Expressway流量服务器证书验证故障排除

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

- 可信CA链
- SAN或CN检查

行为更改

- 低于X14.2.0的版本
- X14.2.0及更高版本

故障排除场景

- 1.签署远程证书的CA不受信任
- 2.证书中不包含连接地址（FQDN或IP）

如何轻松验证

解决方案

相关信息

简介

本文档介绍与Cisco Bug ID CSCwc6961或Cisco Bug ID CSCwa25108关联的Expressway版本X14.2.0及更高版本上的行为更改。

先决条件

要求

Cisco 建议您了解以下主题：

- Expressway基本配置
- MRA基本配置

使用的组件

本文档中的信息基于Cisco Expressway版本X14.2及更高版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

此行为更改由Cisco Bug ID CSCwc标记69661

或Cisco Bug ID CSCwa25108
,Expressway平台上的流量服务器对用于移动和远程访问(MRA)服务的Cisco Unified Communication Manager(CUCM)、Cisco Unified Instant Messaging & Presence(IM&P)和Unity服务器节点执行证书验证。在Expressway平台上升级后，此更改可能会导致MRA登录失败。

安全超文本传输协议(HTTPS)是一种使用传输层安全(TLS)加密通信的安全通信协议。它通过使用在TLS握手过程中交换的TLS证书来创建此安全通道。这有两个目的：身份验证（了解您连接的远程方）和隐私（加密）。 身份验证可防止中间人攻击，并且隐私可防止攻击者窃听和篡改通信。

TLS（证书）验证在看到身份验证时执行，并允许您确保已连接到正确的远程方。验证包括两个单独的项目：

1.受信任证书颁发机构(CA)链

2.主题备用名称(SAN)或公用名称(CN)

可信CA链

对于Expressway-C要信任CUCM/IM&P/Unity发送的证书，它需要能够建立从该证书到其信任的顶级（根）证书颁发机构(CA)的链接。此类链接是将实体证书链接到根CA证书的证书层次结构，称为信任链。为了能够验证此类信任链，每个证书包含两个字段：发行人（或发行人）和主体（或发行人）。

服务器证书（例如CUCM发送到Expressway-C的那个）在Subject字段中通常在CN中具有其完全限定域名(FQDN):

```
        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
```

CUCM cucm.vngtp.lab的服务器证书示例。它在“主题”(Subject)字段的CN属性中具有FQDN，同时还具有其他属性，例如国家(C)、州(ST)、位置(L)。.您还可以看到服务器证书由名为vngtp-ACTIVE-DIR-CA的CA分发（颁发）。

顶级CA（根CA）也可以颁发证书来标识自己。在这样的根CA证书中，您会看到Issuer和Subject具有相同值：

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

它是根CA分发的证书，用于标识自身。

在典型情况下，根CA不会直接颁发服务器证书。相反，它们会为其他CA颁发证书。这些其它CA然后称为中间CA。反过来，中间CA可以直接为其他中间CA颁发服务器证书或证书。您可能会遇到中间的CA 1颁发服务器证书，而中间的CA 1又从中间的CA 2获取证书，以此类推。最后，中间CA直接从根CA获取其证书：

```
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
```

现在，为了让Expressway-C信任CUCM发送的服务器证书，它需要能够从该服务器证书构建信任链，直到创建根CA证书。为此，您需要在Expressway-C的信任存储中上传根CA证书和所有中间CA证书（如果有，如果根CA直接颁发CUCM的服务器证书则不会出现这种情况）。

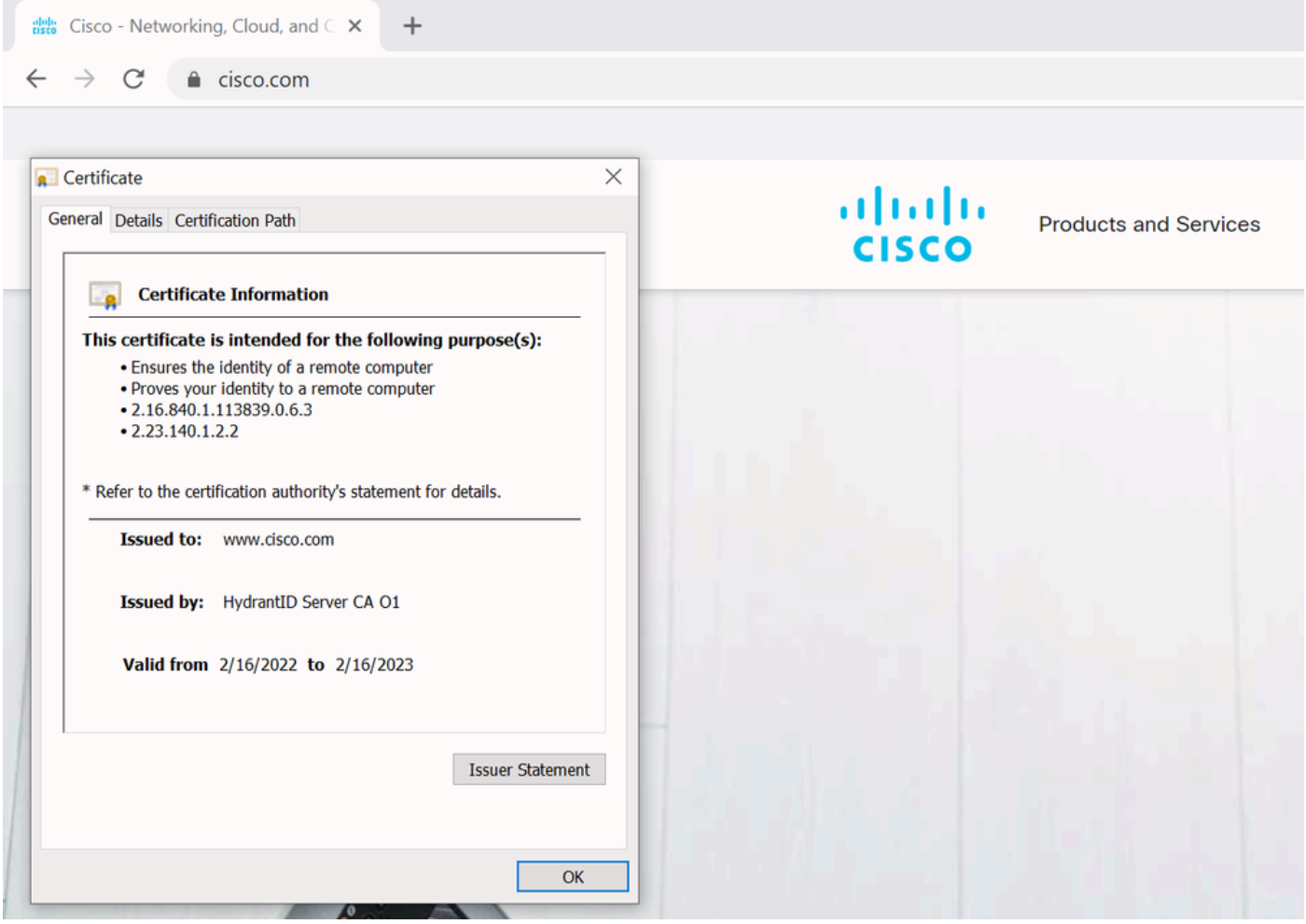
注意：虽然Issuer和Subject字段易于以人工可读的方式构建信任链，但CUCM不会在证书中使用这些字段。相反，它使用X509v3 Authority Key Identifier和X509v3 Subject Key Identifier字段构建信任链。这些密钥包含更准确的证书标识符，然后使用Subject/Issuer字段：可以有2个具有相同Subject/Issuer字段的证书，但其中一个证书已过期，另一个证书仍然有效。它们都有不同的X509v3主题密钥标识符，因此CUCM仍可确定正确的信任链。

