

X 시리즈 서버를 Cisco Meeting Server 어플라이언스 또는 가상 머신으로 교체

목차

[소개](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[X 시리즈 서버를 CMS 어플라이언스 또는 가상 시스템으로 교체](#)

[업무에 대한 수준 높은 설명](#)

[단계별 자세한 지침](#)

[다음을 확인합니다.](#)

[문제 해결](#)

소개

이 문서에서는 Acano X-Series 서버를 CMS(Cisco Meeting Server) VM(Virtual Machine), CMS1000 또는 CMS2000 서버로 안전하고 안정적으로 교체하는 방법에 대해 설명합니다. Acano X-Series 서버 지원이 버전 3.0에서 계속 중단되었습니다. X-Series에서 실행할 수 있는 최신 소프트웨어는 2022년 3월 1일까지 지원되는 2.9.5입니다. 그 이후에는 더 이상 유지 보수 릴리스나 버그 픽스가 없습니다. 즉, Acano X-Series 서버가 있는 경우 그 전에 서버를 교체해야 합니다.

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- CMS 관리
- CMS 업그레이드
- 인증서 생성 및 서명

사용되는 구성 요소

이 문서의 정보는 Cisco Meeting Server(VM 또는 CMS1K 또는 CMS2K) 및 Acano X-Series 서버를 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

배경 정보

X-Series 서버를 교체할 때는 다양한 서버의 통화 용량을 알아야 합니다. 크기 조정 지침은 부록 C(<https://www.cisco.com/c/en/us/support/conferencing/meeting-server/products-installation-and-configuration-guides-list.html>)의 Cisco Meeting Server 구축 설명서를 참조하십시오.

참조할 X 시리즈 크기:

- X1 - 25개의 HD(720p) 통화
- X2 - 125HD(720p) 통화
- X3 - 250HD(720p) 통화

교체 서버 설정 프로세스는 설치 문서에서 찾을 수 있으며 아래 내용은 다루지 않습니다. 설치 가이드는 다음과 같습니다. <https://www.cisco.com/c/en/us/support/conferencing/meeting-server/products-installation-guides-list.html>

X 시리즈 서버를 CMS 어플라이언스 또는 가상 시스템으로 교체

X-Series 서버를 대체할 수 있는 지원되는 방법은 데이터베이스 클러스터에 새 디바이스를 추가하여 데이터베이스의 복사본을 얻는 것입니다.

주의:X-Series 서버의 백업을 사용하여 교체를 구축하지 마십시오.

교체를 완료하기 위해 아래의 모든 단계가 필요한 것은 아닙니다. 새 서버를 이전 서버로 클러스터링하여 데이터베이스의 복사본을 얻는 것이 가장 중요합니다.

마이그레이션 프로세스를 완료하면 모든 데이터베이스 정보(인바운드 규칙, 아웃바운드 규칙, 코스페이스, 통화 ID 등)도 새 서버에 있습니다.

참고:Configuration(컨피그레이션) > General(일반) 및 Configuration(컨피그레이션) > Active Directory(Active Directory) 아래의 GUI(그래픽 사용자 인터페이스)에 입력된 데이터가 데이터베이스에 없습니다. GUI에서 API(Application Programming Interface)로 LDAP(Lightweight Directory Access Protocol) 컨피그레이션을 이동해야 합니다. 아직 이 작업을 수행할 준비가 되지 않은 경우 이 두 페이지의 모든 데이터를 복사하여 새 서버에 다시 입력할 수 있습니다. 해당 정보를 복사할 수 없으므로 LDAP에 LDAP 사용자 이름에 대한 암호도 필요합니다.

먼저 워크플로에 대한 상위 레벨 설명과 그 다음 단계별 지침을 확인할 수 있습니다. 교체 절차에 대한 단계별 지침을 따르는 것이 좋습니다.

업무에 대한 수준 높은 설명

1단계. 이전 Acano X-Series 서버에서 백업 파일을 생성합니다.

2단계. 새 서버의 MMP(Mainboard Management Processor)를 구성하기 위해 정보가 필요한 경우 이전 서버에서 백업 파일 및 logbundle.tar.gz 파일을 다운로드합니다.

