أستكشاف أخطاء التحقق من شهادة خادم حركة مرور Expressway Traffic Server لخدمات MRA وإصلاحها

المحتويات

قمدقملا

يصف اذه المستند تغيير السلوك على إصدارات Expressway من X14.2.0 والإصدارات الأعلى المرتبطة بمعرف تصحيح الأخطاء من Cisco CSCwc69661 أو معرف تصحيح الأخطاء من Cisco CSCwa25108.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- التكوين الأساسي ل Expressway
- التكوين الأساسي MRA

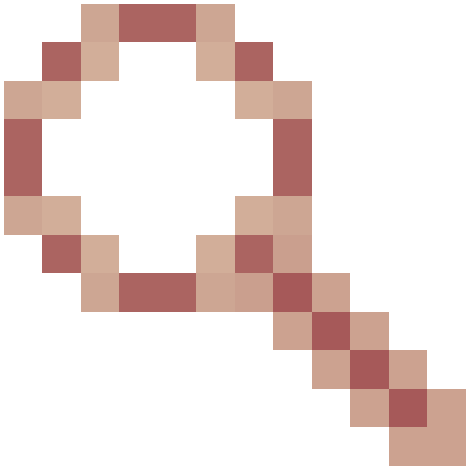
المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى Cisco Expressway على الإصدار X14.2

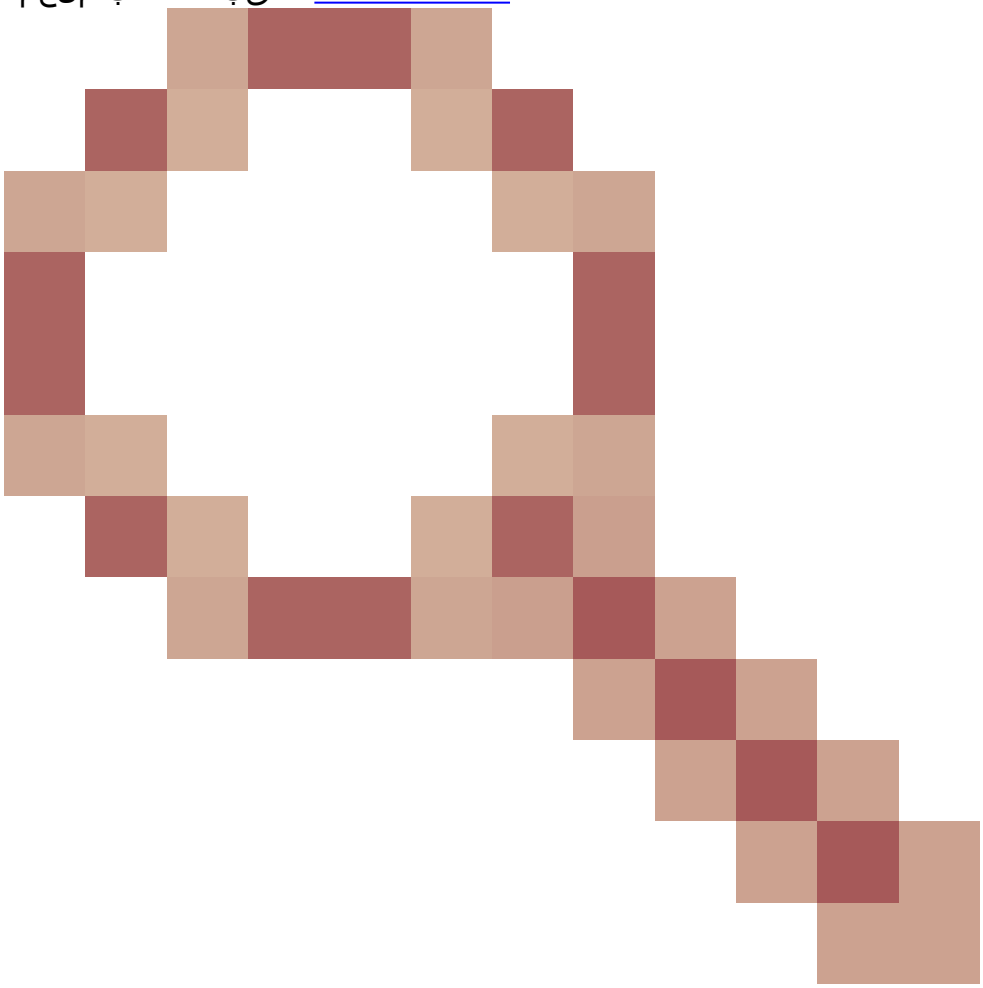
والإصدارات الأحدث.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهم للتأثير المحتمل لأي أمر.

معلومات أساسية



مع هذا التغيير في السلوك معلم ب cisco بق id CSCwc69661



وأ Cisco بق id CSCwa25108
، يقوم خادم حركة المرور على منصة Expressway بإجراء التحقق من شهادة Cisco Unified Communications Manager (CUCM) و Cisco Unified Instant Messaging & Presence (IM&P) وعقد خادم Unity لخدمات Mobile و Remote Access (MRA). قد يؤدي هذا التغيير إلى حدوث حالات فشل في تسجيل الدخول إلى MRA بعد إجراء ترقية على نظام Expressway الأساسي.

برتوكول نقل النص التشعبي الآمن (HTTPS) هو برتوكول اتصال آمن يستخدم أمان طبقة النقل (TLS) لتشفير الاتصال. وهو يقوم بإنشاء هذه القناة الآمنة باستخدام شهادة TLS التي يتم تبادلها في مصافحة TLS. هذا يخدم إثنان غرض: المصادقة (معرفة الطرف البعيد الذي تتصل به) والخصوصية (التشفير). تحمي المصادقة هجمات الدخيل وتمنع الخصوصية المهاجمين من التنصت والعبث بالاتصالات.

يتم إجراء التحقق من TLS (الشهادة) في عين المصادقة ويسمح لك بالتأكد من إتصالك بالطرف البعيد الأيمن. ويتألف التحقق من عنصرين فرديين:

1. سلسلة مرجع التصديق الموثوق به (CA)

2. الاسم البديل للموضوع (SAN) أو الاسم الشائع (CN)

سلسلة المرجع المصدق الموثوق به

لكي تثق Expressway-C في الشهادة التي يرسلها CUCM / IM&P / Unity، يلزم أن تكون قادرة على إنشاء إرتباط من تلك الشهادة إلى المرجع المصدق (الجذر) الأعلى (CA) الذي تثق فيه. يسمى هذا الرابط، وهو تسلسل هرمي من الشهادات التي تربط شهادة كيانات بشهادة مرجع مصدق جذر، سلسلة ثقة. للتمكن من التحقق من سلسلة الثقة هذه، تحتوي كل شهادة على حقلين : المصدر (أو "الصادر بواسطة") والموضوع (أو "الصادر من أجل").

تتضمن شهادات الخادم، مثل واحد من CUCM الذي يرسل إلى Expressway-C، في حقل "الموضوع" بشكل خاص اسم المجال المؤهل بالكامل (FQDN) في CN:

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

مثال على شهادة خادم ل CUCM CUCM.vngtp.lab. يحتوي على FQDN في سمة CN لحقل الموضوع مع سمات أخرى مثل الدولة (C)، الحالة (ST)، الموقع (L)، ... كما يمكنك أن ترى أن المصدر (إصدارها) من قبل مرجع مصدق يسمى vngtp-active-DIR-CA. شهادة الخادم تم تسليمها

يمكن أيضا أن تقوم المراجع المصدقة عالية المستوى (المرجع المصدق الجذر) بإصدار شهادة لتعريف نفسها. في شهادة المرجع المصدق الجذر هذه، نرى أن المصدر والموضوع لهما نفس القيمة :

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

إنها شهادة تم تسليمها من قبل مرجع مصدق جذري لتعريف نفسها.