但根据Cisco Bug ID CSCwa12905,Expressway无法这样做，并且无法将两个不同的（例如自签名）证书上传到具有相同公用名(CN)的Expressway信任存储中。 对此进行更正的方法是CA签名证书，或者为其使用不同的通用名称，或者查看它始终使用相同的证书（可能通过CUCM 14中的重复使用证书功能）。

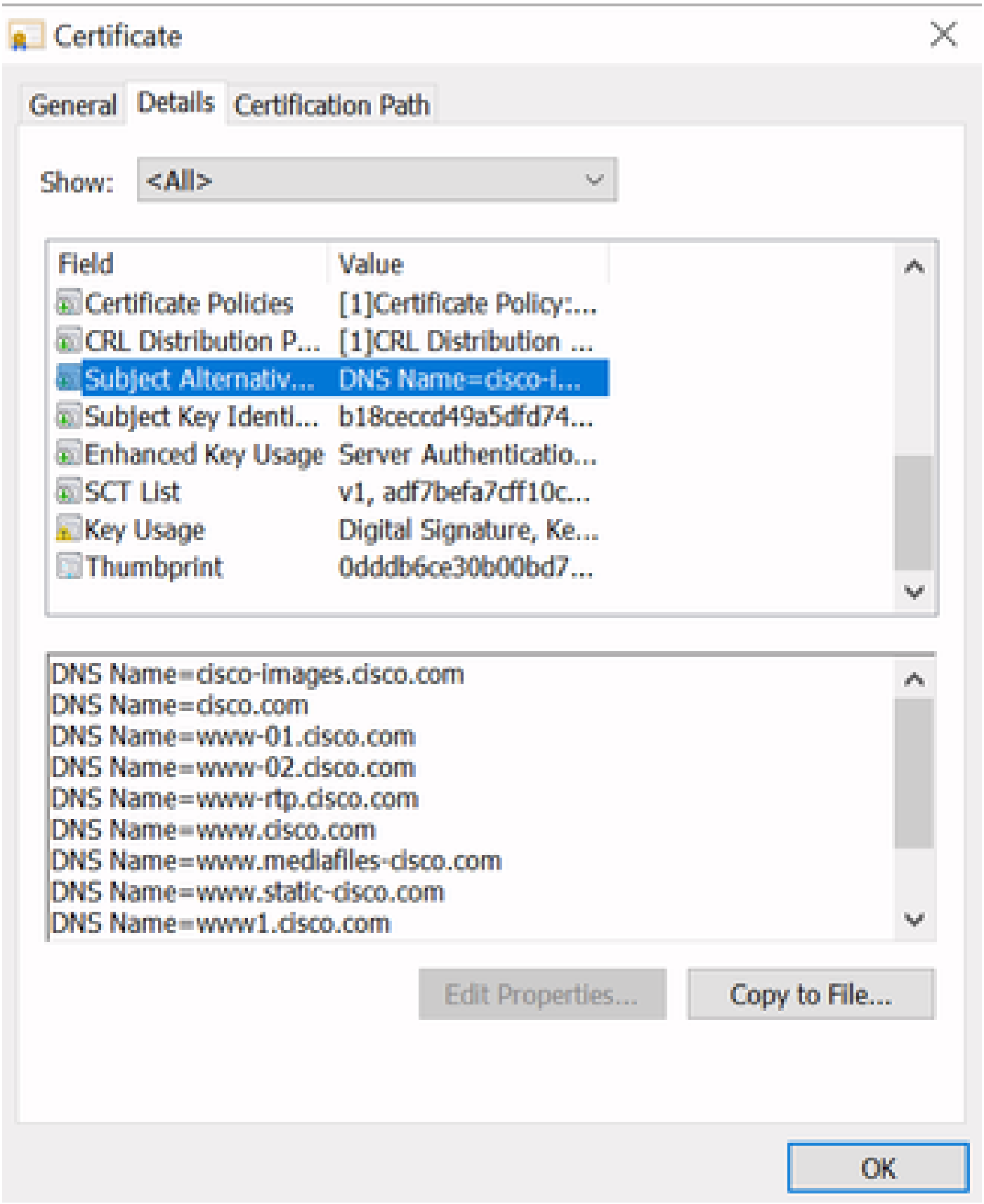
SAN或CN检查

第1步检查信任库，但是，拥有信任库中的CA签名的证书的任何人都将有效。这显然是不够的。因此，另外会进行检查，以验证您专门连接的服务器是否正确。它根据发出请求的地址执行此操作。