3단계. 이전 X-Series 서버에서 MMP에 로그인하여 각 서비스/컨피그레이션의 출력을 얻고 정보를 메모 파일에 복사합니다.

4단계. 새 서버를 설정합니다.

5단계. 새 서버에서 라이선스를 가져옵니다.

6단계. 이전 서버에서 새 서버로 인증서를 복사합니다.

7단계. 이전 서버에 설정된 새 서버에서 MMP 서비스를 활성화합니다.

(Acano X-Series는 관리 전용 관리 인터페이스를 사용할 수 있습니다.A-D 인터페이스를 통해 새 서버를 관리해야 하지만 새 서버의 모든 서비스는 A 인터페이스에 있을 수 있습니다.)

8단계. 이전 서버에서 사용된 동일한 사용자 계정을 새 서버에 만듭니다.

9단계. 데이터베이스를 새 서버에 복사합니다.

10단계. 데이터베이스 클러스터에서 X-Series를 제거합니다.

11단계. 새 서버가 대체하는 X-Series 서버를 종료합니다.

12단계. 새 디바이스의 IP를 교체하려는 기존 X-Series 인터페이스 A IP와 일치하도록 변경합니다. X-Series에서 여러 인터페이스를 사용하는 경우 새 서버에서도 이 인터페이스를 사용해야 합니다. 이렇게 하면 DNS 레코드를 변경할 필요가 없기 때문입니다.

13단계. 원래 배포가 단일 통합 서버가 아닌 경우에만 데이터베이스 클러스터에 서버를 다시 조인합니다.

14단계. API - `api/v1/system/configuration/cluster`의 새 서버에 따라 로드 제한을 조정합니다.

15단계. 구축을 테스트하여 계속 작동하는지 확인합니다.

단계별 자세한 지침

1단계. MMP 명령 백업 스냅샷 `<server_specific_filename>`을 사용하여 백업을 생성합니다.

2단계. 교체하려는 각 X-Series 서버에서 백업 파일 및 `logbundle.tar.gz`(<https://video.cisco.com/video/5810051601001>) 파일을 다운로드합니다.

3단계. X-Series 서버에서 다음 명령을 실행하여 다양한 서비스의 컨피그레이션을 가져온 다음 노트 파일에 저장합니다.이를 통해 새 서버를 재구성하는 방법에 대한 쉬운 참조를 제공합니다.

'webadmin', 'callbridge', 'webbridge', 'xmpp', 'turn', 'ntp 서버 목록', 'tls sip', 'tls dtls', 'tls webadmin', 'database cluster status', 'user list', 'ipv4 a', 'ipv4 b', 'ipv4 c', 'ipv4 admin', 'filer4', 'recorder', 'streamer', 'uploader', 'dloader', 'dscp', 'dscp', 'peedge', 'peedge 323_gateway', 'syslog', 'ldap'

참고:H323_gateway, Sip Edge 및 XMPP는 CMS 3.0에서 더 이상 사용되지 않습니다.

SIP Edge를 사용하는 경우 인터넷을 오가는 트래픽을 라우팅하려면 Cisco Expressway-C 및 E가 있어야 합니다.

H323 게이트웨이를 사용하는 경우 H.323-SIP 상호 작용을 수행하려면 Cisco Expressway 서버를 사용하여 이 게이트웨이를 구성해야 합니다.

XMPP를 사용하는 경우, CMS 3.x로 업그레이드한 후에는 일부 컨피그레이션을 변경해야 합니다.그러나 X 시리즈를 교체하고 잠시 2.9.x를 유지하려는 경우 WebRTC, 레코더 또는 스트리밍을 사용해야 하는 경우 새 서버에서 XMPP를 다시 구성해야 합니다.

[이 문서](#)에서 CMS 3.0으로 업그레이드하기 전에 알아야 할 변경 사항에 대한 자세한 내용을 읽을 수 있습니다.

