Configurazione e risoluzione dei problemi relativi ai requisiti DNS e dei certificati in Microsoft Federation tramite Expressway per Cisco Meeting Server

Sommario

Introduzione

In questo documento vengono descritti i requisiti DNS e dei certificati di Microsoft Lync/Skype for Business per una federazione tra domini diversi su Internet.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Expressway
- CMS (Cisco Meeting Server)
- Server Microsoft Lync o Skype for Business
- CUCM (Cisco Unified Communications Manager)

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Expressway X8.9 o versioni successive
- Cisco Meeting Server (CMS) 2.1.2 o versione successiva
- Server Microsoft Lync 2010, Lync 2013 o Skype for Business - locale o ospitato nel cloud (Office365)

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

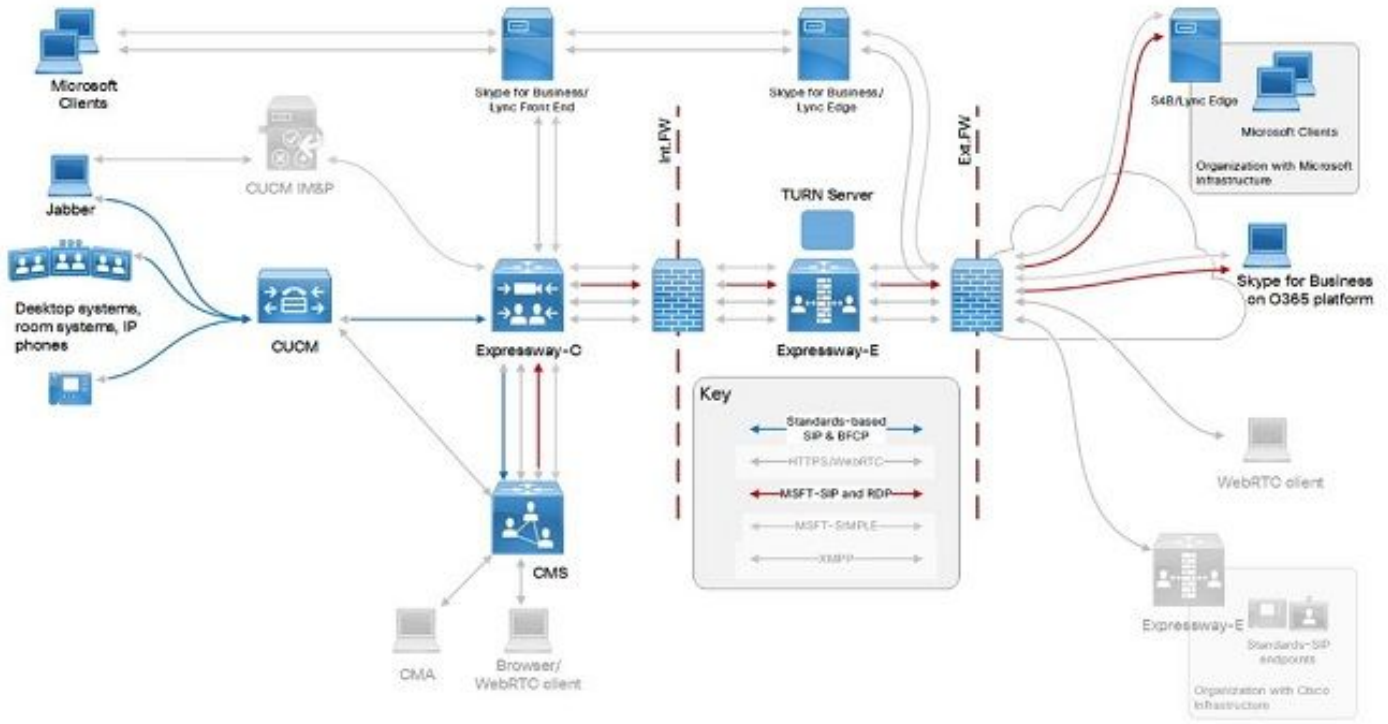
Il documento evidenzia un aspetto specifico dell'integrazione con client Microsoft esterni con l'infrastruttura Cisco utilizzando Expressway e Cisco Meeting Server (CMS). La configurazione di questa integrazione è descritta nella documentazione di **Cisco Expressway Options with Cisco Meeting Server e/o Microsoft Infrastructure** disponibile per la versione in uso nell'elenco delle guide alla configurazione della serie Cisco Expressway.

Il documento corrente è incentrato solo sui requisiti relativi al DNS e ai certificati nell'estremità Microsoft Lync o Skype for Business per la federazione esterna. Le altre configurazioni sono descritte nella guida alla configurazione di cui sopra.

