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

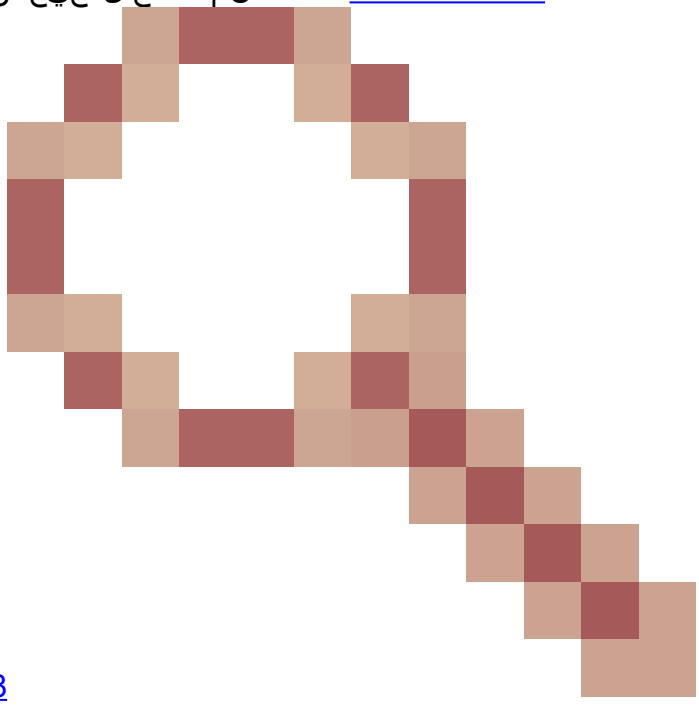
تستند المعلومات الواردة في هذا المستند إلى Cisco Expressway على الإصدار X14.2

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 فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

مع هذا التغيير في السلوك المميز بمعرف تصحيح الأخطاء من Cisco CSCwc69661



أو معرف تصحيح الأخطاء من Cisco CSCwa25108
، يقوم خادم حركة المرور على منصة Expressway بإجراء التحقق من شهادة مدير الاتصالات الموحدة (CUCM) من Cisco والمراسلة الفورية الموحدة والتواجد (IM&P) من Cisco وعقد خادم Unity لخدمات الوصول المحمول والوصول عن بعد (MRA). قد يؤدي هذا التغيير إلى حدوث حالات فشل في تسجيل الدخول إلى MRA بعد إجراء ترقية على نظام Expressway الأساسي.

بروتوكول نقل النص التشعبي الآمن (HTTPS) هو بروتوكول اتصال آمن يستخدم أمان طبقة النقل (TLS) لتشفير الاتصال. وهو يقوم بإنشاء هذه القناة الآمنة باستخدام شهادة TLS التي يتم تبادلها في مصافحة TLS. تخدم هذه الخدمة غرضين: المصادقة (لمعرفة 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 ارسلها CUCM / IM&P / Unity، يلزم أن تكون قادرة على إنشاء ارتباط من تلك الشهادة إلى المرجع المصدق (الجذر) الأعلى (CA) الذي يثق بشهادة كيانات الشهادات التي تربط شهادة من الرمي هو تسلسل، وهو الرابط، هذا يسمى. في كل يحتوي هذه، السلسلة الثقة للتحقق من التمكن من سلسلة ثقة. سلسلة، جذر مصدق مرجع شهادة على حقلين: المصدر (أو "المصدر بواسطة") والموضوع (أو "المصدر 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 يمكننا أن نرى أن شهادة الخادم يتم تسليمها (إصدارها) من قبل مرجع مصدق يسمى vngtp-active-DIR-CA.

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

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

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

في الحالات النموذجية، لا تصدر CA الجذر شهادات الخادم مباشرة. بدلا من ذلك، إنها تصدر شهادات ل CAs أخرى. ويطلق على هذه الأنواع الأخرى من النوع الحادة بعد ذلك اسم شهادات أو شهادات إصدار بدورها الوسيطة CAs يمكن أن توقع. المتوسطة. النوع المرجعية الخادم مباشرة ل CAs الوسيطة الأخرى. يمكن أن يكون لديك حالة حيث يتم إصدار شهادة المرجع حتى يحصل. وهكذا متوسط CA 2 من شهادة على يحصل بدوره الذي، متوسط CA 1 من 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 التوثيق الخاص ب Expressway-C.

