

DNS- en certificaatvereisten op Microsoft Federatie configureren en probleemoplossing via expressserver van Cisco Meeting Server

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Netwerkdigram](#)

[DNS](#)

[Certificaat](#)

[Problemen oplossen](#)

[Symptomen en inlogoverzicht](#)

[Bel naar Microsoft Lync/Skype](#)

[Bel Microsoft Lync/Skype](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft de DNS- en certificeringsvereisten van Microsoft Lync/Skype voor bedrijven voor een federatie tussen verschillende domeinen via het internet.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Express
- CMS (Cisco Meeting Server)
- Microsoft Lync of Skype voor Business-server
- CUCM (Cisco Unified Communications Manager)

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco Express versie X8.9 of hoger
- Cisco Meeting Server (CMS) 2.1.2 of hoger

- Microsoft Lync 2010-server, Lync 2013-server of Skype voor zakelijke server - on-prem of opgenomen in de cloud (Office365)

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Achtergrondinformatie

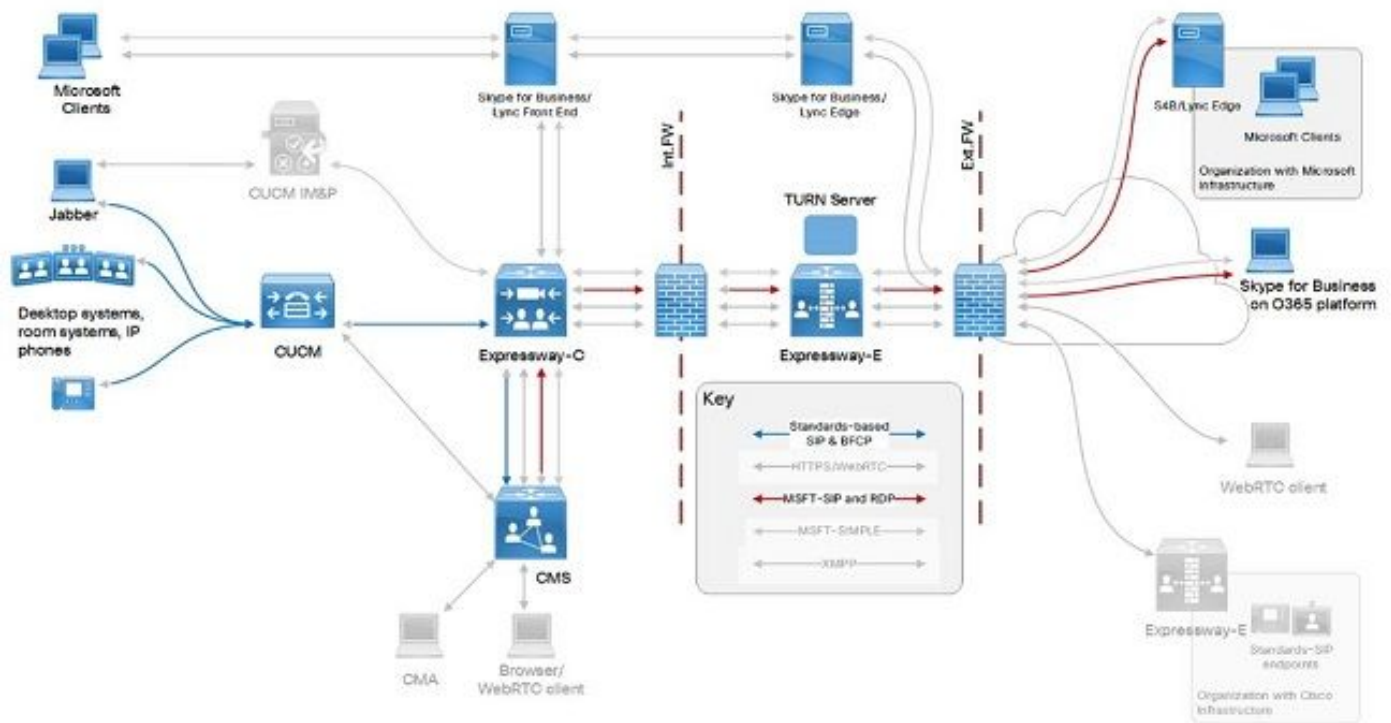
Het document benadrukt een specifiek aspect van de integratie met externe Microsoft-clients met uw Cisco-infrastructuur met behulp van Expressway en Cisco Meeting Server (CMS). De configuratie voor deze integratie is zoals uitgelegd in de **Cisco Expressway Opties met Cisco Meeting Server en/of Microsoft Infrastructuur** documentatie die beschikbaar is voor uw versie in de lijst [Cisco Expressway Series Configuration-gidsen](#).

Het huidige document is alleen gericht op de DNS- en certificeringsvereisten voor Microsoft Lync of Skype voor Business End voor externe federatie. De overige configuraties zijn opgenomen in de bovengenoemde configuratie gids.