في الحالات النموذجية، ال تصدر تراخيص CA الجذر شهادات الخادم مباشرة. بدلا من ذلك، فإنها تصدر شهادات ل CAs أخرى. ويطلق على هذه الأنواع الأخرى من النوى الحادة بعد ذلك اسم النوى المرجعية المتوسطة. يمكن أن تقوم CAs الوسيطة بدورها بإصدار شهادات أو شهادات

الخادم مباشرة ل CAs الوسيطة الأخرى. يمكن أن يكون لديها حالة حيث يتم إصدار شهادة خادم من CA 1 متوسط، الذي بدوره يحصل على شهادة من CA 2 متوسط وهكذا. حتى يحصل المرجع المصدق الوسيط أخيرا على شهادته مباشرة من المرجع المصدق الجذر :

```
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
```

الآن، من أجل أن تثق Expressway-C بشهادة الخادم التي يرسلها CUCM، يجب أن تكون قادرة على بناء سلسلة من الثقة من شهادة الخادم حتى شهادة مرجع مصدق رئيسي. ولتحقيق ذلك، نحتاج إلى تحميل شهادة المرجع المصدق الجذر وكذلك جميع شهادات المرجع المصدق الوسيطة (إذا كانت هناك أي شهادات، وهو ليس الحال إذا كان المرجع المصدق الجذر قد أصدر مباشرة شهادة خادم CUCM) في مخزن الثوثيق الخاص ب Expressway-C.

ملاحظة: على الرغم من أن حقلي المصدر والموضوع يسهل عليهما بناء سلسلة من الثقة بطريقة بشرية يمكن قراءتها، فإن CUCM لا تستخدم هذين الحقلين في الشهادة. وبدلا من ذلك، فإنه يستخدم حقلي "معرف مفتاح المرجع X509v3" و"معرف مفتاح الموضوع X509v3" لبناء سلسلة الثقة. تحتوي هذه المفاتيح على معرفات للشهادات تكون أكثر دقة ثم تستخدم حقول الموضوع/المصدر : يمكن أن تكون هناك شهادتان بنفس حقول الموضوع/المصدر لكن انتهت صلاحية واحدة منهما ولا تزال واحدة صالحة. سيكون لدى كل الطرفين معرف مختلف لمفاتيح الموضوع X509v3 بحيث يظل CUCM قادرا على تحديد سلسلة الثقة الصحيحة.

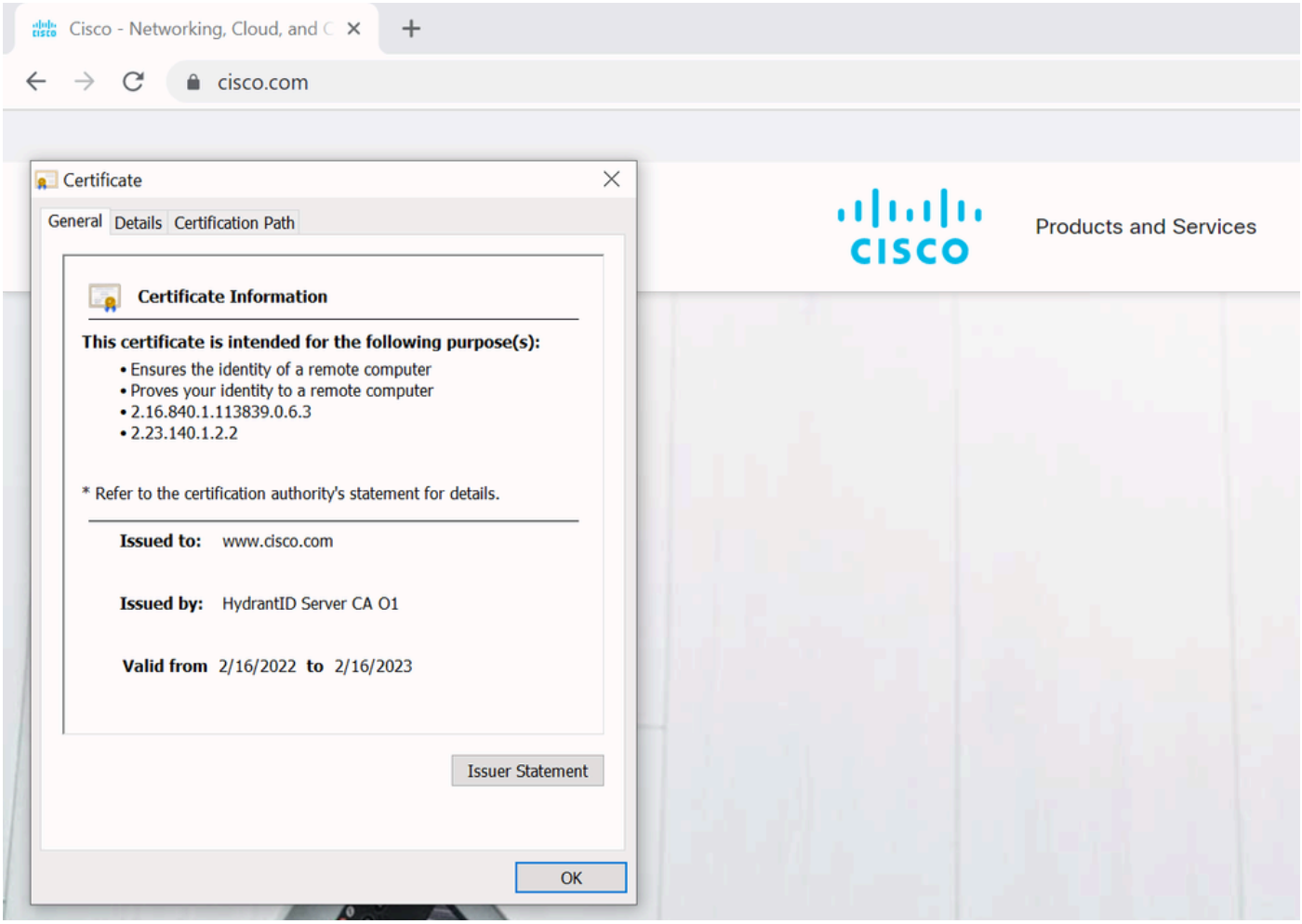
هذه ليست حالة Expressway رغم ذلك وقفا لمعرف تصحيح الأخطاء من Cisco CSCwa12905 ومن غير الممكن تحميل شهادتين مختلفتين (موقعة ذاتيا على سبيل المثال) في مخزن الثقة ل Expressway التي لها نفس الاسم المشترك (CN). الطريقة للتصحيح على هذا، هي أن تقوم ب CA بتوقيع الشهادات وأن تستخدم أسماء عامة مختلفة لها وأن ترى أنها تستخدم دائما نفس الشهادة (من المحتمل من خلال ميزة إعادة إستخدام شهادة في CUCM 14).

فحص SAN وأ CN

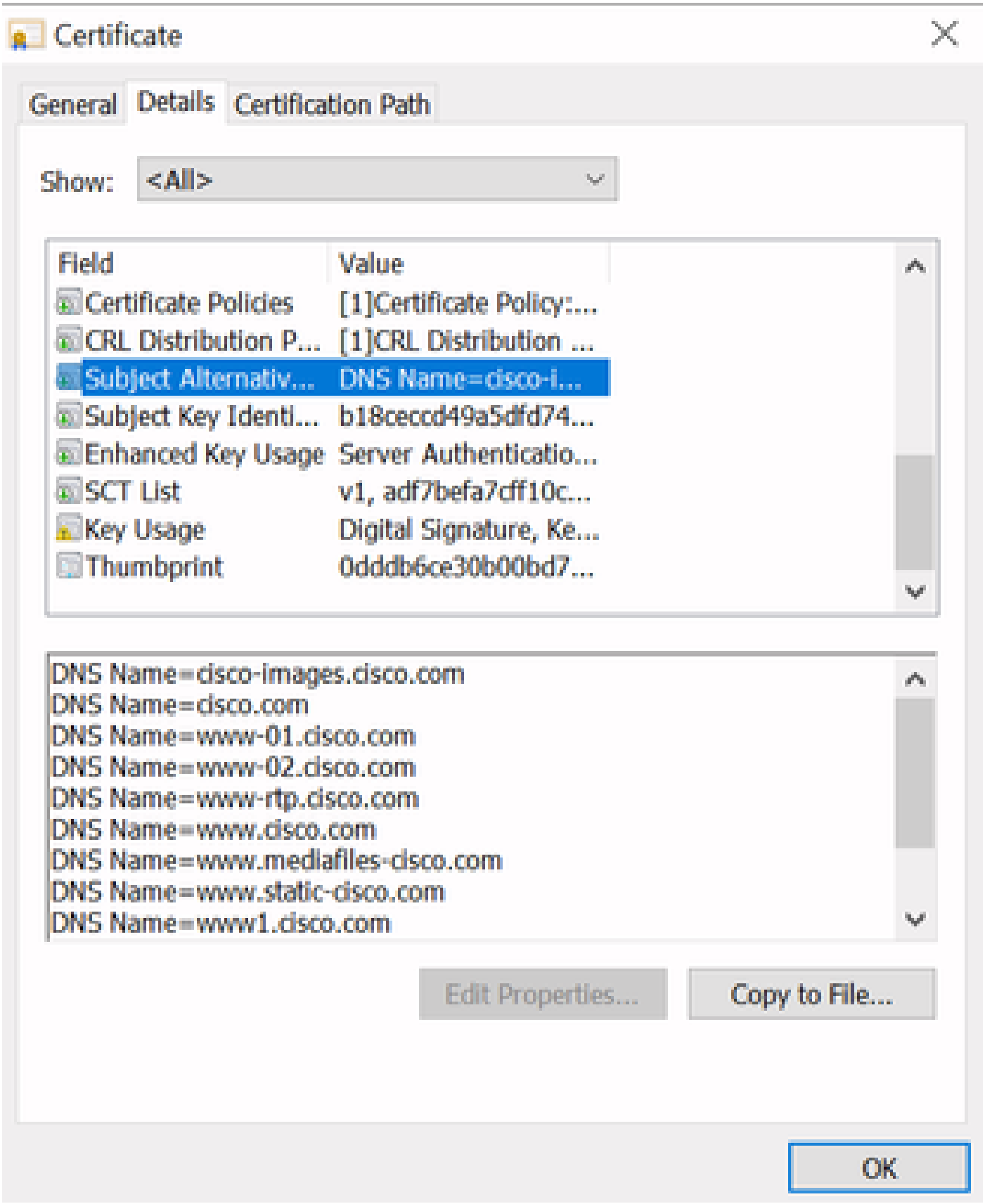
الخطوة 1 تحقق من مخزن التوثيق، ومع ذلك فإن أي شخص لديه شهادة تم توقيعها من قبل مرجع مصدق في مخزن التوثيق سيكون صالحا في ذلك الوقت. ومن الواضح أن هذا غير كاف.

