Cisco Meeting Server 및 비즈니스용 Skype 구성

목차

소개

이 문서에서는 공식 가이드 보완 자료로 Skype for Business를 사용하여 Cisco CMS(Meeting Server) CallBridge 클러스터를 구성하는 방법에 대해 설명합니다.이 문서에서는 단일 CallBridge의 예와 세 개의 CallBridge 클러스터의 또 다른 예를 제공하지만 필요에 따라 CallBridges를 추가할 수 있습니다.두 개의 CallBridge 클러스터도 지원됩니다.

기고자: Rogelio Galindo, Viridiana Fuentes, Cisco TAC 엔지니어

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

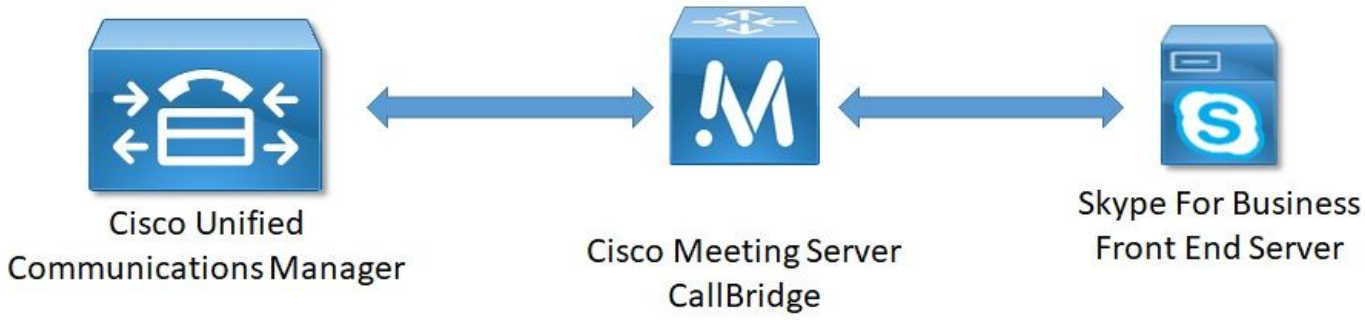
- Cisco CMS(Meeting Server)
- DNS(Domain Name Server)
- 비즈니스용 Skype
- API(Application Programming Interface)

> **참고**:컨피그레이션 가이드는 다음 위치에서 확인할 수 있습니다 .https://www.cisco.com/c/dam/en/us/td/docs/conferencing/ciscoMeetingServer/Deployment_Guide/Version-2-2/Cisco-Meeting-Server-2-2-Scalable-and-Resilient-Deployments.pdf

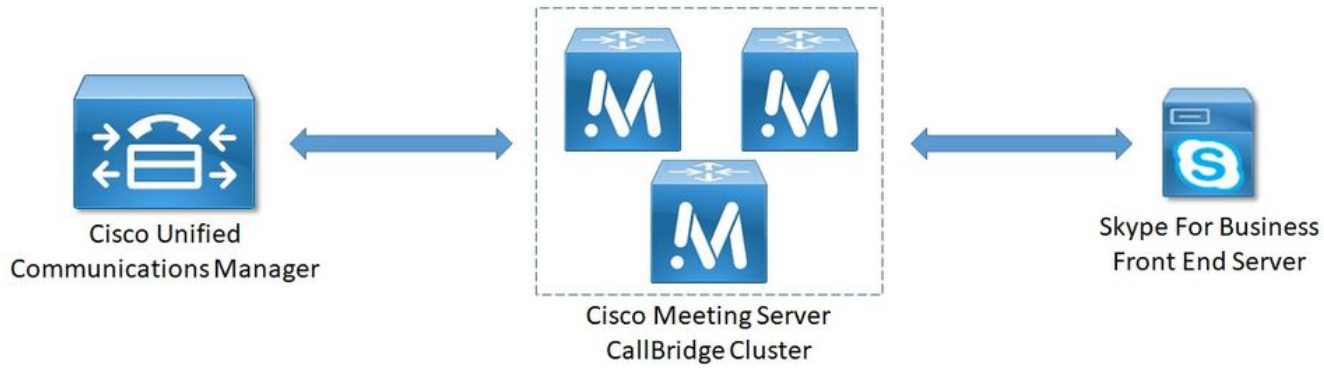
사용되는 구성 요소

- CallBridge 클러스터를 실행하는 CMS 서버 3개, 소프트웨어 버전 2.2.2.
- 비즈니스용 Skype 2015
- AD(Active Directory) Windows Server 2012
- SSH(Secure Shell) 클라이언트
- WinSCP 등의 SFTP(Secure File Transfer Protocol) 클라이언트
- Postman 등의 API 프로그램
- Active Directory, DNS 및 Skype 서버용 원격 데스크톱 세션

네트워크 토폴로지 - 단일 CallBridge



네트워크 토폴로지 - 클러스터링된 CallBridges



Callbridge 인증서 요구 사항 - 단일 CallBridge

표 1a는 단일 CallBridge 환경에 대한 CallBridge 인증서의 예를 제공합니다.

표 1a

CallBridge 인증서	설명
단일 CallBridge	
CN:cms.uc.local	CallBridge FQDN

Callbridge 인증서 요구 사항 - 클러스터링된 CallBridges

표 1b는 클러스터링된 CallBridge 환경에 대한 CallBridge 인증서의 예를 제공합니다.클러스터의 CallBridge 전체에서 단일 인증서를 공유할 수 있습니다.

표 1b

Callbridge 인증서	설명
서버 1:cms1.uc.lo전화	
CN:cms.uc.local	CallBridge 클러스터 FQDN입니다.이 레코드는 모든 CallBridge 클러스터 피어로 확인되어야 합니다.
SAN:cms.uc.local	CallBridge 클러스터 FQDN입니다.이 레코드는 모든 CallBridge 클러스터 피어로 확인되어야 합니다.
SAN:cms1.uc.local	CallBridge 1 FQDN입니다.
SAN:cms2.uc.local	CallBridge 2 FQDN입니다.
SAN:cms3.uc.local	CallBridge 3 FQDN입니다.
서버 2:cms2.uc.lo전화	
CN:cms.uc.local	CallBridge 클러스터 FQDN입니다.이 레코드는 모든 CallBridge 클러스터 피어로 확인되어야 합니다.
SAN:cms.uc.local	CallBridge 클러스터 FQDN입니다.이 레코드는 모든 CallBridge 클러스터 피어로 확인되어야 합니다.
SAN:cms1.uc.local	CallBridge 1 FQDN입니다.
SAN:cms2.uc.local	CallBridge 2 FQDN입니다.
SAN:cms3.uc.local	CallBridge 3 FQDN입니다.
서버 3:cms3.uc.lo전화	
CN:cms.uc.local	CallBridge 클러스터 FQDN입니다.이 레코드는 모든 CallBridge 클러스터 피어로 확인되어야 합니다.
SAN:cms.uc.local	CallBridge 클러스터 FQDN입니다.이 레코드는 모든 CallBridge 클러스터 피어로 확인되어야 합니다.
SAN:cms1.uc.local	CallBridge 1 FQDN입니다.
SAN:cms2.uc.local	CallBridge 2 FQDN입니다.
SAN:cms3.uc.local	CallBridge 3 FQDN입니다.

