Solucionar problemas de verificação de certificado do servidor de tráfego Expressway

Contents

Introdução

Este documento descreve a mudança de comportamento nas versões do Expressway do X14.2.0 e superior vinculada ao bug da Cisco ID CSCwc6961 ou ao bug da Cisco ID CSCwa25108.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Configuração básica do Expressway
- configuração básica de MRA

Componentes Utilizados

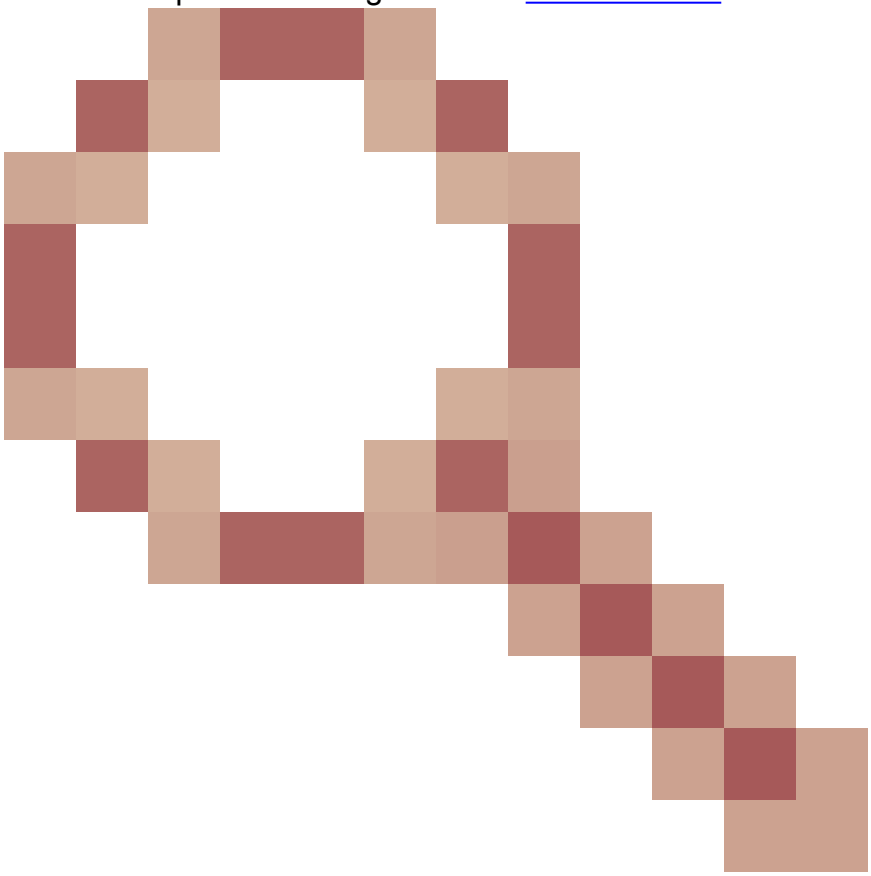
As informações neste documento são baseadas no Cisco Expressway versão X14.2 e superior.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma

configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Com essa mudança de comportamento marcada pela ID de bug da Cisco CSCwc69661



ou ID de bug da Cisco CSCwa25108
, o servidor de tráfego na plataforma Expressway executa a verificação de certificado do Cisco Unified Communication Manager (CUCM), do Cisco Unified Instant Messaging & Presence (IM&P) e dos nós de servidor Unity para os serviços de acesso remoto e móvel (MRA). Essa alteração pode levar a falhas de login de MRA após uma atualização na plataforma Expressway.

O protocolo HTTPS (Hypertext Transfer Protocol Secure) é um protocolo de comunicação seguro que usa o TLS (Transport Layer Security) para criptografar a comunicação. Ele cria esse canal seguro com o uso de um certificado TLS que é trocado no handshake TLS. Isso tem duas finalidades: autenticação (para saber a quem o participante remoto está conectado) e privacidade (a criptografia). A autenticação protege contra ataques de intermediários e a privacidade impede que os invasores interceptem e interfiram na comunicação.

A verificação de TLS (certificado) é realizada aos olhos da autenticação e permite ter certeza de que você se conectou à parte remota certa. A verificação consiste em dois elementos individuais:

1. Cadeia da Autoridade de Certificação Confiável (AC)

2. Nome Alternativo do Assunto (SAN) ou Nome Comum (CN)

Cadeia de CA confiável

Para que o Expressway-C confie no certificado que o CUCM / IM&P / Unity envia, ele precisa ser capaz de estabelecer um link desse certificado para uma Autoridade de Certificação (CA) de nível superior (raiz) em que ele confia. Tal link, uma hierarquia de certificados que vincula um certificado de entidades a um certificado de CA raiz, é chamado de cadeia de confiança. Para poder verificar essa cadeia de confiança, cada certificado contém dois campos: Emitente (ou Emitido por) e Assunto (ou Emitido para).

Os certificados de servidor, como o que o CUCM envia ao Expressway-C, têm no campo Assunto normalmente seu FQDN (Fully Qualified Domain Name, nome de domínio totalmente qualificado) no 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
```

Exemplo de um certificado de servidor para CUCM cucm.vngtp.lab. Ele tem o FQDN no atributo CN do campo Assunto junto com outros atributos como País (C), Estado (ST), Local (L), ... Você também pode ver que o certificado do servidor é distribuído (emitido) por uma CA chamada vngtp-ATIVE-DIR-CA.

As CAs de nível superior (CAs raiz) também podem emitir um certificado para se identificarem. Em tal certificado CA raiz, você verá que o Emissor e o Assunto têm o mesmo valor:

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

É um certificado passado por uma CA raiz para se identificar.

Em uma situação típica, as CAs raiz não emitem diretamente certificados de servidor. Em vez disso, emitem certificados para outras autoridades de certificação. Essas outras CAs são então chamadas de CAs intermediárias. As autoridades de certificação intermediárias podem, por sua vez, emitir diretamente certificados de servidor ou certificados para outras autoridades de certificação intermediárias. Você pode ter uma situação em que um certificado de servidor é emitido pela CA 1 intermediária, que, por sua vez, recebe um certificado da CA 2 intermediária e assim por diante. Até que finalmente, a CA intermediária obtém seu certificado diretamente da CA raiz:

```
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
```

Agora, para que o Expressway-C confie no certificado de servidor que o CUCM envia, ele precisa ser capaz de criar a cadeia de confiança a partir desse certificado de servidor até um certificado de CA raiz. Para que isso aconteça, você precisa carregar o certificado de CA raiz e também todos os certificados de CA intermediários (se houver, o que não é o caso se a CA raiz teria emitido diretamente o certificado de servidor do CUCM) no armazenamento confiável do Expressway-C.

Observação: embora os campos Emissor e Assunto sejam fáceis de criar a cadeia de Confiança de forma legível, o CUCM não usa esses campos no certificado. Em vez disso, ele usa os campos X509v3 Authority Key Identifier e X509v3 Subject Key Identifier para criar a cadeia de confiança. Essas chaves contêm identificadores para os certificados que são mais precisos do que para usar os campos Assunto/Emissor: pode haver 2 certificados com os mesmos campos Assunto/Emissor, mas um deles expirou e o outro ainda é válido. Ambos teriam um identificador de chave de assunto X509v3 diferente para que o CUCM ainda possa determinar a cadeia de confiança correta.

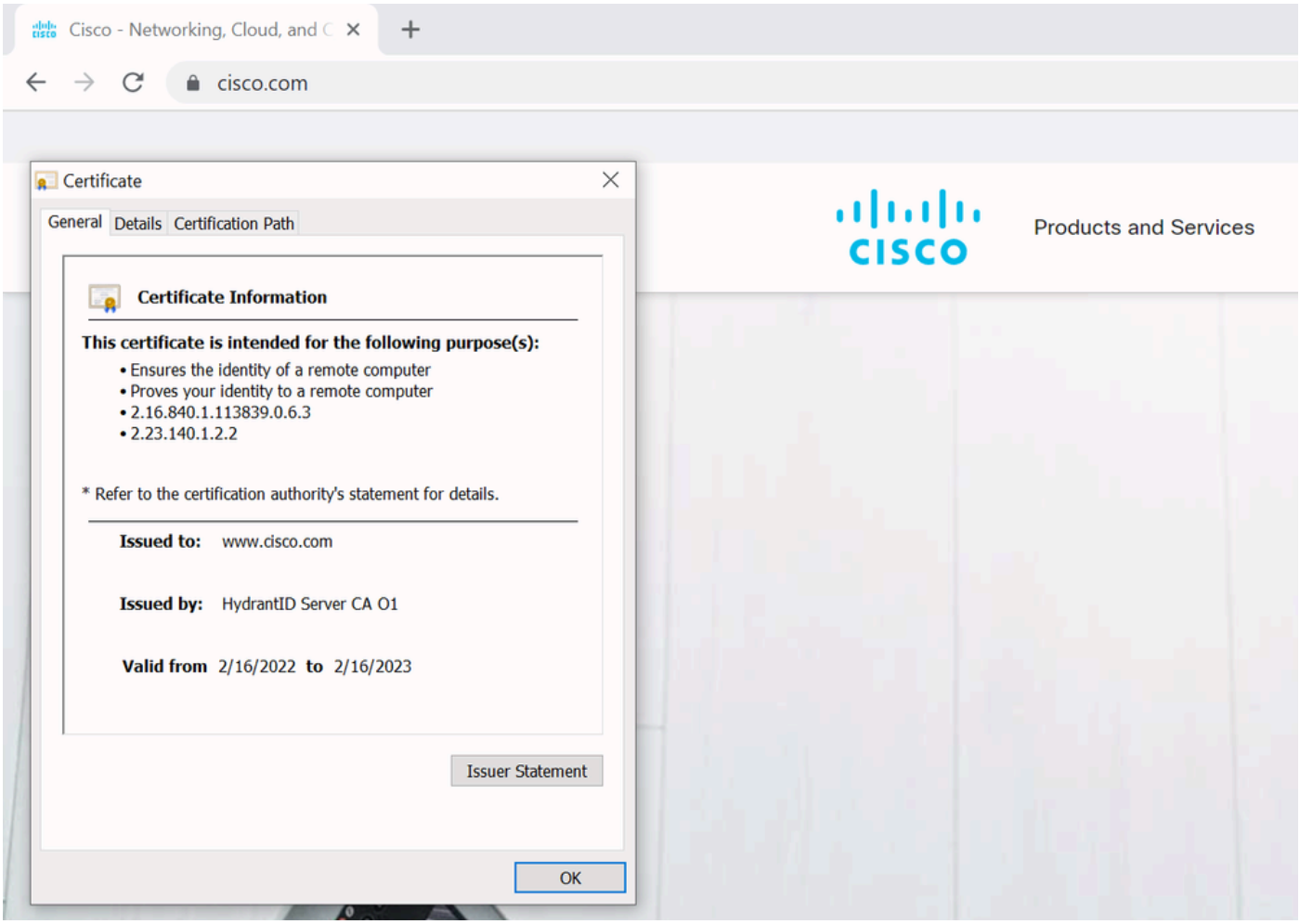
Esse não é o caso do Expressway, embora conforme o bug da Cisco ID CSCwa12905 e não é possível carregar dois certificados diferentes (autoassinados, por exemplo) no armazenamento confiável do Expressway que têm o mesmo nome comum (CN). A maneira de corrigir isso é usar certificados assinados pela CA ou usar nomes comuns diferentes para ele ou ver se ele usa sempre o mesmo certificado (possivelmente por meio do recurso de certificado de reutilização no CUCM 14).

Verificação de SAN ou CN

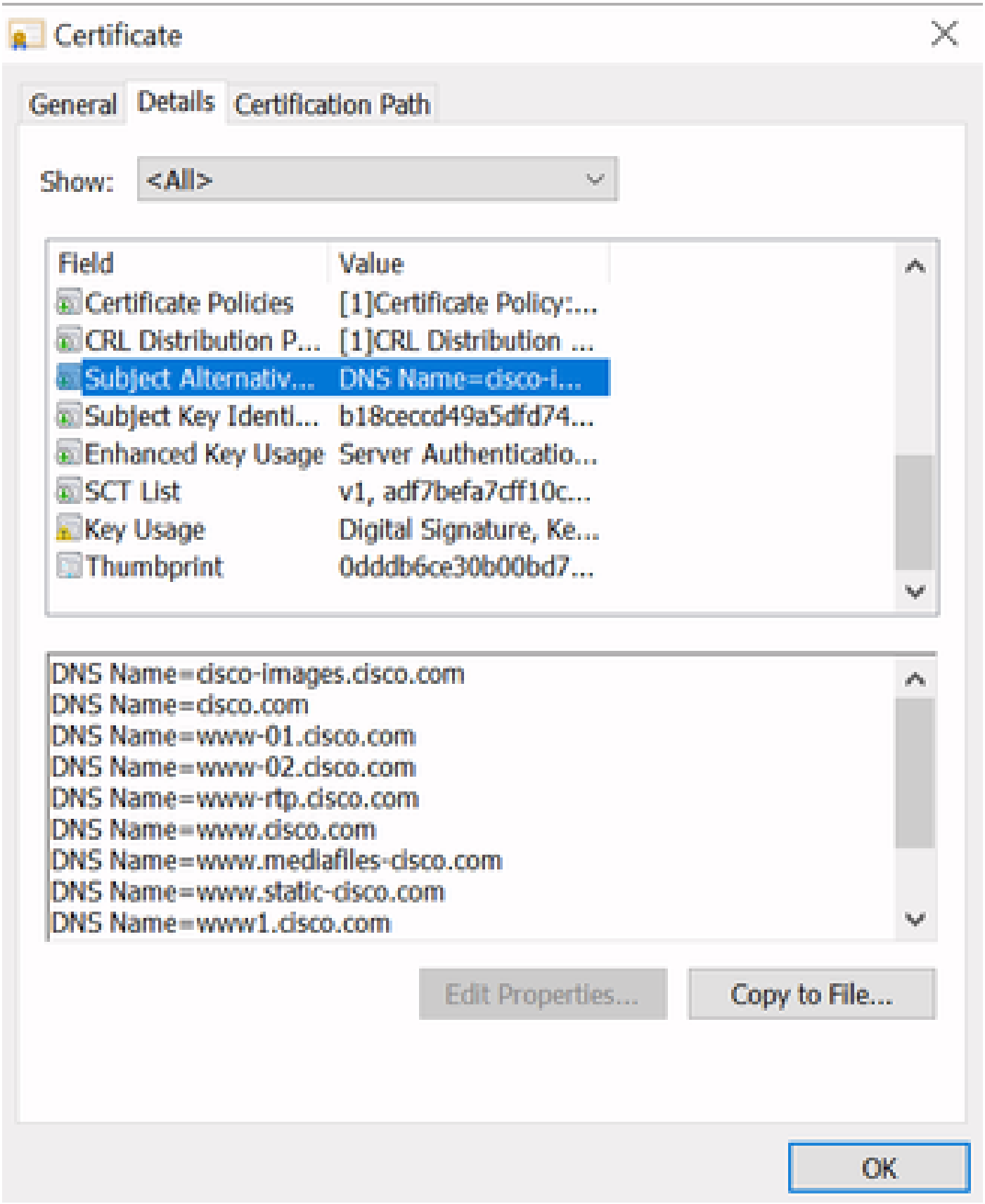
A Etapa 1 faz check-out do repositório de confiança; no entanto, qualquer pessoa que tiver um certificado assinado por uma CA no repositório de confiança será válida. É evidente que isto não é suficiente. Portanto, há uma verificação adicional que valida se o servidor ao qual você se conecta especificamente é realmente o correto. Ele faz isso com base no endereço para o qual o pedido foi feito.

O mesmo tipo de operação acontece em seu navegador, então você pode ver isso em um exemplo. Se você navegar até Cisco.com, verá um ícone de cadeado ao lado do URL inserido e isso significa que a conexão é confiável. Isso é baseado na cadeia de confiança da CA (da primeira seção) e na verificação SAN ou CN. Se você abrir o certificado (através do navegador