Configurazione

Un esempio per il flusso di chiamate e la sua configurazione può essere un endpoint registrato CUCM che chiama un client Skype (on-prem o off-prem, o registrato nel cloud usando Office365), o viceversa - usando il CMS per la conversione tra Standard SIP e protocollo Microsoft. A tale scopo, è possibile utilizzare l'integrazione e il routing delle chiamate tramite i server Expressway, come mostrato nell'immagine seguente, tratta dalla **guida alla configurazione di Cisco Expressway Options with Cisco Meeting Server e/o Microsoft Infrastructure a** cui si fa riferimento alla fine di questo documento.

Esempio di rete



Nota: Questo è solo uno scenario di flusso di chiamata esemplare. Sono possibili anche altri scenari di chiamata.

DNS

Microsoft Lync/Skype for Business utilizza il record SRV **_sipfederationtls._tcp.<domain>** per individuare i server federativi esterni a cui inviare le chiamate (oltre alle informazioni sulla presenza); o per la funzionalità di richiamata basata sul dominio specificato nell'**intestazione From/P-Asserted-Identity** dell'**invito SIP** in ingresso. In questo scenario, i record DNS devono essere disponibili nel DNS pubblico per entrambi i domini per poter essere federati tra loro.

La parte di dominio dell'**FQDN** (nome di dominio completo, Fully Qualified Domain Name) restituita dalla ricerca del record SRV per il dominio deve corrispondere esattamente (non sono consentiti altri domini o sottodomini). Nella tabella seguente viene illustrato un esempio di configurazione DNS per un dominio denominato **example.com**:

record SRV	_sipfederationtls._tcp.example.com	expe.example.com
Un record	expe.example.com	Indirizzo IP di Expressway-E

Attenzione: Il record A a cui viene risolto l'SRV deve corrispondere esattamente al dominio configurato. I sottodomini (ad esempio expe.sub.example.com) o i domini diversi (expe.dummy.com) non verranno considerati attendibili da Microsoft Lync/Skype for Business e questo determinerà errori di chiamata anche se potrebbero avere record A appropriati e risolversi in errori di IP.

Certificato

Microsoft Lync/Skype for Business imposta una connessione TLS tra i domini configurati sui lati Lync ed Expressway. Microsoft Lync/Skype for Business ha i seguenti requisiti di certificati server

per la federazione e i server con cui comunica (Expressway-E in questo documento):

- Il certificato del server presentato dal server corrispondente al record A deve avere quel particolare **FQDN** contenuto nel **Nome alternativo soggetto** (o **Nome comune**, se non si utilizza SAN)
- Il certificato del server presentato dal server deve essere considerato attendibile dai server Microsoft Lync/Skype for Business (firmato da una CA pubblica o da una CA privata i cui certificati radice/intermedi sono stati importati nell'**elenco delle CA attendibili** dei server Microsoft Lync/Skype for Business). Quando si utilizza Office365, sono necessari certificati pubblici firmati da un'autorità di certificazione.

Ad esempio:

Il certificato server del server Expressway-E corrispondente a **expe.example.com**, come illustrato nell'esempio precedente, deve contenere almeno le voci seguenti:

- (Solo se non sono presenti **nomi alternativi soggetto**) **Nome comune** deve essere **expe.example.com**
- (Se sono disponibili **nomi alternativi soggetto**) **Nome alternativo soggetto** deve contenere una **voce expe.example.com**
- L'autorità emittente della parte superiore dell'albero dei certificati deve essere una CA pubblica (altrimenti la CA dovrà essere aggiunta all'**elenco delle CA attendibili** dei server Microsoft Lync/Skype)

Nota:

Il dominio (example.com) su se stesso non deve essere incluso come **Nome alternativo soggetto**.

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

La sezione contiene le informazioni di log e le tracce acquisite da una distribuzione del laboratorio di test con le seguenti specifiche:

- Il dominio Skype è skype.lab
- Il dominio UC (Expressway-E, Expressway-C e CUCM) è steven.lab
- Il dominio CMS per utenti e spazi è acano.steven.lab (è disponibile anche cms.steven.lab)

Poiché è consigliabile utilizzare un dominio separato per Cisco Meeting Server (diverso dall'altro dominio UC su UCM/Expressway), è probabile che si disponga di un dominio diverso sul server Expressway-E e ciò potrebbe causare problemi di integrazione correlati ai requisiti della federazione SIP sul lato del server Microsoft Lync/Skype for Business.

Sintomi ed esame del registro

Quando i requisiti dei certificati DNS non corrispondono sul lato server Microsoft Lync/Skype, si notano i sintomi seguenti:

- Quando si effettua una chiamata dall'infrastruttura UC verso Microsoft Lync/Skype, si vede la chiamata in uscita nella zona DNS della Expressway-E verso Skype, ma si genera

immediatamente un errore (504) di timeout del server, visibile nella pagina **Stato > Cronologia ricerche** di Expressway-E:

- Quando si effettua una chiamata da Microsoft Lync/Skype verso l'infrastruttura UC, la chiamata non arriva su Expressway-E come mostrato nella pagina **Stato > Cronologia ricerche** di Expressway-E.