CMS CLI를 사용하여 인증서의 내용을 볼 수 있습니다.

```
cms1> pki inspect cmsuccluster.cer
Checking ssh public keys...not found
Checking user configured certificates and keys...found
File contains a PEM encoded certificate
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            60:00:00:00:21:db:36:e8:b9:0d:96:44:41:00:00:00:00:00:21
    Signature Algorithm: sha256WithRSAEncryption
```

```
        Issuer: DC=local, DC=uc, CN=DC-CA
        Validity
            Not Before: Mar 16 19:00:53 2018 GMT
            Not After : Mar 16 19:10:53 2020 GMT
        Subject: C=US, ST=NC, L=RTP, O=Systems, OU=Cisco, CN=CMS.UC.local
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:b8:41:69:d9:1d:47:ef:b1:23:70:ae:69:da:e3:
                    ff:12:f8:97:2b:ee:1e:c0:6c:66:e4:95:3f:8a:74:
                    4d:ec:fc:1e:0d:38:56:1b:00:5c:ce:6d:d3:68:13:
                    e4:9d:b6:e7:7d:de:c4:a4:f3:00:02:11:e5:33:06:
                    b4:f6:64:29:c3:77:62:a9:dc:9d:ad:a2:e9:c1:0b:
                    72:f4:18:af:df:d3:e3:f4:4a:5d:66:e5:e8:4f:63:
                    09:15:5f:8e:ec:df:86:fb:35:47:99:db:18:d1:b7:
                    40:4e:b6:b3:b6:66:28:8e:89:15:8b:cc:0f:e6:5c:
                    e6:2d:de:83:6c:f8:e3:46:49:97:a6:a9:0e:6d:b1:
                    65:08:8e:aa:fc:f0:ae:2f:c1:c2:cd:b6:4f:a5:eb:
                    29:32:9a:48:8c:86:6d:1e:3a:c2:22:70:a3:56:e9:
                    17:01:ef:3a:ce:bb:9f:04:47:e5:24:e0:16:ba:c0:
                    85:df:92:4d:51:d2:95:bf:84:f7:9a:2e:c0:31:e9:
                    9f:91:4f:4a:ce:2c:27:17:f8:ae:3e:96:4e:3b:0a:
                    15:1a:66:cf:e9:12:96:e1:17:ee:65:3c:04:7a:c0:
                    a0:b3:09:fd:3e:16:08:c6:0b:36:51:57:cb:d8:09:
                    a3:40:d0:2c:ae:d6:06:e0:8c:06:de:b7:ce:24:83:
                    28:69
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Alternative Name:
                DNS:CMS.UC.local, DNS:CMS.UC.local, DNS:CMS1.UC.local, DNS:CMS2.UC.local,
DNS:CMS3.UC.local
            X509v3 Subject Key Identifier:
                FE:EF:64:D6:85:7A:62:C5:CA:7B:64:10:B7:F9:E7:18:1D:65:0B:70
            X509v3 Authority Key Identifier:
                keyid:B5:FC:2D:1E:7F:D9:3E:68:F4:B2:78:1F:F0:E8:B2:FC:80:7F:9C:E8

            X509v3 CRL Distribution Points:

                Full Name:
                  URI:ldap:///CN=DC-
CA,CN=DC,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=uc,DC=local?certifica
teRevocationList?base?objectClass=cRLDistributionPoint

            Authority Information Access:
                CA Issuers - URI:ldap:///CN=DC-
CA,CN=AIA,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=uc,DC=local?cACertificate?b
ase?objectClass=certificationAuthority

            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
            1.3.6.1.4.1.311.21.7:
                0..&+.....7.....\...........A........N...O..d...
            X509v3 Extended Key Usage:
                TLS Web Server Authentication, TLS Web Client Authentication
            1.3.6.1.4.1.311.21.10:
                0.0
..+.......0
..+.......
    Signature Algorithm: sha256WithRSAEncryption
         83:31:16:15:74:41:98:e4:40:02:70:cc:6e:c0:53:15:8a:7a:
         8a:87:0a:aa:c8:99:ff:5b:23:e4:8b:ce:dd:c0:61:9c:06:b4:
         3d:22:91:b6:91:54:3a:99:8d:6e:db:18:27:ef:f7:5e:60:e6:
         48:a2:dd:d5:85:1d:85:55:79:e0:64:1a:55:22:9e:39:0c:27:
```

```
         53:a4:d8:3f:54:fd:bc:f9:d4:6e:e1:dd:91:49:05:3e:65:59:
         6e:d4:cd:f6:de:90:cb:3d:b3:15:03:4b:b8:9d:41:f1:78:f5:
         d9:42:33:62:b5:18:4f:47:54:c9:fa:58:4b:88:aa:0d:f6:26:
         9b:fb:8f:98:b4:82:96:97:24:fe:02:5b:03:04:67:c2:9e:63:
         3d:02:ae:ef:92:a7:be:ad:ca:7e:4e:d2:1e:54:e6:bf:75:3b:
         72:32:7c:d6:78:3f:5e:b9:e6:43:bd:1c:74:20:46:57:1b:81:
         c2:4b:b4:fc:9f:cc:c9:63:a8:2d:fd:dd:09:3f:24:d6:ac:f7:
         7c:bd:26:80:a5:b4:d1:a7:c8:fb:3d:d4:a7:93:70:d1:5c:77:
         06:9e:1c:f8:6a:81:a5:97:91:e9:21:e9:7a:df:a3:64:ab:ed:
         15:c7:be:89:5f:1e:53:a7:b5:01:55:ab:a2:cd:8f:67:8d:14:
         83:bc:29:a1
cms1>
```

제목 및 X509v3 Subject Alternative Name 필드에 유의하십시오.이러한 기능은 나중에 Microsoft 환경에서 신뢰 관계를 구축할 때 매우 중요합니다.

```
        Subject: C=US, ST=NC, L=RTP, O=Systems, OU=Cisco, CN=CMS.UC.local

            X509v3 Subject Alternative Name:
                DNS:CMS.UC.local, DNS:CMS.UC.local, DNS:CMS1.UC.local, DNS:CMS2.UC.local,
DNS:CMS3.UC.local
```

참고:인증서 컨피그레이션 가이드는 여기에서 찾을 수 있습니다 .https://www.cisco.com/c/dam/en/us/td/docs/conferencing/ciscoMeetingServer/Deployment_Guide/Version-2-2/Certificate-Guidelines-Single-Split_Server-Deployment-2-2.pdf

DNS 레코드 요구 사항 - 단일 CallBridge

표 2a는 DNS 서버를 구성하는 방법의 예를 제공합니다.각 필드가 의미하는 바를 설명합니다.

표 2a

레코드	IP 예	설명
cms.uc.lo전화	10.10.10.1	통화 브리지
fe.skype.로컬	10.10.10.5	Skype 프런트 엔드 FQDN(정규화된 도메인 이름)

DNS 레코드 요구 사항 - 클러스터링된 CallBridges

표 2b는 DNS 서버를 구성하는 방법의 예를 제공합니다.각 필드가 의미하는 바를 설명합니다.

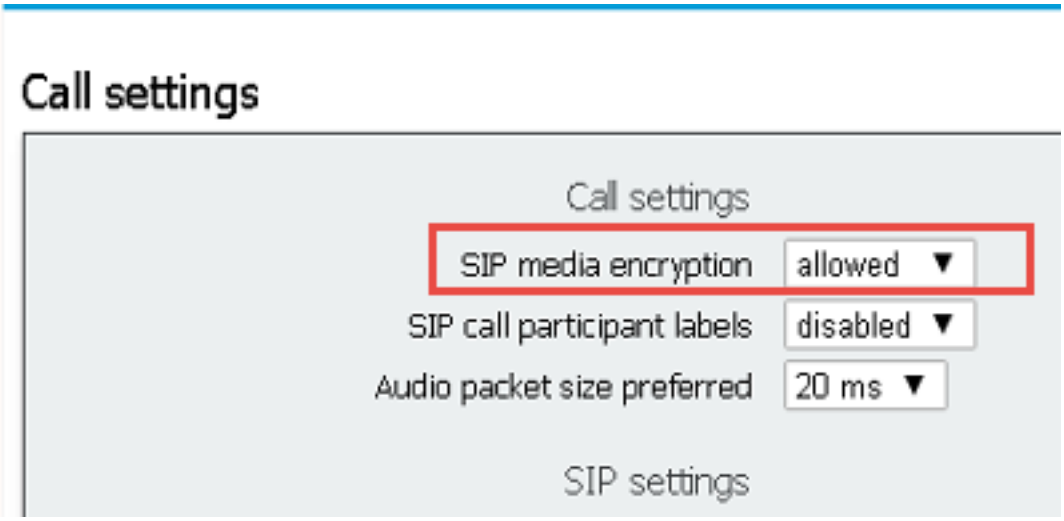
표 2b

레코드	IP 예	설명
cms1.uc.lo전화	10.10.10.1	통화 브리지 1
cms2.uc.lo전화	10.10.10.2	통화 브리지 2
cms3.uc.lo전화	10.10.10.3	통화 브리지 3
cms.uc.lo전화	10.10.10.1 10.10.10.2 10.10.10.3	클러스터의 모든 CallBridge로 확인되는 레코드.이를 CallBridge 클러스터 FQDN(Fully Qualified Domain Name)이라고 합니다.
fe.skype.로컬	10.10.10.5	Skype 프런트 엔드 FQDN(정규화된 도메인 이름)

구성

SIP 미디어 암호화

Configuration(컨피그레이션) **> Call Settings(통화 설정)로 이동합니다.**SIP 미디어 암호화를 허용으로 설정해야 합니다.