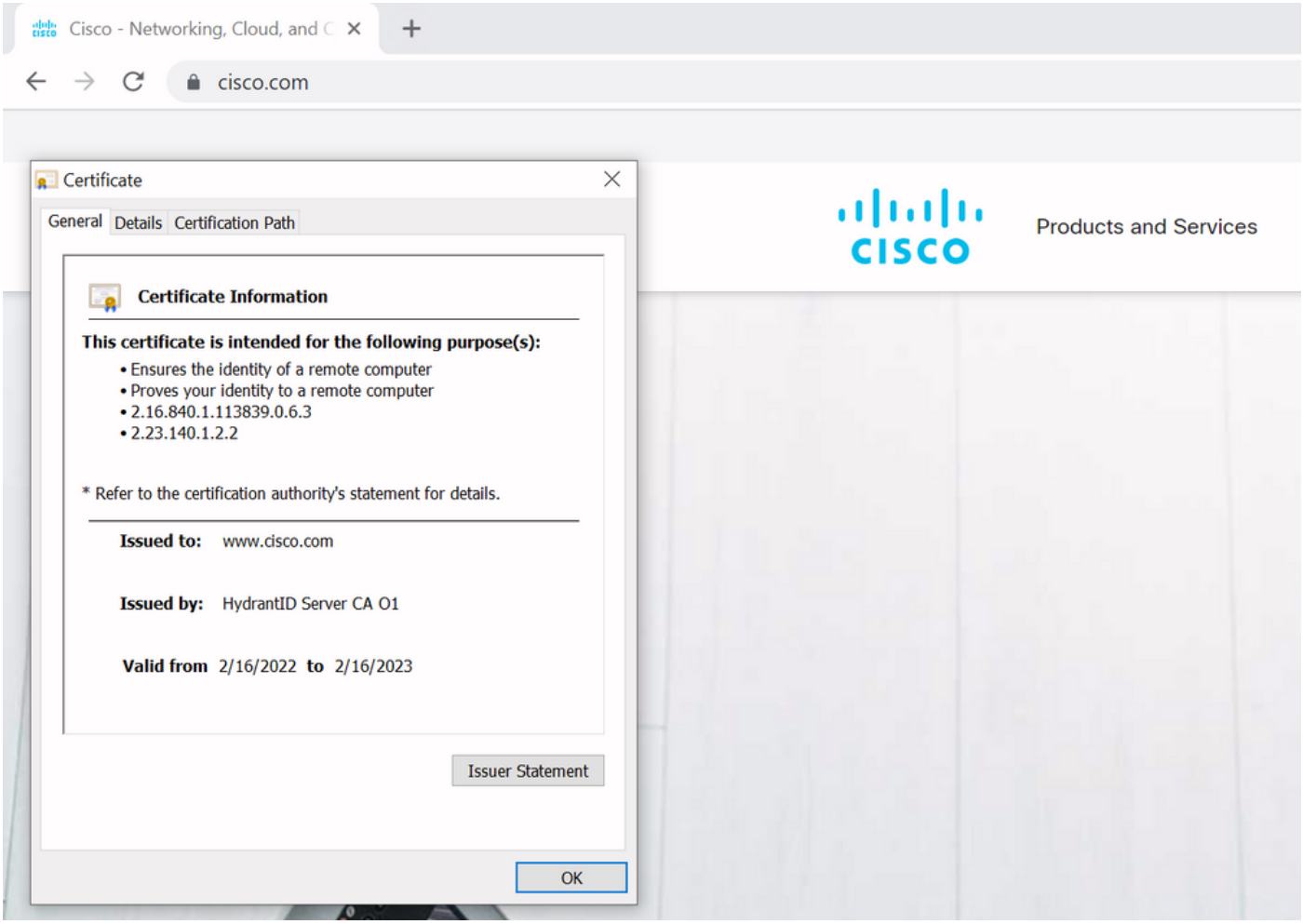
ملاحظة: على الرغم من أن حقلي المصدر والموضوع يسهل عليهما بناء سلسلة من الثقة بطريقة بشرية يمكن قراءتها، فإن CUCM لا تستخدم هذين الحقلين في الشهادة. وبدلا من ذلك، فإنه يستخدم حقلي "معرف مفتاح المرجع X509v3" و"معرف مفتاح الموضوع X509v3" لبناء سلسلة الثقة. تحتوي هذه المفاتيح على معرفات للشهادات تكون أكثر دقة ثم الاستخدام حقول الموضوع/المصدر: يمكن أن تكون هناك شهادتان بنفس حقول الموضوع/المصدر ولكن انتهت صلاحية واحدة منها ولا تزال واحدة صحيحة. 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 أو أن تستخدم أسماء عامة مختلفة له أو أن ترى أنها تستخدم دائما نفس الشهادة (من المحتمل من خلال ميزة إعادة إستخدام شهادة في CUCM 14).

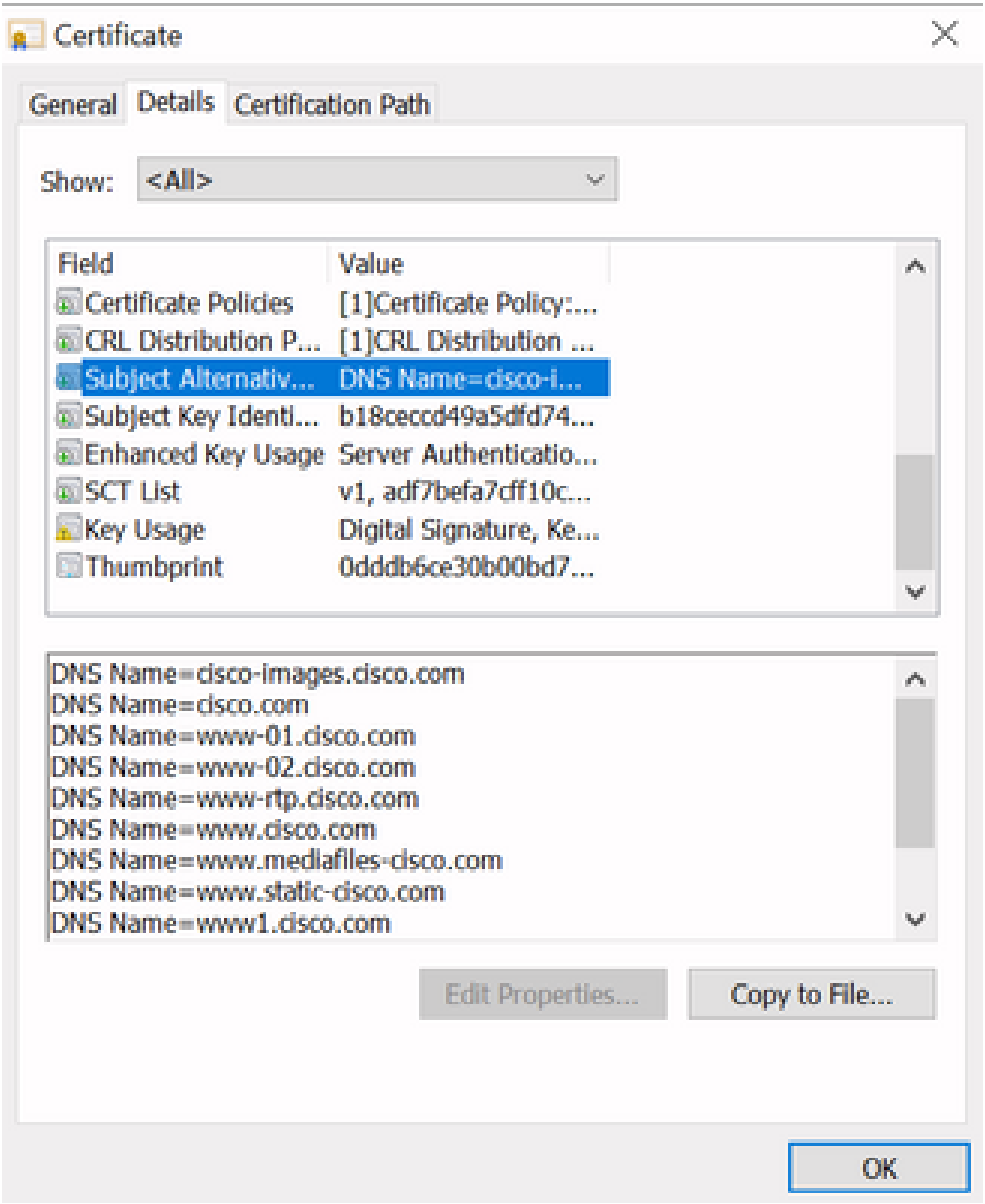
فحص SAN وأ CN

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 وه بالفعل الخادم الصحيح. ويقوم بذلك استنادا إلى العنوان الذي تم تقديم الطلب من أجله.

