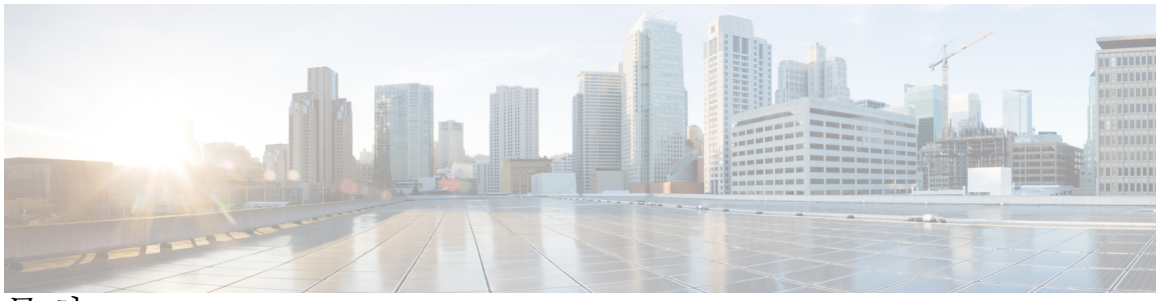
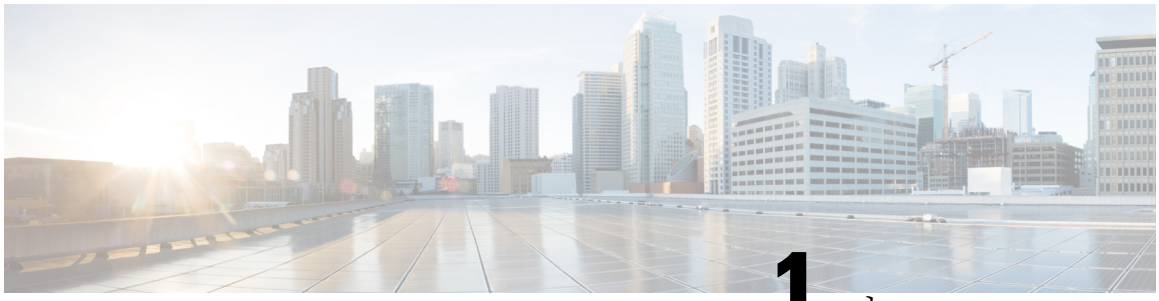
IM and Presence 서비스, 릴리스 15의 구성 및 관리

초판: 2023년 12월 18일

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



목 차



1 장

신규 및 변경된 정보

신규 및 변경된 정보

다음 테이블은 현재 릴리스까지 이 가이드의 주요 기능 변경 사항을 소개합니다. 이 테이블은 가이드에 제공된 모든 변경 사항 또는 이 릴리스의 새 기능에 대한 전체 목록을 제공하지 않습니다.

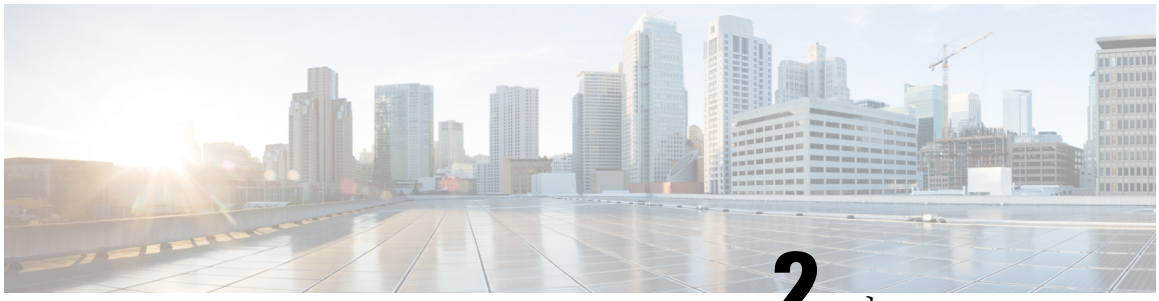
표 ***1: IM and Presence*** 서비스의 새로운 기능 및 변경된 동작

날짜	설명	참고:
2023년 12월 18일	Microsoft 원격 통화 제어 기능 제거.	-

신규 및 변경된 정보

부

시스템 계획



2 장

시스템 계획

IM and Presence 서비스 개요

IM and Presence 서비스 관리는 IM and Presence 서비스 노드에 대한 개별 구성 변경을 수동으로 수행할 수 있게 해주는 웹 기반 애플리케이션입니다. 이 설명서의 절차에서는 이 애플리케이션을 사용하여 기능을 구성하는 방법에 대해 설명합니다.

IM and Presence 서비스에서는 다양한 기능을 갖춘 Cisco Jabber Unified Communications 클라이언트 또는 타사 XMPP 호환 IM and Presence 클라이언트 중 하나를 선택할 수 있습니다. 또한 IM and Presence 서비스는 인스턴트 메시징, 파일 전송을 제공하며 영구 그룹 채팅방을 호스팅하고 구성할 수 있습니다.

IM and Presence 서비스 및 Cisco Unified Communications Manager가 있는 온프레미스 구축에서 다음 서비스를 사용할 수 있습니다.

- 프레즌스
- 인스턴트 메시징
- 파일 전송
- 오디오 통화
- 비디오

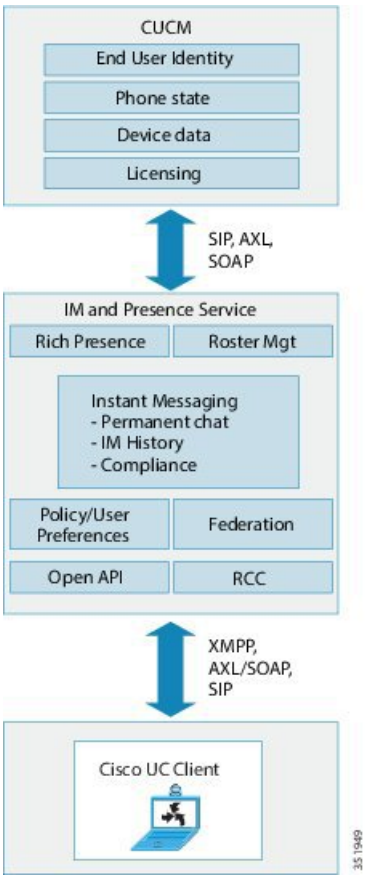
- 음성 메일
- 전화회의

자세한 내용은 Cisco Unified Communications Manager 설명서를 참조하십시오.

IM and Presence 서비스 구성 요소

다음 그림은 Cisco Unified Communications Manager와 IM and Presence 서비스 사이의 주 구성 요소 인터페이스를 비롯한 IM and Presence 서비스 구축의 개요를 제공합니다.

그림 *1: IM and Presence* 서비스 기본 구축



SIP 인터페이스

SIP 인터페이스를 활성화하려면 다음을 구성해야 합니다.

- Cisco Unified Communications Manager에서 프레즌스 정보 교환을 위해 IM and Presence 서비스를 가리키는 SIP 트렁크를 구성해야 합니다.
- IM and Presence 서비스에서 Cisco Unified Communications Manager를 프레즌스 게이트웨이로 구성하면 IM and Presence 서비스가 SIP 트렁크를 통해 SIP 가입 메시지를 Cisco Unified Communications Manager로 보낼 수 있습니다.

AXL/SOAP 인터페이스

AXL/SOAP 인터페이스는 Cisco Unified Communications Manager에서의 데이터베이스 동기화를 처리하고 IM and Presence 서비스 데이터베이스를 채웁니다. 데이터베이스 동기화를 활성화하려면 Cisco 동기화 에이전트 네트워크 서비스가 실행되고 있어야 합니다.

기본적으로 동기화 에이전트는 IM and Presence 서비스 클러스터 내 모든 노드에 사용자를 균일하게 로드 밸런싱합니다. 그러나 사용자를 클러스터의 특정 노드에 수동으로 할당할 수도 있습니다.

단일 또는 듀얼 노드 IM and Presence 서비스에 대해 Cisco Unified Communications Manager로 데이터베이스 동기화를 실행할 경우의 권장 동기화 간격에 대한 지침은 IM and Presence 서비스 SRND 문서를 참조하십시오.

참고 애플리케이션 개발자 상호 작용에 대해서는 AXL 인터페이스가 지원되지 않습니다.

LDAP 인터페이스

Cisco Unified Communications Manager는 수동 구성으로 또는 LDAP를 통해 직접 동기화하여 모든 사용자 정보를 얻습니다. 그런 다음 IM and Presence 서비스는 Cisco Unified Communications Manager의 모든 사용자 정보를 동기화합니다(AXL/SOAP 인터페이스 사용).

IM and Presence 서비스는 Cisco Jabber 클라이언트 및 IM and Presence 서비스 사용자 인터페이스에서 사용자의 LDAP 인증을 제공합니다. Cisco Jabber 사용자가 IM and Presence 서비스에 로그인하고 Cisco Unified Communications Manager에서 LDAP 인증이 활성화되면 IM and Presence 서비스는 사용자 인증을 위해 LDAP 디렉터리로 직접 이동합니다. 사용자가 인증되면 IM and Presence 서비스는 사용자 로그인을 진행할 수 있도록 이 정보를 Cisco Jabber로 전달합니다.

XMPP 인터페이스

XMPP 연결에서는 XMPP 기반 클라이언트의 프레즌스 정보 교환 및 인스턴트 메시징 작업을 다룹니다. IM and Presence 서비스는 XMPP 기반 클라이언트의 임시 및 영구 채팅 방을 지원합니다. IM 게이트웨이는 IM and Presence 서비스 구축에서 SIP 기반 클라이언트와 XMPP 기반 클라이언트 간 IM 상호 운용성을 지원합니다.

CTI 인터페이스

CTI(Computer Telephony Integration) 인터페이스는 IM and Presence 노드의 사용자가 Cisco Unified Communications Manager에서 전화기를 제어하도록 모든 CTI 통신을 처리합니다. Cisco Jabber 클라이언트의 사용자는 CTI 기능을 이용해 사무실 전화기 제어 모드에서 애플리케이션을 실행할 수 있습니다.

Cisco Unified Communications Manager에서 IM and Presence 서비스 사용자에 대해 CTI 기능을 구성하려면, 사용자를 CTI 활성 그룹과 연결하고 해당 사용자에게 할당된 기본 확장을 CTI에 대해 활성화해야 합니다.

Cisco Jabber 사무실 전화기 제어를 구성하려면 CTI 서버와 프로파일을 구성해야 하며, 사무실 전화기 모드에서 애플리케이션을 사용하도록 할 사용자를 해당 프로파일에 할당해야 합니다. 그러나 모

든 CTI 통신은 IM and Presence 서비스 노드를 통해서가 아니라 Cisco Unified Communications Manager와 Cisco Jabber 간에 직접 발생한다는 점에 유의해야 합니다.

Cisco IM and Presence 데이터 모니터 서비스

Cisco IM and Presence 데이터 모니터는 IM and Presence 서비스에서 IDS 복제 상태를 모니터링합니다. 다른 Cisco IM and Presence 서비스는 Cisco IM and Presence 데이터 모니터에 의존하므로 IDS 복제가 안정된 상태가 될 때까지 시작을 지연시킬 수 있습니다.

Cisco IM and Presence 데이터 모니터는 또한 Cisco Unified Communications Manager에서 Cisco Sync Agent의 상태를 확인합니다. IDS 복제가 설정되고 IM and Presence 데이터베이스 게시자 노드의 동기화 에이전트가 Cisco Unified Communications Manager에서 동기화를 완료한 후에야 의존형 서비스의 시작이 허용됩니다. 시간 제한에 도달했으면 IDS 복제 및 동기화 에이전트가 완료되지 않았더라도, 게시자 노드의 Cisco IM and Presence 데이터 모니터는 의존형 서비스의 시작을 허용합니다.

가입자 노드에서, Cisco IM and Presence 데이터 모니터는 IDS 복제가 성공적으로 설정될 때까지 기능 서비스의 시작을 연기합니다. Cisco IM and Presence 데이터 모니터는 클러스터에서 문제의 가입자 노드에 대해서만 기능 서비스의 시작을 연기하며, 하나의 문제 노드 때문에 모든 가입자 노드에서 기능 서비스의 시작을 연기하지는 않습니다. 예를 들어, IDS 복제가 노드1과 노드2에서는 성공적으로 설정되었지만 노드3에서는 그렇지 못한 경우 Cisco IM and Presence 데이터 모니터는 노드1과 노드2에서는 기능 서비스 시작을 허용하되 노드 3에서는 기능 서비스 시작을 연기합니다.

Cisco IM and Presence 데이터 모니터는 IM and Presence 데이터베이스 게시자 노드에서 다르게 동작합니다. 기능 서비스의 시작을 시간 제한이 만료될 때까지만 연기합니다. 시간 제한이 만료되면, IDS 복제가 성공적으로 설정되지 않았더라도 게시자 노드에서 모든 기능 서비스의 시작을 허용합니다.

Cisco IM and Presence 데이터 모니터는 노드에서 기능 서비스 시작을 연기할 때 알람을 생성합니다. 그런 다음 해당 노드에서 IDS 복제가 성공적으로 설정되면 알림을 생성합니다.

Cisco IM and Presence 데이터 모니터는 다중 노드 새로 설치 및 소프트웨어 업그레이드 절차에 모두 영향을 미칩니다. 이 둘은 게시자 노드와 가입자 노드가 동일한 IM and Presence 릴리스에서 실행 중이고 IDS 복제가 가입자 노드에서 성공적으로 설정된 경우에만 완료됩니다.

노드에서 IDS 복제의 상태를 확인하려면 다음 중 하나를 수행하십시오.

- 이 CLI 명령 사용: `utils dbreplication runtimestate`
- Cisco Unified IM and Presence 보고 도구 사용: "IM and Presence Database Status" 보고서에는 클러스터의 자세한 상태가 표시됩니다.

Cisco 동기화 에이전트의 상태를 확인하려면 Cisco Unified CM IM and Presence 관리 인터페이스로 이동하여 진단시스템 대시보드를 선택하십시오. Cisco Unified Communications Manager 퍼블리셔 노드 IP 주소와 동기화 상태가 나타납니다.

계획 개요

시스템을 구성하기 전에 시스템 구축 방법을 계획해야 합니다. IM and Presence 서비스는 서로 다른 회사의 요구 사항을 충족하도록 설계된 다양한 구축 옵션을 제공합니다.

사용자 요구에 맞는 IM and Presence 서비스 구축을 포함하는 Cisco Collaboration 시스템을 설계하는 방법에 대한 자세한 내용은 http://www.cisco.com/c/en/us/support/unified-communications/unified-presence/products-implementation-design-guides-list.html에서 *Cisco Collaboration System* 솔루션 참조 네트워크 설계를 참조하십시오.

구축 계획

시스템을 구성하기 전에 클러스터 토폴로지 및 시스템 구축 방법을 계획해야 합니다.

프로시저

	명령 또는 동작	목적
단계 **1**	협업 구축의 크기	자세한 내용은 http://%20www.cisco.com/c/en/us/support/unified-communications/unified-presence/products-implementation-design-guides-list.html에서 Cisco Collaboration System 솔루션 참조 네트워크 설계의 "협업 솔루션 크기 조정 지침" 장을 참조하십시오.
단계 **2**	구축하려는 기능을 결정합니다.	자세한 내용은 향후 구축 옵션, 10 페이지를 참조하십시오.
단계 **3**	표준 구축 또는IM and Presence 중앙 클러스터 구축을 설치할지 결정	전화와 동일한 클러스터에 IM and Presence 서비스를 구축할지 또는 IM and Presence를 위한 중앙 집중식 클러스터를 구축할지 여부를 결정합니다. 자세한 내용은 표준 구축과 중앙 집중식 클러스터 비교를 참조하십시오.
단계 **4**	구축하려는 클러스터 노드의 수를 계획합니다.	IM and Presence 다중 노드 확장성 기능을 사용하면 사용자 요구 사항에 맞게 구축 크기를 조정할 수 있습니다. 자세한 내용은 다중 노드 확장성 요구 사항, 12 페이지를 참조하십시오.
단계 **5**	이중화를 어떻게 추가할지 계획합니다.	구축을 위한 확장성 옵션, 13 페이지
단계 **6**	지리적 사이트를 계획	단일 위치에서 하드웨어를 유지 관리하기 위해 단일 사이트에 설치할 수 있습니다. 그러나 WAN을 통해 클러스터를 구축하여 여러 사이트를 구축할 때 지리적 이중화를 추가할 수도 있습니다. 자세한 내용은 다음 내용을 참조하십시오. • WAN을 통한 클러스터 내부 구축, 15 페이지

	명령 또는 동작	목적
		• WAN을 통한 클러스터 간 구축, 16 페이지
단계 **7**	SAML 단일 사인온을 구성할 것인지 결정합니다.	자세한 내용은 SAML 싱글 사인온 구축, 16 페이지를 참조하십시오.
단계 **8**	타사 애플리케이션과 통합할 것인지 결정합니다.	여기에는 Microsoft Outlook 일정 통합은 물론 타사 시스템과의 페더레이션도 포함됩니다. 자세한 내용은 타사 통합, 17 페이지를 참조하십시오.

IM and Presence 서비스 구축 규모

Collaboration 배치의 크기를 조정하는 방법에 대한 자세한 내용은 http://www.cisco.com/c/en/us/support/unified-communications/unified-presence/products-implementation-design-guides-list.html에서 *Cisco Collaboration System* 솔루션 참조 네트워크 설계의 "협업 솔루션 크기 조정 지침" 장을 참조하십시오.

향후 구축 옵션

기본 IM, 가용성 및 임시 그룹 채팅은 기본 구축에서 IM and Presence 서비스를 설치하고 사용자를 구성한 후 이용할 수 있는 핵심 기능 중 일부입니다.

기본 구축을 개선하려면 선택적인 기능을 추가할 수 있습니다. 다음 그림에서는 IM and Presence 서비스 기능 구축 옵션을 보여줍니다.

다음 표에는 IM and Presence 서비스에 대한 기능 구축 옵션이 나열되어 있습니다.

표 ***2: IM and Presence*** 서비스의 기능 구축 옵션

핵심 **IM** 및 가용성 기능	고급 **IM** 기능**(**선택사항**)**	풍부한 **Unified Communications** 가용성 기능 **(**선택사항**)**	원격 사무실 전화기 제어**(**선택사항**)**
사용자 가용성 보기 풍부한 텍스트 IM을 안전하게 주고받기 파일 전송 임시 그룹 채팅 연락처 관리 사용자 내역 Cisco Jabber 지원 다중 클라이언트 디바이스 지원: Microsoft windows, MAC, Mobile, 태블릿, IOS, Android, BB Microsoft Office 통합 LDAP 디렉터리 통합 개인 디렉터리 및 친구 목록 개방형 API 시스템 문제 해결	영구 채팅 관리되는 파일 전송 메시지 아카이버 일정표 타사 XMPP 클라이언트 지원 고가용성 확장성: WAN을 통한 클러스터링 및 다중 노드 지원 인터클러스터 피어링 엔터프라이즈 페더레이션: • IM and Presence 서비스 통합 • Cisco Webex Messenger 통합 • Microsoft Lync/비즈니스용 Skype/Office365 Server 통합 • IBM SameTime 통합 • Cisco Jabber XCP 공개 페더레이션: • Google Talk, AOL 통합 • XMMP 서비스 또는 BOT • 타사 Exchange 서비스 통합 IM 규정 준수 SAML SSO(Single Sign On) 사용자 정의 로그인 배너	Cisco 텔레포니 가용성 Microsoft Outlook 일정 통합 (온-프레미스 Exchange 또는 호스트형 Office 365 구축)	원격 Cisco IP 전화기 제어 원격 소프트폰 제어

표준 구축과 중앙 집중식 클러스터 비교

시스템을 설치하기 전에 IMand Presence 서비스의 표준 구축을 구축할지 여부 또는 IMand Presence 서비스 중앙 클러스터를 토폴로지 및 설치에 영향을 주는지 여부를 결정해야 합니다.

- Cisco Unified Communications Manager의 IM and Presence 서비스(표준 구축) - 표준 구축에서 IM and Presence 서비스 클러스터는 Cisco Unified Communications Manager 전화 통신 노드와 동일한 서버에 설치됩니다. IM and Presence 클러스터는 플랫폼 및 전화 통신 클러스터와 동일한 많은 서비스를 공유합니다. 이 옵션을 사용하려면 전화 통신 클러스터를 IM and Presence 클러스터에 1x1 매핑해야 합니다.
- 중앙 집중식 IM and Presence 클러스터 - 이 구축에서 IM and Presence 서비스 클러스터는 전화 통신 클러스터와 별도로 설치됩니다. 토폴로지 계획 방법에 따라 IM and Presence 중앙 클러스터는 전화 통신 클러스터와 완전히 다른 하드웨어 서버에 위치할 수 있습니다. 이 구축 옵션은 전화 통신 클러스터 및 IM and Presence 클러스터의 1x1 매핑 요구 사항을 제거하므로 각 구축 유형을 필요에 맞게 확장할 수 있습니다.

참고 IM and Presence 중앙 클러스터에는 여전히 Cisco Unified Communications Manager 인스턴스가 있습니다. 그러나 이 인스턴스는 사용자 프로비저닝 및 데이터베이스용이며 전화 통신을 처리하지 않습니다. 전화 통신 통합의 경우 IM and Presence 중앙 클러스터는 별도의 Cisco Unified Communictions Manager 전화 통신 클러스터에 연결해야 합니다.

이 문서의 절차는 표준 구축과 중앙 클러스터 구축 모두에 사용할 수 있습니다. 그러나 중앙 클러스터 구축의 경우 전화 통신 클러스터와 IM and Presence 클러스터를 올바르게 정렬하려면 중앙 집중식 구축 구성, 107 페이지 장의 작업을 완료해야 합니다.

다중 노드 확장성 기능

다중 노드 확장성 요구 사항

IM and Presence 서비스는 다중 노드 확장성을 지원합니다.

- 클러스터당 6개 노드
- 클러스터당 사용자 75,000명, 전체 UC(Unified Communication) 모드 구축에서는 노드당 최대 25,000명
- 프레즌스이중화 그룹에서는 사용자 25,000명, 고가용성 구축에서는 클러스터당 사용자 75,000명
- 사용자당 최대 연락처에 대한 관리 가능한 고객 정의 제한(기본적으로 무제한)
- IM and Presence 서비스는 다중 노드 기능으로 클러스터 간 구축을 계속 지원합니다.

OVA 요구 사항

다음과 같은 OVA 요구 사항이 적용됩니다.

- 클러스터 간 구축의 경우에는 최소 15000 사용자의 OVA를 구축해야 합니다. 모든 클러스터가 최소 15,000 사용자 OVA를 실행하는 한 서로 다른 OVA 크기를 실행하는 다른 클러스터를 가질 수 있습니다.
- 영구 채팅 구축의 경우에는 최소 15,000 사용자 OVA를 구축하는 것이 좋습니다.
- 중앙 집중식 구축의 경우 최소 15,000 사용자 OVA를 갖는 25,000 사용자 IM and Presence를 권장합니다. 15,000 사용자 OVA는 25,000 사용자로 증가할 수 있습니다. 25K OVA 템플릿과 고가용성이 활성화된 6개 노드 클러스터를 통해 IM and Presence 서비스 중앙 구축은 최대 75,000개의 클라이언트를 지원합니다. 25K OVA가 있는 75K 사용자를 지원하려면 XCP 라우터의 기본 추적 수준을 정보에서 오류로 변경해야 합니다. 중앙 클러스터의 Unified Communications Manager 퍼블리셔 노드의 경우 다음 요구 사항이 적용됩니다.
  - 25,000 IM and Presence OVA(최대 75,000 사용자)는 중앙 클러스터의 Unified Communications Manager 퍼블리셔 노드에 설치된 10,000 사용자 OVA를 사용하여 구축할 수 있습니다.
  - 15,000 IM and Presence OVA(최대 45,000 사용자)는 중앙 클러스터의 Unified Communications Manager 퍼블리셔 노드에 설치된 7,500 사용자 OVA를 사용하여 구축할 수 있습니다.

참고 여러 디바이스 메시징을 활성화하려는 경우 각 사용자에게 여러 Jabber 클라이언트가 있을 수 있으므로 사용자 수 대신 클라이언트 수를 기준으로 구축을 측정합니다. 예를 들어, 25,000 사용자가 있고 각 사용자에게 Jabber 클라이언트가 두 개 있는 경우, 구축에 50,000 사용자의 용량이 필요합니다.

확장 가능성은 구축 시 클라이언트 수에 따라 다릅니다. VM 구성 요구 사항 및 OVA 템플릿에 대한 자세한 내용은 다음 URL의 *Virtualization for Unified CM IM and Presence*를 참조하십시오. https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-cisco-ucm-im-presence.html.

구축을 위한 확장성 옵션

IM and Presence 서비스 클러스터는 최대 6개의 노드를 지원할 수 있습니다. 처음 설치한 노드 수가 6개 미만인 경우 언제든 추가 노드를 설치할 수 있습니다. 사용자를 더 지원하기 위해 IM and Presence 서비스 구축 규모를 늘리려면 앞서 구성한 다중 노드 구축 모델을 고려해야 합니다. 다음 표에서는 각 다중 노드 구축 모델의 확장성 옵션에 대해 설명합니다.

표 *3:*

구축 모드	확장성 옵션	
	기존 프레즌스 이중화 그룹에 새 노드 추가	새 프레즌스에 새 노드 추가 이중화 그룹
Balanced 비중복 고가용성 구축	기존 프레즌스 이중화 그룹에 새 노드를 추가하면 새 노드는 기존 노드와 동일한 수의 사용자를 지원할 수 있습니다. 프레즌스 이중화 그룹은 이제 두 배의 사용자를 지원할 수 있습니다. 또한 해당 프레즌스 이중화 그룹의 기존 노드와 새 노드에서 사용자에 대한 Balanced 고가용성을 제공합니다.	새 프레즌스 이중화 그룹에 새 노드를 추가하면 구축에서 더 많은 사용자를 지원할 수 있습니다. 이 경우에는 프레즌스 이중화 그룹의 사용자에 대한 Balanced 고가용성이 제공되지 않습니다. Balanced 고가용성을 제공하려면 프레즌스 이중화 그룹에 두 번째 노드를 추가해야 합니다.
Balanced 중복 고가용성 구축	기존 프레즌스 이중화 그룹에 새 노드를 추가하면 새 노드는 기존 노드와 동일한 수의 사용자를 지원할 수 있습니다. 예를 들어 기존 노드가 사용자 5,000명을 지원하면 새 노드도 동일하게 5,000명을 지원합니다. 또한 해당 프레즌스 이중화 그룹의 기존 노드와 새 노드에서 사용자에 대한 Balanced 중복 고가용성을 제공합니다. 참고 기존 노드의 사용자 수에 따라 프레즌스 이중화 그룹 내에서 사용자를 재할당해야 할 수 있습니다.	새 프레즌스 이중화 그룹에 새 노드를 추가하면 구축에서 더 많은 사용자를 지원할 수 있습니다. 이 경우에는 프레즌스 이중화 그룹의 사용자에 대한 Balanced 고가용성이 제공되지 않습니다. Balanced 고가용성을 제공하려면 프레즌스 이중화 그룹에 두 번째 노드를 추가해야 합니다.
Active/Standby 중복 고가용성 구축	기존 프레즌스 이중화 그룹에 새 노드를 추가하면 프레즌스 이중화 그룹의 기존 노드에 있는 사용자를 위한 고가용성이 제공됩니다. 이 경우 고가용성만 향상되며, 구축에서 지원할 수 있는 사용자 수는 늘어나지 않습니다.	새 프레즌스 이중화 그룹에 새 노드를 추가하면 구축에서 더 많은 사용자를 지원할 수 있습니다. 이 경우에는 프레즌스 이중화 그룹의 사용자에 대한 고가용성이 제공되지 않습니다. 고가용성을 제공하려면 프레즌스 이중화 그룹에 두 번째 노드를 추가해야 합니다.

WAN 구축

IM and Presence 서비스는 클러스터 내 구축 및 클러스터 간 구축에서 WAN을 통한 클러스터링을 지원합니다. 이 옵션을 사용하면 구축에 지리적 이중화를 추가할 수 있습니다.

WAN을 통한 클러스터 내부 구축

IM and Presence 서비스는 이 모듈에서 제공하는 대역폭 권장 사항을 사용하여 WAN을 통해 수행되는 클러스터 내부 구축을 지원합니다. IM and Presence 서비스는 WAN을 통해 지리적으로 분산된 단일 프레즌스 이중화 그룹을 지원합니다. 여기에서 프레즌스 이중화 그룹의 각 노드는 각각 별도의 지리적 위치에 배치됩니다.

이 모델은 지리적 중복 및 원격 장애 조치를 제공할 수 있습니다(예: 원격 사이트의 백업 IM and Presence 서비스 노드에 대한 장애 조치). 이 모델에서는 IM and Presence 서비스 노드를 Cisco Unified Communications Manager 데이터베이스 게시자 노드와 같은 곳에 둘 필요가 없습니다. Cisco Jabber 클라이언트는 IM and Presence 서비스 노드에 로컬이거나 원격일 수 있습니다.

이 모델은 클라이언트를 위한 고가용성도 지원합니다. 홈 IM and Presence 서비스 노드에서 서비스나 하드웨어에 장애가 발생하면 클라이언트는 원격 피어 IM and Presence 서비스 노드로 장애 조치합니다. 장애가 발생한 노드가 다시 온라인 상태가 되면 클라이언트는 자동으로 홈 IM and Presence 서비스 노드에 다시 연결됩니다.

원격 장애 조치와 함께 WAN을 통해 IM and Presence 서비스를 구축하는 경우 다음과 같은 제한이 따릅니다.

- 이 모델은 시스템 수준의 고가용성만 지원합니다. 특정 IM and Presence 서비스 구성 요소에는 여전히 단일 실패 지점이 있을 수 있습니다. 이러한 구성 요소는 Cisco Sync Agent, Cisco 클러스터 간 동기화 에이전트 및 Cisco Unified CM IM and Presence 관리 인터페이스입니다.

IM and Presence 서비스는 또한 WAN을 통한 클러스터링 구축에서 여러 프레즌스 이중화 그룹을 지원합니다. WAN을 통한 클러스터링 구축의 규모에 대한 자세한 내용은 IM and Presence 서비스 SRND를 참조하십시오.

자세한 내용은 *IM and Presence* 서비스 솔루션 참조 네트워크 설계(SRND)를 참조하십시오.

WAN을 통한 구축용 다중 노드 구성

WAN을 통한 클러스터 내 구축을 위해 IM and Presence 서비스 다중 노드 기능을 구성하려면 다중 노드 섹션에서 설명한 대로 IM and Presence 서비스 프레즌스 이중화 그룹, 노드 및 사용자 할당을 구성하되, 다음 권장 사항에 유의하십시오.

- 최적의 성능을 얻으려면 사용자 대부분을 홈 IM and Presence 서비스 노드에 할당하는 것이 좋습니다. 이 구축 모델에서는 WAN을 통해 원격 IM and Presence 서비스 노드로 전송되는 메시지 분량이 줄어들지만, 보조 노드에 대한 장애 조치 시간은 장애 조치 대상 사용자의 수에 따라 달라집니다.
- WAN을 통해 고가용성 구축 모델을 구성하려면 프레즌스 이중화 그룹 전체에 DNS SRV 주소를 구성할 수 있습니다. 이 경우 IM and Presence 서비스는 DNS SRV로 지정한 노드에 초기 PUBLISH

요청 메시지를 전송하며, 응답 메시지는 사용자의 호스트 노드를 나타냅니다. 그런 다음 IM and Presence 서비스는 해당 사용자에 대한 모든 하위 요청 PUBLISH 메시지를 호스트 노드로 전송합니다. 이 고가용성 구축 모델을 구성하기 전에, 대역폭이 WAN을 통해 전송될 메시지의 잠재적 분량을 수용할 수 있는지 고려해야 합니다.

WAN을 통한 클러스터 간 구축

IM and Presence 서비스는 이 모듈에서 제공하는 대역폭 권장 사항을 사용하여 수행되는 WAN을 통한 클러스터 간 구축을 지원합니다. 클러스터 간 구축을 구축할 때는 다음 고려 사항이 적용됩니다.

- 인터클러스터 피어 - 독립적인 IM and Presence 서비스 클러스터를 상호 연결하는 피어 관계(인터클러스터 피어라고 함)를 구성할 수 있습니다. 이 인터클러스터 피어 기능을 사용하면 한 IM and Presence 서비스 클러스터의 사용자가 동일한 도메인 내 원격 IM and Presence 서비스 클러스터의 사용자와 통신하고 해당 사용자의 가용성 정보를 수신할 수 있습니다. 인터클러스터 피어를 설정하는 방법에 대한 자세한 내용은 인터클러스터 피어 구성, 172 페이지의 내용을 참조하십시오.
- 노드 이름 - 특정 IM and Presence 서비스 노드에 대해 정의하는 노드 이름을 모든 클러스터의 다른 모든 IM and Presence 서비스 노드에서 확인할 수 있어야 합니다. 따라서 각 IM and Presence 서비스 노드 이름은 노드의 FQDN이어야 합니다. 네트워크에 DNS가 구축되지 않은 경우 각 노드 이름은 IP 주소여야 합니다.
- IM 주소 체계 - 클러스터 간 구축의 경우, 각 클러스터의 모든 노드가 동일한 IM 주소 체계를 사용해야 합니다. 클러스터의 한 노드에서 릴리스 10 이전의 IM and Presence 서비스 버전을 실행 중인 경우, 이전 버전과의 호환성을 유지하려면 모든 노드에서 UserID@Default_Domain IM 주소 체계를 사용하도록 설정해야 합니다.
- 라우터 대 라우터 통신 - 기본적으로 IM and Presence 서비스는 클러스터의 모든 노드를 클러스터 간 라우터 대 라우터 커넥터로서 할당합니다. IM and Presence 서비스는 AXL 인터페이스를 통해 인터클러스터 피어 연결을 설정한 후, 홈 및 원격 클러스터에 있는 모든 클러스터 간 라우터 대 라우터 커넥터 노드의 정보를 동기화합니다.

  TLS를 사용하는 보안 라우터 대 라우터 통신을 구성하여 로컬 클러스터의 각 라우터 대 라우터 커넥터 노드와 원격 클러스터의 각 라우터 커넥터 노드 간의 연결을 보호할 수도 있습니다.

SAML 싱글 사인온 구축

SAML(Security Assertion Markup Language) 싱글 사인온(SSO) 기능을 통해 관리 사용자는 해당 애플리케이션 중 하나에만 로그인한 후 IM and Presence 서비스를 비롯한 여러 Cisco Collaboration 애플리케이션에 액세스할 수 있습니다. 이 기능은 다음과 같은 방법으로 관리자의 작업을 단순화합니다.

- 단일 로그인 후에 여러 Cisco Collaboration 애플리케이션에 액세스하려면 단일 로그인이 필요합니다.
- 하나의 암호만 필요합니다. 더 이상 각 애플리케이션마다 다른 암호를 기억할 필요가 없습니다.
- 관리자는 단일 ID 공급자(IdP)에서 모든 암호 및 인증을 관리할 수 있습니다.

SAML 싱글 사인온을 설정하고 구성하는 방법에 대한 자세한 내용은 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html에서 제공되는 *Cisco Unified Communications* 솔루션용 *SAML SSO* 구축 안내서를 참조하십시오.

타사 통합

IM and Presence 서비스는 다양한 타사 시스템과 통합됩니다. 다음 표에서는 통합에 대해 간략히 설명하고 구성 방법을 설명하는 문서에 대한 링크를 제공합니다.

설명서 제목	포함 내용
IM and Presence 서비스를 위한 Microsoft Outlook 일정 통합	IM and Presence 서비스가 IM and Presence 사용자의 프레즌스 상태에서 Microsoft Outlook의 일정 정보를 사용하기 위해 온프레미스 Microsoft Exchange Server 또는 호스팅된 Office 365 Server에 연결하도록 구성합니다.
IM and Presence 서비스를 위한 도메인 간 페더레이션	다음 시스템을 사용하여 도메인 간 페더레이션을 위한 IM and Presence 서비스를 구성합니다. 이를 통해 IM and Presence 사용자는 다른 시스템의 사용자와 IM and Presence를 교환 할 수 있습니다. • Microsoft Lync • Microsoft 비즈니스용 Skype • Microsoft Office 365 • GoogleTalk • AOL • IBM SameTime • Cisco Webex Messenger • 다른 IM and Presence 서비스 엔터프라이즈
IM and Presence 서비스를 위한 분할된 도메인 내 페더레이션	Microsoft Lync 또는 비즈니스용 Skype를 사용하여 분할된 도메인 내 페더레이션을 위해 IM and Presence 서비스 구성 이 통합을 사용하면 사용자를 IM and Presence서비스로 마이그레이션하는 과정에서 네트워크 내 통신을 유지 관리할 수 있습니다.
IM and Presence 서비스용 Microsoft Lync Server를 통한 원격 통화 제어	Microsoft 원격 통화 제어(RCC)를 위한 Microsoft Lync와의 통합을 위해 Cisco Unified Communications Manager 및 IM and Presence 서비스 구성 이 통합을 통해 엔터프라이즈 사용자는 타사 데스크톱 IM(인스턴트 메시징) 애플리케이션인 Microsoft Lync를 통해 Cisco Unified IP Phone 또는 Cisco IP Communicator 전화기를 제어할 수 있습니다.

타사 클라이언트 통합

이 섹션에서는 타사 클라이언트 통합 요구 사항 중 일부를 설명합니다.

지원되는 타사 **XMPP** 클라이언트

IM and Presence 서비스는 가용성 및 IM(인스턴트 메시징) 서비스를 위해 타사 XMPP 클라이언트 애플리케이션을 IM and Presence 서비스와 통합할 수 있도록 표준 기반 XMPP를 지원합니다. 타사 XMPP 클라이언트는 Cisco SDK(소프트웨어 개발 키트)에 나와 있는 XMPP 표준을 준수해야 합니다.

이 모듈에서는 XMPP 클라이언트와 IM and Presence 서비스를 통합하기 위한 구성 요구 사항에 대해 설명합니다. MPP 기반 API(웹) 클라이언트와 IM and Presence 서비스를 통합하는 경우에는 Cisco 개발자 포털에 있는 IM and Presence 서비스 API용 개발자 설명서도 참조하십시오.

http://developer.cisco.com/

라이선스 요건

XMPP 클라이언트 애플리케이션의 각 사용자에 대해 IM and Presence 서비스 기능을 할당해야 합니다. IM and Presence 기능은 UCL(사용자 연결 라이센싱) 및 CUWL(Cisco Unified Workspace Licensing)에 모두 포함됩니다.

자세한 라이센스 정보는 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html에서 *Cisco Unified Communications Manager* 시스템 구성 설명서의 "스마트 소프트웨어 라이센스" 장을 참조하십시오.

Cisco Unified Communications Manager에서 **XMPP** 클라이언트 통합

XMPP 클라이언트를 통합하기 전에 Cisco Unified Communications Manager에서 다음을 수행하십시오.

- 라이센스 요구 사항을 구성합니다.
- 사용자 및 디바이스를 구성합니다. 디바이스를 각 사용자와 연결하고, 각 사용자를 회선 표시와 연결합니다.

XMPP 연락처 검색을 위한 **LDAP** 통합

XMPP 클라이언트 애플리케이션의 사용자가 LDAP 디렉터리에서 연락처를 검색 및 추가할 수 있도록 하려면 IM and Presence 서비스에서 XMPP 클라이언트에 대해 타사 LDAP 설정을 구성하십시오.

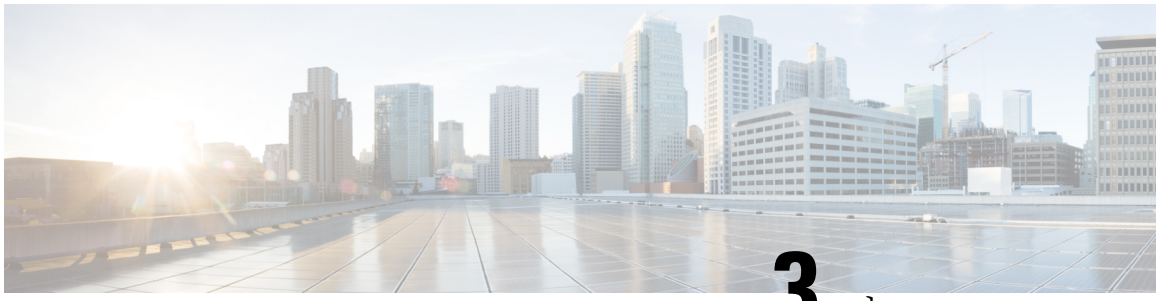
XMPP 클라이언트용 **DNS** 구성

XMPP 클라이언트를 IM and Presence 서비스와 통합하는 경우 구축에서 DNS SRV를 활성화해야 합니다. XMPP 클라이언트는 DNS SRV 쿼리를 수행하여 통신할 XMPP 노드(IM and Presence 서비스)를 찾은 다음, XMPP 노드의 레코드 조회를 수행하여 IP 주소를 얻습니다.

참고 IM and Presence 서비스 구축에 여러 IM 도메인이 구성되어 있는 경우 각 도메인용 DNS SRV 레코드가 필요합니다. 모든 SRV 레코드는 동일한 결과 집합으로 확인될 수 있습니다.

II 부

시스템 구성



3 장

도메인 구성

도메인 개요 구성

IM and Presence 도메인 창에 다음 유형의 도메인이 표시됩니다.

- 관리자 관리 IM 주소 도메인. 수동으로 추가되었지만 사용자에게 아직 할당되지 않은 내부 도메인 또는 동기화 에이전트에 의해 자동으로 추가되었지만 그 이후 사용자의 도메인이 변경되어 더 이상 사용되지 않는 내부 도메인입니다.
- 시스템 관리 IM 주소 도메인. 구축 중에 사용자가 사용하며, 수동 또는 자동으로 추가할 수 있는 내부 도메인입니다.

IM and Presence 도메인 창에 나타나는 도메인은 활성화된 도메인입니다. 도메인을 활성화할 필요가 없습니다. 로컬 IM 주소 도메인을 수동으로 추가, 업데이트 및 삭제할 수 있습니다.

두 개의 클러스터에 도메인을 구성하여 피어 클러스터에서만 사용할 수 있습니다. 이렇게 하면 로컬 클러스터에서는 시스템 관리 도메인처럼 보이지만 피어 클러스터에서만 사용되는 것으로 식별됩니다.

Cisco Sync Agent 서비스는 로컬 클러스터에서(상호 클러스터링이 구성된 경우에는 피어 클러스터에서) 야간 감사를 수행하고 각 사용자의 디렉터리 URI를 확인하며, 고유한 도메인의 목록을 자동으로 작성합니다. 클러스터의 사용자에게 해당 도메인이 할당되면 관리자-관리에서 시스템-관리로 도메인이 변경됩니다. 클러스터의 사용자에 의해 사용되지 않는 도메인은 관리자-관리 도메인으로 다시 변경됩니다.

도메인 구성 예

Cisco Unified Communications Manager IM and Presence Service는 개수와 상관없이 DNS 도메인 전체에서 유연한 노드 구축을 지원합니다. 이 유연성을 지원하려면 구축 내 모든 IM and Presence 서비스

노드의 이름을 FQDN(정규화된 도메인 이름)으로 설정해야 합니다. IM and Presence 서비스에 대한 다음 샘플 노드 구축 옵션을 아래에서 설명합니다.

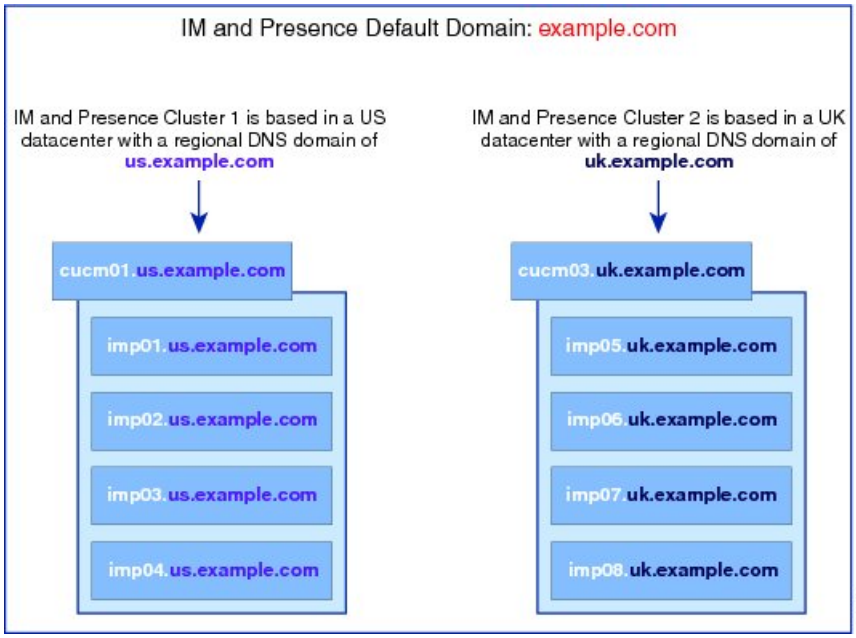
- 다른 DNS 도메인 및 하위 도메인이 있는 다중 클러스터
- 다른 DNS 도메인 및 하위 도메인이 있는 단일 클러스터
- DNS 도메인이 Unified Communications Manager 도메인과 다른 단일 클러스터

참고 특정 IM and Presence 서비스 노드 이름이 호스트 이름만을 기반으로 하는 경우 모든 IM and Presence 서비스 노드에서 동일한 DNS 도메인을 공유해야 합니다.

IM and Presence 서비스 기본 도메인 또는 시스템에서 호스트하는 다른 IM 도메인을 DNS 도메인과 맞출 필요는 없습니다. IM and Presence 서비스 구축에서는 공통 프레즌스 도메인을 사용하는 한편, 노드를 여러 DNS 도메인에 구축할 수 있습니다.

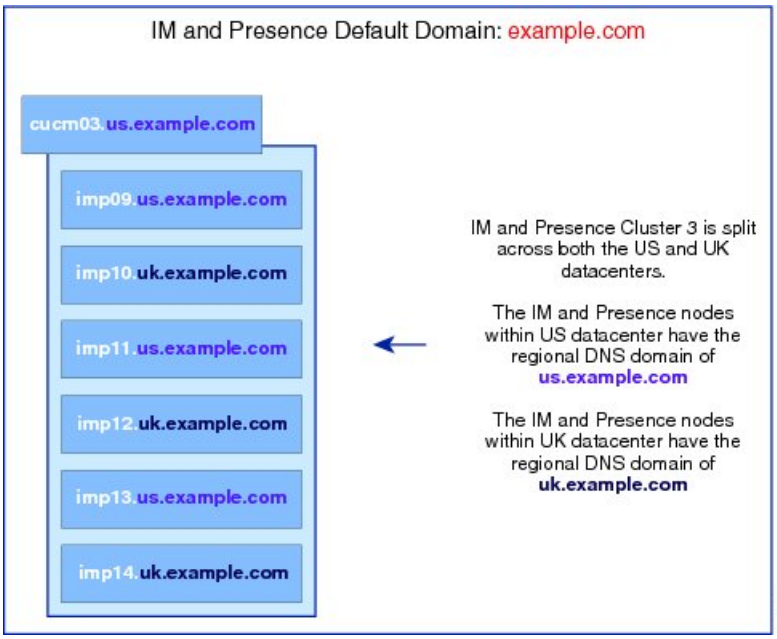
다른 **DNS** 도메인 및 하위 도메인이 있는 다중 클러스터

IM and Presence 서비스는 서로 다른 DNS 도메인 또는 하위 도메인에 있는 하나의 IM and Presence 서비스 클러스터와 연결된 노드를 피어 IM and Presence 서비스 클러스터를 형성하는 노드에 연결하도록 지원합니다. 아래의 다이어그램은 지원되는 샘플 구축 시나리오를 강조 표시합니다.



다른 **DNS** 도메인 및 하위 도메인이 있는 단일 클러스터

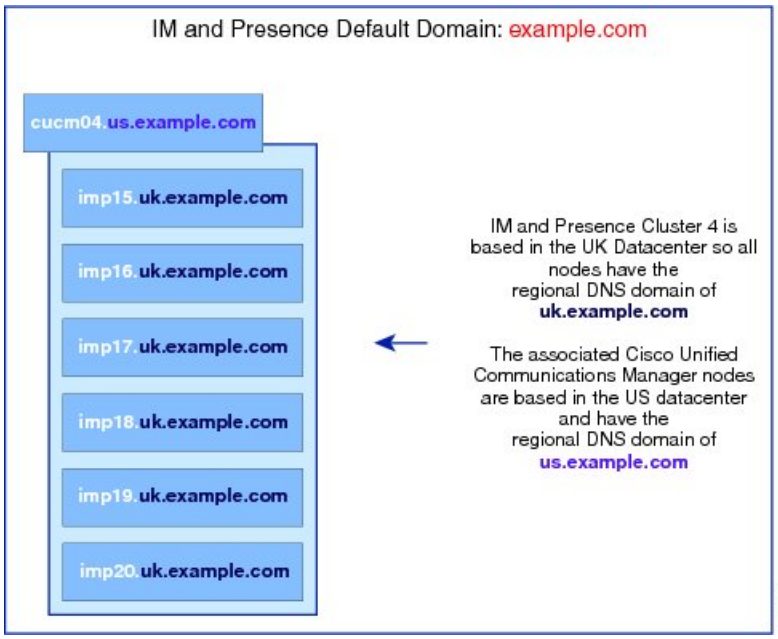
IM and Presence 서비스에서는 IM and Presence 서비스 클러스터 내 노드를 여러 DNS 도메인 또는 하위 도메인에 구축할 수 있도록 지원합니다. 아래의 다이어그램은 지원되는 샘플 구축 시나리오를 강조 표시합니다.



참고 프레즌스 이중화 그룹 내 두 노드가 서로 다른 DNS 도메인 또는 하위 도메인에 있는 시나리오에서도 고가용성은 완벽하게 지원됩니다.

DNS 도메인이 **Unified Communications Manager** 도메인과 다른 단일 클러스터

IM and Presence 서비스에서는 다른 DNS 도메인에 IM and Presence 서비스 노드를 연결된 Cisco 통합 커뮤니케이션 매니저 클러스터에 두는 것이 지원됩니다. 아래의 다이어그램은 지원되는 샘플 구축 시나리오를 강조 표시합니다.



참고 Cisco Unified Communications Manager와의 가용성 통합을 지원하려면 **CUCM** 도메인 SIP 프록시(CUCM Domain SIP Proxy) 서비스 파라미터가 Cisco Unified Communications Manager 클러스터의 DNS 도메인과 일치해야 합니다.

기본적으로 이 서비스 파라미터는 IM and Presence 데이터베이스 게시자 노드의 DNS 도메인으로 설정됩니다. IM and Presence 데이터베이스 게시자 노드의 DNS 도메인이 Cisco Unified Communications Manager 클러스터의 DNS 도메인과 다른 경우 Cisco Unified Communications Manager 클러스터의 도메인을 사용하도록 이 서비스 파라미터를 편집해야 합니다.

도메인 필수 조건 구성

- 이 기능을 이용하려면 모든 IM and Presence 서비스 및 Cisco Unified Communications Manager 노드와 클러스터에서 다중 도메인을 지원해야 합니다. IM and Presence 서비스 클러스터의 모든 노드가 릴리스 10.0 이상을 운영 중인지 확인하십시오.
- 주소 지정을 위한 디렉터리 URI를 구성하는지 확인하십시오. 자세한 내용은 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html에서 *Cisco Unified Communications Manager* 시스템 구성 설명서의 "URI 전화 걸기 구성"을 참조하십시오.

도메인 작업 흐름 구성

이 작업을 완료하여 IM and Presence 서비스에 대한 도메인을 구성합니다.

프로시저

	명령 또는 동작	목적
단계 **1**	고가용성 비활성화, 27 페이지	고가용성이 활성화된 경우 일시적으로 비활성화해야 합니다. 기본 도메인을 변경하려면 일시적으로 서비스를 중지해야 합니다. 고가용성이 활성화 된 상태에서 서비스를 중지하면 시스템 장애 조치가 발생합니다.
단계 **2**	IM and Presence 서비스 비활성화, 28 페이지	도메인을 변경하기 전에 필수 서비스를 중지합니다.
단계 **3**	IM and Presence 서비스의 기본 도메인 구성 , 29 페이지	IM and Presence 서비스 클러스터에 대한 기본 도메인 값을 구성합니다. 이 절차는 DNS 구축과 비 DNS 구축 모두에 적용할 수 있습니다.
단계 **4**	이러한 작업 중 하나를 수행합니다. • IM 주소 도메인 추가 또는 업데이트, 30 페이지 • IM 주소 도메인 삭제 , 31 페이지	(선택 사항) 로컬 클러스터에서 관리자-관리 도메인을 추가, 편집 또는 삭제하려는 경우에만 이러한 작업을 완료하십시오.
단계 **5**	XMPP 클라이언트 및 TLS 인증서 재생성, 32 페이지	TLS XMPP 페더레이션을 사용 중인 경우 계속 진행하여 새 XMPP 클라이언트와 TLS 인증서를 생성합니다.
단계 **6**	IM and Presence 서비스 시작, 32 페이지	도메인 구성을 완료한 후 서비스를 다시 시작합니다.
단계 **7**	프레즌스 이중화 그룹을 위한 고가용성 활성화, 33 페이지	고가용성이 구성된 경우 한 번 더 활성화합니다. 참고 고가용성을 활성화하기 전에 시작한 서비스가 모든 클러스터 노드에서 실행 중인지 확인하십시오.

고가용성 비활성화

고가용성을 구성한 경우 기본 도메인을 구성하기 전에 각 현재 이중화 그룹에서 해당 고 가용성을 비활성화해야 합니다. 기본 도메인 변경에 대한 서비스를 중지하면 고가용성이 활성화된 경우 장애 조치가 발생합니다.

참고 프레즌스 이중화 그룹 세부 정보 페이지는 클러스터에서 고가용성을 비활성화한 경우에도 모든 활성 JSM 세션을 보여줍니다.

시작하기 전에

각 프레즌스 이중화 그룹에서 각 클러스터 노드에 대한 활성 사용자 수를 기록합니다. Cisco Unified CM IM and Presence 관리의 (시스템 > 프레즌스 토폴로지) 창에서 이 정보를 찾을 수 있습니다. 나중에 고가용성을 다시 활성화할 때 이 숫자가 필요합니다.

프로시저

단계 **1** Cisco Unified CM 관리 사용자 인터페이스에서 시스템 > 프레즌스 이중화 그룹을 선택합니다.

단계 **2** 찾기를 클릭하고 그룹을 선택합니다.

단계 **3** 프레즌스 이중화 그룹 구성 창에서 고가용성 활성화 확인란을 선택 취소합니다.

단계 **4** 저장을 클릭합니다.

단계 **5** 각 프레즌스 이중화 그룹에 대해 이 절차를 반복합니다.

단계 **6** 완료되면 최소한 2분 정도 기다렸다가 클러스터에 새로운 HA 설정을 동기화한 다음 추가 변경을 수행합니다

다음에 수행할 작업

IM and Presence 서비스 비활성화, 28 페이지

IM and Presence 서비스 비활성화

이 절차를 사용하여 기본 도메인을 변경하기 전에 IM and Presence 서비스를 중지합니다. 클러스터의 모든 노드에서 이 절차를 수행합니다.

시작하기 전에

고가용성이 비활성화되어 있는지 확인하십시오. 자세한 내용은 고가용성 비활성화, 27 페이지를 참조하십시오.

프로시저

단계 **1** Cisco Unified IM and Presence 서비스 가용성에서 도구 > 제어 센터 - 네트워크 서비스를 선택합니다.

단계 **2** 서버 목록에서 서비스를 비활성할 노드를 선택하고 이동을 클릭합니다.

단계 **3** **IM and Presence** 서비스 영역에서 다음 서비스를 선택 취소합니다.

- **Cisco** 클라이언트 프로파일 에이전트
- **Cisco Sync Agent**
- **Cisco XCP** 라우터

단계 **4** 중지를 클릭합니다.

단계 **5** 관련 링크 드롭다운 목록에서 서비스 활성화를 선택하고 이동을 클릭합니다.

단계 **6** **IM and Presence** 서비스 영역에서 다음 서비스를 선택 취소합니다.

- **Cisco SIP Proxy**
- **Cisco Presence** 엔진

단계 **7** 저장을 클릭합니다.

단계 **8** 이러한 서비스를 비활성화한 모든 노드의 목록을 만듭니다. 기본 도메인에 대한 변경을 완료한 후에 서비스를 다시 시작해야 합니다.

다음에 수행할 작업

IM and Presence 서비스의 기본 도메인을 구성합니다.

- IM and Presence 서비스의 기본 도메인 구성 , 29 페이지

그렇지 않으면 기본 도메인이 이미 구성된 경우 이러한 작업 중 하나를 완료하여 도메인을 추가, 편집 또는 삭제합니다.

- IM 주소 도메인 추가 또는 업데이트, 30 페이지
- IM 주소 도메인 삭제 , 31 페이지

IM and Presence 서비스의 기본 도메인 구성

이 절차를 사용하여 IM and Presence 서비스 클러스터에 대한 기본 도메인 값을 구성합니다. 이 절차는 DNS 또는 비 DNS 구축에 적용할 수 있습니다.

이 절차를 수행하면 IM and Presence 서비스 클러스터의 기본 도메인만 변경됩니다. 해당 클러스터 내 임의의 IM and Presence 서비스 노드와 관련된 DNS 도메인은 변경되지 않습니다. IM and Presence 서비스 노드의 DNS 도메인 변경 방법에 대한 자세한 내용은 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html 에서 *Cisco Unified Communications Manager* 및 *IM and Presence* 서비스의 *IP* 주소 및 호스트 이름 변경을 참조하십시오.

참고 기본 도메인은 IM and Presence 서비스 게시자 노드를 Cisco Unified Communications Manager에 추가할 때 구성됩니다. 노드 설치 중 시스템이 Cisco Unified Communications Manager에서 기본 도메인 값을 검색하지 못하면 기본 도메인 값이 DOMAIN.NOT.SET으로 재설정됩니다. IM and Presence 서비스 기본 도메인 값을 유효한 도메인 값으로 변경하려면 이 절차를 사용하십시오.

시작하기 전에

고가용성이 비활성화되어 있고 필수 IM and Presence 서비스가 중지되었는지 확인하십시오. 자세한 내용은 IM and Presence 서비스 비활성화, 28 페이지의 내용을 참조하십시오.

프로시저

단계 1 IM and Presence 서비스 데이터베이스 게시자 노드에 로그인합니다.

단계 2 **Cisco Unified CM IM and Presence** 관리에서 프레즌스 > 설정 > 고급 구성을 선택합니다.

단계 3 기본 도메인을 선택합니다.

단계 4 도메인 이름 필드에 새 프레즌스 도메인을 입력하고 저장을 클릭합니다.

시스템 업데이트를 완료하는 데 최대 1시간 정도 걸릴 수 있습니다. 업데이트가 실패하면 재시도 버튼이 나타납니다. 재시도를 클릭하여 변경 사항을 다시 적용하거나 취소를 클릭합니다.

다음에 수행할 작업

TLS XMPP 페더레이션을 사용 중인 경우 XMPP 클라이언트 및 TLS 인증서 재생성, 32 페이지로 계속 진행합니다.

IM 주소 도메인 추가 또는 업데이트

로컬 클러스터에서 관리자-관리 도메인을 추가하거나 편집할 수 있습니다. 다른 클러스터와 연결된 시스템-관리 또는 관리자-관리 도메인은 편집할 수 없습니다.

시스템 관리 도메인은 사용되고 있는 상태이므로 편집할 수 없습니다. 해당 IM 주소 도메인의 시스템에 더 이상 사용자가 없는 경우(예: 사용자가 삭제됨) 시스템 관리 도메인은 자동으로 관리자 관리 도메인이 됩니다. 관리자 관리 도메인은 편집하거나 삭제할 수 있습니다.

시작하기 전에

고가용성이 비활성화되어 있고 필수 IM and Presence 서비스가 중지되었는지 확인하십시오. 자세한 내용은 다음 내용을 참조하십시오. IM and Presence 서비스 비활성화, 28 페이지

프로시저

단계 1 **Cisco Unified CM IM and Presence** 관리에서 프레즌스 > > 도메인을 선택합니다.

도메인 찾기 및 나열 창에 모든 관리자 관리 및 시스템 관리 IM 주소 도메인이 표시됩니다.

단계 2 다음 작업 중 하나를 수행합니다.

- 새로 추가를 클릭하여 새 도메인을 추가합니다. 도메인 창이 나타납니다.
- 도메인 목록을 편집할 도메인을 선택합니다. 도메인 창이 나타납니다.

단계 3 도메인 이름 필드에 최대 255자의 고유한 도메인 이름을 입력하고 저장을 클릭합니다.

각 도메인 이름은 클러스터에서 고유해야 합니다. 허용되는 값은 대/소문자(a-zA-Z), 숫자(0-9), 하이픈(-) 또는 점(.)입니다. 점은 도메인 레이블 구분 기호입니다. 도메인 레이블은 하이픈으로 시작할 수

없습니다. 마지막 레이블(예: .com)은 숫자로 시작해서는 안 됩니다. Abc.1om은 잘못된 도메인의 예입니다.

다음에 수행할 작업

TLS XMPP 페더레이션을 사용 중인 경우 XMPP 클라이언트 및 TLS 인증서 재생성, 32 페이지로 계속 진행합니다.

IM 주소 도메인 삭제

Cisco Unified CM IM and Presence 관리 GUI를 사용하여 로컬 클러스터에 있는 관리자 관리 IM 주소 도메인을 삭제할 수 있습니다.

시스템 관리 도메인은 사용되고 있는 상태이므로 삭제할 수 없습니다. 해당 IM 주소 도메인의 시스템에 더 이상 사용자가 없는 경우(예: 사용자가 삭제됨) 시스템 관리 도메인은 자동으로 관리자 관리 도메인이 됩니다. 관리자 관리 도메인은 편집하거나 삭제할 수 있습니다.

참고 로컬 및 피어 클러스터 모두에서 구성된 관리자 관리 도메인을 삭제하는 경우, 해당 도메인은 관리자 관리 도메인 목록에 남아 있기는 하지만 피어 클러스터에서만 구성된 것으로 표시됩니다. 항목을 완전히 제거하려면 구성된 모든 클러스터에서 항목을 삭제해야 합니다.

시작하기 전에

고가용성이 비활성화되어 있고 필수 IM and Presence 서비스가 중지되었는지 확인하십시오. 자세한 내용은 IM and Presence 서비스 비활성화, 28 페이지의 내용을 참조하십시오.

프로시저

단계 **1** **Cisco Unified CM IM and Presence** 관리에서 프레즌스 > 도메인을 선택합니다.

도메인 찾기 및 나열 창에 모든 관리자 관리 및 시스템 관리 IM 주소 도메인이 표시됩니다.

단계 **2** 다음 방법 중 하나를 사용하여 관리자 관리 도메인을 선택한 다음 선택한 항목 삭제를 클릭합니다.

- 삭제할 도메인 옆에 있는 확인란을 선택합니다.
- 모두 선택을 클릭하여 관리자 관리 도메인 목록에 있는 모든 도메인을 선택합니다.

팁 모두 지우기를 클릭하여 선택 항목을 모두 지웁니다.

단계 **3** 확인을 클릭하여 삭제를 확인하거나 취소를 클릭합니다.

다음에 수행할 작업

TLS XMPP 페더레이션을 사용 중인 경우 XMPP 클라이언트 및 TLS 인증서 재생성, 32 페이지로 계속 진행합니다.

XMPP 클라이언트 및 TLS 인증서 재생성

IM 도메인을 변경한 후에는 XMPP 클라이언트 또는 TLS 인증서를 재생성해야 합니다.

프로시저

단계 1 **Cisco Unified CM IM and Presence OS** 관리에서 보안 > 인증서 관리를 선택합니다.
단계 2 찾기를 클릭하여 인증서 목록을 생성합니다.
단계 3 **cup-xmpp-s2s** 인증서를 클릭합니다.
단계 4 인증서 세부정보 창에서 재생성을 클릭합니다.

