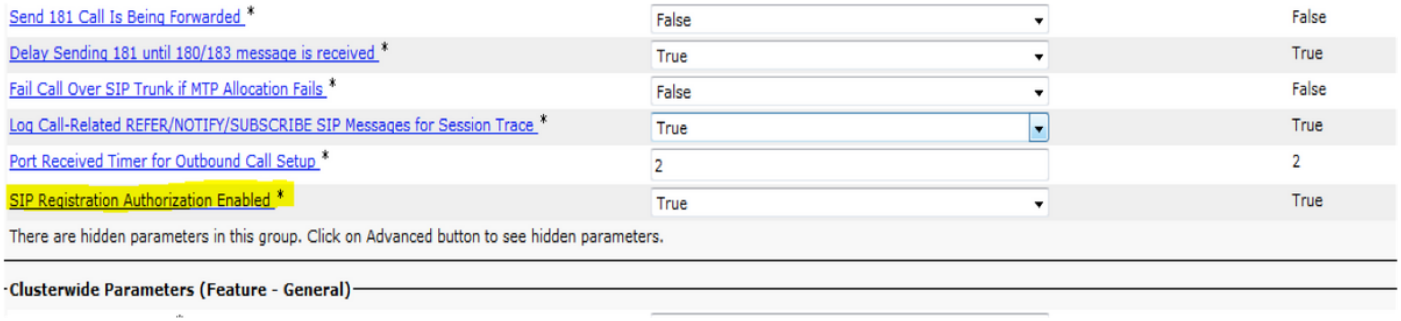
Remarque: Seulement l'autoroute remplissent ces en-têtes d'ID utilisateur

Tableau de résultats de cas d'utilisation

Nombre	Jeux d'essai	Autorisation d'enregistrement de SIP activée	Résultat prévu
1	Le paramètre d'ID utilisateur dans l'en-tête de contact n'est pas présent	Vrai	Autorisez (OK 200)
2	Le paramètre d'ID utilisateur dans l'en-tête de contact s'assortit avec OwnerId en page de config de téléphone	Vrai	Autorisez (OK 200)
3	Le paramètre d'ID utilisateur dans l'en-tête de contact s'assortit avec l'ID utilisateur associé à un périphérique en page d'utilisateur.	Vrai	Autorisez (OK 200)
4	L'en-tête d'ID utilisateur en contact s'assortit avec l'ownerId en page de config de téléphone, n'apparie pas avec l'ID utilisateur configuré en page d'utilisateur	Vrai	Autorisez (OK 200)
5	L'en-tête d'ID utilisateur en contact s'assortit avec l'ID utilisateur en page d'utilisateur, n'apparie pas avec OwnerId en page de config de téléphone	Vrai	Autorisez (OK 200)
6	OwnerId en page de config de téléphone est vide et le périphérique a pas utilisateur associé en page d'utilisateur	Vrai	Autorisez (OK 200)
7	OwnerId dans la page et l'ID utilisateur de config de téléphone configurés pour un périphérique en page d'utilisateur, mais aucune correspondance	Vrai	401 non autorisé

8	ne fondent Plus d'un ID utilisateur actuel dans l'en-tête de contact.	Vrai	401 non autorisé
9	Plusieurs ID utilisateur configuré pour un périphérique en page d'utilisateur	Vrai	Autorisez (ok 200)
10	ID utilisateur d'Unescaping	Vrai	Autorisez (ok 200)
11	Régénérez le registre	Vrai	Mêmes que le message initial de REGISTRE
12	L'en-tête d'ID utilisateur en contact est chaîne vide, OwnerId et ID utilisateur non configurés pour le périphérique	Vrai	Autorisez (ok 200)
13	L'en-tête d'ID utilisateur en contact est chaîne vide, OwnerId/ID utilisateur configuré pour le périphérique	Vrai	401 non autorisé
14	L'ID utilisateur est présent dans l'en-tête de contact, OwnerId/ID utilisateur configuré pour le périphérique, mais aucune correspondance trouvée	Faux	OK 200
15	Plus d'un ID utilisateur actuel dans l'en-tête de contact	Faux	OK 200
16	L'en-tête d'ID utilisateur en contact est chaîne vide, ownerId /UserId configuré pour le périphérique	Faux	OK 200

Activez la caractéristique par l'intermédiaire du paramètre de service de gestionnaire de transmissions (CCM). Il est allumé par défaut et aucune autre configuration n'est exigée.



