Risoluzione dei problemi relativi alla verifica dei certificati del server Expressway Traffic

Sommario

Introduzione

Prerequisiti

- Requisiti
- Componenti usati

Premesse

- Catena CA attendibile
- Controllo SAN o CN

Modifica del comportamento

- Versioni inferiori a X14.2.0
- Versioni di X14.2.0 e successive

Risoluzione dei problemi

- 1. La CA che ha firmato il certificato remoto non è attendibile
- 2. L'indirizzo di connessione (FQDN o IP) non è contenuto nel certificato

Come convalidarlo in modo semplice

Soluzione

Informazioni correlate

Introduzione

Questo documento descrive la modifica del comportamento nelle versioni Expressway di X14.2.0 e versioni successive collegata all'ID bug Cisco CSCwc69661 o all'ID bug Cisco CSCwa25108.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Configurazione di base di Expressway
- Configurazione di base MRA

Componenti usati

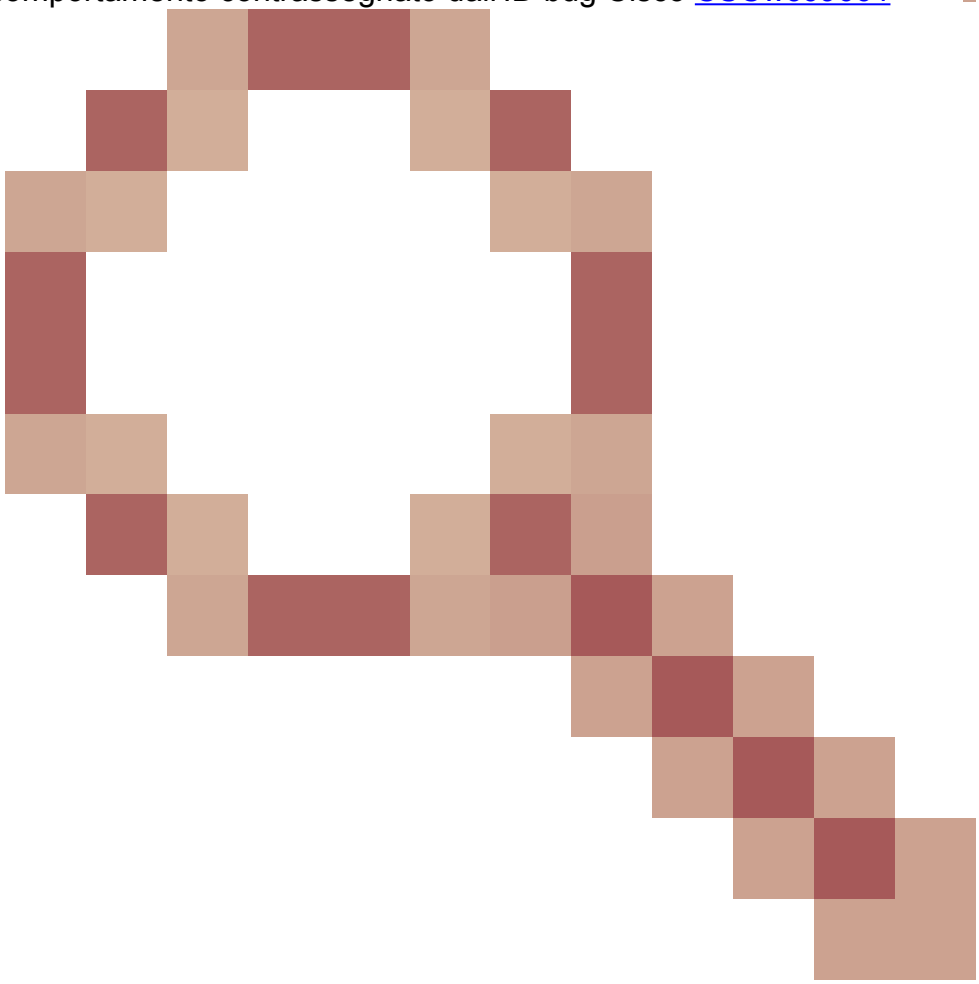
Il riferimento delle informazioni contenute in questo documento è Cisco Expressway versione X14.2 e successive.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico

ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Con questo cambiamento di comportamento contrassegnato dall'ID bug Cisco CSCwc69661



o ID bug Cisco CSCwa25108
, il server di traffico sulla piattaforma Expressway esegue la verifica dei certificati dei nodi server Cisco Unified Communications Manager (CUCM), Cisco Unified Instant Messaging & Presence (IM&P) e Unity per i servizi Mobile e Remote Access (MRA). Questa modifica può causare errori di accesso MRA dopo un aggiornamento della piattaforma Expressway.

HTTPS (Hypertext Transfer Protocol Secure) è un protocollo di comunicazione sicuro che utilizza TLS (Transport Layer Security) per crittografare la comunicazione. Questo canale sicuro viene creato mediante l'utilizzo di un certificato TLS scambiato nell'handshake TLS. Questo serve a due scopi: l'autenticazione (per sapere a chi è la parte remota a cui ci si connette) e la privacy (la crittografia). L'autenticazione protegge dagli attacchi man-in-the-middle e la privacy impedisce agli aggressori di intercettare e manomettere la comunicazione.

La verifica TLS (Certificato) viene eseguita con l'obiettivo dell'autenticazione e consente di essere certi di aver effettuato la connessione alla parte remota corretta. La verifica è costituita da due elementi distinti:

1. Catena di Autorità di certificazione (CA) attendibili

2. Nome alternativo del soggetto (SAN) o nome comune (CN)

Catena CA attendibile

Affinché Expressway-C consideri attendibile il certificato inviato da CUCM / IM&P / Unity, è necessario che sia in grado di stabilire un collegamento da tale certificato a un'Autorità di certificazione (CA) di livello superiore (principale) considerata attendibile. Tale collegamento, ovvero una gerarchia di certificati che collega un certificato di entità a un certificato CA radice, è denominato catena di attendibilità. Per verificare tale catena di attendibilità, ogni certificato contiene due campi: Emittente (o emesso da) e Soggetto (o emesso a).

I certificati server, ad esempio quello inviato da CUCM a Expressway-C, hanno in genere nel campo Oggetto il nome di dominio completo (FQDN, Fully Qualified Domain Name) della 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
```

Esempio di certificato server per CUCM.vngtp.lab. Il nome di dominio completo (FQDN) è presente nell'attributo CN del campo Oggetto insieme ad altri attributi, quali Paese (C), Stato (ST), Posizione (L), ... È inoltre possibile verificare che il certificato del server viene rilasciato da una CA denominata vngtp-ACTIVE-DIR-CA.

Le CA di livello superiore (CA radice) possono inoltre rilasciare un certificato per identificarsi. In un certificato CA radice di questo tipo, il valore di Autorità di certificazione (Issuer) e Oggetto (Subject) è lo stesso:

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

Si tratta di un certificato rilasciato da una CA radice per identificarsi.

In una situazione tipica, le CA radice non rilasciano direttamente certificati server. Al contrario, emettono certificati per altre CA. Tali altre CA vengono quindi definite CA intermedie. Le CA intermedie possono a loro volta emettere direttamente certificati server o certificati per altre CA intermedie. È possibile che un certificato server venga rilasciato dalla CA intermedia 1, che a sua volta ottiene un certificato dalla CA intermedia 2 e così via. Fino a quando, infine, la CA intermedia ottiene il proprio certificato direttamente dalla CA radice:

```
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
```

Ora, affinché Expressway-C consideri attendibile il certificato server inviato da CUCM, è necessario che sia in grado di creare la catena di attendibilità da tale certificato server fino a ottenere un certificato CA radice. A tale scopo, è necessario caricare il certificato CA radice e tutti i certificati CA intermedi (se presenti, il che non è il caso se la CA radice avrebbe rilasciato direttamente il certificato server di CUCM) nell'archivio di attendibilità di Expressway-C.

Nota: sebbene i campi Emittente e Oggetto siano facili da creare e leggibili, CUCM non utilizza questi campi nel certificato. Vengono invece utilizzati i campi Identificatore chiave autorità X509v3 e Identificatore chiave oggetto X509v3 per creare la catena di attendibilità. Tali chiavi contengono identificatori per i certificati più accurati rispetto all'utilizzo dei campi Oggetto/Emittente: possono essere presenti 2 certificati con gli stessi campi Oggetto/Autorità emittente, ma uno di essi è scaduto e uno è ancora valido. Entrambi avrebbero un identificatore di chiave del soggetto X509v3 diverso, in modo che CUCM possa ancora determinare la corretta catena di fiducia.

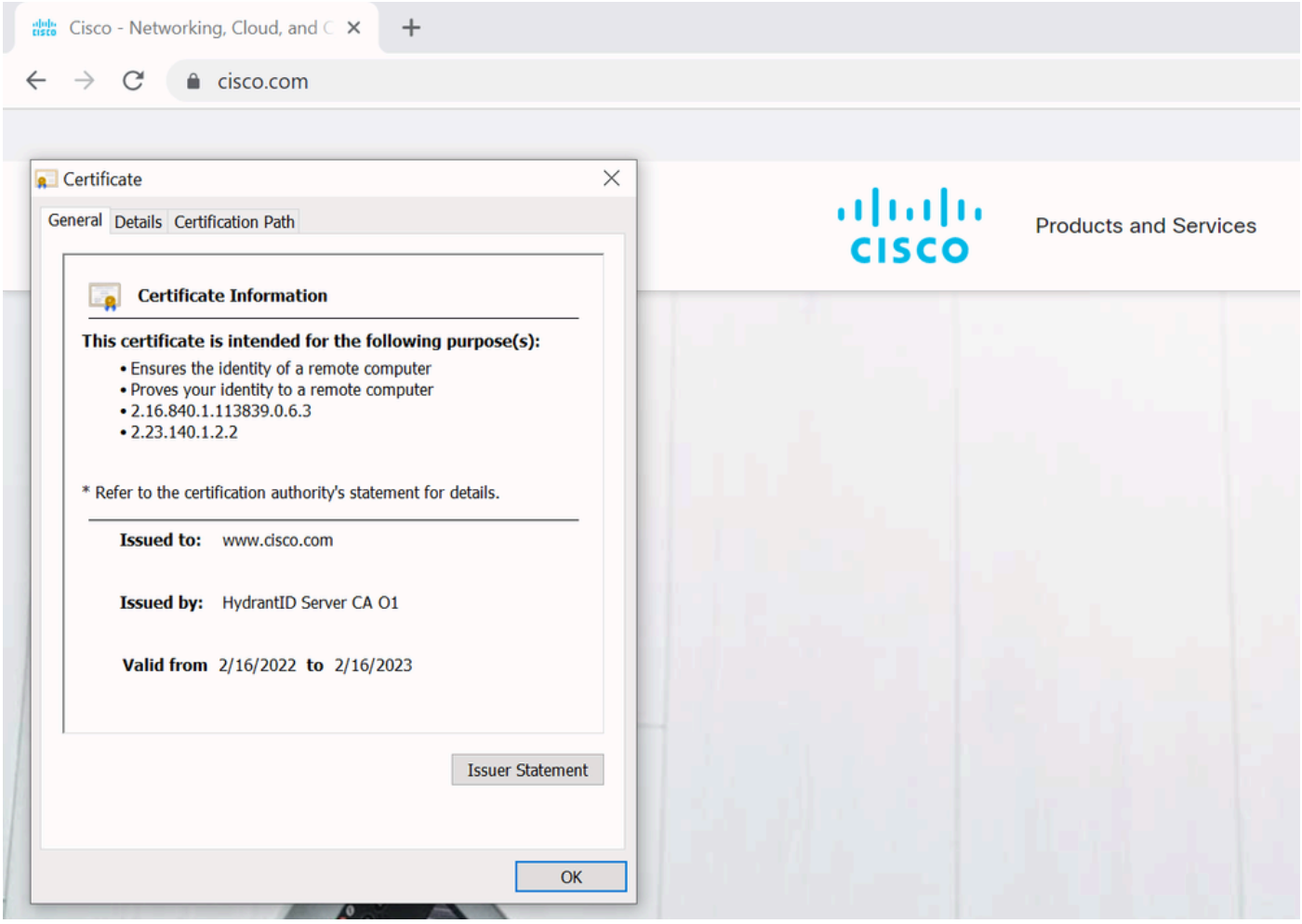
Questo non è il caso di Expressway, tuttavia come per l'ID bug Cisco CSCwa12905, e non è possibile caricare due certificati diversi, ad esempio autofirmati, nell'archivio di attendibilità di Expressway con lo stesso nome comune (CN). Per risolvere il problema, è possibile utilizzare certificati firmati dall'autorità di certificazione o nomi comuni diversi per tali certificati o verificare che utilizzi sempre lo stesso certificato (potenzialmente tramite la funzionalità di riutilizzo dei certificati di CUCM 14).

Controllo SAN o CN

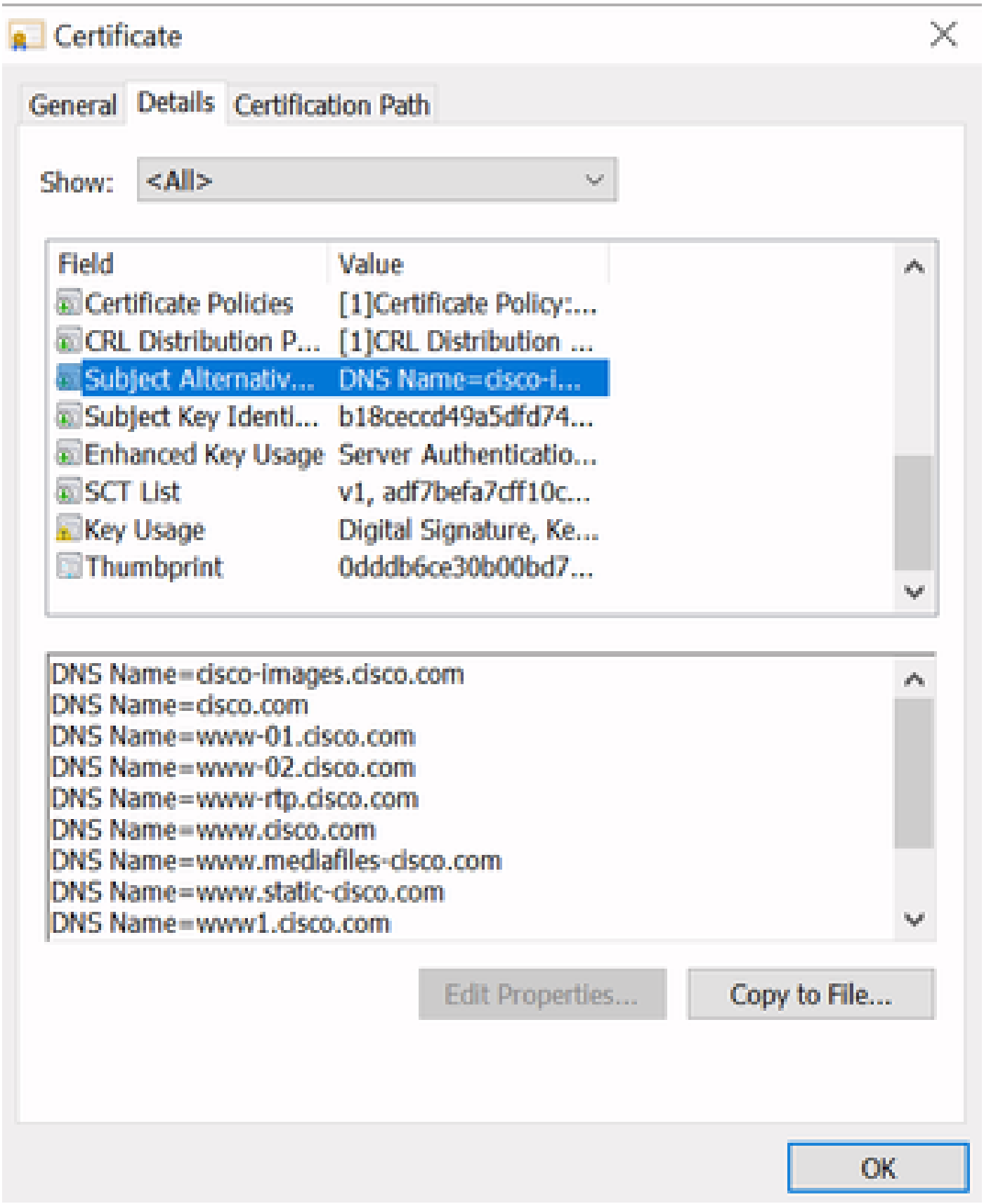
Il passaggio 1 consente di estrarre l'archivio di attendibilità, tuttavia, chiunque disponga di un certificato firmato da una CA nell'archivio di attendibilità sarà valido. Questo chiaramente non è sufficiente. Pertanto, è disponibile un ulteriore controllo che consente di verificare che il server a cui ci si connette sia effettivamente quello corretto. L'indirizzo a cui si riferisce la richiesta è quello indicato nella richiesta.

Lo stesso tipo di operazione si verifica nel browser, quindi è possibile visualizzare questo esempio. Se si sceglie Cisco.com, viene visualizzata un'icona a forma di lucchetto accanto all'URL immesso e la connessione è attendibile. Questo si basa sia sulla catena di attendibilità della CA (dalla prima sezione) sia sul controllo della SAN o della CN. Se si apre il certificato (tramite il

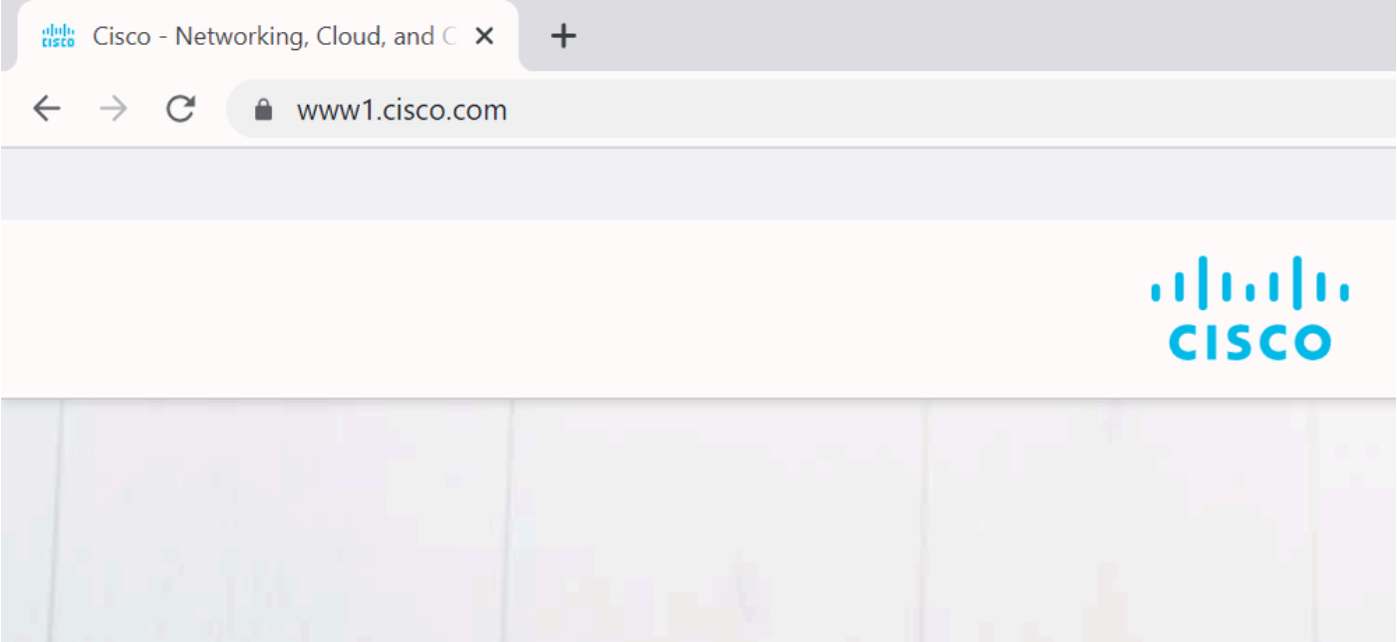
browser facendo clic sull'icona a forma di lucchetto), si noterà che il nome comune (visualizzato in Rilasciato a:) è impostata su Cisco.com e corrisponde esattamente all'indirizzo a cui ci si desidera connettere. In questo modo, è possibile essere certi di connettersi al server corretto, in quanto si considera attendibile la CA che ha firmato il certificato e che esegue la verifica prima che distribuisca il certificato.



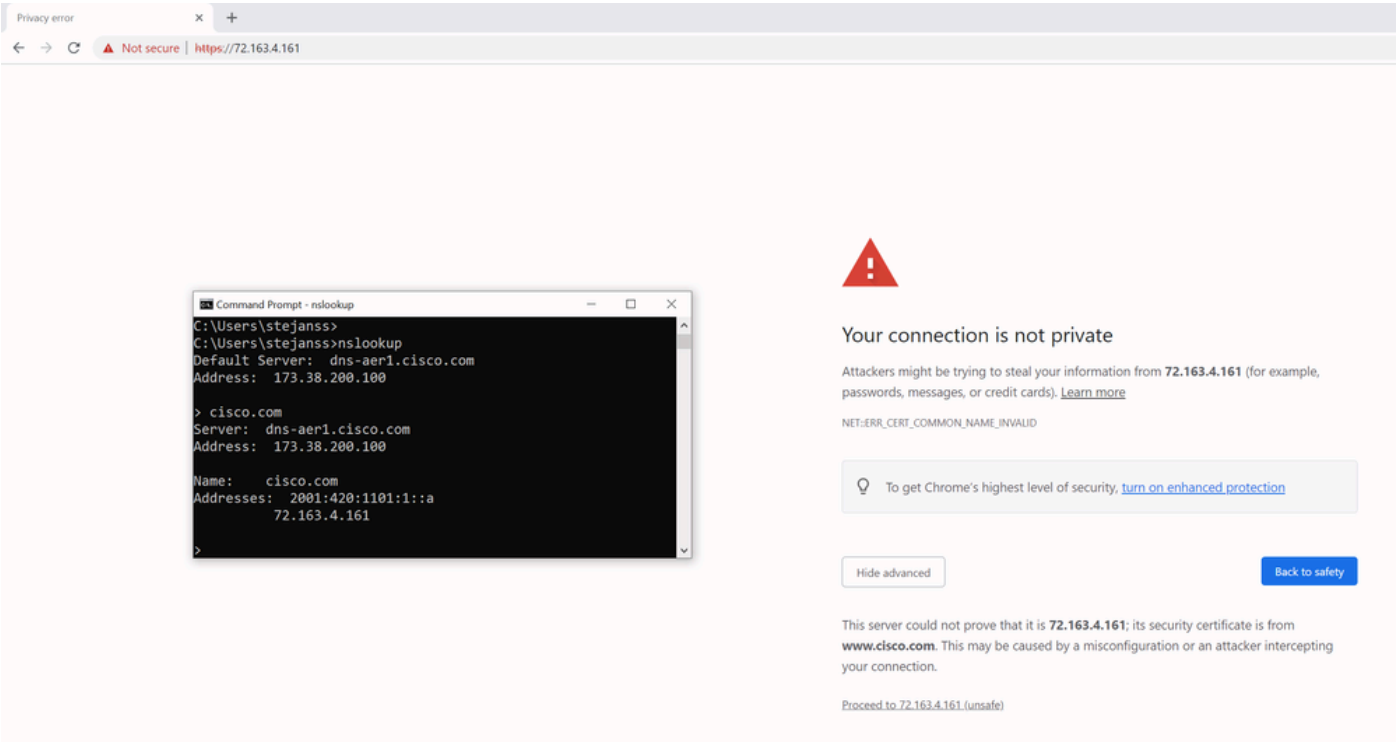
Se si esaminano i dettagli del certificato e in particolare le voci SAN, si osserverà che lo stesso vale per altri FQDN:



Ciò significa che, quando si richiede ad esempio la connessione a Cisco.com, questa viene visualizzata anche come connessione protetta, in quanto è inclusa nelle voci SAN.