لذلك، هناك تحقق إضافي يتحقق من أن الخادم الذي تتصل به هو بالفعل الخادم الصحيح. ويقوم بذلك استنادا إلى العنوان الذي تم تقديم الطلب من أجله.

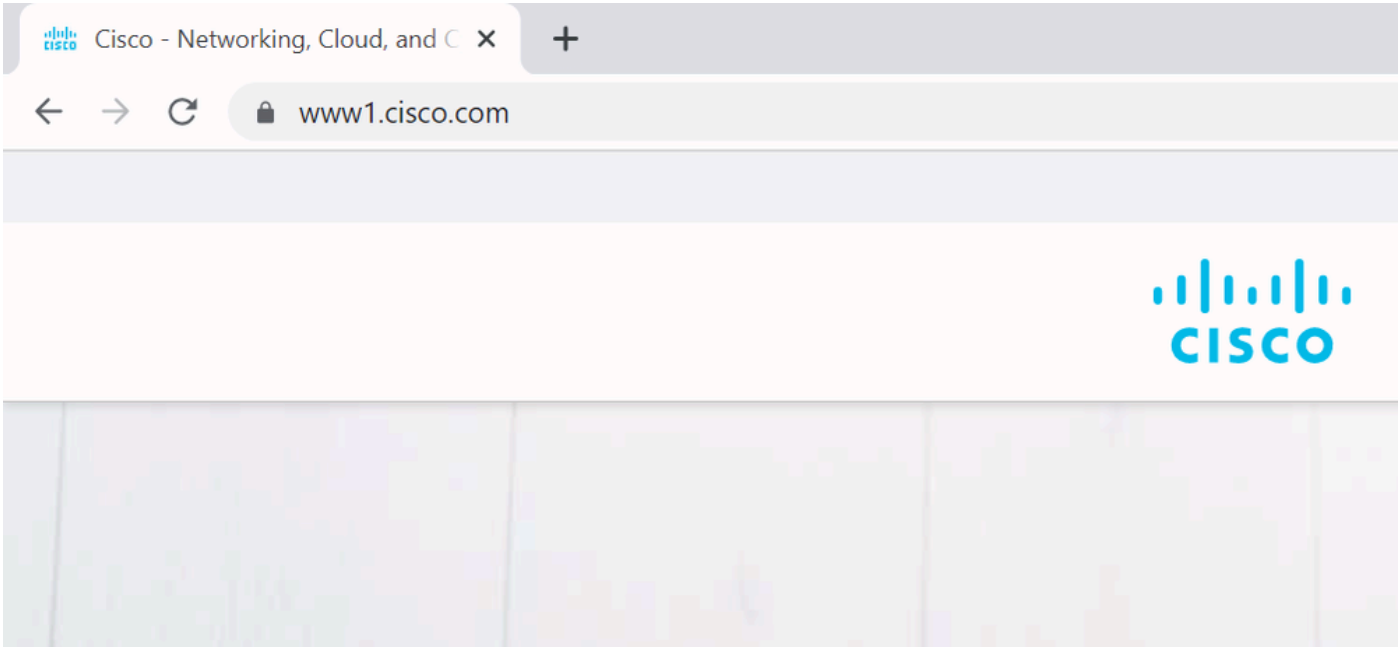
نفس النوع من العمليات تحدث في متصفحك، لذا دعونا ننظر في هذا من خلال مثال. إذا قمت بالاستعراض إلى https://www.cisco.com سترى أيقونة قفل بجوار عنوان URL الذي أدخلته مما يعني أنه اتصال موثوق به. يستند هذا إلى كل من سلسلة شقة CA (من القسم الأول) وكذلك إلى فحص SAN أو CN. إذا فتحنا الشهادة (عن طريق المستعرض بنقرة على أيقونة القفل)، سترى أن الاسم الشائع (يظهر في الحقل 'تم إصداره إلى:') مضبوط على www.cisco.com وهو يتوافق تماما مع العنوان الذي أدرنا الاتصال به. بهذه الطريقة يمكن التأكد من إتصالنا بالخادم الصحيح (لأننا نثق في المرجع المصدق الذي قام بتوقيع الشهادة والذي يقوم بإجراء التحقق قبل تسليم الشهادة).



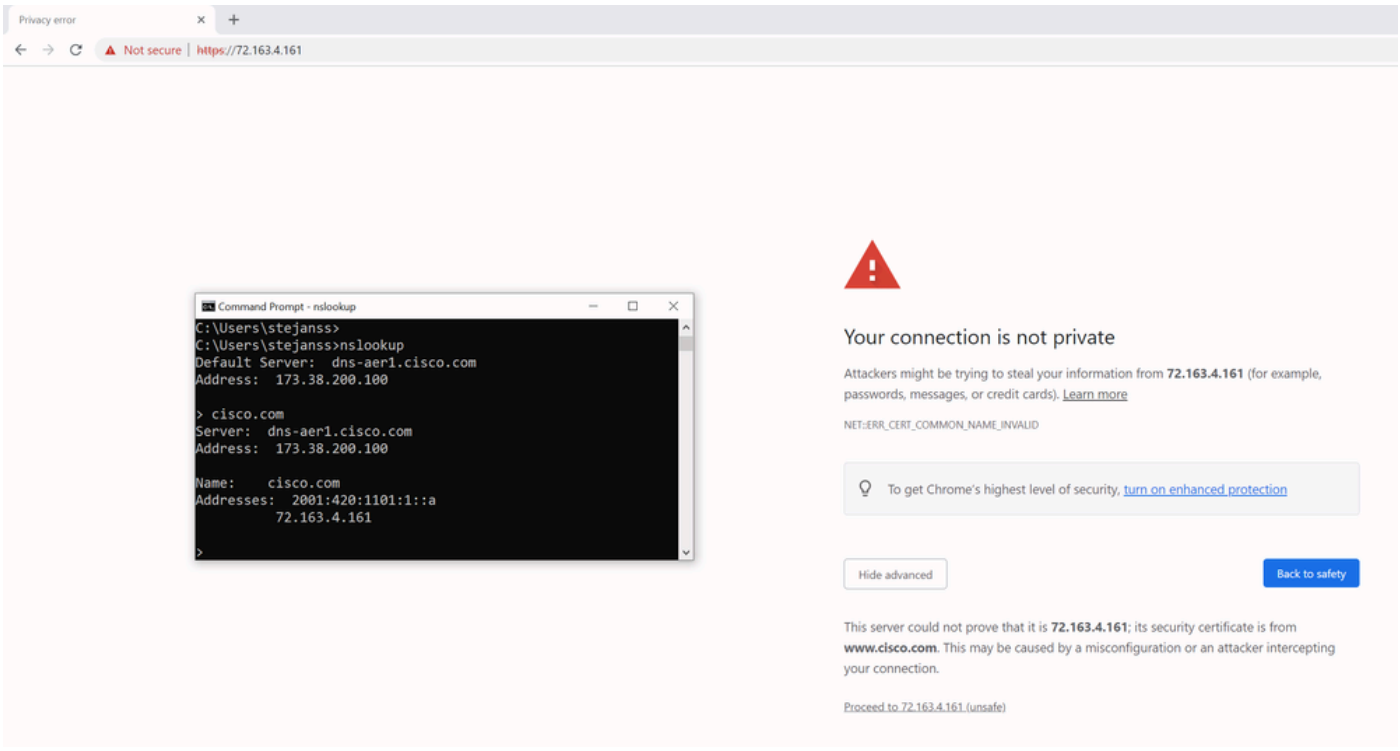
عند الاطلاع على تفاصيل الشهادة وعلى إدخالات شبكة منطقة التخزين (SAN) بشكل خاص، نلاحظ أن نفس الشيء يتكرر بالإضافة إلى بعض إدخالات شبكة منطقة التخزين (FQDN) الأخرى:



