

Appels URI SIP Jabber sur MRA

Contenu

[Introduction](#)

[Scénario](#)

[Hypothèses](#)

[Configuration de l'organisation 1 lorsque Jabber A appelle Jabber B](#)

[Le flux d'appels sortants global devient](#)

[Configuration de l'organisation 1 lorsque Jabber B appelle Jabber A](#)

[Le flux d'appels entrants globaux devient](#)

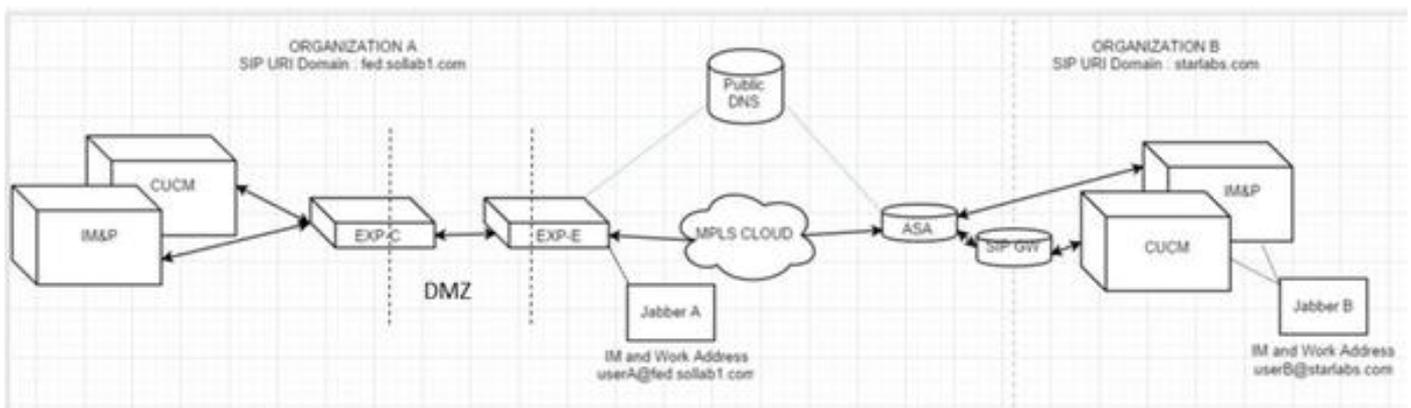
Introduction

Ce document décrit la configuration impliquée sur Cisco Unified Communications Manager (CUCM) et Expressway C et E afin que jabber puisse appeler l'URI (Uniform Resource Identifier) SIP (Session Initiation Protocol) d'un autre utilisateur d'une autre organisation lorsqu'il est connecté via l'accès distant mobile (MRA). La même chose dans le contexte d'Expressway est également appelée flux d'appels B2B.

Scénario

Supposons un scénario dans lequel l'organisation 1 déploie MRA et l'organisation 2 non. Pour l'organisation 2, le périmètre se termine par un dispositif de sécurité adaptatif (ASA), au-delà duquel CUBE est intégré à la grappe CUCM de l'organisation 2.

Comme l'illustre l'image, Jabber A peut être connecté via MRA ou en interne, mais la configuration reste la même sur CUCM, Expressway C et E, pour l'organisation 1.



Hypothèses

Vous pouvez supposer que l'utilisateur Jabber A et l'utilisateur Jabber B sont capables d'échanger

des messages instantanés et de la présence via la fédération XMPP (Extensible Messaging and Presence Protocol), et que leurs adresses de messagerie instantanée sont également leurs URI SIP de travail.

En outre, Jabber A et Jabber B peuvent composer un numéro via l'URI SIP en interne, au sein de leur organisation respective, avec succès.

Dans le scénario ci-dessus, vous supposez que l'organisation 2 a CUCM comme serveur de contrôle d'appels. Cependant, il peut également s'agir d'un serveur de contrôle d'appels d'un autre fournisseur.

Il faut connaître la version tout en intégrant CUCM, Jabber, VCS pour MRA.