Tuttavia, se non si desidera passare a Cisco.com bensì direttamente all'indirizzo IP (indirizzo Web numerato), la connessione non sarà sicura in quanto l'autorità di certificazione che l'ha firmata non è considerata attendibile. Il certificato presentato non contiene l'indirizzo (72.163.4.161) utilizzato per la connessione al server.



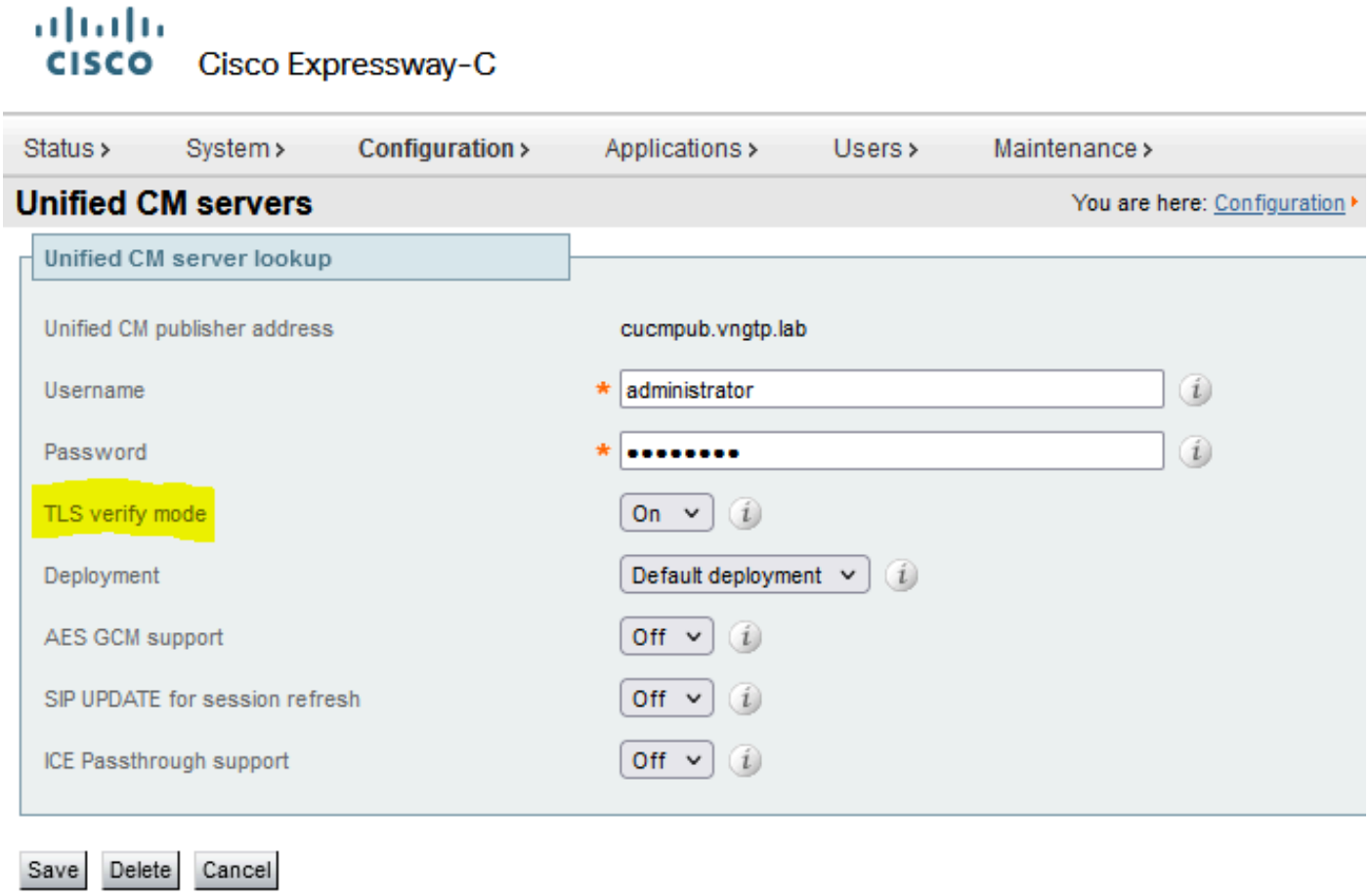
Nel browser, è possibile ignorare questa impostazione, tuttavia, è un'impostazione che è possibile abilitare sulle connessioni TLS che un bypass non è consentito. È pertanto importante che i certificati contengano i nomi CN o SAN corretti che la parte remota intende utilizzare per connettersi.

Modifica del comportamento

I servizi MRA si basano molto su diverse connessioni HTTPS su Expressways verso i server CUCM / IM&P / Unity per autenticarsi correttamente e raccogliere le informazioni appropriate specifiche per il client che esegue il login. Questa comunicazione in genere ha luogo sulle porte 8443 e 6972.

Versioni inferiori a X14.2.0

Nelle versioni precedenti a X14.2.0, server di traffico su Expressway-C che gestisce le connessioni HTTPS protette che non hanno verificato il certificato presentato dall'estremità remota. Questo potrebbe portare ad attacchi di tipo man-in-the-middle. Nella configurazione MRA, è disponibile un'opzione per la verifica del certificato TLS mediante la configurazione della modalità di verifica TLS su Attivata quando si aggiungono i server CUCM / IM&P / Unity in Configurazione > Unified Communications > Unified CM servers / IM and Presence Service nodes / Unity Connection servers. L'opzione di configurazione e la casella delle informazioni rilevanti vengono mostrate come esempio, a indicare che non verifica l'FQDN o l'IP nella SAN, nonché la validità del certificato e se è firmato da una CA attendibile.



Questo controllo di verifica del certificato TLS viene eseguito solo al rilevamento dei server CUCM/IM&P/Unity e non al momento del login MRA quando viene eseguita una query sui vari server. Un primo inconveniente di questa configurazione è che la verifica solo per l'indirizzo dell'autore aggiunto. Non verifica se il certificato nei nodi del sottoscrittore è stato impostato correttamente in quanto recupera le informazioni sul nodo del sottoscrittore (FQDN o IP) dal database del nodo del server di pubblicazione. Un secondo inconveniente di questa

configurazione è che ciò che viene annunciato ai client MRA come informazioni di connessione può essere diverso dall'indirizzo dell'autore che è stato inserito nella configurazione Expressway-C. Ad esempio su CUCM, in Sistema > Server è possibile annunciare il server all'esterno con un indirizzo IP (ad esempio 10.48.36.215) e questo viene poi utilizzato dai client MRA (tramite la connessione Expressway proxy); tuttavia, è possibile aggiungere il CUCM su Expressway-C con il FQDN di cucm.steven.lab. Si supponga quindi che il certificato tomcat di CUCM contenga cucm.steven.lab come voce SAN ma non l'indirizzo IP, quindi il rilevamento con la modalità di verifica TLS impostata su On ha esito positivo, ma le comunicazioni effettive dai client MRA possono avere come destinazione un FQDN o un IP diverso e quindi non superano la verifica TLS.

Versioni di X14.2.0 e successive