인바운드 규칙

표 3에서는 수신 통화 - 통화 일치 컨피그레이션의 모든 필드가 무엇을 의미하는지 설명합니다.

표 3

수신 통화 일치 다이얼 플랜 필드	설명
도메인 이름	이 도메인과 함께 통화가 수신되면 URI의 사용자 부분을 사용하여 활성화된 대상에서 하는 항목을 찾습니다.
우선 순위	이는 규칙이 고려되는 순서를 결정합니다.먼저 더 높은 숫자를 확인합니다.낮은 숫자 지막으로 확인됩니다.
대상 공간	yes로 설정된 경우URI의 사용자 부분이 스페이스와 일치하면 통화가 해당 스페이스에 결됩니다.
대상 사용자	yes로 설정된 경우URI의 사용자 부분이 CMA 사용자와 일치하면 해당 사용자에 대한 를 시도합니다.
대상 IVR	yes로 설정된 경우URI의 사용자 부분이 구성된 IVR과 일치하면 통화가 해당 IVR에 연 니다.
대상 Lync	yes로 설정된 경우URI의 사용자 부분이 비즈니스용 Skype 미팅의 PSTN 전화 걸기 번 일치하는 경우 해당 모임에 듀얼 홈 통화로 연결됩니다.
대상 Lync Simplejoin	yes로 설정된 경우URI의 사용자 부분을 HTTPS 대상으로 변환하고 해당 URL에서 호 되는 Office365 모임을 찾습니다.
테넌트	이 규칙을 고려할 테넌트를 결정합니다.

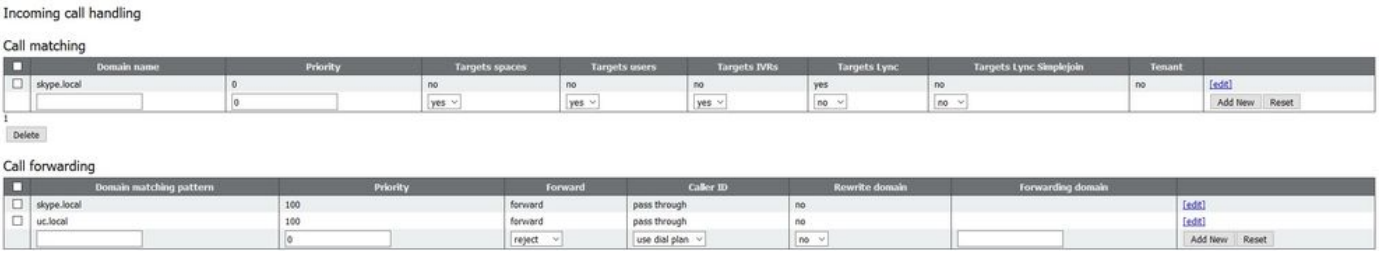
표 4에서는 수신 통화 - 통화 착신 전환 컨피그레이션의 모든 필드가 무엇을 의미하는지 설명합니다.

표 4

수신 통화 착신 전환 다이얼 플랜 필드	설명
도메인 일치 패턴	이 도메인으로 통화가 수신되면 구성된 대로 도메인을 전달하거나 거부합니다.
우선 순위	이는 규칙이 고려되는 순서를 결정합니다.먼저 더 높은 숫자를 확인합니다.낮은 숫자는 막으로 확인됩니다.
앞으로	통화를 착신 전환하도록 설정하면 아웃바운드 규칙에 의해 처리됩니다.통화를 거부하도 설정하면 거부되고 전달되지 않습니다.
발신자 ID	도메인의 시작 부분을 통과하도록 설정된 경우 보존됩니다.다이얼 플랜을 사용하도록 하면 발신 규칙에 구성된 대로 시작 부분이 재작성됩니다.

	참고:CallBridge가 클러스터에 있는 경우 Lync/Skype 도메인과 일치하는 규칙에 통과
	을 사용할 수 없습니다.이렇게 하면 게이트웨이 통화에 대한 프레젠테이션이 중단됩니
도메인 재작성	활성화된 경우 수신자 도메인을 전달 도메인 필드에 구성된 값으로 변경합니다.
포워딩 도메인	재작성 도메인이 활성화된 경우 호출된 도메인이 이 필드의 값으로 변경됩니다.

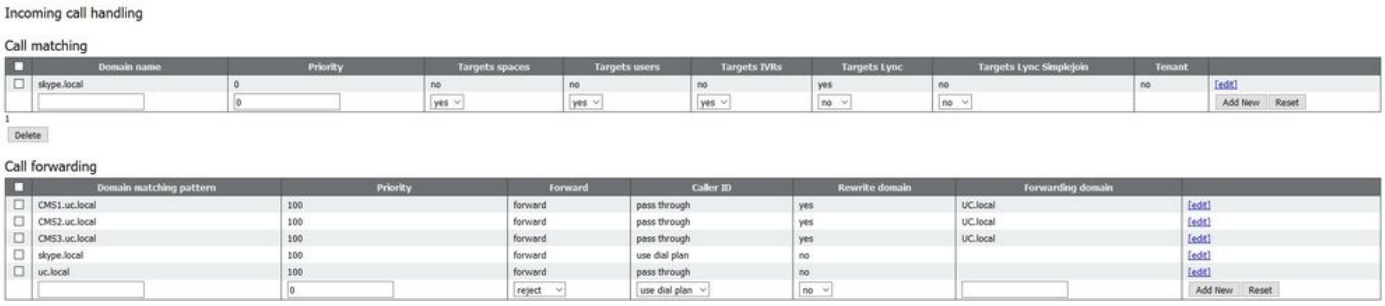
인바운드 규칙 컨피그레이션 예 - 단일 CallBridge



이러한 환경에서는 매우 간단합니다.클러스터링된 CallBridges를 사용하지 않으므로 각 도메인이 발신자 ID로 통과를 사용하도록 설정할 수 있습니다.이 작업은 프레젠테이션 공유가 중단되므로 클러스터링된 환경에서는 수행할 수 없습니다.

또한 "Targets Lync"가 true로 설정된 도메인 Skype.local에 대한 통화 일치 규칙이 있습니다.즉, PSTN 전화 번호로 Lync/Skype 미팅에 전화를 걸면 듀얼 홈 통화로 연결할 수 있어야 합니다.

인바운드 규칙 컨피그레이션 예 - 클러스터링된 CallBridges



이 환경에서는 세 개의 CallBridge로 구성된 CallBridge 클러스터를 사용합니다.따라서 도메인을 uc.local에 다시 작성하도록 구성된 각 CallBridge에 대해 하나의 통화 착신 전환 규칙이 필요합니다.이는 Lync/Skype 사용자가 UC 환경에서 사용자를 콜백할 때 실제로 cms1.uc.local, cms2.uc.local 또는 cms3.uc.local의 도메인에 전화를 걸기 때문입니다.죄송합니다. 이는 클러스터된 CallBridge 환경에서 콘텐츠를 작동하는 데 필요한 컨피그레이션의 제한입니다.uc.local sip 프록시로 통화를 착신 전환하기 전에 이를 uc.local로 다시 변환해야 합니다.

또한 "Targets Lync"가 true로 설정된 도메인 Skype.local에 대한 통화 일치 규칙이 있습니다.즉, PSTN 전화 번호로 Lync/Skype 미팅에 전화를 걸면 듀얼 홈 통화로 연결할 수 있어야 합니다.

아웃바운드 규칙

표 5에서는 아웃바운드 통화 컨피그레이션의 모든 필드가 의미하는 바를 설명합니다.