IM and Presence 서비스 시작

기본 도메인을 변경한 후에 이 절차를 사용하여 모든 클러스터 노드에서 IM and Presence 서비스를 다시 시작합니다.

시작하기 전에

XMPP 클라이언트 및 TLS 인증서 재생성, 32 페이지

프로시저

단계 1 Cisco Unified IM and Presence 서비스 가용성에서 도구 > 제어 센터 - 네트워크 서비스를 선택합니다.
단계 2 서버 목록에서 서비스를 다시 활성화할 노드를 선택하고 이동을 클릭합니다.
단계 3 **IM and Presence** 서비스 영역에서 다음 서비스를 선택합니다.

- **Cisco** 클라이언트 프로파일 에이전트
- **Cisco Sync Agent**
- **Cisco XCP** 라우터

단계 4 재시작을 클릭합니다.
단계 5 관련 링크 드롭다운 목록에서 서비스 활성화를 선택하고 이동을 클릭합니다.
단계 6 **IM and Presence** 서비스 영역에서 다음 서비스를 선택합니다.

- **Cisco SIP Proxy**

- **Cisco Presence** 엔진

단계 **7** 저장을 클릭합니다.

다음에 수행할 작업

프레즌스 이중화 그룹을 위한 고가용성 활성화, 33 페이지

프레즌스 이중화 그룹을 위한 고가용성 활성화

기본 도메인을 변경하고 IM and Presence 서비스를 다시 시작한 후에는 프레즌스 이중화 그룹에 대해 고가용성을 활성화할 수 있습니다.

시작하기 전에

고가용성을 활성화하기 전에 모든 서비스가 IM and Presence 데이터베이스 게시자 노드 및 가입자 노드에서 실행되어야 합니다. 서비스를 다시 시작한 후 30분이 지나지 않은 경우 고가용성을 활성화하기 전에 Cisco Jabber 세션이 다시 생성되었는지 확인하십시오. 그렇지 않으면 세션이 생성되지 않은 Jabber 클라이언트에서 프레즌스가 작동하지 않습니다.

Cisco Jabber 세션 수를 얻으려면 모든 클러스터 노드에서 `show perf query counter "Cisco Presence Engine" Active JsmSessions` CLI 명령을 실행합니다. 활성 세션 수는 고가용성을 비활성화할 때 기록한 사용자 수와 일치해야 합니다.

다음 단계에서 Cisco RTMT(실시간 모니터링 도구)를 사용하여 게시자 및 가입자 모두에서 성능 카운터 `"Cisco Presence 엔진" ActiveJsmSessions`를 모니터링해야 합니다.

- 게시자 또는 가입자를 다시 시작한 후
- Cisco XCP 라우터를 다시 시작한 후
- Cisco Presence 엔진을 다시 시작한 후

고가용성을 활성화하기 전에 `"Cisco Presence 엔진" ActiveJsmSessions`가 노드에 할당된 사용자 수와 동일한지 확인해야 합니다.

참고 사용자 `ActiveJsmSessions` 생성 진행이 완료된 후에만 고가용성을 활성화해야 합니다.

프로시저

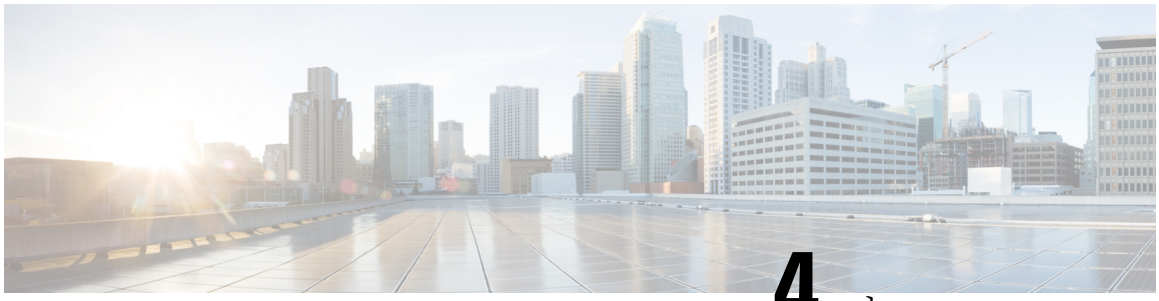
단계 **1** Cisco Unified CM 관리 사용자 인터페이스에서 시스템 > 프레즌스 이중화 그룹을 선택합니다.

단계 **2** 찾기를 클릭하고 그룹을 선택합니다.
프레즌스 이중화 그룹 구성 창이 표시됩니다.

단계 **3** 고가용성 활성화 확인란을 선택합니다.

단계 **4** 저장을 클릭합니다.

단계 **5** 각 프레즌스 이중화 그룹에 대해 이 절차를 반복합니다.



4 장

IPv6 구성

IPv6 구성 개요

IM and Presence 서비스와 Cisco Unified Communications Manager 사이의 연결에 IPv4를 사용하는 경우에도 IM and Presence 서비스의 외부 인터페이스에는 IPv6을 사용할 수 있습니다.

IM and Presence 서비스 노드에서 다음 항목 중 하나에 대해 IPv6을 구성하면 노드는 들어오는 IPv4 패킷을 허용하지 않고 자동으로 IPv4를 사용하지 않습니다.

- 외부 데이터베이스에 대한 연결
- LDAP 서버에 대한 연결
- Exchange 서버에 대한 연결
- 페더레이션 구축

페더레이션의 경우, IPv6이 활성화되어 있는 외부 엔터프라이즈에 대한 페더레이션 링크를 지원하려면 IM and Presence 서비스에서 IPv6을 활성화해야 합니다. IM and Presence 서비스 노드 및 페더레이션 엔터프라이즈 간에 ASA가 설치되어 있는 경우에도 마찬가지입니다. ASA는 IM and Presence 서비스 노드에 대해 투명합니다.

명령줄 인터페이스를 사용하여 IPv6 매개 변수를 구성하는 방법에 대한 자세한 내용은 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html에서 *Cisco Unified Communications Manager* 관리 설명서 및 *Cisco Unified Communications Solutions*용 명령줄 인터페이스 설명서를 참조하십시오.

IPv6 작업 흐름 구성

프로시저

	명령 또는 동작	목적
단계 1	IM and Presence 서비스용 Eth0에서 IPv6 활성화, 36 페이지	클러스터의 각 IM and Presence 서비스 노드의 Eth0 포트에서 IPv6을 활성화합니다. 변경 사항을 적용하려면 각 노드를 재부팅해야 합니다.
단계 2	IPv6 엔터프라이즈 매개 변수 활성화, 37 페이지	Eth0 포트에서 IPv6을 활성화한 후에는 IM and Presence 서비스 클러스터에 대해 IPv6 엔터프라이즈 파라미터를 활성화해야 합니다.
단계 3	서비스 다시 시작 , 37 페이지	변경 사항을 적용하려면 IM and Presence 서비스를 다시 시작해야 합니다.
단계 4	IM and Presence 노드에 IPv6 주소 할당, 38 페이지	IM and Presence 서비스 노드에 IPv6 주소를 할당합니다.

IM and Presence 서비스용 Eth0에서 IPv6 활성화

클러스터에 있는 각 IM and Presence 서비스 노드의 Eth0 포트에서 IPv6을 활성화하려면 Cisco Unified IM and Presence Operating System 관리 GUI를 사용합니다.

프로시저

단계 1 **Cisco Unified IM and Presence OS** 관리에서 설정 > **IP** > 이더넷 **IPv6**을 선택합니다.

단계 2 이더넷 IPv6 구성 창에서 **IPv6** 활성화 확인란을 선택합니다.

단계 3 주소 소스를 선택합니다.

- 라우터 광고
- DHCP
- 수동 입력

수동 입력을 선택한 경우 **IPv6** 주소, 서브넷 마스크 및 기본 게이트웨이 값을 입력합니다.

단계 4 재부팅 시 업데이트 확인란을 선택합니다.

팁 나중에 노드를 수동으로 재부팅하려는 경우(예: 예약된 유지 관리 기간 중) 재부팅 시 업데이트 확인란을 선택하지 마십시오. 그러나 노드를 재부팅하기 전에는 변경 사항이 적용되지 않습니다.

단계 **5** 저장을 클릭합니다.

재부팅 시 업데이트 확인란을 선택한 경우 노드가 재부팅되고 변경 사항이 적용됩니다.

다음에 수행할 작업

IPv6 엔터프라이즈 매개 변수 활성화, 37 페이지

IPv6 엔터프라이즈 매개 변수 활성화

Cisco Unified CM IM and Presence 관리를 사용하여 IM and Presence 서비스 클러스터에 대해 IPv6 엔터프라이즈 파라미터를 활성화합니다.

시작하기 전에

IM and Presence 서비스용 Eth0에서 IPv6 활성화, 36 페이지

프로시저

단계 **1** **Cisco Unified CM IM and Presence** 관리에서 시스템 > 엔터프라이즈 파라미터를 선택합니다.

단계 **2** 엔터프라이즈 파라미터 구성 창의 IPv6 패널에서 **True**를 선택합니다.

단계 **3** 저장을 클릭합니다.

다음에 수행할 작업

서비스 다시 시작 , 37 페이지 변경 사항을 적용합니다.

서비스 다시 시작

이 절차를 사용하여 클러스터에 대해 IPv6 엔터프라이즈 파라미터를 활성화한 후 IM and Presence 서비스를 다시 시작합니다.

팁 Cisco Unified CM IM and Presence 관리를 사용하여 시스템 다시 시작 알림을 모니터링하려면 시스템 > 알림을 선택합니다.

시작하기 전에

IPv6 엔터프라이즈 매개 변수 활성화, 37 페이지

프로시저

단계 **1** Cisco Unified IM and Presence 서비스 가용성에서 도구 > 제어 센터 - 네트워크 서비스를 선택합니다.

단계 **2** 서버 목록에서 서비스를 다시 활성화할 노드를 선택하고 이동을 클릭합니다.

단계 **3** **IM and Presence** 서비스 영역에서 **Cisco XCP** 라우터를 선택합니다.

단계 **4** 재시작을 클릭합니다.

단계 **5** 관련 링크 드롭다운 목록에서 서비스 활성화를 선택하고 이동을 클릭합니다.

단계 **6** **IM and Presence** 서비스 영역에서 다음 서비스를 선택합니다.

- **Cisco SIP Proxy**
- **Cisco Presence** 엔진

단계 **7** 저장을 클릭합니다.

IM and Presence 노드에 IPv6 주소 할당

Cisco Unified Communications Manager에서 이 절차를 사용하여 IM and Presence 노드 IPv6 주소를 할당합니다.

시작하기 전에

또한 Cisco Unified OS 관리에서 IPv6 Eth0 포트를 활성화하고 IPv6 엔터프라이즈 파라미터를 활성화해야 합니다.

프로시저

단계 **1** Cisco Unified Communications Manager 게시자 노드에 로그인합니다.

단계 **2** Cisco Unified CM 관리에서 시스템 > 서버를 선택합니다.

단계 **3** 다음 작업 중 하나를 수행합니다.

- 새 서버를 추가하려면 새로 추가를 클릭합니다.
- 기존 서버를 업데이트하려면 편집할 서버를 클릭합니다.

단계 **4** 새 서버를 추가하는 경우 서버 유형 드롭다운 메뉴에서 **CUCM IM and Presence**를 선택하고 다음을 클릭합니다.

단계 **5** 서버의 **IPv6** 주소를 입력합니다.

단계 **6** 저장을 클릭합니다.

단계 **7** 각 IM and Presence 서비스 클러스터 노드에 대해 반복합니다.

IM and Presence Service용 Eth0에서 IPv6 비활성화

IPv6을 비활성화하려는 경우 IPv6을 사용하지 않으려는 클러스터에 있는 각 IM and Presence 서비스 노드의 Eth0 포트에서 IPv6을 비활성화하려면 **Cisco Unified IM and Presence Operating System** 관리 GUI를 사용합니다. 변경 사항을 적용하려면 노드를 재부팅해야 합니다.

참고 클러스터에 있는 어떤 노드에서도 IPv6을 사용하지 않으려면 클러스터에 대한 IPv6 엔터프라이즈 파라미터를 비활성화해야 합니다.

프로시저

단계 **1** **Cisco Unified CM IM and Presence OS** 관리에서 설정 > **IP** > 이더넷 **IPv6**을 선택합니다.

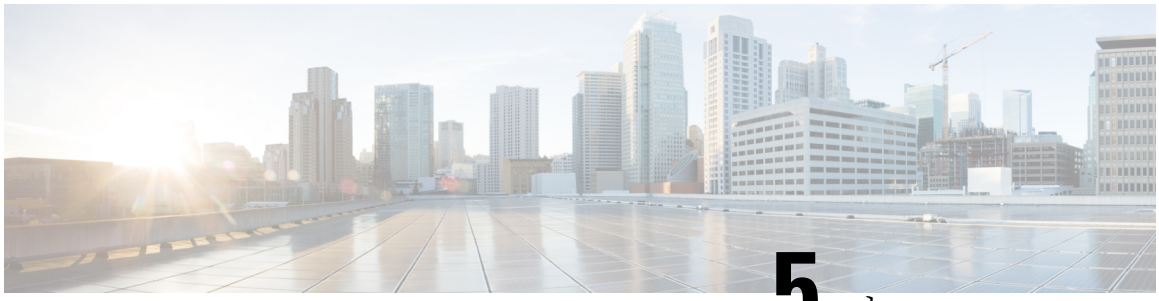
단계 **2** 이더넷 IPv6 구성 창에서 **IPv6** 활성화 확인란을 선택 취소합니다.

단계 **3** 재부팅 시 업데이트 확인란을 선택합니다.

팁 나중에 노드를 수동으로 재부팅하려는 경우(예: 예약된 유지 관리 기간 중) 재부팅 시 업데이트 확인란을 선택하지 마십시오. 그러나 노드를 재부팅하기 전에는 변경 사항이 적용되지 않습니다.

단계 **4** 저장을 클릭합니다.

재부팅 시 업데이트 확인란을 선택한 경우 노드가 재부팅되고 변경 사항이 적용됩니다.



5 장

IM 주소 체계 구성

IM 주소 지정 체계 개요

IM and Presence 서비스는 두 개의 IM 주소 지정 체계를 지원합니다.

- *UserID@Default_Domain*은 IM and Presence 서비스 설치 시 기본 IM 주소 체계입니다.
- 디렉터리 URI IM 주소 체계는 다중 도메인, 사용자 전자 메일 주소와의 정렬 및 Microsoft SIP URI 와의 정렬을 지원합니다.

모든 IM and Presence 서비스 클러스터에서 동일한 IM 주소 체계를 사용해야 합니다.

User@Default_Domain을 사용하는 IM 주소

IM and Presence 서비스의 기본 주소 지정 체계는 *UserID@Default_Domain*입니다.

UserID@Default_Domain IM 주소 체계를 사용하면 모든 IM 주소는 기본 단일 IM 도메인의 일부입니다. 기본 도메인 값은 클러스터 전체에서 일관성이 있어야 합니다. IM 주소는 IM and Presence 기본 도메인의 일부이므로 다중 도메인은 지원되지 않습니다.

UserID는 자유 형식이거나 LDAP와 동기화할 수 있습니다. 다음 필드가 지원됩니다.

- sAMAccountName
- UPN(사용자 계정 이름)
- 전자 메일 주소
- 직원 번호
- 전화 번호

UserID를 Cisco Unified Communications Manager의 LDAP 필드로 매핑하는 경우 해당 LDAP 매핑은 클러스터 전체에서 일관성이 있어야 합니다.

UserID를 전자 메일 주소에 매핑할 수 있지만, 이것이 IM URI와 전자 메일 주소가 동일함을 의미하지는 않습니다. 대신 <*email-address*>*@Default_Domain*이 됩니다. 예를 들어, `amckenzie@example.com@sales-example.com`입니다. AD(Active Directory) 매핑 설정을 선택하면 IM and Presence 서비스 클러스터에 속한 모든 사용자에게 전역으로 적용됩니다. 개별 사용자에 대해 서로 다른 매핑을 설정할 수는 없습니다.

디렉터리 URI를 사용하는 IM 주소

디렉터리 URI 주소 체계는 사용자의 IM 주소를 Cisco Unified Communications Manager 디렉터리 URI와 정렬합니다.

디렉터리 URI IM 주소 체계에서는 다음과 같은 IM 주소 지정 기능을 제공합니다.

- 다중 도메인 지원. IM 주소는 단일 IM and Presence 서비스 도메인을 사용할 필요가 없습니다.
- 사용자 전자 메일 주소와 정렬. 사용자의 전자 메일 주소와 정렬되도록 Cisco Unified Communications Manager 디렉터리 URI를 구성하여 전자 메일, IM, 음성 및 비디오 통신을 위한 일관된 ID를 제공할 수 있습니다.
- Microsoft SIP URI와 정렬. Microsoft SIP URI와 정렬되도록 Cisco Unified Communications Manager 디렉터리 URI를 구성하여, Microsoft OCS/Lync에서 IM and Presence 서비스로 마이그레이션해도 사용자의 ID가 유지되도록 할 수 있습니다.

IM 주소 체계로 디렉터리 URI를 사용하도록 노드를 구성하는 경우에는 디렉터리 URI를 지원하는 클라이언트만 구축하는 것이 좋습니다. 디렉터리 URI IM 주소 체계가 활성화되면 디렉터리 URI를 지원하지 않는 클라이언트는 작동하지 않습니다. 디렉터리 URI를 지원하지 않는 클라이언트를 구축한 경우에는 *UserID@Default_Domain* IM 주소 체계를 사용하고, 디렉터리 URI IM 주소 체계는 사용하지 않는 것이 좋습니다.

디렉터리 URI IM 주소 설정은 전역이므로 클러스터의 모든 사용자에게 적용됩니다. 클러스터의 개별 사용자에 대해 서로 다른 URI IM 주소를 설정할 수 없습니다.

외부 LDAP 디렉터리에서 디렉터리 URI를 제공하는 방법에 대한 자세한 내용은 LDAP 디렉터리 구성, 79 페이지의 내용을 참조하십시오.

여러 IM 도메인

IM and Presence 서비스는 여러 IM 주소 도메인에서 IM 주소 지정을 지원하며 시스템의 모든 도메인을 자동으로 나열합니다. 도메인을 추가, 편집 또는 삭제할 수 있습니다. IM 도메인 구성에 대한 자세한 내용은 도메인 개요 구성, 23 페이지의 내용을 참조하십시오.

Cisco Expressway와 상호 운용되는 경우, http://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-maintenance-guides-list.html에서 *Cisco Expressway* 관리자 설명서를 참조하십시오.

IM 주소 지정 체계 필수 조건

사용하는 IM and Presence 서비스 기본 도메인 및 IM 주소 체계는 모든 IM and Presence 서비스 클러스터에서 일관성이 있어야 합니다. 시작하기 전에, IM and Presence 서비스의 기본 도메인 구성 , 29 페이지

설정하는 IM 주소 체계는 모든 사용자 JID에 영향을 미치며, 설정이 다를 수 있는 클러스터 간 통신을 중단하지 않은 채 단계적인 방식으로 수행될 수는 없습니다.

구축된 클라이언트 중 디렉터리 URI를 IM 주소로서 지원하지 않는 것이 있으면 관리자는 디렉터리 URI IM 주소 체계를 비활성화해야 합니다.

IM 주소 지정 체계 작업 흐름 구성

IM 주소 지정 체계를 구성하려면 다음 순서대로 이 작업을 완료합니다.

프로시저

	명령 또는 동작	목적
단계 **1**	사용자 프로비저닝 확인, 44 페이지	최종 사용자가 올바르게 프로비저닝되고 중복되거나 유효하지 않은 사용자가 없는지 확인합니다.
단계 **2**	고가용성 비활성화, 44 페이지	프레즌스 이중화 그룹의 고가용성을 일시적으로 비활성화해야 합니다. IM 주소 지정 체계를 구성하려면 일시적으로 서비스를 중지해야 합니다. 고가용성이 활성화된 상태에서 서비스를 중지하는 경우 시스템 장애 조치가 발생합니다.
단계 **3**	서비스 중지, 45 페이지	IM 주소 지정 체계 구성을 업데이트하기 전에 필수 IM and Presence 서비스를 중지합니다. 지정된 순서대로 서비스를 중지해야 합니다.
단계 **4**	IM 주소 지정 체계 할당, 46 페이지	이 절차를 사용하여 새 도메인 및 IM 주소 체계를 구성하거나 기존 도메인 및 주소 체계를 업데이트합니다.
단계 **5**	서비스 다시 시작, 47 페이지	IM 주소 지정 체계를 구성했으면, 서비스를 다시 시작합니다. 사용자 주소 정보를 업데이트하거나 새 사용자를 프로비저닝하기 전에 이 작업을 수행해야 합니다. 서비스를 다시 시작할 때 미리 정해진 순서를 따라야 합니다.

	명령 또는 동작	목적
단계 **6**	고가용성 활성화, 48 페이지	IM 주소 지정 체계를 구성하고 IM and Presence 서비스를 다시 시작한 후 프레즌스 이중화 그룹의 고가용성을 활성화할 수 있습니다. 고가용성을 활성화하기 전에 모든 서비스가 IM and Presence 데이터베이스 게시자 노드 및 가입자 노드에서 실행되어야 합니다.
단계 **7**	디렉터리 **URI**을 IM 주소 지정 체계로 선택한 경우: • 디렉터리 URI에 대해 LDAP 소스 할당, 49 페이지 • 수동으로 디렉터리 URI 할당, 50 페이지	(선택 사항) 외부 LDAP 디렉터리의 사용자를 동기화하려면 디렉터리 URI 값에 대한 LDAP 소스 필드를 설정합니다. 비 LDAP 사용자의 경우 디렉터리 URI를 수동으로 제공해야 합니다. 이 작업은 사용자별로 또는 벌크 관리 도구를 통해 수행할 수 있습니다.

사용자 프로비저닝 확인

이 절차를 사용하여 주소 지정 체계를 구성하기 전에 최종 사용자가 올바르게 프로비저닝되었는지 확인합니다.

프로시저

단계 **1** Cisco Unified CM IM and Presence 관리에서 진단 > 시스템 문제 해결 도구를 선택합니다.
시스템 문제 해결 도구가 실행됩니다.

단계 **2** 사용자 문제 해결 도구 섹션에서 최종 사용자가 올바르게 프로비저닝되고 중복되거나 유효하지 않은 사용자가 없는지 확인합니다.

다음에 수행할 작업

고가용성 비활성화, 44 페이지

고가용성 비활성화

클러스터의 각 프레즌스 이중화 그룹에서 고가용성을 비활성화합니다. 주소 지정 체계를 편집하려면 서비스를 일시적으로 중지해야 합니다. 고가용성이 활성화된 상태에서 서비스를 중지하는 경우 시스템 장애 조치가 발생합니다.

참고 프레즌스 이중화 그룹 세부 정보 페이지는 클러스터에서 고가용성을 비활성화한 경우에도 모든 활성 JSM 세션을 보여줍니다.

시작하기 전에

각 프레즌스 이중화 그룹에서 각 클러스터 노드에 대한 활성 사용자 수를 기록합니다. Cisco Unified CM IM and Presence 관리의 (시스템 > 프레즌스 토폴로지) 창에서 이 정보를 찾을 수 있습니다. 나중에 고가용성을 다시 활성화할 때 이 숫자가 필요합니다.

프로시저

단계 **1** Cisco Unified CM 관리 사용자 인터페이스에서 시스템 > 프레즌스 이중화 그룹을 선택합니다.

단계 **2** 찾기를 클릭하고 그룹을 선택합니다.

단계 **3** 프레즌스 이중화 그룹 구성 창에서 고가용성 활성화 확인란을 선택 취소합니다.

단계 **4** 저장을 클릭합니다.

단계 **5** 각 프레즌스 이중화 그룹에 대해 이 절차를 반복합니다.

단계 **6** 완료되면 최소한 2분 정도 기다렸다가 클러스터에 새로운 HA 설정을 동기화한 다음 추가 변경을 수행합니다

다음에 수행할 작업

서비스 중지, 45 페이지

서비스 중지

IM 주소 지정 체계 구성을 업데이트하기 전에 필수 IM and Presence 서비스를 중지합니다. 지정된 순서대로 서비스를 중지해야 합니다.

시작하기 전에

고가용성 비활성화, 44 페이지

프로시저

단계 **1** **Cisco Unified IM and Presence** 서비스 가용성에서 도구 > 제어 센터 – 네트워크 서비스를 선택합니다.

단계 **2** 서비스를 선택하고 중지 버튼을 클릭하여 다음 IM and Presence 서비스를 다음 순서대로 중지합니다.

a) **Cisco Sync Agent**

b) **Cisco** 클라이언트 프로파일 에이전트

단계 **3** 두 서비스가 중지된 후 도구 > 제어 센터-기능 서비스를 선택하고 다음 순서대로 다음과 같은 서비스를 중지합니다.

a) **Cisco Presence** 엔진

b) **Cisco SIP Proxy**

단계 **4** 두 서비스가 중지된 후 도구 > 제어 센터-기능 서비스를 선택하고 다음과 같은 서비스를 중지합니다.

- **Cisco XCP** 라우터

참고 XCP 라우터 서비스를 중지하면 모든 관련 XCP 기능 서비스도 자동으로 중지됩니다.

다음에 수행할 작업

IM 주소 지정 체계 할당, 46 페이지

IM 주소 지정 체계 할당

이 절차를 사용하여 새 도메인 및 IM 주소 체계를 구성하거나 기존 도메인 및 주소 체계를 업데이트합니다.

참고 구성하는 IM 주소 지정 체계는 모든 클러스터 간에 일관성이 있어야 합니다.

시작하기 전에

서비스 중지, 45 페이지

프로시저

단계 **1** **Cisco Unified CM IM and Presence** 관리에서 프레즌스 > 설정 > 고급 구성을 선택합니다.

단계 **2** 새 기본 도메인을 할당하려면 기본 도메인 확인란을 선택하고 텍스트 상자에 새 도메인을 입력합니다.

단계 **3** 주소 체계를 변경하려면 **IM** 주소 체계 확인란을 선택하고 드롭다운 목록 상자에서 다음 옵션 중 하나를 선택합니다.

- **UserID@[Default_Domain]** - 각 IM 사용자 주소는 기본 도메인과 함께 UserID에서 파생됩니다. 이 값이 기본 설정입니다.
- 디렉터리 **URI** - 각 IM 사용자 주소는 Cisco Unified Communications Manager에서 해당 사용자에 대해 구성된 디렉터리 URI와 일치합니다.

  참고 이 옵션을 선택하면 구축된 모든 클라이언트는 IM 주소로 디렉터리 URI를 지원해야 하며 EDI 기반 또는 UDS 기반 디렉터리 통합을 사용해야 합니다. Jabber와의 UDS 기반 통합의 경우 Jabber 릴리스 10.6 이상을 실행해야 합니다.

단계 **4** 저장을 클릭합니다.

상태 영역에서 업데이트 진행 상황을 모니터링할 수 있습니다.

IM 주소 체계로 디렉터리 URI를 선택한 경우, 구축된 클라이언트에서 여러 도메인을 지원하도록 할 것인지 묻는 프롬프트가 표시될 수 있습니다. 확인을 클릭하여 계속 진행하거나 취소를 클릭합니다.

디렉터리 URI 설정이 유효하지 않으면 대화 상자가 나타납니다. 확인을 클릭하여 계속 진행하거나 취소를 클릭한 다음, IM 주소 체계를 구성하기 전에 사용자 설정을 수정합니다.

시스템 업데이트를 완료하는 데 최대 1시간 정도 걸릴 수 있습니다. 재시도를 클릭하여 변경 사항을 다시 적용하거나 취소를 클릭합니다.

다음에 수행할 작업

user@default_domain을 주소 지정 체계로 구성하고 사용자가 디렉터리 URI를 사용하지 않는 경우 서비스 다시 시작, 47 페이지으로 진행합니다.

주소 지정 체계로 디렉터리 URI를 구성한 경우 다음 옵션 중 하나를 선택합니다.

- 디렉터리 URI에 대해 LDAP 소스 할당, 49 페이지
- 수동으로 디렉터리 URI 할당, 50 페이지

IM 주소 예

IM and Presence 서비스에 사용할 수 있는 IM 주소 옵션의 샘플입니다.

IM and Presence 서비스 기본 도메인**:** cisco.com

사용자**:** John Smith

사용자 **ID:** js12345

메일 **ID:** jsmith@cisco-sales.com

SIPURI: john.smith@webex.com

IM 주소 형식	디렉터리 **URI** 매핑	**IM** 주소
<userid>@<domain>	해당 없음	js12345@cisco.com
디렉터리 URI	mailid	jsmith@cisco-sales.com
디렉토리 URI	msRTCSIP-PrimaryUserAddress	john.smith@webex.com

서비스 다시 시작

IM 주소 지정 체계를 구성했으면, 서비스를 다시 시작합니다. 사용자 주소 정보를 업데이트하거나 새 사용자를 프로비저닝하기 전에 이 작업을 수행해야 합니다. 서비스를 다시 시작할 때 미리 정해진 순서를 따라야 합니다.

시작하기 전에

- IM 주소 지정 체계 할당, 46 페이지

- 주소 지정 체계로 디렉터리 URI를 구성한 경우 서비스를 다시 시작하기 전에 다음 옵션 중 하나를 완료합니다.
  - 디렉터리 URI에 대해 LDAP 소스 할당, 49 페이지
  - 수동으로 디렉터리 URI 할당, 50 페이지

프로시저

단계 **1** **Cisco Unified IM and Presence** 서비스 가용성에서 도구 > 제어 센터 – 네트워크 서비스를 선택합니다.

단계 **2** 서비스를 선택하고 시작 버튼을 클릭하여 다음 서비스를 시작합니다.

- **Cisco XCP** 라우터

단계 **3** 서비스가 시작되면 도구 > 제어 센터 - 기능 서비스를 선택하고 다음 순서대로 다음과 같은 서비스를 중지합니다.

a) **Cisco SIP Proxy**
b) **Cisco Presence** 엔진

단계 **4** 다음 단계로 진행하기 전에 모든 노드에서 Cisco Presence 엔진 서비스가 실행 중인지 확인합니다.

단계 **5** 도구 > 제어 센터 - 네트워크 서비스를 선택하고 다음 순서대로 다음과 같은 서비스를 시작합니다.

a) **Cisco** 클라이언트 프로파일 에이전트
b) **Cisco Sync Agent**

다음에 수행할 작업

고가용성 활성화, 48 페이지

고가용성 활성화

IM 주소 지정 체계를 구성하고 서비스를 다시 시작한 후에 이 절차를 사용하여 클러스터에서 각 프레즌스 이중화 그룹에 대해 고가용성을 다시 활성화합니다

시작하기 전에

고가용성을 활성화하기 전에 모든 서비스가 IM and Presence 데이터베이스 게시자 노드 및 가입자 노드에서 실행되어야 합니다. 서비스를 다시 시작한 후 30분이 지나지 않은 경우 고가용성을 활성화하기 전에 Cisco Jabber 세션이 다시 생성되었는지 확인하십시오. 그렇지 않으면 세션이 생성되지 않은 Jabber 클라이언트에서 프레즌스가 작동하지 않습니다.

Cisco Jabber 세션 수를 얻으려면 모든 클러스터 노드에서 `show perf query counter Cisco Presence Engine Active JsmSessions` CLI 명령을 실행합니다. 활성 세션 수는 고가용성을 비활성화할 때 기록한 사용자 수와 일치해야 합니다.

프로시저

단계 1 Cisco Unified IM and Presence 서비스 가용성에서 도구 > 제어 센터 - 네트워크 서비스를 선택합니다.
단계 2 서버 목록에서 서비스를 다시 활성화할 노드를 선택하고 이동을 클릭합니다.
단계 3 **IM and Presence** 서비스 영역에서 다음 서비스를 선택합니다.

- **Cisco** 클라이언트 프로파일 에이전트
- **Cisco Sync Agent**
- **Cisco XCP** 라우터

단계 4 재시작을 클릭합니다.
단계 5 관련 링크 드롭다운 목록에서 서비스 활성화를 선택하고 이동을 클릭합니다.
단계 6 **IM and Presence** 서비스 영역에서 다음 서비스를 선택합니다.

- **Cisco SIP Proxy**
- **Cisco Presence** 엔진

단계 7 저장을 클릭합니다.

디렉터리 URI에 대해 LDAP 소스 할당

외부 LDAP 디렉터리에서 사용자를 동기화하는 경우 이 절차를 사용하여 디렉터리 URI를 할당하는 데 사용되는 외부 LDAP 디렉터리 소스 필드를 할당할 수 있습니다. LDAP 디렉터리 동기화가 발생하면 구성하는 필드 값에서 디렉터리 URI가 할당됩니다.

참고 초기 동기화가 이미 발생한 경우 Cisco Unified Communications Manager의 기존 LDAP 구성에 편집을 적용할 수 없습니다. 외부 LDAP 디렉터리에 추가된 새 항목을 동기화 할 수 있지만 Cisco Unified Communications Manager에서 LDAP 구성을 편집할 수는 없습니다. LDAP 디렉터리를 이미 동기화한 경우:

- 벌크 관리 도구를 사용하여 디렉터리 URI를 사용자에게 할당합니다. 자세한 내용은 *Cisco Unified Communications Manager* 벌크 관리 설명서를 참조하십시오.
- 사용자에게 디렉터리 URI를 수동으로 할당

시작하기 전에

IM 주소 지정 체계 할당, 46 페이지

프로시저

단계 1 Cisco Unified CM 관리에서 시스템 > **LDAP** > **LDAP** 디렉터리를 선택합니다.

단계 2 디렉터리 **URI** 드롭다운 목록에서 다음 옵션 중 하나를 선택합니다.

- 메일: 디렉터리 URI를 사용자 전자 메일 주소에 매핑하여 전자 메일, IM, 음성 및 비디오 통신을 위해 일관된 ID를 제공합니다.
- **msRTCSIP-PrimaryUserAddress**: 디렉터리 URI를 Microsoft OCS/Lync SIP URI에 매핑합니다.

참고 디렉터리 동기화는 LDAP 동기화가 발생할 때까지 프로비저닝되지 않습니다. LDAP 디렉터리 동기화 구성에 대한 자세한 내용은 LDAP 디렉터리 구성, 79 페이지의 내용을 참조하십시오.

다음에 수행할 작업

서비스 다시 시작, 47 페이지

수동으로 디렉터리 **URI** 할당

LDAP를 사용하지 않는 경우 이 절차를 사용하여 사용자별로 수동으로 디렉터리 URI를 입력할 수 있습니다.

참고 벌크 관리 도구를 사용하여 csv 파일을 통해 다수의 최종 사용자에 대한 디렉터리 URI를 제공할 수도 있습니다. 벌크 관리에 대한 자세한 내용은 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html에서 *Cisco Unified Communications Manager* 벌크 관리 설명서를 참조하십시오.

아직 LDAP 디렉터리를 동기화하지 않은 경우 LDAP 디렉터리 동기화를 통해 사용자의 디렉터리 URI를 프로비저닝할 수 있습니다.

시작하기 전에

IM 주소 지정 체계 할당, 46 페이지

프로시저

단계 1 **Cisco Unified CM** 관리에서 사용자 관리 > 최종 사용자를 선택합니다.

단계 2 적절한 검색 조건을 입력하고 찾기를 클릭합니다.

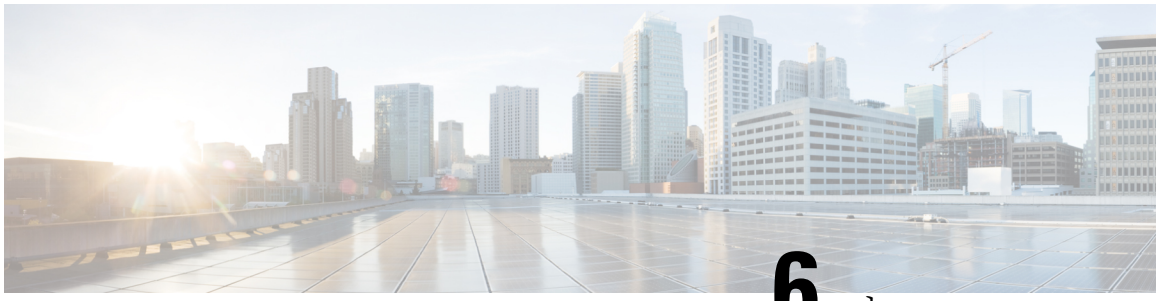
단계 3 구성하려는 최종 사용자를 선택합니다.

단계 4 사용자 정보 영역에서 디렉터리 **URI** 필드에 디렉터리 URI를 입력합니다.

단계 **5** 저장을 클릭합니다.

다음에 수행할 작업

서비스 다시 시작, 47 페이지



6 장

리던던시 및 고가용성 구성

프레즌스 이중화 그룹 개요

프레즌스 이중화 그룹은 동일한 클러스터의 두 개의 IM and Presence 서비스 노드로 구성됩니다. 프레즌스 이중화 그룹의 각 노드는 피어 노드의 상태 또는 하트비트를 모니터링합니다. IM and Presence 서비스 클라이언트 및 애플리케이션에 대한 중복 및 복구 기능을 모두 제공하도록 프레즌스 이중화 그룹을 구성할 수 있습니다.

- 장애 조치 - 그룹의 IM and Presence 서비스 노드에서 하나 이상의 중요 서비스가 실패하거나 그룹의 한 노드가 실패하는 경우 프레즌스 이중화 그룹에서 발생합니다. 클라이언트 해당 그룹의 다른 IM and Presence 서비스 노드에 자동으로 연결됩니다.
- 폴백 - 다음과 같은 상태에 있는 경우 CLI 또는 Cisco Unified Communications Manager에서 폴백 명령이 실행되면 발생합니다.
  - 장애가 발생한 IM and Presence 서비스 노드가 정상 상태로 복구되고 모든 중요 서비스가 실행 중인 경우. 해당 그룹에서 장애 조치된 클라이언트는 복구된 노드(사용 가능하게 된 경우)에 다시 연결됩니다.
  - 백업이 활성화된 IM and Presence 서비스 노드가 중요 서비스 실패로 인해 장애가 발생하고 피어 노드가 [장애 조치됨] 상태에 있으며 자동 복구 폴백을 지원하는 경우

예를 들어, 프레즌스 이중화 그룹을 사용하는 경우 위치 IM and Presence 서비스 노드의 서비스 또는 하드웨어에 장애가 발생하면 Cisco 재버 클라이언트가 백업 IM and Presence 서비스 노드로 대체 작동됩니다. 장애가 발생한 노드가 다시 온라인으로 돌아오면 자동 폴백을 구성한 경우 클라이언트는 자동으로 로컬 IM and Presence 서비스 노드에 연결됩니다. 자동 폴백을 구성하지 않은 경우 장애가 발생한 노드가 온라인 상태가 되면 폴백을 수동으로 시작할 수 있습니다.

중복 및 복구 외에도 프레즌스 이중화 그룹을 사용하면 클러스터에 대해 고가용성을 구성할 수도 있습니다.

고가용성

IM and Presence 서비스는 다중 노드 구축을 위한 고가용성을 지원합니다.

프레즌스 이중화 그룹을 구성한 후에는 그룹에 대해 고가용성을 활성화할 수 있습니다. 고가용성에는 노드 쌍이 필요합니다. 각 노드에는 공통 사용자를 지원할 수 있는 공유 가용성 데이터베이스로 운영되는 독립된 데이터베이스 및 사용자 집합이 있습니다.

모든 IM and Presence 서비스 노드는 단일 IM and Presence 서비스 노드 또는 IM and Presence 서비스 노드 쌍으로 구성할 수 있는 프레즌스 이중화 그룹에 속해야 합니다.

두 가지 다른 모드를 사용하여 고가용성을 구성할 수 있습니다.

- 균형 모드: 이 모드는 구성 요소 장애 또는 정전으로 인해 노드 중 하나가 실패하는 경우 자동 사용자 로드 밸런싱 및 사용자 장애 조치를 통해 중복 고가용성을 제공합니다.
- Active/Standby 모드: Active 노드가 실패하면 Standby 노드는 자동으로 Active 노드를 인수합니다. 이 모드는 자동 로드 밸런싱을 제공하지 않습니다.

IM and Presence 서비스 구축을 고가용성 구축으로서 구성하는 것이 좋습니다. 단일 구축에서 고가용성 및 비 고가용성 프레즌스 이중화 그룹을 모두 구성할 수는 있지만 이 구성은 사용하지 않는 것이 좋습니다.

프레즌스 이중화 그룹 필수 조건

WAN을 통한 구축의 경우 각 IM and Presence 서비스 클러스터에 대해 초당 최소 10메가비트의 전용 대역폭이 필요하며 왕복 대기 시간이 80밀리초를 넘지 않습니다. 대역폭이 권장 대역폭보다 하나라도 작으면 성능에 좋지 않은 영향을 줄 수 있습니다.

프레즌스 이중화 그룹 작업 흐름

IM and Presence 서비스 노드는 프레즌스 이중화 그룹 한 개에만 할당할 수 있습니다. 고가용성을 위해 동일한 클러스터의 두 노드를 프레즌스 이중화 그룹에 할당하고 그룹에 대해 고가용성을 활성화해야 합니다.

프로시저

	명령 또는 동작	목적
단계 **1**	데이터베이스 복제 확인, 55 페이지	IM and Presence 서비스 클러스터에서 데이터베이스 복제가 설정되어 있는지 확인하십시오.

	명령 또는 동작	목적
단계 **2**	서비스 확인, 56 페이지	프레즌스 이중화 그룹에 추가하려는 노드에서 중요 서비스가 실행 중인지 확인합니다.
단계 **3**	프레즌스 이중화 그룹 구성, 57 페이지	IM and Presence 서비스 클라이언트 및 애플리케이션에 대한 중복 및 복구 기능을 제공합니다.
단계 **4**	장애 조치를 위한 하트비트 간격 구성, 57 페이지	(선택 사항) 프레즌스 이중화 그룹의 각 노드는 피어 노드의 상태 또는 하트비트를 모니터링합니다. 각 노드가 피어를 모니터링하는 간격을 구성할 수 있습니다.
단계 **5**	고가용성 활성화, 59 페이지	(선택 사항) 프레즌스 이중화 그룹을 구성할 때 고가용성을 활성화하지 못한 경우 이 절차를 따릅니다.
단계 **6**	사용자 할당 모드 구성, 59 페이지	동기화 에이전트가 IM and Presence 서비스 클러스터의 여러 노드에 사용자를 구축하는 방법을 구성합니다. 이 설정은 시스템이 장애 조치 및 로드 밸런싱을 처리하는 방법에 영향을 미칩니다.

데이터베이스 복제 확인

프레즌스 이중화 그룹에 대해 고가용성을 활성화하기 전에 데이터베이스 복제가 IM and Presence 서비스 클러스터에 설정되어 있는지 확인합니다.

프로시저

단계 **1** 다음 방법 중 하나를 사용하여 CLI 세션을 시작합니다.

- 원격 시스템에서 SSH를 사용하여 Cisco Unified 운영 체제에 안전하게 연결합니다. SSH 클라이언트에서 **ssh *adminname@hostname***을 입력하고 암호를 입력합니다.
- 직렬 포트에 대한 직접 연결에서 자동으로 표시되는 프롬프트에 자격 증명을 입력합니다.

단계 **2** **utils dbreplication status** 명령을 실행하여 데이터베이스 테이블의 오류 또는 불일치를 확인합니다.

단계 **3** **utils dbreplication runtimestate** 명령을 실행하여 노드에서 데이터베이스 복제가 활성 상태인지 확인합니다.

출력에는 모든 노드가 나열되고 데이터베이스 복제가 설정되고 상태가 양호한 경우 각 노드의 복제 설정 값은 **2**입니다.

2 이외의 값이 반환되는 경우 계속하기 전에 오류를 해결해야 합니다.

다음에 수행할 작업

서비스 확인, 56 페이지

서비스 확인

프레즌스 이중화 그룹에 추가하려는 노드에서 중요 서비스가 실행 중인지 확인합니다. 고가용성을 켜기 전에 중요 서비스가 실행 중이어야 합니다. 어느 노드에서도 중요 서비스가 실행 중이지 않은 경우에는 고가용성을 켜면 프레즌스 이중화 그룹이 [실패] 상태가 됩니다. 중요 서비스가 한 노드에서 실행되고 있지 않은 경우에는 고가용성을 켜면 해당 노드가 다른 노드로 장애 조치됩니다.

시작하기 전에

데이터베이스 복제 확인, 55 페이지

프로시저

단계 **1** Cisco Unified IM and Presence 서비스 가용성에서 도구 > 제어 센터 - 네트워크 서비스를 선택합니다.

단계 **2** 서버 목록에서 해당 노드를 선택하고 이동을 클릭합니다.

단계 **3** **IM and Presence** 서비스 영역에서 다음 서비스가 시작되었는지 확인합니다.

- **Cisco** 클라이언트 프로파일 에이전트
- **Cisco Sync Agent**
- **Cisco XCP** 라우터

단계 **4** 관련 링크 드롭다운 목록에서 제어 센터 - 네트워크 서비스를 선택하고 이동을 클릭합니다.

단계 **5** **IM and Presence** 서비스 영역에서 다음 서비스가 시작되었는지 확인합니다.

- **Cisco SIP Proxy**
- **Cisco Presence** 엔진

다음에 수행할 작업

프레즌스 이중화 그룹 구성, 57 페이지

프레즌스 이중화 그룹 구성

Cisco Unified Communications Manager를 사용하여 IM and Presence 서비스 노드에 대한 중복을 구성합니다.

각 프로즌스 이중화 그룹에는 두 개의 IM and Presence 서비스 노드가 포함될 수 있습니다. 각 노드는 하나의 프레즌스 이중화 그룹에만 할당될 수 있습니다. 프레즌스 이중화 그룹에서 노드 2개 모두는 동일한 클러스터에 있어야 하며 동일한 IM and Presence 서비스 데이터베이스 게시자 노드를 가지고 있어야 합니다.

시작하기 전에

- 서비스 확인, 56 페이지
- 프레즌스 이중화 그룹에 추가하려는 IM and Presence Service 서비스 노드가 동일한 소프트웨어 버전을 실행하는지 확인하십시오.

프로시저

단계 **1** **Cisco Unified CM** 관리에서 시스템 > 프레즌스 이중화 그룹을 선택합니다.

단계 **2** 새로 추가를 클릭합니다.

단계 **3** 프레즌스 이중화 그룹의 고유 이름을 입력합니다.

밑줄(_) 및 대시(-)를 포함하여 최대 128자의 영숫자를 입력할 수 있습니다.

단계 **4** 그룹에 대한 설명을 입력합니다.

기호를 비롯해 최대 128자의 영숫자를 입력할 수 있지만 큰따옴표("), 퍼센트 기호(%), 앰퍼샌드(&), 슬래시(\) 또는 꺾쇠 괄호(<>)는 사용할 수 없습니다.

단계 **5** 프레즌스 서버 필드에 다른 IM and Presence 서비스 노드 두 개를 선택하여 그룹에 할당합니다.

단계 **6** (선택 사항) 고가용성 활성화 확인란을 선택하여 프레즌스 이중화 그룹에 대해 고가용성을 활성화할 수 있습니다.

단계 **7** 저장을 클릭합니다.

다음에 수행할 작업

장애 조치를 위한 하트비트 간격 구성, 57 페이지

장애 조치를 위한 하트비트 간격 구성

프레즌스 이중화 그룹의 각 피어가 피어 노드의 하트비트(즉, 상태)를 모니터링하여 피어가 활성 상태인지 확인하기 위한 연결 유지 설정을 결정하는 선택적 서비스 파라미터를 구성합니다. 구성된 타이머가 만료된 후 피어 노드가 응답하지 않는 경우 장애 조치가 시작될 수 있습니다.

참고 이러한 두 파라미터에 대해 기본값을 사용하는 것이 좋습니다. 그러나, 필요에 따라 값을 재구성할 수도 있습니다.

프로시저

단계 **1** Cisco Unified CM IM and Presence 관리에서 시스템 > 서비스 파라미터를 선택합니다.

단계 **2** 서버 드롭다운 목록에서 IM and Presence 노드를 선택합니다.

단계 **3** 서비스 드롭다운 목록에서 **Cisco** 서버 복구 매니저**(**활성**)**를 선택합니다.

단계 **4** 일반 서버 복구 관리자 파라미터**(**클러스터 수준**)**에서 프레즌스 이중화 그룹의 각 노드가 피어 노드의 하트비트를 모니터링하는 데 사용하는 클러스터 수준 연결 유지 설정을 구성합니다. 피어 노드가 응답하지 않는 경우 장애 조치가 시작될 수 있습니다.

- 서비스 포트 - 이 파라미터는 Cisco 서버 복구 매니저가 피어와 통신하는 데 사용하는 포트를 지정합니다. 기본값은 22001입니다.
- 관리 **RPC** 포트 - 이 파라미터는 Cisco 서버 복구 매니저가 admin rpc 요청을 제공하는 데 사용하는 포트를 지정합니다. 기본값은 20075입니다.
- 중요 서비스 지연 - 이 파라미터는 장애 조치가 시작되기 전에 중요한 서비스가 중단될 수 있는 기간을 초 단위로 지정합니다. 기본값은 90입니다.
- 자동 폴백 활성화 - 이 파라미터는 자동 폴백을 수행할지 여부를 지정합니다. 장애 조치가 발생하면 IM and Presence 서비스는 기본 노드가 정상 상태로 돌아온 후 30분이 지나면 자동으로 백업 노드에서 기본 노드로 사용자를 이동시킵니다. 기본값은 false입니다.
- 초기화 연결 유지**(**하트비트**)** 시간 초과 - 이 파라미터는 장애 조치가 시작되기 전에 초기화 중에 피어와의 하트비트가 손실될 수 있는 기간을 초 단위로 지정합니다. 기본값은 120입니다.
- 연결 유지**(**하트비트**)** 시간 초과 - 이 파라미터는 장애 조치가 시작되기 전에 피어와의 하트비트가 손실될 수 있는 기간을 초 단위로 지정합니다. 기본값은 60입니다.
- 연결 유지**(**하트비트**)** 간격 - 이 파라미터는 연결 유지(하트비트) 메시지가 피어에 전송되는 간격을 초 단위로 지정합니다. 기본값은 15입니다.
- **XCP** 인증 서비스의 모니터링 활성화 - 이 파라미터를 사용하여 Cisco XCP 인증 서비스를 모니터링하고 노드에서 서비스 장애가 발생할 때 피어 노드로 자동 페일오버를 시작하도록 시스템을 구성합니다. **XCP** 인증 서비스의 모니터링 활성화 필드에서 서비스 파라미터 값을 참으로 설정합니다.

단계 **5** 다음 추가 파라미터를 구성하여 CUPC 8.5 이상의 클라이언트가 다시 로그인을 시도하기 전에 기다려야 하는 시간을 알려줍니다. 위의 파라미터와 달리 이러한 파라미터는 각 클러스터 노드마다 별도로 구성해야 합니다.

- 클라이언트 재로그인 하한 - 이 파라미터는 CUPC 8.5(이상)가 이 서버에 다시 로그인하기 전에 기다려야 하는 최소 시간(초)을 지정합니다. 기본값은 120입니다.
- 클라이언트 재로그인 상한 - 이 파라미터는 CUPC 8.5(이상)가 이 서버에 다시 로그인하기 전에 기다려야 하는 최대 시간(초)을 지정합니다. 기본값은 537입니다.

단계 **6** 저장을 클릭합니다.

다음에 수행할 작업

프레즌스 이중화 그룹을 구성할 때 고가용성을 활성화하지 못한 경우 이제 고가용성 활성화, 59 페이지.

고가용성 활성화

주의 IM and Presence 서비스 클러스터에서 복제를 설정하지 못하고 중요 서비스가 모두 실행 중인지 확인하지 못하는 경우 프레즌스 이중화 그룹에 대해 고가용성을 활성화하면 즉시 장애 조치될 수 있습니다.

시작하기 전에

- 프레즌스 이중화 그룹 구성, 57 페이지
- IM and Presence 서비스 클러스터에서 복제가 설정되어 있는지 확인하십시오.
- 모든 중요 서비스가 실행 중인지 확인합니다.

프로시저

단계 **1** **Cisco Unified CM** 관리에서 시스템 > 프레즌스 이중화 그룹을 선택합니다.
단계 **2** 검색 기준을 지정하고 찾기를 클릭합니다.
단계 **3** 구성한 프레즌스 이중화 그룹을 선택합니다.
단계 **4** 고가용성을 활성화하려면 고가용성 활성화 확인란을 선택합니다.
단계 **5** 저장을 클릭합니다.

사용자 할당 모드 구성

이 절차를 사용하여 동기화 에이전트가 사용자를 클러스터의 노드에 배포하는 방식을 구성합니다. 이 설정은 로드 밸런싱 및 장애 조치를 관리하는 데 도움이 됩니다.

프로시저

단계 **1** [Cisco Unified CM 관리]에서 시스템 > 엔터프라이즈 파라미터를 선택합니다.

단계 **2** 사용자 관리 파라미터 영역에서 **Presence** 서버에 대한 사용자 할당 모드 파라미터에 대해 다음 옵션 중 하나를 선택합니다.

- 균형 조정됨 - 이 모드는 각 하위 클러스터의 각 노드에 사용자를 균일하게 할당하고, 전체 사용자 수를 각 노드에서 균일하게 조정하려고 시도합니다. 이것이 기본 옵션입니다.
- **Active-Standby** - 이 모드는 모든 사용자를 하위 클러스터의 첫 번째 노드에 할당하고, 두 번째 서버는 백업으로 남겨둡니다.
- 없음 - 이 모드에서는 동기화 에이전트가 클러스터의 노드에 사용자를 할당하지 않습니다.

단계 **3** 저장을 클릭합니다.

수동 장애 조치, 폴백 및 복구 시작

이 절차를 사용하여 프레즌스 이중화 그룹 내에서 IM and Presence 서비스 노드의 수동 장애 조치, 폴백 또는 복구를 시작합니다.

- 수동 장애 조치 - 수동 장애 조치를 시작하면 **Cisco** 서버 복구 매니저는 실패한 노드에서 중요 서비스를 중지합니다. 실패한 노드의 모든 사용자는 연결이 끊어지며 백업 노드로 다시 로그인해야 합니다. 중요 서비스는 수동 폴백을 호출하지 않는 한 다시 시작되지 않습니다.
- 수동 폴백 - 수동 폴백을 시작하면 **Cisco** 서버 복구 매니저는 기본 노드에서 중요 서비스를 다시 시작하고 장애 조치된 모든 사용자의 연결을 끊습니다. 그런 다음 이러한 사용자는 할당된 노드에 다시 로그인해야 합니다.
- 수동 복구 - 프레즌스 이중화 그룹의 두 노드 모두 실패 상태인 경우 수동 복구가 필요합니다. 이 경우 IM and Presence 서비스는 프레즌스 이중화 그룹의 양쪽 노드에서 **Cisco** 서버 복구 매니저 서비스를 다시 시작합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 시스템 > 프레즌스 이중화 그룹을 선택합니다.

단계 **2** 찾기를 클릭하고 해당 노드가 있는 프레즌스 이중화 그룹을 선택합니다.

단계 **3** 다음 중 하나를 수행합니다. 사용 가능한 버튼은 노드의 현재 상태에 따라 달라집니다.

- 활성 노드의 장애 조치를 시작하려면 장애 조치를 클릭합니다.
- 장애 조치된 노드의 폴백을 시작하려면 폴백을 클릭합니다.
- 두 노드가 페일 오버되고 복구하려는 경우 복구를 클릭합니다.

참고 또한 CLI를 사용하여 Cisco Unified Communications Manager 또는 IM and Presence 서비스에서 이러한 작업을 시작할 수도 있습니다. 자세한 내용은 *Command Line Interface Guide for Cisco Unified Communications Solutions*를 참조하십시오.

참고 노드 중 하나가 장애 조치 상태에 있는 동안 최종 사용자를 IM and Presence 서비스 클러스터에 추가할 수 없습니다.

노드 상태 정의

표 *4:* 프레즌스 이중화 그룹 노드 상태 정의

상태	설명
초기화 중	Cisco Server Recovery Manager 서비스가 시작될 때 초기(전환) 상태이며, 임시 상태입니다.
유휴	IM and Presence 서비스가 장애 조치가 발생하고 서비스가 중지되는 유휴 상태에 있습니다. 유휴 상태에서 IM and Presence 서비스 노드는 가용성 또는 인스턴트 메시징 서비스를 제공하지 않습니다. 유휴 상태에서 **Cisco Unified CM** 관리를 사용하여 이 노드에 대한 폴백을 수동으로 시작할 수 있습니다.
정상	안정적인 상태입니다. IM and Presence 서비스 노드가 정상적으로 작동 중입니다. 이 상태에서 **Cisco Unified CM** 관리 사용자 인터페이스를 사용하여 이 노드에 대한 장애 조치를 수동으로 시작할 수 있습니다.
백업 모드에서 실행 중	안정적인 상태입니다. IM and Presence 서비스 노드가 피어 노드에 대한 백업으로 동작하고 있습니다. 사용자가 이(백업) 노드로 이동되었습니다.
인수 중	전환 상태입니다. IM and Presence 서비스 노드가 피어 노드에 대해 인수 중입니다.
장애 조치 중	전환 상태입니다. IM and Presence 서비스 노드가 피어 노드에 의해 인수 중입니다.
장애 조치됨	지속적인 상태입니다. IM and Presence 서비스 노드가 장애 조치되었지만 중요 서비스가 중단되었습니다. 이 상태에서 **Cisco Unified CM** 관리 사용자 인터페이스를 사용하여 이 노드에 대한 폴백을 수동으로 시작할 수 있습니다.
실행 중이 아닌 중요 서비스 장애 조치됨	지속적인 상태입니다. IM and Presence 서비스 노드의 일부 중요 서비스가 중지되거나 실패했습니다.

상태	설명
폴백 중	전환 상태입니다. 백업 모드에서 실행 중인 노드에서 이 IM and Presence 서비스 노드로 폴백하는 중입니다.
회수 중	전환 상태입니다. 실패한 IM and Presence 서비스 노드가 피어에서 회수 중입니다.
실패 모드에서 실행 중	전환 상태 중에 또는 백업 모드에서 실행 중 상태에서 오류가 발생합니다.
알 수 없음	노드 상태를 알 수 없습니다. 가능한 원인은 IM and Presence 서비스 노드에서 고가용성이 활성화되지 않았기 때문입니다. 프레즌스 이중화 그룹의 양쪽 노드에서 서버 복구 관리자 서비스를 다시 시작합니다.

노드 상태, 원인 및 권장 작업

Cisco Unified CM 관리 사용자 인터페이스를 사용하여 그룹을 선택할 때 프레즌스 이중화 그룹 설정 창에서 프레즌스 이중화 그룹에 있는 노드의 상태를 확인할 수 있습니다.

표 *5:* 프레즌스 이중화 그룹 노드 고가용성 상태, 원인 및 권장 작업

노드 **1**		노드 **2**		
상태	이유	상태	이유	원인/권장 작업
정상	정상	정상	정상	정상
장애 조치 중	관리 요청 시	인수 중	관리 요청 시	관리자가 노드 1에서 노드 2로의 수동 대체 작동을 시작했습니다. 수동 대체 작동이 진행 중입니다.
유휴	관리 요청 시	백업 모드에서 실행 중	관리 요청 시	관리자가 시작한 노드 1에서 노드 2로의 수동 장애 조치가 완료되었습니다.
회수 중	관리 요청 시	폴백 중	관리 요청 시	관리자가 노드 2에서 노드 1로의 수동 대체를 시작했습니다. 수동 대체가 진행 중입니다.
유휴	초기화	백업 모드에서 실행 중	관리 요청 시	노드 1이 "유휴" 상태일 때 관리자가 노드 1에서 SRM 서비스를 다시 시작합니다.
유휴	초기화	백업 모드에서 실행 중	초기화	관리자가 프레즌스 이중화 그룹에서 두 노드를 다시 시작하거나 프레즌스 이중화 그룹이 수동 장애 조치 모드에 있을 때 두 노드에서 SRM 서비스를 다시 시작합니다.

노드 **1**		노드 **2**		
상태	이유	상태	이유	원인/권장 작업
유휴	관리 요청 시	백업 모드에서 실행 중	초기화	노드 2가 백업 모드에서 실행 중이지만 노드 1의 하트비트 시간이 초과되기 전에 관리자가 노드 2에서 SRM 서비스를 다시 시작합니다.
장애 조치 중	관리 요청 시	인수 중	초기화	노드 2가 인수 중이지만 노드 1의 하트비트 시간이 초과되기 전에 관리자가 노드 2에서 SRM 서비스를 다시 시작합니다.
회수 중	초기화	폴백 중	관리 요청 시	노드 2의 하트비트 시간이 초과되기 전에 관리자가 회수 중인 노드 1에서 SRM 서비스를 다시 시작합니다. 회수 프로세스가 완료되면 두 노드는 정상 상태로 돌아갑니다.
회수 중	자동 폴백	폴백 중	자동 폴백	노드 2에서 노드 1로의 자동 폴백이 시작되었고 현재 진행 중입니다.
장애 조치됨	초기화 또는 중요 서비스 중지됨	백업 모드에서 실행 중	중요 서비스 중지됨	다음 경우의 하나가 발생하면 노드 1이 장애 조치됨 상태로 전환됩니다. • 노드 1이 재부팅되어 중요 서비스가 백업되는 경우 • 노드 1이 실행 중이 아닌 중요 서비스 장애 조치됨 상태일 때 관리자가 노드 1에서 중요 서비스를 시작하는 경우 노드 1이 장애 조치됨 상태로 전환되면 노드는 관리자가 수동 폴백을 수행하여 프레즌스 이중화 그룹의 노드를 정상 상태로 복원할 준비가 됩니다.
실행 중이 아닌 중요 서비스 장애 조치됨	중요 서비스 중지됨	백업 모드에서 실행 중	중요 서비스 중지됨	노드 1에서 중요 서비스가 중지되었습니다. IM and Presence 서비스가 노드 2로의 자동 대체 작동을 수행합니다. 권장 작업**:** **1.** 중지된 중요 서비스가 있는지 노드 1을 확인하고 해당 서비스를 수동으로 시작해 봅니다. **2.** 노드 1의 중요 서비스가 시작되지 않으면 노드 1을 재부팅합니다. **3.** 재부팅 후에 모든 중요 서비스가 시작되어 실행 중이면 수동 폴백을 수행하여 프레즌스 이중화 그룹의 노드를 정상 상태로 복원합니다.

노드 **1**		노드 **2**		
상태	이유	상태	이유	원인/권장 작업
실행 중이 아닌 중요 서비스 장애 조치됨	데이터베이스 실패	백업 모드에서 실행 중	데이터베이스 실패	노드 1에서 데이터베이스 서비스가 중지되었습니다. IM and Presence 서비스가 노드 2로의 자동 대체 작동을 수행합니다. 권장 작업**:** **1.** 노드 1을 재부팅합니다. **2.** 재부팅 후에 모든 중요 서비스가 시작되어 실행 중이면 수동 폴백을 수행하여 프레즌스 이중화 그룹의 노드를 정상 상태로 복원합니다.
실패 모드에서 실행 중	중요 서비스 시작 실패	실패 모드에서 실행 중	중요 서비스 시작 실패	프레즌스 이중화 그룹의 노드가 다른 노드에서 회수 중일 때 중요 서비스가 시작되지 않습니다. 권장 작업**.** 회수 중인 노드에서 다음 작업을 수행합니다. **1.** 노드에 중지된 중요 서비스가 있는지 확인합니다. 이러한 서비스를 수동으로 시작하려면 프레즌스 이중화 그룹 설정 창에서 복구를 클릭합니다. **2.** 중요 서비스가 시작되지 않으면 노드를 재부팅합니다. **3.** 재부팅 후에 모든 중요 서비스가 시작되어 실행 중이면 수동 폴백을 수행하여 프레즌스 이중화 그룹의 노드를 정상 상태로 복원합니다.
실패 모드에서 실행 중	중요 서비스 중지됨	실패 모드에서 실행 중	중요 서비스 중지됨	백업 노드에서 중요 서비스가 중지됩니다. 두 노드가 모두 실패 상태로 전환됩니다. 권장 작업**:** **1.** 백업 노드에 중지된 중요 서비스가 있는지 확인합니다. 이러한 서비스를 수동으로 시작하려면 프레즌스 이중화 그룹 설정 창에서 복구를 클릭합니다. **2.** 중요 서비스가 시작되지 않으면 노드를 재부팅합니다.

