Dépannage de la vérification du certificat du serveur de trafic Expressway pour les services MRA

Table des matières

Introduction
Conditions préalables
Exigences
Composants utilisés
Informations générales
Chaîne CA de confiance
Vérification SAN ou CN
Changement De Comportement
Versions inférieures à X14.2.0
Versions de X14.2.0 et ultérieures
Scénarios de dépannage
1. L'autorité de certification qui a signé le certificat distant n'est pas approuvée
2. L'adresse de connexion (FQDN ou IP) ne figure pas dans le certificat
Comment le valider facilement
Solution
Informations connexes

Introduction

Ce document décrit le changement de comportement sur les versions Expressway de X14.2.0 et ultérieures liées à l'ID de bogue Cisco <u>CSCwc69661</u> ou à l'ID de bogue Cisco <u>CSCwa25108</u>.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration de base Expressway
- Configuration de base MRA

Composants utilisés

Les informations contenues dans ce document sont basées sur Cisco Expressway version X14.2 et ultérieures.

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 en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales Avec ce changement de comportement marqué par l'ID de bogue Cisco CSCwc6961

ou l'ID de bogue Cisco CSCwa25108

, le serveur de trafic sur la plate-forme Expressway effectue la vérification de certificat des noeuds de serveur Cisco Unified Communication Manager (CUCM), Cisco Unified Instant Messaging & Presence (IM&P) et Unity pour les services Mobile and Remote Access (MRA). Cette modification peut entraîner des échecs de connexion MRA après une mise à niveau sur votre plate-forme Expressway.

Le protocole HTTPS (Hypertext Transfer Protocol Secure) est un protocole de communication sécurisé qui utilise le protocole TLS (Transport Layer Security) pour chiffrer la communication. Il crée ce canal sécurisé en utilisant un certificat TLS qui est échangé lors de la connexion TLS. Ce serveur a deux objectifs : l'authentification (pour savoir à qui vous connectez la partie distante) et la confidentialité (le chiffrement). L'authentification protège contre les attaques de l'homme du milieu et la confidentialité empêche les pirates d'écouter et de falsifier la communication.

La vérification TLS (certificat) est effectuée en vue de l'authentification et vous permet de vous assurer que vous êtes connecté à la partie distante appropriée. La vérification se compose de

deux éléments individuels :

- 1. Chaîne d'autorités de certification (AC) de confiance
- 2. Autre nom du sujet (SAN) ou nom commun (CN)

Chaîne CA de confiance

Pour qu'Expressway-C puisse faire confiance au certificat que CUCM / IM&P / Unity envoie, il doit être en mesure d'établir un lien entre ce certificat et une autorité de certification (CA) de niveau supérieur (racine) à laquelle il fait confiance. Un tel lien, une hiérarchie de certificats qui lie un certificat d'autorité de certification racine, est appelé une chaîne de confiance. Pour pouvoir vérifier une telle chaîne de confiance, chaque certificat contient deux champs : Émetteur (ou 'Émis par') et Objet (ou 'Émis à').

Les certificats de serveur, tels que celui que CUCM envoie à Expressway-C, ont généralement leur nom de domaine complet (FQDN) dans le champ « Subject » du CN :

```
Issuer: DC=lab, DC=vngtp, CN=vngtp-ACTIVE-DIR-CA
Subject: C=BE, ST=Flamish-Brabant, L=Diegem, 0=Cisco, 0U=TAC, CN=cucm.vngtp.lab
```

Exemple de certificat de serveur pour CUCM cucm.vngtp.lab. Il contient le nom de domaine complet dans l'attribut CN du champ Objet ainsi que d'autres attributs tels que le pays (C), l'état (ST), l'emplacement (L), ... Nous pouvons également voir que le certificat du serveur est distribué (émis) par une autorité de certification appelée vngtp-ACTIVE-DIR-CA.

Les autorités de certification de niveau supérieur (CA racine) peuvent également émettre un certificat pour s'identifier. Dans ce certificat d'autorité de certification racine, nous voyons que l'émetteur et l'objet ont la même valeur :

Issuer: DC=lab, DC=vngtp, CN=vngtp-ACTIVE-DIR-CA
Subject: DC=lab, DC=vngtp, CN=vngtp-ACTIVE-DIR-CA

Il s'agit d'un certificat distribué par une autorité de certification racine pour s'identifier.

Dans une situation typique, les autorités de certification racine n'émettent pas directement de certificats de serveur. Au lieu de cela, ils émettent des certificats pour d'autres CA. Ces autres AC sont alors appelées AC intermédiaires. Les autorités de certification intermédiaires peuvent à leur tour émettre directement des certificats de serveur ou des certificats pour d'autres autorités de certification intermédiaires. Nous pouvons avoir une situation où un certificat de serveur est émis par l'intermédiaire CA 1, qui à son tour obtient un certificat de l'intermédiaire CA 2 et ainsi de suite. Jusqu'à ce que l'autorité de certification intermédiaire obtienne son certificat directement de l'autorité de certification racine :

Server certificate : Issuer: DC=lab, DC=vngtp, CN=vngtp-intermediate-CA-1 Subject: C=BE, ST=Flamish-Brabant, L=Diegem, O=Cisco, OU=TAC, CN=cucm.vngtp.lab Intermediate CA 1 certificate : Issuer: DC=lab, DC=vngtp, CN=vngtp-intermediate-CA-2 Subject: DC=lab, DC=vngtp, CN=vngtp-intermediate-CA-1 Intermediate CA 2 certificate : Issuer: DC=lab, DC=vngtp, CN=vngtp-intermediate-CA-3 Subject: DC=lab, DC=vngtp, CN=vngtp-intermediate-CA-2 . . . Intermediate CA n certificate : Issuer: DC=lab, DC=vngtp, CN=vngtp-ACTIVE-DIR-CA Subject: DC=lab, DC=vngtp, CN=vngtp-intermediate-CA-n Root CA certificate : Issuer: DC=lab, DC=vngtp, CN=vngtp-ACTIVE-DIR-CA Subject: DC=lab, DC=vngtp, CN=vngtp-ACTIVE-DIR-C

Maintenant, pour qu'Expressway-C puisse faire confiance au certificat de serveur que CUCM envoie, il doit être en mesure de construire la chaîne de confiance à partir de ce certificat de serveur jusqu'à un certificat d'autorité de certification racine. Pour ce faire, nous devons télécharger le certificat d'autorité de certification racine ainsi que tous les certificats d'autorité de certification racine ainsi que tous les certificats d'autorité de certification racine ainsi que tous les certification racine aurait directement émis le certificat de serveur de CUCM) dans le magasin de confiance d'Expressway-C.