표 5

아웃바운드 다이얼 플랜 필드	설명
도메인	이 도메인으로 나가는 통화의 경우 이 아웃바운드 규칙을 사용합니다.
사용할 SIP 프록시	이 도메인에 대한 통화를 보낼 SIP 프록시
로컬 연락처 도메인	연락처 헤더에 어떤 값이 입력될지 결정합니다.Lync/Skype 통합의 경우 이 값을 CallBridge의 FQDN으로 설정해야 합니다. 참고:Lync/Skype의 SIP 프록시를 사용하는 아웃바운드 규칙의 경우 이 필드를 구성해야 합니다.Lync/Skype가 아닌 SIP 프록시를 사용하는 아웃바운드 규칙의 경우 이 필드를 구성하지 않아도 됩니다.

도메인에서 로컬	그러면 from 헤더에 어떤 값이 입력될지 결정됩니다.SIP 프록시에 표시되는 발신자 ID 주소입 .이 필드를 비워 두면 구성된 "로컬 연락처 도메인"이 사용됩니다.Lync/Skype는 이 URI를 콜백 레젠테이션 공유를 위한 대상 URI로 사용합니다. 참고:통화가 게이트웨이 통화이고 사용된 인바운드 다이얼 규칙에 "발신자 ID"가 패스스루로 설 경우 이 값은 사용되지 않습니다.
트렁크 유형	SIP 프록시와의 통신에 사용할 SIP의 변형을 결정합니다.
동작	이렇게 하면 통화를 완료할 수 없는 일치 시 우선 순위가 낮은 규칙을 계속 확인할지 아니면 검 중지할지 결정됩니다.
우선 순위	이는 규칙이 고려되는 순서를 결정합니다.먼저 더 높은 숫자를 확인합니다.낮은 숫자는 마지막 확인됩니다.
암호화	이는 암호화된 SIP를 사용할지 암호화되지 않은 SIP를 사용할지를 결정합니다.
테넌트	이 규칙을 고려할 테넌트를 결정합니다.
통화 브리지 범위	이 아웃바운드 다이얼 규칙을 고려할 CallBridges를 결정합니다.클러스터링된 CallBridges에서 CallBridge에서 올바른 연락처 도메인을 전송하려면 이 작업이 필요합니다. 참고:이 값은 아래에 설명된 대로 API를 통해서만 설정할 수 있습니다.

아웃바운드 통화 컨피그레이션 예 - 단일 CallBridge

Outbound calls

	Domain	SIP proxy to use	Local contact domain	Local from domain	Trunk type	Behavior	Priority	Encryption	Tenant
☐	UC.local	cucm.uc.local		<use local contact domain>	Standard SIP	Stop	100	Encrypted	no
☐	skype.local	fe.skype.local	cms.uc.local	<use local contact domain>	Lync	Stop	100	Encrypted	no

다시 단일 CallBridge 환경이 클러스터링된 환경보다 훨씬 간단합니다.위에서 언급할 만한 한 가지 사실은 연락처 도메인이 지정되어 있다는 것입니다 .CallBridge의 정규화된 도메인 이름을 로컬 연결 도메인으로 지정하지 않으면 Lync/Skype에서 보안상의 이유로 통화를 거부하기 때문입니다.수신 전달 규칙이 통과(pass through)를 사용하도록 설정되어 있으므로 이 예에서는 실제로 도메인의 을 재작성하지는 않습니다.

아웃바운드 통화 컨피그레이션 예 - 클러스터링된 CallBridges

Outbound calls

	Domain	SIP proxy to use	Local contact domain	Local from domain	Trunk type	Behavior	Priority	Encryption	Tenant	Call Bridge Scope
☐	UC.local	cucm.uc.local		<use local contact domain>	Standard SIP	Stop	0	Encrypted	no	<all>
☐	skype.local	fe01.skype.local	CMS1.UC.local	<use local contact domain>	Lync	Stop	0	Encrypted	no	<local>
☐	skype.local	fe01.skype.local	CMS2.UC.local	<use local contact domain>	Lync	Stop	0	Encrypted	no	cms2.uc.local
☐	skype.local	fe01.skype.local	CMS3.UC.local	<use local contact domain>	Lync	Stop	0	Encrypted	no	cms3.uc.local

이 환경에서는 세 개의 CallBridge로 구성된 CallBridge 클러스터를 사용합니다.따라서 서로 다른 로컬 연락처 도메인, 로컬 from 도메인 및 범위가 있는 각 CallBridge에 대해 하나의 아웃바운드 규칙이 필요합니다.모든 CallBridges에서 Cisco Unified Communications Manager로 통화를 라우팅하려면 하나의 아웃바운드 규칙만 필요합니다.범위를 설정하려면 API를 사용해야 합니다.

API를 사용하여 범위 수정 - 클러스터링된 CallBridges만 해당

아웃바운드 통화 규칙을 생성한 후에는 해당 규칙에 대해 범위가 <all>로 설정됩니다.이는 아웃바운드 규칙이 클러스터의 모든 CallBridges에서 사용됨을 의미합니다.Lync/Skype를 가리키는 아웃바운드 규칙의 경우 현재 사용 중인 CallBridge에 따라 다른 연락처 및 헤더에서 사용해야 합니다.이렇게 하려면 연락처/보낸 사람 필드가 CallBridge와 일치하는 각 CallBridge에 대해 다른 아웃바운드 규칙을 만들어야 합니다.API를 사용하여 이러한 아웃바운드 다이얼 규칙의 범위를 설정하여 해당 규칙과 일치하는 CallBridge에서만 처리되도록 해야 합니다.

클러스터의 모든 CallBridge 목록 가져오기

브라우저에서 CMS API의 /callbridges 페이지로 이동합니다.클러스터의 모든 CallBridges가 표시됩니다.

이제 모든 CallBridges의 ID가 있습니다.ID는 사용자 환경에서 다릅니다.CallBridge cms1.uc.local I를 참조하려면 e4ab61ea-b5b4-4fac-ad4a-9979badea4e4의 ID를 사용해야 합니다.

모든 아웃바운드 다이얼 규칙 목록 가져오기

다음으로, 아웃바운드 규칙을 조회하고 ID를 받아야 합니다.브라우저에서 API의 /outboundDialplanrules 페이지로 이동합니다.

```
<outboundDialPlanRules total="4">
  <outboundDialPlanRule id="7c76b6c7-4c42-45b0-af47-796cb6737e4e">
    <domain>UC.local</domain>
    <priority>0</priority>
  </outboundDialPlanRule>
  <outboundDialPlanRule id="b8cf4056-7f56-43a5-b67b-861253d5ca32">
    <domain>skype.local</domain>
    <priority>0</priority>
  </outboundDialPlanRule>
  <outboundDialPlanRule id="4ae1d777-48b7-423b-a646-a329e1e822af">
    <domain>skype.local</domain>
    <priority>0</priority>
  </outboundDialPlanRule>
  <outboundDialPlanRule id="05f00293-50fd-4c17-9452-dec224b43430">
    <domain>skype.local</domain>
    <priority>0</priority>
  </outboundDialPlanRule>
</outboundDialPlanRules>
```

이제 모든 규칙에 대한 ID가 있는데 어느 게 어느 건지 알 수가 없어요첫 번째 규칙은 UC.local의 규칙이므로 신경 쓰지 않으며, 그 범위를 설정할 필요가 없습니다.Skype.local에 대한 나머지 아웃바운드 규칙의 규칙을 알아야 합니다.따라서 한 번에 하나씩 시작하면 CallBridges와 ID가 일치합니다.

