

Configurer et dépanner DNS et les exigences de certificat sur Microsoft Federation par l'intermédiaire d'Expressway vers le serveur de réunion Cisco

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Informations générales](#)

[Configuration](#)

[Diagramme du réseau](#)

[DNS](#)

[Certificat](#)

[Dépannage](#)

[Révision des symptômes et des journaux](#)

[Appel vers Microsoft Lync/Skype](#)

[Appel de Microsoft Lync/Skype](#)

[Informations connexes](#)

Introduction

Ce document décrit les exigences de certification et en matière de DNS de Microsoft Lync/Skype Entreprise pour une fédération entre différents domaines sur Internet.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco Expressway
- Serveur de réunion Cisco (CMS)
- Serveur Microsoft Lync ou Skype Enterprise
- Gestionnaire de communications unifiées de Cisco (CUCM)

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco Expressway x8.9 ou version ultérieure
- Serveur de réunion Cisco (CMS) 2.1.2 ou version ultérieure
- Serveur Microsoft Lync 2010, serveur Lync 2013 ou serveur Skype for Business - sur site ou hébergé dans le nuage (Office 365)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

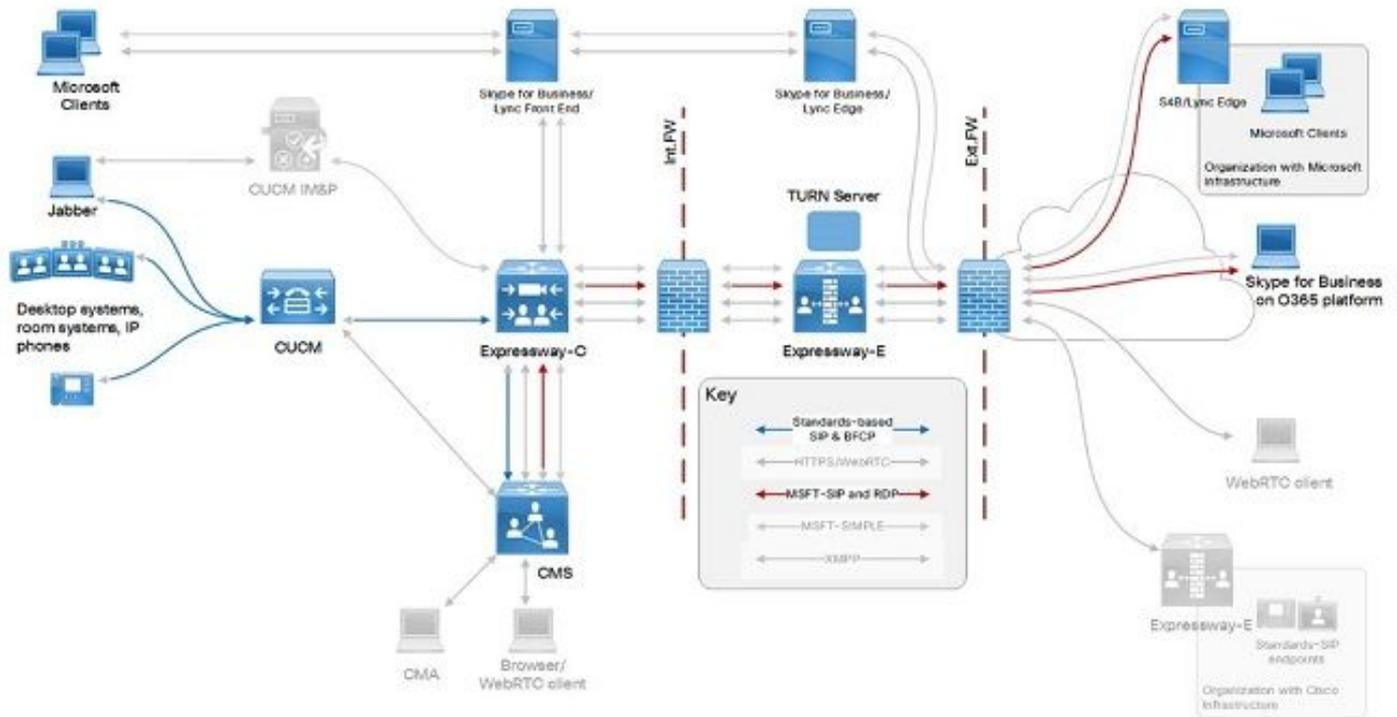
Ce document met en évidence un aspect spécifique de l'intégration avec les clients Microsoft externes dans votre infrastructure Cisco à l'aide d'Expressway et du serveur de réunion Cisco (CMS). La configuration pour cette intégration est comme indiqué dans la documentation sur les **options de Cisco Expressway avec le serveur de réunion Cisco (CMS) ou l'infrastructure Microsoft qui est disponible pour votre version dans la liste des guides de configuration [Cisco Expressway Series](#).**

Le document actuel se concentre uniquement sur les exigences de certification et en matière de DNS de Microsoft Lync ou Skype Entreprise pour fédération externe. Les autres configurations sont abordées dans le guide de configuration mentionné ci-dessus.

