

# Configurez et dépannez les DN et délivrez un certificat les conditions requises sur la fédération de Microsoft par l'intermédiaire de l'autoroute à Cisco rencontrant le serveur

## Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Informations générales](#)

[Configurez](#)

[Diagramme du réseau](#)

[DN](#)

[Certificat](#)

[Dépannez](#)

[Examen de symptômes et de log](#)

[Appel vers Microsoft Lync/Skype](#)

[Appel de Microsoft Lync/Skype](#)

[Informations connexes](#)

## Introduction

Ce document décrit les DN et les conditions requises de certificat de Microsoft Lync/Skype pour l'entreprise pour une fédération entre différents domaines au-dessus de l'Internet.

## Conditions préalables

### Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Autoroute de Cisco
- CMS (Cisco rencontrant le serveur)
- Microsoft Lync ou Skype pour le business server
- CUCM (Cisco Unified Communications Manager)

### [Composants utilisés](#)

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

- Autoroute X8.9 de Cisco ou plus tard
- Cisco rencontrant le serveur (CMS) 2.1.2 ou plus tard
- Serveur de Microsoft Lync 2010, serveur de Lync 2013 ou Skype pour le business server - sur-prem ou hébergé dans le nuage (Office365)

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est vivant, assurez-vous que vous comprenez l'impact potentiel de n'importe quelle commande.

## Informations générales

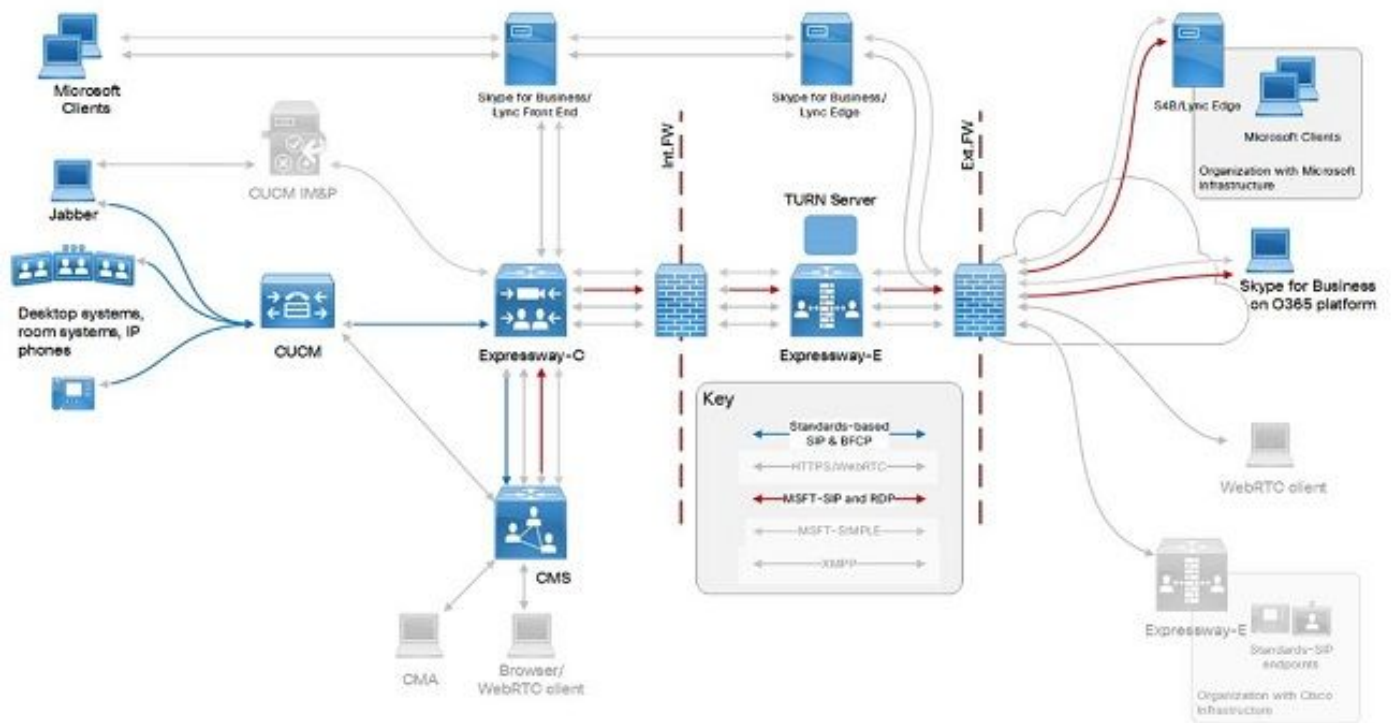
Le document met en valeur un aspect spécifique de l'intégration avec les clients externes de Microsoft avec votre infrastructure Cisco utilisant l'autoroute et le Cisco rencontrant le serveur (CMS). La configuration pour cette intégration est comme expliqué dans les **options d'autoroute de Cisco avec Cisco rencontrant la documentation de serveur et/ou d'infrastructure de Microsoft** qui est disponible pour votre version à la liste de [guides de configuration de gamme d'autoroute de Cisco](#).