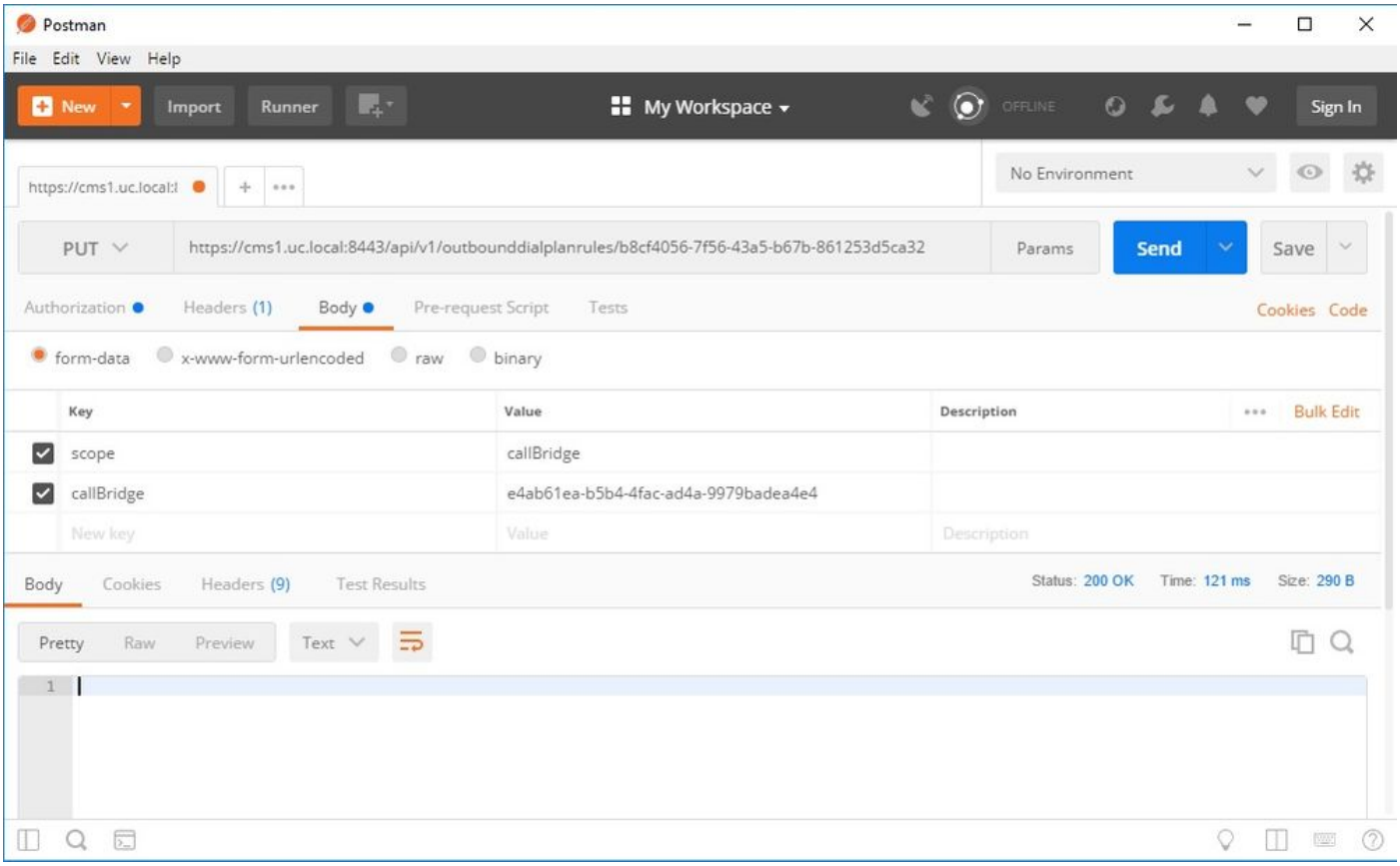
브라우저에서 /outbounddialplanrules/b8cf4056-7f56-43a5-b67b-861253d5ca32로 이동합니다.여기에 나열된 연락처 헤더를 읽으면 이 규칙이 CMS.1.UC.local용임을 알 수 있습니다.따라서 이 규칙의 범위를 CMS.1.UC.local로 설정해야 합니다.

CallBridge 범위 설정

내가 좋아하는 API 툴을 사용하여 다음 본문과 함께 /outbounddialplanrules/b8cf4056-7f56-43a5-b67b-861253d5ca32의 api로 PUT를 보냅니다.

```
scope: callBridge
callBridge: e4ab61ea-b5b4-4fac-ad4a-9979badea4e4
```

이 스크린샷에서는 PostMan을 사용하여 이 요청을 보냅니다.



이 HTTP PUT가 성공한 경우 WebAdmin의 아웃바운드 다이얼 규칙 페이지에 범위가 적용되었음을 반영해야 합니다.CallBridge의 Webadmin에서 범위가 적용된 경우 <local>이 표시되어야 합니다.다른 CallBridge의 Webadmin을 사용하여 아웃바운드 다이얼 규칙을 볼 경우 범위 필드에 CallBridge FQDN이 표시되어야 합니다.<all> 범위는 모든 CallBridges에서 규칙이 사용됨을 의미합니다.<none> 범위는 범위가 사용하도록 설정되었지만 범위와 일치하는 CallBridges가 없음을 의미합니다.

하나의 CallBridge에 대한 범위를 설정한 후에는 각 추가 CallBridge에 대해 구성해야 합니다.이 구성이 완료되면 Skype 도메인에 대한 모든 아웃바운드 규칙에는 범위가 있어야 합니다.

CMS 서비스 계정

WebAdmin의 일반 구성 페이지에는 Lync Edge 설정 섹션이 있습니다.TURN 서비스를 활용하거나 PSTN 전화 접속 번호를 통해 듀얼 홈 회의에 참가하려면 이 옵션을 구성해야 합니다.

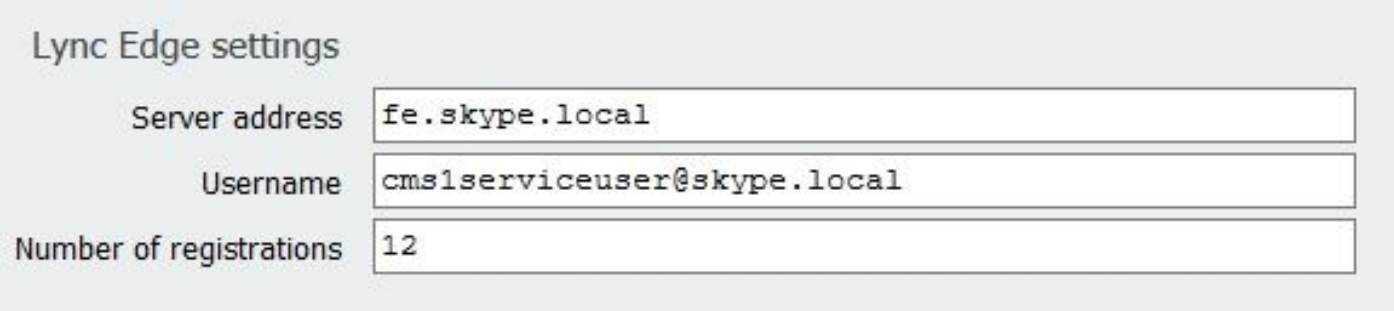
표 6에서는 Lync Edge 설정 구성의 모든 필드가 의미하는 바를 설명합니다.

표 6

Lync Edge 설정 필드	설명
서버 주소	프런트 엔드 풀의 FQDN(Fully Qualified Domain Name)
사용자 이름	CMS에 사용할 서비스 계정의 사용자 이름입니다.
등록 수	등록하려는 사용자 계정 수여기서 값을 구성하지 않으면 위에 나열된 사용자 이름만 등록됩니다에 숫자를 적용하면 1-X 숫자가 URI의 사용자 부분에 접미사로 적용됩니다. 여기서 X는 이 필드성된 번호입니다.