وهذا يعني أنه عندما نطلب الاتصال ب https://www1.cisco.com على سبيل المثال، سيظهر كاتصال آمن أيضا لأنه موجود في إدخالات شبكة التخزين (SAN).



ومع ذلك، عندما تقوم بالاستعراض إلى https://www.cisco.com ولكن مباشرة إلى عنوان IP (https://72.163.4.161)، فإنه يظهر اتصالاً آمناً لأنه يثق في CA الذي قام بتوقيعه ولكن الشهادة المقدمة لنا، والتي تحتوي على العنوان (72.163.4.161) الذي أستخدمناه للاتصال بالخادم.



في المستعرض، يمكنك تجاوز هذا الإعداد، على أي حال، يمكنك تمكينه على إتصالات TLS بحيث لا يتم السماح بالالتفاف. لذلك، من المهم أن تحتوي الشهادات الخاصة بك على أسماء CN أو SAN الصحيحة التي يخطط الطرف البعيد لاستخدامها للاتصال بها.

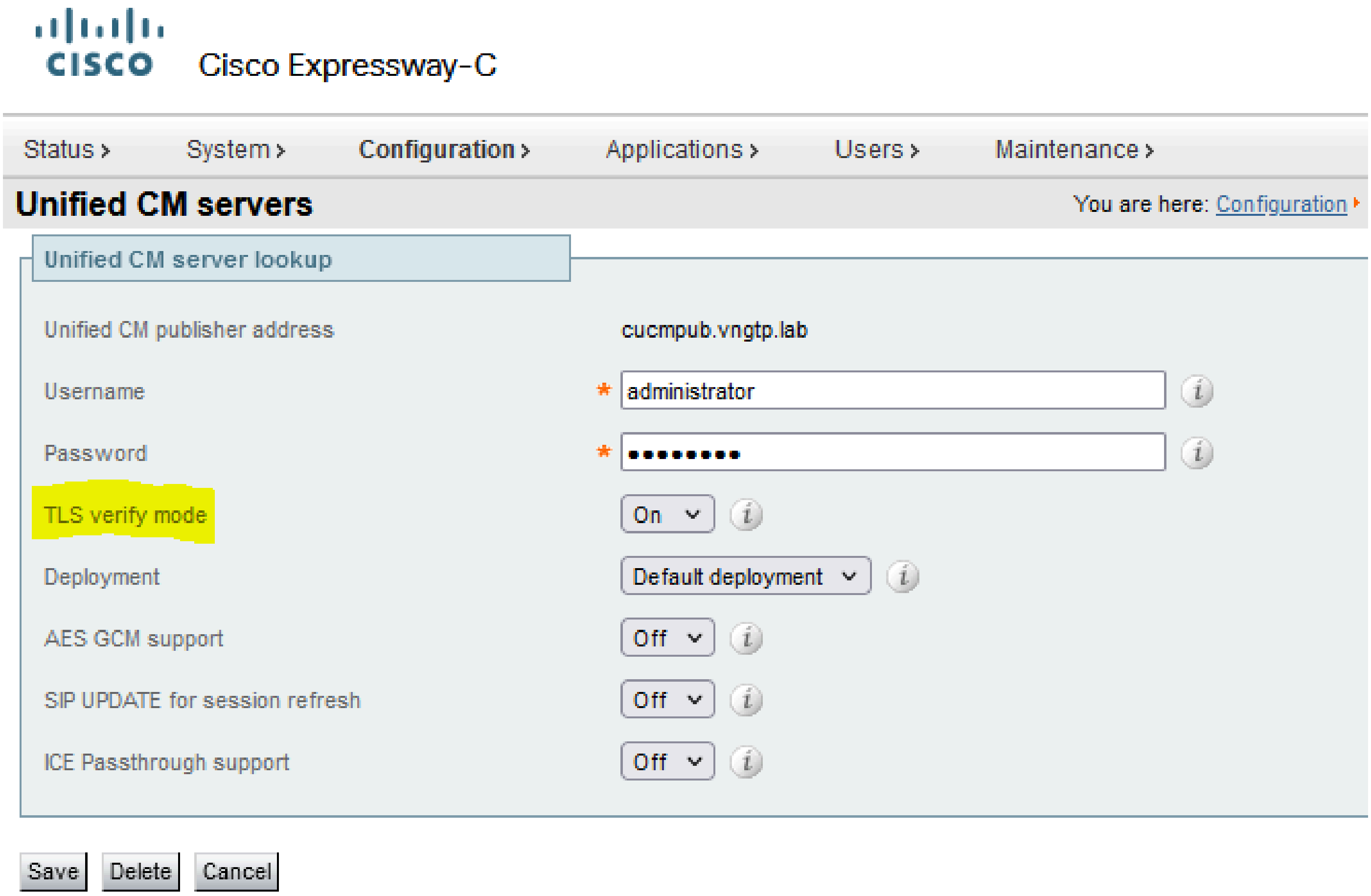
تغيير السلوك

تعتمد خدمات MRA بشكل كبير على العديد من إتصالات HTTPS عبر الطرق السريعة تجاه

خوادم CUCM / IM&P / Unity للمصادقة بشكل صحيح وجمع المعلومات الصحيحة الخاصة بالعميل الذي يقوم بتسجيل الدخول. يحدث هذا الاتصال عادة عبر المنافذ 8443 و 6972.

الإصدارات الأقل من X14.2.0

في الإصدارات الأقل من X14.2.0، لم يتحقق خادم حركة المرور الموجود على Expressway-C الذي يعالج إتصالات HTTPS الآمنة هذه من الشهادة التي تم تقديمها بواسطة الطرف البعيد. قد يؤدي هذا إلى هجمات الدخيل. في تكوين MRA، هناك خيار للتحقق من شهادة TLS من خلال تكوين "وضع التحقق من TLS" إلى "تشغيل" عندما تقوم بإضافة إما CUCM / IM&P / Unity servers تحت التكوين > الاتصالات الموحدة > خوادم CM الموحدة / IM وعقود خدمة التواجد / خوادم اتصال الوحدة. يتم عرض خيار التكوين ومربع المعلومات ذات الصلة كمثال، مما يشير إلى أنه يتحقق من FQDN أو IP في شبكة التخزين (SAN) بالإضافة إلى صلاحية الشهادة وما إذا كانت موقعة من قبل مرجع مصدق ثقة.



يتم التحقق من شهادة TLS هذا فقط من طقل خلال اكتشاف خوادم CUCM / IM&P / Unity وليس في الوقت الذي يتم فيه الاستعلام عن مختلف الخوادم أثناء MRA. المأخذ الأول لهذا التكوين، هو أنه يتحقق منه فقط لعنوان الناشر الذي تقوم بإضافته. لا يتحقق من صحة إعداد الشهادة على عقد المشترك بشكل صحيح حيث أنها تسترجع معلومات عقدة المشترك (FQDN أو IP) من قاعدة بيانات عقدة الناشر. والعيب الثاني من هذا التكوين أيضا، هو أن ما يتم الإعلان عنه لعملاء MRA حيث يمكن أن تختلف معلومات الاتصال عن عنوان الناشر الذي تم وضعه في تكوين Expressway-C. على سبيل المثال، في CUCM، تحت نظام > خادم يمكنك الإعلان عن الخادم باستخدام عنوان IP (10.48.36.215 على سبيل المثال) ويتم إستخدام هذا بعد ذلك من قبل عملاء MRA (عبر اتصال Expressway الوكيل) ومع ذلك يمكنك

إضافة CUCM على Expressway-C مادختساب FQDN نم cucm.steven.lab. ةداهش نأ ضارتفاب tomcat نم CUCM يوتحت على cucm.steven.lab كإدخال إلى SAN سيلو كعونا IP، كلذ دعب جنجح الاكتشاف مع 'TLS Verify Mode' على 'On' ولكن الاتصالات الفعلية من عملاء MRA يمكن أن تستهدف FQDN فلتخم أو IP وبالتالي تفشل التحقق من TLS.