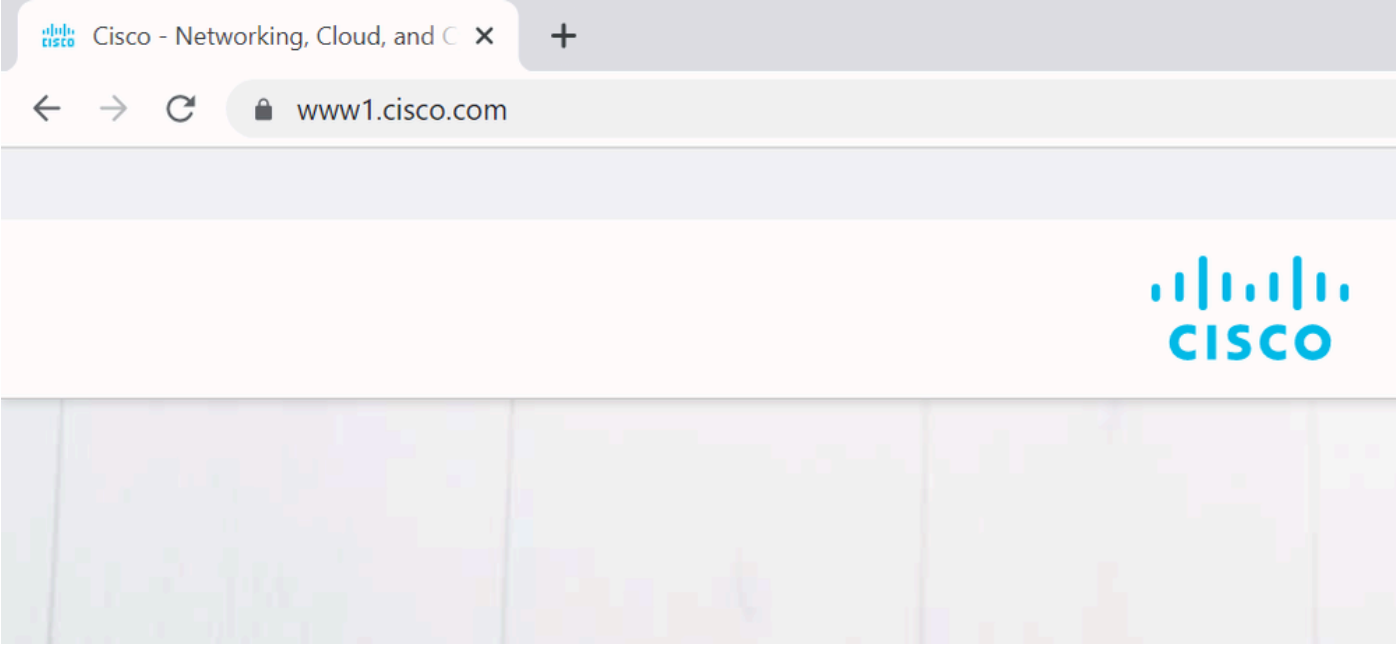
在浏览器中也会发生同样的操作，因此您可以在示例中看到这一点。如果浏览到Cisco.com，您会在输入的URL旁边看到一个锁图标，这意味着它是受信任连接。这既基于CA信任链（来自第一部分），也基于SAN或CN检查。如果您打开证书（通过点击锁定图标通过浏览器打开），您会看到公用名(在Issued to:字段)设置为Cisco.com，该字段与您想要连接的地址完全一致。通过这种方式，您可以确保连接到正确的服务器（因为您信任签署证书并在分发证书之前执行验证的CA）。



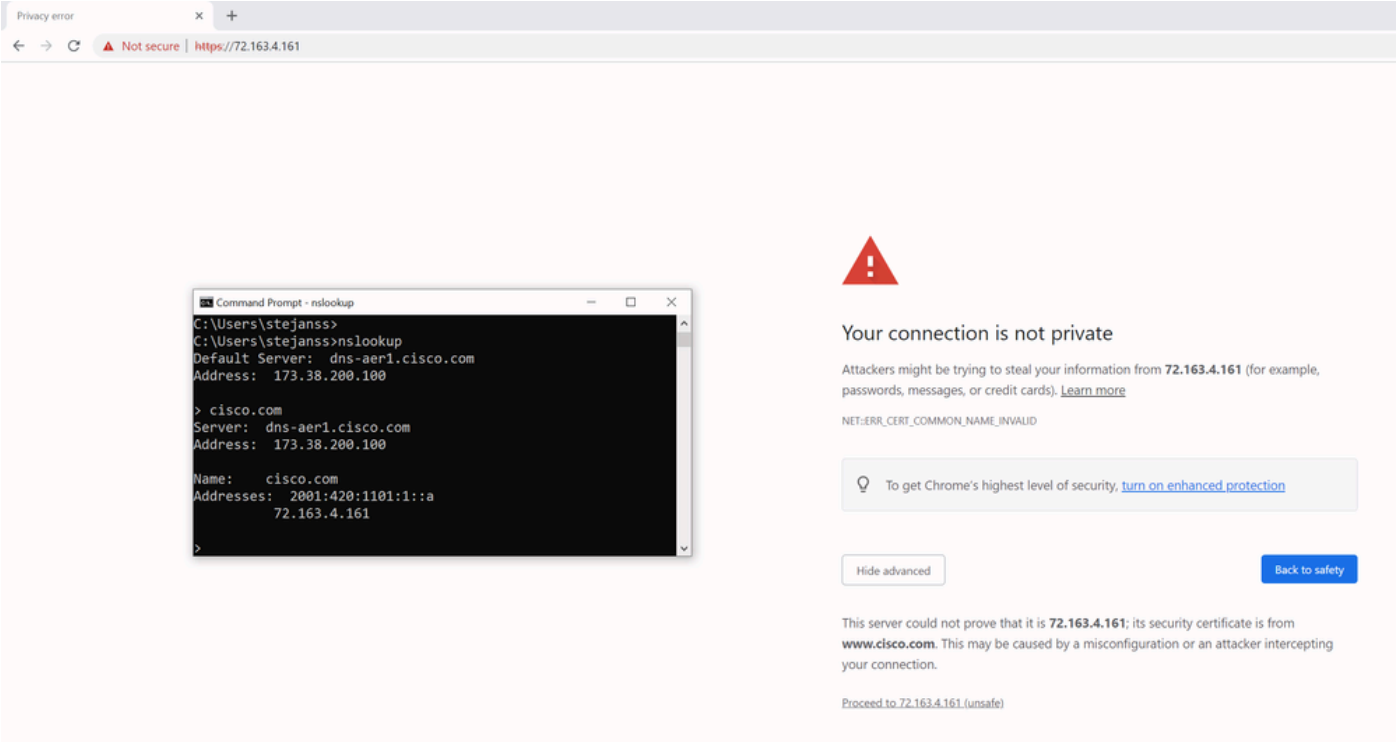
当您查看证书的详细信息（尤其是SAN条目）时，您会看到相同的内容与某些其他FQDN一样：