Le présent document se concentre seulement sur les DN et les conditions requises de certificat sur Microsoft Lync ou le Skype pour l'extrémité d'affaires pour la fédération externe. Les autres configurations sont couvertes dans le guide de configuration ci-dessus référencé.

## Configurez

Un exemple pour l'écoulement d'appel et sa configuration peut être un point final enregistré par CUCM qui compose à Skype un client (sur-prem ou off-prem, ou enregistré dans le nuage utilisant Office365), ou vice versa - utilisant le CMS pour la conversion entre le SIP standard et le protocole de Microsoft. C'est possible par l'intégration et le routage d'appels utilisant des serveurs d'autoroute, suivant les indications de l'image ci-dessous, qui est prise des **options d'autoroute de Cisco avec Cisco rencontrant le guide de configuration de serveur et/ou d'infrastructure de Microsoft** référencé à la fin de ce document.

## Diagramme du réseau



Remarque: C'est juste un scénario exemplaire d'écoulement d'appel. D'autres scénarios d'appel sont également possibles.

## DN

Microsoft Lync/Skype pour l'entreprise emploie l'enregistrement SRV des **\_sipfederationtls.\_tcp.<domain>** afin de découvrir les serveurs externes de fédération auxquels pour envoyer les appels (aussi bien que les informations de présence) ; ou pour la fonctionnalité de rappel de service basée sur le domaine qui est spécifié dans l'**en-tête From/P-Asserted-Identity** du **SIP INVITE** entrant. Dans ce scénario, les enregistrements DNS doivent être disponibles aux DN publics pour les deux domaines afin de se fédérer entre l'un l'autre.

La partie de domaine du **FQDN** (nom de domaine complet) qui est retourné par la consultation d'enregistrement SRV pour le domaine doit s'assortir exactement (on ne permet aucun autre domaine ou sous-domaine). Le tableau suivant affiche un exemple pour la 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 d'autoroute-e**

**Attention** : L'enregistrement A au lequel le SRV le résout, doit être un précis - appariez sur le domaine configuré. Les sous-domaines (par exemple **expe.sub.example.com**) ou les différents domaines (**expe.dummy.com**) pas sont de confiance par Microsoft Lync/Skype pour l'entreprise et ceci aura comme conséquence les échecs d'appel quoiqu'ils puissent avoir les enregistrements appropriés et la résolution A pour corriger l'IPS.