Remarque : bien que les champs Émetteur et Objet soient faciles à créer de manière lisible, CUCM n'utilise pas ces champs dans le certificat. À la place, il utilise les champs « Identificateur de clé d'autorité X509v3 » et « Identificateur de clé d'objet X509v3 » pour construire la chaîne de confiance. Ces clés contiennent des identifiants pour les certificats qui sont plus précis que d'utiliser les champs Subject/Issuer : il peut y avoir 2 certificats avec les mêmes champs Subject/Issuer mais l'un d'eux est expiré et l'autre est toujours valide. Ils auraient tous deux un identifiant de clé d'objet X509v3 différent, de sorte que CUCM puisse toujours déterminer la chaîne de confiance correcte.

Ce n'est pas le cas pour Expressway, bien que selon l'ID de bogue Cisco <u>CSCwa12905</u> et qu'il ne soit pas possible de télécharger deux certificats différents (auto-signés par exemple) dans le magasin de confiance d'Expressway qui ont le même nom commun (CN). La façon de corriger cela, c'est d'utiliser des certificats signés par l'autorité de certification ou d'utiliser des noms communs différents pour cela ou de voir qu'il utilise toujours le même certificat (potentiellement par le biais de la fonctionnalité de réutilisation de certificat dans CUCM 14).

Vérification SAN ou CN

L'étape 1 vérifie le magasin d'approbations, mais toute personne qui a un certificat signé par une autorité de certification dans le magasin d'approbations serait alors valide. Cela n'est évidemment pas suffisant. Par conséquent, il y a une vérification supplémentaire qui confirme que le serveur auquel vous vous connectez spécifiquement est bien le bon. Il le fait en fonction de l'adresse pour

laquelle la demande a été faite.

Le même type d'opération se produit dans votre navigateur, alors laissez-nous regarder à travers un exemple. Si vous naviguez vers <u>https://www.cisco.com</u>, vous voyez une icône de verrou à côté de l'URL que vous avez entrée et cela signifie qu'il s'agit d'une connexion approuvée. Cela est basé à la fois sur la chaîne de confiance CA (de la première section) ainsi que sur le contrôle SAN ou CN. Si nous ouvrons le certificat (via le navigateur par un clic sur l'icône de verrouillage), vous voyez que le nom commun (vu sur le champ 'Émis à : ') est défini sur <u>www.cisco.com</u> et qui correspond exactement à l'adresse à laquelle nous voulions nous connecter. De cette façon, il peut être sûr que nous nous connectons au bon serveur (parce que nous faisons confiance à l'autorité de certification qui a signé le certificat et qui effectue la vérification avant qu'il distribue le certificat).

ertificate	×		
eral Details Certification Path		cisco	Products and Servic
Certificate Information			
This certificate is intended for the followin • Ensures the identity of a remote compute • Proves your identity to a remote compute • 2.16.840.1.113839.0.6.3 • 2.23.140.1.2.2	n g purpose(s): r Pr		
* Refer to the certification authority's statement f	for details.		
Issued to: www.cisco.com			
Issued by: HydrantID Server CA 01			
Valid from 2/16/2022 to 2/16/2023			

Lorsque nous examinons les détails du certificat et en particulier les entrées SAN, nous constatons que la même chose est répétée ainsi que d'autres FQDN :

how: <all></all>	~	
Field	Value	^
Certificate Policies	[1]Certificate Policy:	
CRL Distribution P	[1]CRL Distribution	
Subject Alternativ	DNS Name=cisco-i	
Subject Key Identi	b18ceccd49a5dfd74	
Enhanced Key Usage	Server Authenticatio	
SCT List	v1, adf7befa7cff10c	
Key Usage	Digital Signature, Ke	
🗊 Thumbprint	0dddb6ce30b00bd7	
ONS Name=cisco-imag	es cisco, com	
DNS Name=cisco.com		
DNS Name=www-01.ci	sco.com	
DNS Name=www-02.d	sco.com	
DNS Name=www-rtp.c	isco.com	
DNS Name=www.med	afiles-cisco.com	_
ONS Name=www.static	-cisco.com	
DNS Name=www1.cisc	o.com	~
	Edit Properties	Copy to File

Cela signifie que lorsque nous demandons à nous connecter à <u>https://www1.cisco.com</u> par exemple, cela s'affiche également comme une connexion sécurisée car elle est contenue dans les entrées SAN.

← → C www1.cisco.com		
יוןייוןי כוsco	$\leftrightarrow \rightarrow \mathbf{C}$ \blacksquare www1.cisco.com	
CISCO		սիսիս
		CISCO

Cependant, lorsque nous ne naviguons pas vers <u>https://www.cisco.com</u> mais directement vers l'adresse IP (<u>https://72.163.4.161</u>), alors il n'affiche pas une connexion sécurisée parce qu'il fait confiance à l'autorité de certification qui l'a signé mais le certificat qui nous a été présenté, ne contient pas l'adresse (72.163.4.161) que nous avons utilisée pour nous connecter au serveur.



Dans le navigateur, vous pouvez contourner ce paramètre, mais il s'agit d'un paramètre que vous pouvez activer sur les connexions TLS et qui n'est pas autorisé. Par conséquent, il est important que vos certificats contiennent les bons noms CN ou SAN que la partie distante prévoit d'utiliser afin de se connecter.

Changement De Comportement

Les services MRA s'appuient fortement sur plusieurs connexions HTTPS via Expressways vers les serveurs CUCM / IM&P / Unity pour s'authentifier correctement et collecter les bonnes informations spécifiques au client qui se connecte. Cette communication se produit généralement sur les ports 8443 et 6972.

Versions inférieures à X14.2.0

Dans les versions antérieures à X14.2.0, le serveur de trafic sur Expressway-C qui gère ces connexions HTTPS sécurisées n'a pas vérifié le certificat qui a été présenté par l'extrémité distante. Cela pourrait conduire à des attaques de l'homme du milieu. Dans la configuration MRA, il y a une option pour la vérification du certificat TLS par la configuration du 'Mode de vérification TLS' à 'Activé' quand vous ajouteriez soit CUCM / IM&P / serveurs Unity sous Configuration > Communications unifiées > serveurs Unified CM / noeuds IM and Presence Service / serveurs Unity Connection. L'option de configuration et la boîte d'informations correspondante sont présentées à titre d'exemple, ce qui indique qu'il vérifie le nom de domaine complet ou l'adresse IP dans le SAN, ainsi que la validité du certificat et s'il est signé par une autorité de certification de configure.