这意味着，例如，当您请求连接到Cisco.com时，它将显示为安全连接，因为它包含在SAN条目中。



但是，如果您不浏览Cisco.com，而是直接浏览到IP地址(编号的Web地址)，则不会显示安全连接，因为它不信任签名它的CA。提供的证书不包含您用于连接到服务器的地址(72.163.4.161)。



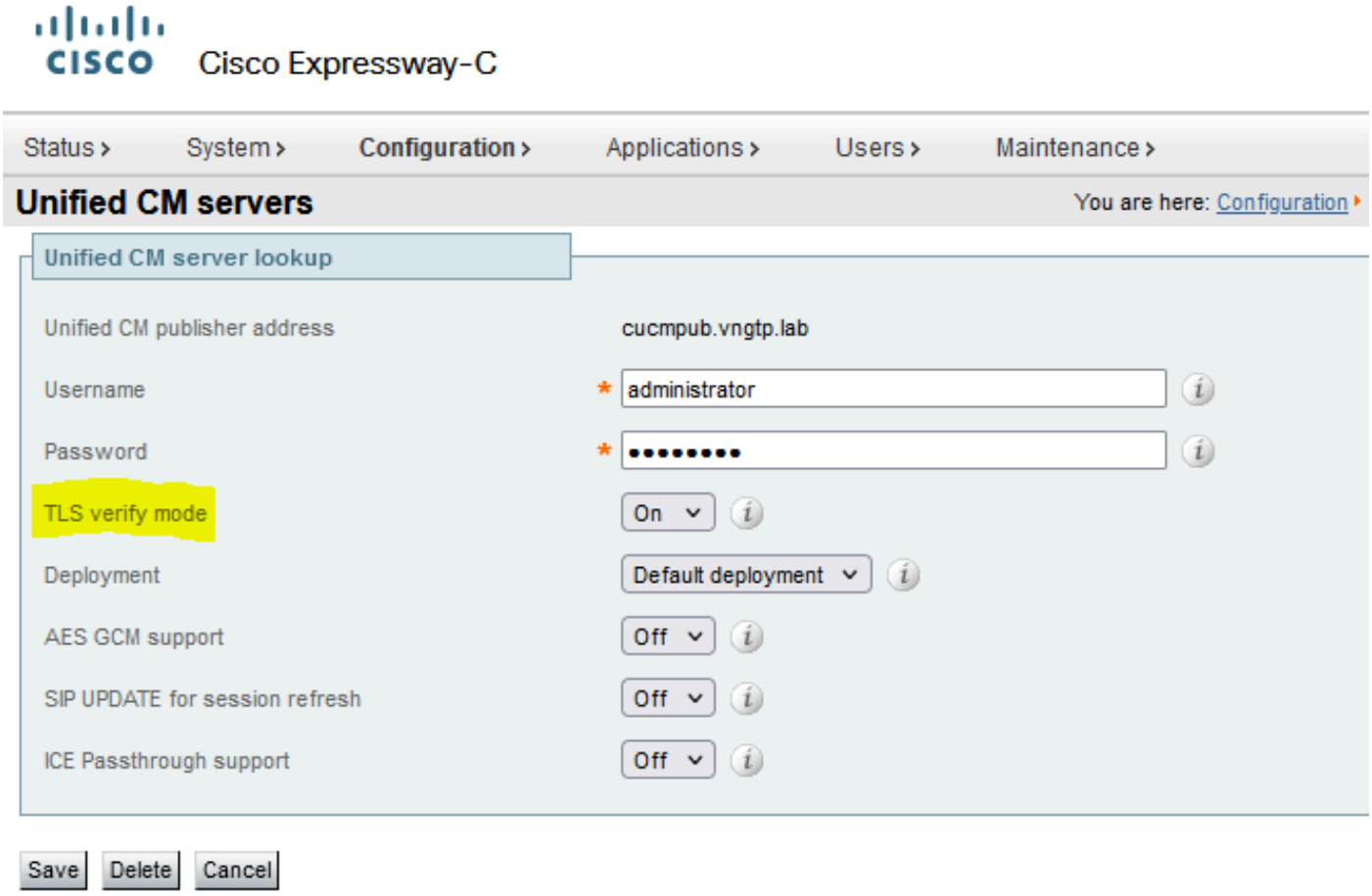
在浏览器中，您可以绕过此设置，但是，在TLS连接上，您可以启用不允许绕行的设置。因此，您的证书必须包含远程方计划用于连接它的正确CN或SAN名称。

行为更改

MRA服务严重依赖通过到CUCM/IM&P/Unity服务器的Expressway上的几个HTTPS连接，以便正确进行身份验证并收集特定于登录客户端的正确信息。此通信通常发生在端口8443和6972上。

低于X14.2.0的版本

在低于X14.2.0的版本中，Expressway-C上的流量服务器处理那些没有验证远程端提供的证书的安全HTTPS连接。这可能导致中间人攻击。在MRA配置上，当您将任一CUCM / IM&P / Unity服务器添加到Configuration > Unified Communications > Unified CM servers / IM and Presence Service nodes / Unity Connection servers下时，可以通过将TLS验证模式'配置为On来进行TLS证书验证。配置选项和相关信息框以示例形式显示，表示它确实验证了SAN中的FQDN或IP，以及证书的有效性以及证书是否由受信任CA签名。



此TLS证书验证检查仅在发现CUCM/IM&P/Unity服务器时完成，而不是在MRA登录期间查询各种服务器时完成。此配置的第一个缺点是，它仅验证您添加的发布者地址。它不会验证订用服务器节点上的证书是否设置正确，因为它从发布服务器节点的数据库中检索订用服务器节点信息（FQDN或IP）。此配置的第二个缺点是，由于连接信息而通告给MRA客户端的内容可能不同于已放入Expressway-C配置的发布方地址。例如，在CUCM上，在System > Server下，可以使用IP地址（例如10.48.36.215）向外通告服务器，然后由MRA客户端使用（通过代理的Expressway连接），但是，您可以在Expressway-C上使用FQDN cucm.steven.lab添加CUCM。因此，假设CUCM的tomcat证书包含cucm.steven.lab作为SAN条目而不是IP地址，则将TLS验证模式设置为On的发现成功，但来自MRA客户端的实际通信可以针对不同的FQDN或IP，从而无法通过TLS验证。