4단계. 새 서버를 설정합니다.X-Series 서버와 동일한 버전의 코드가 있는지 확인합니다.현재 사용할 사용되지 않는 IP를 서버에 지정합니다(`ipv4 <interface> add <address>/<prefix length>`)

<gateway>). 그러나 작업이 완료되면 IP가 X-Series에서 사용된 IP로 변경됩니다. 이는 DNS 레코드 및 인증서에 대한 변경을 방지하기 위한 것입니다. 이전 IP를 다시 사용하지 않으려면 DNS와 인증서를 적절하게 업데이트해야 합니다.

5단계. 새 서버 및 이전 X-Series 서버의 MMP에서 명령 인터페이스 a를 실행하여 A 인터페이스의 MAC 주소를 가져옵니다. 교체하려는 X-Series에서 cms.lic 파일을 다운로드하고 TAC 라이선싱 키를 엽니다. 새 서버의 인터페이스 A MAC 주소와 이전 서버의 MAC를 라이선스 에이전트에게 주고 이전 서버를 새 서버로 교체하도록 지정합니다. 기존 MAC에서 새 MAC로 라이선스를 교체하도록 요청합니다. 그런 다음 새 라이선스 파일이 제공되며, 이 파일을 압축 해제하고, cms.lic로 이름을 바꾸고 새 서버에 업로드해야 합니다.

6단계. 이전 X-Series에서 사용된 인증서, 키 및 CA(Certificate Authority) 파일을 WinSCP 또는 다른 SFTP 프로그램을 사용하여 새 서버에 복사합니다.

7단계. 새 서버에서 현재 이전 X-Series에 있는 것과 동일한 서비스 및 설정을 MMP에서 활성화합니다. 이전과 동일한 구성을 만들려면 3단계에서 수집한 정보를 참조하십시오.

참고: 이러한 새 서버 설정 직후 CMS 3.x로 업그레이드하려는 경우 XMPP, Webbridge, SIP Edge 또는 H323_gateway 구성 요소를 구성할 필요가 없습니다. 이러한 기능은 더 이상 CMS 3.x에서 사용되지 않습니다.

8단계. MMP의 X-Series 서버에 있던 동일한 사용자 계정을 사용자 add <username> <role> 명령을 사용하여 생성합니다(그리고 사용자 규칙 <규칙 이름> <값>을 설정한 경우). CMM(Cisco Meeting Management), TMS(TelePresence Management Suite) 또는 CUCM(Cisco Unified Communications Manager)과 같은 기타 장치는 이러한 어카운트의 기능에 대해 설정할 수 있으므로 새 서버에서 설정해야 합니다.

9단계. 새 서버에 데이터베이스 복사본을 가져옵니다.

9a. 현재 구축이 단일 통합 서버(데이터베이스 클러스터 없음)인 경우 데이터베이스 클러스터를 초기화해야 합니다. CMS 버전 2.7부터는 데이터베이스 클러스터에 인증서가 필요합니다. 따라서 데이터베이스 인증서를 서명하는 데 사용할 수 있는 버전 2.7부터 CMS에 기본 제공 인증 기관이 도입되었습니다.

1. 결합된 단일 X 시리즈 MMP에서 pki selfsigned dbca CN:<회사 이름>(예:pki selfsigned dbca CN:tplab.local)

2. 결합된 단일 X-Series MMP에서 pki csr dbserver CN:xseries.example.com subjectAltName:<newcms1fqdn>

(이 시점에는 DNS A 레코드가 필요하지 않습니다.)

3. 결합된 단일 X-Series MMP에서 pki csr dbclient CN:postgres를 사용하여 데이터베이스 클라이언트에 대한 인증서를 생성합니다.

4. 결합된 단일 X-Series MMP에서 dbca(1단계)를 사용하여 dbserver(2단계) 인증서 pki sign dbserver dbca

5. 결합된 단일 X-Series MMP에서 dbca(1단계)를 사용하여 dbclient(3단계) 인증서 pki 서명 dbclient dbca

6. dbserver.crt, dbserver.key, dbclient.crt 및 dbclient.key 파일을 데이터베이스에 조인할 모든 서버

(데이터베이스 클러스터를 구성하는 노드)에 X-Series에서 새 서버로 복사합니다.