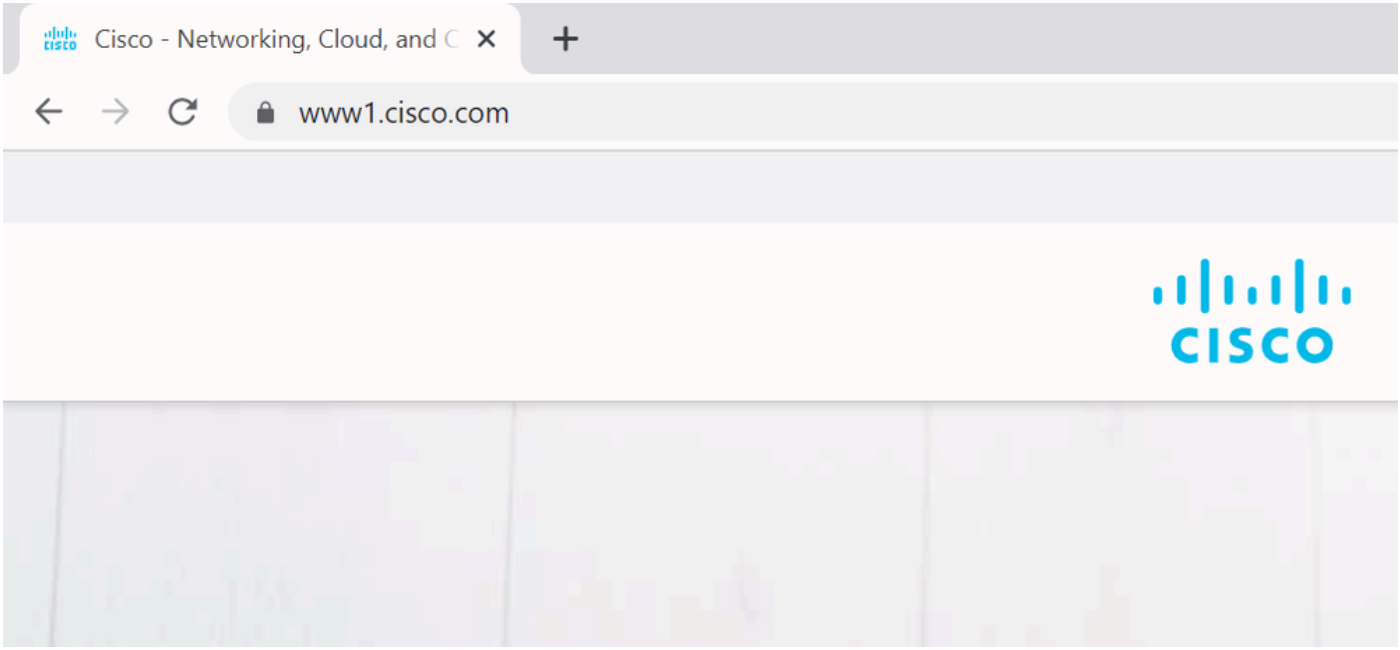
clicando no ícone de cadeado), verá que o Nome comum (exibido em Emitido para: é definido como Cisco.com e isso corresponde exatamente ao endereço ao qual você deseja se conectar. Dessa forma, você pode ter certeza de se conectar ao servidor correto (porque você confia na CA que assinou o certificado e que executa a verificação antes que ele distribua o certificado).



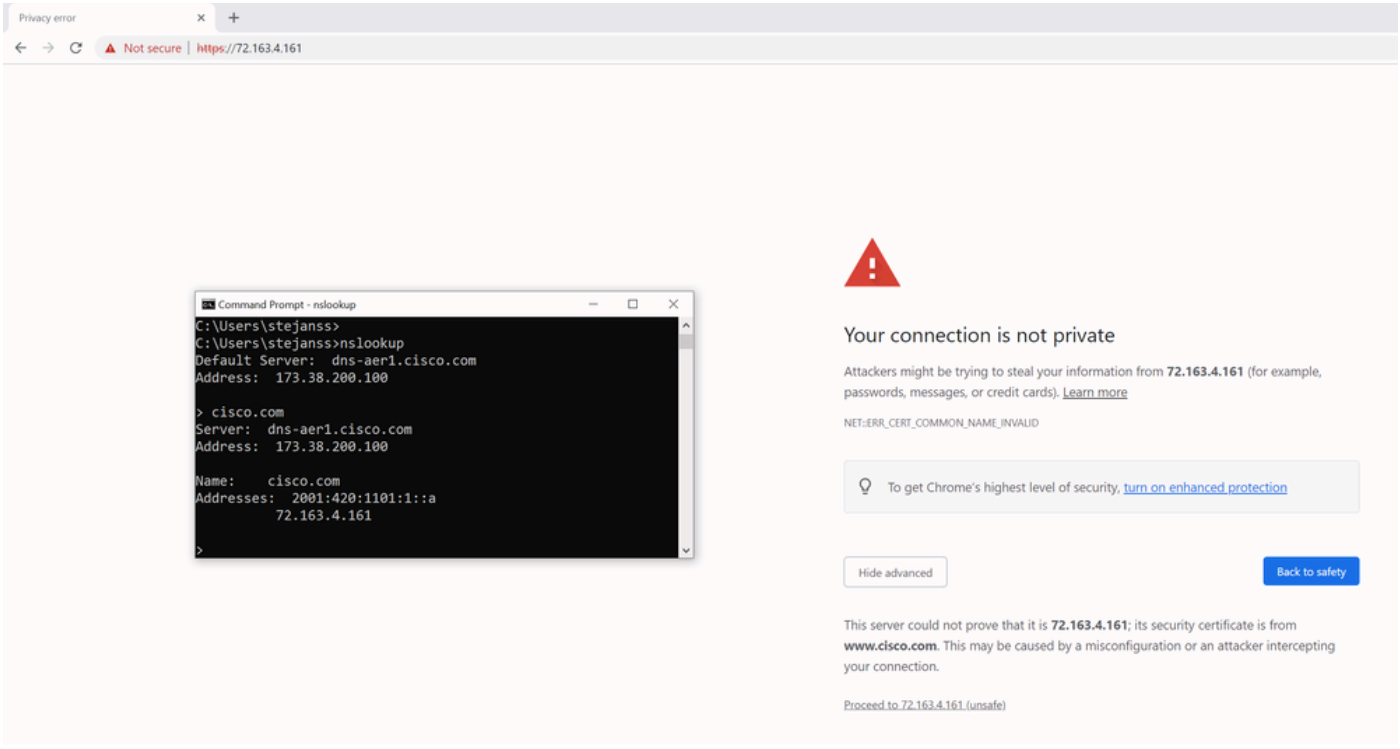
Ao examinar os detalhes do certificado e, em particular, as entradas SAN, você verá que o mesmo se repete, assim como alguns outros FQDNs:



Isso significa que, quando você solicita a conexão com Cisco.com, por exemplo, ela também aparece como uma conexão segura porque está contida nas entradas SAN.



No entanto, quando você não navega para Cisco.com, mas diretamente para o endereço IP (endereço web numerado), ele não mostra uma conexão segura porque não confia no CA que a assinou. O certificado apresentado não contém o endereço (72.163.4.161) que você usou para se conectar ao servidor.



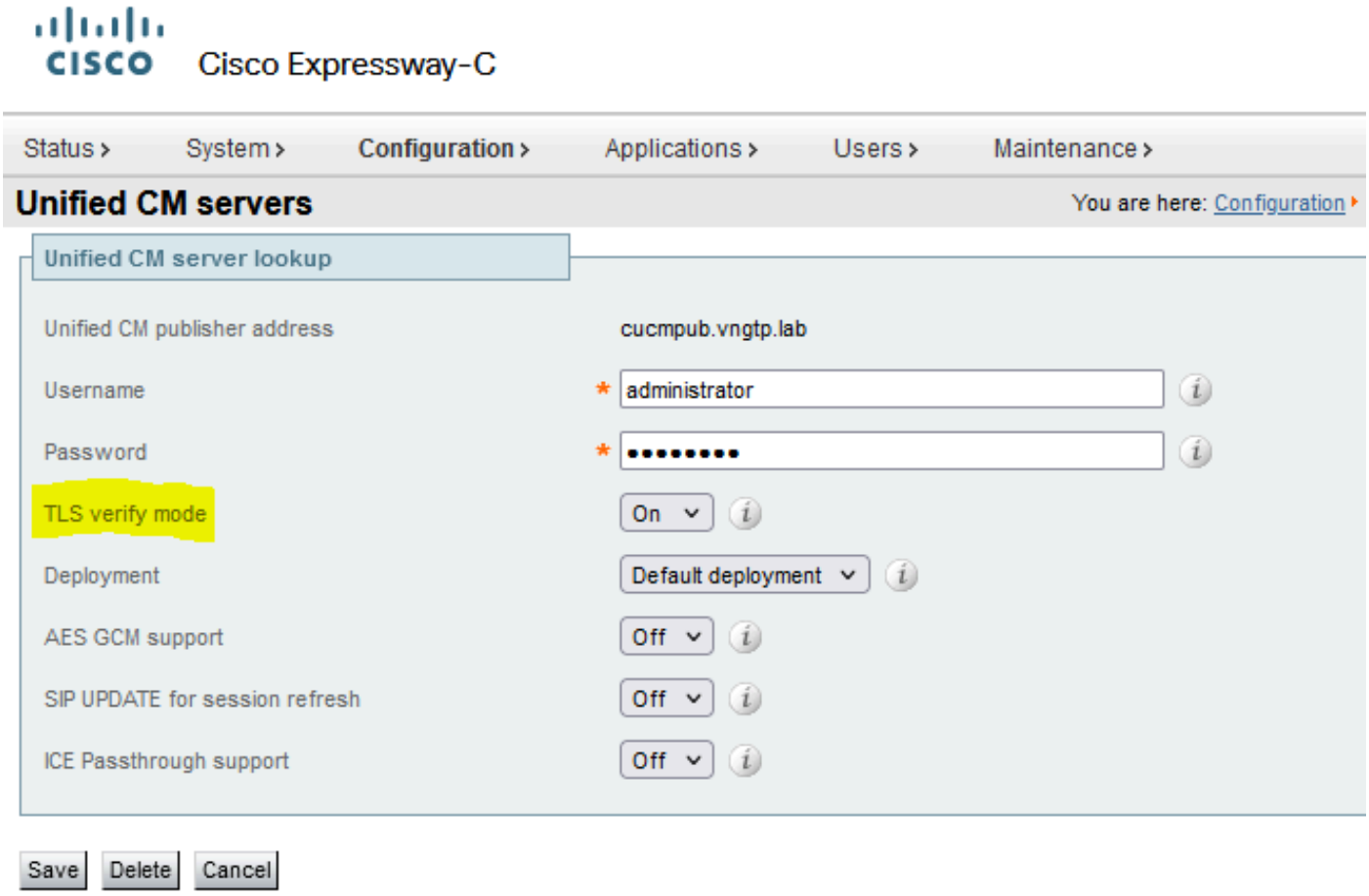
No navegador, você pode ignorar isso. No entanto, é uma configuração que você pode ativar em conexões TLS que um desvio não é permitido. Portanto, é importante que seus certificados contenham os nomes CN ou SAN corretos que a parte remota planeja usar para se conectar a eles.

Mudança de comportamento

Os serviços MRA dependem muito de várias conexões HTTPS nos Expressways em direção aos servidores CUCM / IM&P / Unity para se autenticar corretamente e coletar as informações certas específicas para o cliente que faz login. Essa comunicação geralmente acontece nas portas 8443 e 6972.

Versões anteriores a X14.2.0

Em versões anteriores a X14.2.0, o servidor de tráfego no Expressway-C que trata as conexões HTTPS seguras que não verificam o certificado apresentado pela extremidade remota. Isso pode levar a ataques de intermediários. Na configuração MRA, há uma opção para verificação de certificado TLS pela configuração do Modo de verificação TLS'para On quando você adicionaria servidores CUCM / IM&P / Unity em Configuration > Unified Communications > Unified CM servers / IM and Presence Service nodes / Unity Connection servers. A opção de configuração e a caixa de informações relevantes são mostradas como exemplo, indicando que ela verifica o FQDN ou o IP na SAN, bem como a validade do certificado e se ele está assinado por uma CA confiável.