Questa sezione secondaria spiega come verificare questo scenario utilizzando l'accesso per ulteriori dettagli e controllare cosa esattamente è configurato in modo errato.

Chiama Microsoft Lync/Skype

In questo flusso di chiamate, nella registrazione diagnostica di Expressway-E viene visualizzato SIP INVITE in uscita verso Skype (se è possibile risolvere il record **_sipfederationtls._tcp** SRV in un FQDN e IP), seguito immediatamente da una risposta di **timeout del server 504** senza ulteriori dettagli, come mostrato nel seguente frammento di codice di accesso:

```
2017-03-02T08:10:46.240+01:00 vcse tvcs: UTCTime="2017-03-02 07:10:46,240" Module="network.sip"
Level="DEBUG":  Action="Received" Local-ip="10.48.36.47" Local-port="25002" Src-ip="10.48.36.6"
Src-port="5061" Msg-Hash="13707918855517357847"
 SIPMSG:
 |SIP/2.0 504 Server time-out
 Via: SIP/2.0/TLS 10.48.36.47:5061;egress-
zone=DNSZone1;branch=z9hG4bK42ee6fd77d32cc8925196770b950b33554.731d73c3f4246d6a255e38a9f695bfc0;
proxy-call-id=6b2a018a-2da5-4013-a7e5-4e1455feadf7;rport;received=10.48.36.47;ms-received-
port=25002;ms-received-cid=100
 Via: SIP/2.0/TLS 10.48.36.46:5061;egress-
zone=TraversalZoneClient1;branch=z9hG4bK1f8bbe5926dc6abd06ea964d8fde1450156486;proxy-call-
id=e7e33845-c384-4c28-a42d-016863640fbb;received=10.48.36.46;rport=28119;ingress-
zone=TraversalZoneServer1
 Via: SIP/2.0/TLS
10.48.54.160:52768;branch=z9hG4bK6594a02846406f4a5459d5f58a8d26b3;received=10.48.54.160;ingress-
zone=NeighborZoneAcano1SIP
 Call-ID: f1b3ad5d-183b-4632-b210-c2f9bec71960
 CSeq: 2066245576 INVITE
 From: "DX70 Steven" <sip:2000@acano.steven.lab>;tag=9fea3e7d70afd884
 To: <sip:stejanss@skype.lab>;tag=C65A7B0A8766A5F1D386474833D07882
 Server: RTC/6.0
 Content-Length: 0
```

La stessa risposta viene visualizzata (senza ulteriori informazioni) indipendentemente dal fatto che si tratti di un errore nei record DNS o nel certificato del server di Expressway-E.

Pertanto, per esaminarlo più dettagliatamente, è necessario esaminare la registrazione di Lync/Skype Edge Server, dove è possibile visualizzare gli avvisi e gli errori a seconda dei possibili errori:

- Errore possibile: Il risultato FQDN del record SRV non corrisponde esattamente sul dominio come nell'**intestazione From/P-Asserted-Identity** di INVITE in arrivo su Skype. In questo frammento di log, l'intestazione From/P-Asserted-Identity di SIP INVITE contiene acano.steven.lab come dominio, ma **_sipfederationtls._tcp.acano.steven.lab** punta a **vcse.steven.lab** anziché a **vcse.acano.steven.lab**:

```
TL_WARN(TF_DIAG) [sfvedge\sfvedge]0584.0A44::03/02/2017-07:10:46.230.0000773E
(SIPStack,SIPAdminLog::WriteDiagnosticEvent:SIPAdminLog.cpp(830)) [156659184] $$begin_record
```

Severity: warning Text: **The domain of the message resolved by DNS SRV but none of the FQDNs is in the same domain** Result-Code: 0xc3e93d6f SIPPROXY_E_EPROUTING_MSG_ALLOWED_DOMAIN_NO_SRV_MATCH SIP-Start-Line: INVITE sip:stejanss@skype.lab SIP/2.0 SIP-Call-ID: f1b3ad5d-183b-4632-b210-c2f9bec71960 SIP-CSeq: 2066245576 INVITE Peer: vcse.steven.lab:25002 Data: **domain**="**acano.steven.lab**";**fqdn1**="**vcse.steven.lab**:5061" $$end_record

- Errore possibile: Il certificato del server Expressway-E non contiene il nome di dominio completo risultante dal record SRV **_sipfederationtls._tcp**. Viene inviato lo stesso **SIP INVITE** e **_sipfederationtls._tcp.acano.steven.lab** punta a **vcse.acano.steven.lab**, ma il nome di dominio completo (FQDN) non è incluso nell'elenco SAN dei certificati del server Expressway-E:

TL_ERROR(TF_DIAG) [sfvedge\sfvedge]0B60.0D6C::03/02/2017-06:30:40.025.00005602 (SIPStack,SIPAdminLog::WriteDiagnosticEvent:SIPAdminLog.cpp(833)) [3634190282] $$begin_record Severity: error Text: **Message cannot be routed because the peer's certificate does not contain a matching FQDN** Result-Code: 0xc3e93d67 SIPPROXY_E_ROUTING_MSG_CERT_MISMATCH SIP-Start-Line: INVITE sip:stejanss@skype.lab SIP/2.0 SIP-Call-ID: e144704c-1dd0-4ea7-929f-77e7e071c24c SIP-CSeq: 1567605805 INVITE Peer: vcse.steven.lab:25001 Data: **expected-fqdn**="**vcse.acano.steven.lab**";**certName**="**vcse.steven.lab**";info="The peer certificate does not contain a matching FQDN" $$end_record

Chiamata da Microsoft Lync/Skype

Per questo flusso di chiamata non si vede molto nella registrazione di Expressway-E come il server Skype Edge non invia l'INVITE fuori e si deve fare affidamento sulla registrazione Skype. Utilizzare la registrazione del server Lync/Skype (Edge) o la registrazione del client Lync/Skype per analizzare il problema in modo più approfondito.

Il client Skype che accede a un PC Windows è disponibile al seguente percorso:

C:\Users\<nomeutente>\AppData\Local\Microsoft\Office\16.0\Lync\Tracing\Lync-UccApi-x.UccApiLog

Può essere utile nel caso di utenti di Office 365 Skype quando non è disponibile l'accesso diretto ai server Skype*. In questa registrazione è possibile visualizzare il* messaggio **SIP INVITE** inviato dal client e la risposta appropriata per tale messaggio.

In caso di problemi con il DNS o i requisiti dei certificati su Skype, come indicato in questo documento, si riceveranno le risposte di **timeout di 504 Server** (incluso il motivo dell'errore) dai server Skype:

- Errore possibile: Il risultato FQDN del record SRV non corrisponde esattamente al dominio che si è tentato di chiamare. Questo frammento di registro mostra il tentativo di connessione a un utente o a uno spazio con il dominio **cms.steven.lab** e **_sipfederationtls._tcp.cms.steven.lab** che punta a **vcse.sub.cms.steven.lab**:

SIP/2.0 **504 Server time-out** Authentication-Info: TLS-DSK qop="auth", opaque="FA404B9C", srand="8168D157", snum="38", rspauth="65d8d93b66e5b217115e3b1636bf433c9f5df54a", targetname="SfBFE.skype.lab", realm="SIP Communications Service", version=4 From: "Steven Janssens"

INVITE Via: SIP/2.0/TLS 10.55.186.71:62937;ms-received-port=62937;ms-received-cid=6DA00 ms-diagnostics: 1009;

reason="No match for domain in DNS SRV results";

domain="

cms.steven.lab";

fqdn1="

vcse.sub.cms.steven.lab:5061";source="sip.skype.lab" Server: RTC/6.0 Content-Length: 0

- Errore possibile: Il certificato del server Expressway-E non contiene il nome FQDN risultante dal record SRV _sipfederationtls._tcp. Questo frammento di log mostra il tentativo di connessione a un utente o a uno spazio con il dominio cms.steven.lab per il quale _sipfederationtls._tcp.cms.steven.lab viene risolto correttamente in vcse.cms.steven.lab ma questo nome FQDN non è contenuto nel nome alternativo soggetto sul certificato del server Expressway-E (con nome comune come vcse.steven.lab.steven.steven):

SIP/2.0 **504 Server time-out** Authentication-Info: TLS-DSK qop="auth", opaque="FA404B9C", srand="1D8F66EF", snum="49", rspauth="67836c7ffc0f6132b2304006969a219d9252aabd", targetname="SfBFE.skype.lab", realm="SIP Communications Service", version=4 From: "Steven Janssens"

INVITE Via: SIP/2.0/TLS 10.55.186.71:62937;ms-received-port=62937;ms-received-cid=6DA00 ms-diagnostics: 1010;

reason="Certificate trust with another server could not be established";ErrorType="The peer certificate does not contain a matching FQDN";

tls-target="

vcse.cms.steven.lab";

PeerServer="

vcse.steven.lab";HRESULT="0x80090322(SEC_E_WRONG_PRINCIPAL)";source="sip.skype.lab" Server: RTC/6.0 Content-Length: 0

Informazioni correlate

- Guide alla configurazione di Cisco serie Expressway