7. X-Series에서 모든 서버에 dbca.crt 파일을 복사합니다.

8. 결합된 단일 X-Series MMP에서 데이터베이스 클러스터 certs dbserver.key dbserver.crt dbclient.key dbclient.crt dbca.crt(dbca.crt는 루트 CA 인증서로) 를 실행합니다.

9. 결합된 단일 X-Series MMP에서 데이터베이스 클러스터 localnode a를 실행합니다.

10. 결합된 단일 X-Series MMP에서 데이터베이스 클러스터 초기화를 실행합니다.

11. 결합된 단일 X-Series MMP에서 데이터베이스 클러스터 상태를 실행합니다.다음을 확인해야 합니다.

노드:<XseriesIP> (me):연결된 기본

12. 데이터베이스 클러스터에 조인할 새 서버에서 MMP에서 데이터베이스 클러스터 certs dbserver.key dbserver.crt dbclient.key dbclient.crt dbca.crt를 실행합니다.

13. 조인할 새 서버(데이터베이스와 공동 배치)의 MMP에서

a.데이터베이스 클러스터 localnode a 실행

b.데이터베이스 클러스터 조인 실행 <기본 노드 IP>

이 시점에서 새 서버에는 데이터베이스의 복사본이 있습니다.새 서버의 MMP에서 데이터베이스 클러스터 상태를 실행하여 동기화된 상태로 표시되도록 합니다. 이러한 경우 9단계로 완료하고 10단계로 진행할 수 있습니다. 그러나 동기화되지 않은 경우 데이터베이스 클러스터 구성을 검토하고 서버 간 TCP 5432를 통한 통신을 차단하는 네트워크 상의 아무 것도 없는지 확인해야 합니다.

9b.현재 구축이 이미 데이터베이스 클러스터인 경우 X-Series 서버를 한 번에 하나씩 교체하려고 합니다.X-Series에서 MMP 데이터베이스 클러스터 상태에서 실행하여 서버가 데이터베이스 클러스터에 조인되었는지 또는 연결되었는지 확인합니다.서버의 IP가 데이터베이스 클러스터 목록에 있으면 조인됩니다. 그렇지 않은 경우 마지막 명령이 'database cluster connect'이면 노드가 연결됩니다.

새 노드를 동일한 역할(조인됨 또는 연결됨)으로 다시 추가하려는 경우 X-Series 서버의 역할을 기록해 두십시오. X-Series가 데이터베이스 기본 서버인 경우 먼저 서버를 재부팅하여 복제본이 됩니다.

1. 교체하려는 X-Series에서 서버 키/인증서, 클라이언트 키/인증서 및 CA 인증서에 사용되는 인증서를 기록합니다.

2. 교체하려는 X-Series에서 데이터베이스 클러스터 제거를 실행합니다.

10단계. 결합된 단일 X-Series 서버를 교체하는 경우 10단계로 여기에서 계속합니다. 클러스터인 경우 11단계로 건너웁니다.

이때 새 서버에는 데이터베이스의 복사본이 있습니다. 새 서버의 웹 인터페이스에 로그인하여 이를 확인하고 사용자 및 스페이스 컨피그레이션을 확인할 수 있습니다.확인 후 데이터베이스 클러스터에서 새 서버를 제거하고 IP를 변경합니다.

1. 새 서버에서 '데이터베이스 클러스터 제거'를 실행합니다.

2. X-Series 서버를 종료합니다.
3. 새 서버의 IP를 X-Series 서버에서 사용하는 IP로 변경합니다.
4. 새 서버를 재부팅합니다.
5. CMS 2.9.x 버전을 사용하는 경우 새 서버를 테스트하여 모든 구성이 작동하는지 확인합니다.
6. 새 서버의 웹 관리 페이지에 로그인하여 스페이스 및 사용자를 확인합니다. 이전에 데이터베이스에 조인되었을 때 서버에 있던 모든 스페이스 및 사용자가 복사본을 가져왔을 때 표시되어야 합니다.

11단계. 클러스터의 일부인 X-Series 서버를 교체하는 경우 다음 단계를 수행할 수 있습니다.