노드 **1**		노드 **2**		
상태	이유	상태	이유	원인/권장 작업
네트워크 연결이 끊어져서 노드 1이 중지되었거나 SRM 서비스가 실행 중이 아닙니다.		백업 모드에서 실행 중	피어 중지됨	노드 2가 노드 1에서 하트 비트를 손실했습니다. IM and Presence 서비스가 노드 2로의 자동 대체 작동을 수행합니다. 권장 작업**.** 노드 1이 시작되면 다음 작업을 수행합니다. **1.** 프레즌스 이중화 그룹의 노드 간 네트워크 연결을 확인하고 복구합니다. 노드 간에 네트워크 연결을 재설정하면 노드가 실패 상태로 전환될 수 있습니다. 프레즌스 이중화 그룹 설정 창에서 복구를 선택하여 노드를 정상 상태로 복원합니다. **2.** SRM 서비스를 시작하고 수동 폴백을 수행하여 프레즌스 이중화 그룹의 노드를 정상 상태로 복원합니다. **3.** (노드가 중지된 경우) 노드 1을 복구하고 시작합니다. **4.** 노드가 시작되고 모든 중요 서비스가 실행 중이면 수동 폴백을 수행하여 프레즌스 이중화 그룹의 노드를 정상 상태로 복원합니다.
노드 1이 중지됩니다(전원 차단, 하드웨어 실패, 종료, 재부팅 때문일 수 있음).		백업 모드에서 실행 중	피어 재부팅	노드 1에서 다음 경우가 발생해서 IM and Presence 서비스가 노드 2로의 자동 장애 조치를 수행합니다. • 하드웨어 실패 • 전원 차단 • 재시작 • 종료 권장 작업**:** **1.** 노드 1을 복구하고 시작합니다. **2.** 노드가 시작되고 모든 중요 서비스가 실행 중이면 수동 폴백을 수행하여 프레즌스 이중화 그룹의 노드를 정상 상태로 복원합니다.

노드 **1**		노드 **2**		
상태	이유	상태	이유	원인/권장 작업
실행 중이 아닌 중요 서비스 장애 조치됨 또는 장애 조치됨	초기화	백업 모드	초기화 중에 피어 중지됨	시작 중에 노드 2가 노드 1을 인식하지 못합니다. 권장 작업: 노드 1이 시작되고 모든 중요 서비스가 실행 중이면 수동 폴백을 수행하여 프레즌스 이중화 그룹의 노드를 정상 상태로 복원합니다.
실패 모드에서 실행 중	Cisco 서버 복구 관리자 사용자 인수 실패	실패 모드에서 실행 중	Cisco 서버 복구 관리자 사용자 인수 실패	인계 프로세스 중에 사용자 이동에 실패합니다. 권장 작업: 데이터베이스 오류일 수 있습니다. 프레즌스 이중화 그룹 설정 창에서 복구를 클릭합니다. 문제가 지속되면 노드를 재부팅합니다.
실패 모드에서 실행 중	Cisco 서버 복구 관리자 사용자 회수 실패	실패 모드에서 실행 중	Cisco 서버 복구 관리자 사용자 회수 실패	폴백 프로세스 중에 사용자 이동에 실패합니다. 권장 작업: 데이터베이스 오류일 수 있습니다. 프레즌스 이중화 그룹 설정 창에서 복구를 클릭합니다. 문제가 지속되면 노드를 재부팅합니다.
실패 모드에서 실행 중	알 수 없음	실패 모드에서 실행 중	알 수 없음	다른 노드의 SRM이 실패 상태이거나 내부 시스템 오류가 발생할 때 노드에서 SRM을 다시 시작합니다. 권장 작업: 프레즌스 이중화 그룹 설정 창에서 복구를 클릭합니다. 문제가 지속되면 노드를 재부팅합니다.
백업 활성화됨	데이터베이스 실패 자동 복구	영향받는 서비스 장애 조치	데이터베이스 실패 자동 복구.	백업 노드에서 데이터베이스가 중지됩니다. 피어 노드가 장애 조치 모드에 있고 프레즌스 이중화 그룹의 모든 사용자에 대해 인계될 수 있습니다. 자동 복구 작업은 자동으로 수행되고 모든 사용자가 기본 노드로 이동됩니다.
백업 활성화됨	데이터베이스 실패 자동 복구	영향받는 서비스 장애 조치	중요 서비스 중지 자동 복구	백업 노드에서 중요 서비스가 중지됩니다. 피어 노드가 장애 조치 모드에 있고 프레즌스 이중화 그룹의 모든 사용자에 대해 인계될 수 있습니다. 자동 복구 작업은 자동으로 수행되고 모든 사용자가 피어 노드로 이동됩니다.

노드 1		노드 2		
상태	이유	상태	이유	원인/권장 작업
알 수 없음		알 수 없음		노드 상태를 알 수 없습니다. 가능한 원인은 IM and Presence 서비스 노드에서 고가용성이 활성화되지 않았기 때문입니다. 권장 작업: 프레즌스 이중화 그룹의 양쪽 노드에서 서버 복구 관리자 서비스를 다시 시작합니다.

거의 제로 다운타임으로 IM and Presence 페일오버 향상

노드와 클러스터의 업그레이드 및 페일오버 중에 미치는 영향을 줄여 Jabber 서비스 중단을 최소화하도록 IM and Presence 서비스가 향상되었습니다.

릴리스 14에서 IM and Presence 서비스는 Jabber 클라이언트와의 이중 연결을 지원합니다. 클라이언트쪽에서 활성화된 경우, 이 유형의 연결은 고가용성 페일오버 이벤트 중에 훨씬 짧은 서비스 중단(거의 0)을 보장합니다.

이는 다음을 수행하는 데 도움이 됩니다.

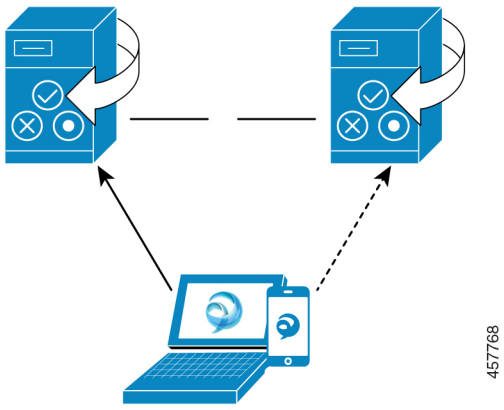
- IM and Presence 서비스의 직접 표준 업그레이드 중에 Jabber 클라이언트에 대한 서비스 중단 최소화
- 기본 및 보조 노드 간 사용자 세션의 원활한 전환 제공

Jabber 클라이언트에서 일부 추가 구성을 사용하여 이 기능을 활성화할 수 있습니다. Jabber에서 이중 연결을 활성화하는 방법에 대한 자세한 내용은 Cisco Jabber 14용 매개 변수 참조 설명서의 *EnableDualConnections* 및 *Inactive_Connection_Activation_Timer* 매개 변수를 참조하십시오.

가능한 가장 짧은 다운타임을 유지하려면 이 향상을 활성화하기 위해 다음 사전 요건을 충족하는지 확인하십시오.

- 업그레이드 중에 HA(고가용성)를 활성화합니다.
- 릴리스 호환성: 모바일 및 원격 액세스 사용자의 경우 Cisco Unified CM 및 IM and Presence 릴리스 14, Jabber 릴리스 14 및 Expressway 14.

그림 ***2: IM Presence*** 페일오버 향상



페일오버의 경우 이 향상으로 인해 다운타임이 거의 0이 됩니다. 이는 Cisco Jabber 클라이언트에서 IM and Presence 노드와 이중 연결을 유지하도록 하여 수행됩니다. 활성 연결은 클라이언트 로그인 프로세스 중에 생성되는 기본 노드와 함께 유지됩니다. 클라이언트 재로그인 하한값 및 클라이언트 재로그인 상한값의 값 사이에 임의 초 수가 경과하면 백업 노드와 비활성 연결이 생성됩니다. 이러한 제한은 Cisco 서버 복구 매니저 서비스에 대한 서비스 매개 변수로 구성됩니다.

페일오버가 발생 하면 Jabber 클라이언트가 '비활성' 연결을 활성화하여 서버와 통신합니다. 비활성 연결이 이미 백업 노드에 생성되었으므로 Jabber 다운타임을 최소화합니다.

참고 Cisco Jabber 클라이언트 제한으로 인해 Jabber에 대한 이 페일오버 향상은 IM and Presence 서비스의 무제한(XU) 버전에서는 작동하지 않습니다. 이는 Jabber 및 IM and Presence 서비스와 같은 XMPP 클라이언트 간의 보안 TLS 연결이 무제한 버전에서 비활성화되어 있기 때문입니다.

제한된 버전에서는 보안 설정 페이지(시스템 > 보안 > 설정)에서 **IM/P** 서비스 보안 모드에 대해 **XMPP** 클라이언트 활성화 옵션이 기본적으로 활성화되어 Jabber에서 작동하도록 페일오버 향상을 활성화합니다. 페일오버 향상을 사용하려는 경우에는 이 모드를 해제하지 않는 것이 좋습니다. 이 제한에 대한 자세한 내용은 CSCvx94284를 참조하십시오.

이중 등록이 설정되었는지 확인하는 방법

이중 등록을 설정하려면 기본 노드의 X 사용자와 보조 노드의 Y 사용자를 할당한 시나리오를 고려하십시오. 기본 노드에서 *JsmSessionsClient* 및 *JsmSessionsClientInactive* 카운터를 선택하면 *JsmSessionsClient*에 연결된 총 사용자 수는 X이고 *JsmSessionsClientInactive*는 Y인 것을 알 수 있습니다. 동시에 보조 노드에서 *JsmSessionsClient*에 연결된 총 사용자 수는 Y이고 *JsmSessionsClientInactive*는 X입니다.

이중 등록을 비활성화하는 방법

서버에서 HA를 비활성화하지 않고 클라이언트 측에서 HA를 비활성화하여 이중 등록을 비활성화할 수 있습니다. 또한 HA를 비활성화하면 서버에서 클라이언트로 이중 등록이 제공되지 않으며 클라이언트가 비활성 연결 설정을 시도할 수 없습니다. Jabber에서 이중 연결을 활성화하는 방법에 대한 자

세한 내용은 Cisco Jabber 14용 매개 변수 참조 설명서의 *EnableDualConnections* 및 *Inactive_Connection_Activation_Timer* 매개 변수를 참조하십시오.

업그레이드 중 제로 다운타임을 모니터링하는 카운터

업그레이드 프로세스를 추적하여 다운타임이 0이 되도록 하려면 실시간 모니터링 도구를 통해 다음 카운터를 모니터링하면 됩니다.

표 *6:* 업그레이드 중 제로 다운타임을 모니터링하는 카운터

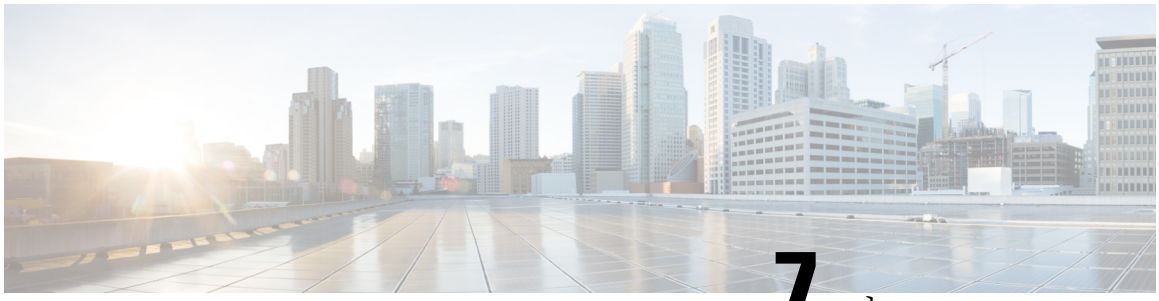
카운터	설명
ActiveJsmSessions	이 카운터는 퍼블리셔 노드에 할당된 활성 사용자 수를 제공합니다. 페일오버 중에 기본(업그레이드됨) 노드의 경우 0이 표시되고 기본 노드에서 백업 노드에 활성 사용자가 추가됩니다.
InactiveJsmSessions	이 카운터는 가입자 노드에 할당된 활성 사용자 수를 제공합니다.
JsmSessionsComposed	이 카운터는 JSM에 대해 활성화된 구성된 세션 수를 나타냅니다.
JsmSessionsClientInactive	이 카운터는 JSM에 대해 비활성 상태인 클라이언트 세션 수를 나타냅니다.
JsmSessionsClient	이 카운터는 JSM에 대해 활성 상태인 클라이언트 세션 수를 나타냅니다.
JsmSessionsClientInactive	이 카운터는 JSM에 대해 비활성 상태인 클라이언트 세션 수를 나타냅니다.

중복 상호 작용 및 제한 사항

기능	상호 작용
사용자 추가	클러스터 노드 중 하나가 장애 조치 상태에 있는 동안 새 사용자를 IM and Presence 서비스 클러스터에 추가할 수 없습니다.
다중 디바이스 메시징	다중 디바이스 메시징 기능은 장애 조치가 발생할 경우 IM and Presence 서비스에서 서버 복구를 지연시킵니다. 다중 디바이스 메시징이 구성된 시스템에서 서버 장애 조치가 발생하면 일반적으로 장애 조치 시간은 **Cisco** 서버 복구 매니저 서비스 파라미터로 지정된 시간의 두 배가 됩니다.

기능	상호 작용
푸시 알림 고가용성	11.5(1)SU3을 기준으로 푸시 알림 구축 시 고가용성이 지원됩니다. 푸시 알림을 활성화하고 노드가 장애 조치되는 경우 iPhone 및 iPad 클라이언트의 Cisco Jabber에서 다음과 같은 문제가 발생합니다. • 포그라운드 모드에 있는 Cisco Jabber 클라이언트의 경우, Jabber 클라이언트는 백업 노드에 자동으로 로그인하고, 기본 노드가 복구될 때까지 이 노드를 인계합니다. 백업 노드가 인계받거나 기본 노드가 복구될 때 서비스 중단이 발생하지 않습니다. • 백그라운드 모드에 있는 Cisco Jabber 클라이언트의 경우 백업 노드가 인계받지만 푸시 알림을 보내기 전에 지연이 있습니다. Jabber 클라이언트는 백그라운드 모드에 있기 때문에 네트워크에 대한 활성 연결이 없으므로 백업 노드에 자동으로 로그인하지 않습니다. 백업 노드는 푸시 알림을 보내기 전에 백그라운드 모드에 있었던 모든 장애 조치된 사용자에 대해 JSM 세션을 다시 만들어야 합니다. 지연의 길이는 시스템 부하에 따라 다릅니다. 테스트 결과 사용자가 HA 페어에 고르게 분산된 15,000명의 사용자 OVA의 경우 장애 조치 후 푸시 알림을 보내려면 10 ~ 20분이 소요됩니다. 이 지연은 백업 노드가 인계될 때 및 기본 노드가 복구된 후에 다시 관찰됩니다. 참고 노드 장애 또는 예기치 않은 Cisco XCP 라우터의 충돌 시 IM 내역을 포함한 사용자의 IM 세션은 사용자 조치 없이 유지됩니다. 그러나 iPhone 또는 iPad 클라이언트의 Cisco Jabber가 일시 중단 모드에 있는 경우 서버에 충돌이 발생했을 때 서버에 대기중인 읽지 않은 메시지를 검색 할 수 없습니다.

기능	상호 작용
사용자의 임시 프레즌스 상태	사용자의 임시 프레즌스 상태는 페일오버, 대체 및 사용자 이동 후의 부실한 프레즌스 상태를 표시합니다. 이는 임시 프레즌스에 대한 구독이 삭제되고 사용자가 임시 프레즌스를 다시 구독하여 사용자의 유효한 임시 프레즌스 상태를 확인해야 하기 때문입니다. 예를 들어 사용자 A가 사용자 B의 임시 프레즌스를 구독하고 사용자 B가 할당된 IM and Presence 노드에서 페일오버가 발생하면 사용자 B가 백업 노드에 다시 로그인한 후에도 사용자 B가 사용자 A에게 오프라인으로 표시됩니다. 이는 사용자 B의 임시 프레즌스에 대한 구독이 삭제되고 사용자 A가 삭제를 인식하지 못하기 때문입니다. 사용자 A는 사용자 B의 임시 프레즌스를 다시 구독해야 합니다. 사용자 A가 Jabber 클라이언트에서 사용자 B의 검색을 삭제 하면 사용자 A가 임시 사용자 B의 검색을 시도 하기 전에 30 초 이상 기다려야 합니다. 그렇지 않은 경우 사용자 A가 사용자 B의 오래 된 것을 볼 수 있습니다. Jabber 클라이언트는 동일한 사용자가 두 검색 간격 동안 30 초 이상 기다려야 유효한 임시 현재 상태를 얻습니다.
IM and Presence 상태	사용자가 한 프레즌스 중복 그룹에서 다른 프레즌스 중복 그룹으로 이동되면 사용자가 이동한 현재 프레즌스 중복 그룹에 IM and Presence 상태가 표시되도록 하려면 사용자가 Jabber 세션에서 로그아웃해야 합니다.



7 장

사용자 설정 구성

최종 사용자 설정 개요

서비스 프로파일 및 기능 그룹 템플릿과 같은 사용자 설정을 사용하여 LDAP 디렉터리 동기화를 통해 일반 설정을 최종 사용자에게 적용할 수 있습니다. LDAP 디렉터리 동기화가 발생하면 구성된 설정이 모든 동기화된 사용자에게 적용됩니다.

참고 이 장에서는 특히 IM and Presence 서비스에 적용되는 사용자 설정에 대해 설명합니다. 음성 메일 및 전화회의와 같은 UC 서비스를 포함한 일반적인 UC 사용자 구성의 경우 *Cisco Unified Communications Manager* 시스템 구성 설명서의 "최종 사용자 구성" 섹션을 참조하십시오. 이러한 구성은 LDAP 동기화의 일환으로 적용할 수 있습니다.

서비스 프로파일

서비스 프로파일에는 일반적인 UC(Unified Communications) 서비스 설정이 포함되어 있습니다. 다른 사용자 그룹에 대해 다른 서비스 프로파일을 구성하여 각 사용자 그룹이 해당 작업에 대해 구성된 적절한 서비스를 갖도록 할 수 있습니다. 최종 사용자가 IM and Presence 서비스에 액세스할 수 있도록 하려면 IM and Presence 서비스가 포함되도록 서비스 프로파일을 구성합니다.

다음 방법을 사용하여 최종 사용자에게 서비스 프로파일을 적용할 수 있습니다.

- LDAP 동기화 사용자의 경우 - LDAP 디렉터리에서 최종 사용자를 가져온 경우 서비스 프로파일을 기능 그룹 템플릿에 할당한 다음 해당 기능 그룹 템플릿을 최종 사용자에게 적용할 수 있습니다. 템플릿의 설정은 모든 동기화된 사용자에게 적용됩니다.
- 활성 사용자(즉, 비 LDAP 사용자)의 경우 - 한 번에 많은 사용자에게 설정을 적용하려면 벌크 관리 도구를 사용하여 csv 파일이나 스프레드시트를 통해 서비스 프로파일 설정을 적용합니다. 벌크 관리 도구를 사용하는 방법에 대한 자세한 내용은 http://www.cisco.com/c/en/us/support/

unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html의 내용을 참조하십시오.

그렇지 않으면 사용자별로 수동으로 사용자 설정을 구성할 수 있습니다.

기능 그룹 템플릿 개요

기능 그룹 템플릿을 사용하면 LDAP 디렉터리 동기화를 통해 일반 설정을 최종 사용자 그룹에 신속하게 적용할 수 있습니다. 예를 들어, 기능 그룹 템플릿을 사용하여 일반 사용자를 위해 IM and Presence 서비스를 사용할 수 있습니다. 이 작업은 IM and Presence 서비스 프로파일을 템플릿에 적용하여 수행할 수 있습니다. 기능 그룹 템플릿을 LDAP 디렉터리 동기화에 적용하면 동기화가 발생하는 경우 구성된 서비스 프로파일 및 사용자 프로파일 설정을 포함한 템플릿의 설정이 모든 동기화된 사용자에게 적용됩니다.

기능 그룹 템플릿 구성에는 기능 그룹 템플릿에 할당할 수 있는 다음 프로파일이 포함됩니다.

- 사용자 프로파일 - 일반 전화기와 전화 회선 설정 집합을 포함합니다. 공통 전화 회선 설정을 할당하는 범용 회선 템플릿과 공통 전화 설정을 할당하는 범용 디바이스 템플릿으로 사용자 프로파일을 구성해야 합니다. 이러한 템플릿은 자체 프로비저닝을 위해 설정된 사용자가 자신의 전화기를 구성할 수 있도록 지원합니다.
- 서비스 프로필 - IM and Presence 서비스, 디렉터리 또는 음성 메일과 같은 일반 UC 서비스 그룹을 포함합니다.

사용자 설정 필수 조건

사용자를 IM and Presence 서비스 클러스터 간에 이동하려면 최종 사용자를 구성하기 전에 사용자를 이동해야 합니다. Cisco Unified CM IM and Presence 관리를 사용하여 사용자를 마이그레이션하고 연락처 목록을 가져오는 방법에 대한 자세한 내용은 .

참고 클러스터간에 사용자를 마이그레이션하면 파티션된 도메인간 페더레이션에 사용되는 사용자 마이그레이션 도구와 혼동해서는 안 됩니다.

참고 VPN을 통해 Cisco Jabber가 연결된 경우 IM and Presence 서비스와 Cisco Jabber 클라이언트 간의 TLS 핸드셰이크 중에 IM and Presence 서버가 클라이언트의 IP 서브넷에 대한 역방향 조회를 수행합니다. 역방향 조회가 실패하면 TLS 핸드셰이크는 클라이언트 시스템에서 시간 초과됩니다.

사용자 설정 작업 흐름 구성

이러한 작업을 수행하여 일반 서비스 및 기능 설정(예: IM and Presence 서비스에 대한 최종 사용자 활성화)으로 사용자 템플릿을 구성합니다. LDAP 동기화를 완료하면 템플릿 설정이 최종 사용자에게 적용됩니다.

참고 이 장에서는 특히 IM and Presence 서비스에 적용되는 작업 흐름 사용자 설정에 대해 설명합니다. 음성 메일 및 전화회의와 같은 UC 서비스를 포함한 일반적인 UC 사용자 구성의 경우 *Cisco Unified Communications Manager* 시스템 구성 설명서의 "최종 사용자 구성" 섹션을 참조하십시오. 이러한 구성은 LDAP 동기화의 일환으로 적용할 수 있습니다.

프로시저

	명령 또는 동작	목적
단계 **1**	사용자 할당 모드 구성, 75 페이지	사용자 지정 모드를 균형 조정, 활성/대기 또는 없음으로 설정합니다.
단계 **2**	IM and Presence UC 서비스 추가, 76 페이지	Cisco Unified Communications Manager에서 IM and Presence UC 서비스를 설정합니다.
단계 **3**	서비스 프로파일 구성, 76 페이지	추가한 IM and Presence UC 서비스가 포함된 서비스 프로파일을 구성합니다.
단계 **4**	기능 그룹 템플릿 구성, 77 페이지	다른 일반적인 기능 설정 이외에 설정한 서비스 프로파일이 포함된 기능 그룹 템플릿을 구성합니다.

다음에 수행할 작업

LDAP 동기화를 완료하여 LDAP 동기화 사용자에게 설정을 적용합니다.

사용자 할당 모드 구성

이 절차를 사용하여 동기화 에이전트가 사용자를 클러스터의 노드에 배포하는 방식을 구성합니다.

프로시저

단계 **1** [Cisco Unified CM 관리]에서 시스템 > 엔터프라이즈 파라미터를 선택합니다.

단계 **2** 사용자 관리 파라미터 영역에서 **Presence** 서버에 대한 사용자 할당 모드 파라미터에 대해 다음 옵션 중 하나를 선택합니다.

- 균형 조정됨 - 이 모드는 각 하위 클러스터의 각 노드에 사용자를 균일하게 할당하고, 전체 사용자 수를 각 노드에서 균일하게 조정하려고 시도합니다. 이것이 기본 옵션입니다.
- **Active-Standby** - 이 모드는 모든 사용자를 하위 클러스터의 첫 번째 노드에 할당하고, 두 번째 서버는 백업으로 남겨둡니다.
- 없음 - 이 모드에서는 동기화 에이전트가 클러스터의 노드에 사용자를 할당하지 않습니다.

단계 **3** 저장을 클릭합니다.

다음에 수행할 작업

IM and Presence UC 서비스 추가, 76 페이지

IM and Presence UC 서비스 추가

Cisco Unified Communications Manager에서 이 절차를 사용하여 IM and Presence 서비스에 대한 UC 서비스를 추가합니다.

프로시저

단계 **1** [Cisco Unified CM 관리]에서 사용자 관리 > 사용자 설정 > **UC** 서비스를 선택합니다.

단계 **2** 새로 추가를 클릭합니다.

단계 **3** **UC** 서비스 유형 드롭다운 목록 상자에서 **IM and Presence**를 선택합니다.

단계 **4** 제품 유형 드롭다운 목록 상자에서 **Unified CM(IMand Presence)**을 선택합니다.

단계 **5** IM and Presence 서비스의 이름 및 설명을 입력합니다.

단계 **6** 호스트 이름/**IP** 주소 필드에 IM and Presence 서비스를 호스팅하는 서버에 대한 호스트 이름, IP 주소 또는 DNS SRV를 입력합니다.

단계 **7** 저장을 클릭합니다.

다음에 수행할 작업

IM and Presence 서비스에 대해 사용자를 활성화하려면 서비스 프로파일에 UC 서비스를 할당하고 해당 프로파일을 사용자에게 할당합니다.

서비스 프로파일 구성, 76 페이지.

서비스 프로파일 구성

이 절차를 사용하여 IM and Presence 서비스를 포함하는 서비스 프로파일을 구성합니다.

시작하기 전에

IM and Presence UC 서비스 추가, 76 페이지

프로시저

단계 **1** [Cisco Unified CM 관리]에서 사용자 관리 > 사용자 설정 > 서비스 프로파일을 선택합니다.

단계 **2** 다음 중 하나를 수행합니다

- 찾기를 클릭하고 기존 프로파일을 선택합니다.
- 새로 추가를 클릭하여 새 프로파일을 만듭니다.

단계 **3** **IM and Presence** 프로파일 섹션에서 기본 IM and Presence 서버를 선택합니다.

단계 **4** 서비스 프로파일 구성 창에서 나머지 필드를 완료합니다. 필드 및 해당 설정에 대한 도움이 필요한 경우 온라인 도움말을 참조하십시오.

단계 **5** 저장을 클릭합니다.

다음에 수행할 작업

기능 그룹 템플릿 구성, 77 페이지

기능 그룹 템플릿 구성

설정한 IM and Presence 지원 서비스 프로파일은 물론 공통 기능 설정을 포함하는 기능 그룹 템플릿을 구성합니다.

시작하기 전에

서비스 프로파일 구성, 76 페이지

프로시저

단계 **1** [Cisco Unified CM 관리]에서 사용자 관리 > 사용자/전화기 추가 > 기능 그룹 템플릿을 선택합니다.

단계 **2** 새로 추가를 클릭합니다.

단계 **3** 기능 그룹 템플릿에 대한 이름 및 설명을 입력합니다.

단계 **4** 이 템플릿을 사용하는 모든 사용자에 대해 로컬 클러스터를 홈 클러스터로 사용하려는 경우 홈 클러스터 확인란을 선택합니다.

단계 **5** 이 템플릿을 사용하는 사용자가 인스턴트 메시징 및 프레전스 정보를 교환하도록 하려면 **Unified CM IM and Presence**에 대해 사용자 활성화 확인란을 선택합니다.

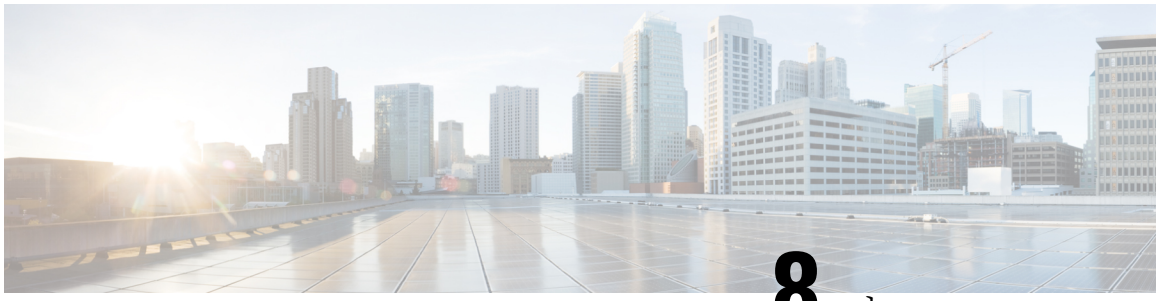
단계 **6** 드롭다운 목록에서 서비스 프로파일 및 사용자 프로파일을 선택합니다.

단계 **7** 기능 그룹 템플릿 구성 창에서 나머지 필드를 완성합니다. 필드 설명은 온라인 도움말을 참조하십시오.

단계 **8** 저장을 클릭합니다.

다음에 수행할 작업

이 기능 그룹 템플릿이 포함된 LDAP 디렉터리 동기화를 구성합니다. LDAP 동기화를 완료하면 템플릿의 IM and Presence 설정이 동기화된 사용자에게 적용됩니다. LDAP 동기화 구성 작업 흐름, 81 페이지 참조



8 장

LDAP 디렉터리 구성

LDAP 동기화 개요

LDAP(Lightweight Directory Access Protocol) 동기화를 사용하면 시스템의 최종 사용자를 프로비저닝하고 구성할 수 있습니다. LDAP 동기화 중 시스템은 외부 LDAP 디렉터리의 사용자 목록 및 관련 사용자 데이터를 Unified Communications Manager 데이터베이스로 가져옵니다. 가져오는 동안 최종 사용자를 구성할 수도 있습니다.

참고 Unified Communications Manager는 LDAPS(SSL이 있는 LDAP)를 지원하지만 StartTLS가 있는 LDAP는 지원하지 않습니다. LDAP 서버 인증서를 Unified Communications Manager에 Tomcat-Trust로 업로드하십시오.

지원되는 LDAP 디렉터리에 대한 정보는 *Cisco Unified Communications Manager* 및 *IM and Presence* 서비스의 호환성 매트릭스를 참조하십시오.

LDAP 동기화는 다음과 같은 기능을 광고합니다.

- 최종 사용자 가져오기—초기 시스템 설정 중에 LDAP 동기화를 사용하여 사용자 목록을 회사 LDAP 디렉토리에서 Unified Communications Manager 데이터베이스로 가져올 수 있습니다. 기능 그룹 템플릿, 사용자 프로파일, 서비스 프로파일, 범용 디바이스 및 회선 템플릿 등의 항목을 미리 구성한 경우에는 사용자에게 구성을 적용하고 동기화 프로세스 중에 구성된 디렉터리 번호와 디렉터리 URI를 할당할 수 있습니다. LDAP 동기화 프로세스는 사용자 및 사용자 특정 데이터 목록을 가져오고 사용자가 설정한 구성 템플릿을 적용합니다.

참고 초기 동기화가 이미 발생한 후에는 LDAP 동기화를 편집할 수 없습니다.

- 예약된 업데이트—예약된 간격으로 여러 LDAP 디렉터리와 동기화하도록 Unified Communications Manager를 구성하여 데이터베이스가 정기적으로 업데이트되고 사용자 데이터가 최신 상태로 유지되도록 할 수 있습니다.
- 최종 사용자 인증—Cisco Unified Communications Manager 데이터베이스가 아닌 LDAP 디렉터리에 대해 최종 사용자 암호를 인증하도록 시스템을 구성할 수 있습니다. LDAP 인증은 회사가 모든 회사 애플리케이션에 대해 최종 사용자에게 단일 암호를 할당하는 기능을 제공합니다. 이 기능은 PIN 또는 애플리케이션 사용자 암호에는 적용되지 않습니다.
- **Cisco** 모바일 및 원격 액세스 클라이언트와 엔드포인트에 대한 디렉터리 서버 사용자 검색— 엔터프라이즈 방화벽 외부에서 작동하는 경우에도 회사 디렉터리 서버를 검색할 수 있습니다. 이 기능을 활성화하면 사용자 데이터 서비스(UDS)가 프록시로 작동하고 사용자 검색 요청을 Unified Communications Manager 데이터베이스로 보내는 대신 회사 디렉터리로 보냅니다.

최종 사용자에 대한 **LDAP** 인증

LDAP 동기화를 사용하면 Cisco Unified Communications Manager 데이터베이스가 아닌 LDAP 디렉터리에 대해 최종 사용자 암호를 인증하도록 시스템을 구성할 수 있습니다. LDAP 인증은 회사가 모든 회사 애플리케이션에 대해 최종 사용자에게 단일 암호를 할당하는 기능을 제공합니다. 이 기능은 PIN 또는 애플리케이션 사용자 암호에는 적용되지 않습니다.

Cisco 모바일 및 원격 액세스 클라이언트와 엔드포인트에 대한 디렉터리 서버 사용자 검색

이전 릴리스에서는 Cisco 모바일 및 원격 액세스 클라이언트(예: Cisco Jabber) 또는 엔드 포인트(예: Cisco DX 80 전화기)를 사용하는 사용자가 엔터프라이즈 방화벽 외부에서 사용자 검색을 수행했을 때 결과는 Cisco Unified Communications Manager 데이터베이스에 저장되는 해당 사용자 계정을 기반으로했습니다. 데이터베이스에는 로컬로 구성되거나 회사 디렉터리에서 동기화되는 사용자 계정이 포함됩니다.

이번 릴리스에서 Cisco 모바일 및 원격 액세스 클라이언트와 엔드포인트는 엔터프라이즈 방화벽 외부에서 작동하는 경우에도 회사 디렉터리 서버를 검색할 수 있습니다. 이 기능을 활성화하면 사용자 데이터 서비스(UDS)가 프록시로 작동하고 사용자 검색 요청을 Cisco Unified Communications Manager 데이터베이스로 보내는 대신 회사 디렉터리로 보냅니다.

다음 결과를 얻으려면 이 기능을 사용합니다.

- 지리적 위치와 상관없이 동일한 사용자 검색 결과 제공 - 모바일 및 원격 액세스 클라이언트와 엔드포인트는 엔터프라이즈 방화벽 외부에 연결되어 있는 경우에도 회사 디렉터리를 사용하여 사용자 검색을 수행할 수 있습니다.
- Cisco Unified Communications Manager 데이터베이스에 구성된 사용자 계정 수 감소 - 이제 모바일 클라이언트는 회사 디렉터리의 사용자를 검색할 수 있습니다. 이전 릴리스에서는 사용자 검색 결과가 데이터베이스에 구성된 사용자를 기반으로 했습니다. 이제 관리자는 더 이상 사용자 검색을 위해 데이터베이스에 사용자 계정을 구성하거나 동기화할 필요가 없습니다. 관리자는

클러스터가 제공하는 사용자 계정만 구성해야 합니다. 데이터베이스의 총 사용자 계정 수를 줄이면 전체 데이터베이스 성능이 향상되면서 소프트웨어 업그레이드 시간도 단축됩니다.

이 기능을 설정하려면 **LDAP** 검색 설정 창에서 엔터프라이즈 디렉터리 서버에 대한 사용자 검색 활성화 옵션을 활성화하고 LDAP 디렉터리 서버 세부 정보를 설정해야 합니다. 자세한 내용은 엔터프라이즈 디렉터리 사용자 검색 구성, 86 페이지 절차를 참조하십시오.

LDAP 동기화 필수 조건

필수 작업

LDAP 디렉터리에서 최종 사용자를 가져오기 전에 다음 작업을 완료하십시오.

- 사용자 액세스 구성
- 인증서 정책 구성
- 기능 그룹 템플릿 구성

데이터를 시스템에 동기화하려는 사용자의 경우, 활성 디렉터리 서버의 전자 메일 ID 필드가 고유한 항목인지 또는 공백으로 남겨져 있는지 확인하십시오.

LDAP 동기화 구성 작업 흐름

다음 작업을 사용하여 외부 LDAP 디렉터리에서 사용자 목록을 가져와서 Unified Communications Manager 데이터베이스로 가져올 수 있습니다.

참고 이미 LDAP 디렉터리를 한 번 동기화한 경우 외부 LDAP 디렉터리의 새 항목을 계속 동기화할 수 있지만 Unified Communications Manager의 새 구성을 LDAP 디렉터리 동기화에 추가할 수는 없습니다. 이 경우 사용자 업데이트 또는 사용자 삽입과 같은 벌크 관리 도구 및 메뉴를 사용할 수 있습니다. *Cisco Unified Communications Manager* 벌크 관리 설명서를 참조하십시오.

프로시저

	명령 또는 동작	목적
단계 **1**	Cisco DirSync 서비스 활성화, 82 페이지	Cisco Unified 서비스 가용성에 로그인하고 Cisco DirSync 서비스를 활성화합니다.
단계 **2**	LDAP 디렉터리 동기화 활성화, 82 페이지	Unified Communications Manager에서 LDAP 디렉터리 동기화를 활성화합니다.

	명령 또는 동작	목적
단계 3	LDAP 필터 만들기, 83 페이지	선택 사항. Unified Communications Manager가 회사 LDAP 디렉터리의 사용자 하위 집합만 동기화하도록 하려면 LDAP 필터를 만듭니다.
단계 4	LDAP 디렉터리 동기화 구성, 84 페이지	필드 설정, LDAP 서버 위치, 동기화 일정 및 액세스 제어 그룹, 기능 그룹 템플릿 및 기본 내선 번호에 대한 할당과 같은 LDAP 디렉터리 동기화 설정을 구성합니다.
단계 5	엔터프라이즈 디렉터리 사용자 검색 구성, 86 페이지	선택 사항. 엔터프라이즈 디렉터리 서버 사용자 검색을 위해 시스템을 구성합니다. 이 절차에 따라 데이터베이스 대신 엔터프라이즈 디렉터리 서버에 대한 사용자 검색을 수행하도록 시스템의 전화기 및 클라이언트를 구성하십시오.
단계 6	LDAP 인증 구성, 88 페이지	선택 사항. 최종 사용자 암호 인증에 LDAP 디렉터리를 사용하려면 LDAP 인증 설정을 구성합니다.
단계 7	LDAP 계약 서비스 파라미터 사용자 지정, 88 페이지	선택 사항. 선택 사항 LDAP 동기화 서비스 파라미터를 구성합니다. 대부분의 구축의 경우 기본값으로 충분합니다.

Cisco DirSync 서비스 활성화

이 절차를 수행하여 Cisco Unified 서비스 가용성에서 Cisco DirSync 서비스를 활성화하십시오. 회사 LDAP 디렉터리에서 최종 사용자 설정을 동기화하려면 이 서비스를 활성화하십시오.

프로시저

단계 1 Cisco Unified 서비스 가용성에서 도구 > 서비스 활성화를 선택합니다.
단계 2 서버 드롭다운 목록에서 게시자 노드를 선택합니다.
단계 3 디렉터리 서비스 아래에서 **Cisco DirSync** 라디오 버튼을 클릭합니다.
단계 4 저장을 클릭합니다.

LDAP 디렉터리 동기화 활성화

회사 LDAP 디렉터리의 최종 사용자 설정을 동기화하기 위해 Unified Communications Manager를 구성하려는 경우, 이 절차를 수행합니다.

참고 이미 LDAP 디렉터리를 한 번 동기화한 경우 외부 LDAP 디렉터리의 새 사용자를 계속 동기화할 수 있지만 Unified Communications Manager의 새 구성을 LDAP 디렉터리 동기화에 추가할 수는 없습니다. 또한 기능 그룹 템플릿 또는 사용자 프로파일과 같은 기본 구성 항목에 편집을 추가할 수도 없습니다. 한 번의 LDAP 동기화를 이미 완료하고 다른 설정을 사용하여 사용자를 추가하려는 경우, 사용자 업데이트 또는 사용자 삽입과 같은 벌크 관리 메뉴를 사용할 수 있습니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 시스템 > **LDAP** > **LDAP** 시스템을 선택합니다.

단계 **2** Cisco Unified Communications Manager가 LDAP 디렉터리에서 사용자를 가져오게 하려는 경우, **LDAP** 서버와 동기화 활성화 확인란을 선택합니다.

단계 **3** **LDAP** 서버 유형 드롭다운 목록에서 회사에서 사용하는 LDAP 디렉터리 서버 유형을 선택합니다.

단계 **4** 사용자 **ID**의 **LDAP** 특성 드롭다운 목록에서 Unified Communications Manager가 최종 사용자 설정 창의 사용자 **ID** 필드에 대해 동기화할 회사 LDAP 디렉터리에서 속성을 선택합니다.

단계 **5** 저장을 클릭합니다.

LDAP 필터 만들기

LDAP 디렉터리에서 사용자의 하위 집합으로 LDAP 동기화를 제한하기 위해 LDAP 필터를 만들 수 있습니다. LDAP 디렉터리에 LDAP 필터를 적용하면 Unified Communications Manager는 LDAP 디렉터리에서 필터와 일치하는 사용자만 가져옵니다.

참고 구성하는 모든 LDAP 필터는 RFC4515에 지정된 LDAP 검색 필터 표준을 준수하십시오.

프로시저

단계 **1** Cisco Unified CM 관리에서 시스템 > **LDAP** > **LDAP** 필터를 선택합니다.

단계 **2** 새로 추가를 클릭하여 새 LDAP 필터를 만듭니다.

단계 **3** 필터 이름 텍스트 상자에 LDAP 필터의 이름을 입력합니다.

단계 **4** 필터 텍스트 상자에 필터를 입력합니다. 필터에는 최대 1024자의 UTF-8 문자를 사용할 수 있으며 괄호 ()로 묶어 주어야 합니다.

단계 **5** 저장을 클릭합니다.

LDAP 디렉터리 동기화 구성

이 절차를 사용하여 LDAP 디렉터리와 동기화하도록 Unified Communications Manager를 구성합니다. LDAP 디렉터리 동기화를 사용하면 최종 사용자 데이터를 외부 LDAP 디렉터리에서 Unified Communications Manager 데이터베이스로 가져와 최종 사용자 구성 창에 표시할 수 있습니다. 범용 회선 및 장치 템플릿을 사용 하는 설정 기능 그룹 템플릿이 있는 경우 새로 프로비저닝된 사용자 및 해당 내선 번호에 대한 설정을 자동으로 할당할 수 있습니다.

팁 액세스 제어 그룹 또는 기능 그룹 템플릿을 할당하는 경우 LDAP 필터를 사용하여 동일한 구성 요구 사항을 가진 사용자 그룹으로 가져오기를 제한할 수 있습니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 시스템 > **LDAP** > **LDAP** 디렉터리를 선택합니다.

단계 **2** 다음 단계 중 하나를 수행합니다.

- 찾기를 클릭하고 기존 LDAP 디렉터리를 선택합니다.
- 새로 추가를 클릭하여 새 LDAP 디렉터리를 만듭니다.

단계 **3** **LDAP** 디렉터리 구성에서 다음을 입력합니다.

a) **LDAP** 구성 이름 필드에서 LDAP 디렉터리에 고유한 이름을 할당합니다.
b) **LDAP** 관리자 고유 이름 필드에 LDAP 디렉터리 서버에 액세스할 수 있는 사용자 ID를 입력합니다.
c) 암호 세부 정보를 입력하고 확인합니다.
d) [**LDAP** 사용자 검색 공간] 필드에 검색 공간 세부 정보를 입력합니다.
e) [사용자 사용자에 대한 **LDAP** 사용자 정의 필터] 필드에서 사용자만 또는 사용자 및 그룹 중 하나를 선택합니다.
f) (선택 사항) 가져 오기를 특정 프로파일을 충족하는 사용자의 하위 집합으로만 제한하려는 경우 그룹에 대한 **LDAP** 사용자 정의 필터 드롭다운 목록에서 LDAP 필터를 선택합니다.

단계 **4** **LDAP** 디렉터리 동기화 일정 필드에서 Unified Communications Manager가 데이터를 외부 LDAP 디렉터리와 동기화하는 데 사용하는 일정을 만듭니다.

단계 **5** 동기화할 표준 사용자 필드 섹션을 완성합니다. 각 최종 사용자 필드에 대한 LDAP 특성을 선택합니다. 동기화 프로세스는 Unified Communications Manager의 최종 사용자 필드에 LDAP 특성의 값을 할당합니다.

단계 **6** URI 다이얼을 배포 하는 경우 사용자의 기본 디렉터리 URI 주소에 사용 될 LDAP 특성을 할당 하십시오.

단계 **7** 동기화 할 사용자 정의 사용자 필드 섹션에서 필수 LDAP 특성을 사용하여 사용자 정의 사용자 필드 이름을 입력합니다.

단계 **8** 가져온 최종 사용자를 모든 가져온 최종 사용자에 공통된 액세스 제어 그룹에 할당하려면 다음을 수행하십시오.

a) 액세스 제어 그룹에 추가를 클릭합니다.

b) 팝업 창에서 가져온 최종 사용자에게 할당할 각 액세스 제어 그룹에 해당하는 확인란을 클릭합니다.

c) 선택한 항목 추가를 클릭합니다.

단계 **9** 기능 그룹 템플릿을 할당하려면 기능 그룹 템플릿 드롭다운 목록에서 해당 템플릿을 선택합니다.

참고 최종 사용자는 사용자가 없을 때만 처음으로 할당된 기능 그룹 템플릿과 동기화됩니다. 기존 기능 그룹 템플릿이 수정되고 연결된 LDAP에 대해 전체 동기화가 수행되는 경우 수정 사항이 업데이트되지 않습니다.

단계 **10** 가져온 전화 번호에 마스크를 적용하여 기본 내선 번호를 할당하려면 다음을 수행하십시오.

a) 동기화된 전화 번호에 마스크를 적용하여 삽입된 사용자에 대한 새 회선 만들기 확인란을 선택합니다.

b) 마스크를 입력합니다. 예를 들어, 가져온 전화 번호가 8889945인 경우 11XX의 마스크는 기본 내선 번호 1145를 만듭니다.

단계 **11** 디렉터리 번호 풀에서 기본 내선 번호를 할당하려면 다음을 수행하십시오.

a) 동기화된 **LDAP** 전화 번호를 기준으로 새 회선이 만들어지지 않은 경우 풀 목록에서 새 회선 할당 확인란을 선택합니다.

b) **DN** 풀 시작 및 **DN** 풀 끝 텍스트 상자에 기본 내선 번호를 선택할 수 있는 디렉터리 번호의 범위를 입력합니다.

단계 **12** (선택사항) Jabber 엔드포인트 프로비저닝 섹션에서 Jabber 장치를 생성하려는 경우 다음 드롭다운에서 자동 프로비저닝에 필요한 Jabber 장치 중 하나를 선택합니다:

- Android용 Cisco 이중 모드(BOT)
- iPhone용 Cisco 이중 모드(TCT)
- 태블릿용 Cisco Jabber(TAB)
- Cisco Unified 클라이언트 서비스 프레임워크(CSF)

참고 **LDAP**에 다시 쓰기 옵션을 사용하면 Unified CM에서 선택한 기본 DN을 LDAP 서버에 다시 쓸 수 있습니다. 다시 쓰기에 사용할 수 있는 LDAP 특성은 **telephoneNumber**, **ipPhone** 및 **mobile**입니다.

단계 **13** **LDAP** 서버 정보 섹션에 LDAP 서버의 호스트 이름 또는 IP 주소를 입력합니다.

단계 **14** TKS를 사용하여 LDAP 서버에 대한 보안 연결을 생성하려면 **TLS** 사용 확인란을 선택합니다.

참고 Tomcat을 다시 시작한 후 보안 포트를 통해 사용자를 동기화하려고 하면 사용자가 동기화되지 않는 경우가 있습니다. 사용자 동기화가 성공적으로 이루어지려면 Cisco DirSync 서비스를 다시 시작해야 합니다.

단계 **15** 저장을 클릭합니다.

단계 **16** LDAP 동기화를 완료 하려면 지금 전체 동기화 수행을 클릭합니다. 그렇지 않으면 예약된 동기화를 기다릴 수 있습니다.

참고 LDAP에서 사용자를 삭제 하면 24 시간 후에 자동으로 Unified Communications Manager에서 해당 사용자가 제거 됩니다. 뿐만 아니라, 삭제 된 사용자가 다음 장치 중 하나에 대한 이동성 사용자로 구성된 경우 이러한 비활성 장치도 자동으로 삭제 됩니다.

- 원격 대상 프로파일
- 원격 대상 프로파일 템플릿
- 모바일 스마트 클라이언트
- CTI 원격 디바이스
- Spark 원격 디바이스
- Nokia S60
- iPhone용 Cisco 이중 모드
- IMS 통합 모바일(기본)
- 통신사업자 통합 모바일
- Android용 Cisco 이중 모드

엔터프라이즈 디렉터리 사용자 검색 구성

이 절차를 사용하여 데이터베이스 대신 엔터프라이즈 디렉터리 서버에 대한 사용자 검색을 수행하도록 시스템의 전화기 및 클라이언트를 구성하십시오.

시작하기 전에

- LDAP 사용자 검색을 위해 선택하는 1차, 2차 및 3차 서버가 Unified Communications Manager 가입자 노드에 연결할 수 있는 네트워크인지 확인하십시오.
- 시스템 > **LDAP** > **LDAP** 시스템에서 **LDAP** 시스템 설정 창의 **LDAP** 서버 유형 드롭다운 목록에서 LDAP 서버 유형을 설정합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 시스템 > **LDAP** > **LDAP** 검색을 선택합니다.

단계 **2** 엔터프라이즈 LDAP 디렉터리 서버를 사용하여 사용자 검색을 수행할 수있도록 하려면 엔터프라이즈 디렉터리 서버에 대한 사용자 검색 활성화 확인란을 선택합니다.

단계 **3** **LDAP** 검색 구성 창에서 필드를 구성합니다. 필드 및 해당 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

단계 **4** 저장을 클릭합니다.

참고 OpenLDAP 서버에서 회의실 객체로 표시된 회의실을 검색하려면 사용자 지정 필터를 (objectClass=intOrgPerson)(objectClass=rooms))로 구성합니다. 따라서 Cisco Jabber 클라이언트가 이름으로 회의실을 검색하고 회의실과 연결된 번호로 전화를 걸 수 있습니다.

회의실 객체에 대해 OpenLDAP 서버에 **givenName** or **sn** or **mail** or **displayName** 또는 **telephonenumber** 특성이 구성된 경우 회의실을 검색할 수 있습니다.

디렉터리 서버의 **UDS** 검색을 위한 **LDAP** 특성

다음 표에는 엔터프라이즈 디렉터리 서버에 대한 사용자 검색 활성화 옵션을 사용할 때 UDS 사용자 검색 요청에서 사용하는 LDAP 특성이 나열되어 있습니다. 이러한 유형의 디렉터리 요청의 경우 UDS는 프록시 역할을 수행하고 검색 요청을 회사 디렉터리 서버로 릴레이합니다.

참고 UDS 사용자 응답 태그는 LDAP 특성 중 하나에 매핑될 수 있습니다. 특성 매핑은 **LDAP** 서버 유형 드롭다운 목록에서 선택한 옵션에 따라 결정됩니다. 시스템 > **LDAP** > **LDAP** 시스템 구성 창에서 이 드롭다운 목록에 액세스합니다.

UDS 사용자 응답 태그	**LDAP** 특성
userName	• samAccountName • uid
firstName	givenName
lastName	sn
middleName	• initials • middleName
nickName	nickName
displayName	displayName
phoneNumber	• telephonenumber • ipPhone
homeNumber	homephone
mobileNumber	mobile
email	mail

UDS 사용자 응답 태그	LDAP 특성
directoryUri	• msRTCSIP-primaryuseraddress • mail
department	• department • departmentNumber
관리자	관리자
title	title
pager	pager

LDAP 인증 구성

회사 LDAP 디렉터리에 할당된 암호에 대해 최종 사용자 암호가 인증되도록 LDAP 인증을 활성화하려면 이 절차를 수행하십시오. 이 구성은 최종 사용자 암호에만 적용되며 최종 사용자 PIN 또는 애플리케이션 사용자 암호에는 적용되지 않습니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 시스템 > **LDAP** > **LDAP** 인증을 선택합니다.

단계 **2** 사용자 인증에 LDAP 디렉터리를 사용하려면 최종 사용자에 대한 **LDAP** 인증 확인란을 선택합니다.

단계 **3** **LDAP** 관리자 고유 이름 필드에 LDAP 디렉터리에 대한 액세스 권한이 있는 LDAP 관리자의 사용자 ID를 입력합니다.

단계 **4** 암호 확인 필드에 LDAP 관리자의 암호를 입력합니다.

단계 **5** [**LDAP** 사용자 검색 기준] 필드에 검색 조건을 입력합니다.

단계 **6** **LDAP** 서버 정보 섹션에 LDAP 서버의 호스트 이름 또는 IP 주소를 입력합니다.

단계 **7** TKS를 사용하여 LDAP 서버에 대한 보안 연결을 생성하려면 **TLS** 사용 확인란을 선택합니다.

단계 **8** 저장을 클릭합니다.

다음에 수행할 작업

LDAP 계약 서비스 파라미터 사용자 지정, 88 페이지

LDAP 계약 서비스 파라미터 사용자 지정

LDAP 계약에 대한 시스템 수준 설정을 사용자 지정하는 서비스 파라미터를 구성하려면 이 절차를 수행하십시오. 이러한 서비스 파라미터를 구성하지 않을 경우 Unified Communications Manager는

LDAP 디렉터리 통합에 대한 기본 설정을 적용합니다. 파라미터에 대한 설명을 보려면 사용자 인터페이스에서 파라미터 이름을 클릭합니다.

서비스 파라미터를 사용하여 아래 설정을 사용자 지정할 수 있습니다.

- 계약의 최대 수—기본값은 20입니다.
- 최대 호스트 수—기본값은 3입니다.
- 호스트 장애 발생 시 재시도 지연(초)—호스트 장애의 기본값은 5입니다.
- **HotList** 장애 발생 시 재시도 지연(분)—hostlist 실패의 기본값은 10입니다.
- **LDAP** 연결 시간 초과(초)—기본값은 5입니다.
- 지연된 동기화 시작 시간(분)—기본값은 5입니다.
- 사용자 고객 맵 감사 시간

프로시저

단계 **1** Cisco Unified CM 관리에서 시스템 > 서비스 파라미터를 선택합니다.
단계 **2** 서버 드롭다운 목록 상자에서 게시자 노드를 선택합니다.
단계 **3** 서비스 드롭다운 목록 상자에서 **Cisco DirSync**를 선택합니다.
단계 **4** Cisco DirSync 서비스 파라미터 값을 구성합니다.
단계 **5** 저장을 클릭합니다.

LDAP 디렉터리 서비스 파라미터

서비스 파라미터	설명
계약의 최대 수	구성할 수 있는 LDAP 디렉터리의 최대 수입니다. 기본 설정은 20입니다.
호스트의 최대 수	장애 조치를 위해 구성할 수 있는 LDAP 호스트 이름의 최대 수입니다. 기본값은 3입니다.
호스트 오류시 재시도 지연(초)	호스트 오류가 발생한 후 Cisco Unified Communications Manager가 첫 번째 LDAP 서버 (호스트 이름)에 대한 연결을 재시도하기까지 지연되는 시간(초)입니다. 기본값은 5입니다.
호스트 목록 오류 시 재시도 지연(분)	호스트 목록 오류가 발생한 후 Cisco Unified Communications Manager가 구성된 모든 LDAP 서버(호스트 이름)를 재시도하기까지 지연되는 시간(분)입니다. 기본값은 10입니다.

서비스 파라미터	설명
LDAP 연결 시간 초과(초)	Cisco Unified Communications Manager가 LDAP 연결을 설정할 때 허용하는 시간(초)입니다. LDAP 서비스 공급자는 지정된 시간 내에 연결을 설정할 수 없는 경우 연결 시도를 중단합니다. 기본값은 5입니다.
지연된 동기화 시작 시간(분)	Cisco DirSync 서비스가 시작된 후 디렉터리 동기화 프로세스를 시작할 때 Cisco Unified Communications Manager가 지연되는 시간(분)입니다. 기본값은 5입니다.

LDAP 동기화된 사용자를 로컬 사용자로 변환

LDAP 동기화된 최종 사용자의 경우 LDAP 디렉터리를 Cisco Unified Communications Manager와 동기화할 때 LDAP 동기화된 사용자를 로컬 사용자로 변환하지 않으면 최종 사용자 구성 창의 필드를 편집할 수 없습니다.

최종 사용자 구성 창에서 LDAP 동기화된 필드를 편집하려면 사용자를 로컬 사용자로 변환합니다. 그러나 이 변환을 수행하면 Cisco Unified Communications Manager가 LDAP 디렉터리와 동기화될 때 최종 사용자가 업데이트되지 않습니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 최종 사용자 > 최종 사용자 관리를 선택합니다.

단계 **2** 찾기를 클릭하고 최종 사용자를 선택합니다.

단계 **3** 로컬 사용자로 변환 버튼을 클릭합니다.

단계 **4** 최종 사용자 구성 창을 업데이트합니다.

단계 **5** 저장을 클릭합니다.

액세스 제어 그룹에 LDAP 동기화된 사용자 할당

이 절차를 수행하여 액세스 제어 그룹에 LDAP 동기화된 사용자를 할당합니다.

시작하기 전에

Cisco Unified Communications Manager는 최종 사용자가 외부 LDAP 디렉터리와 동기화하도록 구성되어야 합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 시스템 > **LDAP** > **LDAP** 디렉터리를 선택합니다.

단계 **2** 찾기를 클릭하고 구성된 LDAP 디렉터리를 선택합니다.

단계 **3** 액세스 제어 그룹에 추가 버튼을 클릭합니다.

단계 **4** 이 LDAP 디렉터리에서 최종 사용자에 적용하려는 액세스 제어 그룹을 선택합니다.

단계 **5** 선택한 항목 추가를 클릭합니다.

단계 **6** 저장을 클릭합니다.

단계 **7** 전체 동기화 수행을 클릭합니다.
Cisco Unified Communications Manager가 외부 LDAP 디렉터리와 동기화하고 동기화된 사용자를 올바른 액세스 제어 그룹에 삽입합니다.

참고 처음으로 액세스 제어 그룹을 추가할 때만 동기화된 사용자가 선택된 액세스 그룹에 삽입됩니다. 이후에 LDAP에 추가하는 그룹은 전체 동기화를 수행한 후 동기화된 사용자에게 적용되지 않습니다.

XMPP 클라이언트에서 연락처를 검색하기 위한 LDAP 디렉터리 통합

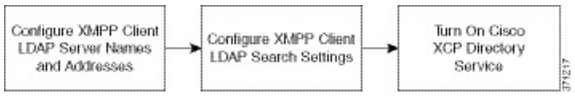
이 항목에서는 타사 XMPP 클라이언트 사용자가 LDAP 디렉터리에서 연락처를 검색 및 추가할 수 있도록 IM and Presence 서비스에서 LDAP 설정을 구성하는 방법에 대해 설명합니다.

IM and Presence 서비스의 JDS 구성 요소는 타사 XMPP 클라이언트와 LDAP 디렉터리의 통신을 처리합니다. 타사 XMPP 클라이언트는 IM and Presence 서비스의 JDS 구성 요소에 쿼리를 전송합니다. JDS 구성 요소는 프로비저닝된 LDAP 서버로 LDAP 쿼리를 전송한 다음 XMPP 클라이언트로 결과를 다시 전송합니다.

여기에 설명된 구성을 수행하기 전에 XMPP 클라이언트를 Cisco Unified Communications Manager 및 IM and Presence 서비스와 통합하기 위한 구성을 수행하십시오. 타사 XMPP 클라이언트 애플리케이션 통합과 관련된 항목을 참조하십시오.

그림 ***3: XMPP*** 클라이언트에서 연락처를 검색하기 위한 ***LDAP*** 디렉터리 통합 워크플로

다음 워크플로 다이어그램은 XMPP 클라이언트에서 연락처를 검색할 수 있도록 LDAP 디렉터리를 통합하는 간단한 단계를 보여줍니다.



다음 표에는 XMPP 클라이언트에서 연락처를 검색할 수 있도록 LDAP 디렉터리를 통합하기 위해 수행해야 할 작업이 나열되어 있습니다. 자세한 지침은 관련 작업을 참조하십시오.

표 *7: XMPP* 클라이언트에서 연락처를 검색하기 위한 *LDAP* 디렉터리 통합의 작업 목록

작업	설명
XMPP 클라이언트 LDAP 서버 이름 및 주소 구성	SSL을 활성화하고 LDAP 서버와 IM and Presence 서비스 간 보안 연결을 설정한 경우 루트 CA 인증서를 xmpp-trust-certificate로서 IM and Presence 서비스에 업로드하십시오. 팁 인증서의 제목 CN은 LDAP 서버의 FQDN과 일치해야 합니다.
XMPP 클라이언트 LDAP 검색 설정 구성	IM and Presence 서비스에서 타사 XMPP 클라이언트에 대해 연락처를 성공적으로 검색하도록 하려면 LDAP 검색 설정을 지정해야 합니다. 기본 LDAP 서버 하나와 백업 LDAP 서버 최대 2개를 지정할 수 있습니다. 팁 선택적으로 LDAP 서버에서 vCards를 검색하는 기능을 설정하거나 IM and Presence 서비스의 로컬 데이터베이스에 vCards를 저장하도록 허용할 수 있습니다.
Cisco XCP 디렉터리 서비스 설정	타사 XMPP 클라이언트의 사용자가 LDAP 디렉터리에서 연락처를 검색 및 추가하도록 허용하려면 XCP 디렉터리 서비스를 설정해야 합니다. 팁 타사 XMPP 클라이언트의 LDAP 서버 및 LDAP 검색 설정을 구성하기 전에는 Cisco XCP 디렉터리 서비스를 설정하지 마십시오. 그렇지 않으면 서비스 실행이 중단될 수 있습니다.

LDAP 계정 잠금 문제

타사 XMPP 클라이언트에 대해 구성한 LDAP 서버에 잘못된 암호를 입력하고 IM and Presence 서비스에 대해 XCP 서비스를 다시 시작하면, JDS 구성 요소는 잘못된 암호로 LDAP 서버에 여러 번 로그인을 시도하게 됩니다. 허용된 실패 횟수 이후 계정을 잠그도록 LDAP 서버가 구성된 경우 LDAP 서버는 특정 시점에 JDS 구성 요소를 잠글 수 있습니다. JDS 구성 요소가 LDAP에 연결된 다른 애플리케이션과 동일한 자격 증명을 사용하는 경우(애플리케이션이 반드시 IM and Presence 서비스에 있어야 하는 것은 아님), 이러한 애플리케이션도 LDAP에서 잠기게 됩니다.

이 문제를 해결하려면 기존 LDAP 사용자와 동일한 역할과 권한을 보유한 별도의 사용자를 구성하고, 이 두 번째 사용자로는 JDS에만 로그인하도록 구성하십시오. LDAP 서버에 잘못된 암호를 입력하면 LDAP 서버에서 JDS 구성 요소만 잠깁니다.

XMPP 클라이언트의 LDAP 서버 이름 및 주소 구성

SSL(Secured Sockets Layer)을 활성화하기로 선택한 경우, LDAP 서버와 IM and Presence 서비스 간 보안 연결을 구성하고 루트 CA(인증 기관) 인증서를 cup-xmpp-trust 인증서로서 IM and Presence 서비스에 업로드하십시오. 인증서의 제목 CN(공통 이름)은 LDAP 서버의 FQDN(정규화된 도메인 이름)과 일치해야 합니다.

인증서 체인(루트 노드에서 신뢰할 수 있는 노드로 하나 이상의 인증서)을 가져오는 경우 리프 노드를 제외한 체인의 모든 인증서를 가져오십시오. 예를 들어 CA가 LDAP 서버에 대한 인증서에 서명하는 경우, CA 인증서만 가져오고 LDAP 서버에 대한 인증서는 가져오지 마십시오.