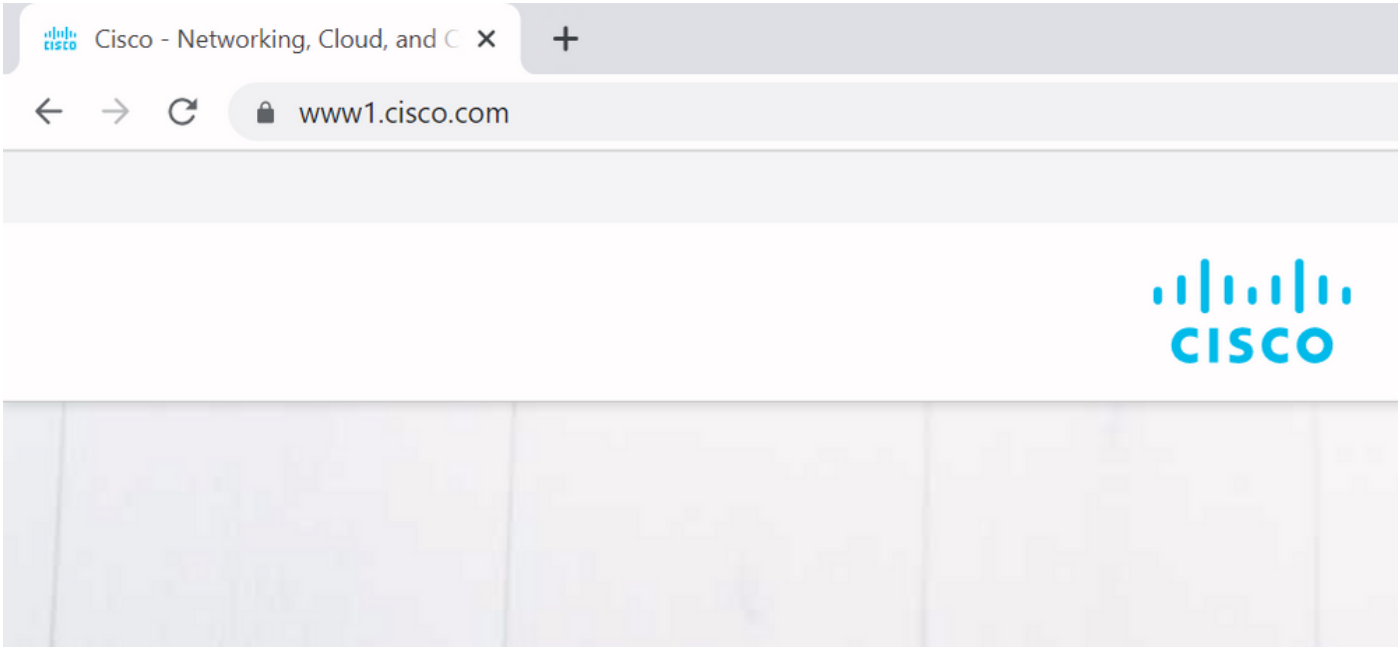
نفس النوع من العمليات تحدث في متصفحك، لذا دعونا ننظر في هذا من خلال مثال. إذا قمت بالاستعراض إلى https://www.cisco.com ستري أيقونة قفل بجوار عنوان URL الذي أدخلته مما يعني أنه اتصال موثوق به. يستند هذا إلى كل من سلسلة ثقة CA (من القسم الأول) وكذلك إلى فحص SAN وأ CN. إذا فتحنا الشهادة (عن طريق المستعرض 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 أدرناه 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).