Configuration de l'organisation 1 lorsque Jabber A appelle Jabber B

Étape 1. Créez un nouveau profil de sécurité de liaison SIP, dont le port d'écoute est 5065, comme illustré sur l'image :

SIP Trunk Security Profile Configuration

Save Delete Copy Reset Apply Config Add New

Status: Ready

SIP Trunk Security Profile Information

Name*	VCS SIP Trunk Profile
Description	VCS SIP Trunk Profile non-secure
Device Security Mode	Non Secure
Incoming Transport Type*	TCP+UDP
Outgoing Transport Type	TCP
<input type="checkbox"/> Enable Digest Authentication	
Nonce Validity Time (mins)*	600
X.509 Subject Name	
Incoming Port*	5065
<input type="checkbox"/> Enable Application level authorization	
<input type="checkbox"/> Accept presence subscription	
<input type="checkbox"/> Accept out-of-dialog refer**	
<input checked="" type="checkbox"/> Accept unsolicited notification	
<input checked="" type="checkbox"/> Accept replaces header	
<input type="checkbox"/> Transmit security status	
<input type="checkbox"/> Allow charging header	
SIP V.150 Outbound SDP Offer Filtering*	Use Default Filter

Étape 2. Créez une ligne principale SIP pointant vers ExpressWay-C et affectez le profil de sécurité de la ligne principale SIP, comme illustré sur l'image :

SIP Information

- Destination

Destination Address is an SRV

Destination Address	Destination Address IPv6	Destination Port
1* 10.106.82.114		5060

MTP Preferred Originating Codec* 711ulaw ▼

BLF Presence Group* Standard Presence group ▼

SIP Trunk Security Profile* VCS SIP Trunk Profile ▼

Rerouting Calling Search Space < None > ▼

Out-Of-Dialog Refer Calling Search Space < None > ▼

SUBSCRIBE Calling Search Space < None > ▼

SIP Profile* Standard SIP Profile For Cisco VCS ▼ [View Details](#)

DTMF Signaling Method* RFC 2833 ▼

- Normalization Script

Note: Un nouveau profil de sécurité de liaison est créé qui écoute le port 5065. Il est affecté à cette nouvelle ligne principale SIP pointant vers Expressway-C parce qu'Expressway-C est déjà configuré pour envoyer des enregistrements Jabber non sécurisés sur 5060 à CUCM lorsque l'utilisateur Jabber se connecte via MRA. Si vous utilisez le profil de sécurité de liaison par défaut, jabber connecté via MRA ne parvient pas à s'enregistrer sur le port 5060 de CUCM.

Étape 3. Créez le modèle de routage SIP pour l'URI de l'organisation 2 et attribuez-le au point de liaison SIP à Expressway-C, comme l'illustre l'image :

SIP Route Pattern Configuration



Save



Delete



Copy



Add New

Status



Status: Ready

Pattern Definition

Pattern Usage	Domain Routing
IPv4 Pattern*	<input type="text" value="starlabs.com"/>
IPv6 Pattern	<input type="text"/>
Description	<input type="text" value="VCS MRA calls"/>
Route Partition	<input type="text" value=" < None >"/>
SIP Trunk/Route List*	<input type="text" value="VCS-MRA-TRNK"/>
<input type="checkbox"/> Block Pattern	

Étape 4. Créez une zone de voisinage sur Expressway-C pointant vers CUCM, comme l'illustre l'image :

Configuration

Name	CUCM-ORG1
Type	Neighbor
Hop count	15

H.323

Mode	Off
------	-----

SIP

Mode	On
Port	5065
Transport	TCP
Accept proxied registrations	Deny
Media encryption mode	Auto
ICE support	Off

Étape 5. Créez une zone de client de traverse sur l'Expressway-C (pas une traverse UC), comme le montre l'image :

EDIT 2016

Type	Traversal client
Hop count	★ 15 ⓘ

Connection credentials

Username	★ cisco ⓘ
Password	★ ●●●●●●●● ⓘ

H.323

Mode	Off ⓘ
------	-------

SIP

Mode	On ⓘ
Port	★ 7003 ⓘ
Transport	TCP ⓘ
Accept proxied registrations	Allow ⓘ
Media encryption mode	Auto ⓘ
ICE support	Off ⓘ
SIP noison mode	Off ⓘ