X14.2.0及更高版本

从X14.2.0版本开始，Expressway服务器会对通过流量服务器发出的每个HTTPS请求执行TLS证书

验证。这意味着，在发现CUCM/IM&P/Unity节点期间，当TLS验证模式设置为Off时，它也会执行该操作。如果验证失败，则TLS握手不会完成，并且请求失败，这可能导致功能丢失（例如冗余），或故障切换问题，或完全登录失败。此外，当TLS验证模式设置为On时，它不保证所有连接都能正常运行（如后面的示例所述）。

Expressway向CUCM/IM&P/Unity节点检查的确切证书如MRA指南部分所示。

除了默认的TLS验证，X14.2中还引入了一个更改，该更改可能通告不同的密码列表首选项顺序，具体取决于您的升级路径。这可能会导致软件升级后出现意外的TLS连接，因为在升级之前，它可能会从CUCM（或其他具有用于ECDSA算法的独立证书的任何产品）请求Cisco Tomcat或Cisco CallManager证书，但在升级之后，它请求ECDSA变体（实际上比RSA更安全的密码变体）。Cisco Tomcat-ECDSA或Cisco CallManager-ECDSA证书可以由其他CA签名，也可以仅由自签名证书签名（默认）。

此密码首选项顺序更改并非始终与您相关，因为它取决于Expressway X14.2.1版本说明中所示的升级路径。简而言之，您可以从Maintenance > Security > Ciphers中看到每个密码列表是否预置了ECDHE-RSA-AES256-GCM-SHA384。如果没有，则它首选更新的ECDSA密码而不是RSA密码。如果是，则您有与前面一样的行为，其中RSA具有更高的优先级。

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**).

在此场景中，TLS验证有两种可能失败，稍后将详细介绍：

1.签署远程证书的CA不受信任。

a.自签名证书

b.由未知CA签名的证书

2.证书中不包含连接地址（FQDN或IP）。

故障排除场景

以下场景显示实验室环境中的类似场景，其中Expressway从X14.0.7升级到X14.2后，MRA登录确实失败。这些场景在日志中有相似之处，但分辨率不同。日志仅由MRA登录之前开始并在MRA登录失败之后停止的诊断日志记录(从Maintenance > Diagnostics > Diagnostic logging)收集。未为其启用其他调试日志记录。

1.签署远程证书的CA不受信任

远程证书可以由未包含在Expressway-C的信任存储中的CA进行签名，也可以是未添加到Expressway-C服务器的信任存储中的自签名证书（本质上也是CA）。