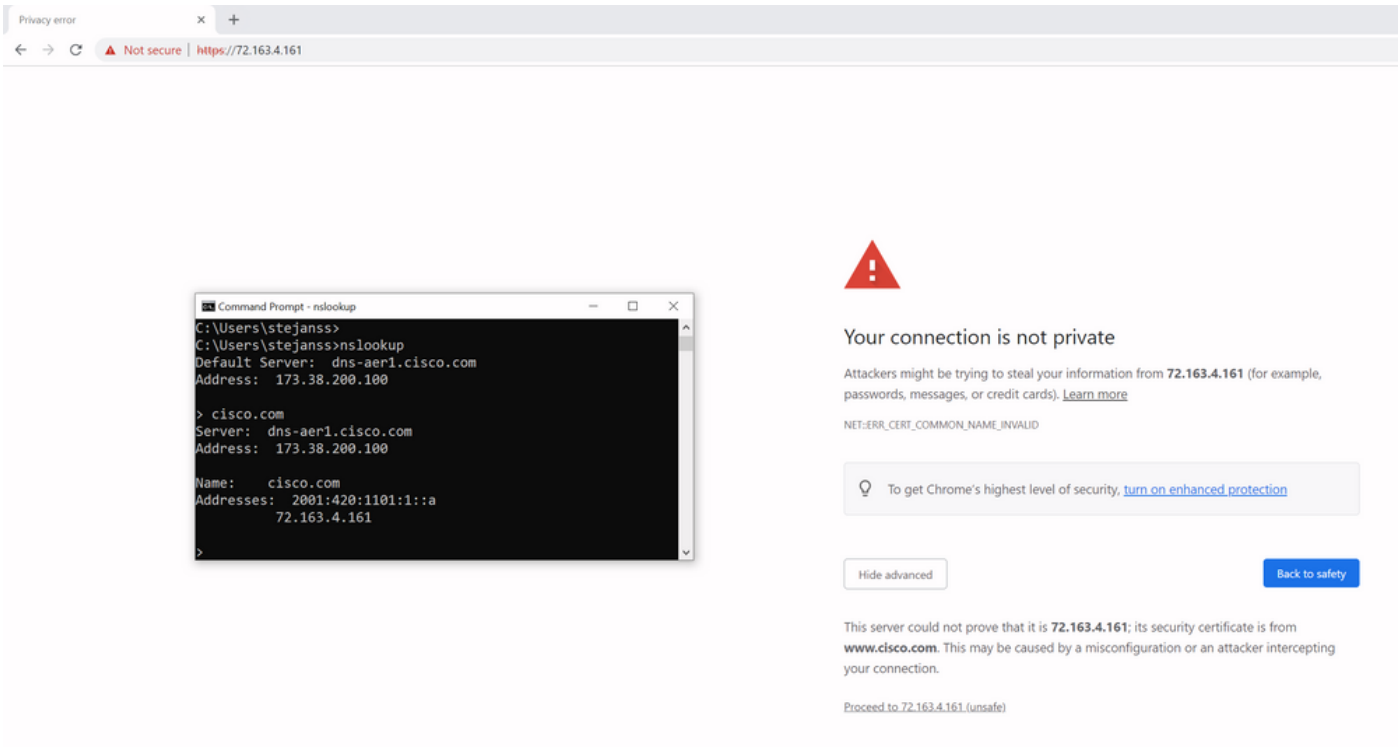
عند الاطلاع على تفاصيل الشهادة وعلى إدخالات شبكة منطقة التخزين (SAN) بشكل خاص، نلاحظ أن نفس الشيء يتكرر بالإضافة إلى بعض إدخالات شبكة منطقة التخزين (FQDN) الأخرى:



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.

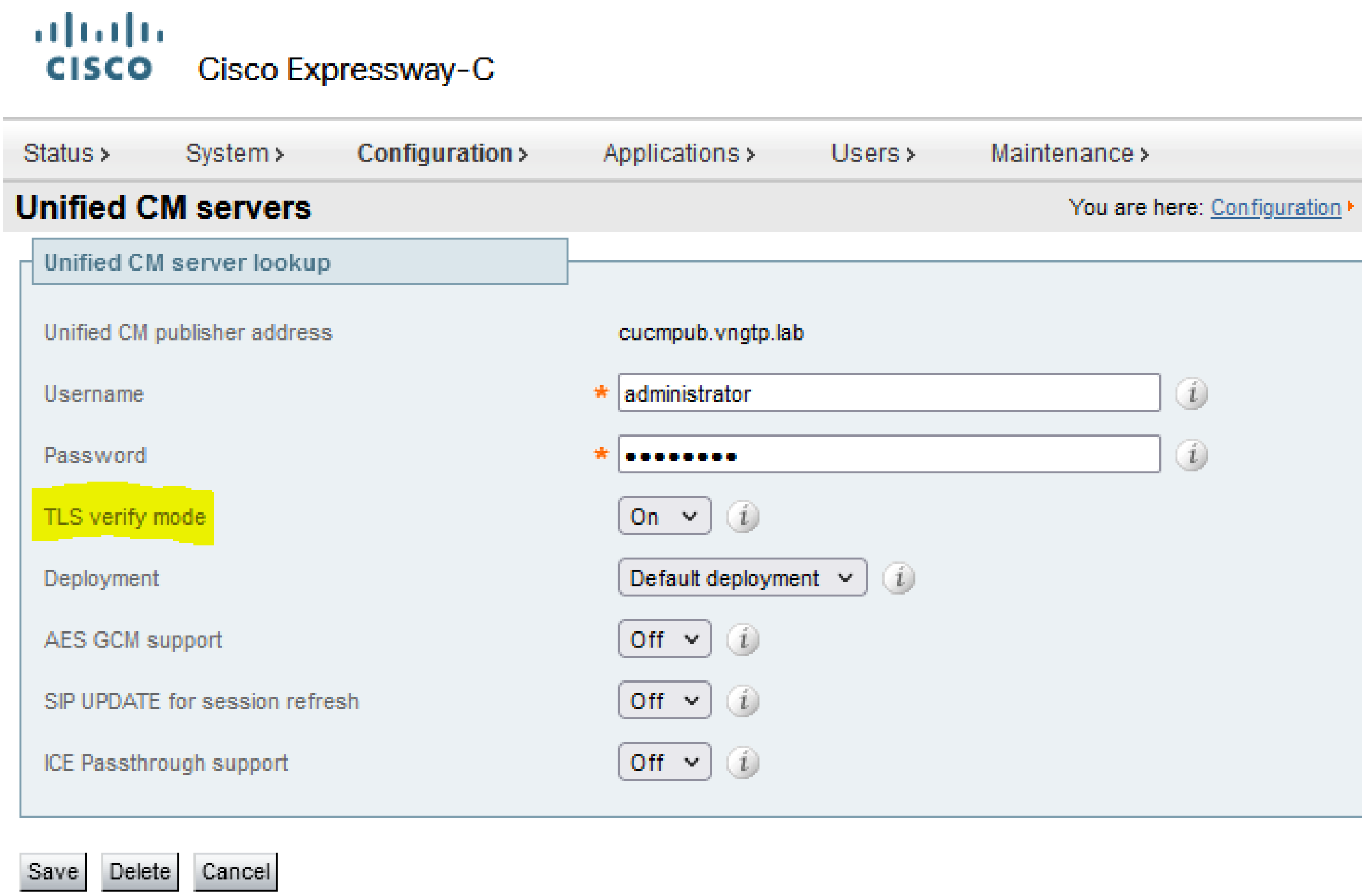
تغيير السلوك

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 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 باستخدام FQDN من cucm.steven.lab. بافتراض أن شهادة tomcat من CUCM تحتوي على cucm.steven.lab كإدخال إلى SAN وليس كعنوان IP، بعد ذلك يتجح الاكتشاف مع 'TLS Verify Mode' على 'On' ولكن الاتصالات الفعلية من عملاء MRA يمكن أن تستهدف FQDN أو IP مختلف وبالتالي تفشل التحقق من TLS.