IM and Presence 서비스와 Cisco Unified Communications Manager 간의 연결이 IPv4이더라도 IPv6을 사용하여 LDAP 서버에 연결할 수 있습니다. IM and Presence 서비스 노드에서 엔터프라이즈 파라미터 또는 ETH0에 대해 IPv6이 비활성화되면, 타사 XMPP 클라이언트에 대해 구성된 외부 LDAP 서버의 호스트 이름이 확인 가능한 IPv6 주소인 경우 해당 노드에서는 여전히 내부 DNS 쿼리를 수행하고 외부 LDAP 서버에 연결할 수 있습니다.

팁 타사 XMPP 클라이언트에 대한 외부 LDAP 서버의 호스트 이름은 **LDAP** 서버 - 타사 **XMPP** 클라이언트 창에서 구성합니다.

시작하기 전에

LDAP 디렉터리의 호스트 이름 또는 IP 주소를 확인합니다.

IPv6을 사용하여 LDAP 서버에 연결하는 경우 LDAP 서버를 구성하기 전에 구축의 각 IM and Presence 서비스 노드에서 엔터프라이즈 파라미터와 Eth0에 대해 IPv6을 활성화합니다.

프로시저

단계 **1** **Cisco Unified CM IM and Presence** 관리애플리케이션 > 타사 클라이언트 > 타사 **LDAP** 서버를 선택합니다.

단계 **2** 새로 추가를 클릭합니다.

단계 **3** LDAP 서버의 ID를 입력합니다.

단계 **4** LDAP 서버의 호스트 이름을 입력합니다.

IPv6 연결의 경우 LDAP 서버의 IPv6 주소를 입력할 수 있습니다.

단계 **5** TCP 또는 SSL 연결을 수신 대기하는 LDAP 서버에서 포트 번호를 지정합니다.

기본 포트는 389입니다. SSL를 활성화할 경우 포트 636을 지정합니다.

단계 **6** LDAP 서버의 사용자 이름과 암호를 지정합니다. 이러한 값은 LDAP 서버에서 구성하는 자격 증명과 일치해야 합니다.

자세한 내용은 LDAP 디렉터리 설명서 또는 LDAP 디렉터리 구성 안내서를 참조하십시오.

단계 **7** LDAP 서버와 통신하는 데 SSL을 사용하려면 **SSL** 활성화를 선택합니다.

참고 SSL이 활성화된 경우 사용자가 입력하는 호스트 이름 값은 LDAP 서버의 호스트 이름이거나 FQDN일 수 있습니다. 사용되는 값은 보안 인증서 **CN** 또는 **SAN** 필드의 값과 일치해야 합니다.

IP 주소를 사용해야 하는 경우 이 값을 **CN** 또는 **SAN** 필드에 대한 인증서에도 사용해야 합니다.

단계 **8** 저장을 클릭합니다.

단계 **9** 클러스터의 모든 노드에서 Cisco XCP 라우터 서비스를 시작합니다(아직 실행되고 있지 않은 경우).

팁

- SSL을 활성화하면 IM and Presence 서비스에서 SSL 연결을 설정한 후 SSL 연결 설정 시 협상 절차 및 데이터 암호화/암호 해독 때문에 XMPP 연락처 검색이 느려질 수 있습니다. 그 결과 사용자가 구축에서 XMPP 연락처 검색을 폭넓게 수행하면 전반적인 시스템 성능에 영향이 미칠 수 있습니다.
- LDAP 서버에 대한 인증서를 업로드한 후 LDAP 서버 호스트 이름 및 포트 값 전달 상태를 확인하려면 인증서 가져오기 도구를 사용할 수 있습니다. **Cisco Unified CM IM and Presence** 관리 시스템 > 보안 > 인증서 가져오기 도구를 선택합니다.
- 타사 XMPP 클라이언트용 LDAP 서버 구성을 업데이트한 경우 Cisco XCP 디렉터리 서비스를 다시 시작하십시오. 이 서비스를 다시 시작하려면 **Cisco Unified IM and Presence** 서비스 가능성 > 도구 > 제어 센터 - 기능 서비스를 선택합니다.

다음에 수행할 작업

계속 진행하여 XMPP 클라이언트용 LDAP 검색 설정을 구성합니다.

XMPP 클라이언트용 LDAP 검색 설정 구성

IM and Presence 서비스에서 타사 XMPP 클라이언트에 대해 연락처를 성공적으로 검색하도록 하려면 LDAP 검색 설정을 지정해야 합니다.

타사 XMPP 클라이언트는 검색 단위로 LDAP 서버에 연결됩니다. 기본 서버에 대한 연결이 실패하면 XMPP 클라이언트는 첫 번째 백업 LDAP 서버를 시도하고, 해당 서버를 사용할 수 없는 경우 두 번째 백업 서버를 시도하는 방식으로 진행합니다. 시스템 장애 조치 중에 LDAP 쿼리가 진행 중이면, 사용 가능한 다음 서버가 이 LDAP 쿼리를 완료합니다.

선택적으로 LDAP 서버에서 vCard 검색 기능을 사용하도록 설정할 수 있습니다. vCard 검색을 설정하면:

- 회사 LDAP 디렉터리는 vCard를 저장합니다.
- XMPP 클라이언트가 자체 vCard 또는 연락처용 vCard를 검색하면, vCard는 JDS 서비스를 통해 LDAP에서 검색됩니다.
- 클라이언트는 회사 LDAP 디렉터리를 편집할 권한이 없으므로 자체 vCard를 설정하거나 수정할 수 없습니다.

LDAP 서버에서 vCard의 검색을 해제하면:

- IM and Presence 서비스는 로컬 데이터베이스에 vCard를 저장합니다.
- XMPP 클라이언트가 자체 vCard 또는 연락처용 vCard를 검색하면, vCard는 로컬 IM and Presence 서비스 데이터베이스에서 검색됩니다.
- 클라이언트는 자체 vCard를 설정하거나 수정할 수 있습니다.

다음 표에는 XMPP 클라이언트용 LDAP 검색 설정이 나열되어 있습니다.

표 ***8: XMPP*** 클라이언트용 ***LDAP*** 검색 설정

필드	설정
LDAP 서버 유형	이 목록에서 LDAP 서버 유형을 선택합니다. • Microsoft Active Directory • 일반 디렉터리 서버 - 지원되는 다른 LDAP 서버 유형(iPlanet, Sun ONE 또는 OpenLDAP)을 사용 중인 경우 이 메뉴를 선택합니다.
사용자 객체 클래스	LDAP 서버 유형에 맞는 사용자 객체 클래스 값을 입력합니다. 이 값은 LDAP 서버에 구성된 사용자 객체 클래스 값과 일치해야 합니다. Microsoft Active Directory를 사용하는 경우 기본값은 'user'입니다.
기본 컨텍스트	LDAP 서버에 맞는 기본 컨텍스트를 입력합니다. 이 값은 LDAP 서버에서 전에 구성한 도메인 및/또는 조직 구조와 일치해야 합니다.
사용자 속성	LDAP 서버 유형에 맞는 사용자 속성 값을 입력합니다. 이 값은 LDAP 서버에 구성된 사용자 속성 값과 일치해야 합니다. Microsoft Active Directory를 사용하는 경우 기본값은 sAMAccountName입니다. 디렉터리 URI IM 주소 체계가 사용되며 디렉터리 URI가 mail 또는 msRTCSIPPrimaryUserAddress로 매핑되는 경우, 사용자 속성으로 mail 또는 msRTCSIPPrimaryUserAddress를 지정해야 합니다.
LDAP 서버 1	기본 LDAP 서버를 선택합니다.
LDAP 서버 2	(선택 사항) 백업 LDAP 서버를 선택합니다.
LDAP 서버 3	(선택 사항) 백업 LDAP 서버를 선택합니다.

시작하기 전에

XMPP 클라이언트용 LDAP 서버의 이름과 주소를 지정합니다.

프로시저

단계 **1** **Cisco Unified CM IM and Presence** 관리애플리케이션 > 타사 클라이언트 > 타사 **LDAP** 설정을 선택합니다.

단계 **2** 필드에 정보를 입력합니다.

단계 **3** 사용자가 연락처에 대한 vCard를 요청하고 LDAP 서버에서 vCard 정보를 검색하도록 하려면 **LDAP** 에서 **vCards** 빌드를 선택합니다. 사용자가 연락처 목록에 추가될 때 클라이언트에서 사용자에 대한 vCard를 자동으로 요청하도록 하려면 이 확인란을 선택하지 않습니다. 이 경우 클라이언트는 로컬 IM and Presence 서비스 데이터베이스에서 vCard 정보를 검색합니다.

단계 **4** vCard FN 필드를 구성하는 데 필요한 LDAP 필드를 입력합니다. 사용자가 연락처의 vCard를 요청하면 클라이언트는 vCard FN 필드의 값을 사용하여 연락처 목록에 있는 연락처의 이름을 표시합니다.

단계 **5** 검색 가능한 LDAP 속성 테이블에서 클라이언트 사용자 필드를 LDAP 사용자 필드에 매핑합니다.

Microsoft Active Directory를 사용하는 경우 IM and Presence 서비스는 테이블의 기본 속성 값을 채웁니다.

단계 **6** 저장을 클릭합니다.

단계 **7** Cisco XCP 라우터 서비스를 시작합니다(아직 실행되고 있지 않은 경우).

팁 타사 XMPP 클라이언트용 LDAP 검색 구성으로 업데이트한 경우 Cisco XCP 디렉터리 서비스를 다시 시작하십시오. 이 서비스를 다시 시작하려면 **Cisco Unified IM and Presence** 서비스 가능성 > 도구 > 제어 센터 - 기능 서비스를 선택합니다.

다음에 수행할 작업

계속 진행하여 Cisco XCP 디렉터리 서비스를 설정합니다.

Cisco XCP 디렉터리 서비스 설정

타사 XMPP 클라이언트의 사용자가 LDAP 디렉터리에서 연락처를 검색 및 추가하도록 허용하려면 Cisco XCP 디렉터리 서비스를 설정해야 합니다. 클러스터의 모든 노드에서 Cisco XCP 디렉터리 서비스를 설정합니다.

참고 타사 XMPP 클라이언트에 대한 LDAP 검색 설정 및 LDAP 서버를 구성하기 전에는 Cisco XCP 디렉터리 서비스를 설정하지 마십시오. Cisco XCP 디렉터리 서비스를 설정한 상태에서 타사 XMPP 클라이언트에 대한 LDAP 검색 설정 및 LDAP 서버를 구성하지 않으면 서비스가 시작된 후 다시 중지됩니다.

시작하기 전에

타사 XMPP 클라이언트에 대한 LDAP 검색 설정 및 LDAP 서버를 구성합니다.

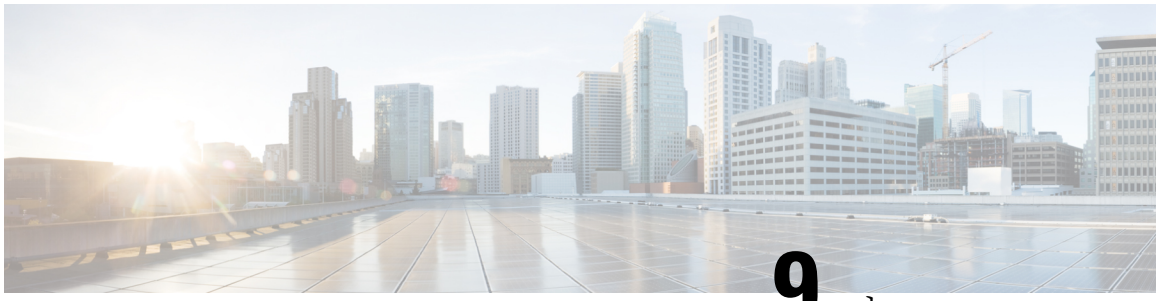
프로시저

단계 **1** **Cisco Unified IM and Presence** 서비스 가용성도구 > 서비스 활성화를 선택합니다.

단계 **2** [서버] 메뉴에서 IM and Presence 서비스 노드를 선택합니다.

단계 **3** **Cisco XCP** 디렉터리 서비스를 선택합니다.

단계 **4** 저장을 클릭합니다.



9 장

IM and Presence 서비스용 Cisco Unified Communications Manager 구성

통합 개요

이 섹션에서는 IM and Presence 서비스에 대한 구성을 완료하기 위해 Cisco Unified Communications Manager에서 완료해야 하는 작업에 대해 자세히 설명합니다.

Cisco Unified Communications Manager 통합 필수 조건

Cisco Unified Communications Manager와 통합하기 위해 IM and Presence 서비스를 구성하기 전에 Cisco Unified Communications Manager에서 다음 일반 구성 작업을 완료해야 합니다. Cisco Unified Communications Manager 구성 방법에 대한 자세한 내용은 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html에서 *Cisco Unified Communications Manager* 시스템 구성 설명서를 참조하십시오.

아래 표에는 IM and Presence 서비스 통합을 위한 필수 구성 작업이 나와 있습니다. 필드 및 해당 옵션에 대한 설명은 온라인 도움말을 참조하십시오.

표 *9: Cisco Unified Communications Manager*의 필수 구성

작업	설명
사용자 자격 증명 정책 수정	사용자를 위한 자격 증명 정책에서 만료 날짜를 설정하는 것이 좋습니다. 자격 증명 만료 날짜가 필요하지 않은 유일한 사용자 유형은 애플리케이션 사용자입니다. LDAP 서버를 사용하여 Cisco Unified Communications Manager에서 사용자를 인증하는 경우, Cisco Unified Communications Manager는 자격 증명 정책을 사용하지 않습니다. **Cisco Unified CM Administration** > 사용자 관리 > 사용자 설정 > 인증서 정책 기본값
전화기 디바이스를 구성하고, DN(디렉터리 번호)을 각 디바이스와 연결	전화기와 클라이언트의 상호 운용을 허용하려면 **CTI**의 디바이스 제어 허용을 활성화합니다. **Cisco Unified CM** 관리 > 디바이스 > 전화기
사용자를 구성하고, 디바이스를 각 사용자와 연결	사용자 ID 값이 각 사용자에 대해 고유한지 확인합니다. **Cisco Unified CM** 관리 > 사용자 관리 > 최종 사용자
사용자를 회선 표시와 연결	자세한 내용은 다음 내용을 참조하십시오. **Cisco Unified CM** 관리 > 디바이스 > 전화기
CTI 활성 사용자 그룹에 사용자 추가	사무실 전화기 제어를 활성화하는 경우 CTI 활성 사용자 그룹에 사용자를 추가해야 합니다. **Cisco Unified CM** 관리 > 사용자 관리 > 사용자 그룹
인증서 교환	Cisco Unified Communications Manager와 IM and Presence 서비스 간의 인증서 교환은 설치 프로세스 중에 자동으로 처리됩니다. 그러나 문제가 발생하여 인증서 교환을 수동으로 완료해야 하는 경우 Cisco Unified Communications Manager와 인증서 교환, 145 페이지의 내용을 참조하십시오.

참고 IM and Presence 서비스에 업로드하는 Cisco Unified Communications Manager Tomcat 인증서에 SAN 필드에 호스트 이름이 포함되어 있는 경우 이 모든 인증서는 IM and Presence 서비스에서 확인할 수 있어야 합니다. IM and Presence 서비스가 DNS를 통해 호스트 이름을 확인할 수 있어야 합니다. 그렇지 않으면 Cisco 동기화 에이전트 서비스가 시작되지 않습니다. 이는 Cisco Unified Communications Manager 서버의 노드 이름에 대한 호스트 이름, IP 주소 또는 FQDN 사용 여부와 상관없이 적용됩니다.

Cisco Unified Communications Manager에서 SIP 트렁크 구성

이러한 작업을 완료하여 Cisco Unified Communications Manager에 대한 SIP 트렁크 연결을 구성합니다.

프로시저

	명령 또는 동작	목적
단계 **1**	SIP 트렁크 보안 프로파일 구성, 100 페이지	Cisco Unified Communications Manager와 IM and Presence 서비스 간의 트렁크 연결을위한 SIP 트렁크 보안 프로파일을 구성합니다.
단계 **2**	IM and Presence 서비스용 SIP 트렁크 구성, 100 페이지	SIP 트렁크에 SIP 트렁크 보안 프로파일을 할당하고 Cisco Unified Communications Manager와 IM and Presence 서비스 간 트렁크 연결을 구성합니다.
단계 **3**	SRV 클러스터 이름 구성, 102 페이지	(선택 사항) Cisco Unified Communications Manager와 IM and Presence 서비스 간의 SIP 트렁크에서 DNS SRV를 사용하고 IM and Presence 기본 도메인이 아닌 다른 SRV 주소를 사용하는 경우에만 이 절차를 완료하십시오. 이 경우, **SRV** 클러스터 이름 서비스 파라미터를 구성합니다. 그렇지 않은 경우 이 작업을 생략할 수 있습니다.
단계 **4**	Presence 게이트웨이 구성, 103 페이지	IM and Presence 서비스에서 Cisco Unified Communications Manager를 프레즌스 게이트웨이로 할당하면 시스템이 프레즌스 정보를 교환할 수 있습니다.
단계 **5**	SIP 게시 트렁크 구성, 102 페이지	(선택 사항) IM and Presence에 대한 SIP 게시 트렁크를 구성하려면 이 절차를 사용하십시오. 이 설정을 활성화하면 Cisco 는 Cisco Unified Communications Manager에서 IM and Presence 서비스를 위해 Cisco Unified Communications Manager 사용이 허가된 사용자와 관련된 모든 회선 표시에 대해 전화기 프레즌스를 게시합니다.
단계 **6**	Cisco Unified Communications Manager에서 서비스 확인, 103 페이지	Cisco Unified Communications Manager에서 필수 서비스가 실행 중인지 확인합니다.

	명령 또는 동작	목적
단계 7	클러스터 외부의 Cisco Unified Communications Manager에 대해 전화기 프레즌스 구성, 104 페이지	IM and Presence 서비스의 TLS 피어 주체로 Cisco Unified Communications Manager를 구성합니다. IM and Presence 서비스 클러스터 외부에 있는 Cisco Unified Communications Manager에서 전화기 프레즌스를 허용하려는 경우 TLS가 필요합니다.

SIP 트렁크 보안 프로파일 구성

Cisco Unified Communications Manager에서 IM and Presence 서비스를 사용하여 트렁크 연결을위한 SIP 트렁크 보안 프로파일을 구성합니다.

프로시저

단계 1 **Cisco Unified CM** 관리 > 시스템 > 보안 > **SIP** 트렁크 보안 프로파일에서 찾기를 클릭합니다.

단계 2 비보안 **SIP** 트렁크 프로파일을 클릭합니다.

단계 3 복사를 클릭합니다.

단계 4 프로파일의 이름을 입력합니다. 예를 들어, `IMP-SIP-Trunk-Profile`.

단계 5 다음 설정을 완료하십시오.

- 디바이스 보안 모드 를 비보안으로 설정합니다.
- 수신 전송 유형을 **TCP+UDP**로 설정합니다.
- 발신 전송 유형을 **TCP**로 설정합니다.

단계 6 다음 확인란을 선택합니다.

- 프레즌스 가입 승인
- 대화 상자를 벗어난 **REFER** 승인
- 원하지 않는 통보 승인
- 대체 헤더 승인

단계 7 저장을 클릭합니다.

다음에 수행할 작업

IM and Presence 서비스용 SIP 트렁크 구성, 100 페이지

IM and Presence 서비스용 SIP 트렁크 구성

Cisco Unified Communications Manager와 IM and Presence 서비스 클러스터간에 SIP 트렁크 연결을 설정합니다.

시작하기 전에

SIP 트렁크 보안 프로파일 구성, 100 페이지

프로시저

단계 1 **Cisco Unified CM** 관리에서 디바이스 > 트렁크를 선택합니다.

단계 2 새로 추가를 클릭합니다.

단계 3 트렁크 유형 드롭다운 목록 상자에서 **SIP** 트렁크를 선택합니다.

단계 4 디바이스 프로토콜 드롭다운 목록 상자에서 **SIP**을 선택합니다.

단계 5 트렁크 서비스 유형 드롭다운 목록 상자에서 없음을 선택합니다.

단계 6 다음을 클릭합니다.

단계 7 디바이스 이름 필드에 트렁크 이름을 입력합니다. 예를 들어, `IMP-SIP-Trunk`.

단계 8 드롭다운 목록 상자에서 디바이스 풀을 선택합니다.

단계 9 **SIP** 정보 섹션에서 IM and Presence 클러스터에 대한 주소 정보를 입력하여 IM and Presence 서비스에 트렁크를 할당합니다.

- IM and Presence 서비스에 대해 DNS SRV 레코드를 사용하는 경우 대상 주소가 **SRV** 확인란을 선택하고 대상 주소 필드에 SRV를 입력합니다.
- 그렇지 않으면 대상 주소 필드에 IM and Presence 게시자 노드의 IP 주소 또는 FQDN을 입력합니다. **(+)** 버튼을 클릭하여 노드를 더 추가합니다. 최대 16개 노드를 입력할 수 있습니다.

a) 대상 주소 필드에 IM and Presence의 IP 주소, FQDN 또는 DNS SRV를 입력합니다.

b) 다중 노드 구축을 구성 중인 경우 대상 주소가 **SRV**를 선택합니다.

이 시나리오에서 Cisco Unified Communications Manager는 DNS SRV 레코드 쿼리를 수행하여 이름을 확인합니다(예: `_sip._tcp.hostname.tld_sip._tcp.hostname.tld`). 단일 노드 구축을 구성 중인 경우 이 확인란을 선택하지 않으면 Cisco Unified Communications Manager에서는 DNS A 레코드 쿼리를 수행하여 이름을 확인합니다(예: `hostname.tld`).

DNS SRV 레코드의 대상 주소로 IM and Presence 서비스 기본 도메인을 사용하는 것이 좋습니다.

참고 DNS SRV 레코드의 대상 주소로 원하는 도메인 값을 지정할 수 있습니다. 지정된 도메인에 사용자를 할당할 필요가 없습니다. IM and Presence 서비스 기본 도메인과 다른 도메인 값을 입력하는 경우, SRV 클러스터 이름(SRV Cluster Name)이라는 IM and Presence 서비스의 SIP 프록시 서비스 파라미터가 DNS SRV 레코드에서 지정한 도메인 값과 일치해야 합니다. 기본 도메인을 사용하는 경우 SRV 클러스터 이름(SRV Cluster Name) 파라미터를 변경할 필요가 없습니다.

두 시나리오 모두에서 Cisco Unified Communications SIP 트렁크 대상 주소는 DNS로 확인 가능해야 하며 IM and Presence 노드에 구성된 SRV 클러스터 이름(SRV Cluster Name)과 일치해야 합니다.

단계 10 대상 포트에 `5060`을 입력합니다.

단계 11 **SIP** 트렁크 보안 프로파일 드롭다운 목록 상자에서 이전 작업에서 만든 SIP 트렁크 보안 프로파일을 선택합니다.

단계 **12** **SIP** 프로파일 드롭다운 목록 상자에서 프로파일을 선택합니다(예: 표준 **SIP** 프로파일).

단계 **13** 저장을 클릭합니다.

다음에 수행할 작업

Cisco Unified Communications Manager와 IM and Presence 서비스 간의 SIP 트렁크에서 DNS SRV를 사용하고 IM and Presence 기본 도메인이 아닌 다른 SRV 주소를 사용하는 경우에만 SRV 클러스터 이름 구성, 102 페이지.

그렇지 않으면, SIP 게시 트렁크 구성, 102 페이지.

SRV 클러스터 이름 구성

Cisco Unified Communications Manager와 IM and Presence 서비스 간의 SIP 트렁크에서 DNS SRV를 사용하고 IM and Presence 기본 도메인이 아닌 다른 SRV 주소를 사용하는 경우에만 **SRV** 클러스터 이름 서비스 파라미터를 구성합니다. 그렇지 않은 경우 이 작업을 생략할 수 있습니다.

프로시저

단계 **1** Cisco Unified CM IM and Presence 관리에서 시스템 > 서비스 파라미터를 선택합니다.

단계 **2** 서버 드롭다운 메뉴에서 IM and Presence 게시자 노드를 선택하고 이동을 클릭합니다.

단계 **3** 서비스 드롭다운에서 **Cisco SIP Proxy** 서비스를 선택합니다.

단계 **4** **SRV** 클러스터 이름 필드에 SRV 주소를 입력합니다.

단계 **5** 저장을 클릭합니다.

SIP 게시 트렁크 구성

IM and Presence에 대한 SIP 게시 트렁크를 구성하려면 이 선택적 절차를 사용하십시오. 이 설정을 활성화하면 Cisco 는 Cisco Unified Communications Manager에서 IM and Presence 서비스를 위해 Cisco Unified Communications Manager 사용이 허가된 사용자와 관련된 모든 회선 표시에 대해 전화기 프레즌스를 게시합니다.

프로시저

단계 **1** Cisco Unified CM IM and Presence 관리에서 프레즌스 > 설정 > 표준 구성을 선택합니다.

단계 **2** **CUCM IM** 및 프레즌스 게시 트렁크 드롭다운 목록에서 Cisco Unified Communications Manager에서 IM and Presence 서비스에 대해 구성한 SIP 트렁크를 선택합니다.

단계 **3** 저장을 클릭합니다.

참고 이 새 설정을 저장하면 Cisco Unified Communications Manager의 **IM and Presence** 게시 트렁크 서비스 파라미터도 이 새 설정으로 업데이트됩니다.

다음에 수행할 작업

Cisco Unified Communications Manager에서 서비스 확인, 103 페이지

Presence 게이트웨이 구성

IM and Presence 서비스에서 이 절차를 사용하여 Cisco Unified Communications Manager를 프레즌스 게이트웨이로 할당합니다. 이 구성을 통해 Cisco Unified Communications Manager와 IM and Presence 서비스 간의 프레즌스 정보 교환이 가능합니다.

프로시저

단계 **1** **Cisco Unified CM IM and Presence** 관리프레즌스 > 게이트웨이에서

단계 **2** 새로 추가를 클릭합니다.

단계 **3** 프레즌스 게이트웨이 드롭다운 목록 상자에서 **CUCM**을 선택합니다.

단계 **4** 설명을 입력합니다.

단계 **5** 프레즌스 게이트웨이 필드에 다음 옵션 중 하나를 입력합니다.

- Cisco Unified Communications Manager 게시자 노드의 IP 주소 또는 FQDN
- Cisco Unified Communications Manager 가입자 노드로 확인되는 DNS SRV

단계 **6** 저장을 클릭합니다.

다음에 수행할 작업

SIP 게시 트렁크 구성, 102 페이지

Cisco Unified Communications Manager에서 서비스 확인

이 절차를 사용하여 Cisco Unified Communications Manager 노드에서 필수 서비스가 실행 중인지 확인합니다.

프로시저

단계 **1** Cisco Unified Serviceability에서 도구 > 제어 센터 - 기능 서비스를 선택합니다.

단계 **2** 서버 메뉴에서 Cisco Unified Communications Manager 클러스터 노드를 선택하고 이동을 클릭합니다.

단계 **3** 다음 서비스가 실행 중인지 확인합니다. 실행되지 않고 있는 경우 시작하십시오.

- Cisco CallManager
- Cisco TFTP
- Cisco CTIManager
- Cisco AXL Web 서비스(IM and Presence 및 Cisco Unified Communications Manager 간 데이터 동기화를 위해)

단계 **4** 위의 서비스 중 하나라도 실행 중이 아니면 서비스를 선택하고 시작을 클릭합니다.

클러스터 외부의 **Cisco Unified Communications Manager**에 대해 전화기 프레즌스 구성

IM and Presence 서비스 클러스터 외부에 있는 Cisco Unified Communications Manager에서 전화기 프레즌스를 허용할 수 있습니다. 그러나 IM and Presence 서비스가 클러스터 외부에 있는 Cisco Unified Communications Manager에서 SIP 게시를 수락하려면 Cisco Unified Communications Manager가 IM and Presence의 TLS에서 신뢰하는 피어로 나열되어야 합니다

프로시저

	명령 또는 동작	목적
단계 **1**	Cisco Unified Communications Manager를 TLS 피어로 추가, 104 페이지	IM and Presence 서비스의 TLS 피어로 Cisco Unified Communications Manager를 추가합니다.
단계 **2**	Unified Communications Manager에 대한 TLS 컨텍스트 구성, 105 페이지	Cisco Unified Communications Manager TLS 피어 추가

Cisco Unified Communications Manager를 TLS 피어로 추가

IM and Presence 서비스가 클러스터 외부에 있는 Cisco Unified Communications Manager에서 SIP 게시를 수락하려면 Cisco Unified Communications Manager가 IM and Presence 서비스의 TLS에서 신뢰하는 피어로 나열되어야 합니다

프로시저

단계 **1** **Cisco Unified CM IM and Presence** 관리 > 시스템 > 보안 > **TLS** 피어 주체에서 새로 추가를 클릭합니다.

단계 **2** 피어 주체 이름 필드에 외부 Cisco Unified Communications Manager의 IP 주소를 입력합니다.

단계 **3** 설명 필드에 노드의 이름을 입력합니다.

단계 **4** 저장을 클릭합니다.

다음에 수행할 작업

TLS 컨텍스트 구성, 166 페이지

Unified Communications Manager에 대한 TLS 컨텍스트 구성

다음 절차에 따라 이전 작업에서 구성한 Cisco Unified Communications Manager TLS 피어를 선택된 TLS 피어에 추가합니다.

시작하기 전에

Cisco Unified Communications Manager를 TLS 피어로 추가, 104 페이지

프로시저

단계 1 **Cisco Unified CM IM and Presence** 관리 > 시스템 > 보안 > **TLS** 컨텍스트 구성에서 찾기를 클릭합니다.

단계 2 **Default_Cisco_UP_SIP_Proxy_Peer_Auth_TLS_Context**를 클릭합니다.

단계 3 사용 가능한 TLS 피어 주체의 목록에서 Cisco Unified Communications Manager에 대해 자신이 구성한 TLS 피어 주체를 선택합니다.

단계 4 이 TLS 피어 주체를 선택한 TLS 피어 주체로 이동합니다.

단계 5 저장을 클릭합니다.

단계 6 모든 클러스터 노드에서 Cisco OAMAgent를 다시 시작합니다.

a) Cisco Unified IM and Presence 서비스 가용성에서 도구 > 제어 센터 - 네트워크 서비스를 선택합니다.
b) 서버 드롭다운 목록 상자에서 IM and Presence 서버를 선택하고 이동을 클릭합니다.
c) **IM and Presence** 서비스 아래에서 **Cisco OAMAgent**를 선택하고 다시 시작을 클릭합니다.
d) 모든 클러스터 노드에서 서비스를 다시 시작합니다.

단계 7 OAM 에이전트가 다시 시작된 후 Cisco Presence 엔진을 다시 시작합니다.

a) 도구 > 제어 센터 - 기능 서비스를 선택합니다.
b) 서버 드롭다운 목록 상자에서 IM and Presence 노드를 선택하고 이동을 클릭합니다.
c) **IM and Presence** 서비스 아래에서 **Cisco Presence** 엔진을 선택하고 다시 시작을 클릭합니다.
d) 모든 클러스터 노드에서 서비스를 다시 시작합니다.

다음에 수행할 작업

Cisco Unified Communications Manager에서 서비스 확인, 103 페이지

10 장

중앙 집중식 구축 구성

중앙 집중식 구축 개요

IM and Presence 중앙 집중식 구축을 사용하면 IM and Presence 구축과 전화 통신 구축을 별도의 클러스터에 구축할 수 있습니다. 중앙 IM and Presence 클러스터는 엔터프라이즈에 대한 IM and Presence 를 처리하고 원격 Cisco Unified Communications Manager 전화 통신 클러스터는 엔터프라이즈에 대한 음성 및 화상 통화를 처리합니다.

중앙 집중식 구축 옵션은 표준 구축과 비교할 때 다음과 같은 이점을 제공합니다.

- 중앙 집중식 구축 옵션은 IM and Presence 서비스 클러스터에 전화 통신 클러스터의 1x1 비율을 요구하지 않습니다. IM and Presence 구축과 전화 통신 구축을 각각 고유 한 필요성에 따라 개별적으로 확장할 수 있습니다.
- IM and Presence 서비스에는 전체 메시 토폴로지가 필요하지 않습니다.
- 전화 통신과 독립적 인 버전 - IM and Presence 중앙 클러스터는 Cisco Unified Communications Manager 전화 통신 클러스터와 다른 버전을 실행할 수 있습니다.
- 중앙 클러스터에서 IM and Presence 업그레이드 및 설정을 관리할 수 있습니다.
- 특히 많은 Cisco Unified Communications Manager 클러스터가 있는 대규모 구축을 위한 비용 절감 옵션
- 제 3자를 통한 간편한 XMPP 페더레이션.

- Microsoft Outlook과 일정 통합을 지원합니다. 구성 세부 정보는 *IM and Presence Service*를 위한 *Microsoft Outlook* 일정 통합 문서를 참조하십시오.

OVA 요구 사항

중앙 집중식 구축의 경우 최소 15,000 사용자 OVA를 갖는 25,000 사용자 IM and Presence를 권장합니다. 15,000 사용자 OVA는 25,000 사용자로 증가할 수 있습니다. 25K OVA 템플릿과 고가용성이 활성화된 6개 노드 클러스터를 통해 IM and Presence 서비스 중앙 구축은 최대 75,000개의 클라이언트를 지원합니다. 25K OVA가 있는 75K 사용자를 지원하려면 XCP 라우터의 기본 추적 수준을 정보에서 오류로 변경해야 합니다. 중앙 클러스터의 Unified Communications Manager 퍼블리셔 노드의 경우 다음 요구 사항이 적용됩니다.

- 25,000 IM and Presence OVA(최대 75,000 사용자)는 중앙 클러스터의 Unified Communications Manager 퍼블리셔 노드에 설치된 10,000 사용자 OVA를 사용하여 구축할 수 있습니다.
- 15,000 IM and Presence OVA(최대 45,000 사용자)는 중앙 클러스터의 Unified Communications Manager 퍼블리셔 노드에 설치된 7,500 사용자 OVA를 사용하여 구축할 수 있습니다.

참고 여러 디바이스 메시징을 활성화하려는 경우 각 사용자에게 여러 Jabber 클라이언트가 있을 수 있으므로 사용자 수 대신 클라이언트 수를 기준으로 구축을 측정합니다. 예를 들어, 25,000 사용자가 있고 각 사용자에게 Jabber 클라이언트가 두 개 있는 경우, 구축에 50,000 사용자의 용량이 필요합니다.

중앙 집중식 구축을 위한 인터클러스터링

인터클러스터링은 두 중앙 집중식 클러스터 간에 지원됩니다. 인터클러스터 피어는 25K(25K OVA) 및 15K(15K OVA) 디바이스가 있는 하나의 클러스터에서 테스트되었으며 성능 문제는 관찰되지 않았습니다.

중앙 집중식 구축 설정 및 표준**(**분산**)** 구축 비교

다음 표에서는 IM and Presence 서비스의 표준 구축과 달리 IM and Presence 중앙 집중식 클러스터 구축을 설정하는 데 따른 몇 가지 차이점에 대해 설명합니다.

설치 단계	표준 구축의 차이점
설치 단계	IM and Presence 중앙 구축의 설치 프로세스는 표준 구축의 설치 프로세스와 동일합니다. 그러나 중앙 배포에서는 IM and Presence 중앙 클러스터가 전화 통신 클러스터와 별도로 설치되며 별도의 하드웨어 서버에 있을 수 있습니다. 토폴로지를 계획하는 방법에 따라 IM and Presence 중앙 클러스터는 전화 통신 클러스터와는 별도의 실제 하드웨어에 설치될 수 있습니다. IM and Presence 중앙 클러스터의 경우 Cisco Unified Communications Manager를 설치 한 다음 IM and Presence 서비스를 동일한 서버에 설치해야 합니다. 그러나 IM and Presence 중앙 클러스터의 Cisco Unified Communications Manager 인스턴스는 데이터베이스 및 사용자 프로비저닝을 주로 대상으로 하며 음성 또는 화상 통화를 처리하지 않습니다.
구성 단계	IM and Presence 서비스 구축을 설치하려면 표준(분산) 구축과 비교하여 다음과 같은 추가 구성이 필요합니다. • 사용자는 전화 통신 클러스터와 IM and Presence 서비스 중앙 클러스터 모두에 동기화되어 두 데이터베이스에 모두 존재해야 합니다. • 전화 통신 클러스터에서는 최종 사용자가 IM and Presence에 대해 활성화되어 있지 않아야 합니다. • 전화 통신 클러스터에서 서비스 프로파일은 IM and Presence 서비스를 포함해하며 IM and Presence 중앙 클러스터를 가리켜야 합니다. • IM and Presence 중앙 클러스터에서 사용자는 IM and Presence 서비스에 대해 활성화되어 있어야 합니다. • IM and Presence 중앙 클러스터의 데이터베이스 게시자 노드에서 사용자의 원격 Cisco Unified Communications Manager 전화 통신 클러스터 피어를 추가합니다. 다음 구성은 IM and Presence 서비스의 표준 구축과 함께 사용되지만 중앙 구축에는 필요하지 않습니다. • 프레즌스 게이트웨이는 필요하지 않습니다. • SIP 게시 트렁크는 필요하지 않습니다. • IM and Presence 중앙 클러스터에는 서비스 프로파일이 필요하지 않습니다. 서비스 프로파일은 중앙 클러스터가 연결하는 전화 통신 클러스터에서 구성됩니다

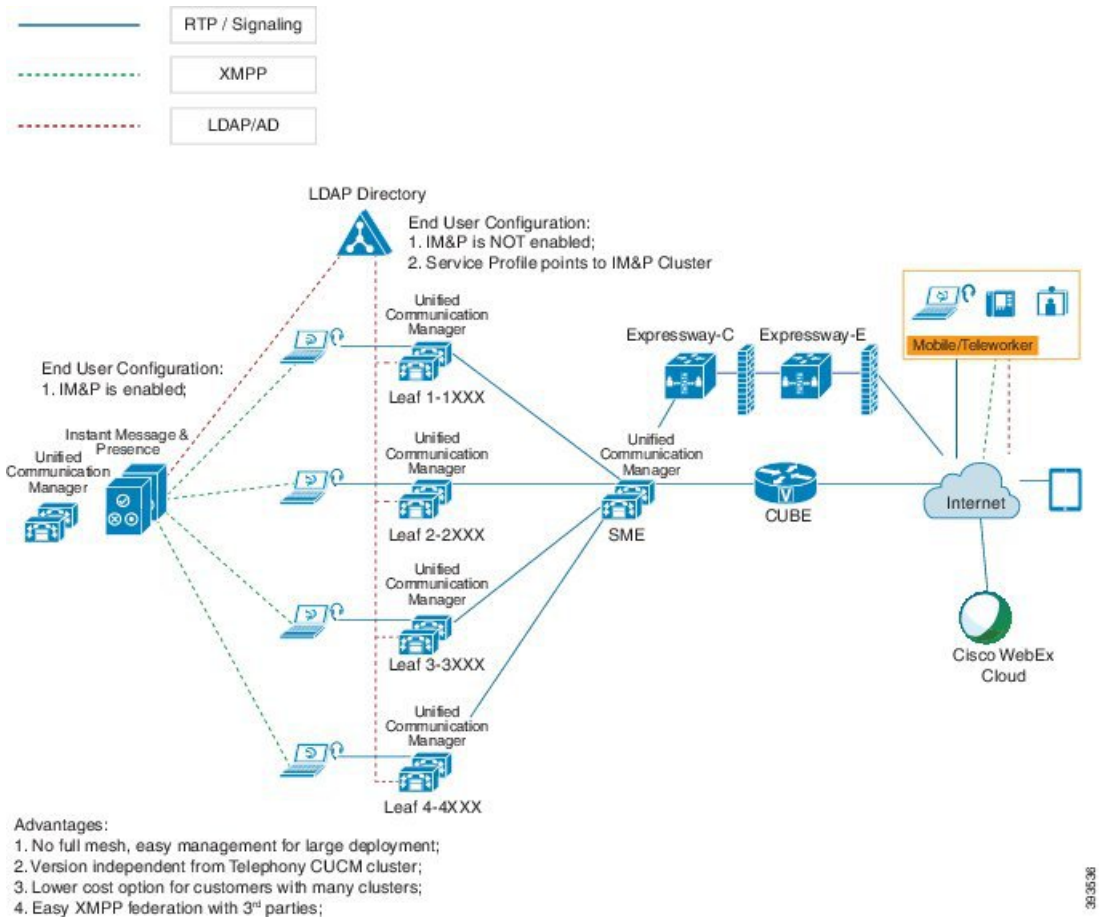
중앙 집중식 클러스터 구축 아키텍처

다음 다이어그램은 이 구축 옵션의 클러스터 아키텍처를 보여줍니다. Cisco Jabber 클라이언트는 음성 및 화상 통화를 위해 여러 Cisco Unified Communications Manager 클러스터에 연결합니다. 이 예에

서 Cisco Unified Communications Manager 전화 통신 클러스터는 Session Management Edition 구축의 리프 클러스터입니다. 리치 프레즌스의 경우 Cisco Jabber 클라이언트는 IM and Presence 서비스 중앙 클러스터에 연결합니다. IM and Presence 중앙 클러스터는 Jabber 클라이언트의 인스턴트 메시징 및 프레즌스를 관리합니다.

참고 IM and Presence 클러스터는 여전히 Cisco Unified Communications Manager에 대한 인스턴스를 포함합니다. 그러나 이 인스턴스는 데이터베이스 및 사용자 프로비저닝 같은 공유 기능을 처리하며, 전화 통신을 처리하지 않습니다.

그림 ***4: IM and Presence*** 서비스 중앙 집중식 클러스터 아키텍처



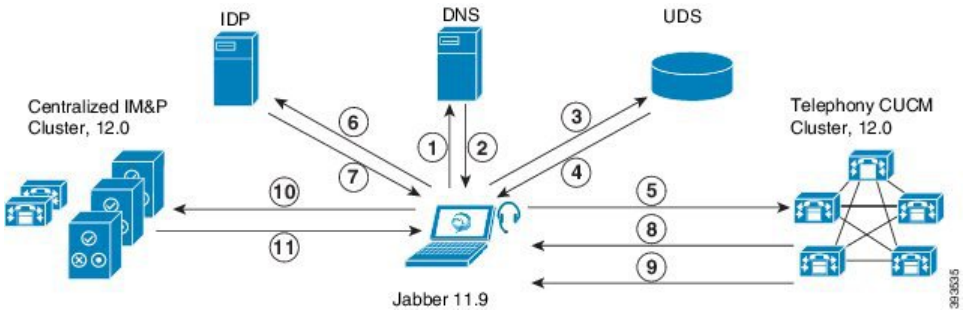
중앙 집중식 클러스터 사용 사례

전화 통신 및 IM and Presence 클러스터를 연결하기 위해 액세스 키 교환을 위한 새로운 시스템이 도입되었습니다. 이 다이어그램은 SSO 로그인에 대한 흐름을 보여줍니다.

- [1]-[2]: DNS를 쿼리하여 SRV 레코드를 가져옵니다.

- [3]-[4]: UDS를 쿼리하여 홈 Cisco Unified Communications Manager 클러스터를 가져옵니다.
- [5]-[8]: SAML SSO를 통해 Cisco Unified Communications Manager 클러스터에서 액세스 토큰 및 새로 고침 토큰을 가져옵니다.
- [9]: UC 서비스 프로파일을 읽습니다. 서비스 프로파일에는 IM and Presence 프로파일이 포함되어 있으며 IM and Presence 중앙 클러스터를 가리킵니다.
- [10]: 클라이언트는 SOAP 및 XMPP 인터페이스를 통해 동일한 액세스 토큰을 사용하여 IM and Presence 클러스터에 등록합니다.
- [11]: 토큰의 유효성이 검사되고 응답이 Jabber 클라이언트로 다시 전송됩니다.

그림 ***5: IM and Presence*** 서비스 중앙 집중식 클러스터 사용 사례



중앙 집중식 구축 필수 조건

다음 요구 사항이 IM and Presence 서비스 중앙 집중식 구축에 적용됩니다.

- IM and Presence 서비스 중앙 클러스터는 릴리스 11.5(1)SU4 이상을 실행 중이어야 합니다.
- IM and Presence 중앙 클러스터에서 실행되는 로컬 Cisco Unified Communications Manager 인스턴스는 IM and Presence 중앙 클러스터와 동일한 릴리스를 실행 중이어야 합니다.
- 원격 Cisco Unified Communications Manager 전화 통신 클러스터는 릴리스 10.5(2) 이상을 실행 중이어야 합니다.
- Cisco Jabber는 릴리스 11.9 이상을 실행 중이어야 합니다.
- 푸시 알림 인스턴트 메시징 지원을 위해 IM and Presence 서비스는 11.5(1)SU4를 실행 중이어야 합니다.
- iOS 디바이스에 대한 모든 인스턴트 메시지에서도 APN(Apple Push Notification 서비스) 솔루션을 사용할 수 있도록 중앙 집중식 IM and Presence 클러스터의 CUCM 퍼블리셔 노드에서 Cisco Cloud 온보딩을 활성화해야 합니다.

  또한 리프 CUCM 클러스터에서 Cisco Cloud 온보딩 옵션을 활성화해야 합니다. 그러면 일반적으로 이러한 클러스터에 등록하는 TCT 디바이스가 iOS용 Jabber 디바이스가 일시 중단되거나 제거되었을 때 APN을 통해 통화를 라우팅할 수 있습니다.

IM and Presence 서비스 클러스터에서 Cisco Cloud 온보딩을 활성화하는 방법에 대한 자세한 내용은 푸시 알림 구축 설명서의 *Cisco Cloud* 온보딩 활성화 장을 참조하십시오.

- Cisco Unified Communications Manager 기능은 IM and Presence 중앙 클러스터에서 실행되는 로컬 인스턴스가 아닌 원격 전화 통신 클러스터에서 실행 중인 Cisco Unified Communications Manager 버전을 기반으로 합니다. 예:
  - 푸시 알림 통화 지원을 위해 원격 전화 통신 클러스터는 11.5(1)SU4 이상을 실행 중이어야 합니다.
  - OAuth 새로 고침 로그인 지원을 위해 원격 Cisco Unified Communications Manager 전화 통신 클러스터는 11.5(1)SU4 이상을 실행 중이어야 합니다.
  - SAML SSO 지원을 위해 원격 전화 통신 클러스터는 11.5(1)SU4 이상을 실행 중이어야 합니다.
- **Cisco AXL** 웹 서비스 기능 서비스를 모든 클러스터에서 실행 중이어야 합니다. 이 서비스는 기본적으로 활성화되어 있지만 Cisco Unified Serviceability의 서비스 활성화 창에서 활성화되었는지 확인할 수 있습니다.
- 중앙 집중식 구축을 통해 Cisco Jabber가 리치 프레즌스를 처리합니다. 사용자의 전화기 프레즌스는 사용자가 Cisco Jabber에 로그인한 경우에만 표시됩니다.

DNS 요구 사항

IM and Presence 중앙 클러스터에는 Cisco Unified Communications Manager 전화 통신 클러스터의 게시자 노드를 가리키는 DNS SRV 레코드가 있어야 합니다. 전화 통신 구축에 ILS 네트워크가 포함되어 있는 경우 DNS SRV가 허브 클러스터를 가리켜야 합니다. 이 DNS SRV 레코드는 "_cisco-uds"를 참조해야 합니다.

SRV 레코드는 특정 서비스를 호스팅하는 컴퓨터를 식별하는 데 사용되는 DNS(Domain Name System) 리소스 레코드입니다. SRV 리소스 레코드는 Active Directory용 도메인 컨트롤러를 찾는 데 사용됩니다. 도메인 컨트롤러에 대한 SRV 로케이터 리소스 레코드를 확인하려면 다음 방법을 사용하십시오.

Active Directory는 SRV 레코드를 다음 폴더에 생성합니다. 여기서 도메인 이름은 설치된 도메인의 이름을 나타냅니다.

- Forward Lookup Zones/Domain_Name/_msdcs/dc/_sites/Default-First-Site-Name/_tcp
- Forward Lookup Zones/Domain_Name/_msdcs/dc/_tcp

이 위치에서 다음 서비스에 대해 SRV 레코드가 나타나야 합니다.

- _kerberos
- _ldap
- _cisco_uds: SRV 레코드를 나타냅니다.

아래에 언급 된 매개 변수는 SRV 레코드 생성 중에 설정되어야 합니다.

- 서비스: _cisco_uds

- 프로토콜 : _tcp
- 가중치: 0부터 시작(0이 우선 순위가 가장 높음)
- 포트 번호: 8443
- 호스트: 서버의 fqdn 이름

Jabber 클라이언트를 실행하는 컴퓨터의 DNS SRV 레코드의 예는 다음과 같습니다.

```
nslookup -type=all _cisco-uds._tcp.dcloud.example.com
Server: ad1.dcloud.example.com
Address: x.x.x.x
_cisco-uds._tcp.dcloud.example.com SRV service location:
priority = 10
weight = 10
port = 8443
svr hostname = cucm2.dcloud.example.com
cucm2.dcloud.example.com internet address = x.x.x.y
```

중앙 집중식 구축 구성 작업 흐름

중앙 집중식 구축 옵션을 사용하도록 새 IM and Presence 서비스 구축을 구성하려면 이 작업을 완료하십시오.

참고 새로운 IM and Presence 서비스 구축에만 이 작업 흐름을 사용하십시오.

표 ***10:*** 중앙 집중식 클러스터 구성 작업 흐름

	IM and Presence 중앙 클러스터	원격 전화 통신 클러스터	목적
1단계	기능 그룹 템플릿을 통한 IM and Presence 활성화, 115 페이지		IM and Presence 중앙 클러스터에서 IM and Presence 서비스를 활성화하는 템플릿을 구성합니다.
단계 **2**	IM and Presence 중앙 클러스터에서 LDAP 동기화 완료, 115 페이지		LDAP 동기화를 완료하여 IM and Presence 중앙 클러스터의 LDAP 동기화된 사용자에게 설정을 전파합니다.
3단계	벌크 관리자를 통해 IM and Presence에 대해 사용자 활성화, 116 페이지		(선택 사항) 이미 LDAP 동기화를 완료한 경우 벌크 관리를 사용하여 사용자에 대한 IM and Presence를 활성화합니다.

	IM and Presence 중앙 클러스터	원격 전화 통신 클러스터	목적
4단계	원격 전화 통신 클러스터 추가, 117 페이지		원격 전화 통신 클러스터를 IM and Presence 중앙 클러스터에 추가합니다.
단계 **5**		IM and Presence UC 서비스 구성, 118 페이지	전화 통신 클러스터에서 IM and Presence 중앙 클러스터를 가리키는 UC 서비스를 추가합니다.
단계 **6**		IM and Presence의 서비스 프로파일 만들기, 119 페이지	서비스 프로파일에 IM and Presence UC 서비스를 추가합니다. Cisco Jabber 클라이언트는 이 프로파일을 사용하여 IM and Presence 중앙 클러스터를 찾습니다.
7단계		전화 통신 클러스터에서 프레즌스 사용자 비활성화, 119 페이지	전화 통신 클러스터에서 IM and Presence 중앙 클러스터를 가리키도록 프레즌스 사용자 설정을 편집합니다.
8단계		OAuth 새로 고침 로그인 구성, 121 페이지	전화 통신 클러스터에서 OAuth를 구성하면 중앙 클러스터에 대해 기능이 활성화됩니다.
9단계		ILS 네트워크 구성, 121 페이지	둘 이상의 전화 통신 클러스터가 있는 경우 ILS를 구성해야 합니다.
단계 **10**		모바일 및 원격 액세스 제한	중앙 집중식 배포의 경우 모바일 및 원격 액세스를 구성합니다.

향후 작업

- 중앙 클러스터를 클러스터 간 네트워크의 일부로 다른 IM and Presence 클러스터에 연결하려면 인터클러스터 피어링을 구성합니다.
- IM and Presence 관리자 콘솔에서 중앙 집중식 구축에 대한 새 항목을 만들 경우 Cisco XCP 인증 서비스를 다시 시작해야 합니다.

기능 그룹 템플릿을 통한 IM and Presence 활성화

중앙 클러스터에 대한 IM and Presence 설정을 사용하여 기능 그룹 템플릿을 구성하려면 이 절차를 사용하십시오. 기능 그룹 템플릿을 LDAP 디렉터리 구성에 추가하여 동기화된 사용자에 대해 IM and Presence를 구성할 수 있습니다.

참고 초기 동기화가 아직 수행되지 않은 LDAP 디렉터리 구성에만 기능 그룹 템플릿을 적용할 수 있습니다. 중앙 클러스터에서 LDAP 구성을 동기화하면 Cisco Unified Communications Manager의 LDAP 구성에 편집을 적용할 수 없습니다. 이미 디렉터리를 동기화한 경우 벌크 관리를 사용하여 사용자에 대한 IM and Presence를 구성해야 합니다. 자세한 내용은 벌크 관리자를 통해 IM and Presence에 대해 사용자 활성화, 116 페이지를 참조하십시오.

프로시저

단계 **1** IM and Presence 중앙 집중식 클러스터의 Cisco Unified CM 관리 인터페이스에 로그인합니다. 이 서버에는 전화 통신이 구성되어 있지 않아야 합니다.

단계 **2** 사용자 관리 > 사용자 전화기/추가 > 기능 그룹 템플릿을 선택합니다.

단계 **3** 다음 중 하나를 수행합니다.

- 찾기를 클릭하고 기존 템플릿을 선택합니다.
- 새로 추가를 클릭하여 새 템플릿을 만듭니다.

단계 **4** 다음 두 확인란을 모두 선택합니다.

- 홈 클러스터
- **Unified CM IM and Presence**에 대한 사용자 활성화

단계 **5** 기능 그룹 템플릿 구성 창에서 나머지 필드를 완성합니다. 필드 및 해당 설정에 대한 도움이 필요한 경우 온라인 도움말을 참조하십시오.

단계 **6** 저장을 클릭합니다.

다음에 수행할 작업

설정을 사용자에게 전파하려면 초기 동기화가 아직 수행되지 않은 LDAP 디렉터리 구성에 기능 그룹 템플릿을 추가한 다음 초기 동기화를 완료해야 합니다.

IM and Presence 중앙 클러스터에서 LDAP 동기화 완료, 115 페이지

IM and Presence 중앙 클러스터에서 LDAP 동기화 완료

IM and Presence 서비스 중앙 클러스터에서 LDAP 동기화를 완료하여 기능 그룹 템플릿을 통해 IM and Presence 서비스로 사용자를 구성하십시오.

참고 초기 동기화가 발생한 후에는 LDAP 동기화 구성에 편집을 적용할 수 없습니다. 초기 동기화가 이미 발생한 경우 대신 벌크 관리를 사용합니다. LDAP 디렉터리 동기화를 설정하는 방법에 대한 추가 정보는 *Cisco Unified Communications Manager* 시스템 구성 설명서의 "최종 사용자 구성" 부분을 참조하십시오.

시작하기 전에

기능 그룹 템플릿을 통한 IM and Presence 활성화, 115 페이지

프로시저

단계 **1** IM and Presence 중앙 집중식 클러스터의 Cisco Unified CM 관리 인터페이스에 로그인합니다. 이 서버에는 전화 통신이 구성되어 있지 않아야 합니다.

단계 **2** 시스템 > **LDAP** > **LDAP** 디렉터리를 선택합니다.

단계 **3** 다음 중 하나를 수행합니다.

a) 찾기를 클릭하고 기존 LDAP 디렉터리 동기화를 선택합니다.

b) 새로 추가를 클릭하여 새 LDAP 디렉터리를 만듭니다.

단계 **4** 기능 그룹 템플릿 드롭 다운 목록 상자에서 이전 작업에서 만든 IM and Presence 기능 그룹 템플릿을 선택합니다.

단계 **5** **LDAP** 디렉터리 창에서 나머지 필드를 완료합니다. 필드 및 해당 설정에 대한 도움이 필요한 경우 온라인 도움말을 참조하십시오.

단계 **6** 저장을 클릭합니다.

단계 **7** 전체 동기화 수행을 클릭합니다.

Cisco Unified Communications Manager는 데이터베이스를 외부 LDAP 디렉터리와 동기화합니다. 최종 사용자는 IM and Presence 서비스로 구성됩니다.

다음에 수행할 작업

원격 전화 통신 클러스터 추가, 117 페이지

벌크 관리자를 통해 **IM and Presence**에 대해 사용자 활성화

사용자를 이미 중앙 클러스터에 동기화하고 해당 사용자가 IM and Presence 서비스를 활성화하지 않은 경우 벌크 관리의 사용자 업데이트 기능을 사용하여 IM and Presence 서비스에 대해 해당 사용자를 활성화합니다.

참고 또한 벌크 관리의 사용자 가져오기 또는 사용자 삽입 기능을 사용하여 CSV 파일을 통해 새 사용자를 가져올 수 있습니다. 절차는 *Cisco Unified Communications Manager* 벌크 관리 설명서를 참조하십시오. 가져온 사용자에게 아래 옵션이 선택되어 있는지 확인합니다.

- 홈 클러스터
- Unified CM IM and Presence에 대한 사용자 활성화

프로시저

단계 **1** Cisco Unified CM 관리에서 벌크 관리 > 사용자 > 사용자 업데이트 > 쿼리를 선택합니다.

단계 **2** 필터에서 홈 클러스터가 활성화됨을 선택하고 찾기를 클릭합니다. 이 창에는 자신의 홈 클러스터인 모든 최종 사용자가 표시됩니다.

단계 **3** 다음을 클릭합니다.
사용자 업데이트 구성 창에서 맨 왼쪽의 확인란은 이 쿼리로 이 설정을 편집할지 여부를 나타냅니다. 왼쪽 확인란을 선택하지 않으면 쿼리가 해당 필드를 업데이트하지 않습니다. 오른쪽 필드는 이 필드에 대한 새로운 설정을 나타냅니다. 두 확인란이 나타나는 경우 왼쪽의 확인란을 선택하여 필드를 업데이트하고 오른쪽 확인란에서 새 설정을 입력해야 합니다.

단계 **4** 서비스 설정에서 다음 각 필드의 왼쪽 확인란을 선택하여 이러한 필드를 업데이트할 것을 나타낸 후 다음과 같이 인접한 설정을 편집합니다.

- 홈 클러스터 - 이 클러스터를 홈 클러스터로 사용하려면 오른쪽 확인란을 선택합니다.
- **Unified CM IM and Presence**에 대한 사용자 활성화 - 오른쪽 확인란을 선택합니다. 이 설정을 사용하면 중앙 클러스터를 이러한 사용자의 IM and Presence 서비스 공급자로 사용할 수 있습니다.

단계 **5** 업데이트하려는 나머지 필드를 완성합니다. 필드 및 해당 설정에 대한 도움이 필요한 경우 온라인 도움말을 참조하십시오.

단계 **6** 작업 정보 아래에서 즉시 실행을 선택합니다.

단계 **7** 제출을 클릭합니다.

원격 전화 통신 클러스터 추가

이 절차를 사용하여 원격 전화 통신 클러스터를 중앙 집중식 IM and Presence 서비스 클러스터에 추가합니다.

참고 전화 통신 클러스터가 둘 이상인 경우 ILS를 구축해야 합니다. 이 경우 IM and Presence 중앙 클러스터가 연결되는 전화 통신 클러스터는 허브 클러스터여야 합니다.

프로시저

단계 **1** IM and Presence 서비스 중앙 집중식 클러스터에서 데이터베이스 게시자 노드에 로그인합니다.

단계 **2** Cisco Unified CM IM and Presence 관리에서 시스템 > 중앙 집중식 구축을 선택합니다.

단계 **3** 현재 원격 Cisco Unified Communications Manager 클러스터 목록을 보려면 찾기를 클릭합니다. 클러스터의 세부 사항을 편집하려면 클러스터를 선택하고 선택 항목 수정을 클릭합니다.

단계 **4** 새로 추가를 클릭하여 새 원격 Cisco Cisco Unified Communications Manager 클러스터를 추가합니다.

단계 **5** 추가할 각 전화 통신 클러스터에 대해 다음 필드를 완료합니다.

- 피어 주소 - 원격 Cisco Unified Communications Manager 전화 통신 클러스터 게시자 노드의 FQDN, 호스트 이름, IPv4 주소 또는 IPv6 주소입니다.
- **AXL** 사용자 이름 - 원격 클러스터에 있는 AXL 계정에 대한 로그인 사용자 이름입니다.
- **AXL** 암호 - 원격 클러스터에 있는 AXL 계정에 대한 암호입니다.

단계 **6** 저장 및 동기화 버튼을 클릭합니다.
IM and Presence 서비스는 키를 원격 클러스터와 동기화합니다.

다음에 수행할 작업

IM and Presence UC 서비스 구성, 118 페이지

IM and Presence UC 서비스 구성

원격 전화 통신 클러스터에서 이 절차를 사용하여 IM and Presence 서비스 중앙 클러스터를 가리키는 UC 서비스를 구성합니다. 전화 통신 클러스터의 사용자는 IM and Presence 중앙 클러스터에서 IM and Presence 서비스를 받게 됩니다.

프로시저

단계 **1** 전화 통신 클러스터의 Cisco Unified CM 관리 인터페이스에 로그인합니다.

단계 **2** 사용자 관리 > 사용자 설정 > **UC** 서비스를 선택합니다.

단계 **3** 다음 중 하나를 수행합니다.

a) 찾기를 클릭하고 편집할 기존 서비스를 선택합니다.
b) 새로 추가를 클릭하여 새 UC 서비스를 만듭니다.

단계 **4** **UC** 서비스 유형 드롭다운 목록에서 **IM and Presence**를 선택하고 다음을 클릭합니다.

단계 **5** 제품 유형 드롭다운 목록 상자에서 **IM and Presence** 서비스를 선택합니다.

단계 **6** 클러스터의 고유한 이름을 입력합니다. 호스트 이름일 필요는 없습니다.

단계 **7** 호스트 이름/**IP** 주소에서 IM and Presence 중앙 클러스터 데이터베이스 게시자 노드의 호스트 이름, IPv4 주소 또는 IPv6 주소를 입력합니다.

단계 **8** 저장을 클릭합니다.

단계 **9** 권장 사항. 호스트 이름/**IP** 주소 필드가 중앙 클러스터의 구독자 노드를 가리키는 두 번째 IM and Presence 서비스를 만들려면 이 절차를 반복하십시오.

다음에 수행할 작업

IM and Presence의 서비스 프로파일 만들기, 119 페이지.

IM and Presence의 서비스 프로파일 만들기

원격 전화 통신 클러스터에서 이 절차를 사용하여 IM and Presence 중앙 클러스터를 가리키는 서비스 프로파일을 만듭니다. 전화 통신 클러스터의 사용자는 이 서비스 프로파일을 사용하여 중앙 클러스터에서 IM and Presence 서비스를 받게 됩니다.

프로시저

단계 **1** [Cisco Unified CM 관리]에서 사용자 관리 > 사용자 설정 > 서비스 프로파일을 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

a) 찾기를 클릭하고 편집할 기존 서비스 프로파일을 선택합니다.
b) 새로 추가를 클릭하여 새 서비스 프로파일을 만듭니다.

단계 **3** **IM and Presence** 프로파일 섹션에서 이전 작업에서 구성한 IM and Presence 서비스를 구성합니다.

a) 기본 드롭다운에서 데이터베이스 게시자 노드 서비스를 선택합니다.
b) 보조 드롭다운에서 가입자 노드 서비스를 선택합니다.

단계 **4** 저장을 클릭합니다.

다음에 수행할 작업

전화 통신 클러스터에서 프레즌스 사용자 비활성화, 119 페이지

전화 통신 클러스터에서 프레즌스 사용자 비활성화

전화 통신 구축에서 이미 LDAP 동기화를 완료한 경우 벌크 관리 도구를 사용하여 IM and Presence 사용자에 대한 전화 통신 클러스터의 사용자 설정을 편집합니다. 이 구성은 프레즌스 사용자가 IM and Presence 서비스의 중앙 집중식 클러스터를 가리 키도록 합니다.