Configureren

Een voorbeeld voor de gespreksstroom en de configuratie ervan kan een geregistreerd CUCM-eindpunt zijn dat naar een Skype-client wordt gedemonteerd (ofwel on-prem of off-prem, of in de cloud geregistreerd via Office365) of omgekeerd, waarbij gebruik wordt gemaakt van CMS voor de conversie tussen de standaard SIP en Microsoft Protocol. Dit is mogelijk door de integratie en het roepen van de routing met behulp van snelwegservers, zoals in de afbeelding hieronder wordt getoond, en die uit de **Cisco Expressway Opties** wordt **genomen met de Cisco Meeting Server en/of de configuratiehandleiding voor de Microsoft Infrastructuur** aan het eind van dit document.

Netwerkdigram



Opmerking: Dit is slechts een voorbeeldscenario voor aanroep flow. Andere callscenario's zijn ook mogelijk.

DNS

Microsoft Lync/Skype voor Business gebruikt de **_sipfederationtls._tcp.<domain>** SRV-record om de externe federatieservers te ontdekken waarop de oproepen naar worden verzonden (evenals de aanwezigheid-informatie); of voor de call-back functionaliteit op basis van het domein dat wordt gespecificeerd in de **From/P-Asserted-Identity header** van de inkomende **SIP INVITE**. In dit scenario moeten de DNS-records op de openbare DNS-server voor beide domeinen beschikbaar zijn om tussen elkaar te kunnen federeren.

Het domeingedeelte van de **FQDN** (Full Qualified Domain Name) dat door de SRV record lookup voor het domein wordt teruggegeven, moet exact overeenkomen (er zijn geen andere domeinen of subdomeinen toegestaan). De volgende tabel toont een voorbeeld voor DNS-configuratie voor een domein met naam **bijvoorbeeld.com**:

```
SRV-record _sipfederationtls._tcp.example.com expe.example.com
Een record expe.example.com IP-adres van Expressway-E
```

Voorzichtig: De A record die SRV oplost tot, moet een exacte overeenkomst zijn op het geconfigureerde domein. Subdomeinen (bijvoorbeeld expe.sub.voorbeeld.com) of verschillende domeinen (expe.dummy.com) zullen niet door Microsoft Lync/Skype voor Business worden vertrouwd en dit zal resulteren in call default, ondanks dat ze wellicht de juiste A records hebben en vastberaden zijn om IP's te corrigeren.

Certificaat

Microsoft Lync/Skype voor Business stelt een TLS-verbinding in tussen de domeinen die zijn

geconfigureerd op de Lync- en expressway-zijkanten. Microsoft Lync/Skype voor Business heeft de volgende vereisten voor servercertificaten voor de federatie en de servers waarmee ze communiceert (Expressway-E in dit document):

- Het servercertificaat dat wordt gepresenteerd door de server die de A record matcht, moet die specifieke **FQDN** hebben die in zijn **Onderwerp Alternatieve Name** (of **Common Name**, indien geen SAN gebruikt) staat
- Het servercertificaat dat door de server wordt gepresenteerd, moet worden vertrouwd door de Microsoft Lync/Skype voor zakelijke servers (ofwel ondertekend door een openbare CA, of door een particuliere CA waarvan de basis-/tussentijdse certificaten zijn ingevoerd in de **Trusted CA-lijst** van de Microsoft Lync/Skype voor zakelijke servers). Merk op dat wanneer u Office365 gebruikt, openbare CA-certificaten vereist zijn.

Bijvoorbeeld:

Het servercertificaat van de Expressway-E-server die **expe.voorbeeldcom** aansluit zoals in het bovenstaande voorbeeld wordt getoond, moet de volgende minimumwaarden hebben:

- (Enkel indien geen **alternatieve doelnamen** zijn vereist, moet **dezelfde naam expe.voorbeelds.com** zijn
- (Indien **Alternatieve Namen voor het onderwerp** beschikbaar zijn) **Onderwerp Alternatieve Naam** moet **entry expe.voorbeeldv.com** bevatten
- De uitgever boven de certificeringsboom moet een openbare CA zijn (anders moet de CA worden toegevoegd aan de **Trusted CA-lijst** van de Microsoft Lync/Skype-servers)

Opmerking:

Het domein (voorbeeld.com) op zichzelf hoeft niet als **Onderwerp Alternatieve Naam** te worden opgenomen.

Problemen oplossen

Deze sectie verschaft informatie die u kunt gebruiken om problemen met uw configuratie op te lossen.

De sectie bevat houtkapinformatie en sporen die uit een testlaboratorium met de volgende specificaties worden genomen:

- Skype-domein is skype.lab
- UC-domein (Expressway-E, Expressway-C en CUCM) is steven.lab
- CMS-domein voor gebruikers en ruimtes is acano.steven.lab (cms.steven.lab is ook beschikbaar)

Aangezien het wordt aanbevolen om een afzonderlijk domein voor uw Cisco Meeting Server te gebruiken (anders dan uw andere UC-domein op UCM/Expressway), is het waarschijnlijk dat u een ander domein hebt op uw Expressway-E-server en dit kan leiden tot integratieproblemen die te maken hebben met de vereisten op SIP-federatie aan de kant van Microsoft Lync/Skype voor Business-server.