CISCO Cisco Expressway-C

Status >	System >	Configuration >	Applications >	Users >	Maintenance >
Unified (CM servers				You are here: Configuration >
Unified C	M server lookup	0]		
Unified CM	publisher address	S	cucmpub.vngtp.la	b	
Username			* administrator		i
Password			*		(j)
TLS verify	mode		On v (i)		
Deploymer	nt		Default deployme	ent 🗸 i	
AES GCM	support		Off v		
SIP UPDAT	E for session refr	esh	Off v		
ICE Passth	rough support		Off v i		



Cette vérification de certificat TLS n'est effectuée qu'au moment de la découverte des serveurs CUCM / IM&P / Unity et non au moment de la connexion MRA où les différents serveurs sont interrogés. Un premier inconvénient de cette configuration est qu'elle ne vérifie que l'adresse de l'éditeur que vous ajoutez. Il ne vérifie pas si le certificat sur les noeuds d'abonné a été correctement configuré lorsqu'il récupère les informations de noeud d'abonné (FQDN ou IP) dans

la base de données du noeud éditeur. Un deuxième inconvénient de cette configuration est que ce qui est annoncé aux clients MRA comme informations de connexion peut être différent de l'adresse de l'éditeur qui a été placée dans la configuration d'Expressway-C. Par exemple, sur CUCM, sous System > Server vous pouvez annoncer le serveur avec une adresse IP (10.48.36.215 par exemple) et ceci est ensuite utilisé par les clients MRA (via la connexion Expressway proxy) mais vous pouvez ajouter le CUCM sur Expressway-C avec le FQDN de cucm.steven.lab. Supposons donc que le certificat tomcat de CUCM contient cucm.steven.lab comme entrée SAN mais pas l'adresse IP, puis la détection avec 'TLS Verify Mode' défini sur 'On' réussit mais les communications réelles des clients MRA peuvent cibler un FQDN ou IP différent et donc échouer la vérification TLS.

Versions de X14.2.0 et ultérieures

A partir de la version X14.2.0, le serveur Expressway effectue la vérification du certificat TLS pour chaque requête HTTPS unique effectuée par le serveur de trafic. Cela signifie qu'il effectue également cette opération lorsque le « mode de vérification TLS » est défini sur « Désactivé » lors de la détection des noeuds CUCM / IM&P / Unity. Lorsque la vérification échoue, la connexion TLS ne se termine pas et la demande échoue, ce qui peut entraîner une perte de fonctionnalité, comme des problèmes de redondance ou de basculement, ou des échecs de connexion complets, par exemple. De même, lorsque le paramètre « TLS Verify Mode » est activé, cela ne garantit pas que toutes les connexions fonctionnent correctement, comme indiqué dans l'exemple ci-après.

Les certificats exacts que l'Expressway vérifie vers les noeuds CUCM / IM&P / Unity sont comme indiqué dans la section du guide d'ARM.

En plus de la vérification TLS par défaut, il y a aussi une modification introduite dans X14.2 qui pourrait annoncer un ordre de préférence différent pour la liste de chiffrement, qui dépend de votre chemin de mise à niveau. Cela peut provoquer des connexions TLS inattendues après une mise à niveau logicielle, car il peut arriver qu'avant la mise à niveau, il ait demandé le certificat Cisco Tomcat ou Cisco CallManager de CUCM (ou de tout autre produit disposant d'un certificat distinct pour l'algorithme ECDSA), mais qu'après la mise à niveau, il demande la variante ECDSA (qui est la variante de chiffrement plus sécurisée en fait que RSA). Les certificats Cisco Tomcat-ECDSA ou Cisco CallManager-ECDSA peuvent être signés par une autre autorité de certification ou simplement par des certificats auto-signés (par défaut).

Cette modification de l'ordre de préférence de chiffrement n'est pas toujours pertinente pour vous, car elle dépend du chemin de mise à niveau indiqué dans les notes de version d'Expressway X14.2.1. En bref, vous pouvez voir à partir de Maintenance > Security > Ciphers pour chacune des listes de chiffrement si elle ne précède pas "ECDHE-RSA-AES256-GCM-SHA384:" ou non. Si ce n'est pas le cas, il préfère le chiffrement ECDSA plus récent au chiffrement RSA. Si c'est le cas, vous avez le comportement précédent avec RSA qui a la préférence la plus élevée.

Cipher Preferences - ECDSA Cipher Preference Over RSA ECDSA certificates are preferred over RSA.

The following points lists the various upgrade path(s) that are mandatory for upgrading ciphers.

When upgrading from version lower than 14.0 to 14.2, the ECDSA would be preferred. If you prefer RSA certificates over ECDSA, then prefix the cipher string with "ECDHE-RSA-AES256-GCM-SHA384:" using either Web User Interface (Maintenance > Security > Ciphers) or CLI command (xConfiguration Ciphers).

When upgrading from version equal or higher than 14.0 to 14.2 or higher version, you have appended "ECDHE-RSA-AES256-GCM-SHA384:" to the default Ciphers List to prefer RSA certificates over ECDSA. If you prefer ECDSA certificates over RSA, then remove "ECDHE-RSA-AES256-GCM-SHA384:" from the cipher string using Web User Interface (Maintenance > Security > Ciphers) or CLI command 2 If you prefer ECDSA certific (xConfiguration Ciphers).

Any customer has a fresh install X14.2 image, ECDSA is being preferred. If you prefer RSA certificates over ECDSA, then prefix the cipher string with "ECDHE-RSA-AES256-GCM-SHA384:" using either Web User Interface (Maintenance > Security > Ciphers) or CLI command (xConfiguration Ciphers).

Dans ce scénario, la vérification TLS peut échouer de deux manières, qui sont décrites en détail plus loin :

- 1. L'autorité de certification qui a signé le certificat distant n'est pas approuvée
- a. Certificat auto-signé
- b. Certificat signé par une AC inconnue
- 2. L'adresse de connexion (FQDN ou IP) ne figure pas dans le certificat

Scénarios de dépannage

Les scénarios suivants présentent un scénario similaire dans un environnement de travaux pratiques où la connexion MRA a échoué après une mise à niveau d'Expressway de X14.0.7 à X14.2. Ils partagent des similitudes dans les journaux, cependant la résolution est différente. Les journaux sont simplement collectés par la journalisation de diagnostic (à partir de Maintenance > Diagnostics > Journalisation de diagnostic) qui a commencé avant la connexion MRA et qui s'est arrêtée après l'échec de la connexion MRA. Aucune journalisation de débogage supplémentaire n'a été activée pour cette application.

1. L'autorité de certification qui a signé le certificat distant n'est pas approuvée

Le certificat distant peut soit être signé par une CA qui n'est pas incluse dans le magasin de confiance de l'Expressway-C, soit être un certificat auto-signé (en fait aussi une CA) qui n'est pas ajouté dans le magasin de confiance du serveur de l'Expressway-C.