Essa verificação de certificado TLS é feita apenas na descoberta dos servidores CUCM / IM&P / Unity e não no momento do login de MRA quando os vários servidores são consultados. Uma primeira desvantagem dessa configuração é que ela apenas verifica o endereço do publicador adicionado. Ele não valida se o certificado nos nós do assinante foi configurado corretamente, pois recupera as informações do nó do assinante (FQDN ou IP) do banco de dados do nó do publicador. Uma segunda desvantagem dessa configuração também é que o que é anunciado

aos clientes MRA como as informações de conexão pode ser diferente do endereço do publicador que foi colocado na configuração Expressway-C. Por exemplo, no CUCM, em System > Server, você pode anunciar o servidor com um endereço IP (10.48.36.215, por exemplo) e isso é usado pelos clientes MRA (através da conexão Expressway com proxy); no entanto, você pode adicionar o CUCM no Expressway-C com o FQDN de cucm.steven.lab. Suponha que o certificado tomcat do CUCM contenha cucm.steven.lab como entrada de SAN, mas não o endereço IP, então a descoberta com o modo de verificação TLS definido como Ativado é bem-sucedida, mas as comunicações reais dos clientes MRA podem ter como destino um FQDN ou IP diferente e, portanto, falhar na verificação TLS.

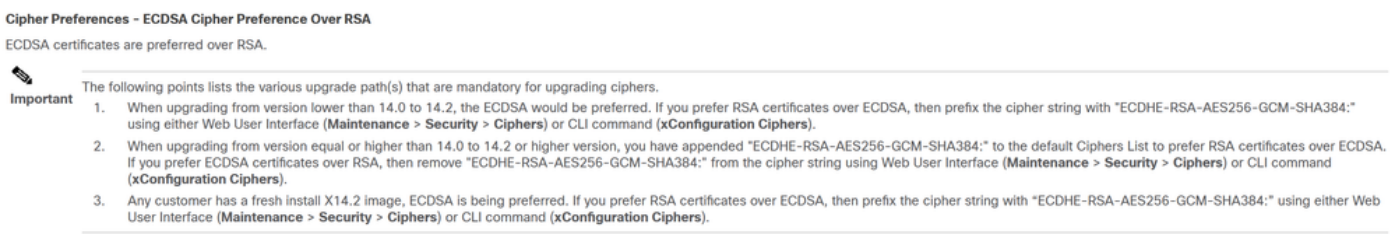
Versões do X14.2.0 e superior

A partir da versão X14.2.0, o servidor Expressway executa a verificação de certificado TLS para cada solicitação HTTPS feita através do servidor de tráfego. Isso significa que ele também executa isso quando o Modo de verificação TLS está definido como Desligado durante a descoberta dos nós CUCM / IM&P / Unity. Quando a verificação não é bem-sucedida, o handshake TLS não é concluído e a solicitação falha, o que pode levar à perda de funcionalidade, como redundância, problemas de failover ou falhas de login completas, por exemplo. Além disso, com o Modo de verificação TLS definido como Ativado, ele não garante que todas as conexões funcionem bem, conforme abordado no exemplo mais adiante.

Os certificados exatos que o Expressway verifica em relação aos nós CUCM / IM&P / Unity são como mostrado na seção do guia MRA.