## Certificat

Microsoft Lync/Skype pour l'entreprise a installé une connexion de TLS entre les domaines

configurés des côtés de Lync et d'autoroute. Microsoft Lync/Skype pour l'entreprise a les conditions requises suivantes de Certificats de serveur pour la fédération et les serveurs qu'elle communique avec (autoroute-e dans ce document) :

- Le certificat de serveur présenté par le serveur appartenant l'enregistrement A doit avoir que le **FQDN** particulier contenu dans son **nom alternatif soumis** (ou **nom commun**, sinon utilisant le SAN)
- Le certificat de serveur présenté par le serveur a besoin sont de confiance par Microsoft Lync/Skype pour des business servers (signé par un public le CA, ou par la racine privée CA lequel/Certificats intermédiaires obtient importé dans la **liste de confiance CA de Microsoft Lync/Skype pour des business servers**). Notez cela en utilisant Office365, public que des Certificats signés CA sont exigés.

Exemple :

Le certificat de serveur du serveur d'autoroute-e appartenant **expe.example.com** comme affiché de l'exemple ci-dessus, doit avoir les entrées minimum suivantes :

- (Seulement si aucun **noms alternatifs soumis**) le **nom commun** doit être **expe.example.com**
- (Si **soumis les noms alternatifs** sont disponibles) le **nom alternatif de sujet** doit contenir une **entrée expe.example.com**
- L'émetteur du dessus de l'arborescence de certificat doit être un public CA (ou le CA devrait être ajouté dans la **liste de confiance CA des** serveurs de Microsoft Lync/Skype)

Remarque:

Le domaine (example.com) sur lui-même n'a pas besoin d'être inclus comme **nom de SubjectAlternative**.

## Dépannez

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

La section contient les informations de journalisation et les suivis qui sont pris d'un déploiement de laboratoire de test avec les caractéristiques suivantes :

- Le domaine de Skype est skype.lab
- Le domaine UC (autoroute-e, autoroute-C et CUCM) est steven.lab
- Le domaine CMS pour des utilisateurs et des espaces est acano.steven.lab (cms.steven.lab est également disponible)

Pendant qu'il est recommandé pour utiliser un domaine distinct pour votre Cisco rencontrant le serveur (différent de votre autre domaine UC sur UCM/Expressway), il est probable que vous ayez un domaine différent sur votre serveur d'autoroute-e et ceci pourrait mener au problème lié d'intégration avec les conditions requises sur la fédération de SIP sur Microsoft Lync/Skype pour le côté du business server.

## Examen de symptômes et de log

Quand les conditions requises sur des Certificats de DN ne sont pas appariées sur le côté serveur de Microsoft Lync/Skype, vous notez les symptômes suivants :

- Quand un appel est fait à partir de votre infrastructure UC vers Microsoft Lync/Skype, vous voyez l'appel sortant sur la zone DNS de votre autoroute-e à Skype, mais des 504) erreurs immédiatement de lancement de délai de temporisation du serveur a (, visibles à la page **d'historique d'état > de recherche de l'autoroute-e** :

2017-03-08 15:42:02 SIP (INVITE) sip.stejanss@skype.lab Microsoft AV Server time-out X64

- Quand un appel est fait à partir de Microsoft Lync/Skype vers votre infrastructure UC, vous ne voyez pas l'appel arriver sur l'autoroute-e comme affiché à la page **d'historique d'état > de recherche de l'autoroute-e**.

Ce paragraphe explique comment vérifier ce scénario utilisant ouvrir une session plus de détails et de contrôle ce qui exactement misconfigured.

## Appel vers Microsoft Lync/Skype

Dans cet écoulement d'appel, vous voyez dans se connecter diagnostique de l'autoroute-e le SIP INVITE sortant vers Skype (s'il peut résoudre l'enregistrement SRV de **\_tcp de \_sipfederationtls. à un FQDN et à un IP**), immédiatement suivi d'une réponse de **minuterie de 504 serveurs** sans tout autre détail comme affiché sur l'extrait se connectant 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 toutes informations supplémentaires) sans se soucier si c'est un défaut sur les enregistrements DNS, ou sur le certificat de serveur de l'autoroute-e.