Dans cet exemple, vous pouvez observer que les requêtes qui vont à CUCM (10.48.36.215 - cucm.steven.lab) sont traitées correctement sur le port 8443 (réponse 200 OK) mais cela génère une erreur (réponse 502) sur le port 6972 pour la connexion TFTP.

```
<#root>
===Success connection on 8443===
2022-07-11T18:55:25.910+02:00 vcsc traffic_server[18242]: UTCTime="2022-07-11 16:55:25,910" Module="nett
2022-07-11T18:55:25.917+02:00 vcsc traffic_server[18242]: UTCTime="2022-07-11 16:55:25,916" Module="nett
2022-07-11T18:55:25.955+02:00 vcsc traffic_server[18242]: UTCTime="2022-07-11 16:55:25,955" Module="nett
2022-07-11T18:55:25.956+02:00 vcsc traffic_server[18242]: UTCTime="2022-07-11 16:55:25,955" Module="nett
200
    "
===Failed connection on 6972===
2022-07-11T18:55:26.000+02:00 vcsc traffic_server[18242]: UTCTime="2022-07-11 16:55:26,000" Module="nett
2022-07-11T18:55:26.006+02:00 vcsc traffic_server[18242]: UTCTime="2022-07-11 16:55:26,000" Module="nett
2022-07-11T18:55:26.006" Module="nett"
2022-
```

2022-07-11T18:55:26.016+02:00 vcsc traffic_server[18242]: UTCTime="2022-07-11 16:55:26,016" Module="net

```
2022-07-11T18:55:26.016+02:00 vcsc traffic_server[18242]: [ET_NET 0]

WARNING: Core server certificate verification failed for

(cucm.steven.lab).

Action=Terminate Error=self signed certificate server=cucm.steven.lab(10.48.36.215)

depth=0

2022-07-11T18:55:26.016+02:00 vcsc traffic_server[18242]: [ET_NET 0]

ERROR: SSL connection failed for

'cucm.steven.lab': error:1416F086:

SSL routines:tls_process_server_certificate:certificate verify failed

2022-07-11T18:55:26.024+02:00 vcsc traffic_server[18242]: UTCTime="2022-07-11 16:55:26,024" Module="net

502 connect failed
```

...

L'erreur « certificate verify failed » indique que l'Expressway-C n'a pas pu valider la connexion TLS. La raison de cette erreur est indiquée sur la ligne d'avertissement car elle indique un certificat auto-signé. Si la profondeur est 0, il s'agit d'un certificat auto-signé. Lorsque la profondeur est supérieure à 0, cela signifie qu'il a une chaîne de certificats et donc qu'il est signé par une CA inconnue (du point de vue d'Expressway-C).

Lorsque nous regardons dans le fichier pcap qui a été collecté aux horodatages mentionnés dans les journaux de texte, vous pouvez voir que CUCM présente le certificat avec CN comme cucmms.steven.lab (et cucm.steven.lab comme SAN) signé par steven-DC-CA à l'Expressway-C sur le port 8443.

eth0_diagnostic_logging_tcpdump00_vcsc_2022-07-11	16_55_44.pcap				
File Edit View Go Capture Analyze Statistics Telepho	ny Wireless Tools Help				
Ito antesidál					
-					
4691 2022-07-11 16:55:25,916610	10.48.36.46	35622 18,48,26,215	S443 TCP	C50	10000 178 74 35622 + 8443 [SYN] Secue Win=64240 Len=0 MSS=1468 SACK PERMu1 TSVal=878578415 TSecue WS=128
4692 2022-07-11 16:55:25.916953	10.48.36.215	8443 10.48.36.46	35622 TCP	CS0	74 8443 + 35622 [SYN, ACK] Seque Ackul Minu28960 Lenue MSSw1460 SACK PERMAI TSValw343633230 TSecrw878570435 MSw128
4693 2022-07-11 16:55:25.916973	10.48.36.46	35622 10.48.36.215	8443 TCP	C50	66 35622 + 8443 [ACK] Seq=1 Ack+1 Win+64256 Len+0 T5val+878570435 T5ecr+343633230
4694 2022-07-11 16:55:25.917832	10.48.36.46	35622 10.48.36.215	8443 TLSv1.2	CSB	583 Client Hello
4695 2022-07-11 16:55:25.938356	10.48.36.215	8443 10.48.36.46	35622 TLSv1.2	CS0	1514 Server Hello
4696 2022-07-11 16:55:25.938390	10.48.36.46	35622 10.48.36.215	\$443 TCP	CS0	66 35622 + 8443 [ACK] Seq=518 Ack=1449 Win=64128 Len=0 TSval=878570457 TSecr=343633251
4697 2022-07-11 16:55:25.938409	10.48.36.215	8443 10.48.36.46	35622 TLSv1.2	CS0	1470 Certificate, Server Key Exchange, Server Hello Done
4698 2022-07-11 16:55:25.938419	10.48.36.46	35622 10.48.36.215	8443 TCP	CSB	66 35622 + 8443 [ACK] Seq=\$18 Ack=2853 kin=63488 Len=0 TSval=878570457 TSecr=343633251
4699 2022-07-11 16:55:25.940107	10.45.36.46	35622 10.48.36.215	8443 TLSV1.2	CS8	192 Cilent Key Exchange, Change Cipher Spec, Encrypted Handshake Message
4/00 2022-0/-11 16:55:25.943034	10.48.36.215	3445 10.48.56.46	55622 TLSV1.2	C50	pes new session iicket, change cipner spec, Encrypten Hannshake Message
4701 2022-07-11 10:55:25.943051 4703 2022-07-11 16:55:25.943277	10.42.36.46	35622 10.46.36.215	8443 TI Sv1. 2	C50	ee J922 + Bees [AK] Schebee ACKESETS HINEMIZE LENE (SVELEG/BS/D001 (SCCHED-S0122)
4703 2022.07.11 16:55:25.943476	10.48.36.215	8443 18.48.36.46	35622 TCP	csa	66.243 + 35622 [JCK] Secul095 Jrkul121 Winu35822 Lenu8 TSV8]u333553256 TSecru828578462
4707 2022-07-11 16:55:25.954796	10.48.36.215	8443 10.48.36.46	35622 TCP	CSB	1514 8443 + 35622 [ACK] Seq=3095 Ack=3121 Win=35072 Len=1448 TSval=343633268 TSecr=878570462 [TCP segment of a reassembled PDU]
4708 2022-07-11 16:55:25.954842	10.48.36.46	35622 10.48.36.215	8443 TCP	CS0	66 35622 + 8443 [ACK] Seq=3121 Ack=4543 Win=64128 Len=0 TSval=878570473 TSecr=343633268
4709 2022-07-11 16:55:25.954861	10.48.36.215	8443 10.48.36.46	35622 TL5v1.2	CS0	1257 Application Data
4710 2022-07-11 16:55:25.954873	10.48.36.46	35622 10.48.36.215	8443 TCP	CS8	66 35622 + 8443 [ACK] Seq=3121 Ack=5734 Win=63488 Len=0 TSval=878570473 TSecr=343633268
4711 2022-07-11 16:55:25.955712	10.48.36.46	35622 10.48.36.215	8443 TLSv1.2	CSB	97 Encrypted Alert
4712 2022-07-11 16:55:25.955750	10.48.36.46	35622 10.48.36.215	8443 TCP	CS0	66 35622 + 8443 [FIN, ACK] Seq=3152 Ack=5734 Win=64128 Len=0 TSval=878570474 TSecr=343633268
4714 2022-07-11 16:55:25.956123	10.48.36.215	8443 10.48.36.46	35622 TL5v1.2	CS0	97 Encrypted Alert
4715 2022-07-11 16:55:25.956170	10.48.36.46	35622 10.48.36.215	8443 TCP	CSB	54 35622 + 8443 [RST] Seq=3153 Hin+0 Len+0
4716 2022-07-11 16:55:25.956232	10.48.36.215	8443 10.48.36.46	35622 TCP	CSB	66 8443 → 35622 [FIN, ACK] Seq=5765 ACK=3153 H1n=35072 Len=0 TSval=343633269 TSecF=878570474
 signedcertifette version: vi (2) serialNumber: 0x66000112866051 signetre (fabilithdSancryption) sister: rändsequence (0) valisity sobjectFubblicke(rinfo catention (id-ce-extroplayer) bitenion (id-ce-extroplayer) bitenion (id-ce-extroplayer) bitenion (id-ce-extroplayer) bitenion (id-ce-subjectations tetenion (id-ce-subjectations) centralNume: dislame (1) dislame: dislame (2) distame: dislame (2))) c=subjectAltname) b tifier) emtifier) emtifier) emtifier) extifier)				
 Extension (id-ms-application: algorithmidentifier (shaluithmidentifier) padding: 0 encrypted: 95ba763741637a2a52071efbu Certificate Length: 910 Certificate Length: 910 Certificate: 306203340620272a00302010 	rtificate-policies) yption) 8f227b9cecc7ec4a470c82b 2021062176f3fc2939a8044 (id	at-commonName= <mark>steven-DC-CA</mark> ,dc=S	teven,dc=lab)		