在本例中，您会发现，发往CUCM(10.48.36.215 - cucm.steven.lab)的请求在端口8443（200 OK响

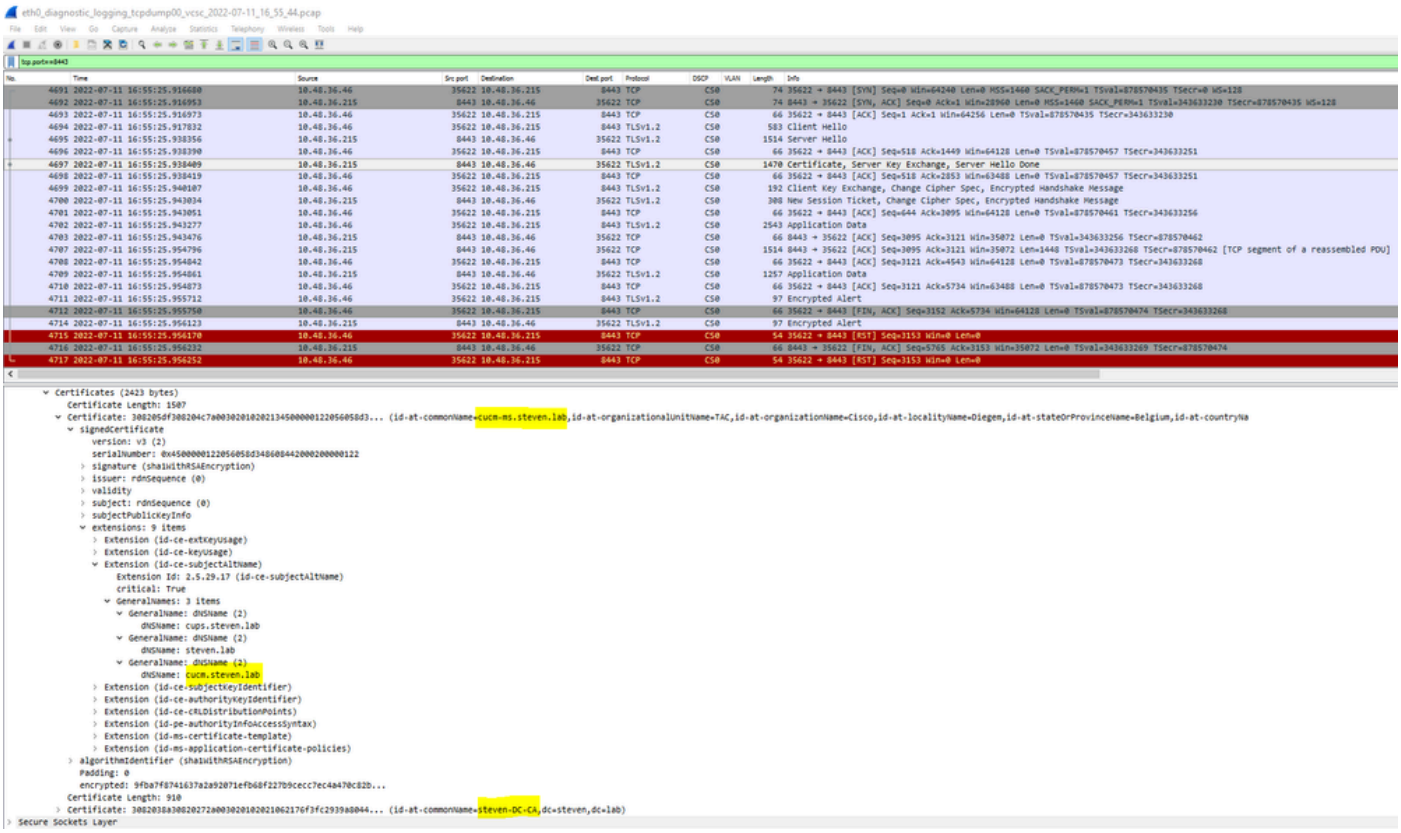
应）上得到正确处理，但是在TFTP连接的端口6972上引发错误（502响应）。

<#root>

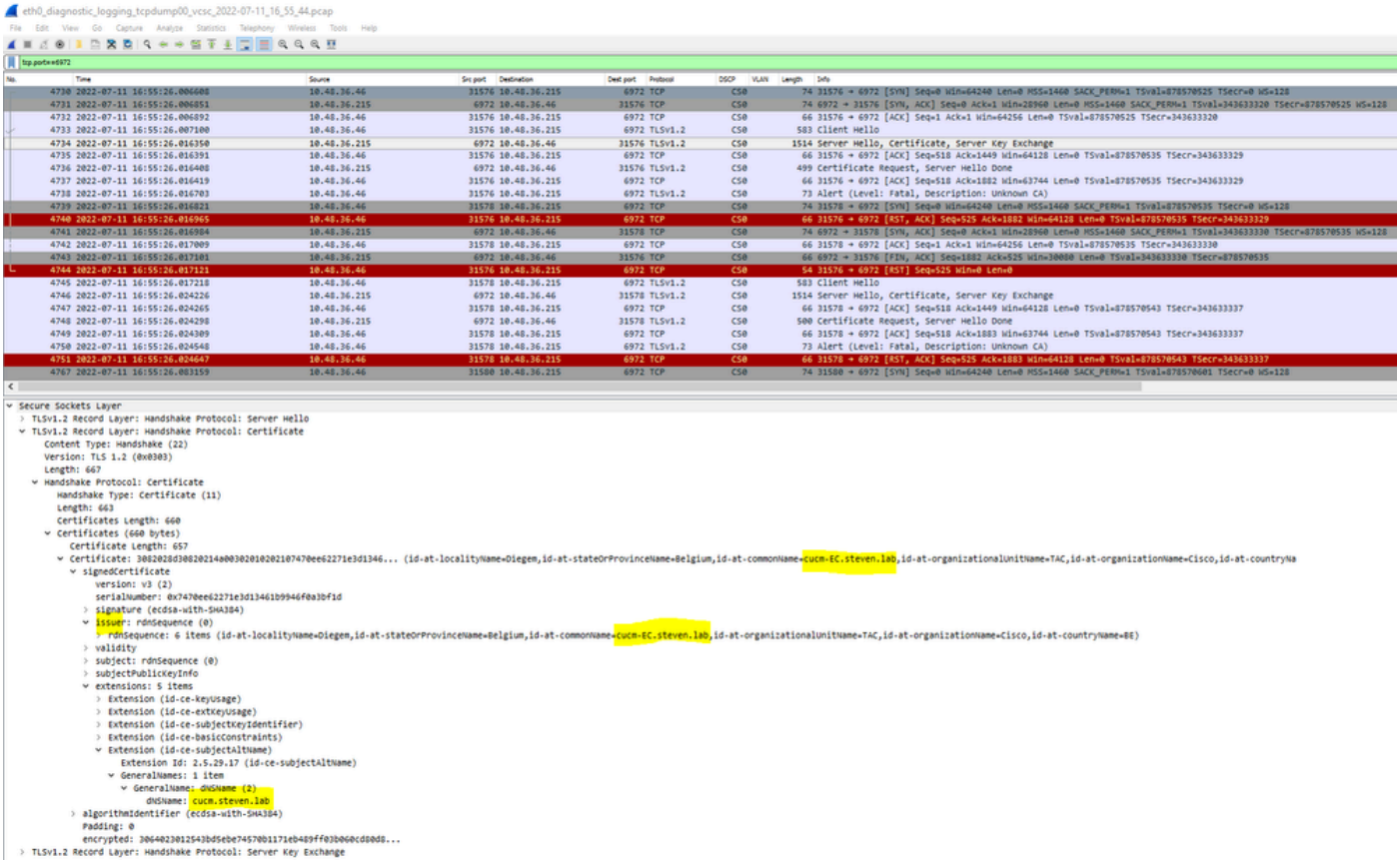
```
===Success connection on 8443===

2022-07-11T18:55:25.910+02:00 vcsc traffic_server[18242]: UTCTime="2022-07-11 16:55:25,910" Module="netw

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

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="netw

2022-07-11T18:55:26.006+02:00 vcsc traffic_server[18242]: UTCTime="2022-07-11 16:55:26,006" Module="netw
2022-07-11T18:55:26.016+02:00 vcsc traffic_server[18242]: UTCTime="2022-07-11 16:55:26,016" Module="netw
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="netw

502 connect failed

"
```

错误，证书验证失败，表示Expressway-C无法验证TLS握手。原因显示在警告行上，因为它表示自签名证书。如果深度显示为0，则为自签名证书。当深度大于0时，这意味着它有一个证书链，因此由未知CA签名（从Expressway-C的角度而言）。

当您查看从文本日志中提及的时间戳收集的pcap文件时，可以看到CUCM将带有CN的证书显示为cucm-ms.steven.lab（和cucm.steven.lab作为SAN），由steven-DC-CA签署，并发送到端口8443上的Expressway-C。