CMS 서비스 계정 컨피그레이션 예

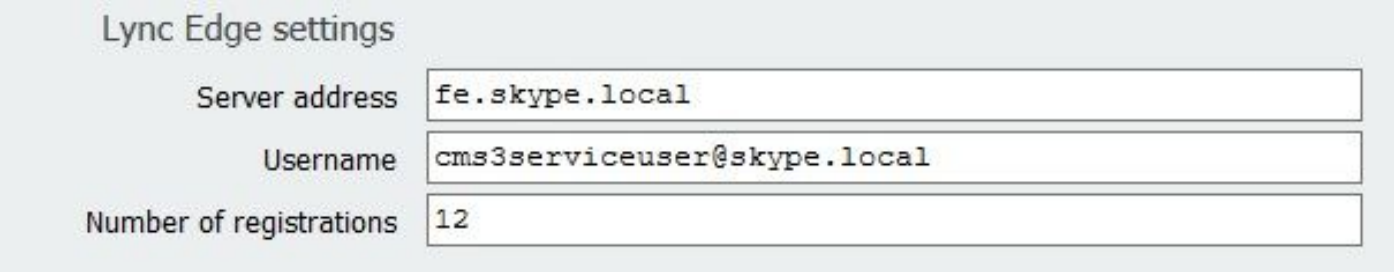
CMS1의 구성:



이 컨피그레이션은 cms1serviceuser1@skype.local, cms1serviceuser2@skype.local, cms1serviceuser3@skype.local, ... cms1serviceuser11@skype.local 및 cms1serviceuser12@skype.local을 fe.skype.local로 등록합니다.이 예에서는 클러스터링된 환경에 있으므로 다른 CallBridges에 대한 서비스 계정을 만들고 별도로 구성해야 합니다.이 예의 사용자 이름은 다릅니다.CMS1에서는 사용자 이름에 cms1이 접두사로 붙습니다. CMS2에서는 사용자 이름에 cms2가 접두사로 붙습니다. CMS3에서는 접두사가 cms3입니다. 이러한 모든 계정은 비즈니스용 Skype 환경에서 만들어지고 활성화됩니다.신뢰할 수 있는 응용 프로그램 풀이 "인증된 것으로 처리"로 구성되어 있으므로 등록할 암호를 제공할 필요가 없습니다.

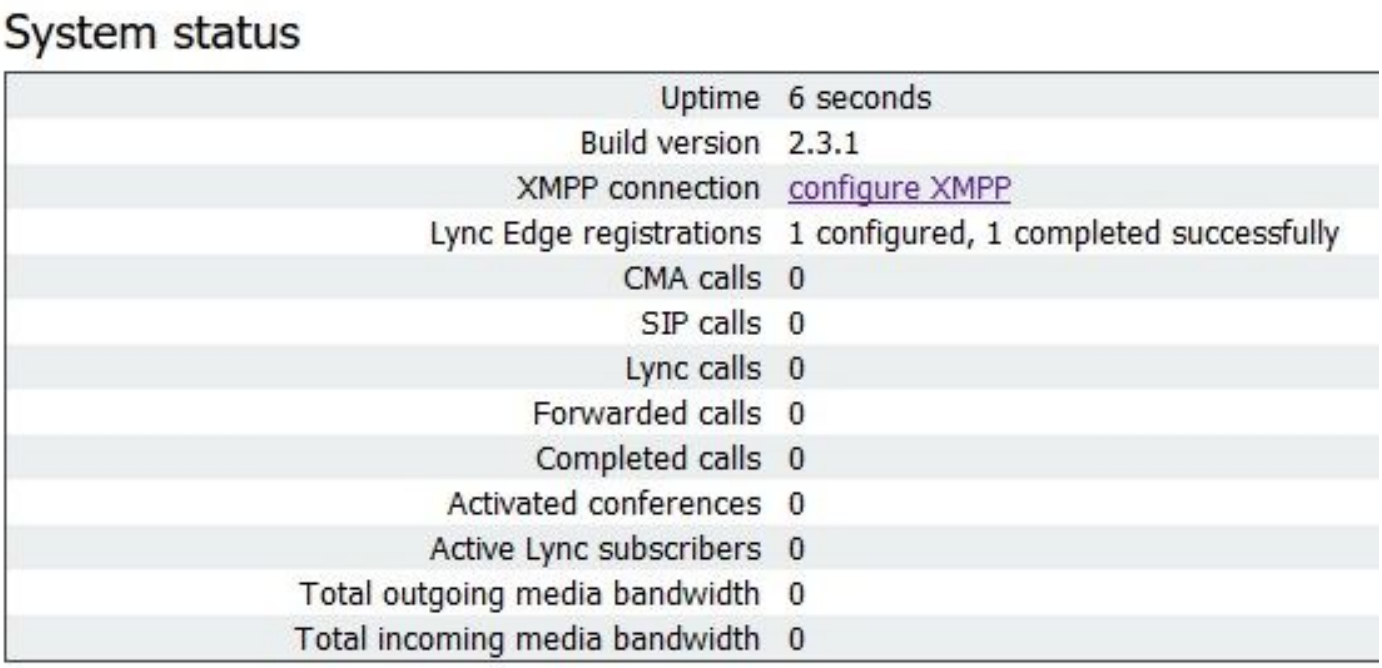
CMS2의 구성:

CMS3의 구성:



CMS 서비스 계정 확인

CMS WebAdmin의 상태 페이지에는 Lync/Skype 사용자가 성공적으로 등록되었는지 여부가 표시됩니다.아래 예에서는 하나의 등록만 구성하며 성공적으로 완료되었습니다.상태가 오랜 기간 동안 진행 중인 등록을 표시하는 경우 SIP 및 DNS 로그를 수집하여 오류가 발생하는 이유를 확인합니다.



Lync/Skype 구성

Lync/Skype 관리 셸에서 아래 명령을 적용합니다.프런트 엔드 서버에 명령을 적용합니다.

> **참고:**권장 명령은 지침을 위한 것입니다.Skype 서버의 구성에 문제가 있는 경우 Lync/Skype 관리자 및/또는 지원 팀에 문의해야 합니다.

단일 CallBridge

먼저 Skype에 CallBridge를 신뢰하라고 알려야 합니다.이를 위해 신뢰할 수 있는 애플리케이션 풀을 추가합니다.Microsoft 용어 "풀"에서는 "클러스터"를 의미합니다. 이 시나리오에서는 클러스터가 하나의 CallBridge 클러스터일 뿐입니다.클러스터의 ID는 CallBridge에서 사용 중인 인증서의 일반 이름과 일치해야 합니다.Microsoft에서는 이를 보안 검사로 사용합니다.SAN에서 ID를 사용한다고 해서 충분하지 않습니다.일반 이름이 일치하지 않으면 Microsoft에서 TCP 연결을 끊습니다.이 명령을 사용할 때 ID는 CallBridge FQDN이어야 합니다.이 연결을 서비스하는 프런트 엔드 풀의 FQDN이어야 하는 등록자입니다.사이트는 Lync/Skype 사이트 식별자여야 합니다.등록자 또는 사이트에 사용해야 하는 값을 잘 모르는 경우 Lync/Skype 관리자에게 문의하십시오.

```
New-CsTrustedApplicationPool -Identity CMS.UC.local -Registrar fe.skype.local -site 1 -RequiresReplication $false -
ThrottleAsServer $true -TreatAsAuthenticated $true
```

다음으로 Microsoft Environment가 포트 5061의 CallBridge(Trusted Application Pool)에서 인바운드 통신을 허용하도록 구성되어야 합니다.

```
New-CsTrustedApplication -ApplicationId AcanoApplication -TrustedApplicationPoolFqdn CMS.UC.local -Port 5061
```

Microsoft 환경은 현재 통화를 수락하도록 구성되어 있지만, 콜백 통화를 할 수 없으며 게이트웨이 통화에 대한 프레젠테이션을 보낼 수 없습니다.이를 수정하려면 고정 경로를 추가해야 합니다.단일 CallBridge 시나리오에서는 UC.local 도메인에 대한 모든 통화를 허용하기 위해 단일 라우트만 있으면 됩니다.아래 명령에서 Destination은 SIP 요청을 보낼 CallBridge의 FQDN입니다.MatchURI 필드는 사용해야 하는 URI의 도메인 부분입니다.Lync/Skype 환경에서는 MatchURI당 하나의 고정 경로만 만들 수 있습니다.

```
$x1=New-CsStaticRoute -TLSRoute -Destination “CMS.UC.local" -MatchUri “UC.local" -Port 5061 -UseDefaultCertificate
$true Set-CsStaticRoutingConfiguration -Identity global -Route @{Add=$x1}
```

마지막으로, Skype에 방금 수행한 모든 변경 사항을 구현하라고 알려야 합니다.

```
Enable-CsTopology
```

클러스터링된 CallBridges

먼저 Skype에 CallBridge 클러스터를 신뢰하도록 해야 합니다.이를 위해 신뢰할 수 있는 애플리케이션 풀을 추가합니다.Microsoft 용어 "풀"에서는 "클러스터"를 의미합니다. 클러스터의 ID는 CallBridge에서 사용 중인 인증서의 일반 이름과 일치해야 합니다. Microsoft에서는 이를 보안 검사로 사용합니다.SAN에서 ID를 사용한다고 해서 충분하지 않습니다.일반 이름이 일치하지 않으면 Microsoft에서 TCP 연결을 끊습니다.이 명령을 사용할 때 ID는 CallBridge FQDN이어