A partire dalla versione X14.2.0, il server Expressway esegue la verifica del certificato TLS per ogni singola richiesta HTTPS effettuata tramite il server di traffico. Ciò significa che questa operazione viene eseguita anche quando la modalità di verifica TLS è impostata su Off durante il rilevamento dei nodi CUCM / IM&P / Unity. Se la verifica non ha esito positivo, l'handshake TLS non viene completato e la richiesta non riesce. Ciò può causare, ad esempio, la perdita di funzionalità quali ridondanza o problemi di failover oppure errori di accesso completi. Inoltre, se la modalità di verifica TLS è impostata su On, non è possibile garantire che tutte le connessioni funzionino correttamente, come illustrato nell'esempio riportato di seguito.

I certificati esatti che Expressway controlla verso i nodi CUCM / IM&P / Unity sono come mostrato nella sezione della guida MRA.

Oltre all'impostazione predefinita per la verifica TLS, in X14.2 è stata introdotta una modifica che potrebbe annunciare un ordine di preferenza diverso per l'elenco di cifratura, a seconda del percorso di aggiornamento. Ciò può causare connessioni TLS impreviste dopo un aggiornamento del software, perché può accadere che prima dell'aggiornamento, abbia richiesto il certificato Cisco Tomcat o Cisco CallManager a CUCM (o a qualsiasi altro prodotto che abbia un certificato separato per l'algoritmo ECDSA) ma che dopo l'aggiornamento, richieda la variante ECDSA (che è la variante di cifratura più sicura di RSA). È possibile che i certificati Cisco Tomcat-ECDSA o Cisco CallManager-ECDSA siano firmati da un'autorità di certificazione diversa o semplicemente autofirmati (impostazione predefinita).

La modifica dell'ordine delle preferenze di cifratura non è sempre rilevante in quanto dipende dal percorso di aggiornamento, come illustrato nelle note di rilascio di Expressway X14.2.1. In breve, è possibile vedere da Manutenzione > Sicurezza > Cifre per ciascuno degli elenchi di cifratura se precede ECDHE-RSA-AES256-GCM-SHA384 o meno. In caso contrario, preferisce la cifratura ECDSA più recente a quella RSA. In caso affermativo, si avrà il comportamento precedente di RSA che ha la preferenza più 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**).

La verifica TLS potrebbe non riuscire in questo scenario in due modi, descritti in dettaglio più avanti:

1. La CA che ha firmato il certificato remoto non è attendibile.

r. Certificato autofirmato

b. Certificato firmato da una CA sconosciuta

2. L'indirizzo di connessione (FQDN o IP) non è contenuto nel certificato.

Risoluzione dei problemi

Gli scenari successivi mostrano uno scenario simile in un ambiente lab in cui il login MRA non è riuscito dopo un aggiornamento di Expressway da X14.0.7 a X14.2. Essi condividono le analogie nei log, tuttavia la risoluzione è diversa. I log vengono raccolti dalla registrazione diagnostica (da Manutenzione **>** Diagnostica **>** Registrazione diagnostica) avviata prima dell'accesso dell'MRA e arrestata dopo l'errore di accesso dell'MRA. Non è stata abilitata alcuna registrazione di debug aggiuntiva.

1. La CA che ha firmato il certificato remoto non è attendibile

Il certificato remoto potrebbe essere firmato da una CA non inclusa nell'archivio di attendibilità di Expressway-C oppure potrebbe essere un certificato autofirmato (in sostanza anche una CA) che non viene aggiunto nell'archivio di attendibilità del server Expressway-C.

Nell'esempio riportato di seguito, è possibile osservare che le richieste inviate a CUCM (10.48.36.215 - cucm.steven.lab) vengono gestite correttamente sulla porta 8443 (risposta 200 OK), ma genera un errore (risposta 502) sulla porta 6972 per la connessione TFTP.

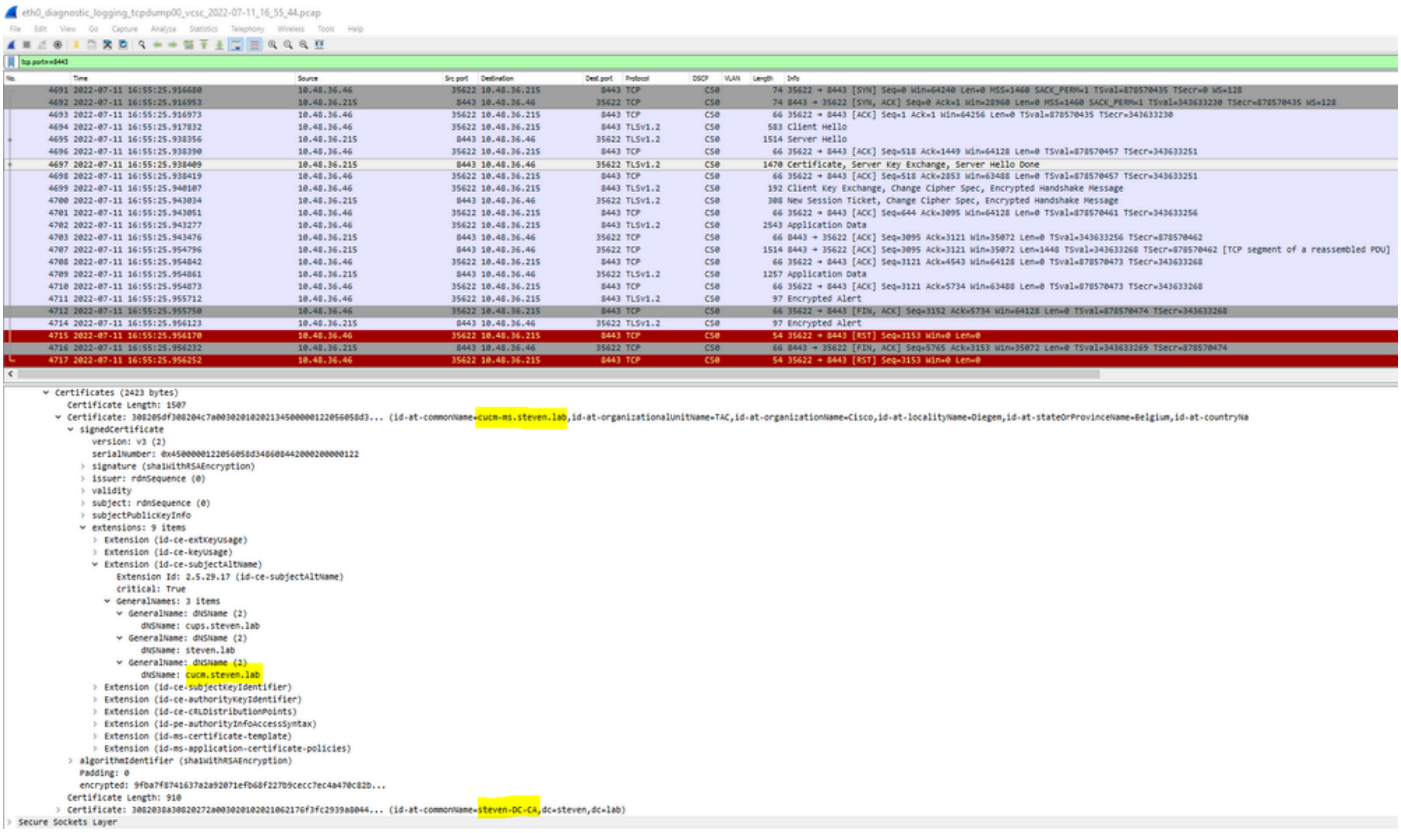
<#root>