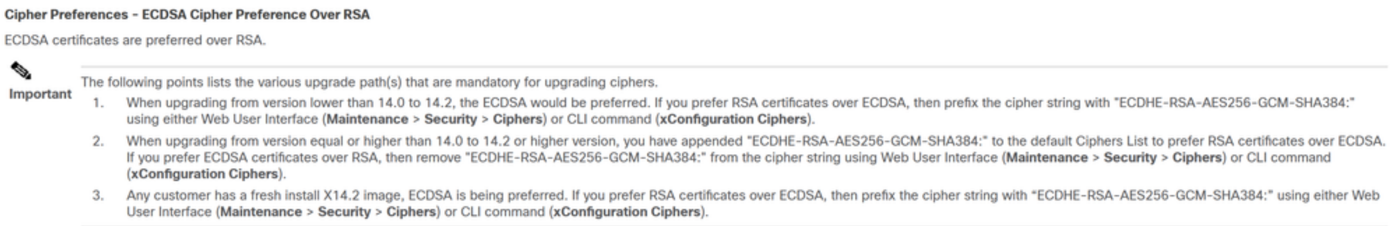
الإصدارات من X14.2.0 والإصدارات الأحدث

من إصدار X14.2.0 فصاعدا، يعمل مادخ Expressway على التحقق من ةداهش TLS لكل بلط HTTPS يتم إجراؤه من اللخ مادخ ةكرح رورم البيانات. وهذا يعني أنه اذ نفذت امدنع اضيأ يتم تعيين "وضع التحقق من TLS" على "إيقاف" أثناء اكتشاف دقع CUCM / IM&P / Unity. امدنع نجحت عملية التحقق من الصحة، لا يتم تأكيد اتصال TLS ويفشل الطلب الذي يمكن أن لوخدلا ليجست لشف وأ لشفلا زواجت وأ راركتلا لكاشملا لثم فئاظولا دقف ىلإ يدؤي الكامل على سبيل المثال. أيضا مع نييعت "وضع التحقق من TLS" على "ليغشتلا"، لا يضمن أن تعمل جميع الاتصالات بشكل صحيح كما هو منصوص عليه في المثال الحالي.

درت الشهادات الدقيقة التي يفحصها الطريق السريع من دقع CUCM / IM&P / Unity كما هو مسق يف حضوم [دليل MRA](#).

بالإضافة إلى الإعداد الافتراضي على التحقق من TLS، كانه أيضا تغيير تم تقديمه في X14.2 والذي يمكن أن يعلن عن ترتيب تفضيل فلتخم لقائمة التشفير، والذي يعتمد على مسار الترقية الخاص بك. قد يتسبب ذلك في حدوث إتصالات TLS غير متوقعة دعب ترقية البرنامج لأنه قد يحدث أن له قبل الترقية المطلوبة شهادة Cisco Tomcat أو Cisco CallManager من CUCM (أو أي منتج آخر يحتوي على شهادة منفصلة لخوارزمية ECDSA) ولكن بعد الترقية فإنه يطلب متغير ECDSA (وهو متغير التشفير الأكثر أمانا في الواقع من RSA). تكون توقيع شهادات Cisco Tomcat-ECDSA أو Cisco CallManager-ECDSA من قبل CA فلتخم أو شهادات ما تزال موقعة ذاتيا (الافتراضي).

لا يكون تغيير أمر تفضيل التشفير هذا ذا صلة بك دائما لأنه يعتمد على مسار الترقية كما هو موضح من [ملاحظات إصدار](#) Expressway X14.2.1. باختصار، يمكنك أن ترى من الصيانة > الأمان > المشفرات لكل واحد من المشفرات ما إذا كان يؤدي إلى إعداد "ECDHE-RSA-AES256-GCM-SHA384:" أم لا. وإذا لم يكن كذلك، فإنه يفضل تشفير ECDSA الأحدث على تشفير RSA. إذا كان كذلك، فسيكون لديك سلوك سابق مع RSA الذي لديه تفضيل أعلى عندئذ.


Cipher Preferences - ECDSA Cipher Preference Over RSA

ECDSA certificates are preferred over RSA.

Important

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

1. 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**).
2. 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 (**xConfiguration Ciphers**).
3. 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**).

هناك طريقتان لفشل التحقق من TLS في هذا السيناريو، ويتم تغطيتهما بالتفصيل الحالي:

1. المرجع المصدق الذي قام بتوقيع الشهادة البعيدة غير موثوق به

أ. شهادة موقعة ذاتيا

ب. الشهادة الموقعة من قبل مرجع مصدق غير معروف

2. ال يوتحي ناونع لاصتالا (FQDN وأ IP) يف ةداهشلا

فاشكتسأ اهحالصإو تاهويرانيسلا

رهظت تاهويرانيسلا ةيلاتلا ويرانيس اهباشم يف ةئيب ةيلمعم ثيح لشف ليجست لوخدلا ىلإ MRA دعب ةيقرت Expressway نم X14.0.7 ىلإ X14.2. ثيح كرتشت هجوأ هبشلا يف تالجسلا، ىلع مغرلا نم فالتخأ ةقدلا. متي عيمجت تالجسلا طقف ةطساوب ليجستلا يصيخشتلا (نم ةنايصلا > تاصيخشتلا > ليجستلا يصيخشتلا) يذلا مت ءدب هليغشت لبق ليجست لوخدلا ىلإ MRA متو هفاقيإ دعب لشف ليجست لوخدلا ىلإ MRA. مل متي نيكمت يأ ليجست حيحصت ءاطخأ يفاضإ هل.

1. عجرملا قدصملا يذلا ماق عيقوتب ةداهشلا ةديعبلا ريغ قوثوم هب

نكمي عيقوت ةداهشلا نع دعب نم لبق عجرم قدصم ريغ نمضم يف نزخملا قوثوملا هب ال (اضيأ قدصم عجرم اهرهوج يف) ايتاذ ةعقوم ةداهش نوكت نأ نكمي وأ Expressway-C مداخلل متت اهتفاضإ يف نزخم قيثوتلا صاخلا مداخب Expressway-C.

يف لاثملا انه، كنكمي ةظحالم نأ تابلطلا يتلا لقتنت ىلإ CUCM (10.48.36.215 - cucm.steven.lab) متي لماعتلا اهعم لكشب حيحص ىلع ذفنملا 8443 (ةباجتسإ 200 OK) اهنكلو ببستت يف ثودح أطخ (ةباجتسإ 502) ىلع ذفنملا 6972 لاصتال TFTP.