Além do padrão na verificação TLS, há também uma alteração introduzida no X14.2 que pode anunciar uma ordem de preferência diferente para a lista de cifras, que depende do seu caminho de atualização. Isso pode causar conexões TLS inesperadas após uma atualização de software, pois pode acontecer que, antes da atualização, ele tenha solicitado o certificado Cisco Tomcat ou Cisco CallManager do CUCM (ou qualquer outro produto que tenha um certificado separado para o algoritmo ECDSA), mas depois da atualização, ele solicite a variante ECDSA (que é a variante de cifra mais segura na verdade do que a RSA). Os certificados Cisco Tomcat-ECDSA ou Cisco CallManager-ECDSA podem ser assinados por uma CA diferente ou apenas certificados ainda autoassinados (o padrão).

Essa alteração de ordem de preferência de codificação nem sempre é relevante para você, pois depende do caminho de atualização, conforme mostrado nas notas de versão do Expressway X14.2.1. Resumindo, você pode ver em Manutenção > Segurança > Cifras para cada uma das listas de cifras se ela contém ou não o prefixo ECDHE-RSA-AES256-GCM-SHA384. Caso contrário, ele prefere a cifra ECDSA mais recente em vez da cifra RSA. Se tiver, você terá o comportamento anterior com RSA que tem a preferência mais alta.



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**).

Há duas maneiras de a verificação de TLS falhar neste cenário, que serão abordadas em detalhes posteriormente:

1. A autoridade de certificação que assinou o certificado remoto não é confiável.

a. Certificado autoassinado

b. Certificado assinado por uma autoridade de certificação desconhecida

2. O Endereço de Conexão (FQDN ou IP) não consta do certificado.

Solucionar problemas de cenários

Os próximos cenários mostram um cenário semelhante em um ambiente de laboratório onde o login de MRA falhou após uma atualização do Expressway de X14.0.7 para X14.2. Eles compartilham semelhanças nos logs, no entanto, a resolução é diferente. Os logs são coletados pelo log de diagnóstico (de Manutenção > Diagnóstico > Log de diagnóstico) que foi iniciado antes do log de MRA e interrompido depois que o log de MRA falhou. Nenhum log de depuração adicional foi habilitado para ele.

1. A AC que Assinou o Certificado Remoto não é Confiável

O certificado remoto pode ser assinado por uma CA que não esteja incluída no armazenamento confiável do Expressway-C ou pode ser um certificado autoassinado (em essência, uma CA também) que não é adicionado no armazenamento confiável do servidor Expressway-C.

No exemplo aqui, você pode observar que as solicitações que vão para o CUCM (10.48.36.215 - cucm.steven.lab) são tratadas corretamente na porta 8443 (resposta 200 OK), mas ela gera um erro (resposta 502) na porta 6972 para a conexão 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="netw