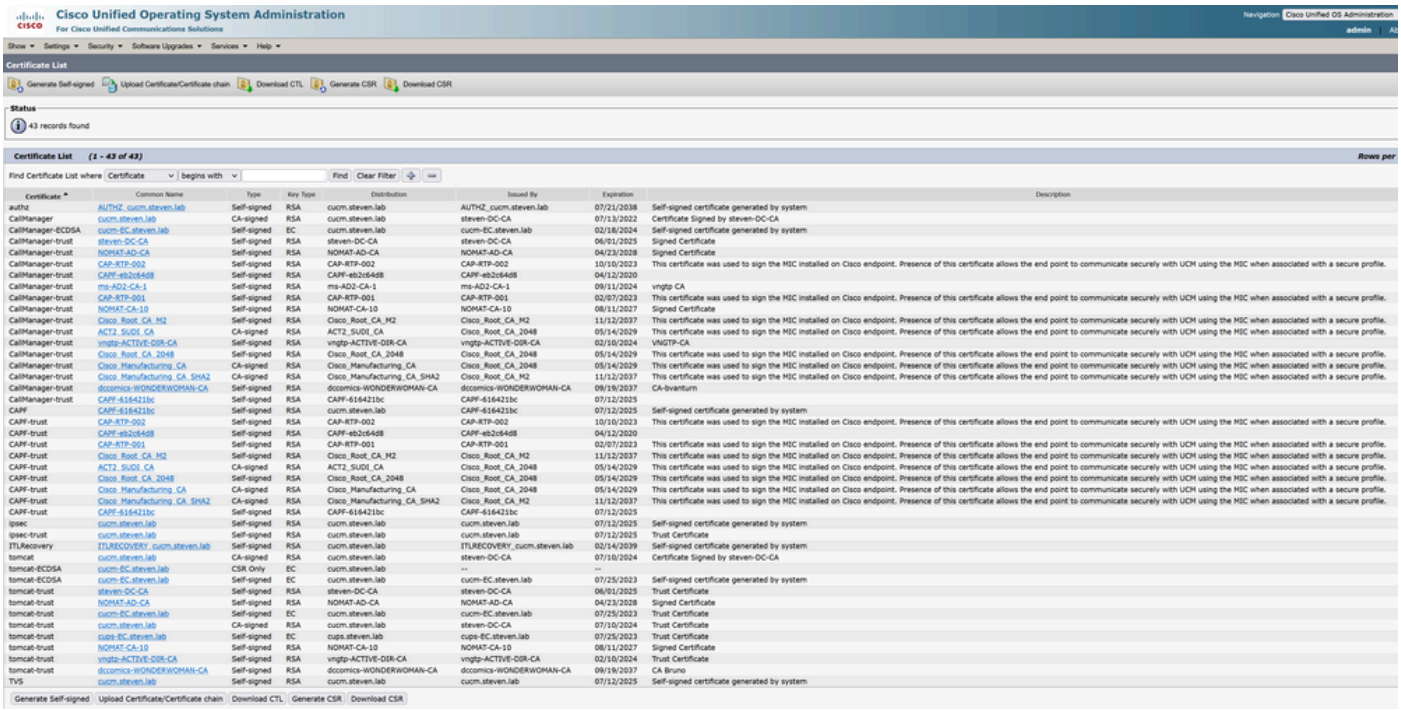


但是，当您检查端口6972上提供的证书时，您可以看到它是自签证书（颁发者自身），其CN设置为cucm-EC.steven.lab。-EC扩展指明这是CUCM上设置的ECDSA证书。



在Cisco Unified OS Administration下的CUCM上，您可以查看Security > Certificate Management下的现有证书，如下所示。它显示不同的tomcat和tomcat-ECDSA证书，其中tomcat是CA签名的（并

受Expressway-C信任），而tomcat-ECDSA证书是自签名的，不受Expressway-C信任。



2.证书中不包含连接地址（FQDN或IP）

除了信任存储之外，流量服务器还验证MRA客户端向哪个连接地址发出请求。例如，当您在CUCM上的System > Server下设置CUCM时，您的CUCM的IP地址(10.48.36.215)，则Expressway-C会将此情况通告给客户端，并且来自客户端（通过Expressway-C代理）的后续请求会以该地址为目标。