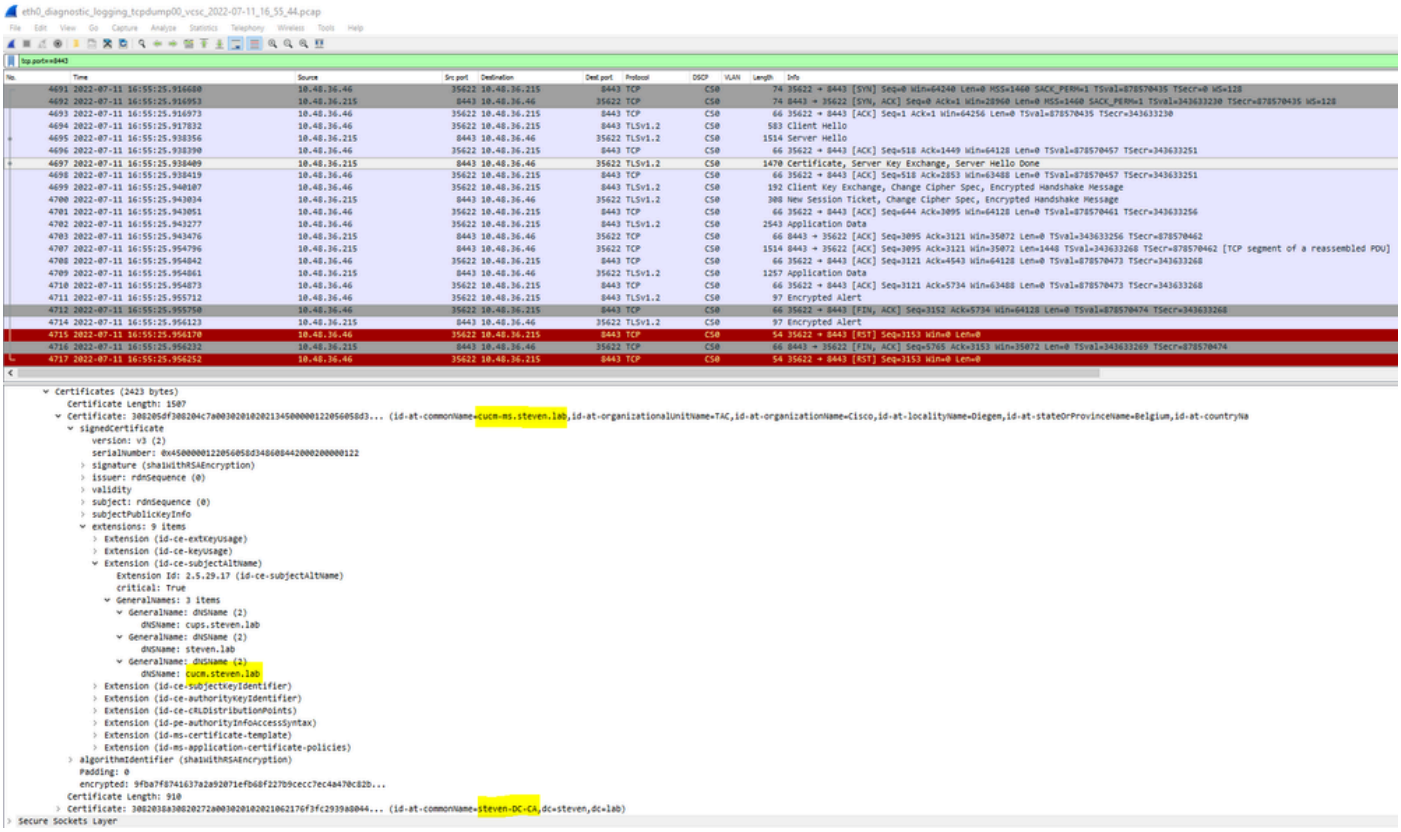
<#root>

```
===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="net

2022-07-11T18:55:25.917+02:00 vcsc traffic_server[18242]:  Event="Request Allowed" Detail="Access allow
2022-07-11T18:55:25.917+02:00 vcsc traffic_server[18242]: UTCTime="2022-07-11 16:55:25,916" Module="net
2022-07-11T18:55:25.955+02:00 vcsc traffic_server[18242]: UTCTime="2022-07-11 16:55:25,955" Module="net
2022-07-11T18:55:25.956+02:00 vcsc traffic_server[18242]: UTCTime="2022-07-11 16:55:25,955" Module="net

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="net

2022-07-11T18:55:26.006+02:00 vcsc traffic_server[18242]: UTCTime="2022-07-11 16:55:26,006" Module="net
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]
```

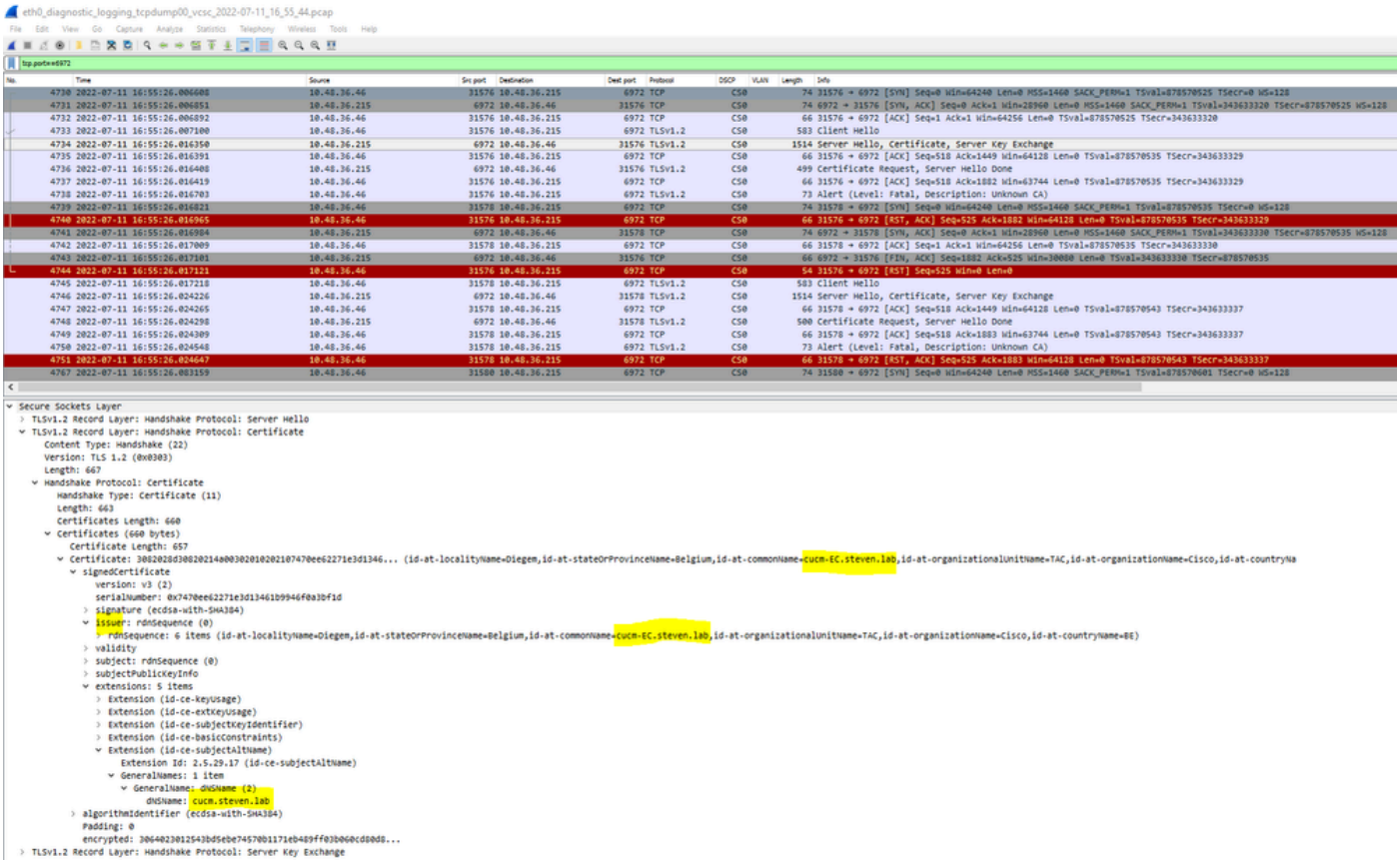
```
ERROR: SSL connection failed for
 'cucm.steven.lab': error:1416F086:
SSL routines:tls_process_server_certificate:certificate verify failed

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
"
```

يشير خطأ "التحقق من صحة الشهادة" إلى حقيقة عدم تمكن Expressway-C من التحقق من صحة مصافحة TLS. وسبب ذلك ظهر في سطر التخزين لأنه يشير إلى شهادة موقعة ذاتيا. إذا كان العمق موضح على هيئة 0، فإنها شهادة موقعة ذاتيا. عندما يكون العمق أعلى من 0، فهذا يعني أن له سلسلة شهادات وبالتالي يتم توقيعه من قبل مرجع مصدق غير معروف (من منظور Expressway-C).