참고 이 절차에서는 전화 통신 클러스터에서 LDAP 동기화를 이미 완료했다고 가정합니다. 그러나 아직 초기 LDAP 동기화를 완료하지 않은 경우 프레즌스 사용자의 중앙 구축 설정을 초기 동기화에 추가할 수 있습니다. 이 경우 전화 통신 클러스터에서 다음을 수행합니다.

- 방금 설정한 서비스 프로파일이 포함된 기능 그룹 템플릿을 구성합니다. 홈 클러스터 옵션을 선택하고 **Unified CM IM and Presence**에 대한 사용자 활성화 옵션을 선택 취소합니다.
- **LDAP** 디렉터리 구성에서 기능 그룹 템플릿을 LDAP 디렉터리 동기화에 추가합니다.
- 초기 동기화를 완료합니다.

기능 그룹 템플릿 및 LDAP 디렉터리 구성에 대한 자세한 내용은 *Cisco Unified Communications Manager* 시스템 구성 설명서의 "최종 사용자 구성" 부분을 참조하십시오.

프로시저

단계 **1** Cisco Unified CM 관리에서 쿼리 > 벌크 관리 > 사용자 > 사용자 업데이트 > 쿼리를 선택합니다.

단계 **2** 필터에서 홈 클러스터가 활성화됨을 선택하고 찾기를 클릭합니다. 이 창에는 자신의 홈 클러스터인 모든 최종 사용자가 표시됩니다.

단계 **3** 다음을 클릭합니다.
사용자 업데이트 구성 창에서 맨 왼쪽의 확인란은 이 쿼리로 이 설정을 편집할지 여부를 나타냅니다. 왼쪽 확인란을 선택하지 않으면 쿼리가 해당 필드를 업데이트하지 않습니다. 오른쪽 필드는 이 필드에 대한 새로운 설정을 나타냅니다. 두 확인란이 나타나는 경우 왼쪽의 확인란을 선택하여 필드를 업데이트하고 오른쪽 확인란에서 새 설정을 입력해야 합니다.

단계 **4** 서비스 설정에서 다음 각 필드의 맨 왼쪽 확인란을 선택하여 이러한 필드를 업데이트할 것을 나타낸 후 다음과 같이 인접한 설정을 편집합니다.

- 홈 클러스터 - 전화 통신 클러스터를 홈 클러스터로 사용하려면 오른쪽 확인란을 선택합니다.
- **Unified CM IM and Presence**에 대한 사용자 활성화 - 오른쪽 확인란을 선택하지 않습니다. 이 설정은 전화 통신 클러스터를 IM and Presence의 공급자로 사용하지 않도록 설정합니다.
- **UC** 서비스 프로파일 - 드롭다운에서 이전 작업에서 구성한 서비스 프로파일을 선택합니다. 이 설정은 IM and Presence 서비스의 공급자가 될 IM and Presence 중앙 클러스터를 사용자에게 알려줍니다.

참고 Expressway 모바일 및 원격 액세스 구성의 경우 https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-and-configuration-guides-list.html 에서 *Cisco Expressway*를 통한 모바일 및 원격 액세스 구축 설명서를 참조하십시오.

단계 **5** 나머지 필드를 완료합니다. 필드 및 해당 설정에 대한 도움이 필요한 경우 온라인 도움말을 참조하십시오.

단계 **6** 작업 정보 아래에서 즉시 실행을 선택합니다.

단계 **7** 제출을 클릭합니다.

다음에 수행할 작업

OAuth 새로 고침 로그인 구성 , 121 페이지

OAuth 새로 고침 로그인 구성

전화 통신 클러스터에서 OAuth 새로 고침 로그인을 활성화합니다. 이렇게 하면 중앙 클러스터에서도 이 기능이 활성화됩니다.

프로시저

단계 **1** 전화 통신 클러스터의 Cisco Unified CM 관리에 로그인합니다.

단계 **2** 시스템 > 엔터프라이즈 파라미터를 선택합니다.

단계 **3** **SSO** 및 **OAuth** 구성 아래에서 새로 고침 로그인을 사용한 **OAuth** 엔터프라이즈 파라미터를 활성화됨으로 설정합니다.

단계 **4** 파라미터 설정을 편집한 경우 저장을 클릭합니다.

참고 OAuth 키가 다시 생성되면 모든 IM and Presence 노드에서 Cisco XCP Authentication Service를 다시 시작해야만 Jabber OAuth 로그인이 됩니다.

ILS 네트워크 구성

둘 이상의 원격 전화 통신 클러스터가 있는 IM and Presence 중앙 집중식 클러스터의 경우 ILS(Intercluster Lookup Service)를 사용하여 IM and Presence 중앙 클러스터에 대한 원격 전화 통신 클러스터를 프로비전할 수 있습니다. ILS는 네트워크를 모니터링하고 새로운 클러스터 또는 주소 변경과 같은 네트워크 변경 사항을 전체 네트워크에 전파합니다.

참고 이 작업 흐름은 IM and Presence 중앙 집중식 클러스터 구축에 대한 ILS 요구 사항에 중점을 둡니다. 전역 다이얼 플랜 복제 또는 URI 다이얼링 구성 같은 전화 통신과 관련된 추가 ILS 구성에 대해서는 *Cisco Unified Communications Manager* 시스템 구성 설명서의 "다이얼 플랜 구성" 섹션을 참조하십시오.

시작하기 전에

ILS를 구축하는 경우 다음을 수행했는지 확인하십시오.

- ILS 네트워크 토폴로지를 계획합니다. 어느 전화 통신 클러스터가 허브 및 스포크인지 알고 있어야 합니다.
- IM and Presence 중앙 클러스터가 연결되는 전화 통신 클러스터는 허브 클러스터여야 합니다.
- 허브 클러스터의 게시자 노드를 가리키는 DNS SRV 레코드를 구성해야 합니다.

ILS 네트워크 설계에 대한 자세한 내용은 http://www.cisco.com/c/en/us/support/unified-communications/unified-presence/products-implementation-design-guides-list.html에 있는 *Cisco Collaboration System* 솔루션 참조 네트워크 설계를 참조하십시오.

프로시저

	명령 또는 동작	목적
단계 **1**	ILS에 대한 클러스터 ID 구성, 122 페이지	각 전화 통신 클러스터에 대해 고유한 클러스터 ID를 설정합니다. 클러스터 ID가 `StandAloneCluster`(기본 설정)로 설정된 동안 ILS는 작동하지 않습니다.
단계 **2**	전화 통신 클러스터에서 ILS 활성화, 122 페이지	ILS 네트워크에서 각 전화 통신 클러스터의 게시자 노드에서 ILS를 구성하고 활성화합니다.
단계 **3**	ILS 네트워크가 실행 중인지 확인, 124 페이지	ILS가 작동 중이면 전화 통신 클러스터의 **ILS** 구성 창에서 "최신" 동기화 상태인모든 원격 클러스터를 볼 수 있습니다.

ILS에 대한 클러스터 ID 구성

ILS 네트워크 내의 각 클러스터에는 고유한 클러스터 ID가 있어야 합니다. 전화 통신 클러스터에 고유한 클러스터 ID를 부여하려면 이 절차를 사용하십시오.

프로시저

단계 **1** 게시자 노드에서 Cisco Unified CM 관리에 로그인합니다.

단계 **2** 시스템 > 엔터프라이즈 파라미터를 선택합니다.

단계 **3** 클러스터 **ID** 파라미터의 값을 `StandAloneCluster`에서 사용자가 설정한 고유한 값으로 변경합니다. 클러스터 ID가 `StandAloneCluster`인 동안 ILS는 작동하지 않습니다.

단계 **4** 저장을 클릭합니다.

단계 **5** ILS 네트워크에 참가시키려는 각 전화 통신 클러스터의 게시자 노드에서 이 절차를 반복합니다. 각 클러스터에는 고유 ID가 있어야 합니다.

다음에 수행할 작업

전화 통신 클러스터에서 ILS 활성화, 122 페이지

전화 통신 클러스터에서 ILS 활성화

이 절차를 사용하여 Cisco Unified Communications Manager 전화 통신 클러스터에서 ILS를 구성하고 활성화합니다.

참고
- 스포크 클러스터를 구성하기 전에 허브 클러스터를 구성합니다.
- 필드 및 해당 설정에 대한 도움이 필요한 경우 온라인 도움말을 참조하십시오.

시작하기 전에

ILS에 대한 클러스터 ID 구성, 122 페이지

프로시저

단계 **1** 전화 통신 클러스터의 게시자 노드에서 Cisco Unified CM 관리에 로그인합니다.

단계 **2** 고급 기능 > **ILS** 구성을 선택합니다.

단계 **3** 역할 드롭다운 목록 상자에서 설정 중인 클러스터의 유형에 따라 허브 클러스터 또는 스포크 클러스터를 선택합니다.

단계 **4** 원격 클러스터와 전역 다이얼 플랜 복제 데이터 교환 확인란을 선택합니다.

단계 **5** **ILS** 인증 세부 정보를 구성합니다.

a) 다양한 클러스터 간에 TLS 인증을 사용하려면 **TLS** 인증서 사용 확인란을 선택합니다.

참고 TLS를 사용하는 경우 클러스터의 노드간에 CA 서명 인증서를 교환해야 합니다.

b) TLS 사용 여부에 관계없이 암호 인증을 사용하려면 암호 사용 확인란을 선택하고 암호 세부 정보를 입력합니다.

단계 **6** 저장을 클릭합니다.

단계 **7** **ILS** 클러스터 등록 팝업에서 등록 세부 정보를 구성합니다.

- 등록 서버 텍스트 상자에 이 클러스터를 연결할 허브 클러스터의 게시자 노드 IP 주소 또는 FQDN을 입력합니다. 네트워크의 첫 번째 허브 클러스터인 경우 필드를 비워 둘 수 있습니다.
- 이 클러스터의 게시자에서 클러스터 간 조회 서비스를 활성화합니다**.** 확인란이 선택되었는지 확인합니다.

단계 **8** 확인을 클릭합니다.

단계 **9** ILS 네트워크에 추가하려는 각 전화 통신 클러스터의 게시자 노드에서 이 절차를 반복합니다. 구성한 동기화 값에 따라 클러스터 정보가 네트워크 전체에 전파되는 동안 지연이 발생할 수 있습니다.

클러스터간에 TLS(전송 계층 보안) 인증을 사용하도록 선택한 경우 ILS 네트워크의 각 클러스터 퍼블리셔 노드간에 Tomcat 인증서를 교환하십시오. [Cisco Unified Operating System 관리]에서 벌크 인증서 관리 기능을 사용하여 다음을 수행합니다.

- 각 클러스터의 게시자 노드에서 중앙 위치로 인증서 내보내기
- ILS 네트워크에서 내보낸 인증서 통합

- 네트워크의 각 클러스터에 있는 게시자 노드로 인증서 가져오기

자세한 내용은 *Cisco Unified Communications Manager* 관리 설명서의 "인증서 관리" 장을 참조하십시오.

다음에 수행할 작업

ILS가 실행되고 인증서를 교환한 후에(필요한 경우), ILS 네트워크가 실행 중인지 확인, 124 페이지

ILS 네트워크가 실행 중인지 확인

이 절차를 사용하여 ILS 네트워크가 실행 중인지 확인하십시오.

프로시저

단계 **1** 전화 통신 클러스터의 게시자 노드에 로그인합니다.

단계 **2** Cisco Unified CM 관리에서 고급 기능 > **ILS** 구성을 선택합니다.

단계 **3** **ILS** 클러스터 및 전역 다이얼 플랜 가져온 카탈로그 섹션을 선택합니다. ILS 네트워크 토폴로지가 나타나야 합니다.

모바일 및 원격 액세스 제한

Cisco Unified Communications 모바일 및 원격 액세스는 Cisco Collaboration Edge Architecture의 핵심 부분입니다. Cisco Jabber와 같은 엔드포인트가 엔터프라이즈 네트워크에 없는 경우, 해당 엔드포인트에서 Cisco Unified Communications Manager에서 제공하는 등록, 통화 제어, 제공, 메시징 및 프레즌스 서비스를 사용할 수 있습니다. Expressway에서 Unified CM 등록을 위한 보안 방화벽 통과 및 회선 측 지원을 제공합니다.

전체 솔루션은 다음과 같은 기능을 제공합니다.

1. 오프-프레미스 액세스 : Jabber 및 EX/MX/SX 시리즈 클라이언트에 대해 네트워크 외부의 일관된 경험.
2. 보안 : 비즈니스 간 통신 보호.
3. 클라우드 서비스 : 풍부한 Webex 통합 및 서비스 공급자 오퍼링을 제공하는 엔터프라이즈급 유연성 및 확장 가능한 솔루션.
4. 게이트웨이 및 상호 운용성 서비스 : 미디어 및 신호 정규화, 비표준 엔드 포인트 지원.

컨피그레이션

Expressway-C의 모든 전화 통신 리프 클러스터에서 모바일 및 원격 액세스를 구성하려면 구성 → **Unified Communications** → **Unified CM** 서버를 선택합니다.

Expressway-C의 중앙 집중식 IM&P 노드 클러스터에서 모바일 및 원격 액세스를 구성하려면 구성 → **Unified Communications** → **IM and Presence** 서비스 노드를 선택합니다.

Expressway-C에서 "모바일 및 원격 액세스"를 활성화하려면 구성 → "모바일 및 원격 액세스" 활성화를 선택하고 아래 표에 따라 제어 옵션을 선택합니다.

표 ***11: OAuth*** 활성화 구성

인증 경로	UCM / LADP 기본 인증
새로 고침을 사용하여 OAuth 토큰으로 인증	켜기
OAuth 토큰으로 인증	켜기
사용자 자격 증명으로 인증	아니요
Jabber iOS 클라이언트가 내장된 Safari 브라우저를 사용하도록 허용	아니요
내부 인증 가용성 확인	예

표 ***12: OAuth*** 비활성화 구성

인증 경로	UCM / LADP 기본 인증
새로 고침을 사용하여 OAuth 토큰으로 인증	끄기
사용자 자격 증명으로 인증	켜기
Jabber iOS 클라이언트가 내장된 Safari 브라우저를 사용하도록 허용	끄기
내부 인증 가용성 확인	예

참고 기본 모바일 및 원격 액세스 구성에 대한 내용은 다음을 참조하십시오. https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-and-configuration-guides-list.html

IM and Presence 중앙 구축을 사용한 업그레이드를 위해서는 재동기화 필요

IM and Presence 중앙 집중식 구축이 있고 IM and Presence 중앙 클러스터 또는 원격 전화 통신 피어 클러스터를 업그레이드하는 경우 업그레이드가 완료된 후 클러스터를 다시 동기화해야 합니다. 클러스터 피어를 선택하고 저장 및 동기화 버튼을 클릭하여 Cisco Unified CM IM and Presence 관리의 중앙 집중식 구축 창에서 클러스터를 다시 동기화할 수 있습니다.

서브도메인에 대해 **SSO** 지원 원격 전화 통신 클러스터를 사용하여 **IM and Presence** 중앙 집중식 클러스터 설정

IM and Presence 중앙 집중식 구축에서 원격 전화 통신 클러스터에 여러 하위 도메인이 있는 경우, SSO가 활성화 된원격 액세스 클라이언트(예: Jabber)에 대한 SOAP 로그인을 활성화할 수 있습니다.

이 섹션에서는 SSO 활성화 원격 전화 통신 클러스터에서 Jabber에 하위 도메인 사용자 로그인을 구성하는 단계를 설명합니다. 중앙 집중식 클러스터 및 해당 중앙 집중식 클러스터와 연결된 SSO 활성화 원격 전화 통신 클러스터로 구성된 중앙 집중식 구축 시나리오를 고려하십시오.

하위 도메인에 대해 SSO 활성화 로그인을 설정하려면 다음 단계를 완료하십시오.

프로시저

단계 **1** Cisco Unified CM 관리에 로그인하고 다음을 수행합니다.

a) LDAP에서 리프 노드로 사용자를 동기화하고 디렉터리 **URI** 필드를 메일 **ID** 및 SSO 활성화로 설정합니다. LDAP 사용자를 동기화하는 방법을 알려면, LDAP 동기화를 참조하십시오 .

b) 동일한 사용자를 원격 전화 통신 노드와 동기화하고 디렉터리 **URI** 필드를 메일 **ID**로 설정합니다.

c) 최종 사용자 설정 페이지(최종 사용자 > 최종 사용자 관리)에서 IM and Presence 노드의 서비스 설정 아래에 있는 **Cisco Unified IM and Presence** 서비스에 대한 사용자 활성화**(**관련 **UC** 서비스 프로파일에서 **IM and Presence** 설정**)** 옵션을 선택하여 중앙 집중식 클러스터와 동일한 사용자를 갖도록 합니다.

d) 최종 사용자 구성 페이지(최종 사용자 > 최종 사용자 관리)에서 권한 정보 섹션을 사용하여 사용자를 CCM(Cisco Call Manager) 최종 사용자 그룹에 추가합니다.

e) 원격 전화 통신 클러스터에서 IM and Presence에 대한 사용자를 비활성화합니다. 이렇게 하려면 **ServiceSettings**에서 **CISCO Unified IM and Presence** 서비스에 대한 사용자 활성화**(**연결된 **UC** 서비스 프로파일에서 **IM and Presence** 설정**)** 옵션의 선택을 취소합니다.

f) 원격 전화 통신 클러스터의 중앙 클러스터에서 UC 서비스를 생성합니다(사용자 관리 > 사용자 설정 > **UC** 서비스 구성).

g) 중앙 클러스터에서 서비스 프로파일을 만들고 이를 시스템의 기본 서비스 프로파일로 설정하고 IM and Presence 노드를 IM and Presence 프로파일에 추가합니다(사용자 관리 > 사용자 설정 > 서비스 프로파일).

h) 중앙 클러스터에서 새로 고침 로그인을 사용한 **OAuth**를 활성화합니다. 엔터프라이즈 파라미터 구성 페이지에서 새로 고침 로그인을 사용한 **OAuth** 파라미터를 활성화로 설정합니다.

단계 **2** Cisco Unified IM and Presence 관리 콘솔에 로그인하고 리프 노드를 IM and Presence 서비스 노드에 추가합니다(시스템 > 중앙 집중식 구축).

중앙 집중식 구축에서 전화기 프레즌스 통합

중앙 집중식 구축에서 중앙 집중식 IM and Presence 노드에 여러 SIP 트렁크를 구성하여 원격 Unified CM 클러스터로부터 전화기 프레즌스 정보를 가져올 수 있습니다.

Unified CM 클러스터를 오직 한 대의 게이트웨이로 구성할 수 있는 표준 구축과는 달리, 시스템은 중앙 집중식 구축에서 이 제한 사항을 해제합니다. 이를 통해 관리자는 IM and Presence 노드에서 여러 CUCM 클러스터를 프레즌스 게이트웨이로 추가할 수 있습니다. 이렇게 하면 원격 Unified CM 클러스터에서 전화기 프레즌스 정보를 얻을 수 있습니다.

다음 절차에서는 원격 Cisco Unified CM 클러스터 및 해당 IM and Presence 노드에 SIP 트렁크 및 기타 추가 설정을 구성하는 단계를 제공합니다.

프로시저

단계 **1** **Cisco Unified CM** 관리 사용자 인터페이스에서 다음을 수행합니다.

a) 디바이스 > 트렁크를 선택합니다. 새 SIP 트렁크를 추가하고 이를 IM and Presence 퍼블리셔를 리프 클러스터로 가리킵니다.

b) 시스템 > 서비스 파라미터 구성을 선택하고 **Call Manager**를 선택합니다. **IM and Presence** 게시 트렁크 필드에 이전 단계에서 추가한 리프 클러스터 트렁크의 IP 주소를 입력합니다.

c) 클러스터에서 사용할 수 있는 모든 사용자에 대해 프레즌스를 활성화합니다. 백엔드의 BAT 파일을 사용하여 최종 사용자 설정 페이지의 모든 사용자에 대해 **Unified CM IM and Presence**에 대해 사용자 활성화**(**관련 **UC** 서비스 프로필에서 **IM and Presence** 설정**)** 확인란을 한 번에 설정할 수 있습니다.

단계 **2** **Cisco Unified CM IM and Presence** 관리에서 다음을 수행합니다.

a) **Cisco Unified CM IM and Presence** 관리 사용자 인터페이스에서 프레즌스 > 프레즌스 게이트웨이를 선택하고 드롭다운 목록에서 원격 CUCM 클러스터의 IP 주소를 입력합니다.

참고 중앙 집중식 구축 페이지에서 삭제하기 전에 프레즌스 게이트웨이 설정 창에서 원격 Unified CM 클러스터를 삭제해야 합니다.

중앙 집중식 배포 페이지에서 원격 CUCM 클러스터 주소를 업데이트하려면 다음 작업을 수행해야 합니다.

- 프레즌스 게이트웨이 구성 창에서 원격 Unified CM 클러스터를 삭제합니다.
- 중앙 집중식 배포 페이지에서 CUCM 주소를 편집합니다.

.

- 프레즌스 게이트웨이 구성 창에서 Unified CM 클러스터를 다시 추가합니다.

b) 시스템 > 보안 > 수신 **ACL**을 선택하고 원격 Cisco Unified CM의 IP 주소를 추가하여 새 ACL을 생성합니다.

중요 이 노트는 릴리스 14SU1부터 적용할 수 있습니다.

참고 IM and Presence가 SIP 메시지를 게시할 것으로 예상되는 모든 원격 Cisco Unified CM 게시자 및 가입자 노드의 IP 주소를 추가하여 새 수신 ACL을 생성합니다.

c) 시스템 > 보안 > **TLS** 피어 주체를 선택하고 원격 Cisco Unified CM의 IP 주소를 추가합니다.

중요 이 노트는 릴리스 14SU1부터 적용할 수 있습니다.

참고 TLS 피어 주체를 생성하고 IM and Presence가 SIP 메시지를 게시할 것으로 예상되는 모든 원격 Cisco Unified CM 게시자 및 가입자 노드의 IP 주소를 추가합니다.

d) 시스템 > 보안 > **TLS** 컨텍스트 구성을 선택합니다. **TLS** 피어 주체 매핑 섹션에서 사용 가능한 **TLS** 피어 주체 상자에서 이전 단계의 원격 Cisco Unified CM에 대해 생성된 TLS 피어 주체를 선택하고 선택된 **TLS** 피어 주체 상자로 이동합니다.

단계 **3** 모든 클러스터 노드에서 **Cisco OAMAgent**를 다시 시작합니다.

단계 **4** **Cisco Presence** 엔진을 다시 시작합니다.

참고 IM and Presence 서비스 중앙 집중식 구축에서 Cisco Jabber 상태를 **DND(**방해 금지**)**로 변경할 수 있습니다. 제어된 Cisco IP 전화기 및 Jabber 디바이스에도 동일한 상태가 반영됩니다. 하지만, 중앙 집중식 구축에서 둘 이상의 디바이스가 동일한 DN(디렉터리 번호)으로 구성된 경우에는 DND 상태 변경이 공유 회선에 반영되지 않습니다.

중앙 집중식 구축 상호 작용 및 제한 사항

기능	상호 작용
ILS 허브 클러스터	ILS 허브 클러스터가 다운되고 둘 이상의 전화 통신 클러스터가 있는 경우 중앙 집중식 클러스터 기능이 작동하지 않습니다.
ILS 구축	IM and Presence 중앙 클러스터를 구축하고 ILS도 구축하는 경우 ILS를 전화 통신 클러스터에만 구축할 수 있습니다. IM and Presence 중앙 클러스터에 대해 Cisco Unified Communications Manager 인스턴스에 ILS를 구축할 수 없습니다. 이 인스턴스는 프로비저닝 전용이며 전화 통신을 처리하지 않습니다.
리치 프레즌스	중앙 집중식 구축에서 사용자의 리치 프레즌스는 Cisco Jabber에 의해 계산됩니다. 사용자의 전화 통신 프레즌스는 사용자가 Jabber에 로그인한 경우에만 표시됩니다.

기능	상호 작용
Unified Communications Manager 클러스터 상태	중앙 집중식 구축에서 Unified Communications Manager 클러스터 상태는 **OAuth** 새로 고침 로그인에 대해 동기화됨으로 표시됩니다. 이 기능은 11.5(1) SU3부터 사용할 수 있습니다. Unified Communications Manager 클러스터를 11.5 1) SU3 또는 이전 릴리스에 추가할 때, OAuth 새로 고침 로그인을 지원하지 않으므로 Cisco Unified CM IM and Presence 관리의 시스템 > 중앙 집중식 구축에서 클러스터 상태가 동기화되지 않은 것으로 표시됩니다. 반면, 이러한 클러스터는 SSO 또는 LDAP 디렉터리 인증서를 사용하는 중앙 집중식 IM and Presence 서비스 구축과 호환됩니다. 참고 Cisco Jabber 사용자 로그인 기능에는 영향을 미치지 않습니다.

11 장

고급 라우팅 구성

□고급라우팅 개요

시스템이 다음 유형의 연결을 설정하는 방법을 결정하려면 고급 라우팅을 구성하십시오.

- 클러스터 내에서 IM and Presence 서비스 노드 간의 클러스터 간 연결.
- 동일한 프레즌스 도메인을 공유하는 IM and Presence 서비스 클러스터 간의 클러스터 간 연결.
- 다른 프레즌스 도메인 간의 페더레이션 연결을 위한 SIP 정적 경로. 정적 경로는 고정 경로이며 동적 경로보다 우선합니다.

클러스터 내 및 클러스터 간 연결

클러스터 간 및 클러스터 내 연결을 설정하는 두 가지 모드가 있습니다.

- 멀티캐스트 DNS(MDNS) - MDNS 라우팅은 DNS 레코드를 사용하여 노드 간의 연결을 설정합니다. 클러스터의 모든 노드가 동일한 멀티캐스트 도메인에 있는 경우 MDNS 라우팅을 사용할 수 있습니다.
- 라우터 대 라우터(기본 옵션) - 라우터 대 라우터는 IP 주소와 사용자 정보를 사용하여 노드 간의 연결을 동적으로 구성합니다. 클러스터의 노드가 동일한 멀티캐스트 도메인에 없거나 다른 서브넷에 있는 경우 라우터 대 라우터 연결을 사용합니다.

참고 MDNS 라우팅은 XCP 경로 패브릭을 연결하는 새 XCP 라우터를 원활하게 지원하기 때문에 Cisco에서는 MDNS 라우팅을 권장합니다.

고급 라우팅 필수 조건

라우팅을 구성하기 전에 시스템이 이러한 요구 사항을 충족하는지 확인하십시오. 요구 사항은 MDNS 라우팅 또는 라우터 대 라우터 등 사용하려는 라우팅 방법 유형에 따라 다릅니다.

MDNS 라우팅 필수 조건

다음 필수 조건이 존재합니다.

- IOS 네트워크에서 멀티캐스트 DNS를 구성해야 합니다. 네트워크에서 멀티캐스트 DNS가 비활성화된 경우, MDNS 패킷은 클러스터의 다른 노드에 도달할 수 없습니다. 일부 네트워크에서는 네트워크의 특정 영역에서 멀티캐스트가 기본적으로 활성화됩니다. 예를 들어, 클러스터를 형성하는 노드를 포함하는 영역에서 활성화될 수 있습니다. 이러한 네트워크에서는 MDNS 라우팅을 사용하기 위해 네트워크에서 추가 구성을 수행할 필요가 없습니다. 네트워크에서 멀티캐스트 DNS가 비활성화된 경우, MDNS 라우팅을 사용하려면 네트워크 장비의 구성을 변경해야 합니다.
- 모든 노드가 동일한 멀티캐스트 도메인에 있는지 확인하십시오.

라우터 대 라우터 필수 조건

네트워크에서 DNS를 사용할 수 있는 경우 클러스터 노드 이름과 마찬가지로 IP 주소, 호스트 이름 또는 FQDN을 사용할 수 있습니다. 그러나 네트워크에서 DNS를 사용할 수 없는 경우 노드 이름에 IP 주소를 사용해야 합니다.

IP 주소를 사용하도록 노드 이름을 재설정해야 하는 경우 http://www.cisco.com/c/en/us/support/%20unified-communications/unified-communications-manager-callmanager/%20products-maintenance-guides-list.html에서 *Cisco* 통합 커뮤니케이션 매니저와 *IM and Presence* 서비스의 *IP* 주소 및 호스트네임 변경에 나오는 "노드 이름 변경"을 참조하십시오.

고급 라우팅 구성 작업 흐름

프로시저

	명령 또는 동작	목적
단계 **1**	라우팅 통신 방법 구성, 133 페이지	라우팅 통신 유형은 IM and Presence 서비스가 클러스터 노드간에 라우터 연결을 설정하는 데 사용하는 라우팅 방법을 결정합니다. 단일 노드 IM and Presence 서비스 구축에서는 라우팅 통신 유형에 기본 설정을 사용하는 것이 좋습니다.
단계 **2**	Cisco XCP 라우터 다시 시작, 134 페이지	라우팅 통신 유형을 편집한 경우 Cisco XCP 라우터를 다시 시작해야 합니다.

	명령 또는 동작	목적
단계 **3**	보안 라우터 대 라우터 통신 구성, 135 페이지.	(선택 사항) 라우터 대 라우터 통신이 구성된 경우 동일한 클러스터 또는 다른 클러스터의 XMPP 라우터 간에 보안 TLS 연결을 구성할 수 있습니다. 참고 이 옵션은 성능을 저하시킬 수 있으므로 안전하지 않은 네트워크를 통해 IM and Presence 서비스가 실행되는 경우에만 이 옵션을 활성화해야 합니다
단계 **4**	클러스터 ID 구성, 135 페이지	MDNS 라우팅을 사용하는 경우, 클러스터 ID가 클러스터 내의 모든 노드에 의해 공유되고 값이 각 클러스터마다 고유한지 확인하십시오. 필요한 경우 이 절차를 사용하여 클러스터 ID를 업데이트할 수 있습니다.
단계 **5**	프레즌스 업데이트의 조절 속도 구성, 136 페이지	(선택 사항) Cisco XCP 라우터로 전송되는 초당 메시지 단위의 가용성(프레즌스) 변경 속도를 구성합니다. 이 설정을 사용하면 IM and Presence 서비스는 구성된 값에 맞게 가용성(프레즌스) 변경 속도를 조절할 때 오버로드를 방지할 수 있습니다.
단계 **6**	정적 경로 구성, 136 페이지	정적 경로를 구성하려면 이 작업을 완료하십시오.

라우팅 통신 방법 구성

라우팅 통신 유형은 IM and Presence 서비스가 클러스터 노드간에 라우터 연결을 설정하는 데 사용하는 라우팅 방법을 결정합니다. 단일 노드 IM and Presence 서비스 구축에서는 라우팅 통신 유형에 기본 설정을 사용하는 것이 좋습니다.

주의 클러스터 구성을 완료하고 사용자 트래픽을 IM and Presence 서비스 구축으로 수용하기 시작하려면 먼저 라우팅 통신 유형을 구성해야 합니다.

시작하기 전에

MDNS 라우팅을 사용하려면 MDNS를 IOS 네트워크 전체에서 활성화해야 합니다.

프로시저

단계 **1** IM and Presence 데이터베이스 게시자 노드에서 Cisco Unified CM IM and Presence 관리에 로그인합니다.

단계 **2** 시스템 > 서비스 파라미터를 선택합니다.

단계 **3** 서버 드롭다운 목록 상자에서 IM and Presence 서비스 노드를 선택합니다.

단계 **4** 서비스 드롭다운 목록 상자에서 **Cisco XCP** 라우터를 선택합니다.

단계 **5** **XCP** 라우터 전역 설정**(**클러스터 수준**)** 아래에서 라우팅 통신 유형 서비스 파라미터에 대한 라우팅 유형을 선택합니다.

- 멀티캐스트 **DNS(MDNS)** - 클러스터의 노드가 동일한 멀티캐스트 도메인에 있는 경우 이 방법을 선택합니다.
- 라우터 대 라우터**(**자동**)** - 클러스터의 노드가 동일한 멀티캐스트 도메인에 있지 않은 경우 이 방법을 선택합니다. 이 값이 기본 설정입니다.

  참고 라우터 대 라우터 연결을 사용하면 IM and Presence 서비스가 XCP 경로 패브릭을 설정하는 동안 구축에서 추가 성능 오버헤드가 발생합니다.

단계 **6** 저장을 클릭합니다.

다음에 수행할 작업

이 설정을 편집한 경우 다음을 수행해야 합니다. Cisco XCP 라우터 다시 시작, 134 페이지

Cisco XCP 라우터 다시 시작

라우팅 통신 유형을 편집한 경우 Cisco XCP 라우터 서비스 다시 시작.

시작하기 전에

라우팅 통신 방법 구성, 133 페이지

프로시저

단계 **1** Cisco Unified IM and Presence 서비스 가용성에서 도구 > 제어 센터 - 네트워크 서비스를 선택합니다.

단계 **2** 서버 목록에서 서비스를 다시 활성화할 노드를 선택하고 이동을 클릭합니다.

단계 **3** **IM and Presence** 서비스 영역에서 **Cisco XCP** 라우터를 선택합니다.

단계 **4** 재시작을 클릭합니다.

다음에 수행할 작업

라우터 대 라우터 라우팅이 구성된 경우, 보안 라우터 대 라우터 통신 구성, 135 페이지.

MDNS 라우팅이 구성된 경우, 클러스터 ID 구성, 135 페이지.

보안 라우터 대 라우터 통신 구성

라우터 대 라우터 통신이 구성된 경우 동일한 클러스터 또는 다른 클러스터의 XMPP 라우터 간에 보안 TLS 연결을 사용하기 위해 이 선택적 절차를 사용할 수 있습니다. IM and Presence 서비스는 클러스터 내부와 클러스터 간에 XMPP 인증서를 XMPP 신뢰 인증서로서 자동 복제합니다.

참고 이 옵션은 성능을 저하시킬 수 있으므로 안전하지 않은 네트워크를 통해 IM and Presence 서비스가 실행되는 경우에만 이 옵션을 활성화해야 합니다.

프로시저

단계 **1** Cisco Unified CM IM and Presence 관리에서 시스템 > 보안 > 설정을 선택합니다.

단계 **2** **XMPP** 라우터 대 라우터 보안 모드 활성화 확인란을 선택합니다.

단계 **3** 저장을 클릭합니다.

다음에 수행할 작업

프레즌스 업데이트의 조절 속도 구성, 136 페이지

클러스터 **ID** 구성

MDNS 라우팅을 사용하는 경우, 클러스터 **ID**가 클러스터 내의 모든 노드에 의해 공유되고 값이 각 클러스터마다 고유한지 확인하십시오. 필요한 경우 이 절차를 사용하여 클러스터 **ID**를 업데이트할 수 있습니다.

참고 설치 시 시스템에서는 고유한 기본 클러스터 **ID**를 각 IM and Presence 서비스 클러스터에 할당합니다. 변경할 필요가 없으면 기본 설정 값을 그대로 두는 것이 좋습니다.

프로시저

단계 **1** IM and Presence 서비스 데이터베이스 게시자 노드에서 Cisco Unified CM IM and Presence 관리에 로그인합니다.

단계 **2** 프레즌스 > 설정 > 표준 구성을 선택합니다.

단계 **3** 클러스터 **ID** 필드의 값을 확인합니다. ID를 편집해야 하는 경우 새 값을 입력합니다.

IM and Presence 서비스에서는 클러스터 ID 값에 밑줄(_)을 사용할 수 없습니다. 클러스터 ID 값에 밑줄 문자가 없는지 확인하십시오.

단계 **4** 저장을 클릭합니다.
클러스터 **ID**를 편집한 경우 새 설정이 모든 클러스터 노드에 복제됩니다.

다음에 수행할 작업

프레즌스 업데이트의 조절 속도 구성, 136 페이지

프레즌스 업데이트의 조절 속도 구성

이 선택적 절차를 사용하여 Cisco XCP 라우터로 전송되는 초당 메시지 단위의 가용성(프레즌스) 변경 속도를 구성합니다. 이 구성을 사용하면 IM and Presence 서비스는 구성된 값에 맞게 가용성(프레즌스) 변경 속도를 다시 조절할 때 오버로드를 방지할 수 있습니다.

프로시저

단계 **1** **Cisco Unified CM IM and Presence** 관리에서 시스템 > 서비스 파라미터를 선택합니다.

단계 **2** 서버 드롭다운 목록 상자에서 IM and Presence 서비스 노드를 선택합니다.

단계 **3** 서비스 드롭다운 목록 상자에서 **Cisco Presence** 엔진을 선택합니다.

단계 **4** 클러스터 수준 파라미터**(**모든 서버에 적용되는 파라미터**)** 섹션에서 프레즌스 변경 조절 속도 서비스 파라미터를 편집합니다. 유효 범위는 10 - 100이며 기본값은 50입니다.

단계 **5** 저장을 클릭합니다.

다음에 수행할 작업

페더레이션 연결을 위한 SIP 정적 경로를 구성하려면, 정적 경로 구성, 136 페이지.

정적 경로 구성

프로시저

	명령 또는 동작	목적
단계 **1**	SIP 프록시 서버 설정 구성, 137 페이지	SIP 프록시 서버 설정을 구성합니다. WAN 구축의 경우 IM and Presence 서비스에서 TCP 방법 이벤트 라우팅을 활성화하는 것이 좋습니다.

	명령 또는 동작	목적
단계 2	IM and Presence 서비스에서 경로 포함 템플릿 구성, 137 페이지	고정 경로에 포함된 와일드카드가 들어 있는 경우 경로 포함 템플릿을 구성해야 합니다.
단계 3	IM and Presence 서비스에서 정적 경로 구성, 139 페이지	정적 경로 설정을 구성합니다.

SIP 프록시 서버 설정 구성

프로시저

단계 1 **Cisco Unified CM IM and Presence** 관리에서 프레즌스 > 라우팅 > 설정을 선택합니다.

단계 2 메서드/경로 기반 라우팅 상태에 대해 켜기를 선택합니다. WAN 구축의 경우 IM and Presence 서비스에서 TCP 방법 이벤트 라우팅을 구성하는 것이 좋습니다.

단계 3 기본 프록시 서버에 대해 기본 **SIP** 프록시 **TCP** 리스너를 선택합니다.

단계 4 저장을 클릭합니다.

IM and Presence 서비스에서 경로 포함 템플릿 구성

고정 경로에 포함된 와일드카드가 들어 있는 경우 경로 포함 템플릿을 구성해야 합니다.

프로시저

단계 1 **Cisco Unified CM IM and Presence** 관리에서 시스템 > 서비스 파라미터를 선택합니다.

단계 2 서버 드롭다운 목록에서 IM and Presence 서비스 노드를 선택합니다.

단계 3 서비스 드롭다운에서 **Cisco SIP Proxy**를 선택합니다.

단계 4 라우팅 파라미터**(**클러스터 수준**)** 아래에 **RouteEmbedTemplate** 필드에 템플릿을 입력합니다. 최대 5개의 템플릿을 정의할 수 있습니다. 단일 경로 포함 템플릿에 대해 정의할 수 있는 정적 경로의 수에는 제한이 없습니다.

단계 5 저장을 클릭합니다.

다음에 수행할 작업

IM and Presence 서비스에서 정적 경로 구성, 139 페이지

경로 포함 템플릿

포함된 와일드카드가 있는 정적 경로 패턴용 경로 포함 템플릿을 정의해야 합니다. 경로 포함 템플릿은 시작 숫자, 숫자 길이 및 포함된 와일드카드 위치에 대한 정보를 포함합니다. 경로 포함 템플릿을 정의하기 전에 아래에 제공한 샘플 템플릿을 고려하십시오.

경로 포함 템플릿을 정의할 때 "." 뒤의 문자는 정적 경로의 실제 전화 통신 자릿수와 일치해야 합니다. 아래의 샘플 경로 포함 템플릿에서는 이러한 문자가 "x"로 표시됩니다.

샘플 경로 포함 템플릿 **A**

경로 포함 템플릿: `74..78xxxxx*`

이 템플릿에서 IM and Presence 서비스는 포함된 와일드카드로 이러한 정적 경로 세트를 활성화합니다.

표 ***13:*** 포함된 와일드카드의 정적 경로 세트 - 템플릿 ***A***

대상 패턴	다음 홉 대상
74..7812345*	1.2.3.4:5060
74..7867890*	5.6.7.8.9:5060
74..7811993*	10.10.11.37:5060

이 템플릿에서 IM and Presence 서비스는 이러한 정적 경로 항목을 활성화하지 않습니다.

- 73..7812345*(초기 문자열이 템플릿이 정의한 '74'가 아님)
- 74..781*(대상 패턴 자릿수 길이가 템플릿과 일치하지 않음)
- 74…7812345*(와일드카드 수가 템플릿과 일치하지 않음)

샘플 경로 포함 템플릿 **B**

경로 포함 템플릿: `471….xx*`

이 템플릿에서 IM and Presence 서비스는 포함된 와일드카드로 이러한 정적 경로 세트를 활성화합니다.

표 ***14:*** 포함된 와일드카드의 정적 경로 세트 - 템플릿 ***B***

대상 패턴	다음 홉 대상
471….34*	20.20.21.22
471…55*	21.21.55.79

이 템플릿에서 IM and Presence 서비스는 이러한 정적 경로 항목을 활성화하지 않습니다.

- 47…344*(초기 문자열이 템플릿이 정의한 '471'이 아님)
- 471…4*(문자열 길이가 템플릿과 일치하지 않음)
- 471.450*(와일드카드 수가 템플릿과 일치하지 않음)

IM and Presence 서비스에서 정적 경로 구성

이 절차를 사용하여 정적 경로를 설정합니다. 필드 및 해당 설정에 대한 도움이 필요한 경우 온라인 도움말을 참조하십시오.

프로시저

단계 **1** **Cisco Unified CM IM and Presence** 관리에서 라우팅 > 정적 경로를 선택합니다.

단계 **2** 새로 추가를 클릭합니다.

단계 **3** 대상 패턴에 경로 패턴을 입력합니다.

단계 **4** 다음 홉 필드에 다음 홉 서버의 IP 주소, FQDN 또는 호스트 이름을 입력합니다.

단계 **5** 다음 홉 포트에 다음 홉 서버의 대상 포트를 입력합니다. 기본 포트는 5060입니다.

단계 **6** 경로 유형 드롭다운에서 경로의 유형 사용자 또는 도메인을 선택합니다.

단계 **7** 프로토콜 유형 드롭다운 목록 상자에서 정적 경로 **TCP**, **UDP** 또는 **TLS**에 대한 프로토콜을 선택합니다.

단계 **8** 정적 경로 구성 창의 나머지 필드를 완료합니다.

단계 **9** 저장을 클릭합니다.

정적 경로 파라미터 설정

다음 표에는 IM and Presence 서비스에 대해 구성할 수 있는 정적 경로 파라미터 설정이 나열되어 있습니다.

표 ***15: IM and Presence*** 서비스의 정적 경로 파라미터

필드	설명
대상 패턴	이 필드는 수신 번호의 패턴을 최대 255자로 지정합니다. SIP 프록시는 동일한 경로 패턴의 정적 경로를 100개까지만 허용합니다. 이 제한을 초과하면 IM and Presence 서비스에서 오류를 기록합니다. 와일드카드 사용 단일 문자용 와일드카드로는 점(".")을 사용하고 여러 문자용 와일드카드로는 별표("*")를 사용할 수 있습니다. IM and Presence 서비스는 정적 경로에서 포함된 '.' 와일드카드 문자를 지원합니다. 그러나 포함된 와일드카드가 있는 정적 경로용 경로 포함 템플릿을 정의해야 합니다. 포함된 와일드카드가 있는 정적 경로는 적어도 하나의 경로 포함 템플릿과 일치해야 합니다. 경로 포함 템플릿 정의에 대한 자세한 내용은 경로 포함 템플릿 항목(아래의 관련 항목 섹션 참조)을 참조하십시오. 전화기의 경우: • 점을 패턴의 끝에 두거나 패턴에 포함할 수 있습니다. 패턴에 점을 포함하는 경우 패턴과 일치하는 경로 포함 템플릿을 만들어야 합니다. • 별표는 패턴의 끝에만 둘 수 있습니다. IP 주소 및 호스트 이름의 경우: • 호스트 이름의 일부로 별표를 사용할 수 있습니다. • 점은 호스트 이름에서 리터럴 값의 역할을 합니다. 이스케이프 처리된 별표 시퀀스 *는 리터럴 *와 일치하며 어디든 둘 수 있습니다.
설명	특정 정적 경로의 설명을 최대 255자로 지정합니다.
다음 홉	대상(다음 홉)의 도메인 이름 및 IP 주소를 지정하며, FQDN(정규화된 도메인 이름) 또는 점 구분 IP 주소일 수 있습니다. IM and Presence 서비스는 DNS SRV 기반 통화 라우팅을 지원합니다. 정적 경로를 위한 다음 홉으로 DNS SRV를 지정하려면 이 파라미터를 DNS SRV 이름으로 설정합니다.
다음 홉 포트	대상(다음 홉)의 포트 번호를 지정합니다. 기본 포트는 5060입니다. IM and Presence 서비스는 DNS SRV 기반 통화 라우팅을 지원합니다. 정적 경로를 위한 다음 홉으로 DNS SRV를 지정하려면 이 파라미터를 0으로 설정합니다.

필드	설명
경로 유형	경로 유형 사용자 또는 도메인을 지정합니다. 기본값은 사용자입니다. 예를 들어, SIP URI "sip:19194762030@myhost.com" 요청에서 사용자 부분은 '19194762030'이고 호스트 부분은 'myhost.com'입니다. 경로 유형으로 사용자를 선택한 경우 IM and Presence 서비스는 SIP 트래픽 라우팅에 대해 사용자 부분 값 '19194762030'을 사용합니다. 경로 유형으로 도메인을 선택하면 IM and Presence 서비스는 SIP 트래픽 라우팅에 "myhost.com"을 사용합니다.
프로토콜 유형	이 경로의 프로토콜 유형(TCP, UDP 또는 TLS)을 지정합니다. 기본값은 TCP입니다.
우선 순위	경로 우선 수준을 지정합니다. 값이 작을수록 우선 순위가 높습니다. 기본값은 1입니다. 값 범위: 1-65535
무게	경로 가중치를 지정합니다. 둘 이상의 경로가 동일한 우선 순위인 경우에만 이 파라미터를 사용하십시오. 값이 클수록 경로의 우선 순위가 높음을 나타납니다. 값 범위: 1-65535 예**:** 다음 세 경로의 관련 우선 순위 및 가중치를 살펴보겠습니다. • 1, 20 • 1, 10 • 2, 50 이 예에서 정적 경로는 올바른 순서대로 나열되어 있습니다. 우선 순위 경로는 최저 값 우선 순위, 즉 1을 기준으로 합니다. 두 경로가 동일한 우선 순위를 공유하므로 가장 큰 값이 있는 가중치 파라미터가 우선 순위 경로를 결정합니다. 이 예에서는 IM and Presence 서비스가 SIP 트래픽을 우선 순위 값 1로 설정된 두 개의 경로에 전달하고, 가중치에 따라 트래픽을 분배합니다. 가중치가 20인 경로는 가중치가 10인 경로의 두 배 트래픽을 수신합니다. 이 예에서는 IM and Presence 서비스가 우선 순위 1 경로를 모두 시도하고 모두 실패한 경우에만 우선 순위 2의 경로 사용을 시도합니다.
대략적 경로 허용	경로가 덜 구체적일 수 있음을 지정합니다. 기본 설정은 켜기입니다.
서비스 중	이 경로가 서비스에서 제외되었음을 지정합니다. 이 경로가 서비스에서 제외되었음을 지정합니다.
경로 차단 확인란	정적 경로를 차단하려면 선택합니다. 기본 설정은 차단하지 않는 것입니다.

12 장

인증서 구성

인증서 개요

인증서는 ID를 보호하고 IM and Presence 서비스 및 다른 시스템 간의 신뢰 관계를 구축하는 데 사용됩니다. 인증서를 사용하여 IM and Presence 서비스를 Cisco Unified Communications Manager, Cisco Jabber 클라이언트 또는 모든 외부 서버에 연결할 수 있습니다. 인증서가 없으면 가짜 DNS 서버가 사용되었는지 또는 다른 서버로 라우팅되었는지 알 수 없습니다.

IM and Presence 서비스에서 사용할 수 있는 두 가지 주요 클래스의 인증서가 있습니다.

- 자체 서명 인증서 - 자체 서명 인증서는 인증서를 발급하는 서버와 동일한 서버에서 서명됩니다. 기업 내에서 비보안 네트워크를 통해 이동하는 연결이 없는 경우 자체 서명 인증서를 사용하여 다른 내부 시스템과 연결할 수 있습니다. 예를 들어 IM and Presence 서비스는 Cisco Unified Communications Manager에 대한 내부 연결을 위해 자체 서명 인증서를 생성할 수 있습니다.
- CA 서명 인증서 - 제 3자 인증 기관(CA)에서 서명된 인증서입니다. 서버/서비스 인증서의 유효성을 제어하는 공용 CA(예: Verisign, Entrust 또는 Digicert) 또는 서버(예: Windows 2003, Linux, Unix, IOS)로 서명할 수 있습니다. CA 서명 인증서는 자체 서명 인증서보다 안전하며 일반적으로 모든 WAN 연결에 사용됩니다. 예를 들어, 페더레이션 연결을 다른 엔터프라이즈 또는 WAN 연결을 사용하는 인터클러스터 피어 구성을 사용하려면 CA 서명 인증서가 외부 시스템과의 신뢰 관계를 구축해야 합니다.

CA 서명 인증서는 자체 서명 인증서보다 안전합니다. 일반적으로 자체 서명 인증서는 내부 연결에 적합하지만 WAN 연결 또는 공용 인터넷을 통과하는 연결의 경우 CA 서명 인증서를 사용해야 합니다.

다중 서버 인증서

또한 IM and Presence 서비스는 일부 시스템 서비스에 대해 다중 서버 SAN 인증서도 지원합니다. 다중 서버 인증서를 위한 CSR(Certificate Signing Request)을 생성하면 인증서가 클러스터 노드에 업로드된 후 결과 다중 서버 인증서 및 서명 인증서의 관련 체인이 모든 클러스터 노드에 자동으로 구축됩니다.

IM and Presence 서비스의 인증서 종류

IM and Presence 서비스 내에서 다른 시스템 구성 요소에는 다른 유형의 인증서가 필요합니다. 다음 표에서는 IM and Presence 서비스의 클라이언트와 서비스에 필요한 서로 다른 인증서에 대해 설명합니다.

참고 인증서 이름이 -ECDSA로 끝나면 인증서/키 유형은 Elliptic Curve(EC)입니다. 그렇지 않으면, RSA입니다.

표 ***16:*** 인증서 종류 및 서비스

인증서 종류	서비스	인증서 신뢰 저장	다중 서버 지원	참고
tomcat, tomcat-ECDSA	Cisco 클라이언트 프로파일 에이전트, Cisco AXL 웹 서비스, Cisco Tomcat	tomcat- trust	예	IM and Presence 서비스에 대한 클라이언트 인증의 일부로서 Cisco Jabber 클라이언트에 표시됩니다. Cisco Unified CM IM and Presence 관리 사용자 인터페이스를 탐색할 때 웹 브라우저에 표시됩니다. 연결된 trust-store는 사용자 자격 증명을 구성된 LDAP 서버로 인증하기 위해 IM and Presence 서비스에서 설정한 연결을 확인하는 데 사용됩니다.
ipsec		ipsec-신뢰	아니요	IPSec 정책이 활성화될 때 사용됩니다.
cup, cup-ECDSA	Cisco SIP Proxy, Cisco Presence 엔진	cup-trust	아니요	SIP 페더레이션 사용자를 위해 IM and Presence를 가져오기 위해 Expressway-C에 인증서를 제공합니다. IM and Presence 프록시는 클라이언트와 서버 역할을 모두 수행합니다. 프레즌스 엔진은 Exchange/Office 365 통신에 이러한 인증서를 사용하여 일정 프레즌스를 얻습니다. 프레즌스 엔진은 클라이언트 전용으로 작동합니다.

인증서 종류	서비스	인증서 신뢰 저장	다중 서버 지원	참고
cup-xmpp, cup-xmpp-ECDSA	Cisco XCP 연결 관리자, Cisco XCP Web 연결 관리자, Cisco XCP 디렉터리 서비스, Cisco XCP 라우터 서비스	cup-XMPP-trust	예	XMPP 세션을 생성하는 동안 Cisco Jabber 클라이언트, 타사 XMPP 클라이언트 또는 CAXL 기반 애플리케이션에 표시됩니다. 연결된 trust-store는 타사 XMPP 클라이언트에 대해 LDAP 검색 작업을 수행하는 과정에서 Cisco XCP 디렉터리 서비스가 설정한 연결을 확인하는 데 사용됩니다. 연결된 trust-store는 라우팅 통신 유형이 라우터 대 라우터로 설정된 경우 IM and Presence 서비스 서버 간 보안 연결을 설정할 때 Cisco XCP 라우터 서비스에 의해 사용됩니다.
cup-xmpp-s2s, cup-xmpp-s2s-ECDSA	Cisco XCP XMPP 페더레이션 연결 관리자	cup-XMPP-trust	예	외부에서 제휴된 XMPP 시스템을 연결할 때 XMPP 도메인 간 페더레이션에 대해 표시됩니다.

인증서 필수 조건

Cisco Unified Communications Manager에서 다음 항목을 구성합니다.

- IM and Presence 서비스용 SIP 트렁크 보안 프로파일을 구성합니다.
- IM and Presence 서비스에 대한 SIP 트렁크를 구성합니다.
  - 보안 프로파일을 SIP 트렁크와 연결합니다.
  - IM and Presence 서비스 인증서의 주체 CN(공통 이름)으로 SIP 트렁크를 구성합니다.

Cisco Unified Communications Manager와 인증서 교환

Cisco Unified Communications Manager와 인증서를 교환하려면 이 작업을 완료하십시오.

참고 Cisco Unified Communications Manager와 IM and Presence 서비스 간의 인증서 교환은 설치 프로세스 중에 자동으로 처리됩니다. 그러나 인증서 교환을 수동으로 완료해야 하는 경우 이 작업을 완료하십시오.

프로시저

	명령 또는 동작	목적
단계 1	Cisco Unified Communications Manager 인증서를 IM and Presence 서비스로 가져오기, 146 페이지	Cisco Unified Communications Manager의 인증서를 IM and Presence 서비스로 가져옵니다.
단계 2	IM and Presence 서비스에서 인증서 다운로드, 147 페이지	IM and Presence 서비스에서 인증서를 다운로드합니다. 인증서를 Cisco Unified Communications Manager로 가져와야 합니다.
단계 3	IM and Presence 인증서를 Cisco Unified Communications Manager로 가져오기, 147 페이지	인증서 교환을 완료하려면 IM and Presence 서비스 인증서를 Cisco Unified Communications Manager의 Callmanager-trust 저장소로 가져옵니다.

Cisco Unified Communications Manager 인증서를 IM and Presence 서비스로 가져오기

이 절차를 사용하여 Cisco Unified Communications Manager의 인증서를 IM and Presence 서비스로 가져옵니다.

프로시저

단계 1 **Cisco Unified CM IM and Presence** 관리에서 시스템 > 보안 > 인증서 가져오기 도구를 선택합니다.

단계 2 인증서 신뢰 저장 메뉴에서 **IM and Presence(IM/P)** 서비스 신뢰를 선택합니다.

단계 3 Cisco Unified Communications Manager 노드의 IP 주소, 호스트 이름 또는 FQDN을 입력합니다.

단계 4 Cisco Unified Communications Manager 노드와 통신하기 위한 포트 번호를 입력합니다.

단계 5 제출을 클릭합니다.

참고 인증서 가져오기 도구는 가져오기 작업을 완료한 후 Cisco Unified Communications Manager에 성공적으로 연결되었는지 여부, Cisco Unified Communications Manager에서 인증서가 성공적으로 다운로드되었는지 여부를 보고합니다. 인증서 가져오기 도구에서 실패를 보고하는 경우 온라인 도움말의 권장 작업을 참조하십시오. **Cisco Unified IM and Presence OS** 관리보안 > 인증서 관리를 선택하여 수동으로 인증서를 가져올 수도 있습니다.

참고 협상된 TLS 암호화에 따라 인증서 가져 오기 도구는 RSA 기반 인증서 또는 ECDSA 기반 인증서를 다운로드합니다.

단계 6 Cisco SIP Proxy 서비스를 다시 시작합니다.

a) Cisco Unified IM and Presence 서비스 가용성의 IM and Presence에서 도구 > 제어 센터 - 기능 서비스를 선택합니다.

b) 서버 드롭다운 목록 상자에서 IM and Presence 서비스 클러스터 노드를 선택하고 이동을 클릭합니다.
c) **Cisco SIP Proxy**를 선택하고 다시 시작을 클릭합니다.

다음에 수행할 작업

IM and Presence 서비스에서 인증서 다운로드, 147 페이지

IM and Presence 서비스에서 인증서 다운로드

이 절차를 사용하여 IM and Presence 서비스에서 인증서를 다운로드합니다. 인증서를 Cisco Unified Communications Manager로 가져와야 합니다.

프로시저

단계 **1** **Cisco Unified IM and Presence OS** 관리의 IM and Presence에서 보안 > 인증서 관리를 선택합니다.
단계 **2** 찾기를 클릭합니다.
단계 **3** `cup.pem` 파일을 선택합니다.

참고 `cup ECDSA.pem`도 사용할 수 있는 옵션입니다.

단계 **4** 다운로드를 클릭하고 파일을 로컬 컴퓨터에 저장합니다.

팁 cup.csr 파일 액세스와 관련하여 IM and Presence 서비스에 표시되는 오류는 무시하십시오. CA(인증 기관)에서는 사용자가 Cisco Unified Communications Manager와 교환하는 인증서에 서명할 필요가 없습니다.

다음에 수행할 작업

IM and Presence 인증서를 Cisco Unified Communications Manager로 가져오기, 147 페이지

IM and Presence 인증서를 Cisco Unified Communications Manager로 가져오기

인증서 교환을 완료하려면 IM and Presence 서비스 인증서를 Cisco Unified Communications Manager의 Callmanager-trust 저장소로 가져옵니다.

시작하기 전에

IM and Presence 서비스에서 인증서 다운로드, 147 페이지

프로시저

단계 **1** Cisco Unified OS 관리에 로그인합니다.

단계 **2** 보안 > 인증서 관리를 선택합니다.

단계 **3** 인증서 업로드를 클릭합니다.

단계 **4** 인증서 이름 메뉴에서 **Callmanager-trust**를 선택합니다.

단계 **5** 찾아보기를 선택하고 IM and Presence 서비스에서 이전에 다운로드한 인증서를 선택합니다.

단계 **6** 파일 업로드를 클릭합니다.

단계 **7** Cisco CallManager 서비스를 다시 시작합니다.

a) Cisco Unified Serviceability에서 도구 > 제어 센터 - 기능 서비스를 선택합니다.

b) 서버 드롭다운 목록 상자에서 Cisco Unified Communications Manager 노드를 선택하고 이동을 클릭합니다.

c) **Cisco CallManager** 서비스를 선택하고 다시 시작을 클릭합니다.

IM and Presence 서비스에 CA(인증 기관) 설치

IM and Presence 서비스에서 제3자 CA(인증 기관)에서 서명한 인증서를 사용하려면 먼저 해당 CA의 루트 신뢰 인증서 체인을 IM and Presence 서비스에 설치해야 합니다.

프로시저

	명령 또는 동작	목적
단계 **1**	CA 루트 인증서 체인 업로드, 148 페이지	이 절차를 사용하여 제3자 인증 기관에서 IM and Presence 서비스로 CA 루트 인증서 체인을 업로드합니다.
단계 **2**	Cisco 클러스터 간 동기화 에이전트 서비스 다시 시작, 149 페이지	인증서를 업로드한 후, Cisco 클러스터 간 동기화 에이전트 서비스를 다시 시작합니다.
단계 **3**	CA 인증서가 다른 클러스터에 동기화되었는지 확인, 150 페이지	CA 인증서 체인이 모든 피어 클러스터에 복제되었는지 확인합니다.

CA 루트 인증서 체인 업로드

이 절차를 사용하여 서명 인증 기관(CA)의 인증서를 IM and Presence 데이터베이스 게시자 노드로 업로드합니다. 체인은 체인의 여러 인증서로 구성될 수 있으며, 각 인증서는 후속 인증서에 서명합니다.

- 루트 인증서 > 중간 1 인증서 > 중간 2 인증서

프로시저

단계 1 IM and Presence 데이터베이스 게시자 노드에서 Cisco Unified IM and Presence OS 관리에 로그인합니다.

단계 2 보안 > 인증서 관리를 선택합니다.

단계 3 인증서/인증서 체인 업로드를 클릭합니다.

단계 4 인증서 이름 드롭다운 목록에서 다음 중 하나를 선택합니다.

- CA 서명 tomact 인증서를 업로드하는 경우 **tomcat-trust**를 선택합니다.
- CA 서명 cup-xmpp 인증서 또는 CA 서명 cup-xmpp-s2s를 업로드하는 경우 **cup-xmpp-trust**를 선택합니다.

단계 5 서명 인증서에 대한 설명을 입력합니다.

단계 6 찾아보기를 클릭하여 루트 인증서에 대한 파일을 찾습니다.

단계 7 파일 업로드를 클릭합니다.

단계 8 인증서/인증서 체인 업로드 창을 사용하여 같은 방법으로 각 중간 인증서를 업로드합니다. 각 중간 인증서에 대해 체인에 선행 인증서의 이름을 입력해야 합니다.

다음에 수행할 작업

Cisco 클러스터 간 동기화 에이전트 서비스 다시 시작, 149 페이지

Cisco 클러스터 간 동기화 에이전트 서비스 다시 시작

IM and Presence 데이터베이스 게시자 노드에 루트 및 중간 인증서를 업로드한 후에는 해당 노드에서 Cisco 클러스터 간 동기화 에이전트 서비스를 다시 시작해야 합니다. 이 서비스를 다시 시작하면 CA 인증서가 다른 모든 클러스터에 즉시 동기화됩니다.

프로시저

단계 1 Cisco Unified IM and Presence 서비스 가용성에서 도구 > 제어 센터 - 네트워크 서비스를 선택합니다.

단계 2 서버 드롭다운 목록 상자에서 인증서를 가져온 IM and Presence 서비스 노드를 선택하고 이동을 클릭합니다.

참고 또한 명령줄 인터페이스에서 `utils service restart Cisco Intercluster Sync Agent` 명령을 사용하여 Cisco 클러스터 간 동기화 에이전트 서비스를 다시 시작할 수도 있습니다.

단계 3 **Cisco** 클러스터 간 동기화 에이전트 서비스를 선택하고 다시 시작을 클릭합니다.

다음에 수행할 작업

클러스터 간 동기화 확인, 153 페이지

CA 인증서가 다른 클러스터에 동기화되었는지 확인

Cisco 클러스터 간 동기화 에이전트 서비스가 다시 시작되면 CA 인증서가 다른 클러스터에 올바르게 동기화되었는지 확인해야 합니다. 다른 각 IM and Presence 데이터베이스 게시자 노드에서 다음 절차를 완료하십시오.

참고 다음 절차의 정보는 -ECDSA로 끝나는 인증서에도 적용됩니다.

프로시저

단계 **1** **Cisco Unified CM IM and Presence** 관리에서 진단 > 시스템 문제 해결 도구를 선택합니다.

단계 **2** 상호 클러스터링 문제 해결 도구 아래에서 각 **TLS** 사용 인터클러스터 피어가 보안 인증서를 성공적으로 교환했는지 확인하십시오**.** 테스트를 찾아보고 통과했는지 확인합니다.

단계 **3** 테스트에 오류가 표시되면 인터클러스터 피어 IP 주소를 확인합니다. CA 인증서를 업로드한 클러스터를 참조해야 합니다. 다음 단계를 진행하여 문제를 해결합니다.

단계 **4** 프레즌스 > 클러스터 간을 선택하고 시스템 문제 해결 도구 페이지에서 확인한 인터클러스터 피어와 관련된 링크를 클릭합니다.

단계 **5** 강제 수동 동기화를 클릭합니다.

단계 **6** 인터클러스터 피어 상태 패널에서 자동 새로 고침으로 60초를 허용합니다.

단계 **7** 인증서 상태 필드에 "연결이 안전합니다"가 표시되는지 확인합니다.