Étape 6. Créez une zone de serveur de traverse sur l'Expressway-E (pas une traverse UC), comme illustré sur l'image :

Edit zone

Type	Traversal server
Hop count	★ 15 ⓘ

Connection credentials	
Username	★ cisco ⓘ
Password	Add/Edit local authentication database

H.323	
Mode	Off ⓘ

SIP	
Mode	On ⓘ
Port	★ 7003 ⓘ
Transport	TCP ⓘ
Accept proxied registrations	Allow ⓘ
Media encryption mode	Auto ⓘ
ICE support	Off ⓘ
...	Off ⓘ

Étape 7. Créez une zone DNS sur Expressway-C, qui sera utilisée pour effectuer une recherche DNS SRV pour l'URI de l'organisation 2, comme l'illustre l'image :

Configuration

Name	★ VCS-MRA-DNS i
Type	DNS
Hop count	★ 15 i

H.323

Mode	Off ▼ i
------	--

SIP

Mode	On ▼ i
TLS verify mode	Off ▼ i
Fallback transport protocol	UDP ▼ i
Media encryption mode	Auto ▼ i
ICE support	Off ▼ i

Une fois toutes les zones créées, vous devez définir des règles de recherche sur Expressway C et E afin que le routage puisse avoir lieu.

Étape 8. La règle de recherche sur Expressway-C consiste à transférer l'**invitation SIP** destinée à l'URI starlabs.com vers Expressway-E, sur la nouvelle zone de traversée que vous avez créée, comme l'illustre l'image :

Configuration

Rule name	★ Inside-to-Outside-MRA-CUCMORG2 i
Description	i
Priority	★ 99 i
Protocol	SIP ▼ i
Source	Any ▼ i
Request must be authenticated	No ▼ i
Mode	Alias pattern match ▼ i
Pattern type	Regex ▼ i
Pattern string	★ .*@starlabs.com\$ i
Pattern behavior	Leave ▼ i
On successful match	Continue ▼ i
Target	★ b2b ▼ i
State	Enabled ▼ i

Étape 9. Règle de recherche sur Expressway-E, pour transférer l'**invitation SIP** destinée à l'URI starlabs.com à la ZONE DNS, une fois que l'appel atteint Expressway-E via la zone de traversée, que vous avez fait, comme illustré dans l'image :

The screenshot shows the configuration for a rule named "CUCM to VCSe to DNS". The rule is enabled and has a priority of 130. It is configured for SIP protocol, using a named source "b2b". The request must not be authenticated. The mode is set to "Alias pattern match" with a "Regex" pattern string of ".*@starlabs.com\$". On a successful match, the action is to "Continue" to the "VCS-MRA-DNS" target.

Rule name	CUCM to VCSe to DNS
Description	VCS MRA calls
Priority	130
Protocol	SIP
Source	Named
Source name	b2b
Request must be authenticated	No
Mode	Alias pattern match
Pattern type	Regex
Pattern string	.*@starlabs.com\$
Pattern behavior	Leave
On successful match	Continue
Target	VCS-MRA-DNS
State	Enabled

Étape 10. Une fois l'appel atteint la zone DNS, Expressway-C effectue une recherche DNS SRV pour **_sips.tcp.starlabs.com**, **_sip._tcp.starlabs.com** et **_sip._udp.starlabs.com** contre le serveur DNS public.