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="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

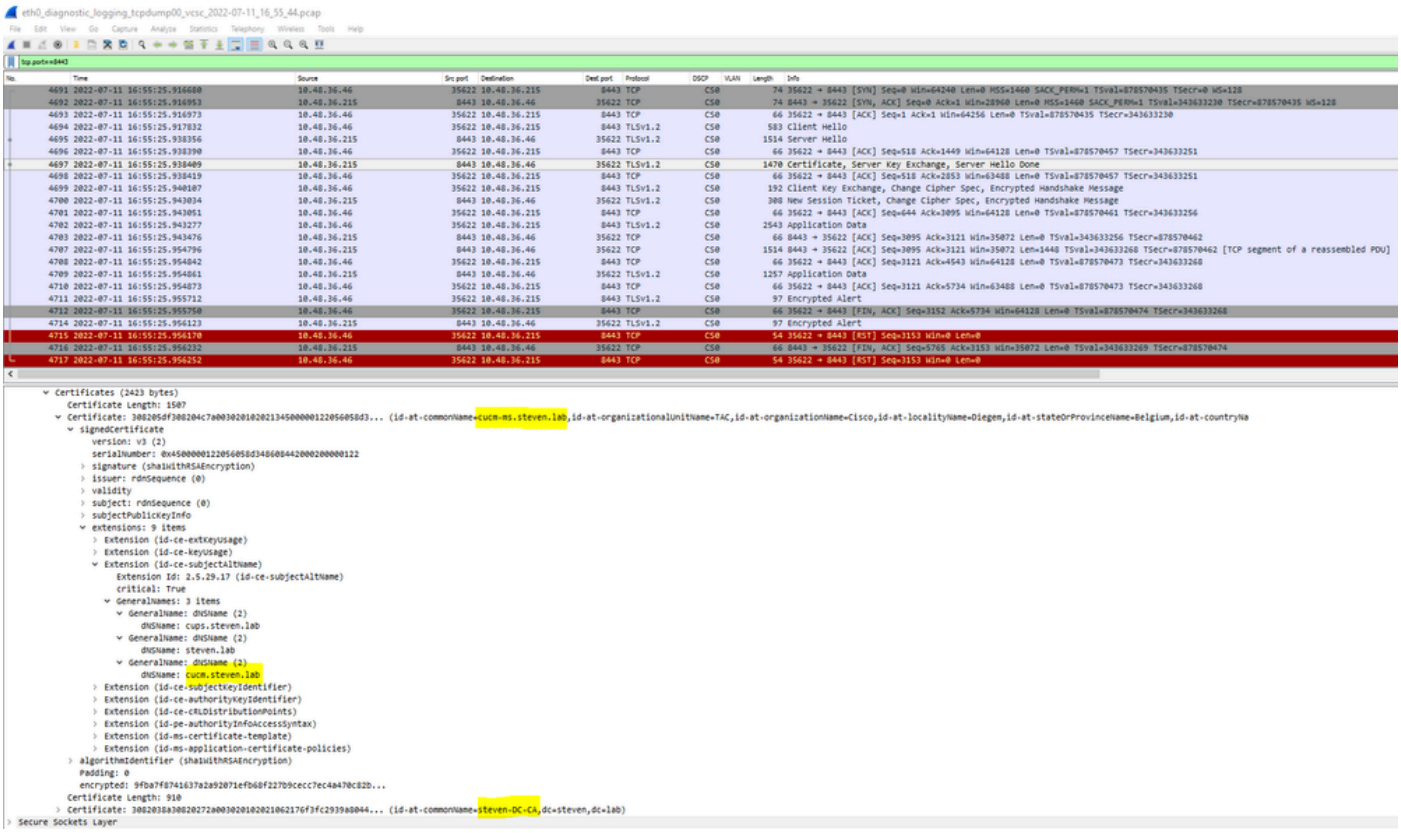
2022-07-11T18:55:26.024+02:00 vcsc traffic_server[18242]: UTCTime="2022-07-11 16:55:26,024" Module="net

502 connect failed

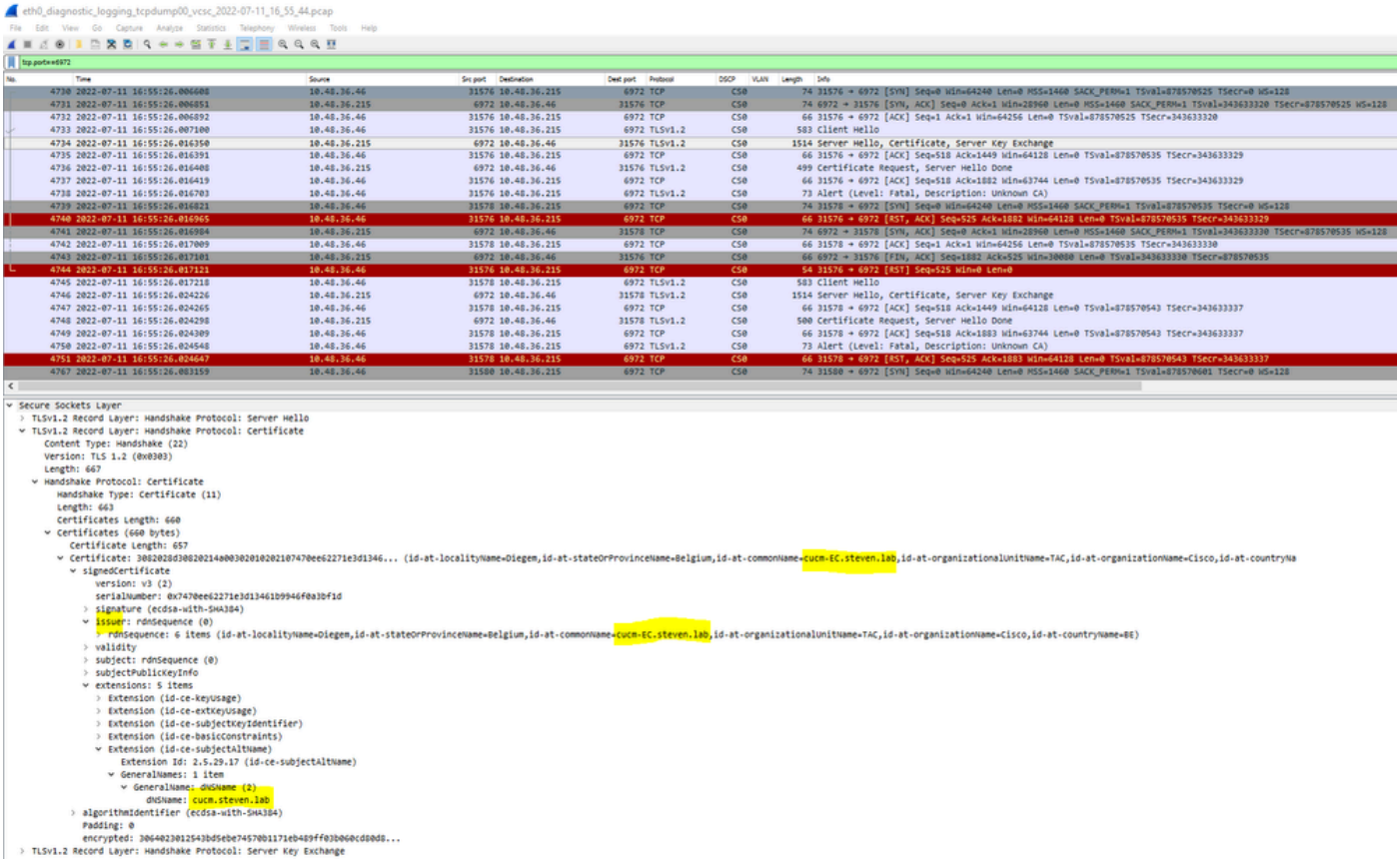
"

O erro de, verificação de certificado falhou, indica o fato de que o Expressway-C não pôde validar o handshake TLS. A razão para isso é mostrada na linha de aviso, pois indica um certificado autoassinado. Se a profundidade for mostrada como 0, é um certificado autoassinado. Quando a profundidade é maior que 0, isso significa que ela tem uma cadeia de certificados e, portanto, é assinada por uma CA desconhecida (da perspectiva do Expressway-C).

Ao examinar o arquivo pcap que foi coletado nos carimbos de data e hora mencionados nos logs de texto, você pode ver que o CUCM apresenta o certificado com CN como cucm-ms.steven.lab (e cucm.steven.lab como SAN) assinado por steven-DC-CA para o Expressway-C na porta 8443.

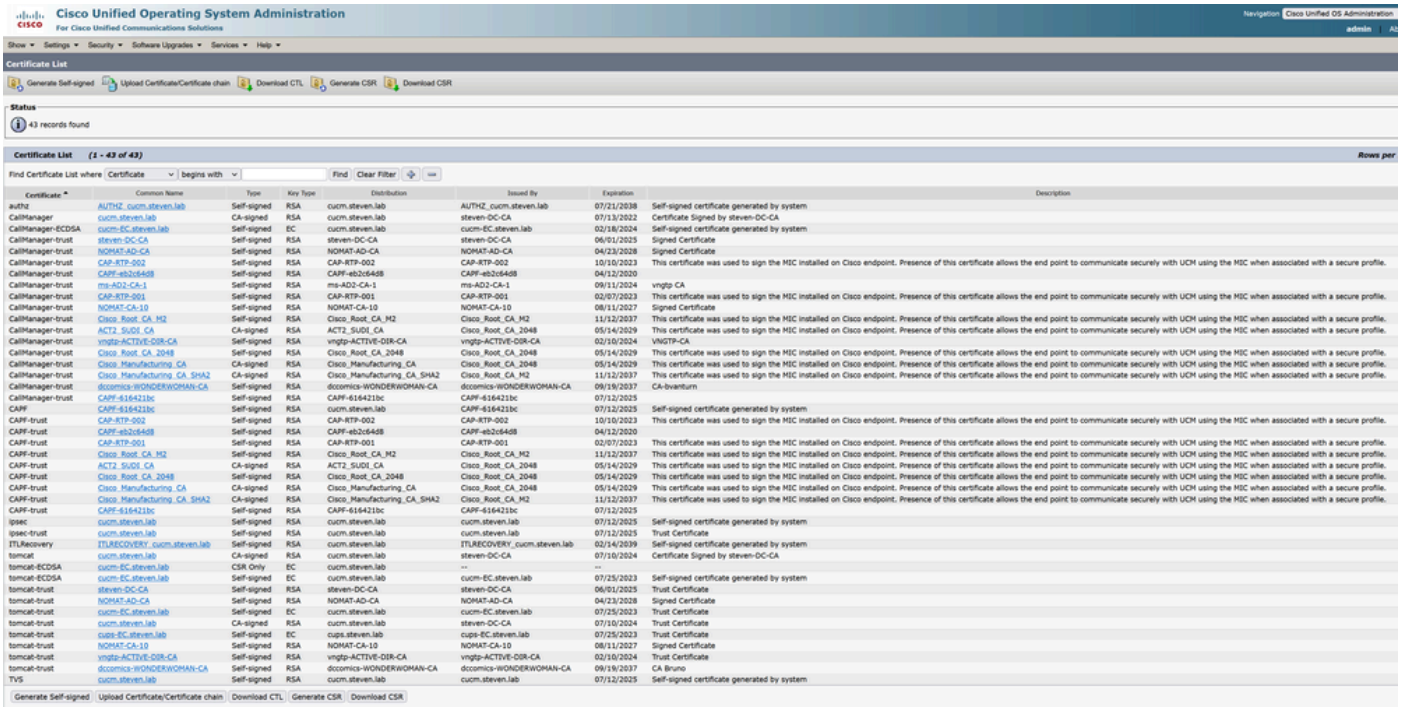


Mas, ao inspecionar o certificado apresentado na porta 6972, você pode ver que ele é um certificado autoassinado (o próprio Emissor) com CN configurado como cucm-EC.steven.lab. A extensão -EC dá a indicação de que este é o certificado ECDSA configurado no CUCM.



No CUCM no Cisco Unified OS Administration, você pode ver os certificados em vigor em

Segurança > Gerenciamento de certificado como mostrado, por exemplo, aqui. Ele mostra um certificado diferente para tomcat e tomcat-ECDSA onde o tomcat é assinado por CA (e confiável pelo Expressway-C) enquanto o certificado tomcat-ECDSA é autoassinado e não confiável pelo Expressway-C aqui.



2. O Endereço de Conexão (FQDN ou IP) não consta do Certificado

Além do armazenamento confiável, o servidor de tráfego também verifica o endereço de conexão para o qual o cliente MRA faz a solicitação. Por exemplo, quando você tiver configurado no CUCM em System > Server seu CUCM com o endereço IP (10.48.36.215), o Expressway-C anunciará isso como tal ao cliente e as solicitações subsequentes do cliente (com proxy através do Expressway-C) serão direcionadas a esse endereço.

Quando esse endereço de conexão específico não está contido no certificado do servidor, a verificação TLS também falha e um erro 502 é lançado, resultando em falha de login de MRA, por exemplo.

<#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
```