Symptomen en inlogoverzicht

Wanneer de vereisten voor DNS-certificaten niet aan de kant van Microsoft Lync/Skype-server zijn

aangepast, krijgt u de volgende symptomen te zien:

- Wanneer vanuit uw UC-infrastructuur naar Microsoft Lync/Skype wordt gebeld, wordt de DNS-zone van uw Expressway-E-verbinding gevolgd door Skype. Vervolgens wordt onmiddellijk een (504) Time-outfout voor server geplaatst, zichtbaar op de **Status > Search History** van expressway-E:

```
2017-03-02T08:10:46.240+01:00 sip@vcse sip@vcse Microsoft Ki/ Server time-out 100
```

- Wanneer een telefoontje van Microsoft Lync/Skype wordt naar uw UC-infrastructuur, ziet u de oproep niet die op de Expressway-E wordt ontvangen zoals weergegeven op de **Status > Zoeken Geschiedenis** van expressway-E.

In dit subdeel wordt uitgelegd hoe u dit scenario kunt verifiëren met behulp van de vastlegging in meer details en kunt u controleren wat er precies verkeerd is ingesteld.

Bel naar Microsoft Lync/Skype

In deze call flow zie je in de diagnostische houtkap van de Expressway-E de SIP INVITE die naar Skype gaat (als deze de **_sipfederationtls** kan oplossen. **_tcp** SRV record naar een FQDN en IP), direct gevolgd door een **504 Time-out** reactie op de server zonder verdere details zoals te zien op het volgende logfragment:

```
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:stejjanss@skype.lab>;tag=C65A7B0A8766A5F1D386474833D07882
Server: RTC/6.0
Content-Length: 0
```

Deze respons wordt ook weergegeven (zonder verdere informatie) ongeacht of het een fout is op de DNS-records of op het servercertificaat van de Expressway-E.

U moet de vastlegging van de Lync/Skype Edge-server dus gedetailleerd bekijken, zodat u de waarschuwingen en fouten kunt zien, afhankelijk van de mogelijke fouten die zich voordoen:

- Mogelijke fout: Het FQDN-resultaat van SRV-record komt niet exact overeen met het domein zoals in de header **From/P-Asserted-Identity** van INVITE die via Skype wordt ontvangen. In dit logfragment bevat de **From/P-Asserted-Identity** header van SIP INVITE **acano.steven.lab** als domein, maar **_sipfederationtls._tcp.acano.steven.lab** wijst naar **vcse.steven.lab** in plaats van **vcse.acano.steven.steven.:**

```
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
```

- Mogelijke fout: Het certificaat van de expressway-E server bevat niet de FQDN resulteerde uit het `_sipfederationtls._tcp` SRV record. Dezelfde SIP INVITE wordt verstuurd en `_sipfederationtls._tcp.acano.steven.lab` wijst naar `vcse.acano.steven.lab`, maar dat FQDN niet is opgenomen in de certificaat SAN-lijst van de Expressway-E server:

```
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
```

Bel Microsoft Lync/Skype

Voor deze gespreksstroom zie je niet veel in de vastlegging van de expressway-E, omdat de Skype Edge-server geen INVITE uitstuurt en u afhankelijk moet zijn van de Skype-vastlegging. Gebruik de bestandsindeling van de Lync/Skype (Edge)-server of de Lync/Skype-client-houtkap zelf om het probleem grondiger te onderzoeken.

De Skype-client-houtkap op een Windows-pc is op het volgende pad beschikbaar:

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

Het kan handig zijn in het geval van Office365 Skype-gebruikers wanneer er geen directe toegang tot de Skype-servers beschikbaar is. In deze vastlegging kan je het SIP INVITE bericht zien dat door de client wordt verstuurd en de juiste reactie daarop.

Als u problemen ondervindt met DNS- of certificeringsvereisten op Skype zoals in dit document, ontvangt u de **time-out-reacties** van de **504-server** (inclusief een reden voor de fout) van de Skype-servers:

- Mogelijke fout: Het FQDN-resultaat van SRV-record komt niet exact overeen met het domein dat probeert te worden aangeroepen. Dit logfragment toont een poging om naar een gebruiker of ruimte te bellen met domein `cms.steven.lab` en de `_sipfederationtls._tcp.cms.steven.lab` wijst naar `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

- Mogelijke fout: Het sneltoets-E server certificaat bevat niet de FQDN resulterend uit het SRV_sipfederationtls._tcp SRV record. Dit logfragment toont poging om naar een gebruiker of ruimte met domein cms.steven.lab te bellen waarvoor _sipfederationtls._tcp.cms.steven.lab correct heeft opgelost ven.lab maar deze FQDN zit niet in de Alternatieve Naam Onderwerp op het certificaat van de server van Expressway-E (met **Gemeenschappelijke Naam** als vcse.steven.lab):

SIP/2.0_504 Server time-out Authentication-Info: TLS-DSK qop="auth", opaque="FA404B9C",
srand="1D8F66EF", snum="49", rspauth="67836c7ffc0f6132b2304006969a219d9252aab",
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

Gerelateerde informatie

- [Cisco Express Gateway Series configuratie-gidsen](#)