```
===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 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]
```

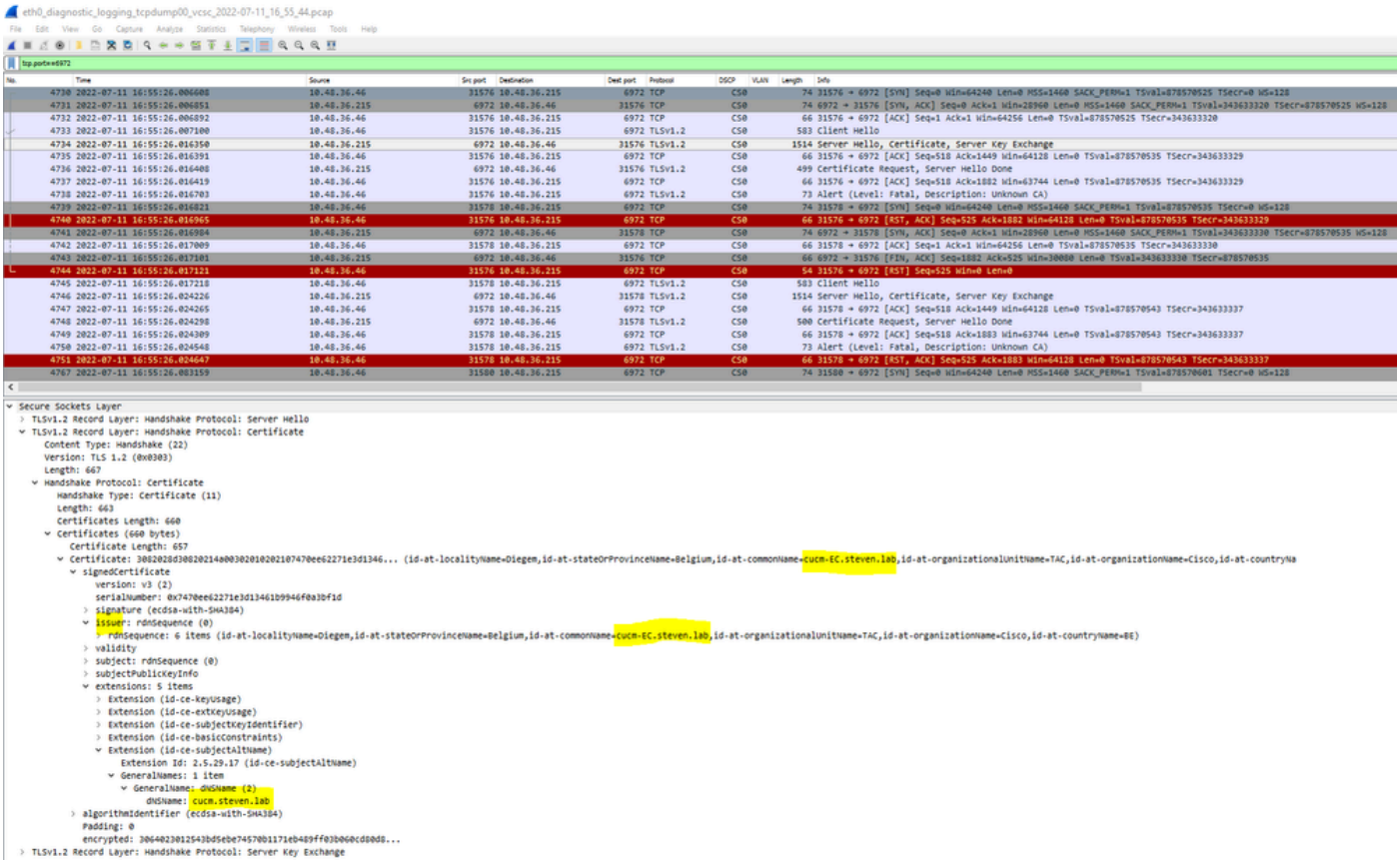
```
WARNING: Core server certificate verification failed for
 (cucm.steven.lab).
Action=Terminate Error=self signed certificate server=cucm.steven.lab(10.48.36.215)