الإصدارات من X14.2.0 والإصدارات الأحدث

من إصدار X14.2.0 فصاعدا، يعمل خادم Expressway على التحقق من شهادة TLS لكل طلب HTTPS يتم إجراؤه من خلال خادم حركة مرور البيانات. وهذا يعني أنه تنفذ هذا أيضا عندما يتم تعيين "وضع التحقق من TLS" على "إيقاف" أثناء اكتشاف عقد CUCM / IM&P / Unity. عندما لا تنجح عملية التحقق من الصحة، لا يتم تأكيد اتصال TLS ويفشل الطلب الذي يمكن أن يؤدي إلى فقد الوظائف مثل مشاكل التكرار أو ازدواج الفشل أو فشل تسجيل الدخول الكامل على سبيل المثال. أيضا مع تعيين "وضع التحقق من TLS" على "تشغيل"، لا يضمن أن تعمل جميع الاتصالات بشكل صحيح كما هو منصوص عليه في المثال الحالي.

ترد الشهادات الدقيقة التي يفحصها الطريق السريع من عقد CUCM / IM&P / Unity كما هو موضح في قسم [دليل MRA](#).

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

ال يكون تغيير أمر تفضيل التشفير هذا ذا صلة بك دائما لأنه يعتمد على مسار الترقية كما هو موضح من [إصدار الملاحظات](#) 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 ال. 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 الحق:

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 ويرانيسلا تاهالصإو اهحال

رهظت ويرانيسلا ةيلاتلا ويرانيس اهباشم يف ةئيب ةيلمعم ثيح لشف ليجست لوخدلا ىلإ MRA دعب ةيقرت Expressway نم X14.0.7 ىلإ X14.2. يتلا نوهباشتي يف تالجسلا، ىلع مغرلا نم نأ ةقدلا ةفلتخم. يتم عيمجت تالجسلا طقف ةطساوب ليجستلا يصيخشتلا (نم ةنايصلا > تاصيخشتلا > ليجستلا يصيخشتلا) يذلا مت ءدب يف 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 مداخلل Expressway-C وأ نكمي نأ نوكت ةداهش ةعقوم ايتاذ (يف رهوجلا عجرم قدصم ايتاذ) ال 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 اهلماعت لكشب حيحص ىلع ذفنملا 8443 (ةباجتسإ 200 OK) نكلو اهنكلو ثدحي أطخ (ةباجتسإ 502) ىلع ذفنملا 6972 لاصتال TFTP.

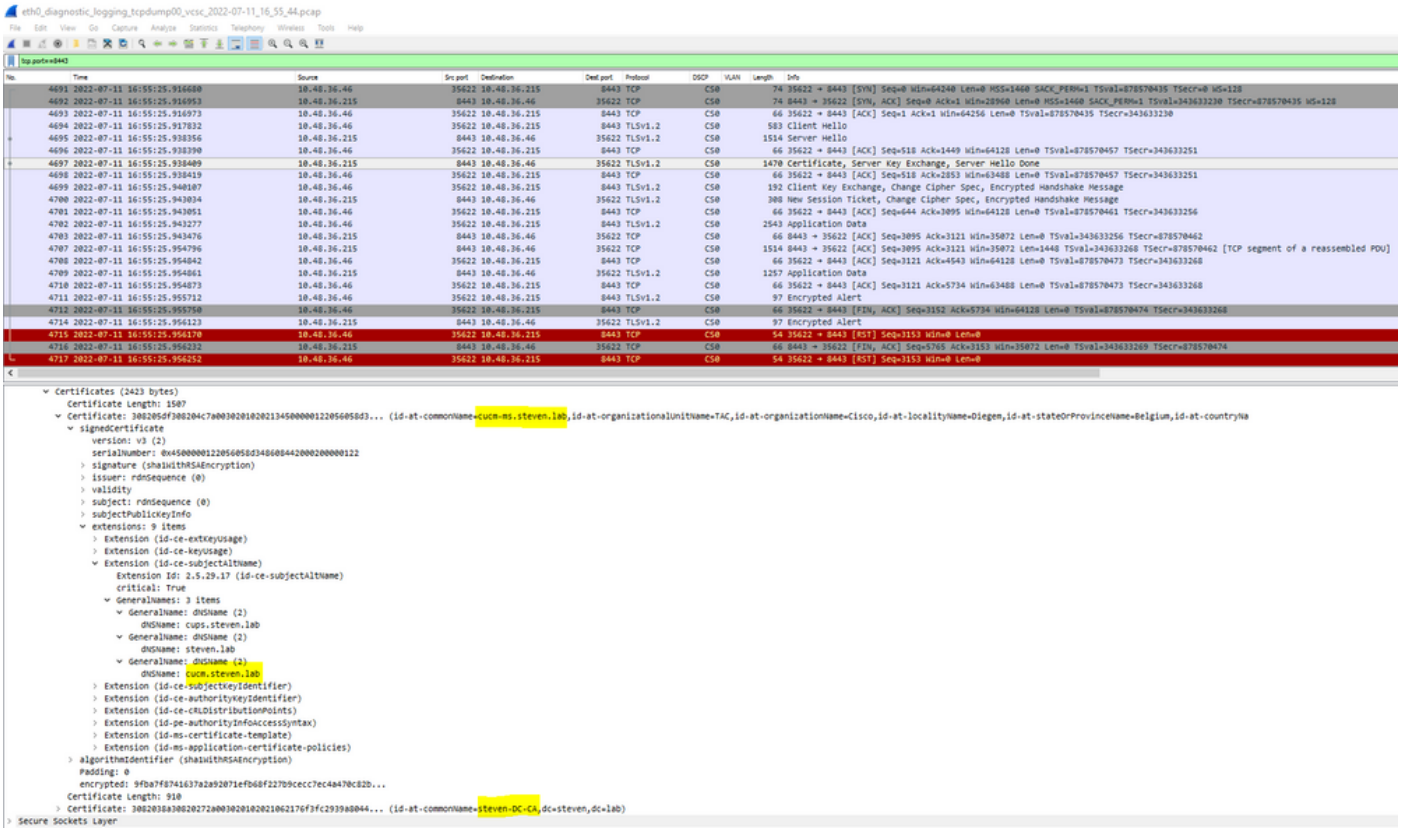
<#root>

```
===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]
```