Mais lorsque nous examinons le certificat présenté sur le port 6972, vous pouvez voir qu'il s'agit d'un certificat auto-signé (l'émetteur est lui-même) avec le CN configuré comme cucm-EC.steven.lab. L'extension -EC indique qu'il s'agit du certificat ECDSA configuré sur CUCM.

th0_diagnostic_logging_tcpdump00_vcsc_2022+07+1 Edit View Go Capture Analyze Statistics Teleph	1_16_55_44.pcap hony Wireless Tools Help				
(∠● ■□\$\$\$ 9 + + 51 ∓ ± 🚍	<u>=</u> q q q <u>u</u>				
p.porte=6972					
	Source	Src port Destination	Cest port Protocol	DSOP VLAN	
4730 2022-07-11 16:55:26.006608	10.45.36.46	315/6 10.48.36.215	6972 TCP	CS0	74 315/6 4 6972 [STN] Stelle Winnersche Lenne Posities Sack_Permit Invarias/as/9525 ISECHE Mariza 74 315/6 4 6972 [STN] Stelle Arabier Lenne Posities Sack_Permit Invarias/as/9525 ISECHE Mariza 74 315/6 4 6972 [STN] Stelle Arabier Lenne Posities Sack_Permit Invarias/as/9525 ISECHE Mariza 74 315/6 4 6972 [STN] Stelle Arabier Lenne Posities Sack_Permit Invarias/as/9525 ISECHE Mariza 74 315/6 4 6972 [STN] Stelle Arabier Lenne Posities Sack_Permit Invarias/as/9525 ISECHE Mariza 74 315/6 4 6972 [STN] Stelle Arabier Lenne Posities Sack_Permit Invarias/as/9526 [Straff Arabier Stelle Arabie
4732 2022-07-11 16:55:26 006092	10.40.26.46	31576 10 40 26 215	6972 TCP	(50	24 07/4 * 332/0 [319, Mak] Septe Maket maintaine close role maintaine and and interpretation (Statement Statement
4733 2022.07.11 16:55:26.007100	10.42.35.45	21576 10.48.26.215	6972 TLSv1.2	cse	ses client wells
4734 2022-07-11 16:55:35 016350	10 48 36 215	6972 18 48 36 46	31576 TLSv1 2	C50	1512 Carupa Mallo Cartificata Carupa Yay Evchange
4735 2022-07-11 16:55:26.016391	10.48.36.46	31576 10.48.36.215	6972 TCP	C58	66 31576 + 6972 14/21 Sensitis arkitele kineda 128 Jeneñ TSval-875578535 TSerr-343633329
4736 2022-07-11 16:55:26.016408	10,48,36,215	6972 10.48.36.46	31576 TLSv1.2	cse	499 Certificate Request, Server Hello Done
4737 2022-07-11 16:55:26.016419	10.48.36.46	31576 10.48.36.215	6972 TCP	cse	66 31576 + 6972 [ACK] SequS18 ACK+1882 Win+63744 Len+0 TSval+878570535 TSecr=343633329
4738 2022-07-11 16:55:26.016703	10.48.36.46	31576 10.48.36.215	6972 TLSV1.2	cse	73 Alert (Level: Fatal, Description: Unknown CA)
4739 2022-07-11 16:55:26.016821	10.48.36.46	31578 10.48.36.215	6972 TCP	C50	74 31578 + 6972 [SYN] Seque Win=64240 Len=0 MSS=1460 SACK PERM=1 TSval=878570535 TSecr=0 MS=128
4740 2022-07-11 16:55:26.016965	10.48.36.46	31576 10.48.36.215	6972 TCP	C50	66 31576 + 6972 [RST, ACK] Seg=525 Ack=1882 Win=64128 Len=0 TSval=878570535 TSecr=343633329
4741 2022-07-11 16:55:26.016984	10,48,36,215	6972 10.48.36.46	31578 TCP	CSB	74 6972 + 31578 [SYN, ACK] Seq+0 Ack+1 Hin+28960 Len+0 MSS+1460 SACK PERM+1 TSV81+343633330 TSecr+878570535 W
4742 2022-07-11 16:55:26.017009	10,48,36,46	31578 10.48.36.215	6972 TCP	CSB	66 31578 + 6972 [ACK] Seg=1 Ack=1 Win=64256 Len=0 TSval=878570535 TSecr=343633330
4743 2022-07-11 16:55:26.017101	10.48.36.215	6972 10.48.36.46	31576 TCP	CS8	66 6972 + 31576 [FIN, ACK] Seq=1882 Ack=525 Win=30080 Len=0 TSval=343633330 TSecr=878570535
4744 2022-07-11 16:55:26.017121	10.48.36.46	31576 10.48.36.215	6972 TCP	CS8	54 31576 + 6972 [RST] Seq=525 Win+0 Len+0
4745 2022-07-11 16:55:26.017218	10.48.36.46	31578 10.48.36.215	6972 TLSv1.2	CS0	583 Client Hello
4746 2022-07-11 16:55:26.024226	10.48.36.215	6972 10.48.36.46	31578 TLSv1.2	CS0	1514 Server Hello, Certificate, Server Key Exchange
4747 2022-07-11 16:55:26.024265	10.48.36.46	31578 10.48.36.215	6972 TCP	CS0	66 31578 + 6972 [ACK] Seq=518 Ack=1449 Win=64128 Len=0 TSval=878570543 TSecr=343633337
4748 2022-07-11 16:55:26.024298	10.48.36.215	6972 10.48.36.46	31578 TLSv1.2	CS0	500 Certificate Request, Server Hello Done
4749 2022-07-11 16:55:26.024309	10.48.36.46	31578 10.48.36.215	6972 TCP	CSB	66 31578 → 6972 [ACK] Seq=518 Ack=1883 Win+63744 Len+0 TSv01=878570543 TSecr=343633337
4750 2022-07-11 16:55:26.024548	10.48.36.46	31578 10.48.36.215	6972 TLSv1.2	CS0	73 Alert (Level: Fatal, Description: Unknown CA)
4751 2022-07-11 16:55:26.024647	10.48.36.46	31578 10.48.36.215	6972 TCP	CS8	66 31578 → 6972 [RST, ACK] Seq=525 Ack=1883 Win=64128 Len=0 TSval=878570543 TSecr=343633337
4767 2022-07-11 16:55:26.083159	10.48.36.46	31580 10.48.36.215	6972 TCP	CSB	74 31588 → 6972 [SYN] Seq=0 Win+64240 Len+0 MSS=1460 SACK_PERM=1 TSval+878578601 TSecr+0 MS=128
Length: 663 Certificates Length: 660 V Certificates (660 bytes) Certificate Length: 657 V Certificate: 302303/30220214s0030201 V signedCertificate	0202107470ee62271e3d1346 (i	d-at-localityName=Diegem,id-at-st	ateOrProvinceName+Belgi	lum,id-at-comm	nName <mark>«curm=EC.steven.lab</mark> ,id-at-organizationalunitName=TAC,id-at-organizationName=Cisco,id-at-countryNa
<pre>version: v3 (2) serialNumber: 8x7470ee62271e1d13 > signature (ecds-with-SkA364) v issuer: indisequence (0) - rdisequence: 6 items (id-at-lo > validity > subject: rdisequence (0)</pre>	461b9946f0a3bf1d ocalityName-Diegen,id-at-stateC	rProvinceName=Belgium,id-at-comm	onName <mark>-cucm-EC.steven.l</mark>	ab <mark>,</mark> id-at-organ	izationalUnitName=TAC,id-at-organizationName=Cisco,id-at-countryName=8E)
 > subjectbublickeyInfo > extensions: 5 items > Extension (id-ce-kryusage) > Extension (id-ce-extryusage) > Extension (id-ce-subjectkeyIdd > Extension (id-ce-subjectkeyIdd > Extension (id-ce-subjectke)table > Extension (id-ce-subjectkaltua 	entifier) ints) me)				
Extension Id: 2.5.29.17 (id	i-ce-subjectAltName) ab A354)				
encrypted: 3064023012543bdSebe74570 TLSv1.2 Record Layer: Handshake Protocol: Ser	ab1171eb4s9ff03b060cds0ds rver Key Exchange				