当该特定连接地址未包含在服务器证书中时，TLS验证也会失败，并引发502错误，从而导致MRA登录失败。

<#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
```

其中c3RldmVuLmxhYi9odHRwcy8xMC40OC4zNi4yMTUvODQ0Mw将(base64)转换为steven.lab/https/10.48.36.215/8443，这表示它必须将指向10.48.36.215的连接作为连接地址，而不是转换为cucm.steven.lab。如数据包捕获所示，CUCM tomcat证书不包含SAN中的IP地址，因此引发错误。

如何轻松验证

您可以通过以下步骤验证您是否容易遇到此行为更改：

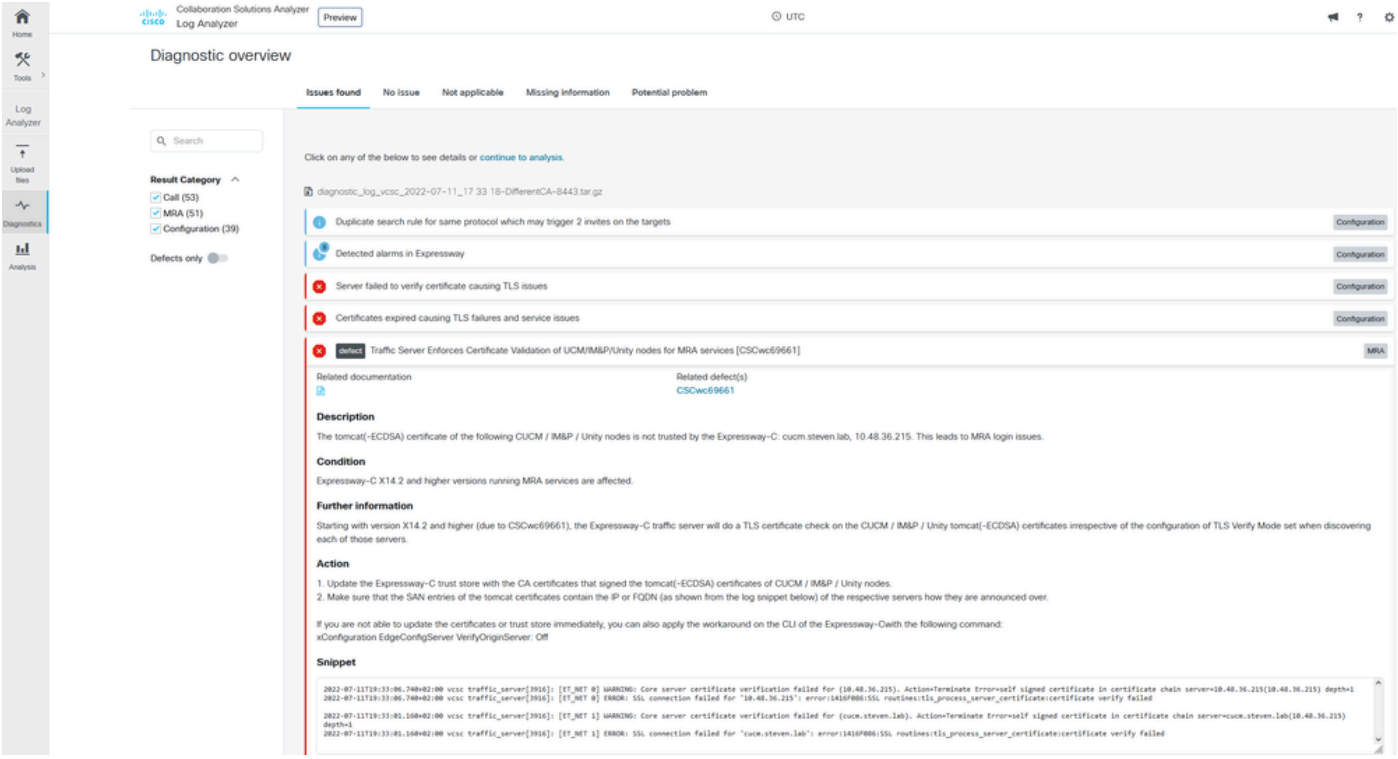
1.在Expressway-E和C服务器上启动诊断日志记录（最好启用TCPDumps），从Maintenance > Diagnostics > Diagnostic Logging（如果是集群，从主节点启动就足够了）

2.尝试登录MRA或在升级后测试中断的功能

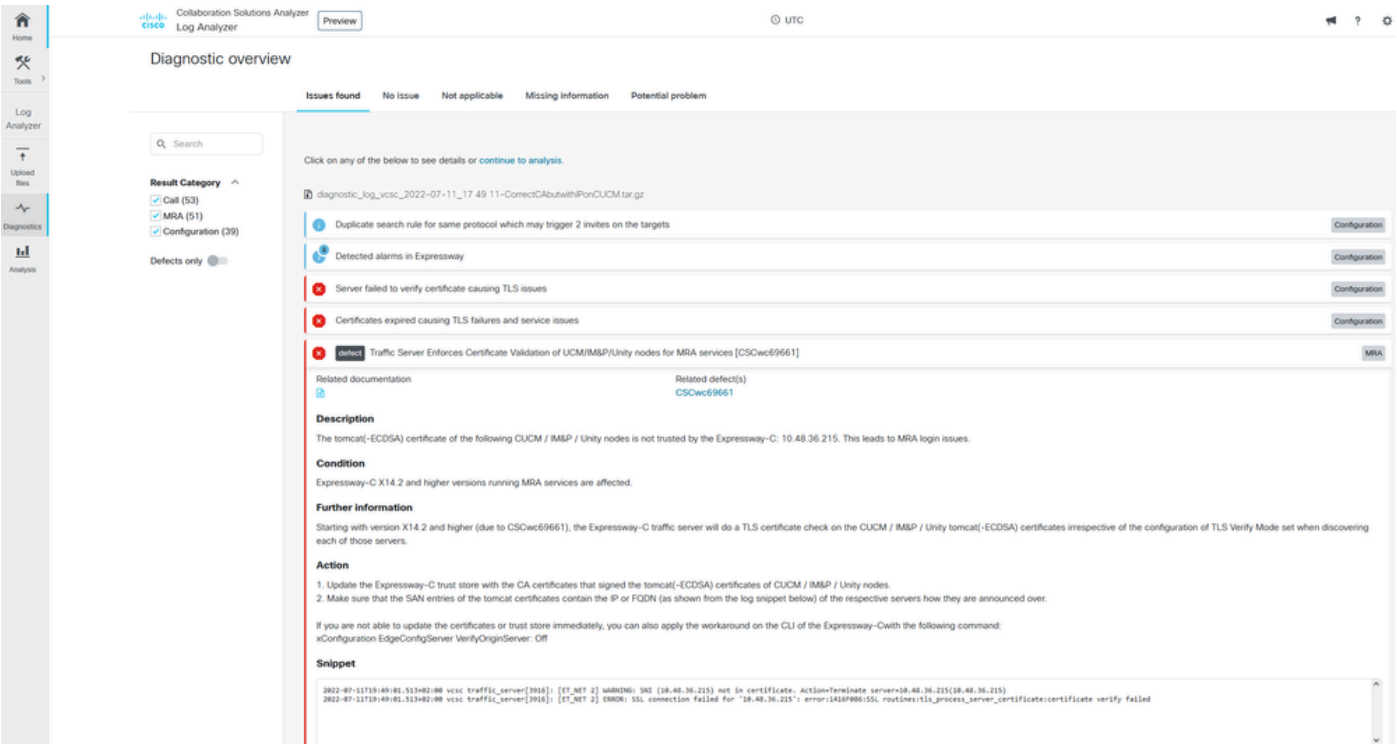
3.等待失败，然后停止Expressway-E和C服务器上的诊断日志记录（如果是集群，请确保分别从集群的每个节点收集日志）

4.上传并分析协作解决方案分析器工具上的日志。

5.如果遇到问题，它会为每个受影响的服务器选取与此更改相关的最新警告和错误行



CA诊断签名



SNI诊断签名

解决方案

长期解决方案是确保TLS验证正常工作。要执行的操作取决于显示的警告消息。

当您观察到“警告：(<server-FQDN-or-IP>)的核心服务器证书验证失败。 Action=Terminate Error=self signed certificate server=cucm.steven.lab(10.48.36.215)depth=x”消息，然后您需要相应地更新Expressway-C服务器上的信任库。使用签署此证书的CA链（深度> 0）或使用Maintenance > Security > Trusted CA Certificate中的自签名证书（深度= 0）。确保在群集中的每台服务器上执行此操作。另一种方法是，通过Expressway-C信任存储上的已知CA对远程证书进行签名。

注意：Expressway不允许您将两个不同（例如自签名）证书上传到Expressway的信任存储中，这些证书与思科漏洞ID CSCwa12905具有相同的公用名称(CN)。为了更正此问题，请转到CA签名的证书或将您的CUCM升级到版本14，您可以在其中为Tomcat和CallManager重复使用相同的（自签名）证书。

当您观察到“警告：SNI(<server-FQDN-or-IP>)not in certificate"消息，则表示此服务器FQDN或IP未包含在提供的证书中。您可以调整证书以包含该信息，也可以修改配置(例如使用CUCM System > Server修改服务器证书中包含的配置)，然后刷新Expressway-C服务器上的配置以将其考虑在内。

相关信息

短期解决方案是应用所记录的解决方法，以回退到X14.2.0之前的先前行为。您可以使用新引入的命令通过Expressway-C服务器节点上的CLI执行此操作：

```
xConfiguration EdgeConfigServer VerifyOriginServer: Off
```

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。