Ainsi pour le passer en revue plus en détail, vous devez regarder dans le serveur de périphérie de Lync/Skype se connectant, où vous pouvez voir les avertissements et les erreurs selon les défauts de occurrence possibles :

- Défaut possible : Les résultats FQDN de l'enregistrement SRV ne s'assortissent pas exactement sur le domaine comme dans l'**en-tête From/P-Asserted-Identity** de l'INVITATION entrante à Skype. Dans cet extrait de log, l'**en-tête From/P-Asserted-Identity** du SIP INVITE contient **acano.steven.lab** comme domaine, mais les **\_sipfederationtls. \_tcp.acano.steven.lab** indique **vcse.steven.lab** au lieu de **vcse.acano.steven.lab** :

```
(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
```

- Défaut possible : Le certificat de serveur d'autoroute-e ne contient pas le FQDN a résulté de l'enregistrement SRV de **\_tcp de \_sipfederationtls**. Le même SIP INVITE est envoyé et les **\_sipfederationtls. \_tcp.acano.steven.lab** indique vcse.acano.steven.lab, mais ce FQDN n'est pas contenu dans la liste du certificat de serveur d'autoroute-e SAN :

```
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 cet écoulement d'appel vous ne voyez pas beaucoup dans se connecter de l'autoroute-e car le serveur de périphérie de Skype n'envoie pas l'INVITATION et vous devez compter sur se connecter de Skype. Utilisez le serveur de Lync/Skype (périphérie) se connectant, ou le client de Lync/Skype se connectant pour étudier la question dans plus de profondeur.

Le client de Skype ouvrant une session 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 être utile dans le cas des utilisateurs Skype Office365 quand aucun accès direct aux serveurs de Skype n'est disponible. En ce se connecter, vous pouvez voir le message de SIP INVITE envoyé par le client et la réponse appropriée pour celui.

Si vous vous exécutez dans des questions avec des DN ou délivrez un certificat des conditions requises sur Skype selon ce document, vous recevez les **504** réponses de **minuterie de serveur** (raison y compris de la panne) des serveurs de Skype :

- Défaut possible : Les résultats FQDN de l'enregistrement SRV ne s'assortissent pas exactement sur le domaine essayé pour s'appeler. Cette tentative d'expositions d'extrait de log de composer à un utilisateur ou à un espace avec le domaine **cms.steven.lab** et les **\_sipfederationtls. \_tcp.cms.steven.lab** indique **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" <sip:stejanss@skype.lab>;tag=280f2bf329;epid=c21eec507a To:
<sip:stejanss.space@cms.steven.lab>;tag=98283FD4A66E24FFB4967CDB73149B25 Call-ID:
d0bce97cce8a45fcbb8cc973ba0282da CSeq: 1 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
```

- Défaut possible : Le certificat de serveur d'autoroute-e ne contient pas le FQDN a résulté de l'enregistrement SRV de **\_tcp de \_sipfederationtls**. Cette tentative d'expositions d'extrait de

log de composer à un utilisateur ou à un espace avec le domaine **cms.steven.lab** pour lequel les **\_sipfederationtls.\_tcp.cms.steven.lab** les résout correctement à **vcse.cms.steven.lab** mais à ce FQDN notcontained dans les noms alternatifs soumis sur le **certificat de serveur d'autoroute-e (avec le nom commun comme 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"<sip:stejanss@skype.lab>;tag=a1ea5f9a46;epid=c21eec507a To:
<sip:stejanss.space@cms.steven.lab>;tag=B7D9BF35417873B07792AAD244E6B230 Call-ID:
5e38e39898cf40188170f0d70644a87b CSeq: 1 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_PRINCI
PAL)";source="sip.skype.lab" Server: RTC/6.0 Content-Length: 0
```

## [Informations connexes](#)

- [Guides de configuration de gamme d'autoroute de Cisco](#)