Sur CUCM sous Cisco Unified OS Administration, vous pouvez consulter les certificats en place

sous Security > Certificate Management comme indiqué par exemple ici. Il affiche un certificat différent pour tomcat et tomcat-ECDSA où le tomcat est CA signé (et approuvé par l'Expressway-C) tandis que le certificat tomcat-ECDSA est auto-signé et non approuvé par l'Expressway-C ici.

alada Cisco	Unified Operating Sy	stem Adr	ninistra	ition			Navigation Caso Unified OS Administration
CISCO For Cisco	Unified Communications Solutions						admin Az
Show . Settings .	Security · Software Upgrades · Se	rvices + Help	•				
Certificate List							
Generate Self-signe	d 🐴 Upload Certificate/Certificate ch	ain 🔋 Down	load CTL 🧯	Generate CSR 🔋 Download CSF	1		
Status							
(i) 43 records found							
Certificate List	(1 - 43 of 43)						Rows per
Find Certificate List wh	ere Certificate v begins with	h ¥		Find Clear Filter 💠 📟			
Certificate *	Common Name	Type	Key Type	Distribution	Issued By	Expiration	Description
authz	AUTHZ_cuom.steven.lab	Self-signed	RSA	cucm.steven.lab	AUTHZ_cuom.steven.lab	07/21/2038	Self-signed certificate generated by system
CalManager	cucm.steven.lab	CA-signed	RSA	cucm.steven.lab	steven-DC-CA	07/13/2022	Certificate Signed by steven-DC-CA
CaliManager-ECDSA	cucm-EC.steven.lab	Self-signed	EC .	cucm.steven.lab	cucm-EC.steven.lab	02/18/2024	Self-signed certificate generated by system
CalManager-trust	steven-DC-CA	Self-signed	RSA	steven-DC-CA	steven-OC-CA	06/01/2025	Signed Certificate
CalManager-trust	NOMAT-AD-CA	Self-signed	RSA	NOMAT-AD-CA	NOMAT-AD-CA	04/23/2028	Signed Certificate
CalManager-trust	CAP-RTP-002	Self-signed	RSA	CAP-RTP-002	CAP-RTP-002	10/10/2023	This certificate was used to sign the MIC installed on Cisco endpoint. Presence of this certificate allows the end point to communicate securely with UCM using the MIC when associated with a secure profile.
CalManager-trust	CAPF-eb2c64d8	Self-signed	RSA	CAPF-eb2c64d8	CAPF-eb2c64d8	04/12/2020	
CaliManager-trust	ms-AD2-GA-1	Self-signed	RSA	ms-AD2-CA-1	ms-AD2-CA-1	09/11/2024	Vingto CA
Califianager-oust	CAP-RIP-001	Ser-signed	RSA	CAP-RIP-001	CAP-RIP-001	02/07/2023	This definition was used to sign the MIC installed on Cisco endpoint. Presence or this definitiate allows the end point to communicate securely with UCH using the MIC when associated with a secure prome.
Califianager-trust	NUMAT-CA-10	Ser-signed	RSA DEA	NOMAI-CA-10	NOMAT-CA-10	08/11/2027	
Califianager-trust	ACTO FUEL CA HE	Ser-signed	RSA	ACTO SUDI CA	Cisco Root CA 2048	11/12/2037	This certificate was used to sign the FLC installed on Case emports. Presence of this certificate allows the end point to communicate securely with UCH using the FLC when associated with a secure prome.
CalManager-trust	Units_BOOLSO	Calfutined	PSA	undout/TTUE/DIR/CA	untra CTUE OR CA	02/10/2024	This certificate less uses or sign the risk moving on Cisco englority, mesence or this certificate allows the end point, to commonly are year end of using the risk meen associated with a secure prome. Vivotta-Zi
Califianaper-trust	Cisco Root CA 2048	Self-signed	RSA	Cisco Boot CA 2048	Cisco Root CA 2048	05/14/2029	This certificate was used to sign the MIC installed on Cisco endopint. Resence of this certificate allows the end point to communicate securely with UCH using the MIC installed on Cisco endopint. Resence of this certificate allows the end point to communicate securely with UCH using the MIC installed on the AIC
CalManager-trust	Cisco Manufacturing CA	CA-signed	RSA	Cisco Manufacturios CA	Cisco Root CA 2048	05/14/2029	This certificate was used to sign the MIC installed on Cisco endooint. Presence of this certificate allows the end point to communicate securely with UCH using the MIC when associated with a secure profile.
CalManager-trust	Cisco Manufacturing CA SHA2	CA-signed	RSA	Cisco Manufacturing CA SHA2	Cisco Root CA M2	11/12/2037	This certificate was used to sign the HIC installed on Cisco endpoint. Presence of this certificate allows the end point to communicate securely with UCH using the HIC when associated with a secure profile.
CaliManager-trust	dccomics-WONDERWOMAN-CA	Self-signed	RSA	docomics-WONDERWOMAN-CA	dccomics-WONDERWOMAN-CA	09/19/2037	CA-byanturn
CaliManager-trust	CAPF-616421bc	Self-signed	RSA	CAPF-616421bc	CAPF-616421bc	07/12/2025	
CAPF	CAPF-616421bc	Self-signed	RSA	cucm.steven.lab	CAPF-616421bc	07/12/2025	Self-signed certificate generated by system