야 합니다.ComputerFqdn은 클러스터에 있는 첫 번째 CallBridge의 FQDN이어야 합니다.Lync/Skype 환경에 표시할 ComputerFqdn을 지정하여 이 ComputerFqdn은 단일 서버만 있는 클러스터가 아님을 나타냅니다.이 연결을 서비스하는 프런트 엔드 풀의 FQDN이어야 하는 등록자입니다.사이트는 Lync/Skype 사이트 식별자여야 합니다.등록자 또는 사이트에 사용해야 하는 값을 잘 모르는 경우 Lync/Skype 관리자에게 문의하십시오.

```
New-CsTrustedApplicationPool -Identity CMS.UC.local -ComputerFqdn CMS1.UC.local -Registrar fe.skype.local -site 1 -
RequiresReplication $false -ThrottleAsServer $true -TreatAsAuthenticated $true
```

이 환경에서는 두 CallBridges를 신뢰할 수 있는 응용 프로그램 컴퓨터로 추가해야 합니다.위의 신뢰할 수 있는 응용 프로그램 풀을 만들 때 첫 번째 CallBridge가 이미 추가되었습니다.이러한 컴퓨터를 추가할 때 방금 만든 풀과 연결해야 합니다.이는 Skype에 신뢰할 수 있는 추가 컴퓨터가 클러스터에 있음을 알려줍니다.여기에 있는 모든 컴퓨터 ID는 CallBridge 인증서에 SAN으로 나열되어야 합니다. 이러한 ID는 CallBridges의 아웃바운드 다이얼 규칙의 연락처 헤더와도 일치해야 합니다.일치하지 않으면 Microsoft에서 TCP 연결을 끊습니다.

```
New-CsTrustedApplicationComputer -Identity CMS2.UC.local -Pool CMS.UC.local New-CsTrustedApplicationComputer -
Identity CMS3.UC.local -Pool CMS.UC.local
```

다음으로 Microsoft Environment가 포트 5061의 CallBridge 클러스터(신뢰할 수 있는 애플리케이션 풀)에서 인바운드 통신을 허용하도록 구성되어야 합니다.

```
New-CsTrustedApplication -ApplicationId AcanoApplication -TrustedApplicationPoolFqdn CMS.UC.local -Port 5061
```

Microsoft 환경은 현재 통화를 수락하도록 구성되어 있지만, 콜백 통화를 할 수 없으며 게이트웨이 통화에 대한 프레젠테이션을 보낼 수 없습니다.이를 수정하려면 고정 경로를 추가해야 합니다.먼저 UC.local 도메인에 대한 모든 통화를 허용하려면 고정 경로를 추가해야 합니다.아래 명령에서 Destination은 SIP 요청을 보낼 CallBridge의 FQDN입니다.MatchURI 필드는 사용해야 하는 URI의 도메인 부분입니다.Lync/Skype 환경에서는 MatchURI당 하나의 고정 경로만 만들 수 있습니다.대상은 CallBridge 클러스터의 FQDN이며 클러스터의 모든 구성원에 대한 DNS A 레코드가 있으므로 Lync/Skype는 모든 CallBridges로 트래픽을 보낼 수 있습니다.따라서 다운될 경우 클러스터에 있는 다른 CallBridge로 도메인에 대한 요청을 자동으로 라우팅할 수 있습니다.

```
$x1=New-CsStaticRoute -TLSRoute -Destination “CMS.UC.local" -MatchUri “UC.local" -Port 5061 -UseDefaultCertificate
$true Set-CsStaticRoutingConfiguration -Identity global -Route @{Add=$x1}
```

다음으로, 클러스터의 각 CallBridge에 대해 추가 고정 경로를 생성해야 합니다.이는 콜백 및 프레젠테이션이 작동해야 하는 요구 사항입니다.

```
$x2=New-CsStaticRoute -TLSRoute -Destination “CMS1.UC.local" -MatchUri “CMS1.UC.local" -Port 5061 -
UseDefaultCertificate $true Set-CsStaticRoutingConfiguration -Identity global -Route @{Add=$x2} $x3=New-
CsStaticRoute -TLSRoute -Destination “CMS2.UC.local" -MatchUri “CMS2.UC.local" -Port 5061 -UseDefaultCertificate
$true Set-CsStaticRoutingConfiguration -Identity global -Route @{Add=$x3} $x4=New-CsStaticRoute -TLSRoute -
Destination “CMS3.UC.local" -MatchUri “CMS3.UC.local" -Port 5061 -UseDefaultCertificate $true Set-
CsStaticRoutingConfiguration -Identity global -Route @{Add=$x4}
```

마지막으로, Skype에 방금 수행한 모든 변경 사항을 구현하라고 알려야 합니다.

```
Enable-CsTopology
```

문제 해결

CMS에서 로그 수집

문제를 진단하는 첫 번째 단계는 문제의 위치를 확인하는 것입니다.이를 위해 Cisco Meeting Server에서 로그를 분석해야 하지만 먼저 로그를 수집해야 합니다.로그에 대한 개인 권장 사항은 다음과 같습니다.

먼저 WebAdmin 인터페이스를 통해 모든 CallBridge에 대해 SIP 및 DNS 디버깅을 활성화합니다.이렇게 하려면 WebAdmin으로 이동한 다음 Logs > Detailed Tracing으로 이동합니다.여기에서 30분 동안 SIP 및 DNS 로깅을 활성화합니다.문제를 파악하고 진단하는 데 충분한 시간이 필요합니다.모든 CallBridges는 로그 설정이 클러스터 전체에서 공유되지 않으므로 개별적으로 수행해야 합니다.

둘째, 모든 CallBridges에서 패킷 캡처를 활성화합니다.SSH를 통해 각 CallBridge에 연결하고 pcap <interface> 명령을 실행합니다. 여기서 <interface>는 인터페이스 트래픽입니다.대부분의 경우 인터페이스 a가 됩니다.따라서 "pcap a" 명령은 연결된 CallBridge에 대해 인터페이스 a에서 패킷 캡처를 시작합니다.

패킷 캡처가 모든 인터페이스에서 실행되면 다음 단계는 문제를 생성하는 것입니다.계속 진행하여 전화를 걸거나 실패한 모든 작업을 수행합니다.이 작업이 완료되면 모든 패킷 캡처가 종료됩니다.이 작업은 모든 SSH 창에 Ctrl-C를 입력하여 수행할 수 있습니다.패킷 캡처가 완료되면 생성된 파일의 이름이 화면에 기록됩니다.다음 단계에서 이 파일 이름을 다운로드해야 하므로 이 파일 이름을 계속 추적합니다.

마지막으로 CallBridges에서 로그를 수집해야 합니다.이를 위해 SFTP를 통해 각 CallBridge에 연결합니다.logbundle.tar.gz 파일과 생성된 패킷 캡처 파일을 다운로드합니다.이 파일은 CMS2.2 이상에서만 사용할 수 있습니다.CMS 버전 2.3 이상에는 CMS의 전체 컨피그레이션이 포함됩니다.버전 2.2를 실행 중인 경우 인바운드/아웃바운드 규칙이 포함되지 않으므로 해당 페이지의 스크린샷과 Lync Edge 설정을 참조용으로 사용하는 것이 좋습니다.로그가 가져온 CallBridge와 일치하는 이름을 가진 별도의 폴더에 수집된 로그/스크린샷을 저장해야 합니다.이렇게 하면 로그가 혼합되지 않도록 할 수 있습니다.

Lync/Skype 구성 보기

이러한 명령은 Lync/Skype 구성을 트러블슈팅할 때 매우 유용합니다.이 문서에서는 컨피그레이션을 만들고 보는 명령이 제공되지만 컨피그레이션을 제거하는 명령은 제공되지 않습니다.이는 Lync/Skype 환경을 완전히 이해하는 관리자가 수행하지 않는 한 구성을 제거하는 것이 위험할 수 있기 때문입니다.구성을 제거해야 하는 경우 Lync/Skype 관리자에게 문의하여 구성을 제거하십시오.