1. 해제할 X-Series 서버를 종료합니다.
2. 새 서버의 IP를 X-Series 서버의 데이터베이스 로컬 노드 인터페이스(일반적으로 a)에서 이전에 사용한 IP로 변경합니다.
3. SFTP 프로그램을 사용하여 서버 키/인증서, 클라이언트 키/인증서 및 CA 인증서를 새 서버에 복사합니다.
4. 새 서버에서 '**database cluster localnode a**' 명령을 실행합니다.

7a 새 노드를 데이터베이스 클러스터에 조인할 경우 '**database cluster certs <server.key> <server.crt> <client.key> <client.crt> <ca.crt>**' 명령을 실행합니다.

5b 새 노드를 데이터베이스 클러스터에 연결(데이터베이스와 함께 배치되지 않음)하려면 '**database cluster certs <client.key> <client.crt> <ca.crt>**' 명령을 실행합니다.

6a 새 노드를 조인해야 하는 경우(데이터베이스와 함께 배치) 다음 명령을 실행합니다. '**데이터베이스 클러스터 조인 <기본 노드 IP>**'

6b 새 노드를 연결(데이터베이스와 공동 위치 아님)해야 할 경우 '**database cluster connect <primary node IP>**' 명령을 실행합니다.

서비스 해제해야 하는 각 X 시리즈에 대해 9b 및 11 단계를 반복합니다.

12단계. 이 시점에서 새 CMS 서버는 데이터베이스의 복사본을 갖게 됩니다. 또는 연결된 경우 데이터베이스 노드에 연결하는 방법을 알고 있고 이전과 동일한 IP 주소를 가지고 있습니다.

13단계. 구축에서 로드 밸런싱을 사용할 수 있습니까?

Loadbalancing=True로 설정된 API에서 CallBridgeGroups와 함께 CMS 호출 로드 밸런싱을 사용하는 경우 환경에 있는 새 서버의 권장 제한에 일치하도록 로드 제한을 변경해야 합니다. **api/v1/system/configuration/cluster**로 이동하여 그에 따라 loadlimit을 업데이트합니다.

시스템	권장 로드 제한
CMS1000 M5v2	120000
CMS1000 M4 또는 M5v1	96000
CMS2000 M5v2	875000
CMS2000	700000
VM(vCPU 수 x 1250)	예: 70 vCPU x 1250 = 87500

14단계. 이 작업을 수행하기 전에 XMPP 클러스터가 있고 잠시 동안 CMS 2.9.x에 있으려면 XMPP 클러스터를 재구축해야 합니다.

MMP 명령

모든 XMPP 노드에서 구성

- 1.xmpp 재설정
- 2 .xmpp 도메인 <도메인 이름>
- 3 .xmpp 수신 대기 <인터페이스 화이트리스트>
- 4.xmpp certs <keyfile> <certificate file> <cert-bundle>
- 5.xmpp 클러스터 트러스트 <xmpp cert>

첫 번째 노드의 구성

- 6.xmpp 활성화
- 7 .xmpp callbridge add <callbridge name>
- 8.xmpp callbridge add <callbridge name>
- 9 .xmpp callbridge add <callbridge name>
10. xmpp callbridge add <callbridge name>
11. xmpp callbridge 목록
12. xmpp 비활성화
13. xmpp 클러스터 활성화
14. xmpp 클러스터 초기화
15. xmpp 활성화
- 16.xmpp 클러스터 상태

두 번째 및 세 번째 노드 구성

17. xmpp 활성화
18. xmpp callbridge add-secret <callbridge name>
19. callbridge secret을 입력합니다.
20. xmpp callbridge add-secret <callbridge name>
21. callbridge 암호를 입력합니다.
22. xmpp callbridge add-secret <callbridge name>
23. callbridge 암호를 입력합니다.
24. xmpp callbridge add-secret <callbridge name>
25. callbridge 암호를 입력합니다.

26. xmpp 비활성화
27. xmpp 클러스터 활성화
28. xmpp 활성화
- 29.xmpp 클러스터 가입 <클러스터>

웹 관리자에서 XMPP 설정 구성

CallBridge 서비스가 있는 각 서버에서

30. 위에 구성된 이 Callbridge 고유 이름을 입력합니다.
31. 도메인을 입력합니다.
32. 메모장에서 암호를 입력합니다.
33. webadmin 상태 페이지에서 인증을 확인합니다.