단계 **8** 인증서 상태 필드에 "연결이 안전합니다"가 표시되지 않으면 IM and Presence 데이터베이스 게시자 노드에서 Cisco 클러스터 간 동기화 에이전트 서비스를 다시 시작하고 5~7단계를 반복합니다.

- 관리 CLI에서 서비스를 다시 시작하려면 utils service restart Cisco Intercluster Sync Agent 명령을 실행합니다.
- 또는 Cisco Unified IM and Presence 서비스 가용성 GUI에서 이 서비스를 다시 시작할 수도 있습니다.

단계 **9** 인증서 상태 필드에 이제 "연결이 안전합니다"가 표시되는지 확인합니다. 이 표시는 클러스터 간 동기화가 클러스터 사이에서 올바르게 설정되었고, 업로드한 CA 인증서가 다른 클러스터에 동기화되었음을 의미합니다.

다음에 수행할 작업

서명 인증서를 각 IM and Presence 서비스 노드에 업로드합니다.

IM and Presence 서비스로 인증서 업로드

IM and Presence 서비스에 인증서를 업로드하려면 다음 작업을 완료하십시오. CA 서명 인증서 또는 자체 서명 인증서를 업로드할 수 있습니다.

시작하기 전에

제3자 CA(인증 기관)에서 서명한 CA 서명 인증서를 사용하려면 해당 CA의 루트 인증서 체인이 IM and Presence 서비스에 이미 설치되어 있어야 합니다. 자세한 내용은 IM and Presence 서비스에 CA(인증 기관) 설치, 148 페이지의 내용을 참조하십시오.

프로시저

	명령 또는 동작	목적
단계 **1**	인증서 업로드, 151 페이지	서명된 인증서를 IM and Presence 서비스에 업로드합니다.
단계 **2**	Cisco Tomcat 서비스 다시 시작, 152 페이지	(Tomcat 인증서만 해당). Cisco Tomcat 서비스를 다시 시작합니다.
단계 **3**	클러스터 간 동기화 확인, 153 페이지	(Tomcat 인증서만 해당). 클러스터 내 영향받는 모든 노드에 대해 Cisco Tomcat 서비스가 다시 시작되었으면 클러스터 간 동기화가 제대로 작동하는지 확인해야 합니다.
단계 **4**	모든 노드에서 Cisco XCP 라우터 서비스 다시 시작, 153 페이지	인증서를 cup-xmpp 저장소에 업로드한 경우 모든 클러스터 노드에서 Cisco XMP 라우터를 다시 시작합니다.
단계 **5**	Cisco XCP XMPP 페더레이션 연결 관리자 서비스 다시 시작, 154 페이지	(XMPP 페더레이션만 해당). XMPP 페더레이션을 위해 cup-xmpp 저장소로 인증서를 업로드한 경우 Cisco XCPXMPP 페더레이션 연결 관리자 서비스를 다시 시작합니다.
단계 **6**	XMPP 페더레이션 보안 인증서에서 와일드카드 활성화, 154 페이지	(XMPP 페더레이션만 해당). TLS를 통한 XMPP 페더레이션을 위한 cup-xmpp 저장소로 인증서를 업로드한 경우 XMPP 보안 인증서에 대해 와일드카드를 활성화해야 합니다. 이는 그룹 채팅에 필요합니다.

인증서 업로드

이 절차를 사용하여 각 IM and Presence 서비스 노드에 업로드합니다.

참고 클러스터에 대한 모든 필수 tomcat 인증서에 서명하고 동시에 업로드하는 것이 좋습니다. 이 프로세스를 수행하면 클러스터 간 통신 복구에 소요되는 시간이 단축됩니다.

참고 다음 절차의 정보는 -ECDSA로 끝나는 인증서에도 적용됩니다.

시작하기 전에

인증서가 CA에 의해 서명된 경우 해당 CA의 루트 인증서 체인도 설치했어야 합니다. 그렇지 않으면 CA 서명 인증서를 신뢰하지 않습니다. CA 인증서가 모든 클러스터에 대해 올바르게 동기화되었으면 적절한 서명 인증서를 각 IM and Presence 서비스 노드에 업로드할 수 있습니다.

프로시저

단계 **1** **Cisco Unified IM and Presence OS** 관리에서 보안 > 인증서 관리를 선택합니다.
단계 **2** 인증서/인증서 체인 업로드를 클릭합니다.
단계 **3** 인증서 목적을 선택합니다. 예를 들어 **tomcat**.
단계 **4** 서명 인증서에 대한 설명을 입력합니다.
단계 **5** 찾아보기를 클릭하고 업로드할 파일을 찾습니다.
단계 **6** 파일 업로드를 클릭합니다.
단계 **7** 각 IM and Presence 서비스 노드에 대해 반복합니다.

다음에 수행할 작업

Cisco Tomcat 서비스를 다시 시작합니다.

Cisco Tomcat 서비스 다시 시작

각 IM and Presence 서비스 노드에 tomcat 인증서를 업로드한 후에는 각 노드에서 Cisco Tomcat 서비스를 다시 시작해야 합니다.

프로시저

단계 **1** 관리자 CLI에 로그인합니다.
단계 **2** `utils service restart Cisco Tomcat` 명령을 실행합니다.
단계 **3** 각 노드에 대해 반복합니다.

다음에 수행할 작업

클러스터 간 동기화가 제대로 작동하는지 확인합니다.

클러스터 간 동기화 확인

클러스터 내 영향받는 모든 노드에 대해 Cisco Tomcat 서비스가 다시 시작되었으면 클러스터 간 동기화가 제대로 작동하는지 확인해야 합니다. 다른 클러스터의 각 IM and Presence 데이터베이스 게시자 노드에서 다음 절차를 완료하십시오.

프로시저

단계 **1** **Cisco Unified CM IM and Presence** 관리에서 진단 > 시스템 문제 해결 도구를 선택합니다.

단계 **2** 상호 클러스터링 문제 해결 도구 아래에서 각 **TLS** 사용 인터클러스터 피어가 보안 인증서를 성공적으로 교환했는지 확인하십시오**.** 테스트를 찾아보고 통과했는지 확인합니다.

단계 **3** 테스트에 오류가 표시되면 인터클러스터 피어 IP 주소를 확인합니다. CA 인증서를 업로드한 클러스터를 참조해야 합니다. 다음 단계를 진행하여 문제를 해결합니다.

단계 **4** 프레즌스 > 클러스터 간을 선택하고 시스템 문제 해결 도구 페이지에서 확인한 인터클러스터 피어와 관련된 링크를 클릭합니다.

단계 **5** 강제 수동 동기화를 클릭합니다.

단계 **6** 피어의 **Tomcat** 인증서도 재동기화 확인란을 선택하고 확인을 클릭합니다.

단계 **7** 인터클러스터 피어 상태 패널에서 자동 새로 고침으로 60초를 허용합니다.

단계 **8** 인증서 상태 필드에 "연결이 안전합니다"가 표시되는지 확인합니다.

단계 **9** 인증서 상태 필드에 "연결이 안전합니다"가 표시되지 않으면 IM and Presence 데이터베이스 게시자 노드에서 Cisco 클러스터 간 동기화 에이전트 서비스를 다시 시작하고 5~8단계를 반복합니다.

- 관리자는 다음 명령을 실행 하는 CLI에서 서비스를 다시 시작 하려면: utils 서비스 Cisco 클러스터 간 동기화 에이전트를 다시 시작 합니다.
- 또는 Cisco Unified IM and Presence 서비스 가용성 GUI에서 이 서비스를 다시 시작할 수도 있습니다.

단계 **10** 인증서 상태 필드에 이제 "연결이 안전합니다"가 표시되는지 확인합니다. 표시되면, 이 클러스터와 인증서가 업로드된 클러스터 사이에 클러스터 간 동기화가 다시 설정된 것입니다.

모든 노드에서 **Cisco XCP** 라우터 서비스 다시 시작

cup-xmpp 및/또는 cup-xmpp-ECDSA 인증서를 각 IM and Presence 서비스 노드에 업로드한 후에는 각 노드에서 Cisco XCP 라우터 서비스를 다시 시작해야 합니다.

참고 Cisco Unified IM and Presence 서비스 가용성 GUI에서 Cisco XCP 라우터 서비스를 다시 시작할 수도 있습니다.

프로시저

단계 **1** 관리자 CLI에 로그인합니다.

단계 **2** utils service restart Cisco XCP Router 명령을 실행합니다.

단계 **3** 각 노드에 대해 반복합니다.

Cisco XCP XMPP 페더레이션 연결 관리자 서비스 다시 시작

cup-xmpp-s2s 및/또는 cup-xmpp-s2s-ECDSA 인증서를 각 IM and Presence 서비스 페더레이션 노드에 업로드한 후에는 각 페더레이션 노드에서 Cisco XCP XMPP 페더레이션 연결 관리자 서비스를 다시 시작해야 합니다.

프로시저

단계 **1** 관리자 CLI에 로그인합니다.

단계 **2** utils service restart Cisco XCP XMPP Federation Connection Manager 명령을 실행합니다.

단계 **3** 각 페더레이션 노드에 대해 반복합니다.

XMPP 페더레이션 보안 인증서에서 와일드카드 활성화

TLS를 통한 XMPP 페더레이션 파트너 간 그룹 채팅을 지원하려면 XMPP 보안 인증서에 대한 와일드카드를 활성화해야 합니다.

기본적으로 XMPP 페더레이션 보안 인증서 `cup-xmpp-s2s` 및 `cup-xmpp-s2s-ECDSA`에는 IM and Presence 서비스 구축에서 호스트하는 모든 도메인이 포함됩니다. 이들은 SAN(Subject Alternative Name) 항목으로서 인증서 내에 추가됩니다. 호스트된 모든 도메인에 대한 와일드카드를 동일한 인증서 내에서 제공해야 합니다. 따라서 XMPP 보안 인증서에는 SAN 항목 "example.com" 대신 SAN 항목 "*.example.com"을 포함해야 합니다. 그룹 채팅 서버 별칭은 IM and Presence 서비스 시스템에 호스트된 도메인 중 하나의 하위 도메인이므로 와일드카드가 필요합니다. 예: “conference.example.com”.

참고 모든 노드에서 `cup-xmpp-s2s` 또는 `cup-xmpp-s2s-ECDSA` 인증서를 보려면 **Cisco Unified IM and Presence OS** 관리 > 보안 > 인증서 관리를 선택하고 **cup-xmpp-s2s** 또는 **cup-xmpp-s2s-ECDSA** 링크를 클릭합니다.

프로시저

단계 **1** 시스템 > 보안 설정을 선택합니다.

단계 **2** **XMPP** 페더레이션 보안 인증서에서 와일드카드 활성화를 선택합니다.

단계 **3** 저장을 클릭합니다.

다음에 수행할 작업

Cisco XMPP 페더레이션 연결 관리자 서비스가 실행되고 있으며 XMPP 페더레이션이 활성화된 클러스터 내 모든 노드에서 XMPP 페더레이션 보안 인증서를 다시 생성해야 합니다. TLS를 통한 XMPP 페더레이션 그룹 채팅을 지원하려면 모든 IM and Presence 서비스 클러스터에서 이 보안 설정을 활성화해야 합니다.

Generate a CSR(CSR 생성)

이 절차를 사용하여 인증서 서명 요청(CSR)을 생성합니다. CA 서명 인증서를 제공할 수 있도록 제3자 CA에 제출할 CSR이 필요합니다.

프로시저

단계 **1** Cisco Unified OS 관리에서 보안 > 인증서 관리를 선택합니다.

단계 **2** **CSR** 생성 버튼을 클릭합니다. 인증서 서명 요청 생성 팝업 창이 나타납니다.

단계 **3** 인증서 목적 드롭다운 목록에서 생성하는 인증서의 유형을 선택합니다.

단계 **4** 서버 드롭다운 목록에서 IM and Presence 서버를 선택합니다. 다중 서버 인증서의 경우 다중 서버**(SAN)**를 선택합니다.

단계 **5** 키 길이 및 해시 알고리즘을 입력합니다.

단계 **6** 나머지 필드를 작성하고 생성을 클릭합니다.

단계 **7** CSR을 로컬 컴퓨터에 다운로드합니다.

a) **CSR** 다운로드를 클릭합니다.
b) 인증서 용도 드롭다운 목록에서 인증서 이름을 선택합니다.
c) **CSR** 다운로드

다음에 수행할 작업

CA 서명 인증서를 발급할 수 있도록 CSR을 제3자 인증 기관에 제출합니다.

인증서 서명 요청 키 사용 확장

다음 표에는 Unified Communications Manager 및 IM and Presence Service CA 인증서에 대한 인증서 서명 요청(CSR)의 주요 용도 확장이 나와 있습니다.

표 ***17: Cisco Unified Communications Manager CSR*** 키 용도 확장

	다중 서버	확장 키 사용			키 사용				
		서버 인증 **(1.3.6.1.5.5.7.3.1)**	클라이언트 인증 **(1.3.6.1.5.5.7.3.2)**	**IP** 보안 엔드 시스템 **(1.3.6.1.5.5.7.3.5)**	디지털 서명	키 암호화	데이터 암호화	키 인증서 서명	키 계약
CallManager CallManager-ECDSA	Y	Y	Y		Y	N	Y		
CAPF(게시자에만 해당)	N	Y	N		Y	N		Y	
ipsec	N	Y	Y	Y	Y	Y	Y		
tomcat tomcat-ECDSA	Y	Y	Y		Y	N	Y		
TVS	N	Y	Y		Y	Y	Y		

표 ***18: IM and Presence Service CSR*** 키 사용 확장

	다중 서버	확장 키 사용			키 사용				
		서버 인증 **(1.3.6.1.5.5.7.3.1)**	클라이언트 인증 **(1.3.6.1.5.5.7.3.2)**	**IP** 보안 엔드 시스템 **(1.3.6.1.5.5.7.3.5)**	디지털 서명	키 암호화	데이터 암호화	키 인증서 서명	키 계약
cup cup-ECDSA	N	Y	Y	Y	Y	Y	Y		
cup-XMPP cup-xmpp-ECDSA	Y	Y	Y	Y	Y	Y	Y		
cup-XMPP-s2s cup-xmpp-s2s-ECDSA	Y	Y	Y	Y	Y	Y	Y		
ipsec	N	Y	Y	Y	Y	Y	Y		
tomcat tomcat-ECDSA	Y	Y	Y		Y	Y	Y		

참고 '데이터 암호화' 비트가 CA 서명 인증서 프로세스의 일부로 변경되거나 제거되지 않았는지 확인하십시오.

셀프 서명 인증서 생성

이 절차를 사용하여 자체 서명 인증서를 생성합니다.

프로시저

단계 **1** Cisco Unified OS 관리에서 보안 > 인증서 관리를 선택합니다.
단계 **2** 자체 서명 생성을 클릭합니다. 새 자체 서명 인증서 생성 팝업 창이 나타납니다.
단계 **3** 인증서 목적 드롭다운 목록에서 생성하는 인증서의 유형을 선택합니다.
단계 **4** 구축 드롭다운에서 서버의 이름을 입력합니다.
단계 **5** 적절한 키 길이를 선택합니다.
단계 **6** 해시 알고리즘에서 암호화 알고리즘을 선택합니다. 예를 들어 SHA256.
단계 **7** 생성을 클릭합니다.

IM and Presence 서비스에서 자체 서명 신뢰 인증서 삭제

동일한 클러스터에서 노드 간 서비스 가용성에 대한 교차 탐색을 지원하기 위해, IM and Presence 서비스와 Cisco Unified Communications Manager 간 Cisco Tomcat 서비스 신뢰 저장소가 자동으로 동기화됩니다.

원래의 자체 서명 신뢰 인증서를 CA 서명 인증서로 바꾼 경우 원래의 자체 서명 신뢰 인증서가 서비스 신뢰 저장소에 유지됩니다. 이 절차를 사용하여 IM and Presence 서비스 및 Cisco Unified Communications Manager 노드에서 자체 서명 인증서를 삭제할 수 있습니다.

시작하기 전에

중요 CA 서명 인증서를 추가한 경우 Cisco 클러스터 간 동기화 에이전트 서비스가 지정된 IM and Presence 서비스 노드에서 정기적인 정리 작업을 수행하기 위해서는 30분을 대기해야 합니다.

프로시저

단계 **1** Cisco Unified IM and Presence Operating System 관리에서 보안 > 인증서 관리를 선택합니다.
단계 **2** 찾기를 클릭합니다.

인증서 목록이 나타납니다.

참고 인증서 이름은 서비스 이름 및 인증서 유형의 두 부분으로 구성됩니다. 예를 들어 tomcat-trust에서 tomcat은 서비스 이름이고 trust는 인증서 유형입니다.

삭제할 수 있는 자체 서명 신뢰 인증서는 다음과 같습니다.

- Tomcat 및 Tomcat-ECDSA — tomcat-trust
- Cup-xmpp 및 Cup-xmpp-ECDSA — cup-xmpp-trust
- Cup-xmpp-s2s 및 Cup-xmpp-s2s-ECDSA — cup-xmpp-trust
- Cup 및 Cup-ECDSA — cup-trust
- Ipsec - ipsec-trust

단계 **3** 삭제하고자 하는 자체 서명 신뢰 인증서의 링크를 클릭합니다.

중요 서비스 신뢰 저장소와 연결된 서비스에 대해 CA 서명 인증서를 구성했는지 확인하십시오.

인증서 상세정보를 표시하는 새 창이 나타납니다.

단계 **4** 삭제를 클릭합니다.

참고 해당 인증서를 삭제할 권한이 있는 경우에만 삭제 버튼이 나타납니다.

단계 **5** 구축 전체에서 불필요한 자체 서명 신뢰 인증서를 모두 제거하려면 클러스터의 각 IM and Presence 서비스 노드 및 인터클러스터 피어에 대해 위 절차를 반복하십시오.

다음에 수행할 작업

서비스가 Tomcat이면 Cisco Unified Communications Manager 노드에서 IM and Presence 서비스 노드의 자체 서명 tomcat-trust 인증서를 확인해야 합니다. Cisco Unified Communications Manager에서 자체 서명 Tomcat-Trust 인증서 삭제, 158 페이지를 참조하십시오.

Cisco Unified Communications Manager에서 자체 서명 Tomcat-Trust 인증서 삭제

클러스터의 각 노드에 대한 Cisco Unified Communications Manager 서비스 신뢰 저장소에는 자체 서명 tomcat-trust 인증서가 있습니다. Cisco Unified Communications Manager 노드에서 삭제할 인증서는 이러한 인증서뿐입니다.

참고 다음 절차에 있는 정보는 EC 인증서에도 적용됩니다.

시작하기 전에

CA 서명 인증서로 클러스터의 IM and Presence 서비스 노드를 구성한 다음, Cisco Unified Communications Manager 노드로 인증서가 전파되기까지 30분 정도 기다렸는지 확인합니다.

프로시저

단계 **1** **Cisco Unified Operating System** 관리에서 보안 > 인증서 관리를 선택합니다.

인증서 목록 창이 표시됩니다.

단계 **2** 검색 결과를 필터링하려면 드롭다운 목록에서 인증서 및 시작 단어를 선택하고 빈 필드에 tomcat-trust를 입력합니다. 찾기를 클릭합니다.

인증서 목록 창이 확장되면서 tomcat-trust 인증서가 나열됩니다.

단계 **3** 이름에 IM and Presence 서비스 노드의 호스트네임 또는 FQDN이 포함된 링크를 확인합니다. 이것은 이 서비스 및 IM and Presence 서비스 노드와 연결된 SSC(자가서명 인증서)입니다.

단계 **4** IM and Presence 서비스 노드의 자체 서명 tomcat-trust 인증서에 대한 링크를 클릭합니다.

tomcat-trust 인증서 상세정보를 표시하는 새 창이 나타납니다.

단계 **5** 인증서 상세정보에서 발급자 이름 CN= 값 및 주체 이름 CN= 값이 일치하는지 검토하여 이것이 자체 서명 인증서인지 확인합니다.

단계 **6** 이것이 자체 서명 인증서인지를 확인했으며 CA 서명 인증서가 Cisco Unified Communications Manager 노드로 전파된 것이 확실하면 삭제를 클릭합니다.

참고 삭제 권한이 있는 인증서에 대해서만 삭제 버튼이 나타납니다.

단계 **7** 클러스터의 각 IM and Presence 서비스 노드에 대해 4~6단계를 반복합니다.

인증서 모니터링 작업 흐름

이 작업을 수행하여 인증서 상태 및 만료를 자동으로 모니터링하도록 시스템을 구성하십시오.

- 인증서가 만료에 도달하면 전자 메일을 보냅니다.
- 만료된 인증서를 해지합니다.

프로시저

	명령 또는 동작	목적
단계 **1**	인증서 모니터 알림 구성, 160 페이지	자동 인증서 모니터링을 구성합니다. 시스템은 인증서 상태를 주기적으로 확인하고 인증서의 만료가 다가오면 사용자에게 전자 메일을 보냅니다.
단계 **2**	OCSP를 통해 인증서 해지 구성, 160 페이지	시스템이 만료된 인증서를 자동으로 취소하도록 OCSP를 구성합니다.

인증서 모니터 알림 구성

Unified Communications Manager 또는 IM and Presence Service에 대한 자동화된 인증서 모니터링을 구성합니다. 시스템은 인증서 상태를 주기적으로 확인하고 인증서의 만료가 다가오면 사용자에게 전자 메일을 보냅니다.

참고 **Cisco** 인증서 만료 모니터 네트워크 서비스가 실행 중이어야 합니다. 이 서비스는 기본적으로 활성화되어 있지만 도구 > 제어 센터 - 네트워크 서비스를 선택하고 **Cisco** 인증서 만료 모니터 서비스 상태가 실행 중인지 확인하여 Cisco 통합 서비스 가용성에서 서비스가 실행 중인지 확인할 수 있습니다.

프로시저

단계 **1** Cisco Unified OS 관리(Unified Communications Manager 인증서 모니터링의 경우) 또는 Cisco Unified IM and Presence 관리(IM and Presence Service 인증서 모니터링의 경우)에 로그인합니다.

단계 **2** 보안 > 인증서 모니터를 선택합니다.

단계 **3** 알림 시작 시간 필드에 숫자 값을 입력합니다. 이 값은 시스템이 만료 예정을 통지하기 시작한 인증서 만료 전 일 수를 나타냅니다.

단계 **4** 알림 빈도 필드에 알림 빈도를 입력합니다.

단계 **5** (선택 사항) 시스템이 예정된 인증서 만료에 대한 전자 메일 알림을 보내도록 하려면 전자 메일 알림 활성화 확인란을 선택합니다.

단계 **6** 인증서 상태 검사에 LSC 인증서를 포함시키려면 **LSC** 모니터링 활성화 확인란을 선택합니다.

단계 **7** 전자 메일 **ID** 필드에 시스템에서 알림을 보낼 전자 메일 주소를 입력합니다. 세미콜론으로 구분하여 여러 개의 전자 메일 주소를 입력할 수 있습니다.

단계 **8** 저장을 클릭합니다.

참고 인증서 모니터 서비스는 기본적으로 24시간 마다 실행됩니다. 인증서 모니터 서비스를 다시 시작하면 서비스를 시작한 다음 24시간 후에만 실행되도록 다시 일정을 계산합니다. 간격은 인증서가 만료일 7일 전까지도 변경되지 않습니다. 인증서가 만료되었거나 만료 1일 전이 되면 1시간 마다 실행됩니다.

다음에 수행할 작업

시스템이 만료된 인증서를 자동으로 취소하도록 OCSP(온라인 인증서 상태 프로토콜)를 구성합니다. 자세한 내용은 OCSP를 통해 인증서 해지 구성, 160 페이지을 참조하십시오.

OCSP를 통해 인증서 해지 구성

OCSP(온라인 인증서 상태 프로토콜)를 사용하여 인증서 상태를 정기적으로 확인하고 만료된 인증서를 자동으로 해지할 수 있습니다.

시작하기 전에

시스템에 OCSP 검사에 필요한 인증서가 있는지 확인하십시오. OCSP 응답 특성으로 구성된 루트 또는 중간 CA 인증서를 사용하거나 tomcat-trust에 업로드된 지정된 OCSP 서명 인증서를 사용할 수 있습니다.

프로시저

단계 **1** Cisco Unified OS 관리(Unified Communications Manager 인증서 해지의 경우) 또는 Cisco Unified IM and Presence 관리(IM and Presence Service 인증서 해지의 경우)에 로그인합니다.

단계 **2** 보안 > 인증서 해지를 선택합니다.

단계 **3** **OCSP** 활성화 확인란을 선택하고 다음 작업 중 하나를 수행합니다.

- OCSP 확인을 위해 OCSP 응답자를 지정하려면 구성된 **OCSP URI** 사용 버튼을 선택하고 **OCSP**가 구성된 **URI** 필드에 응답자의 URI를 입력합니다.
- 인증서가 OCSP 응답자 URI로 구성된 경우 인증서에서 **OCSP URI** 사용 버튼을 선택합니다.

단계 **4** 해지 확인 활성화 확인란을 선택합니다.

단계 **5** 해지 확인을 위한 간격 기간과 함께 모두 확인 필드를 완료합니다.

단계 **6** 저장을 클릭합니다.

단계 **7** (선택 사항) CTI, IPsec 또는 LDAP 링크가있는 경우 수명이 긴 연결에 OCSP 해지 지원을 활성화하려면 위의 단계 외에도 다음 단계를 완료해야 합니다.

a) [Cisco Unified CM 관리]에서 시스템 > 엔터프라이즈 파라미터를 선택합니다.

b) 인증서 해지 및 만료 아래에서 인증서 유효성 확인 파라미터를 **True**로 설정합니다.

c) 유효성 확인 빈도 파라미터에 대한 값을구성합니다.

참고 인증서 해지 창의 해지 확인 활성화 파라미터의 간격 값은 유효성 확인 빈도 엔터프라이즈 파라미터의 값보다 우선합니다.

d) 저장을 클릭합니다.

13 장

보안 설정 구성

보안 개요

이 장에는 IM and Presence 서비스의 보안 설정을 구성하는 절차가 포함되어 있습니다. IM and Presence 서비스에서 보안 TLS 연결을 구성하고 FIPS 모드와 같은 향상된 보안 설정을 활성화할 수 있습니다.

IM and Presence 서비스는 Cisco Unified Communications Manager와 플랫폼을 공유합니다. Cisco Unified Communications Manager에서 보안을 구성하는 방법에 대한 자세한 내용은 *Cisco Unified Communications Manager* 보안 설명서를 참조하십시오.

보안 설정 구성 작업 흐름

IM and Presence 서비스로 보안을 설정하려면 이 선택적 작업을 완료하십시오.

프로시저

	명령 또는 동작	목적
단계 **1**	로그인 배너 만들기, 164 페이지	IM and Presence 서비스 인터페이스에 로그인할 때 사용자가 확인해야 하는 로그인 배너를 만듭니다.
단계 **2**	보안 XMPP 연결 구성 , 164 페이지	XMPP 보안을 구성하려면 이 작업을 완료하십시오.
단계 **3**	TLS 피어 주체 구성, 165 페이지	TLS 피어를 설정하려면 이 작업을 구성하십시오.
단계 **4**	TLS 컨텍스트 구성, 166 페이지	TLS 피어에 대한 TLS 컨텍스트 및 TLS 암호를 구성합니다.

	명령 또는 동작	목적
단계 **5**	FIPS 모드, 167 페이지	구축이 FIPS와 호환되도록 하려면 FIPS 모드를 활성화할 수 있습니다. 보안을 강화하기 위해 향상된 보안 모드 및 일반 준수 모드를 활성화할 수도 있습니다.

로그인 배너 만들기

사용자가 IM and Presence 서비스 인터페이스에 로그인할 때 표시되는 배너를 만들 수 있습니다. 텍스트 편집기를 사용하여 .txt 파일을 만들고, 사용자에게 전달할 중요한 알림을 포함하고, Cisco Unified IM and Presence OS 관리 페이지에 업로드하면 됩니다.

이 배너는 모든 IM and Presence 서비스 인터페이스에 표시되어, 사용자가 로그인하기 전에 법적 고지 사항을 비롯한 중요한 정보를 알립니다. 사용자가 로그인하기 전에 Cisco Unified CM IM and Presence 관리, Cisco Unified IM and Presence Operating System 관리, Cisco Unified IM and Presence 서비스 가용성, Cisco Unified IM and Presence 보고, IM and Presence 재해 복구 시스템 등의 인터페이스에 이 배너가 표시됩니다.

프로시저

단계 **1** .txt 파일을 만들고 배너에 표시할 내용을 작성합니다.

단계 **2** Cisco Unified IM and Presence Operating System 관리에 로그인합니다.

단계 **3** 소프트웨어 업그레이드 > 사용자 정의 로그온 메시지를 선택합니다.

단계 **4** 찾아보기를 클릭하여 .txt 파일을 찾습니다.

단계 **5** 파일 업로드를 클릭합니다.

대부분의 IM and Presence 서비스 인터페이스에서 로그인 전후에 배너가 나타납니다.

참고 각 IM and Presence 서비스 노드에 .txt 파일을 별도로 업로드해야 합니다.

보안 **XMPP** 연결 구성

이 절차를 사용하여 TLS를 사용하여 보안 XMPP 연결을 활성화하십시오.

프로시저

단계 **1** Cisco Unified CM IM and Presence 관리에서 시스템 > 보안 > 설정을 선택합니다.

단계 **2** 다음 XMPP 보안 설정을 활성화하려면 해당 확인란을 선택하십시오.

표 *19: IM and Presence* 서비스에 대한 *XMPP* 보안 설정

설정	설명
IM/P 서비스 보안 모드에 대해 XMPP 클라이언트 활성화	이 기능을 활성화하면 IM and Presence 서비스가 클러스터의 XMPP 클라이언트 애플리케이션과의 보안 TLS 연결을 설정합니다. 이 설정은 기본적으로 활성화됩니다. XMPP 클라이언트 애플리케이션이 비보안 모드에서 클라이언트 로그인 자격 증명을 보호할 수 없다면 이 보안 모드를 해제하지 않는 것이 좋습니다. 보안 모드를 해제하는 경우 다른 방식으로 XMPP 클라이언트-노드 통신을 보호할 수 있는지 확인하십시오.
XMPP 라우터 대 라우터 보안 모드 활성화	이 설정을 활성화하면 IM and Presence 서비스는 동일한 클러스터 또는 다른 클러스터의 XMPP 라우터 간에 TLS 보안 연결을 설정합니다. IM and Presence 서비스는 클러스터 내부와 클러스터 간에 XMPP 인증서를 XMPP 신뢰 인증서로서 자동 복제합니다. XMPP 라우터는 동일한 클러스터 또는 다른 클러스터에 있으며 TLS 연결 설정이 가능한 다른 XMPP 라우터와 TLS 연결을 설정하려고 시도합니다.
IM/P 서비스 보안 모드에 대해 웹 클라이언트 활성화	이 설정을 활성화하면 IM and Presence 서비스는 IM and Presence 서비스 노드와 XMPP 기반 API 클라이언트 애플리케이션 간에 TLS 보안 연결을 설정합니다. 이 설정을 사용하는 경우 IM and Presence 서비스의 cup-xmpp-trust 저장소에 웹 클라이언트용 인증서 또는 서명 인증서를 업로드하십시오.

단계 **3** 저장을 클릭합니다.

다음에 수행할 작업

IM/P 서비스 보안 모드에 대해 **XMPP** 클라이언트 활성화 설정을 업데이트한 경우 Cisco XCP Connection Manager를 다시 시작합니다.

IM and Presence 서비스에서 SIP 보안 설정 구성

TLS 피어 주체 구성

IM and Presence 서비스 인증서 가져오기가 완료되면 IM and Presence 서비스는 자동으로 TLS 피어 주체를 TLS 피어 주체 목록 및 TLS 컨텍스트 목록에 추가하려고 시도합니다. TLS 피어 주체 및 TLS 컨텍스트 구성이 요구 사항에 맞게 설정되었는지 확인하십시오.

프로시저

단계 **1** **Cisco Unified CM IM and Presence** 관리에서 시스템 > 보안 > **TLS** 피어 주체를 선택합니다.

단계 **2** 새로 추가를 클릭합니다.

단계 **3** 피어 주체 이름에 대해 다음 작업 중 하나를 수행합니다.

a) 노드가 제공하는 인증서의 주체 CN을 입력합니다.

b) 인증서를 열고 CN을 찾아 여기에 붙여 넣습니다.

단계 **4** 설명 필드에 노드의 이름을 입력합니다.

단계 **5** 저장을 클릭합니다.

다음에 수행할 작업

계속 진행하여 TLS 컨텍스트를 구성합니다.

TLS 컨텍스트 구성

이 절차를 사용하여 TLS 컨텍스트와 TLS 암호를 TLS 피어 주체에 할당합니다.

참고 IM and Presence 서비스 인증서 가져오기가 완료되면 IM and Presence 서비스는 자동으로 TLS 피어 주체를 TLS 피어 주체 목록 및 TLS 컨텍스트 목록에 추가하려고 시도합니다.

시작하기 전에

TLS 피어 주체 구성, 165 페이지

프로시저

단계 **1** **Cisco Unified CM IM and Presence** 관리에서 시스템 > 보안 > **TLS** 컨텍스트 구성을 선택합니다.

단계 **2** 찾기를 클릭합니다.

단계 **3** **Default_Cisco_UPS_SIP_Proxy_Peer_Auth_TLS_Context**를 선택합니다.

단계 **4** 사용 가능한 TLS 피어 주체의 목록에서 자신이 구성한 TLS 피어 주체를 선택합니다.

단계 **5** > 화살표를 사용하여 이 TLS 피어 주체를 선택한 **TLS** 피어 주체로 이동합니다.

단계 **6** **TLS** 암호화 매핑 옵션을 구성합니다.

a) 사용 가능한 **TLS** 암호 및 선택한 **TLS** 암호 상자에서 사용할 수 있는 TLS 암호화 목록을 검토합니다.

b) 현재 선택되지 않은 TLS 암호를 활성화하려면 > 화살표를 사용하여 암호를 선택한 **TLS** 암호로 이동합니다.

단계 **7** 저장을 클릭합니다.

단계 **8** Cisco SIP Proxy 서비스를 다시 시작합니다.

a) Cisco Unified IM and Presence 서비스 가용성에서 도구 > 제어 센터 - 기능 서비스를 선택합니다.

b) 서버 드롭다운 목록 상자에서 IM and Presence 서비스 클러스터 노드를 선택하고 이동을 클릭합니다.

c) **Cisco SIP Proxy** 서비스를 선택하고 다시 시작을 클릭합니다.

FIPS 모드

IM and Presence 서비스에는 시스템이 암호화, 데이터와 신호 암호화 및 감사 로깅과 같은 항목과 관련된 보다 엄격한 보안 지침 및 위험 관리 제어에서 작동할 수 있도록 하는 향상된 시스템 보안 모드 세트가 포함되어 있습니다

- FIPS 모드 - IM and Presence 서비스는 FIPS 모드에서 작동하도록 구성할 수 있습니다. FIPS 모드는 미국 및 캐나다 정부의 암호화 모듈 표준인 FIPS 또는 연방 정보 처리 표준을 준수합니다.
- 향상된 보안 모드 - 향상된 보안 모드는 FIPS 지원 시스템에서 실행되며 데이터 암호화 요구 사항, 엄격한 자격 증명 정책, 연락처 검색에 대한 사용자 인증 및 보다 엄격한 감사 로깅 요구 사항과 같은 추가 위험 관리 제어 기능을 제공합니다.
- 공통 기준 모드 - 공통 기준 모드는 시스템이 TLS 및 X.509 v3 인증서 사용과 같은 공통 기준 지침을 준수할 수 있도록 하는 추가 제어 기능을 제공하는 FIPS 지원 시스템에서도 실행됩니다.

참고 외부 데이터베이스가 MSSQL인 경우 메시지 아카이버, 텍스트 전화 회의 관리자 및 파일 전송 관리자와 같은 서비스가 일반 기준 모드에서 작동하려면 다음을 수행해야 합니다.

1. TLS 1.1 이상을 지원하도록 MSSQL 데이터베이스를 호스팅하는 서버를 구성합니다.
2. IM and Presence 서비스에 데이터베이스 인증서를 다시 업로드합니다.
3. 외부 데이터베이스 구성 페이지에서 **SSL** 활성화 확인란을 선택합니다. **Cisco Unified CM IM and Presence** 관리 > 메시징 > 외부 서버 설정 > 외부 데이터베이스를 선택하여 외부 데이터베이스를 구성합니다.

Cisco Unified Communicatiosn Manager 및 IM and Presence 서비스에서 FIPS 모드, 보안 강화 모드 및 공통 기준 모드를 활성화하는 방법에 대한 자세한 내용은 https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html 에서 *Cisco Unified Communications Manager* 보안 설명서의 "FIPS 모드 설정" 장을 참조하십시오.

Microsoft Outlook 일정 통합용 FIPS

IM and Cisco Presence 서비스 서버에서 FIPS 모드가 활성화된 경우 Exchange 웹 서비스 정보를 가져올 수 있도록 NTLMv2만 지원됩니다. FIPS 모드가 비활성화된 경우 NTLMv1과 NTLMv2 모두 기존 동작에 따라 지원됩니다. 기본 인증은 FIPS 모드를 활성화 또는 비활성화하는 것과 관계 없이 두 경우 모두 지원됩니다.

Microsoft Outlook 일정 통합 기능을 통해 Exchange Server와의 연결을 설정하기 위해 프레즌스 엔진에서 사용하는 인증 유형을 확인하기 위해 **FIPS** 모드 **Exchange Server** 인증이라는 프레즌스 엔진 서비스에 대한 새 서비스 매개 변수가 도입되었습니다.

FIPS 모드 **Exchange Server** 인증 서비스 매개 변수를 자동 또는 기본 전용으로 설정할 수 있습니다.

자동으로 설정된 서비스 매개 변수: 프레즌스 엔진이 NTLMv2를 먼저 협상하고 NTLMv2 협상이 실패할 경우에만 "기본 인증"으로 대체합니다. NTLMv1는 FIPS 모드에서 협상되지 않습니다.

기본 전용으로 설정된 서비스 매개 변수: Exchange Server가 NTLM 및 기본 인증을 모두 허용하도록 구성되어 있더라도 프레즌스 엔진은 강제로 "기본 인증"을 사용합니다.

참고 서비스 매개 변수 설정을 변경하면 Cisco 프레즌스 엔진을 다시 시작해야 합니다.

14 장

인터클러스터 피어 구성

인터클러스터 피어링 개요

인터클러스터 피어링은 한 클러스터 내의 사용자가 동일한 도메인 내의 다른 클러스터에 있는 사용자의 프레즌스에 가입하고 통신할 수 있는 기능을 제공합니다. 대규모 구축의 경우 인터클러스터 피어링을 사용하여 원격 IM and Presence 클러스터를 연결할 수 있습니다.

인터클러스터 피어링은 로컬 및 원격 클러스터의 데이터베이스 게시자 노드에서 구성됩니다.

클러스터 간 구축을 위한 크기 조정 및 성능 권장 사항은 http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/uc_system/design/guides/UCgoList.html#48016에서 제공되는 *Cisco Collaboration System* 솔루션 참조 네트워크 설계*(SRND)*의 "협업 인스턴트 메시징 및 프레즌스" 장을 참조하십시오.

인터클러스터 피어 필수 조건

네트워크에서 IM and Presence 서비스 인터클러스터 피어를 구성하기 전에 다음에 유의하십시오.

- 시스템 토폴로지를 구성하고 필요에 따라 모든 클러스터에 대해 사용자를 할당합니다.
- 인터클러스터 피어 연결이 제대로 작동하려면 두 클러스터 사이에 방화벽이 있는 경우 다음 포트를 열어 두어야 합니다.
  - 8443 (AXL)
  - 7400 (XMPP)
  - 5060 (SIP) (SIP 페더레이션을 사용 중인 경우만 해당)

- 클러스터 간 구축의 경우에는 최소 15000 사용자의 OVA를 구축해야 합니다. 모든 클러스터가 최소 15,000 사용자 OVA를 실행하는 한 서로 다른 OVA 크기를 실행하는 다른 클러스터를 가질 수 있습니다.

참고 IM and Presence 서비스를 Cisco Business Edition 6000 서버에 구축하는 경우 인터클러스터 피어가 지원되지 않습니다.

인터클러스터 피어 구성 작업 흐름

프로시저

	명령 또는 동작	목적
단계 **1**	사용자 프로비저닝 확인, 171 페이지	인터클러스터 피어를 구성하기 전에 최종 사용자가 올바르게 프로비전되었는지 확인합니다.
단계 **2**	Cisco AXL 웹 서비스 활성화, 171 페이지	Cisco AXL 웹 서비스는 모든 로컬 및 원격 IM and Presence 노드에서 활성화되어 있어야 합니다. 서비스가 실행 중인지 확인하려면 이 절차를 사용하십시오.
단계 **3**	동기화 에이전트 활성화, 172 페이지	각 인터클러스터 피어의 데이터베이스 게시자 노드에서 동기화 에이전트를 활성화합니다.
단계 **4**	인터클러스터 피어 구성, 172 페이지	인터클러스터 피어를 설정하려면 각 클러스터의 데이터베이스 게시자 노드에서 이 작업을 완료합니다.
단계 **5**	클러스터 간 동기화 에이전트가 켜져 있는지 확인, 174 페이지	클러스터 간 동기화 에이전트가 IM and Presence 서비스 클러스터의 모든 노드에서 실행 중이어야 합니다. 클러스터 간 동기화 에이전트 파라미터가 실행 중인지 확인하려면 이 절차를 사용하십시오.
단계 **6**	인터클러스터 피어 상태 확인, 175 페이지	인터클러스터 피어 구성이 작동하는지 확인합니다.
단계 **7**	클러스터 간 동기화 에이전트 Tomcat 신뢰 인증서 업데이트, 176 페이지	인터클러스터 피어의 tomcat 인증서가 동기화되지 않은 상태이면 Tomcat 신뢰 인증서를 업데이트합니다.

	명령 또는 동작	목적
단계 **8**	인터클러스터 피어 주기적 동기화 실패에 대한 자동 복구 활성화, 176 페이지	이 절차를 사용하여 클러스터 간 주기적 동기화 실패에 대한 자동 복구를 활성화합니다.
단계 **9**	인터클러스터 피어 동기화 간격 구성, 177 페이지	이 절차를 사용하여 인터클러스터 피어 동기화에 대한 시간 간격을 설정합니다.
단계 **10**	인터클러스터 피어 주기적 동기화에 대한 인증서 동기화 비활성화, 177 페이지	이 절차를 사용하여 클러스터 간 주기적 동기화의 일부로 인증서 동기화의 비활성화/활성화를 구성합니다.

사용자 프로비저닝 확인

이 절차를 사용하여 인터클러스터 피어를 구성하기 전에 최종 사용자가 올바르게 프로비전되었는지 확인합니다.

프로시저

단계 **1** Cisco Unified CM IM and Presence 관리에서 진단 > 시스템 문제 해결 도구를 선택합니다.
시스템 문제 해결 도구가 실행됩니다.

단계 **2** 사용자 문제 해결 도구 섹션에서 최종 사용자가 올바르게 프로비저닝되고 중복되거나 유효하지 않은 사용자가 없는지 확인합니다.

다음에 수행할 작업

Cisco AXL 웹 서비스 활성화, 171 페이지

Cisco AXL 웹 서비스 활성화

Cisco AXL 웹 서비스는 모든 로컬 및 원격 IM and Presence 클러스터 노드에서 실행되고 있어야 합니다. 기본적으로 이 서비스는 실행 중입니다. 그러나 이 절차를 사용하여 이 서비스가 실행 중인지 확인할 수 있습니다.

참고 Cisco AXL 웹 서비스를 활성화하면 AXL 권한이 있는 클러스터 간 애플리케이션 사용자가 생성됩니다. 원격 IM and Presence 서비스 노드에 인터클러스터 피어를 구성할 때 클러스터 간 애플리케이션 사용자의 사용자 이름과 암호가 필요합니다.

프로시저

단계 **1** Cisco Unified IM and Presence 서비스 가용성에서 도구 > 제어 센터 - 기능 서비스를 선택합니다.

단계 **2** 서버 목록에서 서비스를 다시 활성화할 노드를 선택하고 이동을 클릭합니다.

단계 **3** 데이터베이스 및 관리 서비스 영역에서 **Cisco AXL** 웹 서비스의 상태를 확인합니다.

- 서비스가 시작됨인 경우 작업이 필요하지 않습니다.
- 서비스가 실행 중이 아님인 경우 서비스를 선택하고 다시 시작을 클릭합니다.

단계 **4** 로컬 및 원격 클러스터의 모든 클러스터 노드에서 이 절차를 반복합니다.

다음에 수행할 작업

동기화 에이전트 활성화, 172 페이지

동기화 에이전트 활성화

Cisco 동기화 에이전트는 로컬 및 원격 IM and Presence 데이터베이스 게시자 노드에서 각 인터클러스터 피어의 데이터베이스 게시자 노드에서 실행되어야 합니다.

프로시저

단계 **1** Cisco Unified IM and Presence 서비스 가용성에서 도구 > 제어 센터 - 네트워크 서비스를 선택합니다.

단계 **2** 서버 드롭다운 목록 상자에서 IM and Presence 데이터베이스 게시자 노드를 선택하고 이동을 클릭합니다.

단계 **3** **IM and Presence** 서비스 아래에서 **Cisco** 동기화 에이전트 상태가 실행 중인지 확인합니다.

단계 **4** 서비스가 실행 중이 아님인 경우 서비스를 선택하고 다시 시작을 클릭합니다.

단계 **5** 각 클러스터에서 이 절차를 반복합니다.

다음에 수행할 작업

Cisco 동기화 에이전트가 Cisco Unified Communications Manager에서 사용자 동기화를 완료한 후,인터클러스터 피어 구성, 172 페이지

인터클러스터 피어 구성

인터클러스터 피어 관계를 설정하려면 로컬 및 원격 클러스터 모두에 대해 데이터베이스 게시자 노드에서 이 절차를 사용하십시오.

시작하기 전에

- 로컬 및 원격 클러스터의 Cisco Unified Communications Manager에서 동기화 에이전트가 사용자 동기화를 완료했는지 확인합니다. 동기화 에이전트가 사용자 동기화를 완료하기 전에 인터클러스터 피어 연결을 구성하는 경우, 클러스터간 피어 연결의 상태가 실패로 표시됩니다.
- 원격 IM and Presence 서비스 노드에서 클러스터 간 애플리케이션 사용자의 AXL 사용자 이름과 암호를 준비합니다.

프로시저

단계 **1** Cisco Unified CM IM and Presence 관리에서 프레즌스 > 클러스터 간을 선택합니다.

단계 **2** 새로 추가를 클릭합니다.

단계 **3** 피어 주소 필드에 원격 클러스터 데이터베이스 게시자 노드의 노드 이름을 입력합니다. 이 필드는 IP 주소, 호스트 이름 또는 FQDN일 수 있지만 서버를 정의하는 실제 노드 이름과 일치해야 합니다.

참고
- 노드 이름이 사용하는 주소 유형을 확인하려면 원격 클러스터의 Cisco Unified CM IM and Presence 관리에 로그인하고 시스템 > 프레즌스 토폴로지를 선택합니다. 이 창은 각 클러스터 노드의 노드 이름과 서버 세부 사항을 표시합니다.
- 다중 클러스터 환경에 속하는 클러스터에서 스플릿 브레인 시나리오가 발생할 수 있습니다. 예를 들어, 클러스터 A가 있고 해당 다중 클러스터 피어는 클러스터 B, C, D 및 E입니다. 클러스터 A의 노드는 스플릿 브레인 시나리오 중 다중 클러스터 환경에서 다른 클러스터 B, C, D 및 E와 통신해야 하므로 스플릿 브레인 시나리오에서 DNS에 연결할 수 있어야 합니다.

  스플릿 브레인 시나리오에서 클러스터 A의 노드가 DNS에 연결할 수 없는 경우 A, B, C, D 및 E 클러스터 노드의 IP 주소는 호스트 이름과 FQDN이 아닌 노드 이름으로 설정되어야 합니다.

  클러스터 A, B, C, D 및 E의 노드가 FQDN이나 호스트 이름을 사용하여 정의되고 스플릿 브레인 시나리오에서 DNS에 연결할 수 없는 경우, 클러스터 A와 B, C, D, E 사이에 IM Presence 업데이트 손실과 IM 기록 손실이 발생하는 등의 서비스 중단이 발생합니다.

단계 **4** AXL 자격 증명을 입력합니다.

단계 **5** SIP 통신의 기본 프로토콜을 선택합니다.

참고 Cisco에서는 모든 IM and Presence 서비스 클러스터에서 클러스터 간 트렁크 전송 유형으로 **TCP**(기본 설정)를 사용할 것을 권장합니다. 이 구성이 네트워크 구성 및 보안 요구 사항에 적합한 경우 이 설정을 변경할 수 있습니다.

단계 **6** 저장을 클릭합니다.

단계 **7** GUI 헤더의 오른쪽 상단에 있는 알림을 확인합니다. **Cisco XCP** 라우터를 다시 시작하라는 알림 메시지가 표시되면 다음을 수행하십시오. 그렇지 않은 경우 이 단계를 생략할 수 있습니다.

a) Cisco Unified IM and Presence 서비스 가용성에서 도구 > 제어 센터 - 네트워크 서비스를 선택합니다.
b) 서버 드롭다운 목록 상자에서 IM and Presence 노드를 선택하고 이동을 클릭합니다.
c) **Cisco XCP** 라우터를 선택하고 다시 시작을 클릭합니다.
d) 모든 클러스터 노드에 대해 이 단계를 반복합니다.

단계 **8** 각 원격 피어 클러스터의 데이터베이스 게시자 노드에서 이 절차를 반복합니다.

팁 클러스터 간 전송 프로토콜로 **TLS**를 선택하면 IM and Presence 서비스는 자동으로 안전한 TLS 연결을 설정하기 위해 인터클러스터 피어 사이에서 인증서를 교환하려고 시도합니다. IM and Presence 서비스는 인증서 교환의 성공 여부를 인터클러스터 피어 상태 섹션에 표시합니다.

다음에 수행할 작업

클러스터 간 동기화 에이전트가 켜져 있는지 확인, 174 페이지

XCP 라우터 서비스 다시 시작

로컬 클러스터의 모든 노드는 물론 원격 클러스터의 모든 노드에서 Cisco XCP 라우터 서비스 다시 시작.

시작하기 전에

인터클러스터 피어 구성, 172 페이지

프로시저

단계 **1** Cisco Unified IM and Presence 서비스 가용성에서 도구 > 제어 센터 - 네트워크 서비스를 선택합니다.
단계 **2** 서버 목록에서 서비스를 다시 활성화할 노드를 선택하고 이동을 클릭합니다.
단계 **3** **IM and Presence** 서비스 영역에서 **Cisco XCP** 라우터를 선택합니다.
단계 **4** 재시작을 클릭합니다.

다음에 수행할 작업

클러스터 간 동기화 에이전트가 켜져 있는지 확인, 174 페이지

클러스터 간 동기화 에이전트가 켜져 있는지 확인

클러스터 간 동기화 에이전트 네트워크 서비스는 인터클러스터 피어 간에 사용자 정보를 동기화합니다. 이 절차를 사용하여 서비스가 각 인터클러스터 피어의 모든 클러스터 노드에서 실행되고 있는지 확인하십시오.

프로시저

단계 **1** Cisco Unified IM and Presence 서비스 가용성에서 도구 > 제어 센터 - 네트워크 서비스를 선택합니다.
단계 **2** 서버 메뉴에서 IM and Presence 노드를 선택하고 이동을 클릭합니다.
단계 **3** **Cisco** 클러스터 간 동기화 에이전트의 상태가 실행 중을 표시하는지 확인합니다.
단계 **4** 서비스가 실행 중이 아니면 서비스를 선택하고 시작을 클릭합니다.
단계 **5** 각 인터클러스터 피어의 모든 클러스터 노드에 대해 이 절차를 반복합니다.

다음에 수행할 작업

인터클러스터 피어 상태 확인, 175 페이지

인터클러스터 피어 상태 확인

이 절차를 사용하여 인터클러스터 피어 구성이 제대로 작동하는지 확인합니다.

프로시저

단계 **1** **Cisco Unified CM IM and Presence** 관리에서 프레즌스 > 클러스터 간을 선택합니다.
단계 **2** 검색 기준 메뉴에서 피어 주소를 선택합니다.
단계 **3** 찾기를 클릭합니다.
단계 **4** 인터클러스터 피어 상태 창에서:
a) 인터클러스터 피어의 각 결과 항목 옆에 확인 표시가 있는지 확인합니다.
b) 연결된 사용자 값이 원격 클러스터에 있는 사용자의 수와 같은지 확인합니다.
c) 클러스터 간 투명 프로토콜로 **TLS**를 선택하면 **CertificateStatus** 항목은 TLS 연결의 상태를 표시하며, IM and Presence 서비스가 클러스터 간에 보안 인증서를 성공적으로 교환했는지를 나타냅니다. 인증서가 동기화되지 않은 경우 tomcat-trust 인증서를 수동으로 업데이트해야 합니다(이 모듈에서 설명한 대로). 다른 인증서 교환 오류의 경우 권장 작업에 대한 온라인 도움말을 확인하십시오.
단계 **5** 시스템 문제 해결 도구 실행.
a) Cisco Unified CM IM and Presence 관리에서 진단 > 시스템 문제 해결 도구를 선택합니다.
b) 클러스터 간 문제 해결 도구 섹션에서 각 인터클러스터 피어 연결 항목의 상태 옆에 확인 표시가 있는지 확인합니다.

다음에 수행할 작업

클러스터 간 동기화 에이전트 Tomcat 신뢰 인증서 업데이트, 176 페이지

클러스터 간 동기화 에이전트 **Tomcat** 신뢰 인증서 업데이트

로컬 클러스터에서 연결 오류가 발생하고 손상된 Tomcat 신뢰 인증서가 원격 클러스터와 연결된 경우 이 절차를 사용하여 Tomcat 신뢰 인증서를 업데이트합니다.

인터클러스터 피어의 tomcat 인증서가 동기화되지 않은 상태이면 Tomcat 신뢰 인증서를 업데이트해야 합니다. 클러스터 간 구축에서, 기존의 인터클러스터 피어 구성을 다시 사용해 새 원격 클러스터를 가리키는 경우 이 오류가 발생할 수 있습니다. 이 오류는 새로운 IM and Presence 서비스 설치 시에, IM and Presence 서비스 호스트 또는 도메인 이름을 변경하는 경우 또는 Tomcat 인증서를 다시 생성하는 경우에도 발생할 수 있습니다.

프로시저

단계 **1** **Cisco Unified CM IM and Presence** 관리에서 프레즌스 > 클러스터 간을 선택합니다.

단계 **2** 강제 동기화를 클릭하여 인증서를 원격 클러스터와 동기화합니다.

단계 **3** 표시되는 확인 창에서 피어의 **Tomcat** 인증서도 재동기화를 선택합니다.

단계 **4** 확인을 클릭합니다.

참고 자동으로 동기화되지 않은 인증서가 있는 경우 인터클러스터 피어 구성 창으로 이동합니다. X로 표시된 모든 인증서는 수동으로 복사해야 하는 누락된 인증서입니다.

인터클러스터 피어 주기적 동기화 실패에 대한 자동 복구 활성화

클러스터 간 동기화의 주기적 동기화가 2시간 이상 지속되면 Cisco 클러스터 간 동기화 에이전트에서 "InterClusterSyncAgentPeerPeriodicSyncingFailure" 경보를 발생시키고 자동으로 다시 시작하도록 하려면 이 절차를 사용하여 이 서비스 파라미터를 활성화하십시오.

프로시저

단계 **1** **Cisco Unified CM IM and Presence** 관리에서 시스템 > 서비스 파라미터를 선택합니다.

단계 **2** 서버 목록에서 “일반 클러스터 간 동기화 에이전트 파라미터”를 설정할 IM and Presence 노드를 선택합니다.

단계 **3** 서비스 목록에서 **Cisco** 클러스터 간 동기화 에이전트**(**활성**)**를 선택합니다.

단계 **4** 인터클러스터 피어 주기적 동기화 실패에 대한 자동 복구 활성화 서비스 파라미터를 활성화됨으로 설정합니다.

단계 **5** 저장을 클릭합니다.

참고 "인터클러스터 피어 주기적 동기화 실패에 대한 자동 복구 활성화" 서비스 파라미터가 활성화됨으로 설정되어 있고 주기적 동기화가 2시간 이상 지속된 경우:

- ***InterClusterSyncAgentPeerPeriodicSyncingFailure*** 경보가 생성됩니다.
- ***Cisco*** 클러스터 간 동기화 에이전트 서비스가 자동으로 다시 시작됩니다.

"인터클러스터 피어 주기적 동기화 실패에 대한 자동 복구 활성화"가 비활성화된 경우:

- ***InterClusterSyncAgentPeerPeriodicSyncingFailure*** 경보가 생성됩니다.
- ***Cisco*** 클러스터 간 동기화 에이전트 서비스가 자동으로 다시 시작되지 않습니다.

인터클러스터 피어 동기화 간격 구성

이 절차를 사용하여 인터클러스터 피어 동기화에 대한 시간 간격을 설정합니다. 인터클러스터 피어 주기적 동기화 간격**(**분**)** 서비스 파라미터를 사용하여 동적 ICSA 주기적 동기화에 대한 시간 간격을 구성할 수 있습니다. 인터클러스터 피어 동기화 간격의 기본 설정은 30분입니다.

프로시저

단계 **1** **Cisco Unified CM IM and Presence** 관리에서 시스템 > 서비스 파라미터를 선택합니다.

단계 **2** 서버 목록에서 "일반 클러스터 간 동기화 에이전트 파라미터"를 설정할 IM and Presence 노드를 선택합니다.

단계 **3** 서비스 목록에서 **Cisco** 클러스터 간 동기화 에이전트**(**활성**)**를 선택합니다.

단계 **4** 인터클러스터 피어 주기적 동기화 간격**(**분**)** 서비스 파라미터를 원하는 간격으로 설정합니다. 범위는 30 ~ 1444이고 기본값은 30분입니다.

단계 **5** 저장을 클릭합니다.

참고 새 설정은 다음 클러스터 간 동기화 후에 적용됩니다.

인터클러스터 피어 동기화가 실패하면 4개의 동기화 기간이 완료될 때까지 Cisco 클러스터 간 동기화 에이전트 서비스가 다시 시작됩니다. 예를 들어, 파라미터가 40분으로 설정된 경우 160분(4*40) 후에 서비스가 다시 시작됩니다.

인터클러스터 피어 주기적 동기화에 대한 인증서 동기화 비활성화

이 절차를 사용하여 클러스터 간 동기화 프로세스의 일부로 인증서 동기화를 비활성화할 수 있습니다. 서비스 파라미터 클러스터 간 주기적 동기화 중 인증서 동기화를 사용하면 관리자가 클러스터 간 주기적 동기화의 일부로 인증서 동기화를 비활성화하거나 활성화할 수 있습니다. 이 서비스 파라미터의 기본값은 인증서 동기화를 수행하는 것입니다.

프로시저

단계 **1** **Cisco Unified CM IM and Presence** 관리에서 시스템 > 서비스 파라미터를 선택합니다.

단계 **2** 서버 목록에서 일반 클러스터 간 동기화 에이전트 파라미터를 설정할 IM and Presence 노드를 선택합니다.

단계 **3** 서비스 목록에서 **Cisco** 클러스터 간 동기화 에이전트**(**활성**)**를 선택합니다.

단계 **4** 서비스 파라미터 클러스터 간 주기적인 동기화 중 인증서 동기화를 인증서 동기화를 수행하지 않음으로 설정합니다.

단계 **5** 저장을 클릭합니다.

참고 클러스터 간 주기적 동기화 중 인증서 동기화와 관련된 성능 저하 또는 높은 CPU 스파이크가 발생하는 경우 이 절차를 사용하여 서비스 파라미터를 설정할 수 있습니다.

인터클러스터 피어 연결 삭제

인터클러스터 피어 관계를 제거하려면 이 절차를 사용합니다.

프로시저

단계 **1** IM and Presence 서비스 데이터베이스 게시자 노드에 로그인합니다.

단계 **2** Cisco Unified CM IM and Presence 관리에서 프레즌스 > 클러스터 간을 선택합니다.

단계 **3** 찾기를 클릭하고 제거할 인터클러스터 피어를 선택합니다.

단계 **4** 삭제를 클릭합니다.

단계 **5** 피어 클러스터에서 이 단계를 반복합니다.

참고 인터클러스터 피어를 삭제한 후 IM and Presence 클러스터 내 각 노드에서 XCP 라우터를 다시 시작하지 않도록 IM and Presence 서비스가 향상되었습니다. 이 향상된 기능을 통해 관리자는 중단 없는 Jabber 서비스를 보장하면서 노드를 순차적으로 다시 시작함으로써 발생하는 오버헤드를 크게 줄여 대규모 클러스터를 효율적으로 관리할 수 있습니다.

인터클러스터 피어 상호 작용 및 제한 사항

기능	상호 작용 및 제한 사항
Cisco Business Edition 6000	IM and Presence 서비스를 Cisco Business Edition 6000 서버에 구축하는 경우 인터클러스터 피어가 지원되지 않습니다.

기능	상호 작용 및 제한 사항
클러스터 제한	인터클러스터 피어를 사용하면 클러스터가 중앙 집중식인지 또는 분산되었는지 여부와 관계 없이 클러스터 간 메시에 최대 30개의 IM and Presence 서비스 클러스터를 구축할 수 있습니다.
다중 클러스터 구축에서 클러스터 간 동기화 에이전트 리소스 부족	다수의 클러스터를 사용하는 다중 클러스터 구축에서 ICSA에 더 많은 리소스가 필요합니다. 리소스 부족으로 인해 ICSA 또는 SRM과 관련된 문제가 발생할 경우 아래에 언급된 Cisco SIP 프록시 서비스 파라미터를 기본값 20에서 새 값 10으로 변경하는 것이 좋습니다. • 최대 프로세스 수 • 최대 예비 프로세스 수 • 최대 프로세스 수 SIP 프록시 서비스를 다시 시작하여 변경 사항을 적용합니다. SRM 및 ICSA 서비스를 다시 시작합니다.
Intercluster 동기화 에이전트 및 DNS	Intercluster 동기화 에이전트는 DNS를 사용하여 피어 클러스터의 tomcat 인증서(SAN 항목)에 나열된 모든 CUCM 및 IM&P 서버를 모두 확인합니다. DNS 확인이 실패하면 Intercluster 동기화 에이전트가 원격 피어에 연결되지 않습니다.

15 장

푸시 알림 구성

푸시 알림 개요

클러스터에서 푸시 알림이 활성화되면 Unified Communications Manager와 IM and Presence 서비스는 Google 및 Apple의 클라우드 기반 푸시 알림 서비스를 사용하여 음성 및 화상 통화, 인스턴트 메시지 알림을 일시 중지 모드(백그라운드 모드라고도 함)에서 실행 중인 Android 및 iOS 클라이언트의 Cisco Jabber 또는 Cisco Webex에 푸시합니다. 푸시 알림을 사용하면 시스템이 Cisco Jabber 또는 Cisco Webex와 지속적인 통신을 유지할 수 있습니다. 푸시 알림은 엔터프라이즈 네트워크 내에서 연결되는 Android 및 iOS 클라이언트의 Cisco Jabber 및 Cisco Webex 및 Expressway의 모바일 및 원격 액세스 기능을 통해 온프레미스 배포에 등록하는 클라이언트 모두에 필요합니다.