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
"
```

L'errore di, verifica certificato non riuscita, indica che Expressway-C non è stato in grado di convalidare l'handshake TLS. Il motivo è indicato nella riga di avviso in quanto indica un certificato autofirmato. Se la profondità è indicata da 0, si tratta di un certificato autofirmato. Quando la profondità è maggiore di 0, significa che dispone di una catena di certificati e pertanto è firmata da un'autorità di certificazione sconosciuta (dal punto di vista di Expressway-C).

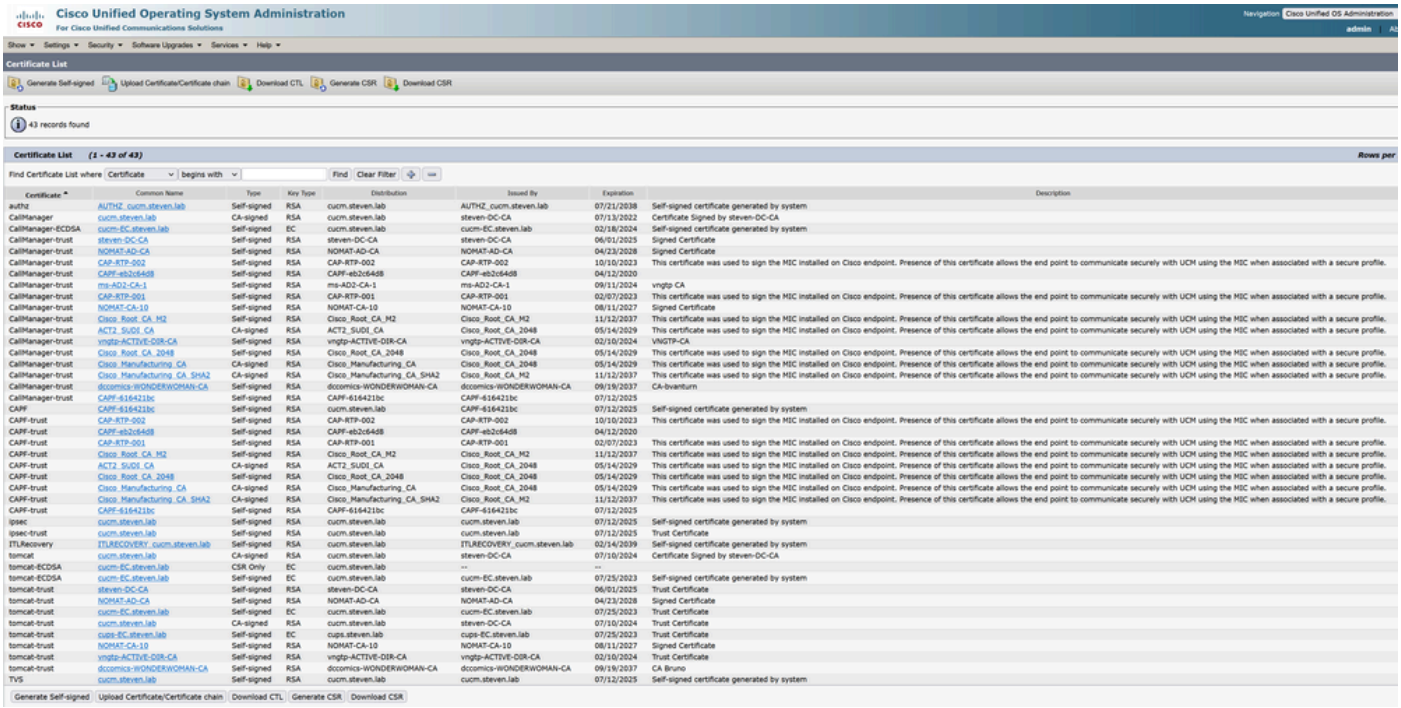
Se si controlla il file pcap che è stato raccolto in base ai timestamp indicati dai log di testo, è possibile notare che CUCM presenta il certificato con CN come cucm-ms.steven.lab (e cucm.steven.lab come SAN) firmato da steven-DC-CA per Expressway-C sulla porta 8443.



Tuttavia, quando si controlla il certificato presentato sulla porta 6972, si osserverà che si tratta di un certificato autofirmato (l'autorità emittente è se stessa) con CN impostato come cucm-EC.steven.lab. L'estensione -EC fornisce l'indicazione che si tratta del certificato ECDSA installato su CUCM.



In CUCM in Cisco Unified OS Administration (Amministrazione del sistema operativo unificato Cisco), è possibile esaminare i certificati in uso in Protezione > Gestione certificati, come mostrato di seguito. Mostra un certificato diverso per tomcat e tomcat-ECDSA dove il tomcat è firmato CA (e considerato attendibile da Expressway-C) mentre il certificato tomcat-ECDSA è autofirmato e non considerato attendibile da Expressway-C.



2. L'indirizzo di connessione (FQDN o IP) non è contenuto nel certificato

Oltre all'archivio di attendibilità, il server del traffico verifica anche l'indirizzo di connessione verso cui il client di Autorità registrazione integrità effettua la richiesta. Ad esempio, se avete impostato su CUCM in Sistema > Server il vostro CUCM con l'indirizzo IP (10.48.36.215), Expressway-C lo annuncia come tale al client e le richieste successive dal client (proxy attraverso Expressway-C) sono mirate a questo indirizzo.

Quando l'indirizzo di connessione non è contenuto nel certificato del server, anche la verifica TLS ha esito negativo e viene generato un errore 502 che, ad esempio, genera un errore di accesso MRA.

<#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/c3RldmVuLmxhYi9odHRwcy8xMC40OC4zNi4yMTUvODQOMw/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
```