CAPF-trust	CAP-RTP-002	Self-signed	RSA	CAP-RTP-002	CAP-RTP-002	10/10/2023	This certificate was used to sign the MIC installed on Cisco endpoint. Presence of this certificate allows the end point to communicate securely with UCM using the MIC when associated with a secure profile.
CAPF-trust	CAPF-eb2c64d8	Self-signed	RSA	CAPF-eb2c64d8	CAPF-eb2c64d8	04/12/2020	
CAPF-trust	CAP-RTP-001	Self-signed	RSA	CAP-RTP-001	CAP-RTP-001	02/07/2023	This certificate was used to sign the MIC installed on Cisco endpoint. Presence of this certificate allows the end point to communicate securely with UCM using the MIC when associated with a secure profile.
CAPF-trust	Cisco Root CA M2	Self-signed	RSA	Cisco_Root_CA_M2	Cisco_Root_CA_M2	11/12/2037	This certificate was used to sign the MIC installed on Cisco endpoint. Presence of this certificate allows the end point to communicate securely with UCM using the MIC when associated with a secure profile.
CAPF-trust	ACT2_SUDI_CA	CA-signed	RSA	ACT2_SUDI_CA	Cisco_Root_CA_2048	05/14/2029	This certificate was used to sign the MIC installed on Cisco endpoint. Presence of this certificate allows the end point to communicate securely with UCM using the MIC when associated with a secure profile.
CAPF-trust	Cisco Root CA 2048	Self-signed	RSA	Cisco_Root_CA_2048	Cisco_Root_CA_2048	05/14/2029	This certificate was used to sign the MIC installed on Cisco endpoint. Presence of this certificate allows the end point to communicate securely with UCH using the MIC when associated with a secure profile.
CAPF-trust	Cisco Manufacturing CA	CA-signed	RSA	Cisco_Manufacturing_CA	Cisco_Root_CA_2048	05/14/2029	This certificate was used to sign the MIC installed on Cisco endpoint. Presence of this certificate allows the end point to communicate securely with UCH using the MIC when associated with a secure profile.
CAPF-trust	Cisco Manufacturing CA SHA2	CA-signed	RSA	Cisco_Manufacturing_CA_SHA2	Cisco_Root_CA_M2	11/12/2037	This certificate was used to sign the MIC installed on Cisco endpoint. Presence of this certificate allows the end point to communicate securely with UCH using the MIC when associated with a secure profile.
CAPF-trust	CAPF-616421bc	Self-signed	RSA	CAPF-6164210c	CAPF-616421bc	07/12/2025	
ipsec	cucm.steven.sap	Ser-signed	KSA	cucm.steven.lab	cucm.steven.iab	07/12/2025	see-signed certificate generated by system
ipsec-trust	cucm.steven.lab	Self-signed	RSA	cucm.steven.lab	cuom.steven.lab	07/12/2025	Trust Certificate
Trustecovery	Indecovery coonsoeventab	Ser-signed	RSA	cucm.steven.tab	TICKECOVERT_COOM.steven.iab	02/14/2039	sensepres certificate generates by system
Internal Activity	Course of states lab	CERONIN	RC RC	cuon steven lab	Steven OC/CA	07/10/2024	Certificate signed by server-CC-CA
New at-ECDSA	curre-EC sheves lab	Salf-sinned	EC.	ourm steven lab	current FC stream lab	07/25/2023	Salf-closed certificate cenerated by cystem
Inment-Inust	deven DC-CA	Salf-sized	REA	steven-DC-CA	deven DC-CA	06/01/2025	uner angenes sestement generationers of all annes. Third frankfillanda
tomcat-trust	NOMAT-AD-CA	Self-signed	RSA	NOMAT-AD-CA	NOMAT-AD-CA	04/23/2028	Stored Certificate
tomcat-trust	cucm-EC.steven.lab	Self-signed	EC	cucm.steven.lab	cucm-EC.steven.lab	07/25/2023	Trust Certificate
tomcat-trust	cucm.steven.lab	CA-signed	RSA	cucm.steven.lab	steven-DC-CA	07/10/2024	Trust Certificate
tomcat-trust	cups-EC.steven.lab	Self-signed	8C	cups.steven.lab	cups-EC.steven.lab	07/25/2023	Trust Certificate
tomcat-trust	NOMAT-CA-10	Self-signed	RSA	NOMAT-CA-10	NOMAT-CA-10	08/11/2027	Signed Certificate
tomcat-trust	yngtp-ACTIVE-DIR-CA	Self-signed	RSA	vngtp-ACTIVE-DIR-CA	vngtp-ACTIVE-DIR-CA	02/10/2024	Trust Certificate
tomcat-trust	dccomics-WONDERWOMAN-CA	Self-signed	RSA	docomics-WONDERWOMAN-CA	dccomics-WONDERWOMAN-CA	09/19/2037	CA Bruno
TVS	cucm.steven.lab	Self-signed	RSA	cucm.steven.lab	cucm.steven.lab	07/12/2025	Self-signed certificate generated by system

2. L'adresse de connexion (FQDN ou IP) ne figure pas dans le certificat

Outre le magasin de confiance, le serveur de trafic vérifie également l'adresse de connexion vers laquelle le client MRA effectue la requête. Par exemple, lorsque vous avez configuré sur CUCM sous System > Server votre CUCM avec l'adresse IP (10.48.36.215), alors l'Expressway-C annonce ceci comme tel au client et les requêtes suivantes du client (envoyées par proxy via l'Expressway-C) sont ciblées vers cette adresse.