Configuration

Un exemple du flux d'appels et de sa configuration peut être celui d'un point d'accès CUCM enregistré qui appelle vers un client Skype (sur site ou hors site, ou enregistré dans le nuage à l'aide d'Office 365), ou vice-versa, en utilisant le CMS pour la conversion entre le standard SIP et le protocole de Microsoft. Cela est possible par l'intermédiaire de l'intégration et du routage d'appels à l'aide de serveurs Expressway, comme illustré dans l'image ci-dessous, qui provient du guide de configuration des **options de Cisco Expressway avec le serveur de réunion Cisco (CMS) ou l'infrastructure Microsoft** mentionné à la fin de ce document.

Diagramme du réseau



Note: Il s'agit uniquement d'un exemple de scénario de flux d'appels. D'autres scénarios d'appels sont aussi possibles.

DNS

Microsoft Lync/Skype Entreprise utilise l'enregistrement SRV `_sipfederationtls._tcp.<domain>` afin de détecter les serveurs de fédération externes vers lesquels envoyer les appels (ainsi que l'information sur la présence); ou pour les fonctionnalités de rappel basées sur le domaine qui est indiqué dans l'en-tête `From/P-Asserted-Identity` de l'invitation SIP entrante. Dans ce scénario, les enregistrements DNS doivent être disponibles dans le DNS public des deux domaines pour qu'ils puissent se fédérer l'un avec l'autre.

La partie domaine du FQDN (nom de domaine complet) qui est renvoyée par la consultation d'enregistrement SRV pour le domaine doit correspondre exactement (aucun autre domaine ou sous-domaine n'est autorisé). Le tableau suivant présente un exemple de configuration DNS pour le domaine avec le nom `example.com` :

Enregistrement SRV `_sipfederationtls._tcp.example.com` `expe.example.com`
 Un enregistrement `expe.example.com` Adresse IP Expressway-E

Attention : L'enregistrement A où le SRV mène doit correspondre exactement au domaine configuré. Les sous-domaines (par exemple `expe.sub.example.com`) ou les domaines différents (`expe.dummy.com`) ne seront pas approuvés par Microsoft Lync/Skype Entreprise et entraîneront des échecs d'appel même s'ils ont des enregistrements A appropriés et une résolution pour corriger les adresses IP.

Certificat

Microsoft Lync/Skype Entreprise configure une connexion TLS entre les domaines configurés sur

les côtés Lync et Expressway. Microsoft Lync/Skype Entreprise a les exigences de certificats de serveur suivantes pour la fédération et les serveurs avec lesquels elle communique (Expressway-E dans ce document) :

- Le certificat du serveur présenté par le serveur correspondant à l'enregistrement A doit avoir le **nom de domaine complet (FQDN) contenu dans son autre nom du sujet (SAN) (ou nom usuel**, si l'on n'utilise pas le SAN)
- Les serveurs de Microsoft Lync/Skype Entreprise doivent faire confiance au certificat du serveur présenté par le serveur (soit signé par une autorité de certification publique, ou une autorité de certification privée dont les certificats racine/intermédiaires ont été importés dans la **liste des autorités de certification de confiance des** serveurs de Microsoft Lync/Skype Entreprise). Prenez note que lorsque vous utilisez Office 365, des certificats signés par une autorité de certification publique sont exigés.

Exemple :

Le certificat du serveur du serveur Expressway-E correspondant à **expe.example.com**, comme indiqué dans l'exemple ci-dessus, doit avoir les entrées minimales suivantes :

- (Uniquement s'il n'y a aucun **autre nom du sujet [SAN]**) le nom usuel doit être **expe.example.com**
- (Si d'autres noms du sujet sont disponibles) L'autre nom du sujet (SAN) doit contenir une entrée **expe.example.com**
- L'émetteur au sommet de l'arborescence du certificat doit être une autorité de certification publique (sans quoi l'autorité de certification devrait être ajoutée dans la **liste d'autorités de certification de confiance des serveurs Microsoft Lync/Skype**)

Note:

Le domaine (exemple.com) en lui-même n'a pas besoin d'être inclus en tant que **Nom alternatif d'objet**.

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

La section contient des informations sur la journalisation et des traces qui sont prises d'un déploiement de laboratoire de test avec les conditions suivantes :

- Le domaine de Skype est **skype.lab**
- Le domaine UC (Expressway-E, Expressway-C et CUCM) est **steven.lab**
- Le domaine CMS pour les utilisateurs et les espaces est **acano.steven.lab** (**cms.steven.lab** est aussi disponible)

Comme il est recommandé d'utiliser un domaine distinct pour votre serveur de réunion Cisco (différent de votre autre domaine UC sur UCM/Expressway), il est probable que vous ayez un autre domaine sur votre serveur Expressway-E et cela pourrait mener à des problèmes d'intégration liés aux exigences sur la fédération SIP du côté du serveur de Microsoft Lync/Skype Entreprise.