Vérifiez

En-tête de contact

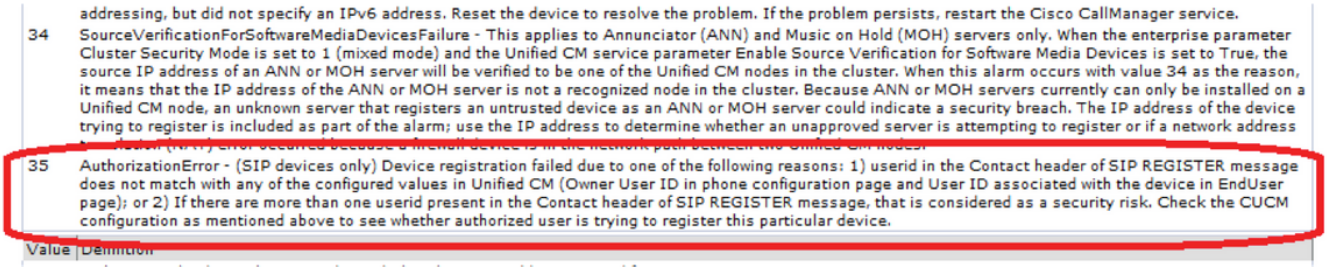
CUCM vérifie l'en-tête de contact du message de REGISTRE pour la modification par l'autoroute

```
Contact: <sip:ffeffb75-880e-f58f-a8ec-f5025d0f9136@10.50.179.6:5060;transport=tcp;orig-
hostport=192.168.0.121:55854>;+sip.instance="<urn:uuid:00000000-0000-0000-0000-
00506005457e>";+u.sip!model.ccm.cisco.com="604";+u.sip!userid.ccm.cisco.com="mjavie
r";+u.sip!serialno.ccm.cisco.com=A1AZ20D00153;audio=TRUE;video=TRUE;mobility="fixed";
duplex="full";description="TANDBERG-SIP"
```

Nouvelle alarme (AuthorizationErrorwithWarningLevel)

Une nouvelle alarme (AuthorizationErrorwithWarningLevel) est maintenant disponible quand il y a

panne d'autorisation d'enregistrement de SIP



Value	Definition
	addressing, but did not specify an IPv6 address. Reset the device to resolve the problem. If the problem persists, restart the Cisco CallManager service.
34	SourceVerificationForSoftwareMediaDevicesFailure - This applies to Annunciator (ANN) and Music on Hold (MOH) servers only. When the enterprise parameter Cluster Security Mode is set to 1 (mixed mode) and the Unified CM service parameter Enable Source Verification for Software Media Devices is set to True, the source IP address of an ANN or MOH server will be verified to be one of the Unified CM nodes in the cluster. When this alarm occurs with value 34 as the reason, it means that the IP address of the ANN or MOH server is not a recognized node in the cluster. Because ANN or MOH servers currently can only be installed on a Unified CM node, an unknown server that registers an untrusted device as an ANN or MOH server could indicate a security breach. The IP address of the device trying to register is included as part of the alarm; use the IP address to determine whether an unapproved server is attempting to register or if a network address
35	AuthorizationError - (SIP devices only) Device registration failed due to one of the following reasons: 1) userid in the Contact header of SIP REGISTER message does not match with any of the configured values in Unified CM (Owner User ID in phone configuration page and User ID associated with the device in EndUser page); or 2) If there are more than one userid present in the Contact header of SIP REGISTER message, that is considered as a security risk. Check the CUCM configuration as mentioned above to see whether authorized user is trying to register this particular device.

Dépannez

Recherchez les tentatives d'autorisation dans CCM la sortie de débogage de suivis

Exemples réussis d'autorisation :

Scénario 1 :

Contact: <sip:ffeffb75-880e-f58f-a8ec-f5025d0f9136@10.50.179.6:5060;transport=tcp;orig-hostport=192.168.0.121:55854>;+sip.instance="<urn:uuid:00000000-0000-0000-0000-00506005457e>";+u.sip!model.ccm.cisco.com="604";**+u.sip!userid.ccm.cisco.com="mjavier"**;+u.sip!serialno.ccm.cisco.com=A1AZ20D00153;audio=TRUE;video=TRUE;mobility="fixed";duplex="full";description="TANDBERG-SIP"

Scénario 2 :

Contact: <sip:ffeffb75-880e-f58f-a8ec-f5025d0f9136@10.50.179.6:5060;transport=tcp;orig-hostport=192.168.0.121:55854>;+sip.instance="<urn:uuid:00000000-0000-0000-0000-00506005457e>";+u.sip!model.ccm.cisco.com="604";**+u.sip!userid.ccm.cisco.com="mjavier"**;+u.sip!serialno.ccm.cisco.com=A1AZ20D00153;audio=TRUE;video=TRUE;mobility="fixed";duplex="full";description="TANDBERG-SIP"

Exemple d'autorisation défaillante et d'alarme :

Contact: <sip:ffeffb75-880e-f58f-a8ec-f5025d0f9136@10.50.179.6:5060;transport=tcp;orig-hostport=192.168.0.121:55854>;+sip.instance="<urn:uuid:00000000-0000-0000-0000-00506005457e>";+u.sip!model.ccm.cisco.com="604";**+u.sip!userid.ccm.cisco.com="mjavier"**;+u.sip!serialno.ccm.cisco.com=A1AZ20D00153;audio=TRUE;video=TRUE;mobility="fixed";duplex="full";description="TANDBERG-SIP"