Lorsque cette adresse de connexion particulière n'est pas contenue dans le certificat du serveur, la vérification TLS échoue également et une erreur 502 est générée qui entraîne un échec de connexion MRA, par exemple.

<#root>

```
2022-07-11T19:49:01.472+02:00 vcsc traffic_server[3916]: UTCTime="2022-07-11 17:49:01,472" Module="netwood with the server server
```

```
• • •
```

```
2022-07-11T19:49:01.491+02:00 vcsc traffic_server[3916]: [ET_NET 2]
```

WARNING: SNI (

```
10.48.36.215
) not in certificate
. Action=Terminate server=10.48.36.215(10.48.36.215)
2022-07-11T19:49:01.491+02:00 vcsc traffic_server[3916]: [ET_NET 2]
ERROR: SSL connection failed for
  '10.48.36.215': error:1416F086:
SSL routines:tls_process_server_certificate:certificate verify failed
```

Où c3RldmVuLmxhYi9odHRwcy8xMC40OC4zNi4yMTUvODQ0Mw se traduit (base64) par steven.lab/https/10.48.36.215/8443, ce qui montre qu'il doit établir la connexion vers 10.48.36.215 comme adresse de connexion plutôt que vers cucm.steven.lab. Comme indiqué dans les captures de paquets, le certificat tomcat CUCM ne contient pas l'adresse IP dans le SAN et l'erreur est donc générée.

Comment le valider facilement

Vous pouvez vérifier si vous êtes confronté à ce changement de comportement facilement avec les étapes suivantes :

1. Démarrez la journalisation de diagnostic sur le(s) serveur(s) Expressway-E et C (idéalement avec TCPDumps activé) à partir de Maintenance > Diagnostics > Diagnostic Logging (dans le cas d'un cluster, il suffit de le démarrer à partir du noeud principal)

2. Essayez une connexion MRA ou testez la fonctionnalité interrompue après la mise à niveau

3. Attendez qu'il échoue, puis arrêtez la journalisation de diagnostic sur les serveurs Expressway-E et C (dans le cas d'un cluster, assurez-vous de collecter les journaux de chaque noeud du cluster individuellement)

4. Téléchargez et analysez les journaux sur l'outil Collaboration Solution Analyzer

5. Si vous rencontrez le problème, il récupère les lignes d'avertissement et d'erreur les plus récentes relatives à cette modification pour chacun des serveurs affectés

Second	1	Collaboration Solutions Analyzer	Proview © UTC	r ? Ø
Addy Image: Section Control Image: Section Con	Tools >	Diagnostic overview	Issues found No issue Not applicable Missing information Potential problem	
2022-07-111313/01.16040200 vice treffic_sever(1935): [f1_9f1 1] (B000: SA connection failed for 'constant-als') enversion/MARCOSA readousity_press_sever_certificate verify failed	Log Anahyzer T Ushan Man Dagmatics I Anatysis	Q. Search Image: Call (53) Image: Call (54) Image: Call (54)	state book No son Not applicitie Marging Hommanian Posterial problem	Dontpuration Configuration Dontpuration Dontpuration IMERA

Signature de diagnostic CA

Â	Collaboration Solutions Analyze CISCO Log Analyzer	Preview © UTC	# ? Ø
Tools	Diagnostic overview	Issues found No Issue Not applicable Missing Information Potential problem	
Log Analyzer T Upbood Bres Depresenters Int Analyzer	Q. Search Result Category ∧ Q Cate (53) MRA (51) Configuration (39) Defects only ●	<pre>k tool is in too any displace is in the particule is integrition in the particule is inte</pre>	Contoursion Contoursion Contoursion BBDA discovering
			*

Signature de diagnostic SNI

Solution

La solution à long terme consiste à s'assurer que la vérification TLS fonctionne correctement. L'action à effectuer dépend du message d'avertissement affiché.

Lorsque vous observez l'AVERTISSEMENT : La vérification du certificat du serveur principal a

échoué pour (<server-FQDN-or-IP>). Action=Terminate Error=self signed certificate server=cucm.steven.lab(10.48.36.215) depth=x message, vous devez alors mettre à jour le magasin de confiance sur les serveurs Expressway-C en conséquence. Soit avec la chaîne AC qui a signé ce certificat (profondeur > 0) soit avec le certificat auto-signé (profondeur = 0) de Maintenance > Security > Trusted CA Certificate. Assurez-vous d'effectuer cette action sur chaque serveur du cluster. Une autre option consisterait à signer le certificat distant par une autorité de certification connue sur le magasin de confiance d'Expressway-C.

Remarque : Expressway ne permet pas de télécharger deux certificats différents (autosignés par exemple) dans le magasin de confiance d'Expressway qui ont le même nom commun (CN) que celui indiqué par l'ID de bogue Cisco <u>CSCwa12905</u>. Afin de corriger cela, passez aux certificats signés par l'autorité de certification ou mettez à niveau votre CUCM vers la version 14 où vous pouvez réutiliser le même certificat (auto-signé) pour Tomcat et CallManager.

Lorsque vous observez le message WARNING : SNI (<server-FQDN-or-IP>) not in certificate, alors il indique que ce FQDN ou IP de serveur n'est pas contenu dans le certificat qui a été présenté. Vous pouvez soit adapter le certificat pour inclure ces informations, soit modifier la configuration (comme dans CUCM sur System > Server pour qu'elle corresponde à un élément contenu dans le certificat du serveur), puis actualiser la configuration sur le serveur Expressway-C pour qu'elle soit prise en compte.

Informations connexes

La solution à court terme est d'appliquer la solution de contournement comme documenté pour revenir au comportement précédent avant X14.2.0. Vous pouvez effectuer cette opération par le biais de l'interface de ligne de commande sur les noeuds du serveur Expressway-C avec la commande récemment introduite :

xConfiguration EdgeConfigServer VerifyOriginServer: Off

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.