푸시 알림 작동 방식

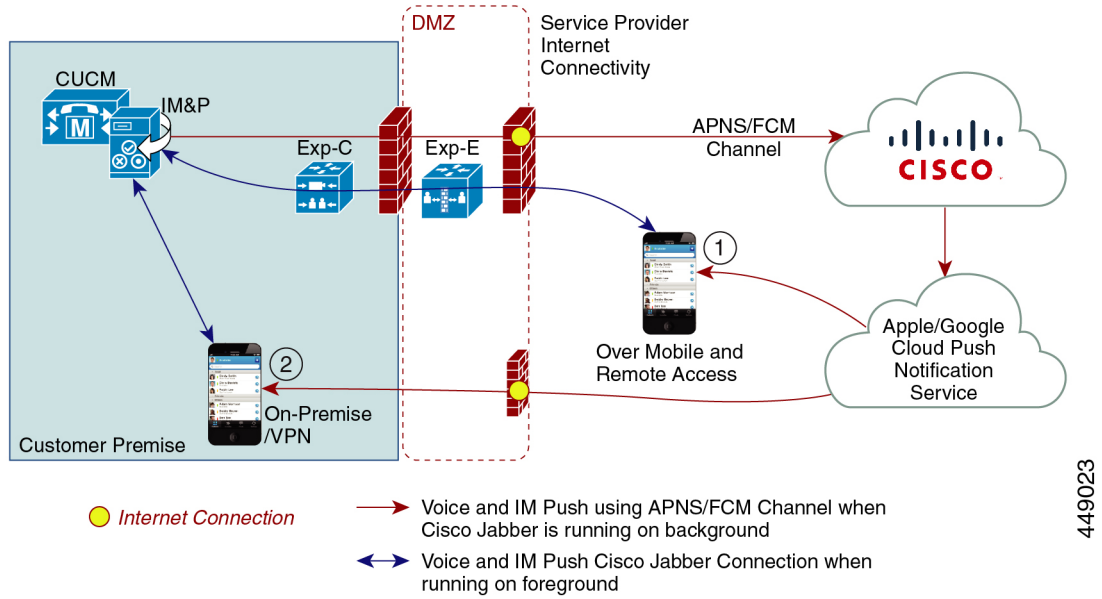
시작 시, Android 및 iOS 플랫폼 디바이스에 설치된 클라이언트는 Unified Communications Manager, IM and Presence 서비스 및 Google과 Apple 클라우드에 등록됩니다. 모바일 및 원격 액세스 구축을 사용하는 경우 클라이언트는 Expressway를 통해 온-프레미스 서버에 등록됩니다. Cisco Jabber 및 Cisco Webex 클라이언트가 포그라운드 모드로 유지되는 한 Unified Communications Manager와 IM and Presence 서비스는 클라이언트에 직접 전화 및 인스턴트 메시지를 보낼 수 있습니다.

그러나 Cisco Jabber 또는 Cisco Webex 클라이언트가 일시 중지 모드(예: 배터리 수명 유지를 위해)로 전환되면 표준 통신 채널을 사용할 수 없으므로 Unified Communications Manager와 IM and Presence 서비스는 클라이언트와 직접 통신할 수 없습니다. 푸시 알림은 파트너 클라우드를 통해 클라이언트에 연결할 수 있는 또 다른 채널을 제공합니다.

참고 다음 조건 중 하나라도 해당되면 Cisco Jabber 및 Cisco Webex는 일시 중단 모드로 실행되고 있는 것으로 간주됩니다.

- Cisco Jabber 또는 Cisco Webex 애플리케이션이 화면 밖(즉, 백그라운드에서)에서 실행 중임
- Android 또는 iOS 기기가 잠겨 있음
- Android 또는 iOS 디바이스 화면이 꺼져 있음

그림 *6:* 푸시 알림 아키텍처



위의 다이어그램은 Android and iOS용 Cisco Jabber 또는 Cisco Webex 클라이언트가 백그라운드에서 실행되거나 중 될 때 수행되는 작업을 표시합니다. 이 그림은 (1) Expressway를 통해 온프레미스 Cisco Unified Communications Manager 및 IM and Presence 서비스 구축과 연결되는 모바일 및 원격 액세스 구축, (2) 엔터프라이즈 네트워크 내에서 온프레미스 구축에 직접 연결하는 Android 및 iOS용 Cisco Jabber 또는 Cisco Webex 클라이언트를 보여줍니다.

참고 Apple 클라이언트 및 지원되는 Android 클라이언트에 대한 iOS13의 경우 음성 통화 및 메시지는 별도의 푸시 알림 채널 (' VoIP ' 및 ' Message ')을 사용하여 백그라운드 모드에서 실행 중인 클라이언트에 연결 합니다. 그러나, 두 채널에 대한 일반 흐름은 동일 합니다. IOS 12에서는 음성 통화와 메시지가 동일한 채널을 사용하여 전달 됩니다.

Cisco Jabber 및 **Cisco Webex**에 대한 푸시 알림 동작

다음 표에서는 Cisco Jabber 또는 IM and 현재 서비스에 등록 된 Cisco Webex iOS 클라이언트에 대한 iOS 12 및 iOS 13의 동작에 대해 설명 합니다Unified Communications Manager.

Cisco Jabber 또는 **Cisco Webex** 클라이언트가 실행되고 있습니다.	**Cisco Jabber**가 **iOS12** 디바이스에서 실행되고 있습니다.	**Cisco Jabber**가 **iOS13** 디바이스 또는 **Android** 디바이스에서 실행되고 있습니다.
포그라운드 모드	음성 및 영상 통화 Unified Communications Manager 표준 SIP communications 채널을 사용하여 Cisco Jabber 또는 Cisco Webex 클라이언트에 음성 및 영상 통화를 직접 전송 합니다. 통화의 경우에 Unified Communications Manager도 푸시 알림은 포그라운드 모드에 있는 Cisco Jabber 또는 Cisco Webex 클라이언트로 전송 됩니다. 그러나 표준 SIP 채널은 푸시 알림 채널이 아닌 통화를 설정 하는 데 사용 됩니다. 메시지 IM and 현재 서비스는 표준 SIP 통신 채널을 사용하여 메시지를 클라이언트에 직접 전송 합니다. 메시지의 경우 푸시 알림은 포그라운드 모드에 있는 클라이언트로 전송되지 않습니다.	동작은 iOS12와 동일합니다.

Cisco Jabber 또는 **Cisco Webex** 클라이언트가 실행되고 있습니다.	**Cisco Jabber**가 **iOS12** 디바이스에서 실행되고 있습니다.	**Cisco Jabber**가 **iOS13** 디바이스 또는 **Android** 디바이스에서 실행되고 있습니다.
일시 중지 모드(백그라운드 모드)	음성 또는 영상 통화 표준 통신 채널을 사용할 수 없습니다. 통합 CM은 푸시 알림 채널을 사용합니다. 알림을 받으면 Cisco Jabber 또는 Cisco Webex 클라이언트는 자동으로 포그라운드 모드로 다시 들어가고 클라이언트의 전화벨이 울립니다. 메시징 표준 통신 채널을 사용할 수 없습니다. IM and Presence 서비스는 푸시 알림 채널을 사용하여 다음과 같이 IM 알림을 보냅니다. **1.** IM and Presence 서비스는 Cisco 클라우드의 Push REST 서비스로 IM 알림을 보내고, 알림은 Apple 클라우드로 전달됩니다. **2.** Apple 클라우드는 IM 알림을 Cisco Jabber 또는 Cisco Webex 클라이언트에 푸시하고 Cisco Jabber 또는 Cisco Webex 클라이언트에 알림이 나타납니다. **3.** 사용자가 알림을 클릭하면 Cisco Jabber 또는 Cisco Webex 클라이언트가 포그라운드로 돌아갑니다. Cisco Jabber 또는 Cisco Webex 클라이언트는 IM and Presence 서비스로 세션을 재개하고 인스턴트 메시지를 다운로드합니다. 참고 Cisco Jabber 또는 Cisco Webex 클라이언트가 일시 중지 모드에 있는 동안 사용자의 프레즌스 상태가 자리 비움으로 표시됩니다.	IOS13를 사용 하는 경우 통화 트래픽 및 메시지 트래픽은 별도의 푸시 알림 채널로 분할 됩니다. 통화에 대한 ' VoIP ' 채널 및 메시징의 "메시지" 채널이 구분 됩니다. 음성 또는 영상 통화 표준 통신 채널을 사용할 수 없습니다. 통합 CM은 푸시 알림 ' VoIP ' 채널을 사용합니다. Jabber는 VoIP 알림을 수신 하면 발신자 ID를 사용하여 CallKit를 실행합니다. 이 동작은 Cisco Jabber 또는 Cisco Webex iOS 클라이언트의 경우 보류됩니다. 메시징 표준 통신 채널을 사용할 수 없습니다. IM and 현재 서비스에서 푸시 알림 ' 메시지 ' 채널을 사용합니다. **1.** IM and Presence 서비스는 Cisco 클라우드의 Push REST 서비스로 IM 알림을 보내고, 알림은 Apple 클라우드로 전달됩니다. **2.** Apple 클라우드는 IM 알림을 Cisco Jabber 또는 Cisco Webex 클라이언트로 푸시합니다. **3.** 사용자가 알림을 클릭하면 Cisco Jabber 또는 Cisco Webex 클라이언트가 포그라운드로 돌아갑니다. Cisco Jabber 또는 Cisco Webex 클라이언트는 IM and Presence 서비스로 세션을 재개하고 메시지를 다운로드합니다. 참고 Cisco Jabber 또는 Cisco Webex 클라이언트가 일시 중지 모드에 있는 동안 사용자의 프레즌스 상태가 자리 비움으로 표시됩니다.

푸시 알림에 대해 지원되는 클라이언트

클라이언트	**OS**	플랫폼 클라우드	클라우드 서비스
iPhone 및 iPad의 Cisco Jabber	iOS	Apple	Apple 푸시 알림 서비스 APN)
Android의 Cisco Jabber	Android	Google	Android PNS 서비스
iOS의 Webex	iOS	Apple	Apple 푸시 알림 서비스 APN)
Android의 Webex	Android	Google	Android PNS 서비스

iOS13에서 푸시 알림 작동 방식

IOS13에서 Apple은 유형 VoIP를 사용 하는 일시 중단 된 앱에 대한 푸시 알림을 iOS12와 비교 하 여 처리 합니다. 7 월 2020에서 모든 새 앱 및 앱 업데이트는 iOS 13 SDK를 사용하여 빌드됩니다.

Cisco Unified Communications Manager 및 im and 현재 서비스는 음성 및 IM 메시지를 모두 푸시하는 데 VOIP 알림 채널을 사용합니다.

- 모든 오디오 영상 통화의 경우 CUCM 서버는 " **VoIP**" 유형의 푸시 알림을 전송 합니다.
- 모든 메시지에 대해 IM&P 서버는 "메시지" 유형의 푸시 알림을 전송합니다.

CUCM는 VoIP 푸시 알림을 우선 순위가 높은 알림으로 고려하고 지연 없이 제공합니다.

다음 다이어그램은 Apple이 **iOS12** 및 **iOS13**에서 푸시 알림을 처리하는 방법을 표시합니다.

여기에 이미지 표시

여기에 이미지 표시

각 사용 사례와 버전 간에 발생하는 작업에 대한 자세한 설명은 다음 표를 참조하십시오.

푸시 알림 구성

푸시 알림을 구성하고 구축하는 방법에 대한 자세한 내용은 https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html에서 *iPhone* 및 *iPad*에서 *Cisco Jabber*에 대한 푸시 알림을 참조하십시오.

III 부

기능 구성

16 장

가용성 및 인스턴트 메시징 구성

가용성 및 인스턴트 메시징 개요

IM and Presence 서비스를 사용하면 해당 가용성 상태를 자신의 연락처와 공유할 수 있습니다.

포인트 투 포인트 인스턴트 메시징은 동시에 두 사용자 간 실시간 대화를 지원합니다. IM and Presence 서비스는 송신자에서 수신자로 사용자 간 메시지를 직접 교환합니다. 포인트 투 포인트 인스턴트 메시지 교환을 수행하려면 사용자가 각자의 인스턴트 메시지 클라이언트에서 온라인 상태여야 합니다.

인스턴트 메시징 기능은 다음을 포함합니다.

인스턴트 메시징 포킹

사용자가 여러 인스턴트 메시지 클라이언트에 로그인한 연락처에게 인스턴트 메시지를 보내면 IM and Presence 서비스는 각 클라이언트에 인스턴트 메시지를 전달합니다. IM and Presence 서비스에서는 연락처 사용자가 응답할 때까지 계속해서 각 클라이언트에 인스턴트 메시지를 포킹합니다. 연락처 사용자가 응답하면 IM and Presence 서비스에서는 연락처 사용자가 응답한 클라이언트로만 인스턴트 메시지를 전달합니다.

오프라인 인스턴트 메시징

사용자가 로그인하지 않은(오프라인) 연락처에게 인스턴트 메시지를 보내면 IM and Presence 서비스는 인스턴트 메시지를 저장하고 오프라인 연락처가 인스턴트 메시지 클라이언트에 다시 로그인한 후 메시지를 전달합니다.

브로드캐스트 인스턴트 메시징

사용자는 인스턴트 메시지를 여러 연락처에 동시에 보낼 수 있습니다(예: 한 사용자가 대규모 그룹 연락처에 알림 전송).

모든 인스턴트 메시지 클라이언트가 브로드캐스팅을 지원하는 것은 아닙니다.

최대 연락처 목록 크기

사용자에 대한 최대 연락처 목록 크기를 구성합니다. 이것은 사용자가 연락처 목록에 추가할 수 있는 연락처 수입니다. 이 설정은 Cisco Jabber 클라이언트 애플리케이션 및 타사 클라이언트 애플리케이션의 연락처 목록에 적용됩니다.

최대 연락처 수에 도달한 사용자는 연락처 목록에 새 연락처를 추가할 수 없으며, 다른 사용자들도 이들을 연락처로서 추가할 수 없습니다. 특정 사용자가 최대 연락처 목록 크기에 근접한 상태에서 연락처 최대 목록 크기를 초과하는 연락처 목록을 추가하는 경우 IM and Presence 서비스는 초과되는 연락처를 추가하지 않습니다. 예를 들어, IM and Presence 서비스의 최대 연락처 목록 크기가 200이고, 사용자에게 195개의 연락처가 있고, 새 연락처 6개를 목록에 추가하려고 시도할 경우 IM and Presence 서비스는 5개의 연락처를 추가하고 6번째 연락처는 추가하지 않습니다.

팁 **Cisco Unified CM IM and Presence** 관리의 시스템 문제 해결 프로그램은 연락처 목록 제한에 도달한 사용자가 있는지를 표시합니다.

가용성 및 인스턴트 메시징 필수 조건

SIP to SIP 인스턴트 메시징의 경우 IM and Presence 서비스에서 다음 서비스가 실행되고 있어야 합니다.

- Cisco SIP Proxy
- Cisco Presence 엔진
- Cisco XCP 라우터

SIP to XMPP 인스턴트 메시징의 경우 IM and Presence 서비스에서 다음 서비스가 실행되고 있어야 합니다.

- Cisco SIP Proxy
- Cisco Presence 엔진
- Cisco XCP 라우터
- Cisco XCP 텍스트 전화회의 관리자

가용성 및 인스턴트 메시징 작업 흐름

IM and Presence 서비스에서 가용성 및 인스턴트 메시징을 구성하려면 다음 작업을 수행하십시오.

프로시저

	명령 또는 동작	목적
단계 **1**	프레즌스 공유 구성, 191 페이지	이 절차를 사용하여 프레즌스 및 IM 가용성 공유에 대한 클러스터 수준 설정을 구성합니다. 프레즌스 공유를 통해 사용자는 서로의 IM 가용성 상태를 볼 수 있습니다.
단계 **2**	임시 프레즌스 가입 구성, 192 페이지	임시 프레즌스 가입을 구성합니다. 이 설정을 사용하면 연락처 목록에 없는 다른 사용자의 프레즌스 상태를 일시적으로 볼 수 있습니다.
단계 **3**	인스턴트 메시징 활성화, 193 페이지	사용자가 인스턴트 메시지를 교환할 수 있도록 시스템을 구성합니다.

프레즌스 공유 구성

이 절차를 사용하여 프레즌스 및 IM 가용성 공유에 대한 클러스터 수준 설정을 구성합니다. 프레즌스 공유를 통해 사용자는 서로의 IM 가용성 상태를 볼 수 있습니다.

참고 가용성 공유가 꺼져 있을 때:

- 사용자는 클라이언트 애플리케이션에서 자신의 가용성 상태를 볼 수 있지만 다른 사용자의 상태는 회색으로 표시됩니다.
- 사용자가 채팅방에 입장하면 대화 가능 상태가 알 수 없음으로 표시됩니다.

프로시저

단계 **1** **Cisco Unified CM IM and Presence** 관리에서 프레즌스 > 설정 > 표준 구성을 선택합니다.

단계 **2** 클러스터 수준의 프레즌스 공유를 활성화하려면 가용성 공유 활성화 확인란을 선택합니다.

참고 개별 Cisco Jabber 사용자는 해당 Cisco Jabber 클라이언트의 정책 설정을 재구성하여 자신의 Jabber 클라이언트에 대해 이 설정을 활성화 또는 비활성화할 수 있습니다.

단계 **3** 사용자가 다른 사용자의 승인없이 다른 사용자의 프레즌스를 볼 수있게 하려면 사용자에게 승인에 대한 메시지를 표시하지 않고 다른 사용자의 사용 가능성을 볼 수 있도록 허용 확인란을 선택합니다. 그렇지 않으면, 모든 프레즌스 요청은 다른 사용자의 승인을 받아야 합니다.

참고 개별 최종 사용자는 해당 Cisco Jabber 클라이언트 내에서 정책 설정을 재구성하여 이 설정을 무시할 수 있습니다.

단계 **4** 최대 연락처 목록 크기 및 최대 관찰자 수(사용자당) 설정의 .최대 값을 구성합니다. 최대 값을 사용하지 않으려면 각각에 대해 제한 없음 확인란을 선택합니다.

단계 **5** (선택 사항) Cisco Jabber 사용자가 연락처 목록에 없는 다른 사용자의 프레즌스 상태를 일시적으로 가입할 수 있게 하려면 임시 프레즌스 가입 활성화 확인란을 선택하고 추가 임시 프레즌스 설정을 구성합니다.

단계 **6** 프레즌스 설정 창에서 추가 설정을 완료합니다. 필드 및 해당 설정에 대한 도움이 필요한 경우 온라인 도움말을 참조하십시오.

단계 **7** 저장을 클릭합니다.

단계 **8** **Cisco XCP** 라우터 및 **Cisco Presence** 엔진 서비스를 다시 시작합니다.

a) Cisco Unified IM and Presence 서비스 가용성에 로그인하고 도구 > 제어 센터 - 기능 서비스를 선택합니다.

b) **Cisco Presence** 엔진 서비스를 선택하고 다시 시작을 클릭합니다.

c) 도구제어 센터 > - 네트워크 서비스를 선택합니다.

d) **Cisco XCP** 라우터 서비스를 선택하고 다시 시작을 클릭합니다.

참고 편집한 필드에 따라 서비스를 다시 시작할 필요가 없을 수도 있습니다. 편집한 필드에 대한 정보는 온라인 도움말을 참조하십시오.

다음에 수행할 작업

인스턴트 메시징 활성화, 193 페이지

임시 프레즌스 가입 구성

임시 프레즌스 가입을 사용하면 연락처 목록에 없는 다른 사용자의 프레즌스 상태를 일시적으로 볼 수 있습니다.

시작하기 전에

프레즌스 공유 구성, 191 페이지

프로시저

단계 **1** **Cisco Unified CM IM and Presence** 관리에서 프레즌스 > 설정 > 표준을 선택합니다.

단계 **2** Cisco Jabber 사용자를 위해 임시 프레즌스 가입을 켜려면 임시 프레즌스 가입 활성화 확인란을 선택합니다.

단계 **3** IM and Presence 서비스에서 한 번에 허용할 최대 활성 임시 가입 수를 설정합니다. 값을 영(0)으로 설정하면 IM and Presence 서비스는 활성 임시 가입을 무제한 허용합니다.

단계 **4** 임시 프레즌스 가입의 TTL(Time-to-Live) 값을 설정합니다(초 단위).

TTL 값이 만료되면 IM and Presence 서비스는 임시 프레즌스 가입을 삭제하고, 더 이상 해당 사용자의 사용 가능성 상태를 임시로 모니터링하지 않습니다.

참고 사용자가 아직 임시 프레즌스 가입의 인스턴스 메시지를 보고 있는 동안 TTL 값이 만료되면 사용 가능성 상태가 현재로 표시되지 않습니다.

단계 **5** 저장을 클릭합니다.

참고 이 설정의 경우 IM and Presence 서비스에서 서비스를 다시 시작할 필요가 없습니다. 그러나 Cisco Jabber 사용자는 IM and Presence 서비스에서 최신 임시 프레즌스 가입 설정을 검색하려면 로그아웃하고 다시 로그인해야 합니다.

다음에 수행할 작업

인스턴트 메시징 활성화, 193 페이지

인스턴트 메시징 활성화

사용자가 인스턴트 메시지를 교환할 수 있도록 시스템을 구성합니다.

시작하기 전에

프레즌스 공유 구성, 191 페이지

프로시저

단계 **1** **Cisco Unified CM IM and Presence** 관리에서 메시징 > 설정을 선택합니다.

단계 **2** 인스턴트 메시징 활성화 확인란을 선택합니다.

단계 **3** 구축 요구 사항을 충족하는 확인란 옵션을 선택합니다. 필드 설명은 온라인 도움말을 참조하십시오.

- 오프라인 인스턴트 메시징 표시 안 함
- 인스턴트 메시지 내역을 기록하도록 허용**(**지원되는 클라이언트만 해당**)**
- 인스턴트 메시지에서 잘라내기 및 붙여넣기 허용

단계 **4** 저장을 클릭합니다.

가용성 및 인스턴트 메시징 상호 작용 및 제한 사항

기능	제한 사항
가용성 공유	이 설정을 끄면 사용자는 자신의 가용성 상태만 볼 수 있습니다. 가용성 정보는 클러스터의 다른 사용자와 공유되지 않습니다. 또한 클러스터 외부에서 수신된 가용성 정보는 공유되지 않습니다.

기능	제한 사항
인스턴트 메시지	Cisco XCP 라우터가 갑자기 종료되거나 사용자가 이를 중지했다가 다시 시작하면 시작할 때 또는 중단 기간에 전송되었던 인스턴트 메시지가 대상 사용자에게 전달되지 않을 수 있습니다. 메시지를 보낸 사용자에게 경고 메시지가 전송되지 못할 수도 있습니다. 자세한 내용은 관리자가 Cisco XCP 라우터 추적 파일 rtr-jsm-1에서 "jsm db 종료 후 패킷 삭제"를 포함하는 오류 로그 줄을 확인할 수 있습니다.

17 장

임시 및 영구 채팅 구성

그룹 채팅방 개요

그룹 채팅은 두 명 이상의 사용자 간의 인스턴트 메시징 세션입니다. IM and Presence 서비스는 임시 채팅방 또는 영구 채팅방에서 그룹 채팅을 지원합니다. 인스턴트 메시징을 활성화하면 임시 채팅방 지원은 기본적으로 활성화되지만 영구 채팅방을 지원하도록 시스템을 구성해야 합니다.

임시 채팅방

임시 채팅방은 한 명의 사용자가 여전히 채팅방에 연결되어 있는 동안에만 존재하는 그룹 채팅 세션입니다. 임시 채팅방은 마지막 사용자가 룸에서 떠나면 시스템에서 삭제됩니다. 인스턴트 메시지 대화의 레코드는 영구적으로 유지되지 않습니다. 인스턴트 메시징이 활성화되면 임시 채팅방이 기본적으로 활성화됩니다.

임시 채팅 회의실은 기본적으로 공개 회의실이지만, 비공개로 다시 구성할 수 있습니다. 그러나 사용자가 공개 또는 비공개 임의 회의실에 참가할 수 있는 방법은 사용 중인 XMPP 클라이언트의 유형에 따라 다릅니다.

- 임시 채팅 회의실(공개 또는 비공개)에 참가하려면 Cisco Jabber 사용자를 초대해야 합니다.
- 타사 XMPP 클라이언트의 사용자는 임의 채팅 회의실(공개 또는 개인)에 참가하기 위해 초대될 수 있고, 회의실 검색 서비스를 통해 참가할 수 있는 공개 전용 임시 회의실을 검색할 수 있습니다.

영구 채팅방

영구 채팅방은 모든 사용자가 룸에서 나간 후에도 존재하는 그룹 채팅 세션입니다. 사용자는 토론을 계속하기 위해 시간이 지나면 같은 방으로 돌아올 것으로 예상됩니다.

영구 채팅방은 사용자들이 특정 주제에 대해 협력하고 지식을 공유하며, 해당 주제에 대해 논의된 아카이브를 검색하고(이 기능이 IM and Presence 서비스에서 활성화된 경우), 해당 주제에 대한 토론에 실시간으로 참여하도록 만들었습니다.

영구 채팅방을 위해 시스템을 구성해야 합니다. 또한 영구 채팅을 위해서는 외부 데이터베이스를 구축해야 합니다.

영구 채팅방은 IOS 및 Android 클라이언트를 포함하여 데스크톱 및 모바일 Jabber 클라이언트 모두에서 지원됩니다. 모바일 클라이언트의 경우 최소한 Jabber 릴리스 12.1(0)을 실행해야 합니다.

그룹 채팅 필수 조건

임시 채팅 필수 조건

임시 채팅방을 구축하는 경우 인스턴트 메시징이 활성화되어 있어야 합니다. 자세한 내용은 인스턴트 메시징 활성화, 193 페이지를 참조하십시오.

영구 채팅 필수 조건

영구 채팅방을 구축하는 경우:

- 인스턴트 메시징이 활성화되어 있는지 확인합니다. 자세한 내용은 인스턴트 메시징 활성화, 193 페이지를 참조하십시오.
- 외부 데이터베이스를 구축해야 합니다. 데이터베이스 설정 및 지원 정보는 http://www.cisco.com/c/en/us/support/unified-communications/unified-presence/products-installation-and-configuration-guides-list.html에서 *IM and Presence* 서비스 데이터베이스 설정 설명서를 참조하십시오.
- 영구 채팅을 위한 고가용성을 구축할지 여부를 결정합니다. 이 구축 유형은 영구 채팅방에 이중화와 장애 조치를 추가합니다. 그러나 외부 데이터베이스 요구 사항은 고가용성 없이 기능을 구축하는 경우와 약간 다릅니다.
- 영구 채팅 구축의 경우에는 최소 15,000 사용자 OVA를 구축하는 것이 좋습니다.

그룹 채팅 및 영구 채팅 작업 흐름

프로시저

	명령 또는 동작	목적
단계 **1**	그룹 채팅 시스템 관리자 구성, 198 페이지	영구 채팅 시스템을 관리할 시스템 관리자를 추가합니다.
단계 **2**	채팅방 설정 구성, 198 페이지	기본 채팅방 설정을 구성합니다. 선택적으로 영구 채팅을 활성화합니다.
단계 **3**	Cisco XCP 텍스트 전화회의 관리자 다시 시작, 199 페이지	영구 채팅을 구축하는 경우 Cisco XCP 텍스트 전화회의 관리자 서비스가 실행 중인지 확인하십시오.
단계 **4**	영구 채팅을 위한 외부 데이터베이스 설정, 200 페이지	영구 채팅의 경우 노드당 고유한 외부 데이터베이스 인스턴스를 구성해야 합니다. 참고 영구 채팅을 위한 고가용성을 구축하는 경우 HA를 구축할 때와 데이터베이스 요구 사항이 약간 다르므로 이 장의 나머지 작업을 건너 뛸 수 있습니다.
단계 **5**	외부 데이터베이스 연결 추가, 200 페이지	IM and Presence 서비스에서 외부 데이터베이스에 대한 연결을 설정합니다.
단계 **6**	Persistent Chat용 MSSQL 데이터베이스에 대한 Windows 인증, 201 페이지	MSSQL 외부 데이터베이스에 대한 연결을 설정할 때 Windows 인증을 활성화할 수 있습니다.
단계 **7**	한 외부 데이터베이스에서 다른 외부 데이터베이스로 채팅방 마이그레이션	IM and Presence 서비스에서 기존 외부 데이터베이스의 모든 채팅방 및 그룹을 동일한 데이터베이스 유형 또는 다른 유형의 다른 채팅방 및 그룹으로 마이그레이션합니다. 외부 데이터베이스 마이그레이션을 수행하는 방법에 대한 자세한 내용은 Cisco IM and Presence 데이터베이스 설정 설명서 12.5(1) SU2 릴리스의 "한 외부 데이터베이스에서 다른 외부 데이터베이스로 채팅방 마이그레이션" 섹션을 참조하십시오.

그룹 채팅 시스템 관리자 구성

영구 채팅 시스템을 관리할 시스템 관리자를 추가합니다.

프로시저

단계 **1** 메시징 > 그룹 채팅 시스템 관리자를 선택합니다.

단계 **2** 그룹 채팅 시스템 관리자 권한 활성화를 선택합니다.

설정을 활성화 또는 비활성화하는 경우 Cisco XCP 라우터를 다시 시작합니다. 시스템 관리자 설정이 활성화되면 시스템 관리자를 동적으로 추가할 수 있습니다.

단계 **3** 새로 추가를 클릭합니다.

단계 **4** IM 주소를 입력합니다.

예제

IM 주소는 name@domain 형식이어야 합니다.

단계 **5** 별칭 및 설명을 입력합니다.

단계 **6** 저장을 클릭합니다.

다음에 수행할 작업

채팅방 설정 구성, 198 페이지

채팅방 설정 구성

룸 구성원 및 점유율 설정, 룸당 최대 사용자 수와 같은 기본 채팅방 설정을 구성합니다.

선택적으로 영구 채팅 활성화 확인란을 선택하여 영구 채팅을 활성화할 수 있습니다.

프로시저

단계 **1** Cisco Unified CM IM and Presence 관리에서 메시징 > 그룹 채팅 및 영구 채팅을 선택합니다.

단계 **2** 시스템에서 기본 그룹 채팅 서버 별칭을 자동으로 관리합니다 확인란을 선택 또는 선택 취소하여 시스템에서 채팅 노드 별칭을 관리하도록 할지 여부를 구성합니다.

- 선택 - 시스템이 채팅 노드 별칭을 자동으로 할당합니다. 이는 기본값입니다.
- 선택 취소 - 관리자가 자신의 채팅 노드 별칭을 할당할 수 있습니다.

단계 **3** 모든 참가자가 룸에서 나간 후에도 채팅방을 유지하려면 영구 채팅 활성화 확인란을 선택합니다.

참고 이는 클러스터 수준 설정입니다. 클러스터의 노드에서 영구 채팅을 활성화한 경우 모든 클러스터의 클라이언트가 해당 노드에서 호스팅되는 노드 및 채팅방의 텍스트 전화회의 인스턴스를 검색할 수 있습니다.

원격 클러스터의 영구 채팅이 활성화되지 않은 경우에도 원격 클러스터의 사용자가 로컬 클러스터의 텍스트 전화회의 인스턴스 및 채팅방을 검색할 수 있습니다.

단계 **4** 영구 채팅을 활성화하도록 선택한 경우 다음 각 필드에 대한 값을 구성합니다.

- 허용되는 영구 채팅방의 최대 수
- 데이터베이스에 대한 연결 수
- 데이터베이스 연결 하트비트 간격(초)
- 영구 채팅방에 대한 시간 제한 값(분)

참고 Cisco 지원에서 지시하는 경우가 아니면 데이터베이스 연결 하트비트 간격 값을 영(0)으로 설정하지 마십시오. 방화벽 전체에서 연결을 유지하는 데에는 일반적으로 하트비트 간격이 사용됩니다.

단계 **5** 룸 설정 아래에서 최대 룸 수를 할당합니다.

단계 **6** 그룹 채팅 및 영구 채팅 설정 창에서 나머지 설정을 완료합니다. 필드 및 해당 설정에 대한 도움이 필요한 경우 온라인 도움말을 참조하십시오.

단계 **7** 저장을 클릭합니다.

다음에 수행할 작업

Cisco XCP 텍스트 전화회의 관리자 다시 시작, 199 페이지

Cisco XCP 텍스트 전화회의 관리자 다시 시작

채팅 설정을 편집했거나 하나 이상의 별칭을 채팅 노드에 추가한 경우 **Cisco XCP** 텍스트 전화회의 관리자 서비스를 다시 시작합니다.

프로시저

단계 **1** **Cisco Unified IM and Presence Service** 가용성에서 도구 > 제어 센터 - 기능 서비스를 선택합니다.

단계 **2** 서버 드롭다운 목록에서 IM and Presence 노드를 선택하고 이동을 클릭합니다.

단계 **3** **IM and Presence** 서비스 섹션에서 **Cisco XCP** 텍스트 전화회의 관리자 라디오 버튼을 클릭하고 시작 또는 다시 시작을 클릭합니다.

단계 **4** 재시작하는 데 시간이 걸릴 수 있음을 알리는 메시지가 표시되면 확인을 클릭합니다.

단계 **5** (선택 사항) 서비스가 완전히 다시 시작되었는지 확인하려면 새로 고침을 클릭합니다.

다음에 수행할 작업

영구 채팅에 대한 고가용성을 구축하는 경우 영구 채팅의 고가용성 작업 흐름, 214 페이지(으)로 이동합니다..

그렇지 않으면, 영구 채팅을 위한 외부 데이터베이스 설정, 200 페이지.

영구 채팅을 위한 외부 데이터베이스 설정

참고 이 항목에서는 고가용성이 없는 영구 채팅에 대해 설명합니다. 영구 채팅을 위한 고가용성을 구축하는 경우 외부 데이터베이스 설정 정보 대신 해당 장을 참조하십시오.

영구 채팅방을 구성하는 경우 영구 채팅방을 호스팅하는 각 노드에 대해 별도의 외부 데이터베이스 인스턴스를 설정해야 합니다. 그 외에도,

- 영구 채팅이 활성화된 경우, 외부 데이터베이스를 텍스트 전화회의 관리자 서비스와 연결해야 하며 데이터베이스가 활성 상태이고 도달 가능해야 합니다. 그렇지 않으면 텍스트 전화회의 관리자가 시작되지 않습니다.
- 영구 채팅 로깅을 위해 외부 데이터베이스를 사용하는 경우 데이터베이스가 정보량을 처리할만큼 충분히 큰지 확인하십시오. 채팅방의 모든 메시지를 보관하는 것은 선택 사항이지만, 그렇게 할 경우 노드의 트래픽이 증가하고 디스크의 공간을 소모하게 됩니다.
- 외부 데이터베이스 정리 유틸리티를 사용하여 데이터베이스 크기를 모니터링하고 만료된 레코드를 자동으로 삭제하는 작업을 설정합니다.
- 외부 데이터베이스에 대한 연결 수를 구성하기 전에 기록 중인 IM의 수 및 그에 따른 전체적인 트래픽의 양을 고려해야 합니다. 구성하는 연결 수에 따라 시스템 규모가 결정됩니다. 시스템 기본값이 대부분의 설치에 적합하지만 특정 구축에 맞게 매개 변수를 수정할 수도 있습니다.

외부 데이터베이스를 설정하는 방법에 대한 지침은 http://www.cisco.com/c/en/us/support/unified-communications/unified-presence/products-installation-and-configuration-guides-list.html에서 *IM and Presence Service* 외부 데이터베이스 설정 설명서를 참조하십시오.

다음에 수행할 작업

외부 데이터베이스 연결 추가, 200 페이지

외부 데이터베이스 연결 추가

IM and Presence 서비스에서 영구 채팅 외부 데이터베이스에 대한 연결을 구성합니다. 전체 IM and Presence 인터클러스터에 최소한 하나의 고유한 논리적 외부 데이터베이스 인스턴스(테이블 스페이스)가 필요합니다.

프로시저

단계 1 Cisco Unified CM IM and Presence 관리에서 메시징 > 외부 서버 설정 > 외부 데이터베이스를 선택합니다.

단계 2 새로 추가를 클릭합니다.

단계 3 데이터베이스 이름 필드에 데이터베이스 인스턴스 이름을 입력합니다.

단계 4 데이터베이스 유형 드롭다운에서 구축하는 외부 데이터베이스의 유형을 선택합니다.

단계 5 데이터베이스에 대한 사용자 이름 및 암호 정보를 입력합니다.

단계 6 호스트 이름 필드에 데이터베이스의 호스트이름 또는 IP 주소를 입력합니다.

단계 7 나머지 설정은 외부 데이터베이스 설정 창에서 완료합니다. 필드 및 해당 설정에 대한 도움이 필요한 경우 온라인 도움말을 참조하십시오.

단계 8 저장을 클릭합니다.

단계 9 이 절차를 반복하여 각 외부 데이터베이스 인스턴스에 대한 연결을 만듭니다.

Persistent Chat용 MSSQL 데이터베이스에 대한 Windows 인증

Persistent Chat용 MSSQL 외부 데이터베이스에 대한 Windows 인증을 활성화하려면

시작하기 전에

중요 릴리스 14SU2부터 지원됩니다.

외부 데이터베이스 연결을 설정하는 방법은 외부 데이터베이스 연결 추가, 200 페이지를 참조하십시오.

프로시저

	명령 또는 동작	목적
단계 1	데이터베이스 유형 드롭다운에서 외부 데이터베이스 유형을 **Microsoft SQL** 서버로 선택합니다.	
단계 2	**Windows** 인증 활성화 확인란에 체크 표시합니다.	
단계 3	도메인 필드에 Windows 도메인 이름을 입력합니다.	

	명령 또는 동작	목적
단계 **4**	Windows 사용자의 사용자 이름 및 암호 정보를 입력합니다.	참고 Windows 인증을 사용하면 도메인 수준에서 Windows 그룹을 만들 수 있고, 전체 그룹용 MSSQL 서버에 로그인을 만들 수 있습니다.

그룹 채팅 및 영구 채팅 상호 작용 및 제한 사항

표 ***20:*** 그룹 채팅 및 영구 채팅 상호 작용 및 제한 사항

기능 상호 작용	제한 사항
룸 입장 보관	룸 입장과 퇴장을 기록하는 것은 선택 사항입니다. 트래픽이 증가하고 외부 데이터베이스 서버의 공간을 소모하기 때문입니다.
익명 룸에서 채팅	Cisco Jabber를 통한 채팅(그룹 채팅 또는 영구 채팅)을 구축하는 경우 그룹 채팅 및 영구 채팅 설정 창에서 방은 기본적으로 익명입니다. 및 방 소유자는 방을 익명으로 할지 여부를 변경할 수 있습니다. 옵션을 선택하지 않았는지 확인하십시오 . 확인란이 하나라도 선택된 경우 채팅이 실패합니다.
데이터베이스 연결 문제	텍스트 전화회의 관리자 서비스가 시작된 후 외부 데이터베이스와의 연결이 실패하면 텍스트 전화회의 관리자 서비스는 활성 상태로 유지되고 작동하지만, 메시지가 더 이상 데이터베이스에 기록되지 않으며 연결이 복구될 때까지 새로운 영구 채팅 방을 만들 수 없습니다.
OVA 요구 사항	영구 채팅 또는 인터클러스터 피어링을 구축하는 경우 이러한 기능에 대해 구축할 수 있는 최소 OVA 크기는 5000 사용자 OVA입니다. 최소 15,000 사용자 OVA를 구축하는 것이 좋습니다. 중앙 집중식 구축은 사용자 크기에 따라 25,000 사용자 OVA가 필요할 수 있습니다. OVA 옵션과 사용자 용량에 대한 자세한 내용은 다음 사이트를 참조하십시오. 참고 모든 IMP 노드에는 적어도 15,000 사용자 OVA를 구축하는 것이 좋습니다. https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-cisco-ucm-im-presence.html
Microsoft SQL Server의 영구 채팅 문자 제한	메시지 본문(HTML 태그 + 문자 메시지 포함)이 4000자를 초과하는 채팅 메시지는 전달되지 않습니다. 이러한 메시지는 거부되고 보관되지 않습니다. 이 문제는 Microsoft SQL Server가 릴리스 11.5(1)SU3 이후의 외부 데이터베이스로 사용되는 경우에 발생합니다. 자세한 내용은 CSCvd89705를 참조하십시오.

기능 상호 작용	제한 사항
피어 클러스터가 지원되지 않는 릴리스를 실행 중인 Jabber 모바일용 영구 채팅	Jabber 모바일용 영구 채팅은 11.5(1)SU5에 도입되었으며 이전 11.5(1)SU 릴리스에서는 지원되지 않습니다. 이 기능은 12.0(1) 또는 12.0(1)SU1에 지원되지 않습니다. 이 릴리스에 구축된 Jabber 모바일용 영구 채팅이 있고 Jabber 모바일용 영구 채팅방을 지원하지 않는 피어 클러스터로 인터클러스터 피어링을 설정한 경우 다음 조건이 Jabber 모바일 클라이언트에 적용됩니다. 영구 채팅방이 지원되지 않는 릴리스(예: 11.5(1))에서 호스팅되는 경우: • 지원되는 클러스터에서 호스팅되는 Jabber 모바일 클라이언트는 지원되지 않는 클러스터에서 호스팅되는 영구 채팅방에 참가할 수 있지만 룸을 음소거하는 옵션이 없습니다. 전역 음소거 옵션이 표시되지만 작동하지 않습니다. • 지원되지 않는 피어 클러스터에서 호스팅되는 Jabber 모바일 클라이언트는 영구 채팅방에 참가할 수 없습니다. 영구 채팅방이 지원되는 릴리스에서 호스팅되는 경우(예: 11.5(1)SU5 : • 지원되는 클러스터에서 호스팅되는 Jabber 모바일 클라이언트 참가자는 모바일 기능에 대한 모든 영구 채팅을 갖습니다. • 지원되지 않는 피어 클러스터의 Jabber 모바일 클라이언트는 영구 채팅방에 참가할 수 없습니다. 참고 Jabber 구성 파일(*(jabber-config.xml)*)이 IM 기록을 비활성로 설정하면 영구 채팅의 검색 기능이 작동하지 않습니다.
외부 데이터베이스 연결 및 Cisco XCP 텍스트 컨퍼런스 서비스	스플릿 브레인 시나리오에서 가입자 또는 게시자가 피어 텍스트 컨퍼런스 서비스를 감지하거나 노드가 다운되면 가입자 또는 게시자가 정상에서 백업으로 전환을 시도합니다. 피어의 채팅 회의실의 로드가 외부 데이터베이스에 연결되지 못하면 이 작업 중에 Cisco XCP 텍스트 컨퍼런스 서비스가 종료됩니다.

기능 상호 작용	제한 사항
고가용성이 구성된 경우 지원되는 영구 채팅방 수입니다.	IM&P 구축에서 지원되는 최대 영구 채팅방 수는 하위 클러스터 당 5000입니다. 고가용성이 활성화된 경우 노드당 최대 2500개의 룸을 생성하는 것이 좋습니다. (시스템에서는 노드당 최대 5000개의 채팅방을 만들 수 있습니다.) 고가용성 구축에서 노드당 2500개 이상의 채팅방이 구성된 경우 페일오버 중에 백업 노드에서 호스트되는 5000개 이상의 채팅방이 있을 수 있습니다. 이로 인해 트래픽 로드에 따라 예기치 않은 성능 문제가 발생할 수 있습니다. 시스템에 있는 5000개 룸에 대한 로드는 룸에 있는 참가자 수, 룸의 메시지 교환 속도 및 메시지 크기에 따라서도 달라집니다. Cisco Collaboration Sizing Tool을 사용하여 영구 채팅 구축에 적합한 OVA 설정이 있는지 확인합니다. Collaboration Sizing Tool에 대한 자세한 내용은 다음을 참조하십시오. https://cucst.cloudapps.cisco.com/landing 하위 클러스터의 두 노드 사이에서 채팅방의 균형이 동일하게 조정되도록 하는 것이 좋습니다. IM&P 클러스터에 두 개 이상의 하위 클러스터가 있는 경우 모든 하위 클러스터에 있는 룸에 부하를 분산하는 것이 좋습니다. 현재 IM&P에는 자동으로 룸의 부하를 분산하는 메커니즘이 없습니다. 룸의 부하 분산 책임은 룸을 만드는 사용자와 동일합니다. 룸을 만드는 동안 사용자는 Jabber 기능을 사용하여 룸 생성에 임의 노드를 자동으로 선택하도록 해야 합니다.
임시 채팅 회의실 비공개	임시 채팅 회의실은 기본적으로 공개되지만 다음 구성을 사용하여 구성원 전용으로 구성할 수 있습니다. 1. Cisco Unified CM IM and Presence 관리에서 메시징 > 그룹 채팅 및 영구 채팅을 선택합니다. 2. 회의실은 기본적으로 구성원 전용임 확인란을 선택합니다. 3. 회의실 소유자는 회의실을 구성원 전용으로 할지 여부를 변경할 수 있습니다. 확인란을 선택 취소합니다. 4. 중재자만 구성원 전용 회의실에 사람들을 초대할 수 있습니다. 확인란을 선택 취소합니다. 5. 저장을 클릭합니다. 6. Cisco XCP 텍스트 컨퍼런스 서비스 다시 시작

영구 채팅 예(HA 없음)

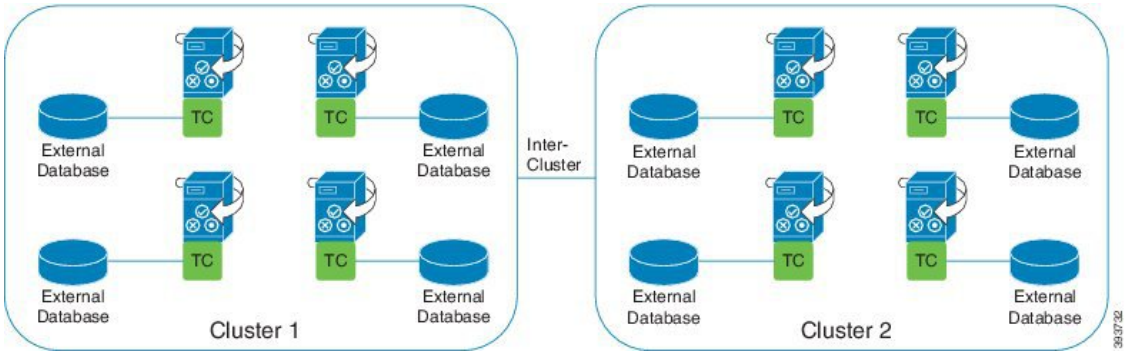
다음 두 예는 영구 채팅 기능을 설명하며, 영구 채팅을 위한 고가용성이 구축되는 인터클러스터 피어링과 함께 영구 채팅 기능을 보여줍니다.

참고 영구 채팅을 구축하는 경우 영구 채팅방에 이중화를 추가하려면 영구 채팅에 대한 고가용성을 표시해야 합니다.

영구 채팅(HA 제외) 모든 클러스터 간에 활성화됨

영구 채팅(HA 제외) 이 클러스터 간 네트워크에 있는 모든 노드에서 활성화됩니다. 모든 노드에는 영구 채팅과 관련된 외부 데이터베이스가 있으므로 모든 노드가 영구 채팅방을 호스팅할 수 있습니다.

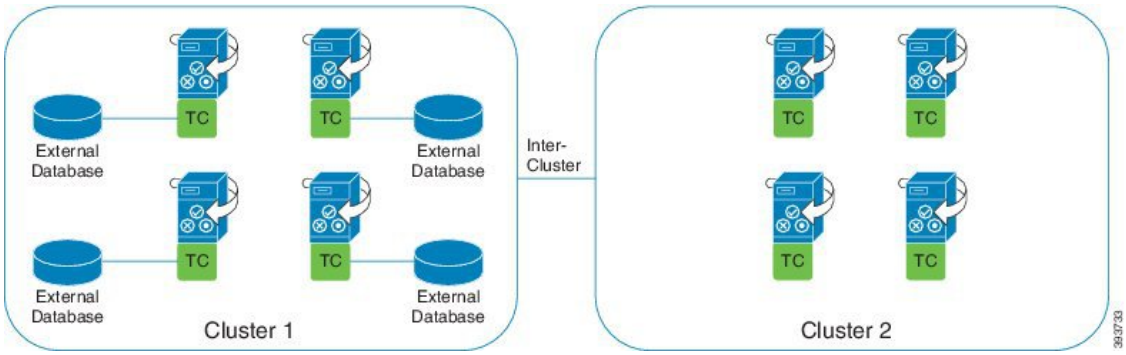
Cisco 텍스트 전화회의 서비스는 어느 클러스터의 모든 노드에서 실행되므로 두 클러스터의 모든 사용자가 어느 클러스터의 모든 노드에서 호스팅되는 영구 채팅방에 참가할 수 있습니다.



영구 채팅(HA 제외) 클러스터 간 네트워크의 한 클러스터에서 활성화됨

클러스터 1의 노드만 영구 채팅(HA 없음)으로 구성되고 외부 데이터베이스가 있습니다. 노드가 영구 채팅방을 호스팅하도록 구성되지 않았으므로 클러스터 2에는 외부 데이터베이스가 필요하지 않습니다.

그러나 어느 한 클러스터의 모든 노드에서 Cisco 텍스트 전화회의 관리자 서비스가 실행 중이기 때문에 클러스터의 모든 사용자가 클러스터 1에서 호스팅되는 영구 채팅방에 참가할 수 있습니다.



IM and Presence의 영구 채팅 경계

이 섹션에서는 IM and Presence의 영구 채팅(PChat) 경계를 나타내는 매트릭스와 다양한 종속성을 명확히 보여주는 예를 설명합니다.

영구 채팅 경계를 파생시키기 위해 다음과 같이 가정합니다.

1. 별칭/서버/하위 클러스터/클러스터당 회의실 수와 관련해서:
    1. 서버에 여러 텍스트 컨퍼런싱 별칭이 포함될 수 있습니다.
    2. 하위 클러스터에는 두 개의 서버(노드)가 있습니다.
    3. 클러스터에는 하위 클러스터가 3개까지 있을 수 있습니다.
2. HA(고가용성)가 활성화되면 지원되는 모든 회의실 수가 절반이 됩니다. 허용되는 최대 채팅 방 수에 허용되는 최대 값은 2,500입니다.
3. 예: 각 회의실에 100명의 사용자가 평균이라고 가정할 때 IM and Presence 서비스는 다음을 지원할 수 있습니다.
    1. HA를 사용하지 않는 경우 서버당 3500 채팅방
    2. HA를 사용하는 경우 서버당 1750 채팅방
    3. 분당 한 회의실에 메시지 하나를 가정하면 서버당 최대 273개 채팅방을 활성화할 수 있습니다.

다음은 이러한 종속성을 명확히 설명하는 몇 가지 예입니다.

다음 수식을 사용하여 지원되는 총 회의실을 희생하여 각 시간 단위로 지원되는 회의실을 늘릴 수 있습니다.

지원되는 새 회의실 수 = 지원되는 현재 회의실 수 * 타임 슬라이스**(%)**당 지원되는 현재 회의실 수 / 타임 슬라이스**(%)**당 지원되는 새 회의실

표 ***21: 25K OVA*** 영구 채팅방 용량 표*(*서버당*)*

회의실당평균사용자수	지원되는 **PChat** 회의실 수	타임슬라이스당지원되는 채팅방 메시지 빈도 **= 1/**분	타임슬라이스당지원되는 채팅방 메시지 빈도 **= 3/**분
2	5000	100%	100%
5	5000	100%	58%
10	5000	99%	33%
15	5000	69%	23%
20	5000	53%	18%

회의실당평균사용자수	지원되는 **PChat** 회의실 수	타임슬라이스당지원되는 채팅방 메시지 빈도 **= 1/**분	타임슬라이스당지원되는 채팅방 메시지 빈도 **= 3/**분
30	5000	36%	12%
50	5000	22%	7%
100	3497	16%	5%
200	2064	14%	5%
500	926	12%	4%
1,000	482	12%	4%

참고 사용자의 30%가 두 대의 디바이스/클라이언트를 가지고 있다고 가정합니다.

25K OVA의 예**:**

회의실당 평균 사용자 수 = 10

메시지 빈도 = 3/분

지원되는 현재 회의실 수 = 5000

타임 슬라이스당 지원되는 현재 회의실 = 33%

타임 슬라이스당 지원되는 새 회의실 = 50%

결과**:**

지원되는 새 회의실 = 5000 * 33/50 = 3300

표 ***22: 15K OVA*** 영구 채팅방 용량 표***(***서버당***)***

회의실당평균사용자수	지원되는 **PChat** 회의실 수	타임슬라이스당지원되는 채팅방 메시지 빈도 **= 1/**분	타임슬라이스당지원되는 채팅방 메시지 빈도 **= 3/**분
2	5000	100%	80%
5	5000	100%	41%
10	5000	67%	22%
15	5000	46%	15%
20	5000	35%	12%
30	5000	24%	8%

회의실당평균사용자수	지원되는 **PChat** 회의실 수	타임슬라이스당지원되는 채팅방 메시지 빈도 **= 1/**분	타임슬라이스당지원되는 채팅방 메시지 빈도 **= 3/**분
50	5000	14%	5%
100	3497	10%	3%
200	2064	9%	3%
500	926	8%	3%
1,000	482	7%	2%

참고 사용자의 30%가 두 대의 디바이스/클라이언트를 가지고 있다고 가정합니다.

15K OVA의 예**:**

회의실당 평균 사용자 수 = 5

메시지 빈도 = 3/분

지원되는 현재 회의실 수 = 5000

타임 슬라이스당 지원되는 현재 회의실 = 41%

타임 슬라이스당 지원되는 새 회의실 = 50%

결과**:**

지원되는 새 회의실 = 5000 * 41/50 = 4100

표 ***23: 5K OVA*** 영구 채팅방 용량 표**(**서버당**)**

회의실당평균사용자수	지원되는 **PChat** 회의실 수	타임슬라이스당지원되는 채팅방 메시지 빈도 **= 1/**분	타임슬라이스당지원되는 채팅방 메시지 빈도 **= 3/**분
2	5000	94%	31%
5	5000	53%	18%
10	4654	33%	11%
15	4261	26%	9%
20	3929	21%	7%
30	3399	17%	6%
50	2677	13%	4%

회의실당 평균 사용자 수	지원되는 **PChat** 회의실 수	타임 슬라이스당 지원되는 채팅방 메시지 빈도 **= 1/**분	타임 슬라이스당 지원되는 채팅방 메시지 빈도 **= 3/**분
100	1748	10%	3%
200	1032	9%	3%
500	463	8%	3%
1,000	241	7%	2%

참고 사용자의 30%가 두 대의 디바이스/클라이언트를 가지고 있다고 가정합니다.

5K OVA의 예**:**

회의실당 평균 사용자 수 = 2

메시지 빈도 = 3/분

지원되는 현재 회의실 수 = 5000

타임 슬라이스당 지원되는 현재 회의실 = 31%

타임 슬라이스당 지원되는 새 회의실 = 50%

결과**:**

지원되는 새 회의실 = 5000 * 31/50 = 3100

18 장

영구 채팅을 위한 고가용성 구성

영구 채팅의 고가용성 개요

영구 채팅의 고가용성(HA)은 영구 채팅방을 사용하고 프레즌스 이중화 그룹으로 구성된 시스템 이중화가 있는 경우 구축할 수있는 옵션 기능입니다.

영구 채팅의 고가용성은 영구 채팅방에 이중화 및 장애 조치 기능을 추가합니다. IM and Presence 서비스 노드 장애 또는 텍스트 전화회의(TC) 서비스가 실패할 경우 해당 서비스에서 호스팅하는 모든 영구 채팅방은 백업 노드 또는 TC 서비스에 의해 자동으로 호스팅됩니다. 장애 조치 후에 Cisco Jabber 클라이언트는 영구 채팅방을 원활하게 계속 사용할 수 있습니다.

외부 데이터베이스

영구 채팅(비 HA)과 영구 채팅 HA 설정의 주요 차이점은 외부 데이터베이스 요구 사항입니다.

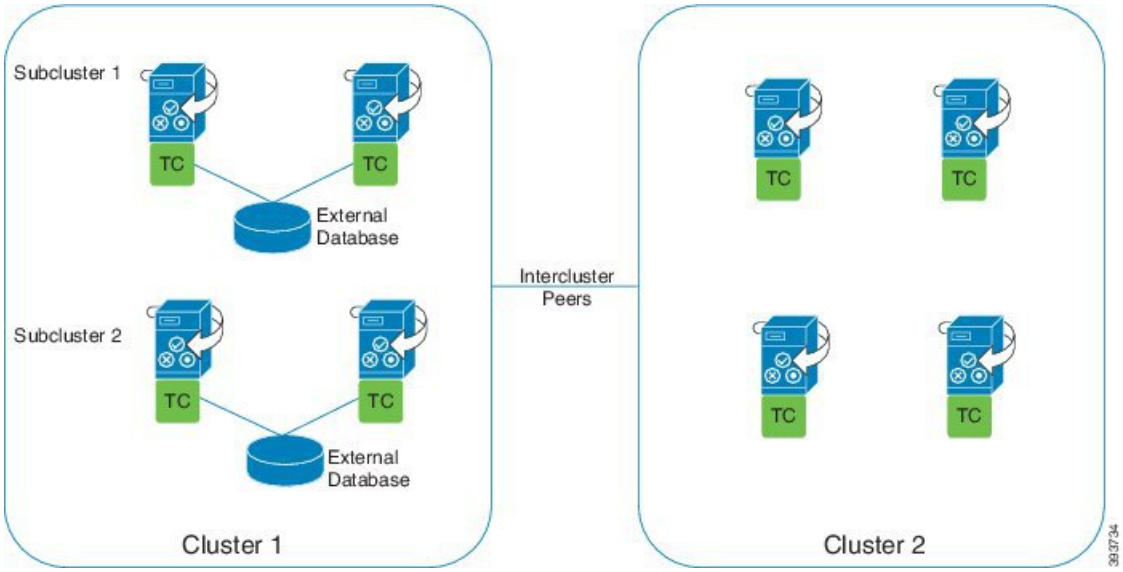
- 영구 채팅이 HA 없이 구축되는 경우 외부 데이터베이스는 개별 채팅 노드에만 연결됩니다. 영구 채팅방을 호스팅하는 각 노드에는 별도의 외부 데이터베이스 인스턴스가 필요합니다. 채팅 노드가 실패하는 경우 해당 노드에서 호스팅된 영구 채팅방은 채팅 노드가 다시 시작될 때까지 사용할 수 없게 됩니다.
- 영구 채팅의 고가용성(HA)이 구축된 경우 외부 데이터베이스 인스턴스는 하위 클러스터(프레즌스 이중화 그룹)의 두 노드에 모두 연결됩니다. 영구 채팅 노드에 장애가 발생하는 경우 하위 클러스터의 백업 노드가 이를 인계 받아 채팅을 중단없이 계속할 수 있습니다.

영구 채팅의 고가용성 - 인터클러스터 예

다음 그림은 영구 채팅 고가용성이 클러스터 1에만 구축된 클러스터 간 네트워크를 표시합니다. 영구 채팅 고가용성을 사용하면 각 하위 클러스터는 외부 데이터베이스를 호스팅합니다. 클러스터 2에는 영구 채팅 고가용성이 활성화되어 있지 않으므로 외부 데이터베이스 요구 사항이 없습니다. 그러

나 Cisco 텍스트 전화회의 관리자 서비스는 모든 노드에서 실행되므로 클러스터 2의 사용자는 클러스터 1에서 호스팅되는 영구 채팅방에 참가할 수 있습니다.

참고 이 예에서는 클러스터 1의 채팅 방만 영구 채팅 방을 호스트 하도록 구성 됩니다. 외부 데이터베이스 인스턴스와 함께 클러스터 2 노드에 영구 채팅 지원을 추가할 수도 있습니다. 이 경우 어느 한 클러스터의 모든 사용자가 어느 한 클러스터의 모든 노드에서 호스팅되는 영구 채팅방에 참가할 수 있습니다.



영구 채팅(비 HA) 및 영구 채팅 HA 요구 사항 비교

영구 채팅방을 구축하는 경우 영구 채팅방에 장애 조치 기능을 추가 할뿐만 아니라 영구 채팅을 위한 고가용성을 구축하는 것이 좋습니다. 그러나, 이는 필수가 아닙니다.

다음 표에서는 고가용성을 사용하거나 사용하지 않고 구축된 영구 채팅 간의 차이점에 대해 설명합니다.

표 *24:* 고가용성을 사용하거나 사용하지 않는 영구 채팅 비교

	영구 채팅**(HA** 없음**)**	영구 채팅 **HA**
데이터베이스 요구 사항	영구 채팅방을 호스팅하는 각 클러스터 노드에 대해 별도의 외부 데이터베이스 인스턴스가 필요합니다. 이러한 외부 데이터베이스 인스턴스는 동일한 외부 데이터베이스 서버에서 생성될 수 있습니다. 권장**:** 최적의 성능 및 확장성을 위해 각 노드 또는 이중화 그룹에 대해 고유한 논리 외부 데이터베이스 인스턴스를 IM and Presence 클러스터에 구축합니다. 그러나, 이는 필수가 아닙니다. 최소 요구 사항**:** IM and Presence 클러스터 간 네트워크에서 영구 채팅을 위해 하나 이상의 외부 데이터베이스 인스턴스가 있어야 합니다. 그러나이 구축은 사용률이 높은 네트워크에서는 적절하지 않을 수 있습니다. 지원 되는 데이터베이스 형식 • PostgreSql(버전 9.1 이상) • Oracle • Microsoft SQL Server	영구 채팅방을 호스팅하는 각 하위 클러스터(프레즌스 이중화 그룹)에 대해 별도의 외부 데이터베이스 인스턴스가 필요합니다. 이러한 외부 데이터베이스 인스턴스는 동일한 외부 데이터베이스 서버에서 생성될 수 있습니다. 권장**:** 최적의 성능 및 확장성을 위해 IM and Presence 클러스터 내의 각 하위 클러스터에 대해 별도의 외부 데이터베이스 인스턴스를 구축합니다. 그러나, 이는 필수가 아닙니다. 최소 요구 사항**:** IM and Presence 클러스터 간 네트워크에서 영구 채팅 HA를 위해 하나 이상의 외부 데이터베이스 인스턴스가 있어야 합니다. 그러나이 구축은 사용률이 높은 네트워크에서는 적절하지 않을 수 있습니다. 지원 되는 데이터베이스 형식 • PostgreSql(버전 9.1 이상) • Oracle • Microsoft SQL Server(11.5(1)SU2)
영구 채팅 노드가 실패할 때의 행동	• 실패한 노드에서 호스팅되는 영구 채팅방은 노드가 다시 복구될 때까지 액세스할 수 없습니다. • 장애가 발생한 노드에서 호스팅되는 사용자는 클러스터 이중화가 구성된 경우 하위 클러스터의 백업 노드로 장애 조치됩니다. 그러나 장애가 발생한 노드에서는 영구 채팅방에 액세스할 수 없습니다.	• 영구 채팅방은 하위 클러스터의 백업 노드로 장애 조치합니다. 사용자는 서비스 중단없이 메시징을 계속할 수 있습니다. • 장애가 발생한 노드에서 호스팅되는 모든 사용자도 장애 조치됩니다.

영구 채팅의 고가용성 필수 조건

영구 채팅을 위한 고가용성을 구성하기 전에 다음 사항을 확인하십시오.

- 영구 채팅방이 활성화되었습니다. 자세한 내용은 채팅방 설정 구성, 198 페이지를 참조하십시오.

- 고가용성은 각 프레즌스 이중화 그룹에서 활성화됩니다. 자세한 내용은 프레즌스 이중화 그룹 작업 흐름, 54 페이지를 참조하십시오.
- 외부 데이터베이스를 구성했습니다. 데이터베이스 설정 및 지원 정보는 *IM and Presence* 서비스 데이터베이스 설정 설명서를 참조하십시오.

영구 채팅의 고가용성 작업 흐름

프로시저

	명령 또는 동작	목적
단계 **1**	외부 데이터베이스 설정, 214 페이지	영구 채팅방이 호스팅되는 각 하위 클러스터에 대해 별도의 외부 데이터베이스 인스턴스가 필요합니다. 이러한 별도의 외부 데이터베이스 인스턴스는 동일한 데이터베이스 서버에서 호스팅될 수 있습니다.
단계 **2**	외부 데이터베이스 연결 추가, 215 페이지	IM and Presence 서비스에서 외부 데이터베이스에 대한 연결을 구성합니다.
단계 **3**	영구 채팅의 고가용성 설정 확인, 215 페이지	영구 채팅 고가용성에 대한 시스템 설정을 확인하십시오.
단계 **4**	Cisco XCP 텍스트 전화회의 관리자 서비스 시작, 216 페이지	모든 노드에서 Cisco XCP 텍스트 전화회의 관리자 서비스가 중지된 경우, 이 절차를 사용하여 서비스를 시작하십시오.
단계 **5**	외부 데이터베이스 병합, 217 페이지	(선택 사항) 영구 채팅이 여러 외부 데이터베이스로 구성된 이전 릴리스에서 업그레이드하는 경우이 절차를 사용하여 외부 데이터베이스를 단일 데이터베이스로 병합합니다.