Onde c3RldmVuLmxhYi9odHRwcy8xMC40OC4zNi4yMTUvODQ0Mw traduz (base64) para steven.lab/https/10.48.36.215/8443, o que mostra que ele deve fazer a conexão em direção a 10.48.36.215 como o endereço de conexão, em vez de para cucm.steven.lab. Como mostrado nas capturas de pacote, o certificado tomcat CUCM não contém o endereço IP na SAN e, portanto, o erro é lançado.

Como validá-la facilmente

É possível validar se você se depara com essa mudança de comportamento facilmente com as próximas etapas:

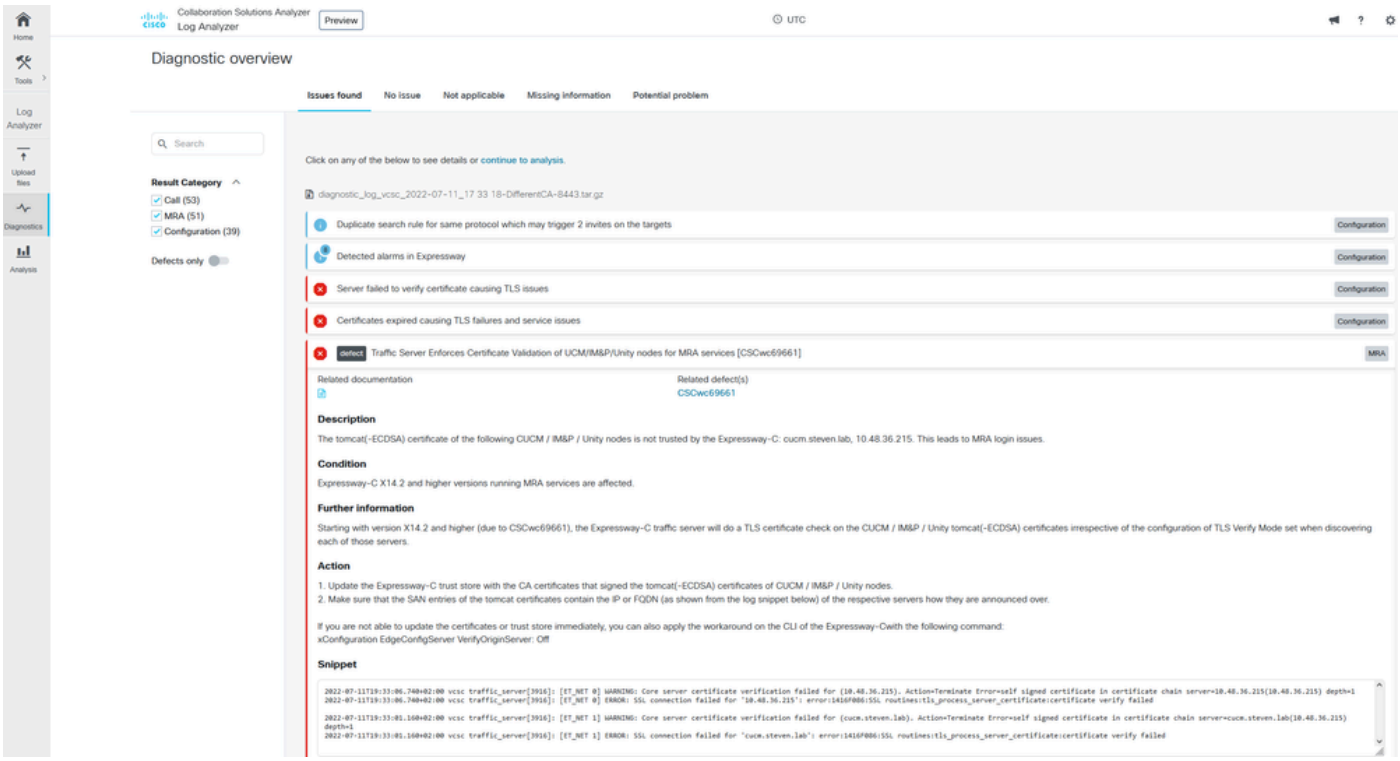
1. Inicie o log de diagnóstico no(s) servidor(es) Expressway-E e C (idealmente com TCPDumps ativados) de Manutenção > Diagnóstico > Log de Diagnóstico (no caso de um cluster, é suficiente iniciá-lo a partir do nó primário)