명령을 사용합니다	설명
Get-CsTrustedApplicationPool	이 명령은 Lync/Skype에서 신뢰하는 클러스터(풀)를 나열합니다.이 풀의 ID는 CallBridge 인증서의 일반 이름과 일치해야 합니다. 단일 CallBridge 환경에서도 여기에 하나의 CallBridge 클러스터(풀)를 지정해야 합니다.
Get-CsTrustedApplicationComputer	이 명령은 Lync/Skype에서 신뢰하는 서버 및 이러한 서버가 연결된 풀을 나열합니다.여기에 있는 모든 컴퓨터는 CallBridges에서 보낸 인증서에서 식별되어야 합니다.단일 CallBridge 환경에서 이 이름은 일반적으로 일반 이름입니다.클러스터링된 환경에서는 이러한 컴퓨터가 SAN(Subject Alternative Name) 항목으로 나열되어야 합니다.또한 여기에 있는 모든 컴퓨터는 CallBridge 아웃바운드 다이얼 규칙의 로컬 연락처 도메인 항목으로 식별되어야 합니다.
Get-CsTrustedApplication	이 명령은 신뢰할 수 있는 애플리케이션 풀과 통신할 수 있는 서비스를 나열합니다.Lync/Skype와의 CMS 통신을 위해 TLS 암호화 SIP에 TCP 포트 5061을 사용합니다.
Get-CsStaticRoutingConfiguration | Select-Object -ExpandProperty 경로	이 명령은 Lync/Skype가 요청 전달에 사용하는 고정 경로를 나열합니다.MatchURI 필드는 SIP 메시지의 대상 도메인입니다.XML의 "TLS Fqdn" 필드에는 이 트래픽에 대한 대상 서버가 표시됩니다.

Lync/Skype Get 명령의 출력 예

다음은 이 문서에서 다루는 세 가지 CallBridge 클러스터 시나리오에서 실행된 위의 Lync/Skype 가져오기 명령의 출력입니다

```
PS C:\Users\administrator.SKYPE> Get-CsTrustedApplicationPool


Identity             : TrustedApplicationPool:CMS.UC.local
Registrar            : Registrar:lyncpoolfe01.skype.local
FileStore            :
ThrottleAsServer     : True
TreatAsAuthenticated : True
OutboundOnly         : False
RequiresReplication  : False
AudioPortStart       :
AudioPortCount       : 0
AppSharingPortStart  :
AppSharingPortCount  : 0
VideoPortStart       :
VideoPortCount       : 0
Applications         : {urn:application:acanoapplication}
DependentServiceList : {}
ServiceId            : 1-ExternalServer-1
SiteId               : Site:RTP
PoolFqdn             : CMS.UC.local
Version              : 7
Role                 : TrustedApplicationPool



PS C:\Users\administrator.SKYPE> Get-CsTrustedApplicationComputer


Identity : CMS1.UC.local
```

```
Pool     : CMS.UC.local
Fqdn     : CMS1.UC.local

Identity : CMS2.UC.local
Pool     : CMS.UC.local
Fqdn     : CMS2.UC.local

Identity : CMS3.UC.local
Pool     : CMS.UC.local
Fqdn     : CMS3.UC.local



PS C:\Users\administrator.SKYPE> Get-CsTrustedApplication


Identity                   : CMS.UC.local/urn:application:acanoapplication
ComputerGruus              : {CMS1.UC.local
sip:CMS1.UC.local@skype.local;gruu;opaque=srvr:acanoapplication:GMqDXW_1rVCEMQi4qS6ZxwAA,
CMS2.UC.local

sip:CMS2.UC.local@skype.local;gruu;opaque=srvr:acanoapplication:_Z9CnV49LFufGDXjnFFi4gAA,
CMS3.UC.local
sip:CMS3.UC.local@skype.local;gruu;opaque=srvr:acanoapplication:dt8XJKciSlGhEeT62tyNogAA}
ServiceGruu                :
sip:CMS.UC.local@skype.local;gruu;opaque=srvr:acanoapplication:dQFM4E4YgV6J0rjuNgqxIgAA
Protocol                   : Mtls
ApplicationId              : urn:application:acanoapplication
TrustedApplicationPoolFqdn : CMS.UC.local
Port                       : 5061
LegacyApplicationName      : acanoapplication



PS C:\Users\administrator.SKYPE> Get-CsStaticRoutingConfiguration | Select-Object -
ExpandProperty Route


Transport               :
TransportChoice=Certificate=Microsoft.Rtc.Management.WritableConfig.Settings.SipProxy.UseDefault
Cert;Fqdn=CMS.UC.local;Port=5061
MatchUri                : UC.local
MatchOnlyPhoneUri       : False
Enabled                 : True
ReplaceHostInRequestUri : False
Element                 : <Route
xmlns="urn:schema:Microsoft.Rtc.Management.Settings.SipProxy.2008" MatchUri="UC.local"
MatchOnlyPhoneUri="false" Enabled="true" ReplaceHostInRequestUri="false">
                            <Transport Port="5061">
                              <TLS Fqdn="CMS.UC.local">
                                <UseDefaultCert />
                              </TLS>
                            </Transport>
                          </Route>

Transport               :
TransportChoice=Certificate=Microsoft.Rtc.Management.WritableConfig.Settings.SipProxy.UseDefault
Cert;Fqdn=CMS1.UC.local;Port=5061
MatchUri                : CMS1.UC.local
MatchOnlyPhoneUri       : False
Enabled                 : True
ReplaceHostInRequestUri : False
Element                 : <Route
xmlns="urn:schema:Microsoft.Rtc.Management.Settings.SipProxy.2008" MatchUri="CMS1.UC.local"
```

```
MatchOnlyPhoneUri="false" Enabled="true" ReplaceHostInRequestUri="false">
                            <Transport Port="5061">
                              <TLS Fqdn="CMS1.UC.local">
                                <UseDefaultCert />
                              </TLS>
                            </Transport>
                          </Route>

Transport               :
TransportChoice=Certificate=Microsoft.Rtc.Management.WritableConfig.Settings.SipProxy.UseDefault
Cert;Fqdn=CMS2.UC.local;Port=5061
MatchUri                : CMS2.UC.local
MatchOnlyPhoneUri       : False
Enabled                 : True
ReplaceHostInRequestUri : False
Element                 : <Route
xmlns="urn:schema:Microsoft.Rtc.Management.Settings.SipProxy.2008" MatchUri="CMS2.UC.local"
MatchOnlyPhoneUri="false" Enabled="true" ReplaceHostInRequestUri="false">
                            <Transport Port="5061">
                              <TLS Fqdn="CMS2.UC.local">
                                <UseDefaultCert />
                              </TLS>
                            </Transport>
                          </Route>

Transport               :
TransportChoice=Certificate=Microsoft.Rtc.Management.WritableConfig.Settings.SipProxy.UseDefault
Cert;Fqdn=CMS3.UC.local;Port=5061
MatchUri                : CMS3.UC.local
MatchOnlyPhoneUri       : False
Enabled                 : True
ReplaceHostInRequestUri : False
Element                 : <Route
xmlns="urn:schema:Microsoft.Rtc.Management.Settings.SipProxy.2008" MatchUri="CMS3.UC.local"
MatchOnlyPhoneUri="false" Enabled="true" ReplaceHostInRequestUri="false">
                            <Transport Port="5061">
                              <TLS Fqdn="CMS3.UC.local">
                                <UseDefaultCert />
                              </TLS>
                            </Transport>
                          </Route>



PS C:\Users\administrator.SKYPE>
```

TAC에 문의

이 구현에 오류가 발생하면 Cisco TAC에 문의하십시오.서비스 요청을 열 때 이 문서에 대한 링크를 포함하십시오.TAC 엔지니어가 구성을 이해하는 데 도움이 됩니다.또한 위에서 설명한 대로 Cisco Meeting Server 로그가 케이스에 첨부되고 Lync/Skype 프런트 엔드에서 모든 Get 명령의 출력이 사례 노트에 입력될 경우 매우 유용합니다.이 정보를 포함하지 않을 경우 TAC 엔지니어가 가장 먼저 요청하는 정보 중 하나가 될 것입니다. 케이스를 열기 전에 먼저 수집하십시오.