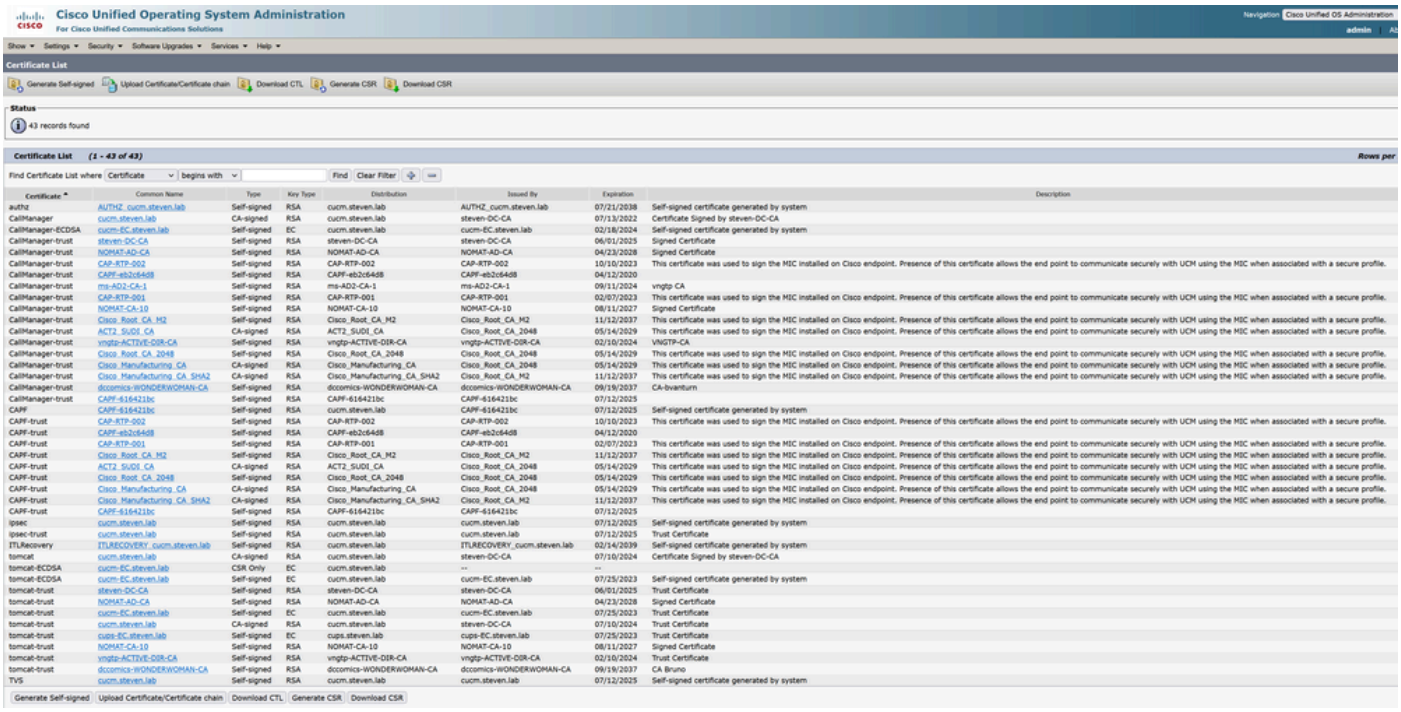
عندما ننظر في ملف PCAP الذي تم تجميعه في الطوابع الزمنية المذكورة من سجلات النص، يمكنك أن ترى أن CUCM يقدم الشهادة مع CN على هيئة CUCM-ms.steven.lab (و cucm.steven.lab على هيئة SAN) موقعة من قبل Steven-DC-CA إلى Expressway-C على المنفذ 8443.



ولكن عندما نفحص الشهادة المقدمة على المنفذ 6972، يمكنك أن ترى أنها شهادة موقعة ذاتيا (المصدر نفسه) مع إعداد CN على هيئة CUCM-EC.Steven.lab. يعطي امتداد -EC إشارة إلى أن هذه هي شهادة ECDSA التي تم إعدادها على CUCM.



في CUCM تحت إدارة Cisco Unified OS، يمكنك النظر إلى الشهادات الموضحة تحت التأمين > إدارة الشهادات كما هو موضح هنا على سبيل المثال. تظهر شهادة مختلفة لـ Tomcat و Tomcat-ECDSA حيث يكون Tomcat CA موقع (وموثوق به من قبل Expressway-C) بينما شهادة Tomcat-ECDSA موقعة ذاتيا وغير موثوق بها من قبل Expressway-C هنا.



2. عنوان الاتصال (FQDN أو IP) غير موجود في الشهادة

بالإضافة إلى مخزن الثقة، يتحقق خادم حركة مرور البيانات أيضا من عنوان الاتصال الذي

ليمع موقي MRA بتبقدت ميدقتب بلطلا نم أجله. على سبيل المثال، عند إعداد CUCM نمض النظام > مداخ CUCM الخاص كب مادختساب ناونع IP (10.48.36.215)، نلعي Expressway-C نع كلذ اذهب (لالخ نم ليكول Expressway-C) ليمعلا نم ةقحاللا تابلطلا فادهتسإ متيو ليمعلل العنوان.

متيو كلذك TLS نم ققحتلا لشفي ،مداخلا ةداهش نمض اذه لاصتالا ناونع نوكي ال امدنع إلى 502 أطخ ءاقلإ يف لشف هنع جتني ليجست الدخول إلى MRA على سبيل المثال.

<#root>

```
2022-07-11T19:49:01.472+02:00 vcsc traffic_server[3916]: UTCTime="2022-07-11 17:49:01,472" Module="netw
HTTPMSG:
|GET http://vcs_control.steven.lab:8443/c3RldmVuLmxhYi9odHRwcy8xMC40OC4zNi4yMTUvODQ0Mw/cucm-uds/user/em
...

2022-07-11T19:49:01.478+02:00 vcsc traffic_server[3916]: UTCTime="2022-07-11 17:49:01,478" Module="netw
2022-07-11T19:49:01.478+02:00 vcsc traffic_server[3916]: UTCTime="2022-07-11 17:49:01,478" Module="netw
HTTPMSG:
|GET /cucm-uds/user/emusk/devices?max=100 HTTP/1.1
...

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
```

حيث تمت ةمجرت c3RldmVuLmxhYi9odHRwcy8xMC40OC4zNi4yMTUvODQ0Mw (base64) إلى steven.lab/https/10.48.36.215/8443، والذي يظهر أنه يجب أن يقوم بالاتصال نحو 10.48.36.215 ناونعك لاصتا لدبلا نم cucm.steven.lab. امك وه حضوم يف مزح الالتقاط، ال تحتوي ةداهش CUCM TOMCAT على ناونع IP يف ةكبش التخزين (SAN) نمو مث متي إلقاء الخطأ.

كيفية التحقق نم صحتها بسهولة

يمكنك التحقق امم إذا تنك ديرت رييغت اذه السلوك بسهولة مادختساب الخطوات التالية:

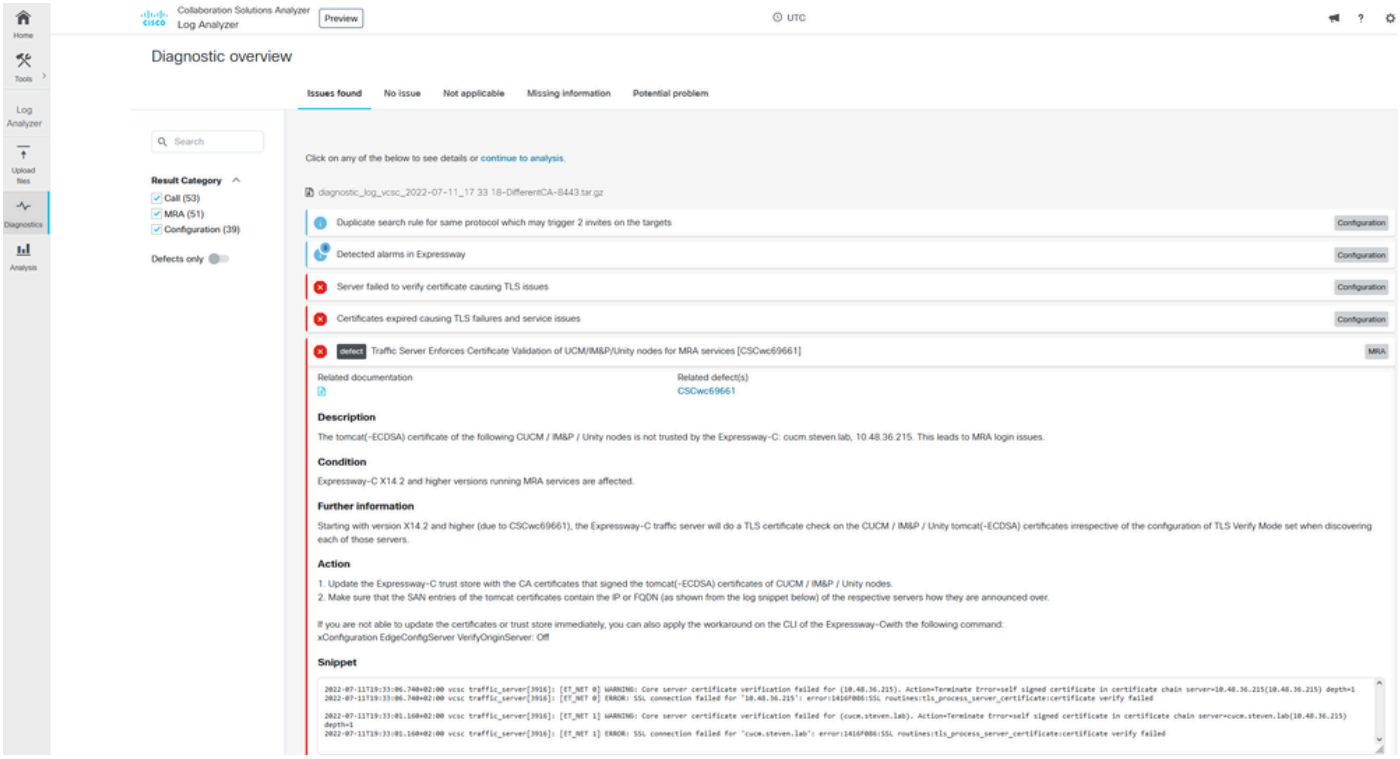
1. عدب التسجيل التشخيصي على مداخ (مداوخ) Expressway-E و C (نيكمت عم ايجذومن TCPDumps) نم الصيانة > التشخيصات > التسجيل التشخيصي (في ةلاح ماظن ةعومجم، يكون ايفاك لتشغيله نم العقدة الأساسية)