2. Tente um login de MRA ou teste a funcionalidade interrompida após a atualização

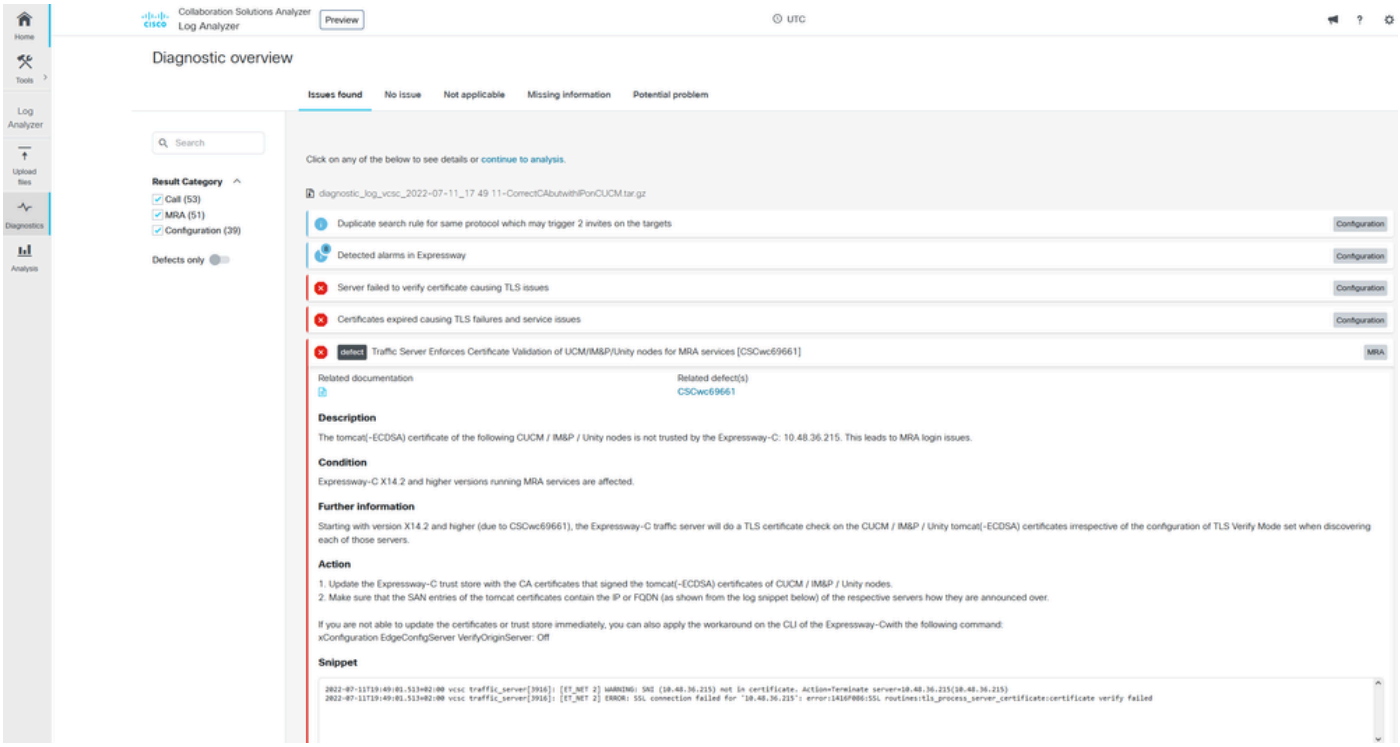
3. Aguarde até que haja falha e pare o log de diagnóstico no(s) servidor(es) Expressway-E e C (no caso de um cluster, certifique-se de coletar os logs de cada nó individual do cluster individualmente)

4. Carregue e analise os logs na ferramenta Collaboration Solution Analyzer.

5. Se você encontrar o problema, ele selecionará as linhas de aviso e de erro mais recentes relacionadas a essa alteração para cada um dos servidores afetados



assinatura de diagnóstico de CA



Assinatura de diagnóstico SNI

Solução

A solução a longo prazo é garantir que a verificação TLS funcione bem. A ação a ser executada depende da mensagem de aviso exibida.

Ao observar a mensagem "AVISO: Falha na verificação do certificado do servidor principal para

(<server-FQDN-or-IP>). Action=Terminate Error=self signed certificate server=cucm.steven.lab(10.48.36.215) depth=x", então você precisa atualizar o armazenamento confiável nos servidores Expressway-C adequadamente. Com a cadeia de CAs que assinou este certificado (profundidade > 0) ou com o certificado autoassinado (profundidade = 0) em Manutenção > Segurança > Certificado de CA Confiável. Certifique-se de executar esta ação em todos os servidores do cluster. Outra opção seria assinar o certificado remoto por uma CA conhecida no repositório de confiança do Expressway-C.

Observação: o Expressway não permite que você carregue dois certificados diferentes (autoassinados, por exemplo) no armazenamento confiável do Expressway que têm o mesmo Nome Comum (CN) conforme a ID de bug da Cisco CSCwa12905. Para corrigir isso, vá para certificados assinados pela CA ou atualize seu CUCM para a versão 14, onde você pode reutilizar o mesmo certificado (autoassinado) para Tomcat e CallManager.

Ao observar a mensagem "AVISO: Mensagem SNI (<server-FQDN-or-IP>) not in certificate", indica que esse FQDN ou IP do servidor não está contido no certificado que foi apresentado. Você pode adaptar o certificado para incluir essas informações ou pode modificar a configuração (como com Sistema CUCM > Servidor para algo que esteja contido no certificado do servidor) e, em seguida, atualizar a configuração no servidor Expressway-C para que ela seja levada em conta.

Informações Relacionadas

A solução de curto prazo é aplicar a solução alternativa conforme documentado para fallback para o comportamento anterior antes de X14.2.0. Você pode executar isso através da CLI nos nós do servidor Expressway-C com o comando recém-introduzido:

```
xConfiguration EdgeConfigServer VerifyOriginServer: Off
```

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.