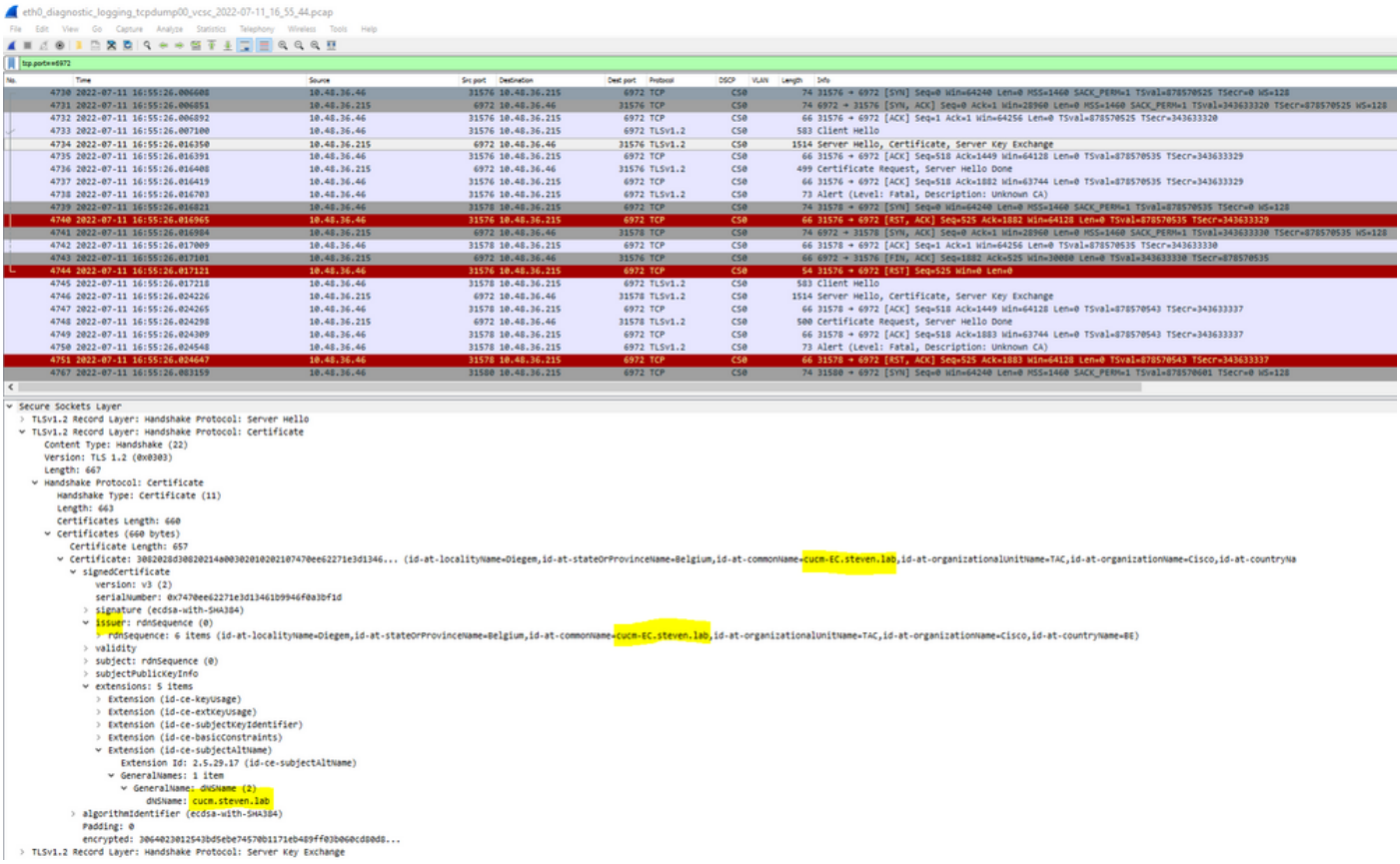
```
ERROR: SSL connection failed for
 'cucm.steven.lab': error:1416F086:
SSL routines:tls_process_server_certificate:certificate verify failed

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

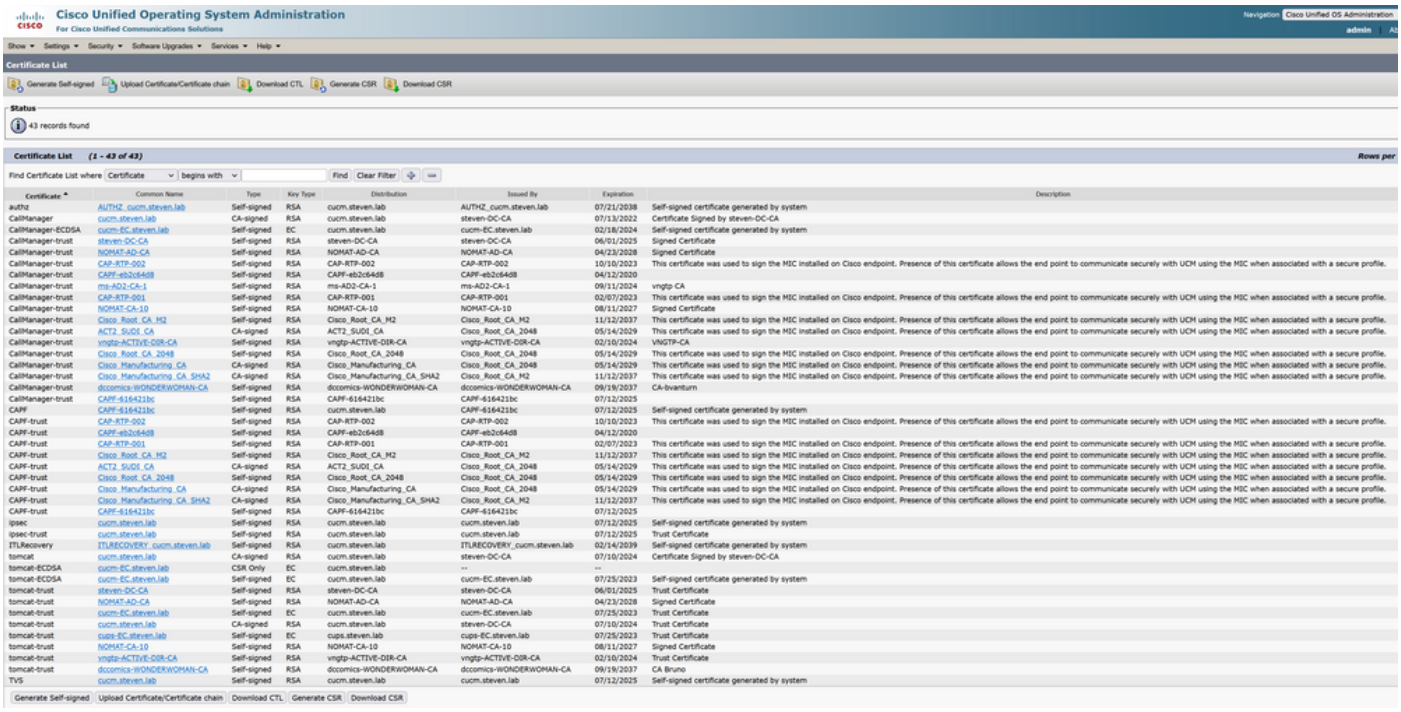
عندما ننظر في ملف PCAP الذي تم تجميعه في الطوابع الزمنية المذكورة من سجلات النص، يمكنك أن ترى أن CUCM يقدم الشهادة مع CN على هيئة CUCM-ms.steven.lab (و cucm.steven.lab على هيئة SAN) موقعة من قبل Steven-DC-CA إلى Expressway-C على المنفذ 8443.



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

ماظنلا نمض CUCM دادعإ دنع ،لاثملا ليبس ىلع .هلجأ نم بلطلا ميدقتب MRA ليمع موقي > CUCM مداخ IP (10.48.36.215)، كب صاخلا مادختساب ناونع Expressway-C نلعي كلذ نع اذهب (Expressway-C لالخ نم ليكولا) ليمعلا نم ةقحاللا تابلطلا فادهتسإ متيو ليمعلل ناونعلا.

متيو كلذك TLS نم ققحتلا لشفي ،مداخلا ةداهش نمض اذه لاصتالا ناونع نوكي ال امدنع ىلإ MRA ىلع ليجست لوخدلا يف لشف هنع جتني 502 أطخ ءاقلإ لاثملا ليبس ىلع.