dove c3RldmVuLmxhYi9odHRwcy8xMC40OC4zNi4yMTUvODQ0Mw converte (base64) in steven.lab/https/10.48.36.215/8443, a indicare che è necessario impostare la connessione a 10.48.36.215 come indirizzo di connessione anziché a cucm.steven.lab. Come mostrato nelle acquisizioni del pacchetto, il certificato tomcat CUCM non contiene l'indirizzo IP nella SAN e quindi viene generato l'errore.

Come convalidarlo in modo semplice

È possibile verificare se il comportamento cambia facilmente con i passaggi successivi:

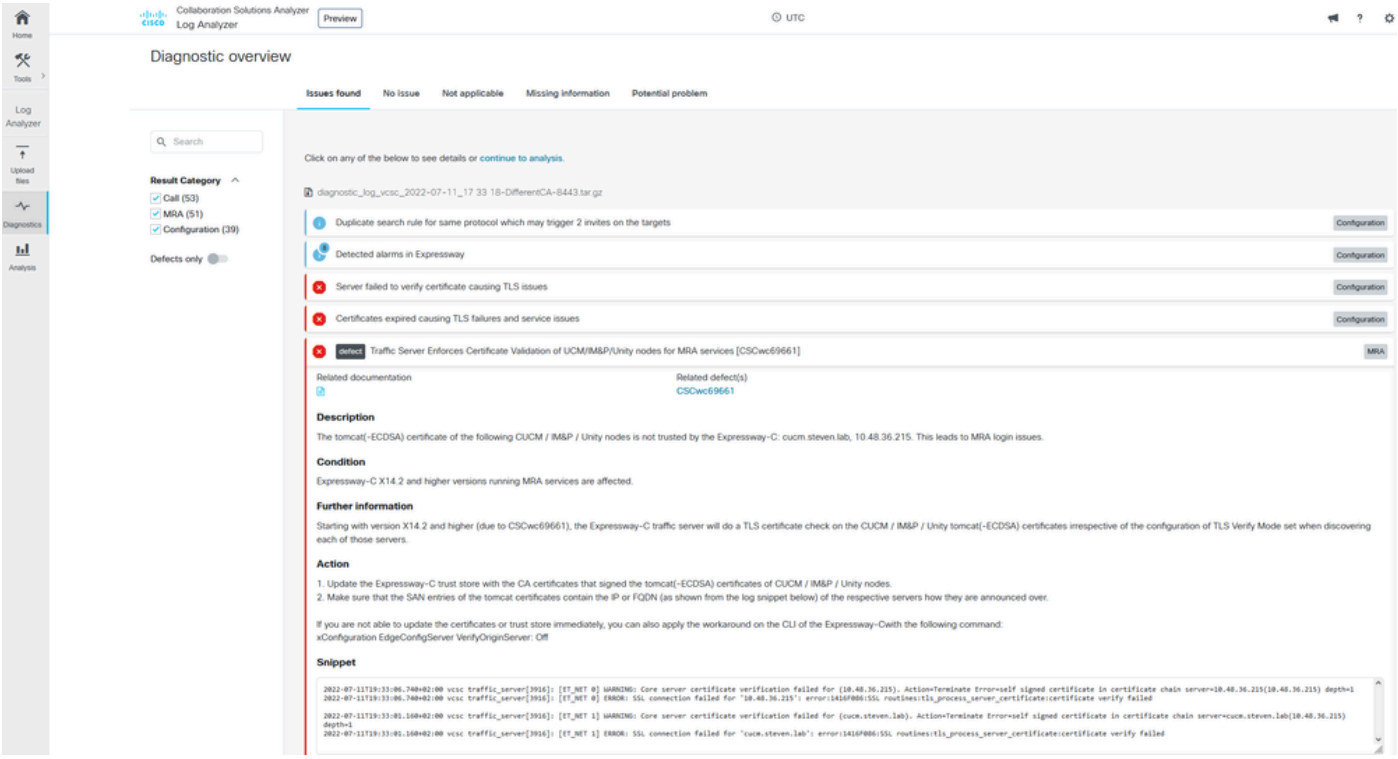
1. Avviare la registrazione diagnostica sui server Expressway-E e C (idealmente con TCPDump abilitato) da Manutenzione > Diagnostica > Registrazione diagnostica (nel caso di un cluster, è sufficiente avviarlo dal nodo primario)