Dans les journaux Exp-E , vous pouvez voir ceci comme :

```
2016-03-09T09:48:35+05:30 VCSECOL tvcs: UTCTime="2016-03-09 04:18:35,399" Module="network.dns" Level="DEBUG": Detail="Sending DNS query" Name="_sip._tcp.starlabs.com" Type="SRV (IPv4 and IPv6) "
```

```
2016-03-09T09:48:35+05:30 VCSECOL tvcs: UTCTime="2016-03-09 04:18:35,400" Module="network.dns" Level="DEBUG": Detail="Resolved hostname to: ['IPv4''TCP''14.160.103.10:5060'] (A/AAAA) Number of relevant records retrieved: 1"
```

À partir de la recherche DNS SRV , Exp-E obtient l'IP et le port pour le saut suivant, pour atteindre l'organisation 2. Dans ce scénario, le DNS SRV **_sip._tcp.starlabs.com** résout au nom de domaine complet public/IP et au port 5060 de l'ASA pour l'organisation 2.

Le flux d'appels sortants global devient

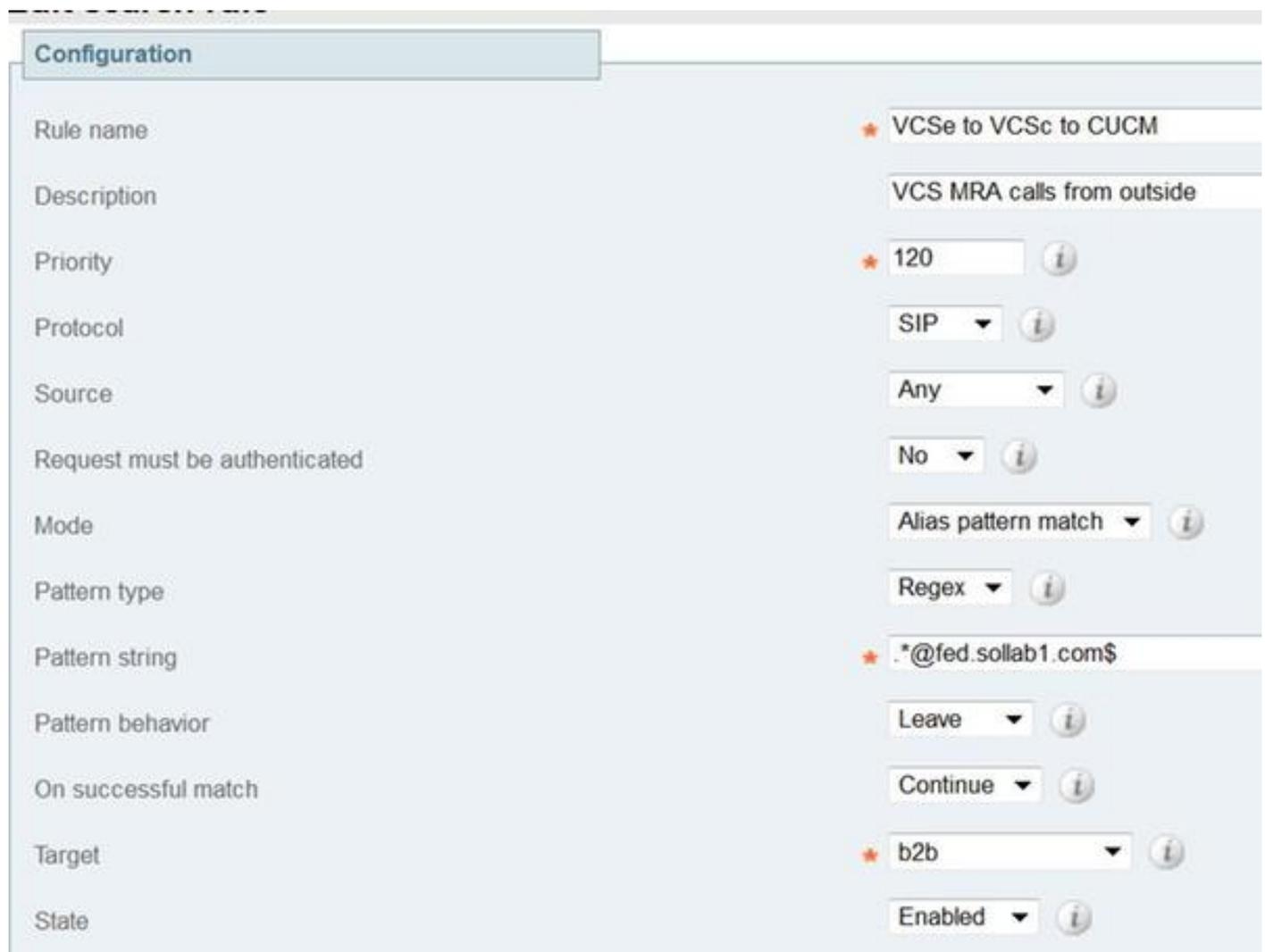
1. Jabber A compose **userB@starlabs.com** en tant qu'URI SIP.
2. SIP Invite atteint CUCM (via Exp-E → Exp-C).
3. CUCM effectue une analyse de chiffres qui correspond au **modèle de route SIP**.
4. CUCM achemine l'appel vers Exp-C via la ligne principale SIP.