2. لواح ليجست الدخول إلى MRA أو رابتخإ الوظيفة المعطلة بعد الترقية

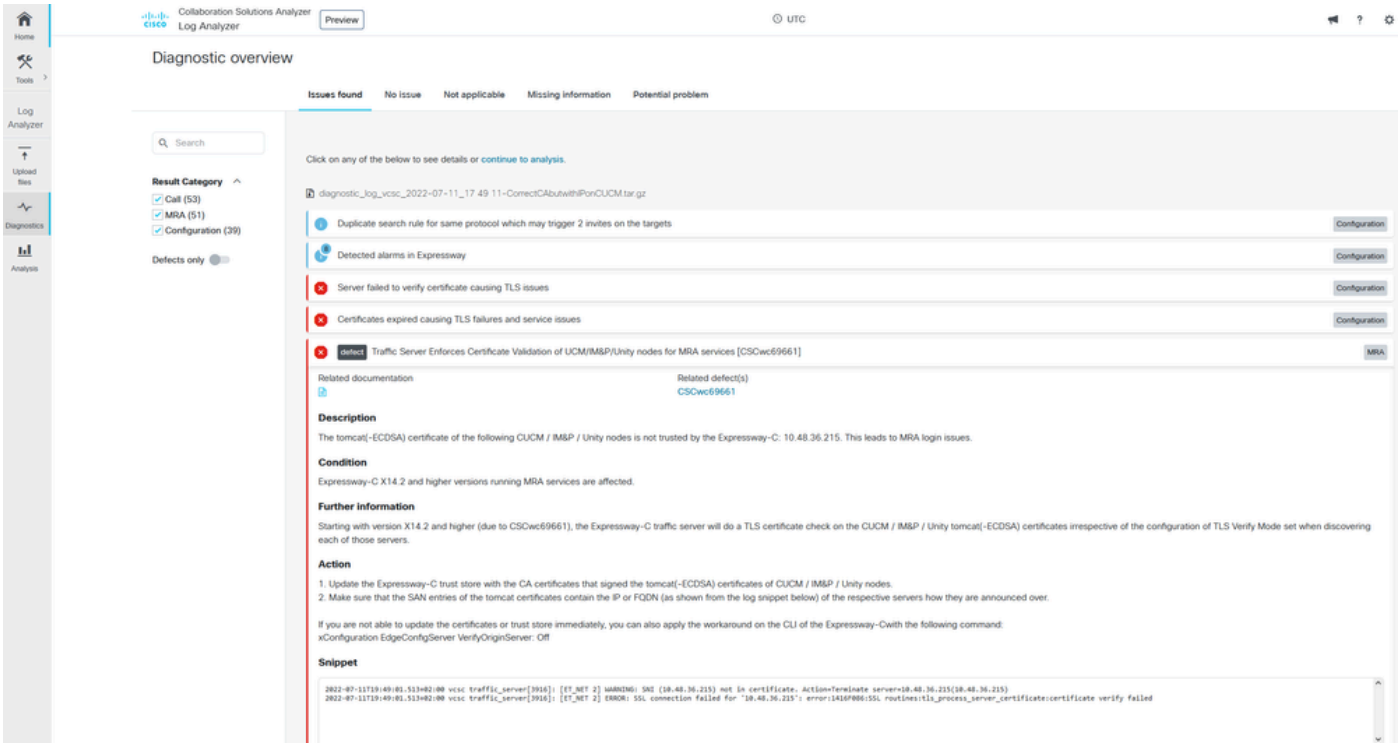
3. انتظر حتى يفشل التسجيل التشخيصي على خادم (خوادم) Expressway-E و C ثم قم بإيقاف التسجيل التشخيصي (في حالة مجموعة، تأكد من جمع السجلات من كل عقدة من المجموعة بشكل فردي)

4. تحميل السجلات الموجودة على [أداة محلل حلول التعاون](#) وتحليلها

5. إذا واجهت هذه المشكلة، فإنها تلتقط أحدث خطوط التحذير والخطأ المتعلقة بهذا التغيير لكل خادم من الخوادم المتأثرة



توقيع تشخيص CA



الحل

الحل طويل المدى هو التأكد من أن التحقق من TLS يعمل بشكل جيد. يعتمد الإجراء الذي سيتم تنفيذه على رسالة التحذير المعروضة.

عندما تلاحظون التحذير: فشل التحقق من شهادة الخادم الأساسي ل (<server-FQDN-or-IP>). الإجراء=End Error=Self Signed Certificate Server=cucm.steven.lab(10.48.36.215) depth=x message، ثم تحتاج إلى تحديث مخزن الثقة على خوادم Expressway-C وفقا لذلك. إما باستخدام سلسلة المرجع المصدق التي وقعت على هذه الشهادة (العمق > 0) أو باستخدام شهادة ذاتية التوقيع (العمق = 0) من الصيانة > التأمين > شهادة المرجع المصدق الثقة. تأكد من تنفيذ هذا الإجراء على كل خادم في نظام المجموعة. خيار آخر هو توقيع الشهادة عن بعد بواسطة مرجع مصدق معروف في مخزن ثقة Expressway-C.

ملاحظة: ال يسمح Expressway بتحميل شهادتين مختلفتين (ذاتيا موقعة على سبيل المثال) إلى مخزن Expressway للثقة لهما نفس الاسم المشترك (CN) وفقا لمعرف تصحيح الأخطاء من Cisco CSCwa12905. لتصحيح ذلك، انتقل إلى الشهادات الموقعة من CA أو قم بترقية CUCM إلى الإصدار 14 حيث يمكنك إعادة استخدام نفس الشهادة (ذاتيا موقعة) ل Tomcat و CallManager.

عندما تلاحظون التحذير: SNI (<server-FQDN-or-IP>) غير موجود في رسالة الشهادة، ثم يشير إلى أن FQDN أو IP هذا الخادم غير موجود في الشهادة التي تم تقديمها. يمكنك إما تكييف الشهادة لتضمين هذه المعلومات أو يمكنك تعديل التكوين (مثل CUCM على النظام > الخادم إلى شيء موجود في شهادة الخادم) ثم تحديث التكوين على خادم Expressway-C حتى يتم وضعه في الاعتبار.

معلومات ذات صلة

الحل قصير المدى هو تطبيق الحل البديل كما هو موثق للرجوع إلى السلوك السابق قبل X14.2.0. يمكنك تنفيذ ذلك من خلال CLI (واجهة سطر الأوامر) على عقدة خادم Expressway-C باستخدام الأمر الذي تم تقديمه حديثا:

```
xConfiguration EdgeConfigServer VerifyOriginServer: Off
```

تقنية المعلومات

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).