2. Tentare di eseguire il login a un MRA o testare la funzionalità interrotta dopo l'aggiornamento

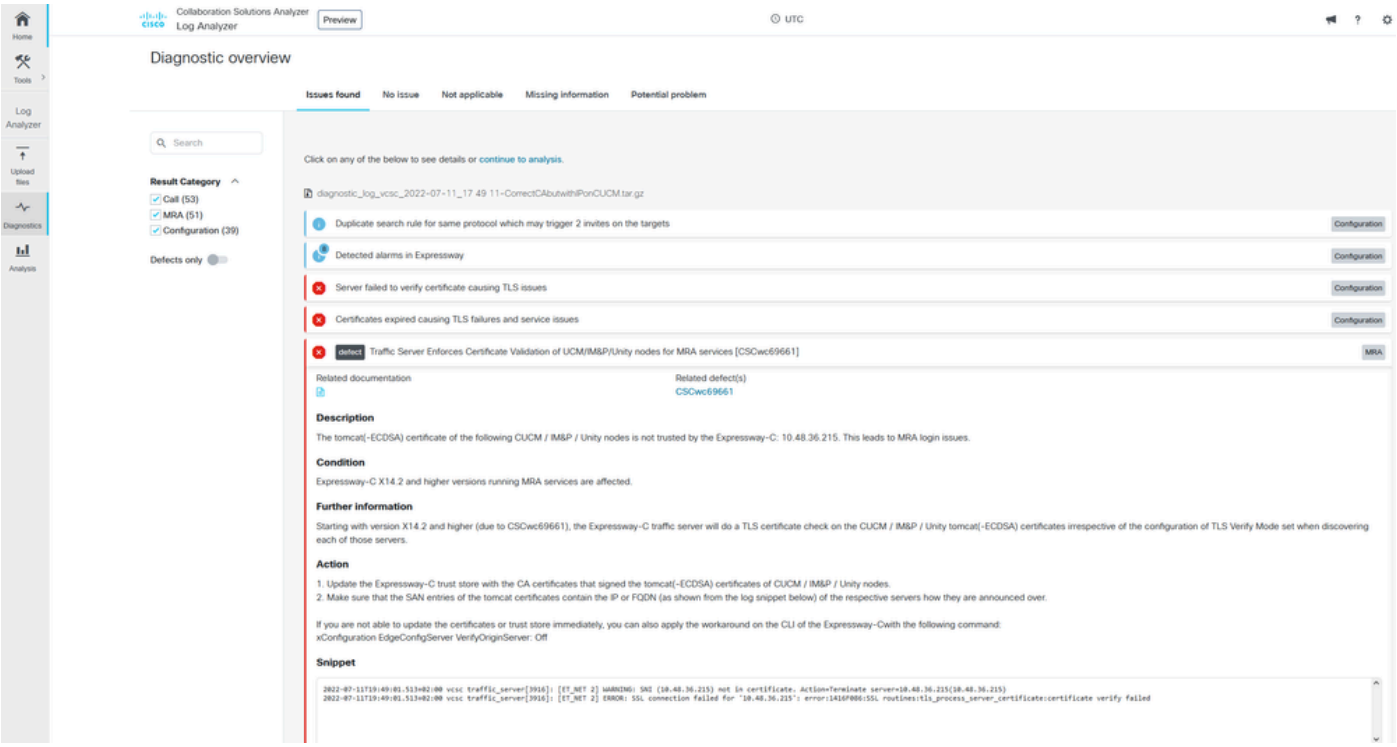
3. Attendere che si verifichi un errore e quindi arrestare la registrazione diagnostica sui server Expressway-E e C (nel caso di un cluster, assicurarsi di raccogliere i log da ogni singolo nodo del cluster)

4. Caricare e analizzare i registri nello strumento Collaboration Solution Analyzer.

5. Se si verifica il problema, vengono selezionate le righe di avvertenza e di errore più recenti relative alla modifica per ognuno dei server interessati



Firma diagnostica CA



Firma diagnostica SNI

Soluzione

La soluzione a lungo termine consiste nell'assicurare che la verifica TLS funzioni correttamente. L'azione da eseguire dipende dal messaggio di avviso visualizzato.

Quando si osserva il messaggio di avviso: Verifica del certificato del server di base non riuscita

per (<server-FQDN-or-IP>). Action=Terminate Error=self-signed certificate server=cucm.steven.lab(10.48.36.215) depth=x" message, quindi è necessario aggiornare l'archivio di attendibilità sui server Expressway-C di conseguenza. Con la catena di CA che ha firmato il certificato (profondità > 0) o con il certificato autofirmato (profondità = 0) da Manutenzione > Sicurezza > Certificato CA attendibile. Accertarsi di eseguire questa azione in ogni server del cluster. In alternativa, è possibile firmare il certificato remoto da una CA nota nell'archivio di attendibilità di Expressway-C.

Nota: Expressway non consente di caricare due certificati diversi (autofirmati, ad esempio) nell'archivio di attendibilità di Expressway con lo stesso nome comune (CN) dell'ID bug Cisco CSCwa12905. Per risolvere il problema, passare ai certificati firmati da CA o aggiornare CUCM alla versione 14, dove è possibile riutilizzare lo stesso certificato (autofirmato) per Tomcat e CallManager.

Quando si osserva il messaggio di avviso: SNI (<server-FQDN-or-IP>) not in certificate" (SNI (<server-FQDN-or-IP>) not in certificate, quindi indica che l'FQDN o l'IP del server non è contenuto nel certificato presentato. È possibile adattare il certificato in modo da includere tali informazioni oppure modificare la configurazione (come con Sistema CUCM > Server a un elemento contenuto nel certificato del server) e quindi aggiornare la configurazione nel server Expressway-C in modo da tenerne conto.

Informazioni correlate

La soluzione a breve termine consiste nell'applicare la soluzione descritta nella documentazione per ripristinare il comportamento precedente prima di X14.2.0. È possibile eseguire questa operazione tramite la CLI sui nodi del server Expressway-C con il nuovo comando:

```
xConfiguration EdgeConfigServer VerifyOriginServer: Off
```

Informazioni su questa traduzione
Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).