5. Exp-C reçoit l'appel sur la zone de voisinage CUCM et la règle de recherche transmet l'appel à la zone de traversée que nous avons effectuée.
6. L'appel atteint maintenant l'Exp-E via la zone de traversée et la règle de recherche transfère l'appel vers la zone DNS.
7. Une fois la zone DNS atteinte, la recherche DNS SRV pour `_sip._tcp.starlabs.com` par rapport au serveur DNS public se produit, ce qui passe au prochain saut pour atteindre l'organisation 2.

Configuration de l'organisation 1 lorsque Jabber B appelle Jabber A

Supposons maintenant que l'organisation 2 a son propre plan de numérotation configuré pour acheminer un appel URI SIP vers l'organisation 1, lorsque jabber B appelle Jabber A. Voyons les modifications nécessaires pour obtenir l'invitation SIP entrante, acheminée vers CUCM de l'organisation 1.

Étape 1. Règle de recherche entrante sur Expressway-E, pour l'envoi d'une invitation SIP entrante de l'organisation 2 vers Exp-C, pour le domaine URI SIP **fed.sollab1.com**, comme illustré dans l'image :



The screenshot shows the configuration page for a rule named "VCSe to VCSc to CUCM". The configuration is as follows:

Field	Value
Rule name	VCSe to VCSc to CUCM
Description	VCS MRA calls from outside
Priority	120
Protocol	SIP
Source	Any
Request must be authenticated	No
Mode	Alias pattern match
Pattern type	Regex
Pattern string	.*@fed.sollab1.com\$
Pattern behavior	Leave
On successful match	Continue
Target	b2b
State	Enabled

Étape 2. Règle de recherche entrante sur Expressway-C, pour l'envoi d'une invitation SIP entrante d'Exp-E à CUCM, pour le domaine URI SIP **fed.sollab1.com**, comme illustré dans l'image :

Configuration	
Rule name	★ Outside-to-Inside-MRA
Description	VCS MRA calls from outside
Priority	★ 98 ⓘ
Protocol	SIP ⓘ
Source	Named ⓘ
Source name	★ b2b ⓘ
Request must be authenticated	No ⓘ
Mode	Alias pattern match ⓘ
Pattern type	Regex ⓘ
Pattern string	★ .*@fed.sollab1.com\$ ⓘ
Pattern behavior	Leave ⓘ
On successful match	Continue ⓘ
Target	★ CUCM-ORG1 ⓘ
State	Enabled ⓘ

Le flux d'appels entrants globaux devient

1. INVITE SIP entrante de Jabber B pour **userA@fed.sollab1.com** atteint Exp-E.
2. La règle de recherche sur Exp-E transfère l'appel vers Exp-C, via la zone de traversée.
3. Règle de recherche sur Exp-C , transfère l'appel au cluster CUCM via la zone voisine CUCM.
4. CUCM envoie l'invitation SIP à Jabber A enregistrée sur MRA (via Exp-C → Exp-E).

Note: Des licences multimédias riches sont nécessaires sur Expressway-C et Expressway-E pour que les appels B2B fonctionnent.

Note: Assurez-vous que les ports appropriés du client sont ouverts sur le pare-feu.