Révision des symptômes et des journaux

Lorsque les exigences envers les certificats DNS ne sont pas rencontrées du côté du serveur de Microsoft Lync/Skype, vous remarquerez les symptômes suivants :

- Lorsqu'un appel est passé à partir de votre infrastructure UC vers Microsoft Lync/Skype, vous verrez l'appel sortant sur la zone DNS de votre Expressway-E vers Skype, mais affichant immédiatement une erreur de délai d'attente du serveur (504), bien visible sur la page **Status > Search History (État > Historique de recherche) dans Expressway-E** :

```
2017-03-02T08:10:46.240+01:00 sip (INVITE) sip.stejanss@skype.lab Microsoft #/ Server time-out 100%
```

- Lorsqu'un appel est passé à partir de Microsoft Lync/Skype vers votre infrastructure UC, vous ne voyez pas l'appel arriver sur Expressway-E, comme indiqué à la page **Status > Search History (État > Historique de recherche) de Expressway-E**.

Cette sous-section explique plus en détail comment vérifier ce scénario à l'aide de la journalisation et vérifier exactement ce qui est mal configuré.

Appel vers Microsoft Lync/Skype

Dans ce flux d'appels, vous voyez dans la journalisation de diagnostic de l'Expressway-E l'invitation SIP sortir vers Skype (si elle peut mener l'enregistrement SRV **_sipfederationtls._tcp** vers un FQDN et une IP), immédiatement suivie d'une erreur 504 de délai d'attente de serveur comme réponse sans détails supplémentaires, comme indiqué sur l'extrait de journalisation suivant :

```
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 même réponse est affichée (sans détails supplémentaires), que ce soit pour une défaillance sur les enregistrements DNS, ou sur le certificat du serveur de l'Expressway-E.

Donc, pour une révision plus en détail, vous devez examiner les journaux du serveur de Lync/Skype Edge, où vous pouvez voir les avertissements et les erreurs en fonction des défaillances possibles :

- Défaillance possible : Le résultat du nom de domaine complet (FQDN) de l'enregistrement SRV ne correspond pas exactement sur le domaine en tant que l'en-tête **From/P-Asserted-**

Identity de l'invitation entrante sur Skype. Dans cet extrait de journal, l'en-tête From/P-Asserted-Identity de l'invitation SIP contient acano.steven.lab en tant que domaine, mais `_sipfederationtls._tcp.acano.steven.lab` pointe vers `vcse.steven.lab` au lieu de `vcse.acano.steven..` ::

```
TL WARN(TF DIAG) [sfvedge\svedge]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
```

- Défaillance possible : Le certificat du serveur d'Expressway-E ne contient pas le FQDN entraîné par l'enregistrement SRV `_sipfederationtls._tcp`. La même invitation SIP est envoyée et `_sipfederationtls._tcp.acano.steven.lab` pointe vers `vcse.acano.steven.lab`, mais ce FQDN n'est pas contenu dans la liste de SAN du certificat du serveur d'Expressway-E :

```
TL ERROR(TF DIAG) [sfvedge\svedge]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
```

Appel de Microsoft Lync/Skype

Pour ce flux d'appel, vous ne voyez pas beaucoup de la journalisation d'Expressway-E puisque le serveur de Skype Edge n'envoie pas l'invitation et vous devez vous fier à la journalisation de Skype. Utilisez soit la journalisation du serveur de Lync/Skype (Edge), soit la journalisation des clients elle-même pour examiner le problème plus en profondeur.

La journalisation des clients de Skype sur un PC Windows est disponible au chemin suivant :

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

Il peut s'avérer utile dans le cas des utilisateurs de Skype avec Office 365 lorsqu'aucun accès direct aux serveurs de Skype n'est disponible. Dans cette journalisation, vous pouvez voir l'invitation SIP envoyée par le client et la réponse appropriée pour cela.

Si vous rencontrez des problèmes avec les exigences de certification et en matière de DNS sur Skype comme décrit dans ce document, vous recevez des réponses **d'erreur 504 de délai d'attente de serveur (y compris une raison pour la défaillance) des serveurs de Skype** :

- Défaillance possible : Le résultat du nom de domaine complet (FQDN) de l'enregistrement SRV ne correspond pas exactement sur le domaine que l'on tente d'appeler. Cet extrait de journal indique une tentative d'appel à un utilisateur ou un espace avec le domaine `cms.steven.lab` et le `_sipfederationtls._tcp.cms.steven.lab` pointe vers à `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

- Défaillance possible : Le certificat du serveur d'Expressway-E ne contient pas le FQDN entraîné par l'enregistrement SRV **_sipfederationtls._tcp**. Cet extrait de journal montre une tentative de numérotation vers un utilisateur ou un espace avec le domaine **cms.steven.lab** pour lequel **_sipfederationtls._tcp.cms.steven.lab** résout correctement en **vcse.cms.steven.lab** mais ce nom de domaine complet ne figure pas dans les noms de remplacement d'objet sur le certificat du serveur Expressway-E (avec CommonName) **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

Informations connexes

- [Guides de configuration de la gamme Expressway de Cisco](#)