예

모든 XMPP 노드에서 구성

- 1.xmpp 재설정
- 2 .xmpp 도메인 example.com
- 3 .xmpp 수신 대기
- 4.xmpp certs xmppcluster.key xmppcluster.cer root.cer
- 5.xmpp 클러스터 트러스트 xmppcluster.cer *** 참고 1

첫 번째 노드의 구성

- 6xmpp 활성화
- 7 .xmpp callbridge add cb1
- 8.xmpp callbridge add cb2
- 9 .xmpp callbridge add cb3
10. xmpp callbridge add cb4 *** 참고 2
11. xmpp callbridge list <— 이 출력을 메모장에 복사
12. xmpp 비활성화
13. xmpp 클러스터 활성화
14. xmpp 클러스터 초기화
15. xmpp 활성화
- 16.xmpp 클러스터 상태

두 번째 및 세 번째 노드 구성

17. xmpp 활성화
18. xmpp callbridge add-secret cb1
19. callbridge 암호를 입력합니다.<메모장에서 cb1에 대
밀 복사>
20. xmpp callbridge add-secret cb2
21. callbridge 암호를 입력합니다.<메모장에서 cb2 암호
>
22. xmpp callbridge add-secret cb3
- 23:callbridge 암호 입력:<메모장에서 cb3에 대한 암호 복
>
24. xmpp callbridge add-secret cb4 *** 참고 3

25. callbridge 암호를 입력합니다.<메모장에서 cb4 암호
>
26. xmpp 비활성화
27. xmpp 클러스터 활성화
28. xmpp 활성화
29. xmpp 클러스터 조인 <노드 1의 IP 주소 또는 FQDN>

웹 관리자에서 XMPP 설정 구성

CallBridge 서비스가 있는 각 서버에서

30. callbridge1 등에 cb1을 입력합니다.
31. 도메인 입력:example.com
32. 해당 callbridge에 대한 메모장의 암호를 입력합니다.
33. webadmin 상태 페이지에서 인증을 확인합니다.

참고 1: 예를 들어 xmpp 클러스터 트러스트는 XMPP 인증서입니다. 인증서에 SAN(Subject Alternative Name) 특성의 모든 XMPP 서버 FQDN이 포함되거나 와일드카드 인증서이기 때문입니다. 각 XMPP 서버에 자체 인증서가 있는 경우 이를 결합하여 xmpp 클러스터 트러스트로 추가해야 합니다.

참고 2: `xmpp callbridge add cb4`. xmpp 서버보다 더 많은 callbridge를 가질 수 있는 예로 이 단계를 추가했습니다. 이 단계는 필요하지 않지만 예로 추가되었습니다.

참고 3: `xmpp callbridge ad-secret cb4` 참고 2와 함께 진행하려면 이 단계를 추가했습니다. 4개의 callbridge가 있는 경우 xmpp 클러스터의 모든 노드에 4개를 모두 추가해야 합니다.

CMS 2.9.x 버전을 계속 사용하는 경우, 이제 테스트와 검증을 시작하여 새 서버가 예상대로 작동하는지 확인할 수 있습니다.

다음을 확인합니다.

새 서버로 마이그레이션한 후 모든 사용자 및 스페이스가 표시되고 SIP 통화가 계속 작동하는지 확인합니다. CMS 2.9.x 버전을 사용하는 경우 XMPP가 계속 작동하는지 확인합니다(WebRTC 사용자는 계속 가입/로그인할 수 있으며 레코더는 연결할 수 있음 등). CMS와 통신하고 있는 모든 서버가 여전히 작동하는지 확인합니다(CMM(Cisco Meeting Manager), CUCM(Cisco Unified Communications Manager), TMS(TelePresence Management Suite), Expressway). MMP에서 'syslog follow'를 실행하여 해결해야 할 오류가 있는지 확인하는 것도 좋습니다.

문제 해결

문제가 발생하면 X-Series 서버로 돌아가거나 Cisco TAC에 지원을 요청할 수 있습니다.