<#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

ثيح متت ةمجرت c3RldmVuLmxhYi9odHRwcy8xMC40OC4zNi4yMTUvODQ0Mw (base64) ىلإ steven.lab/https/10.48.36.215/8443، يذلاو رهظي هنأ بجي نأ موقي لاصتالاب وحن 10.48.36.215 ةداهش يوتحت ال ،تاقاطبلا مزح يف حضوم وه امك .cucm.steven.lab نم الدب لاصتا ناونعك CUCM TOMCAT ىلع ناونع IP يف ةكبش نيزختلا (SAN) نمو مث متي ءاقلإ أطخلا.

كيفية التحقق نم اهتحص ةلوهسب

كنكمي التحقق امم اذإ تنك ريغت ديرت اذه كولسلا ةلوهسب مادختساب تاوطخلا التالية:

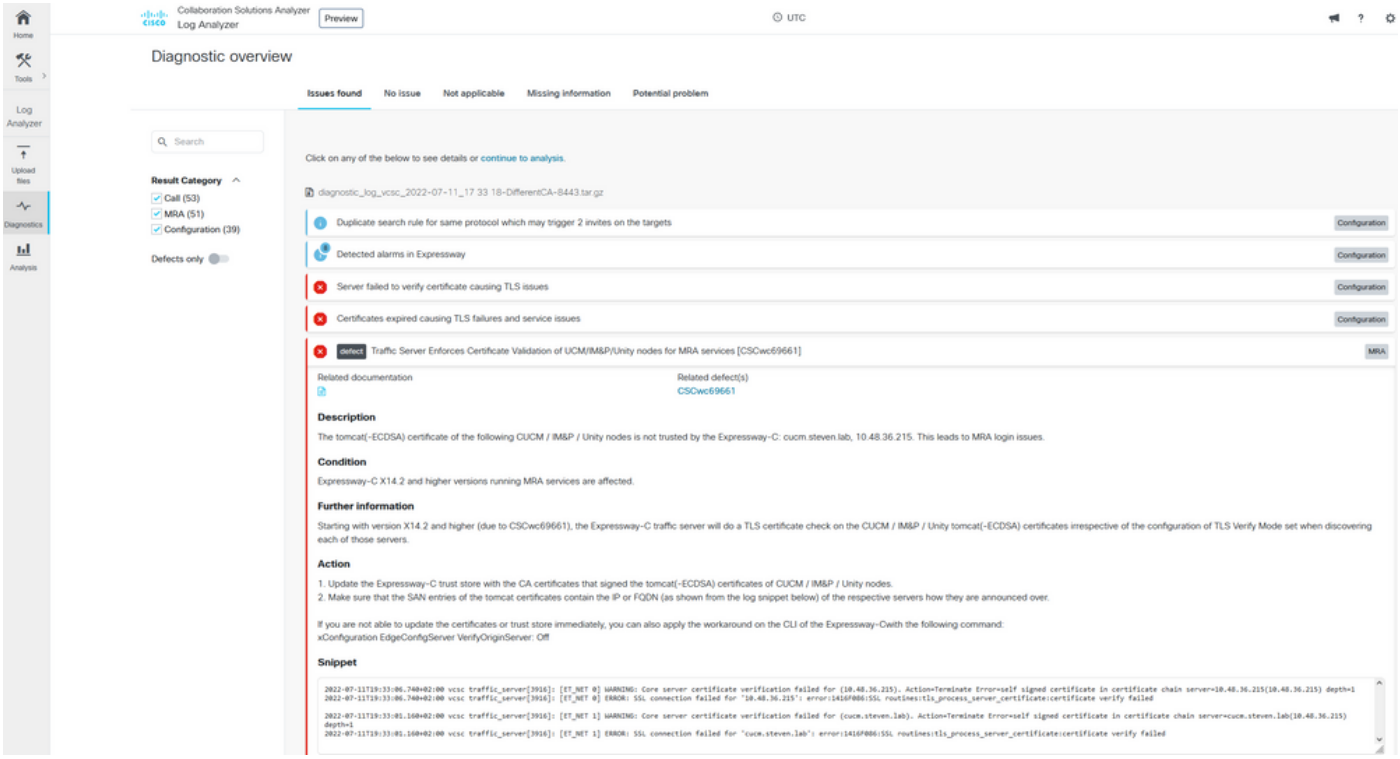
1. ءدب ليجستلا يصيخشتلا ىلع مداخ (مداوخ) Expressway-E و C (نيكمت عم ايجذومن TCPDumps) نم ةنايصلا > تاصيخشتلا > ليجستلا يصيخشتلا (يف ةلاح ماظن ةعومجم، يكو نوكي ايفاك ليغشتل هنم ةدقعلا ةيساسألا)

2. لواح ليجست لوخدلا ىلإ MRA وأ رابتخإ ةفيظولا ةلطعملا دعب ةيقرتلا

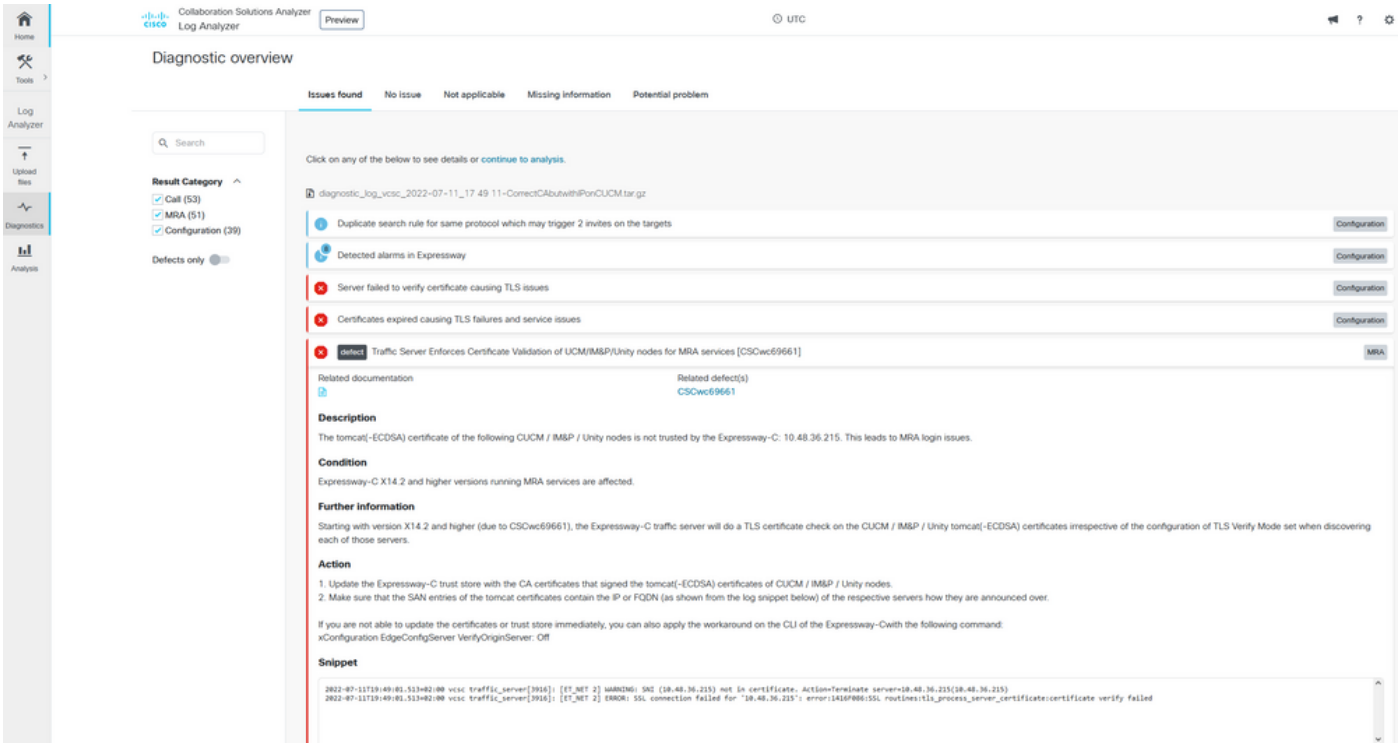
3. انتظر حتى يفشل التسجيل التشخيصي على خادم (خوادم) Expressway-E و C ثم قم بإيقاف التسجيل التشخيصي (في حالة مجموعة، تأكد من جمع السجلات من كل عقدة من المجموعة بشكل فردي)

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 وهو التأكد من أن التحقق من TLS يعمل بشكل جيد. يعتمد الإجراء الذي سيتم تنفيذه على رسالة التحذير المعروضة.

عند ملاحظة التحذير: فشل التحقق من شهادة الخادم الأساسي لـ (<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 موقعة ذاتيا (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: لا تسمح Expressway بتحميل شهادتين مختلفتين (موقعة ذاتيا على سبيل المثال) إلى مخزن الضمان لـ Expressway لديهما نفس الاسم المشترك (CN) طبقا لمعرفة تصحيح الأخطاء من Cisco CSCwa12905. لتصحيح هذا الأمر، قم بالاتصال إلى الشهادات الموقعة من CA أو ترقية CUM إلى الإصدار 14 حيث يمكنك إعادة إستخدام نفس الشهادة (الموقعة ذاتيا) لـ Tomcat و CallManager.

عندما تلاحظ التحذير: SNI (<server-FQDN-أو IP>) غير موجود في رسالة الشهادة، فإنه 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 الأجل وهو تطبيق الحل كما وهو موثق للرجوع إلى السلوك السابق قبل X14.2.0. يمكنك تنفيذ ذلك من خلال CLI (واجهة سطر الأوامر) على عقد 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).