외부 데이터베이스 설정

영구 채팅을 위한 고가용성을 구축하려면 영구 채팅방이 호스팅되는 각 하위 클러스터에 대해 별도의 외부 데이터베이스 인스턴스가 필요합니다. 이러한 별도의 외부 데이터베이스 인스턴스는 동일한 데이터베이스 서버에서 호스팅될 수 있습니다.

하위 클러스터 쌍의 IM and Presence 노드 (프레 즌 스 그룹 Redudancy) 중복입니다. 6개의 노드로 구성된 IM and Presence 클러스터에는 최대 세 개의 하위 클러스터를 가질 수 있습니다. 6개의 노드로 구성된 IM and Presence 클러스터에서 영구 채팅용 HA가 활성화된 경우 세 개의 외부 데이터베이스 인스턴스와 세 개의 하위 클러스터 쌍이 있습니다.

PostgreSQL, Oracle 또는 Microsoft SQL Server를 외부 데이터베이스 연결에 사용할 수 있습니다. 설정에 대한 자세한 내용은 *IM and Presence* 서비스용 데이터베이스 설정 설명서를 참조하십시오.

다음에 수행할 작업

외부 데이터베이스 연결 추가, 215 페이지

외부 데이터베이스 연결 추가

IM and Presence 서비스에서 영구 채팅 외부 데이터베이스 인스턴스에 대한 고가용성 연결을 구성합니다. 하위 클러스터의 두 노드가 동일하고 고유한 논리 외부 데이터베이스 인스턴스에 지정되었는지 확인합니다.

프로시저

단계 **1** Cisco Unified CM IM and Presence 관리에서 메시징 > 외부 서버 설정 > 외부 데이터베이스를 선택합니다.

단계 **2** 새로 추가를 클릭합니다.

단계 **3** 데이터베이스 이름 필드에 데이터베이스 인스턴스 이름을 입력합니다.

단계 **4** 데이터베이스 유형 드롭다운에서 구축하는 외부 데이터베이스의 유형을 선택합니다.

단계 **5** 데이터베이스에 대한 사용자 이름 및 암호 정보를 입력합니다.

단계 **6** 호스트 이름 필드에 데이터베이스의 호스트이름 또는 IP 주소를 입력합니다.

단계 **7** 나머지 설정은 외부 데이터베이스 설정 창에서 완료합니다. 필드 및 해당 설정에 대한 도움이 필요한 경우 온라인 도움말을 참조하십시오.

단계 **8** 저장을 클릭합니다.

단계 **9** 이 절차를 반복하여 각 외부 데이터베이스 인스턴스에 대한 연결을 만듭니다.

다음에 수행할 작업

영구 채팅의 고가용성 설정 확인, 215 페이지

영구 채팅의 고가용성 설정 확인

이 절차를 사용하여 시스템이 영구 채팅을 위한 고가용성(HA)으로 설정되었는지 확인하십시오.

참고 프레즌스 이중화 그룹(하위 클러스터)에 대해 이미 고가용성을 활성화했으며 채팅방 구성에 영구 채팅이 포함된 경우 영구 채팅의 고가용성을 완료할 수 있습니다.

프로시저

단계 **1** 각 하위 클러스터에서 고가용성이 활성화되었는지 확인합니다.

a) Cisco Unified CM 관리에서 시스템 > 프레즌스 이중화 그룹을 선택합니다.
b) 찾기를 클릭하고 확인하려는 프레즌스 이중화 그룹을 선택합니다.
c) 고가용성 활성화 확인란이 선택되었는지 확인합니다. 확인란이 선택 취소된 경우 확인란을 선택합니다.
d) 저장을 클릭합니다.
e) 클러스터의 각 이중화 그룹에 대해 이러한 단계를 반복합니다.

단계 **2** 영구 채팅이 활성화되었는지 확인합니다.

a) Cisco Unified CM 관리에서 메시징 > 그룹 채팅 및 영구 채팅을 선택합니다.
b) 영구 채팅 활성화 확인란이 선택되었는지 확인합니다. 확인란이 선택 취소된 경우 확인란을 선택합니다.
c) 저장을 클릭합니다.

단계 **3** Cisco Unified CM 관리에서 **Cisco XCP** 텍스트 전화회의 관리자 서비스가 모든 클러스터 노드에서 실행 중인지 확인합니다.

a) 시스템 > 프레즌스 토폴로지를 선택합니다.
b) 각 클러스터 노드에서 보기를 클릭하여 노드 세부 정보를 봅니다.
c) 노드 상태에서 **Cisco XCP** 텍스트 전화회의 관리자 서비스가 시작됨인지 확인합니다.
d) 왼쪽 탐색 모음에서 프레즌스 토폴로지를 클릭하여 클러스터 토폴로지로 돌아가서 모든 클러스터 노드의 상태를 확인할 때까지 위의 단계를 반복합니다.

다음에 수행할 작업

Cisco XCP 텍스트 전화회의 관리자 서비스를 활성화해야 하는 경우 Cisco XCP 텍스트 전화회의 관리자 서비스 시작, 216 페이지.

Cisco XCP 텍스트 전화회의 관리자 서비스 시작

이 절차를 사용하여 Cisco XCP 텍스트 전화회의 관리자 서비스를 시작합니다. 이 서비스는 해당 노드의 사용자가 영구 채팅방에 참가할 수 있도록 모든 클러스터 노드에서 실행되어야 합니다.

프로시저

단계 **1** **Cisco Unified IM and Presence Service** 가용성에서 도구 > 제어 센터 - 기능 서비스를 선택합니다.
단계 **2** 서버 드롭다운 목록에서 IM and Presence 클러스터 노드를 선택하고 이동을 클릭합니다.
단계 **3** **IM and Presence** 서비스에서 **Cisco XCP** 텍스트 전화회의 관리자를 선택하고 시작을 클릭합니다.
단계 **4** 확인을 클릭합니다.
단계 **5** (선택 사항) 서비스가 완전히 다시 시작되었는지 확인하려면 새로 고침을 클릭합니다.

외부 데이터베이스 병합

이 절차를 사용하여 외부 데이터베이스를 병합합니다.

참고 외부 데이터베이스 병합에 Microsoft SQL 데이터베이스는 지원되지 않습니다.

(선택 사항) 11.5(1) 이전 릴리스에서 업그레이드했고 여러 외부 데이터베이스를 사용하여 이중화를 관리하는 경우 외부 데이터베이스 병합 도구를 사용하여 외부 데이터베이스를 단일 데이터베이스로 병합합니다.

예제

11.5(1) 이전 릴리스에서 업그레이드했고 각 영구 채팅 노드가 별도의 외부 데이터베이스 인스턴스에 연결되도록 구성된 영구 채팅이 있는 경우 이 절차를 사용하여 하위 클러스터의 두 데이터베이스를 두 노드에 연결하는 단일 데이터베이스로 병합합니다.

시작하기 전에

- 2개의 소스 대상 데이터베이스가 프레즌스 이중화 그룹의 각 IM and Presence Service 노드에 올바르게 할당되었는지 확인합니다. 그러면 두 스키마가 모두 유효한지 확인됩니다.
- 대상 데이터베이스의 테이블스페이스를 백업합니다.
- 대상 데이터베이스에 새로 병합된 데이터베이스를 위한 충분한 공간이 있는지 확인합니다.
- 원본 및 대상 데이터베이스에 대해 생성된 데이터베이스 사용자에게 다음 명령을 실행할 권한이 있는지 확인하십시오.
  - `CREATE TABLE`
  - `CREATE PUBLIC DATABASE LINK`
- 데이터베이스 사용자에게 이러한 권한이 없는 경우 다음 명령을 사용하여 권한을 부여할 수 있습니다.
  - PostgreSQL:

    `CREATE EXTENTION` - 그러면 dblink가 생성되고 수퍼 사용자 또는 dbowner 권한이 필요합니다. 그런 후에 다음을 실행하여 dblink에 대한 권한을 실행합니다.

    ```
    GRANT EXECUTE ON FUNCTION DBLINK_CONNECT(text) to <user>

    GRANT EXECUTE ON FUNCTION DBLINK_CONNECT(text,text) to <user>
    ```

  - Oracle:

    ```
    GRANT CREATE TABLE TO <user_name>;

    GRANT CREATE PUBLIC DATABASE LINK TO <user_name>;
    ```

- PostgreSQL 외부 데이터베이스를 사용하는 경우 pg_hba.conf 파일에 다음 액세스가 구성되어 있는지 확인하십시오.

- IM and Presence 게시자 노드는 각 외부 데이터베이스에 대한 모든 액세스 권한이 있어야 합니다.
- 외부 PostgreSQL 데이터베이스는 각 데이터베이스 인스턴스에 대한 모든 액세스 권한이 있어야 합니다. 예를 들어 외부 데이터베이스가 192.168.10.1에 구성된 경우 각 데이터베이스 인스턴스는 pg_hba.conf 파일에서 `host dbName username 192.168.10.0/24 password`로 구성되어야 합니다.

프로시저

단계 **1** IM and Presence 서비스 게시자 노드에서 **Cisco Unified CM IM and Presence** 관리에 로그인합니다.

단계 **2** 프레즌스 이중화 이중화 그룹의 각 IM and Presence 노드에 대한 시스템 > 서비스 창에서 Cisco XCP 텍스트 전화회의 서비스를 중지합니다.

단계 **3** 메시징 > 외부 서버 설정 > 외부 데이터베이스 작업을 클릭합니다.

단계 **4** 병합 작업 목록을 표시하려면 찾기를 클릭합니다. 병합 작업 추가를 선택하여 새 작업을 추가합니다.

단계 **5** 외부 데이터베이스 병합 창에서 다음 세부 정보를 입력합니다.

- 데이터베이스 유형 드롭다운 목록에서 **Oracle** 또는 **Postgres**를 선택합니다.
- 두 원본 데이터베이스의 IP 주소와 호스트 이름 및 병합된 데이터가 포함될 대상 데이터베이스를 선택합니다.

데이터베이스 유형으로 Oracle을 선택한 경우, 테이블 스페이스 이름과 데이터베이스 이름을 입력합니다. Postgres를 데이터베이스 유형으로 선택한 경우에는 데이터베이스 이름을 입력합니다.

단계 **6** 기능 테이블 창에 텍스트 Conference(TC) 확인란이 기본적으로 선택됩니다. 현재 릴리스의 경우 다른 옵션은 사용할 수 없습니다.

단계 **7** 선택한 테이블 유휴성 검사를 클릭합니다.

참고 Cisco XCP 텍스트 전화회의 서비스가 중지되지 않은 경우 오류 메시지가 나타납니다. 서비스가 중지되었으면 유효성 검사가 완료됩니다.

단계 **8** 유효성 검사 세부 정보 창에 오류가 없는 경우 선택한 테이블 병합을 클릭합니다.

단계 **9** 병합이 성공적으로 완료되면 외부 데이터베이스 작업 찾기 및 나열 창이 로드됩니다. 찾기를 클릭하여 창을 새로 고치고 새 작업을 봅니다.

찾기를 클릭하여 창을 새로 고치고 새 작업을 봅니다.

세부 정보를 보려는 경우 작업의 **ID**를 클릭합니다.

단계 **10** Cisco XCP 라우터 서비스 다시 시작.

단계 **11** IM and Presence 서비스 노드에서 Cisco XCP 텍스트 전화회의 서비스를 시작합니다.

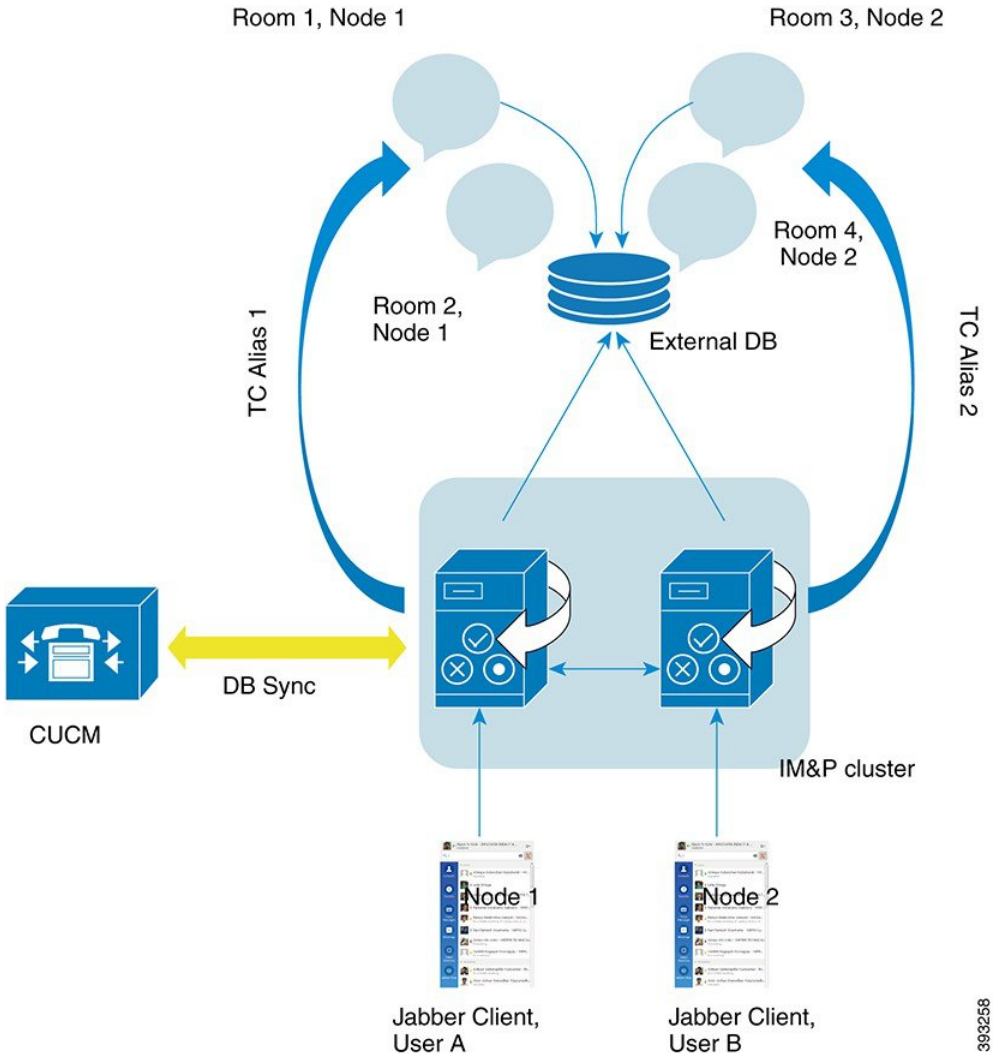
단계 **12** 새로 병합된 외부 데이터베이스(대상 데이터베이스)를 프레즌스 이중화 그룹에 다시 할당해야 합니다

영구 채팅의 고가용성 사용 사례

다음 흐름은 장애 조치 및 페일백에 대한 영구 채팅 흐름의 고가용성을 보여줍니다. 이 예에서는 두 개의 노드가 있는 IM and Presence 클러스터에 대해 설명합니다. IM and Presence 클러스터는 최대 6개의 노드를 가질 수 있으며 3개의 하위 클러스터를 허용합니다. 영구 채팅방이 모든 노드에서 호스팅되는 경우 3개의 별도 외부 데이터베이스 인스턴스가 필요합니다.

참고 이 기능 향상을 위해 TC(텍스트 전화회의) 서비스가 중요한 서비스가 되었습니다. 결과적으로 장애 조치가 Cisco XCP 라우터 서비스와 같은 노드의 다른 중요한 서비스의 장애로 인해 발생하더라도 TC 고가용성 장애 조치 흐름은 동일하게 유지됩니다.

그림 *7:* 영구 채팅을 위한 고가용성 구조



영구 채팅의 고가용성 장애 조치 사용 사례

이 예의 경우 2개의 고가용성(HA) 쌍 또는 하위 클러스터가 있는 4개의 IM and Presence 노드에 4명의 사용자가 있습니다. 사용자는 다음과 같이 할당됩니다.

하위 클러스터 **1**	하위 클러스터 **2**
• Andy는 노드 1A에 있고 1A는 채팅방을 호스팅 • Bob은 노드 1B에 있음	• Catherine은 노드 2A에 있음 • Deborah는 노드 2B에 있음

1. 4명의 사용자 모두 노드 1A에서 호스팅되는 동일한 채팅방에서 채팅하고 있습니다.
2. 노드 1A에서 텍스트 전화회의(TC) 서비스가 실패합니다.
3. 90초 후 SRM(서버 복구 관리자)은 TC 중요 서비스의 실패를 판별하고 자동 장애 조치를 시작합니다.
4. HA 상태 백업 모드에서 실행 중 상태로 전환하기 전에 노드 1B는 1A에서 사용자를 인계하고 실행 중이 아닌 중요 서비스 대체 작동됨 상태로 전환합니다.
5. HA 장애 조치 모델에 따라 Andy는 노드 1A에서 자동으로 로그아웃되고 백업 노드 1B에 로그인됩니다.
6. 다른 사용자는 영향을 받지 않지만 이제 노드 1B에서 호스팅되는 채팅방에 메시지를 계속 게시합니다.
7. Andy는 영구 채팅방에 입장하고 메시지를 계속 읽거나 룸에 게시합니다.

영구 채팅의 고가용성 폴백 사용 사례

이 예의 경우 2개의 고가용성(HA) 쌍 또는 하위 클러스터가 있는 4개의 IM and Presence 노드에 4명의 사용자가 있습니다. 사용자는 다음과 같이 할당됩니다.

하위 클러스터 **1**	하위 클러스터 **2**
• Andy는 노드 1A에 있고 1A는 채팅방을 호스팅 • Bob은 노드 1B에 있음	• Catherine은 노드 2A에 있음 • Deborah는 노드 2B에 있음

1. 4명의 사용자 모두 노드 1A에서 호스팅되는 동일한 채팅방에서 채팅하고 있습니다.
2. 노드 1A에서 텍스트 전화회의(TC) 서비스가 실패합니다.
3. HA 상태 백업 모드에서 실행 중으로 전환하기 전에 노드 1B는 1A에서 사용자를 인계하고 실행 중이 아닌 중요 서비스 대체 작동됨으로 전환합니다.
4. HA 장애 조치 모델에 따라 Andy는 자동으로 로그아웃되고 백업 노드 1B에 로그인됩니다.

5. Bob, Catherine 및 Deborah는 영향을 받지 않지만 이제 노드 1B에서 호스팅되는 채팅방에 메시지를 계속 게시합니다.
6. IM and Presence IM 서비스 관리자가 수동 폴백을 시작합니다.
7. 노드 1A는 회수 중으로 전환되고 노드 1B는 폴백 중으로 전환됩니다.
8. Andy는 노드 1B에서 로그아웃됩니다. Bob, Catherine 및 Deborah는 영구 채팅방을 계속 사용하고 폴백이 발생하면 룸이 노드 1A로 다시 이동합니다.
9. 노드 1B는 HA 상태 폴백 중에서 정상으로 폴백하고 피어 노드 룸을 언로드합니다.
10. 노드 1A는 HA 상태 **Taking Back**에서 정상으로 이동하고 채팅방을 다시로드합니다.
11. Andy는 영구 채팅방에 입장하고 메시지를 계속 읽거나 룸에 게시합니다.

19 장

관리되는 파일 전송 구성

관리되는 파일 전송 개요

MFT(관리되는 파일 전송)를 사용하면 Cisco Jabber와 같은 IM and Presence 서비스를 통해 다른 사용자, 임시 그룹 채팅 방 및 영구 채팅 방에 파일을 전송할 수 있습니다. 파일은 외부 파일 서버의 저장소에 저장되며, 트랜잭션은 외부 데이터베이스에 기록됩니다.

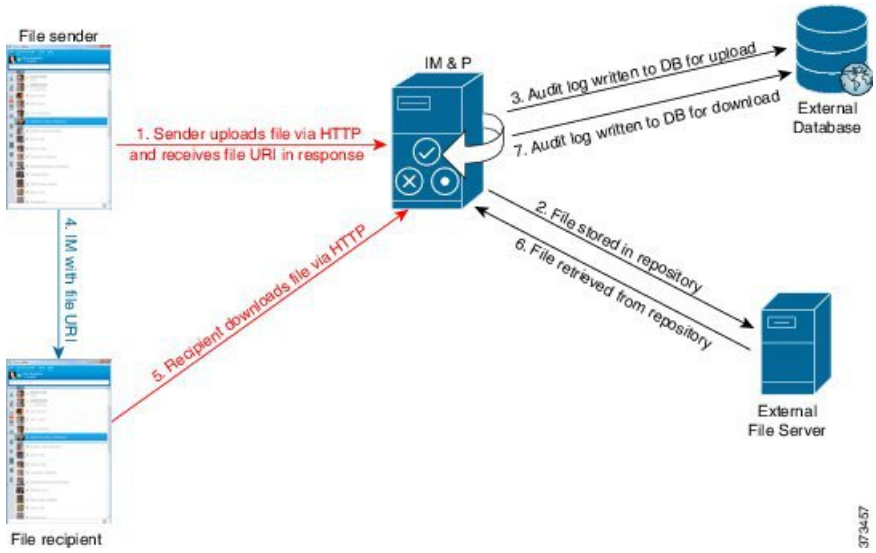
관리되는 파일 전송 기능을 구축하려면 다음 서버도 구축해야 합니다.

- 외부 데이터베이스 - 모든 파일 전송은 외부 데이터베이스에 기록됩니다.
- 외부 파일 서버 - 전송된 각 파일의 사본은 외부 파일 서버의 저장소에 저장됩니다.

참고 이 구성은 파일 전송과 관련된 것이며, 규정 준수를 위한 메시지 아카이버 기능에는 영향을 미치지 않습니다.

사용 사례는 다음을 참조하십시오. 관리되는 파일 전송 통화 흐름, 224 페이지

관리되는 파일 전송 통화 흐름



1. 보낸 사람은 파일을 HTTP를 통해 IM and Presence 서버에 업로드하고 서버는 파일에 대한 URI로 응답합니다.
2. IM and Presence 서비스 서버는 파일을 저장소로 파일 서버 저장소로 보냅니다.
3. IM and Presence 서비스는 외부 데이터베이스 로그 테이블에 항목을 기록하여 업로드를 기록합니다.
4. 보낸 사람은 받는 사람에게 IM을 보냅니다. IM에는 파일의 URI이 포함됩니다.
5. 수신자가 파일에 대한 IM and Presence 서비스에 대한 HTTP 요청을 보냅니다. IM and Presence 서비스는 저장소(6)에서 파일을 읽고 로그 테이블(7)에 다운로드를 기록한 다음 파일을 수신자에게 보냅니다.

그룹 채팅 또는 영구 채팅 방에 파일을 전송하는 흐름도 유사합니다. 단, 송신자는 채팅 방으로 IM을 전송하고, 각 채팅 방 참가자는 파일 다운로드에 대한 별도의 요청을 전송합니다.

참고 파일 업로드가 발생하면 특정 도메인의 엔터프라이즈에서 사용 가능한 모든 관리되는 파일 전송 서비스 중 하나가 선택됩니다. 이 관리되는 파일 전송 서비스가 실행되는 노드와 연결된 외부 데이터베이스 및 외부 파일 서버에 파일 업로드 내용이 기록됩니다. 사용자가 이 파일을 다운로드하면 이 두 번째 사용자의 위치와 상관없이, 동일한 관리되는 파일 전송 서버가 요청을 처리하고 동일한 외부 데이터베이스 및 외부 파일 서버에 내용을 기록합니다.

관리되는 파일 전송 필수 조건

- 외부 데이터베이스 및 외부 파일 서버도 구축해야 합니다.

- 모든 클라이언트는 자신이 할당된 IM and Presence 서비스 노드의 전체 FQDN을 확인할 수 있어야 합니다. 관리되는 파일 전송이 작동하기 위해 필요합니다.

외부 데이터베이스 필수 조건

팁 영구 채팅 및/또는 메시지 아카이버를 구축하는 경우 모든 기능에 동일한 외부 데이터베이스 및 파일 서버를 할당할 수 있습니다. 서버 용량을 결정할 때 잠재적인 IM 트래픽, 전송된 파일 수 및 파일 크기를 고려해야 합니다.

외부 데이터베이스를 설치하고 구성합니다. 지원되는 데이터베이스를 포함한 자세한 내용은 *IM and Presence* 서비스용 데이터베이스 설정 설명서를 참조하십시오.

다음 지침도 따르십시오.

- IM and Presence 서비스 클러스터에 있는 IM and Presence 서비스 노드마다 하나의 고유한 논리적 외부 데이터베이스 인스턴스가 필요합니다.
- 외부 데이터베이스는 가상화된 플랫폼과 가상화되지 않은 플랫폼 모두에서 지원됩니다.
- 기록되는 메타데이터의 전체 목록은 *Cisco Unified Communications Manager*의 *IM and Presence* 서비스용 데이터베이스 설정의 "외부 데이터베이스 도구" 장에서 AFT_LOG 표를 참조하십시오.
- IPv6을 사용하여 외부 데이터베이스에 연결하는 경우 IPv6 설정에 대한 자세한 내용은 IPv6 작업 흐름 구성, 36 페이지을 확인하십시오.

외부 파일 서버 요구 사항

외부 파일 서버를 설정할 때 다음 지침을 따르십시오.

- 파일 서버 용량에 따라 각 IM and Presence 서비스 노드에는 고유한 Cisco XCP 파일 전송 관리자 파일 서버 디렉터리가 필요하지만, 동일한 물리적 파일 서버 설치를 노드 간에 공유할 수 있습니다.
- 파일 서버는 ext4 파일 시스템, SSHv2 및 SSH 도구를 지원해야 합니다.
- 파일 서버는 4.9, 6.x 및 7.x 사이의 OpenSSH 버전을 지원해야 합니다.

중요 이 노트는 릴리스 14SU3부터 적용할 수 있습니다.

참고 OpenSSH 버전 8.x는 릴리스 14SU3부터 지원됩니다.

- IM and Presence 서비스와 외부 파일 서버 간 네트워크 처리량은 초당 60메가바이트보다 커야 합니다.

  관리되는 파일 전송을 활성화한 후에 파일 서버 전송 속도를 결정한 후에 `show fileserver transferspeed` CLI 명령을 사용할 수 있습니다. 시스템이 사용 중일 때 이 명령을 실행하면 명령에서 반환되는 값에 영향을 줄 수 있습니다. 이 명령에 대한 자세한 정보는 이 링크에 있는 *Cisco Unified Communications* 솔루션의 명령줄 인터페이스 안내서를 참조하십시오

외부 파일 서버에 대한 파티션 권장 사항

서버에서 실행되는 다른 애플리케이션이 사용하지 못하도록 파일 전송 저장소 전용으로 하나 이상의 별도 파티션을 만드는 것이 좋습니다. 모든 파일 저장소 디렉터리를 이 파티션에 만들어야 합니다.

다음을 고려하십시오.

- 파티션을 만들 경우 IM and Presence 서비스 기본 파일 크기 설정(0)을 사용하면 파일을 최대 4GB까지 전송할 수 있습니다. 관리되는 파일 전송을 설정할 때에는 이 설정을 낮출 수 있습니다.
- 일일 업로드 수 및 평균 파일 크기를 고려합니다.
- 예상되는 파일의 양을 수용할 수 있을 정도로 파티션의 디스크 공간이 충분한지 확인합니다.
- 예를 들어, 사용자 12,000명이 평균 파일 크기 100KB로 시간당 2개의 파일을 전송하는 경우 하루 8시간 동안 19.2GB가 필요합니다

외부 파일 서버에 대한 디렉터리 구조

첫 번째 파일 전송이 발생하면 다음 예에서 설명하는 것처럼 타임스탬프 처리된 하위 디렉터리가 자동으로 생성됩니다.

- IM and Presence 서비스 노드에서 `/opt/mftFileStore/node_1/` 경로를 만듭니다.
- 디렉터리 `/files/`가 자동 생성됩니다.
- 세 개의 `/chat_type/` 디렉터리(`im`, `persistent`, `groupchat`)가 자동으로 생성됩니다.
- 날짜 디렉터리 `/YYYYMMDD/`가 자동 생성됩니다.
- 시간 디렉터리 `/HH/`가 자동 생성됩니다. 시간당 파일이 1,000개 이상 전송되는 경우 추가 롤오버 디렉터리 `/HH.n/`이 생성됩니다.
- 자동 생성되고 인코딩된 리소스 이름으로 파일이 저장되므로, 앞으로는 `file_name`으로 언급됩니다.

이 예에서 파일의 전체 경로:
`/opt/mftFileStore/node_1/files/chat_type/YYYYMMDD/HH/file_name`

이 예제 경로 사용 시:

- 2014년 8월 11일 15.00~15.59 UTC에 1대1 IM 중 전송된 파일은 다음 디렉터리에 저장됩니다./`opt/mftFileStore/node_1/files/im/20140811/15/file_name`

2014년 8월 11일 16.00~16.59 UTC에 영구 그룹 채팅 중 전송된 파일은 다음 디렉터리에 저장됩니다. `/opt/mftFileStore/node_1/files/persistent/20140811/16/file_name`

- 2014년 8월 11일 16.00~16.59 UTC에 임시 채팅 중 전송된 1001번째 파일은 다음 디렉터리에 저장됩니다. `/opt/mftFileStore/node_1/files/groupchat/20140811/16.1/file_name`
- 한 시간 동안 파일 전송이 발생하지 않으면 해당 기간에 대해 디렉터리가 생성되지 않습니다.

참고 IM and Presence 서비스와 파일 서버 간 트래픽은 SSHFS를 사용하여 암호화되지만, 파일 내용은 암호화되지 않은 형식으로 파일 서버에 기록됩니다.

외부 파일 서버에 대한 사용자 인증

IM and Presence 서비스는 SSH 키를 사용하여 자체 인증 및 파일 서버 인증을 수행합니다.

- IM and Presence 서비스 공개 키는 파일 서버에 저장됩니다.
- 연결하는 동안 SSHFS는 IM and Presence 서비스 개인 키를 확인합니다. 이렇게 하면 모든 파일의 내용이 암호화됩니다.
- 파일 서버 공개 키는 IM and Presence 서비스에 저장됩니다. 이렇게 하면 IM and Presence 서비스는 구성된 파일 서버에 연결되며 메시지 가로채기(man-in-the-middle) 공격이 최소화됩니다.

참고 노드의 할당이 제거되면 노드 공개 키가 무효화됩니다. 노드가 다시 할당되면 새 노드 공개 키가 자동으로 생성되며 외부 파일 서버에서 키를 다시 구성해야 합니다.

외부 파일 서버 요구 사항

외부 파일 서버를 설정할 때 다음 지침을 따르십시오.

- 파일 서버 용량에 따라 각 IM and Presence 서비스 노드에는 고유한 Cisco XCP 파일 전송 관리자 파일 서버 디렉터리가 필요하지만, 동일한 물리적 파일 서버 설치를 노드 간에 공유할 수 있습니다.
- 파일 서버는 ext4 파일 시스템, SSHv2 및 SSH 도구를 지원해야 합니다.
- 파일 서버는 4.9, 6.x 및 7.x 사이의 OpenSSH 버전을 지원해야 합니다.

중요 이 노트는 릴리스 14SU3부터 적용할 수 있습니다.

참고 OpenSSH 버전 8.x는 릴리스 14SU3부터 지원됩니다.

- IM and Presence 서비스와 외부 파일 서버 간 네트워크 처리량은 초당 60메가바이트보다 커야 합니다.

  관리되는 파일 전송을 활성화한 후에 파일 서버 전송 속도를 결정한 후에 `show fileserver transferspeed` CLI 명령을 사용할 수 있습니다. 시스템이 사용 중일 때 이 명령을 실행하면 명령에서 반환되는 값에 영향을 줄 수 있습니다. 이 명령에 대한 자세한 정보는 이 링크에 있는 *Cisco Unified Communications* 솔루션의 명령줄 인터페이스 안내서를 참조하십시오

외부 파일 서버에 대한 파티션 권장 사항

서버에서 실행되는 다른 애플리케이션이 사용하지 못하도록 파일 전송 저장소 전용으로 하나 이상의 별도 파티션을 만드는 것이 좋습니다. 모든 파일 저장소 디렉터리를 이 파티션에 만들어야 합니다.

다음을 고려하십시오.

- 파티션을 만들 경우 IM and Presence 서비스 기본 파일 크기 설정(0)을 사용하면 파일을 최대 4GB까지 전송할 수 있습니다. 관리되는 파일 전송을 설정할 때에는 이 설정을 낮출 수 있습니다.
- 일일 업로드 수 및 평균 파일 크기를 고려합니다.
- 예상되는 파일의 양을 수용할 수 있을 정도로 파티션의 디스크 공간이 충분한지 확인합니다.
- 예를 들어, 사용자 12,000명이 평균 파일 크기 100KB로 시간당 2개의 파일을 전송하는 경우 하루 8시간 동안 19.2GB가 필요합니다

외부 파일 서버에 대한 디렉터리 구조

첫 번째 파일 전송이 발생하면 다음 예에서 설명하는 것처럼 타임스탬프 처리된 하위 디렉터리가 자동으로 생성됩니다.

- IM and Presence 서비스 노드에서 `/opt/mftFileStore/node_1/` 경로를 만듭니다.
- 디렉터리 `/files/`가 자동 생성됩니다.
- 세 개의 `/chat_type/` 디렉터리(`im`, `persistent`, `groupchat`)가 자동으로 생성됩니다.
- 날짜 디렉터리 `/YYYYMMDD/`가 자동 생성됩니다.
- 시간 디렉터리 `/HH/`가 자동 생성됩니다. 시간당 파일이 1,000개 이상 전송되는 경우 추가 롤오버 디렉터리 `/HH.n/`이 생성됩니다.
- 자동 생성되고 인코딩된 리소스 이름으로 파일이 저장되므로, 앞으로는 `file_name`으로 언급됩니다.

이 예에서 파일의 전체 경로:
`/opt/mftFileStore/node_1/files/chat_type/YYYYMMDD/HH/file_name`

이 예제 경로 사용 시:

- 2014년 8월 11일 15.00~15.59 UTC에 1대1 IM 중 전송된 파일은 다음 디렉터리에 저장됩니다./`opt/mftFileStore/node_1/files/im/20140811/15/file_name`

2014년 8월 11일 16.00~16.59 UTC에 영구 그룹 채팅 중 전송된 파일은 다음 디렉터리에 저장됩니다. `/opt/mftFileStore/node_1/files/persistent/20140811/16/file_name`

- 2014년 8월 11일 16.00~16.59 UTC에 임시 채팅 중 전송된 1001번째 파일은 다음 디렉터리에 저장됩니다. `/opt/mftFileStore/node_1/files/groupchat/20140811/16.1/file_name`
- 한 시간 동안 파일 전송이 발생하지 않으면 해당 기간에 대해 디렉터리가 생성되지 않습니다.

참고 IM and Presence 서비스와 파일 서버 간 트래픽은 SSHFS를 사용하여 암호화되지만, 파일 내용은 암호화되지 않은 형식으로 파일 서버에 기록됩니다.

외부 파일 서버에 대한 사용자 인증

IM and Presence 서비스는 SSH 키를 사용하여 자체 인증 및 파일 서버 인증을 수행합니다.

- IM and Presence 서비스 공개 키는 파일 서버에 저장됩니다.
- 연결하는 동안 SSHFS는 IM and Presence 서비스 개인 키를 확인합니다. 이렇게 하면 모든 파일의 내용이 암호화됩니다.
- 파일 서버 공개 키는 IM and Presence 서비스에 저장됩니다. 이렇게 하면 IM and Presence 서비스는 구성된 파일 서버에 연결되며 메시지 가로채기(man-in-the-middle) 공격이 최소화됩니다.

참고 노드의 할당이 제거되면 노드 공개 키가 무효화됩니다. 노드가 다시 할당되면 새 노드 공개 키가 자동으로 생성되며 외부 파일 서버에서 키를 다시 구성해야 합니다.

외부 파일 서버에 대한 파티션 권장 사항

서버에서 실행되는 다른 애플리케이션이 사용하지 못하도록 파일 전송 저장소 전용으로 하나 이상의 별도 파티션을 만드는 것이 좋습니다. 모든 파일 저장소 디렉터리를 이 파티션에 만들어야 합니다.

다음을 고려하십시오.

- 파티션을 만들 경우 IM and Presence 서비스 기본 파일 크기 설정(0)을 사용하면 파일을 최대 4GB까지 전송할 수 있습니다. 관리되는 파일 전송을 설정할 때에는 이 설정을 낮출 수 있습니다.
- 일일 업로드 수 및 평균 파일 크기를 고려합니다.
- 예상되는 파일의 양을 수용할 수 있을 정도로 파티션의 디스크 공간이 충분한지 확인합니다.
- 예를 들어, 사용자 12,000명이 평균 파일 크기 100KB로 시간당 2개의 파일을 전송하는 경우 하루 8시간 동안 19.2GB가 필요합니다

외부 파일 서버 사용자 인증

IM and Presence 서비스는 SSH 키를 사용하여 자체 인증 및 파일 서버 인증을 수행합니다.

- IM and Presence 서비스 공개 키는 파일 서버에 저장됩니다.
- 연결하는 동안 SSHFS는 IM and Presence 서비스 개인 키를 확인합니다. 이렇게 하면 모든 파일의 내용이 암호화됩니다.
- 파일 서버 공개 키는 IM and Presence 서비스에 저장됩니다. 이렇게 하면 IM and Presence 서비스는 구성된 파일 서버에 연결되며 메시지 가로채기(man-in-the-middle) 공격이 최소화됩니다.

참고 노드의 할당이 제거되면 노드 공개 키가 무효화됩니다. 노드가 다시 할당되면 새 노드 공개 키가 자동으로 생성되며 외부 파일 서버에서 키를 다시 구성해야 합니다.

외부 파일 서버 디렉터리 구조

첫 번째 파일 전송이 발생하면 다음 예에서 설명하는 것처럼 타임스탬프 처리된 하위 디렉터리가 자동으로 생성됩니다.

- IM and Presence 서비스 노드에서 `/opt/mftFileStore/node_1/` 경로를 만듭니다.
- 디렉터리 `/files/`가 자동 생성됩니다.
- 세 개의 `/chat_type/` 디렉터리(`im`, `persistent`, `groupchat`)가 자동으로 생성됩니다.
- 날짜 디렉터리 `/YYYYMMDD/`가 자동 생성됩니다.
- 시간 디렉터리 `/HH/`가 자동 생성됩니다. 시간당 파일이 1,000개 이상 전송되는 경우 추가 롤오버 디렉터리 `/HH.n/`이 생성됩니다.
- 자동 생성되고 인코딩된 리소스 이름으로 파일이 저장되므로, 앞으로는 `file_name`으로 언급됩니다.

이 예에서 파일의 전체 경로:
`/opt/mftFileStore/node_1/files/chat_type/YYYYMMDD/HH/file_name`

이 예제 경로 사용 시:

- 2014년 8월 11일 15.00~15.59 UTC에 1대1 IM 중 전송된 파일은 다음 디렉터리에 저장됩니다./`opt/mftFileStore/node_1/files/im/20140811/15/file_name`

  2014년 8월 11일 16.00~16.59 UTC에 영구 그룹 채팅 중 전송된 파일은 다음 디렉터리에 저장됩니다. `/opt/mftFileStore/node_1/files/persistent/20140811/16/file_name`
- 2014년 8월 11일 16.00~16.59 UTC에 임시 채팅 중 전송된 1001번째 파일은 다음 디렉터리에 저장됩니다. `/opt/mftFileStore/node_1/files/groupchat/20140811/16.1/file_name`
- 한 시간 동안 파일 전송이 발생하지 않으면 해당 기간에 대해 디렉터리가 생성되지 않습니다.

참고 IM and Presence 서비스와 파일 서버 간 트래픽은 SSHFS를 사용하여 암호화되지만, 파일 내용은 암호화되지 않은 형식으로 파일 서버에 기록됩니다.

관리되는 파일 전송 작업 흐름

IM and Presence 서비스에서 관리되는 파일 전송 기능을 설정하고 외부 파일 서버를 설정하려면 다음 작업을 완료하십시오.

시작하기 전에

관리되는 파일 전송을 위해 외부 데이터베이스와 외부 파일 서버를 모두 설정합니다. 요구 사항은 다음을 참조하십시오.

- 외부 데이터베이스 필수 조건, 225 페이지
- 외부 파일 서버 요구 사항, 225 페이지

외부 데이터베이스를 구성하는 방법에 대한 내용은 https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html에서 *IM and Presence Service* 외부 데이터베이스 설정 설명서를 참조하십시오.

프로시저

	명령 또는 동작	목적
단계 **1**	외부 데이터베이스 연결 추가, 232 페이지	IM and Presence 서비스에서 외부 데이터베이스에 대한 연결을 구성합니다.
단계 **2**	외부 파일 서버 설정, 233 페이지	파일 서버에서 사용자, 디렉터리, 소유권, 사용 권한 및 기타 작업을 설정하기 전에 외부 파일 서버를 설정합니다.
단계 **3**	외부 파일 서버에 대한 사용자 만들기, 234 페이지	외부 파일 서버에 대한 사용자를 설정합니다.
단계 **4**	외부 파일 서버용 디렉터리 설정, 235 페이지	외부 파일 서버의 최상위 디렉터리 구조를 설정합니다.
단계 **5**	외부 파일 서버 공개 키 얻기, 236 페이지	외부 파일 서버 공개 키를 얻습니다.
단계 **6**	IM and Presence 서비스에서 외부 파일 서버 프로비저닝, 237 페이지	다음 외부 파일 서버 정보를 확인합니다.

	명령 또는 동작	목적
단계 **7**	Cisco XCP 파일 전송 관리자 활성화 확인, 239 페이지	관리되는 파일 전송을 활성화할 각 노드에서 Cisco XCP 파일 전송 관리자 서비스가 활성 상태여야 합니다.
단계 **8**	관리되는 파일 전송 활성화, 240 페이지	IM and Presence 서비스에서 관리되는 파일 전송을 활성화합니다.
단계 **9**	외부 서버 상태 확인, 242 페이지	외부 데이터베이스 설정 및 외부 파일 서버 설정에 문제가 없는지 확인하십시오.

외부 데이터베이스 연결 추가

IM and Presence 서비스에서 외부 데이터베이스에 대한 연결을 구성합니다. 관리되는 파일 전송을 사용하려면 각 IM and Presence 서비스 클러스터 노드마다 고유한 외부 데이터베이스 인스턴스가 필요합니다.

시작하기 전에

각 외부 데이터베이스를 설정합니다. 자세한 내용은 다음 위치에 있는 *M and Presence Service* 외부 데이터베이스 설정 설명서를 참조하십시오.

https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html

프로시저

단계 **1** Cisco Unified CM IM and Presence 관리에서 메시징 > 외부 서버 설정 > 외부 데이터베이스를 선택합니다.

단계 **2** 새로 추가를 클릭합니다.

단계 **3** 데이터베이스 이름 필드에 데이터베이스 인스턴스 이름을 입력합니다.

단계 **4** 데이터베이스 유형 드롭다운에서 구축하는 외부 데이터베이스의 유형을 선택합니다.

단계 **5** 데이터베이스에 대한 사용자 이름 및 암호 정보를 입력합니다.

단계 **6** 호스트 이름 필드에 데이터베이스의 호스트이름 또는 IP 주소를 입력합니다.

단계 **7** 나머지 설정은 외부 데이터베이스 설정 창에서 완료합니다. 필드 및 해당 설정에 대한 도움이 필요한 경우 온라인 도움말을 참조하십시오.

단계 **8** 저장을 클릭합니다.

단계 **9** 이 절차를 반복하여 각 외부 데이터베이스 인스턴스에 대한 연결을 만듭니다.

외부 파일 서버 설정

파일 서버에서 사용자, 디렉터리, 소유권, 사용 권한 및 기타 작업을 설정하기 전에 외부 파일 서버를 설정합니다.

시작하기 전에

외부 파일 서버에 대한 설계 권장 사항을 검토합니다. 자세한 내용은 외부 파일 서버 요구 사항, 225 페이지를 참조하십시오.

프로시저

단계 **1** 지원되는 Linux 버전을 설치합니다.

단계 **2** 루트에서 다음 명령 중 하나를 입력하여 파일 서버가 SSHv2 및 OpenSSH 4.9 이상을 지원하는지 확인합니다.

```
# telnet localhost 22
Trying ::1...
Connected to localhost.
Escape character is '^]'.
SSH-2.0-OpenSSH_5.3
```

또는

```
# ssh -v localhost
OpenSSH_5.3p1, OpenSSL 1.0.0-fips 29 Mar 2010
debug1: Reading configuration data /root/.ssh/config ...
...debug1: Local version string SSH-2.0-OpenSSH_5.3
...
```

단계 **3** 개인/공개 키 인증을 허용하려면 `/etc/ssh/sshd_config` 파일의 다음 필드가 *yes*로 설정되었는지 확인하십시오.

- RSAAuthentication *yes*
- PubkeyAuthentication *yes*

파일에서 이들이 주석 처리된 경우 설정을 그대로 둘 수 있습니다.

팁 보안을 강화하려면 파일 전송 사용자에 대한 암호 로그인도 비활성할 수 있습니다(이 예에서는 (*mftuser*). 그러면 SSH 공개/개인 키 인증으로만 로그인할 수 있게 됩니다.

단계 **4** 서버에서 실행되는 다른 애플리케이션이 사용하지 못하도록 파일 전송 저장소 전용으로 하나 이상의 별도 파티션을 만드는 것이 좋습니다. 모든 파일 저장소 디렉터리를 이 파티션에 만들어야 합니다.

다음에 수행할 작업

외부 파일 서버에 대한 사용자 만들기, 234 페이지

외부 파일 서버에 대한 사용자 만들기

외부 파일 서버에 대한 사용자를 설정합니다.

시작하기 전에

외부 파일 서버 설정, 233 페이지

프로시저

단계 **1** 파일 서버 루트에서 관리되는 파일 전송 기능을 위한 사용자를 만듭니다. 이 사용자는 파일 저장소 디렉터리 구조(예: *mftuser*)를 소유하고 홈 디렉터리(**-m**)를 강제로 만듭니다.

```
# useradd -mmftuser
# passwdmftuser
```

단계 **2** 관리되는 파일 전송 사용자로 전환합니다.

```
# sumftuser
```

단계 **3** 키 저장소로 사용되는 *~mftuser* 홈 디렉터리 아래에 `.ssh` 디렉터리를 만듭니다.

```
$ mkdir~mftuser/.ssh/
```

단계 **4** 관리형 파일 전송이 활성화된 각 노드의 공개 키 텍스트를 유지하는 데 사용되는 `.ssh` 디렉터리 아래에 `authorized_keys` 파일을 만듭니다.

```
$ touch~mftuser/.ssh/authorized_keys
```

단계 **5** 암호 없는 SSH의 작동을 위한 올바른 권한을 설정합니다.

```
$ chmod 700 ~mftuser (디렉터리)
$ chmod 700 ~/.ssh (디렉터리)
$ chmod 700 ~/.ssh/authorized_keys (파일)
```

참고 일부 Linux 시스템에서는 SSH 구성에 따라 이러한 권한이 달라질 수 있습니다.

다음에 수행할 작업

외부 파일 서버용 디렉터리 설정, 235 페이지

외부 파일 서버용 디렉터리 설정

외부 파일 서버의 최상위 디렉터리 구조를 설정합니다.

원하는 디렉터리 구조를 원하는 디렉터리 이름으로 생성할 수 있습니다. 관리되는 파일 전송이 활성화된 각 노드에 대해 디렉터리를 생성하십시오. 나중에 IM and Presence 서비스에서 관리되는 파일 전송을 활성화할 때 각 디렉터리를 노드에 할당해야 합니다.

중요 관리되는 파일 전송이 활성화된 각 노드에 대해 디렉터리를 생성해야 합니다.

참고 파일 서버 파티션/디렉터리가 파일 저장에 사용되는 IM and Presence 서비스 디렉터리에 마운트됩니다.

시작하기 전에

외부 파일 서버에 대한 사용자 만들기, 234 페이지

프로시저

단계 **1** 루트 사용자로 전환합니다.

```
$ exit
```

단계 **2** 최상위 디렉터리 구조(이 예에서는 `/opt/mftFileStore/`를 사용)를 사용하여 관리되는 파일 전송이 활성화된 모든 IM and Presence 서비스 노드에 대한 디렉터리를 보관합니다.

```
# mkdir -p /opt/mftFileStore/
```

단계 **3** *mftuser*에 `/opt/mftFileStore/` 디렉터리의 유일한 소유권을 부여합니다.

```
# chownmftuser:mftuser /opt/mftFileStore/
```

단계 **4** *mftuser*에 `mftFileStore` 디렉터리에 대한 유일한 사용 권한을 부여합니다.

```
# chmod 700 /opt/mftFileStore/
```

단계 **5** *mftuser*로 전환합니다.

```
# sumftuser
```

단계 **6** 각 관리되는 파일 전송이 활성화된 노드에 대해 `/opt/mftFileStore/` 아래에 하위 디렉터리를 만듭니다. (나중에 관리되는 파일 전송을 활성화할 때 노드에 각 디렉터리를 할당합니다.)

```
$ mkdir /opt/mftFileStore/{node_1,node_2,node_3}
```

참고
- 이러한 디렉터리와 경로는 Cisco Unified CM IM and Presence 관리에서 파일 서버를 프로비저닝할 때 구성하는 외부 파일 서버 디렉터리 필드에서 사용됩니다.
- 이 파일 서버에 여러 IM and Presence 서비스 노드를 작성하는 경우, 이 예에서 3개 노드{*node_1*,*node_2*,*node_3*}에 대해 한 것처럼 각 노드에 대해 대상 디렉터리를 정의해야 합니다.
- 각 노드의 디렉터리 내에서 전송 유형 하위 디렉터리(`im`, `groupchat` 및 `persistent`는 모든 후속 디렉터리와 마찬가지로 IM and Presence 서비스에 의해 자동으로 생성됩니다.

다음에 수행할 작업

외부 파일 서버 공개 키 얻기, 236 페이지

외부 파일 서버 공개 키 얻기

외부 파일 서버 공개 키를 얻습니다.

시작하기 전에

외부 파일 서버용 디렉터리 설정, 235 페이지

프로시저

단계 **1** 파일 서버의 공개 키를 검색하려면 다음을 입력합니다.

```
$ ssh-keyscan -t rsa host
```

여기서 호스트는 파일 서버의 호스트 이름, FQDN 또는 IP 주소입니다.

경고!
- 중간자 공격을 방지하기 위해 파일 서버 공개 키가 위조된 경우 **ssh-keyscan -t rsa***host* 명령에서 반환되는 공개 키 값이 파일 서버의 실제 공개 키인지 확인해야 합니다.
- 파일 서버에서 `ssh_host_rsa_key.pub` 파일(본 시스템에서는 `/etc/ssh/` 아래에 있음)의 위치로 이동하고 공개 키 파일의 내용에서 호스트(호스트는 파일 서버의 `ssh_host_rsa_key.pub` 파일에 없음)를 제외한 내용이 **ssh-keyscan -t rsa***host* 명령에서 반환하는 공개 키 파일과 일치하는지 확인합니다.

단계 **2** `ssh_host_rsa_key.pub` 파일 내용이 아닌 **ssh-keyscan -t rsa***host* 명령의 결과를 복사합니다. 서버 호스트 이름 FQDN 또는 IP 주소부터 끝까지 전체 키 값을 복사해야 합니다.

참고 서버 키는 IP 주소로 시작될 수도 있지만 대부분의 경우 호스트 이름 또는 FQDN으로 시작됩니다.

예를 들면 다음을 복사합니다.

hostname ssh-rsa AAAQEAzRevlQCH1KFAnXwhd5UvEFzJs...

...a7y49d+/Am6+ZxkLc4ux5xXZueL3GSGt4rQUy3rp/sdug+/+N9MQ==

(줄임표 추가됨)

단계 **3** **ssh-keyscan -t rsa***host* 명령의 결과를 텍스트 파일에 저장합니다. 이 파일은 *IM and Presence* 서비스에서 외부 파일 서버 구축 절차 중에 파일 서버를 구성할 때 필요합니다.

단계 **4** 생성한 `authorized_keys` 파일을 열어 둡니다. 나중에 IM and Presence 서비스에서 파일 서버를 프로비저닝할 때 필요합니다.

참고 공개 키를 검색할 수 없는 경우 추가 도움말은 외부 파일 서버 공개 키 및 개인 키 문제 해결, 242 페이지의 내용을 참조하십시오.

다음에 수행할 작업

IM and Presence 서비스에서 외부 파일 서버 프로비저닝, 237 페이지

IM and Presence 서비스에서 외부 파일 서버 프로비저닝

관리되는 파일 전송을 활성화할 클러스터의 각 노드에 대해 외부 파일 서버 인스턴스를 하나씩 구성해야 합니다.

외부 파일 서버 인스턴스는 외부 파일 서버의 물리적 인스턴스일 필요가 없습니다. 그러나 지정된 호스트 이름에서, 각 외부 파일 서버 인스턴스에 대해 고유한 외부 파일 서버 디렉터리를 지정해야 합니다. 동일한 노드에서 모든 외부 파일 서버 인스턴스를 구성할 수 있습니다.

시작하기 전에

외부 파일 서버 공개 키 얻기, 236 페이지

다음 외부 파일 서버 정보를 확인합니다.

- 호스트 이름, FQDN 또는 IP 주소
- 공개 키
- 파일 저장소 디렉터리 경로
- 사용자 이름

프로시저

단계 **1** **Cisco Unified CM IM and Presence** 관리에서 메시징 > 외부 서버 설정 > 외부 파일 서버를 선택합니다.

단계 **2** 새로 추가를 클릭합니다.

외부 파일 서버 창이 나타납니다.

단계 **3** 서버 상세정보를 입력합니다. 필드와 해당 구성 옵션에 대한 도움말은 외부 파일 서버 필드, 238 페이지의 내용을 참조하십시오.

단계 **4** 저장을 클릭합니다.

단계 **5** 관리되는 파일 전송이 활성화된 각 클러스터 노드에 대해 별도의 외부 파일 서버 인스턴스를 만들 때까지 이 절차를 반복합니다.

다음에 수행할 작업

Cisco XCP 파일 전송 관리자 활성화 확인, 239 페이지

외부 파일 서버 필드

필드	설명
이름	파일 서버 이름을 입력합니다. 서버 이름은 보는 즉시 이해할 수 있는 이름으로 지정하는 것이 좋습니다. 최대 문자 수: 128. 허용 값은 영숫자, 대시, 밑줄입니다.
호스트/IP 주소	파일 서버의 호스트 이름 또는 IP 주소를 입력합니다. 참고 • 호스트/IP 주소 필드에 입력하는 값은 외부 파일 서버 공개 키 필드에 입력하는 키의 시작 부분과 일치해야 합니다. • 이 설정을 변경하는 경우 Cisco XCP 라우터 서비스를 다시 시작해야 합니다.

필드	설명
외부 파일 서버 공개 키	파일 서버의 공개 키(텍스트 파일로 저장하도록 안내된 키)를 이 필드에 붙여 넣습니다. 키를 저장하지 않은 경우 파일 서버에서 다음 명령을 실행하여 파일 서버에서 키를 검색할 수 있습니다. `$ ssh-keyscan -t rsa`*host* 여기서 *host*는 파일 서버의 IP 주소, 호스트 이름 또는 FQDN입니다. 호스트 이름, FQDN 또는 IP 주소로 시작하는 전체 키 텍스트를 복사하여 끝에 붙여 넣어야 합니다. 예를 들면 다음을 복사합니다. extFileServer.cisco.com ssh-rsa AAAQEAzRevlQCH1KFAnXwhd5UvEFzJs... ...a7y49d+/Am6+ZxkLc4ux5xXZueL3GSGt4rQUy3rp/sdug+/+N9MQ== (줄임표 추가됨) 중요 이 값은 호스트/IP 주소 필드에 입력한 호스트 이름, FQDN 또는 IP 주소로 시작해야 합니다. 예를 들어 호스트/IP 주소 필드에 extFileServer를 사용한 경우, 이 필드는 extFileServer로 시작하고 뒤에 rsa 키가 와야 합니다.
외부 파일 서버 디렉터리	파일 서버 디렉터리 계층의 상위에 대한 경로. 예를 들어, `/opt/mftFileStore/node_1/`
사용자 이름	외부 파일 서버 관리자의 사용자 이름

Cisco XCP 파일 전송 관리자 활성화 확인

관리되는 파일 전송을 활성화할 각 노드에서 Cisco XCP 파일 전송 관리자 서비스가 활성 상태여야 합니다.

외부 데이터베이스와 외부 파일 서버가 할당된 경우 및 서비스가 데이터베이스에 연결되어 파일 서버를 마운트할 수 있는 경우에만 이 서비스를 시작할 수 있습니다.

시작하기 전에

IM and Presence 서비스에서 외부 파일 서버 프로비저닝, 237 페이지

프로시저

단계 **1** 클러스터의 한 노드에서 **Cisco Unified IM and Presence** 서비스 가용성 사용자 인터페이스에 로그인합니다.

단계 **2** 도구 > 서비스 활성화를 선택합니다.

단계 **3** 서버 드롭다운에서 관리되는 파일 전송이 활성화된 노드를 선택하고 이동을 클릭합니다.

단계 **4** **Cisco XCP** 파일 전송 관리자 서비스의 활성화 상태가 활성화됨으로 표시되는지 확인합니다.

단계 **5** 서비스가 비활성화된 경우 **Cisco XCP** 파일 전송 관리자 확인란을 선택하고 저장을 클릭합니다.

단계 **6** 관리되는 파일 전송이 활성화된 모든 클러스터 노드에 대해 이 절차를 반복합니다.

다음에 수행할 작업

관리되는 파일 전송 활성화, 240 페이지

관리되는 파일 전송 활성화

IM and Presence 서비스에서 관리되는 파일 전송을 활성화합니다.

프로시저

단계 **1** **Cisco Unified CM IM and Presence** 관리에 로그인하고 메시징 > 파일 전송을 선택합니다. 파일 전송 창이 열립니다.

단계 **2** 파일 전송 구성 영역에서 구축 유형에 따라 관리되는 파일 전송 또는 관리되는/피어 투 피어 파일 전송을 선택합니다. 를 참조하십시오. 파일 전송 옵션, 241 페이지

단계 **3** 최대 파일 크기를 입력합니다. 영(0)을 입력하면 최대 크기(4GB)가 적용됩니다.

참고 이 변경 사항을 적용하려면 Cisco XCP 라우터 서비스를 다시 시작해야 합니다.

단계 **4** [관리되는 파일 전송 할당] 영역에서 클러스터의 각 노드에 대해 외부 데이터베이스 및 외부 파일 서버를 할당합니다.

a) 외부 데이터베이스 - 드롭다운 목록에서 외부 데이터베이스의 이름을 선택합니다.

b) 외부 파일 서버 - 드롭다운 목록에서 외부 파일 서버의 이름을 선택합니다.

단계 **5** 저장을 클릭합니다.

저장을 클릭하면 각 할당에 대해 노드 공개 키 링크가 나타납니다.

단계 **6** 관리되는 파일 전송이 활성화된 클러스터의 각 노드에 대해, 노드 전체의 공개 키를 외부 파일 서버의 `authorized_keys`에 복사해야 합니다.

a) 노드의 공개 키를 표시하려면 [관리되는 파일 전송 할당] 영역으로 스크롤하여 노드 공개 키 링크를 클릭합니다. 노드의 IP 주소, 호스트 이름 또는 FQDN을 비롯한 대화 상자의 전체 내용을 복사합니다.

예제:

```
ssh-rsa yc2EAAAABIwAAAQEAp2g+S2XDEzptN11S5h5nwVleKBnfG2pdW6KiLfzu/sFLegioIIqA8jBguNY/...
...5s+tusrtBBuciCkH5gfXwrsFS0O0AlfFvwnfq1xmKmIS9W2rf0Qp+A+G4MVpTxHgaonw== imp@imp_node
```

(줄임표 추가됨)

경고! • 관리되는 파일 전송 기능이 구성되고 파일 전송 유형이 비활성화됨 또는 피어 투 피어로 변경되면, 모든 관리되는 파일 전송 설정이 삭제됩니다.

• 외부 데이터베이스 및 파일 서버에서 노드의 할당이 취소되면 노드의 키가 무효화됩니다.

b) 외부 파일 서버에서 이 서버가 열려 있지 않은 경우에는 *mftuser*의 홈 디렉터리 아래에 만든 `~mftuser/.ssh/authorized_keys` 파일을 열고 (새 줄에) 각 노드의 공용 키를 추가합니다.

참고 `authorized_keys` 파일은 파일 서버에 할당된 IM and Presence 서비스 노드에서 활성화된 각 관리되는 파일 전송에 대한 공개 키를 포함해야 합니다.

c) `authorized_keys` 파일을 저장하고 닫습니다.

단계 **7** (선택 사항) 관리되는 파일 전송 서비스 파라미터를 구성하여 외부 파일 서버 디스크 공간에 대해 RTMT 경보가 생성되는 임계값을 정의합니다.

단계 **8** 관리되는 파일 전송이 활성화된 모든 노드에서 Cisco XCP 라우터 서비스 다시 시작. Cisco XCP 라우터 서비스 다시 시작을 참조하십시오.

다음에 수행할 작업

외부 서버 상태 확인, 242 페이지

파일 전송 옵션

파일 전송 창에서 다음 파일 전송 옵션 중 하나를 구성할 수 있습니다.

파일 전송 옵션	설명
비활성화됨	클러스터에 대해 파일 전송이 비활성화됩니다.
피어-투-피어	일대일 파일 전송이 허용되지만, 서버에 파일이 아카이브 또는 저장되지 않습니다. 그룹 채팅 파일 전송은 지원되지 않습니다.
관리되는 파일 전송	일대일 및 그룹 파일 전송이 허용됩니다. 파일 전송은 데이터베이스에 기록되고 전송된 파일은 서버에 저장됩니다. 클라이언트는 관리되는 파일 전송도 지원해야 합니다. 그렇지 않으면 파일 전송이 허용되지 않습니다.
관리되는/피어-투-피어 파일 전송	일대일 및 그룹 파일 전송이 허용됩니다. 클라이언트가 관리되는 파일 전송을 지원하는 경우에만 파일 전송은 데이터베이스에 기록되고 전송된 파일은 서버에 저장됩니다. 클라이언트가 관리되는 파일 전송을 지원하지 않으면 이 옵션은 피어 투 피어 옵션과 동일합니다.

참고 관리되는 파일 전송이 노드에 구성되어 있고 파일 전송 유형을 비활성화됨 또는 피어 투 피어로 변경하는 경우, 해당 노드에서 외부 데이터베이스 및 외부 파일 서버에 매핑된 설정이 삭제된다는 점에 유의해야 합니다. 데이터베이스 및 파일 서버의 구성은 유지되지만, 노드에 대해 관리되는 파일 전송을 다시 활성화하면 이러한 구성을 다시 할당해야 합니다.

사전 업그레이드 설정에 따라, IM and Presence 서비스 릴리스 10.5(2) 이상으로 업그레이드한 후 비활성화됨 또는 피어 투 피어가 선택됩니다.

외부 서버 상태 확인

외부 데이터베이스 설정 및 외부 파일 서버 설정에 문제가 없는지 확인하십시오.

시작하기 전에

관리되는 파일 전송 활성화, 240 페이지

프로시저

단계 **1** 외부 데이터베이스의 상태를 확인하려면:

a) **Cisco Unified CM IM and Presence** 관리에서 메시징 > 외부 서버 설정 > 외부 데이터베이스를 선택합니다.

b) [외부 데이터베이스 상태] 영역에서 제공된 정보를 선택합니다.

단계 **2** 외부 파일 서버가 할당되었는지 확인해야 하는 IM and Presence 서비스 노드에서 다음을 수행하십시오.

a) **Cisco Unified CM IM and Presence** 관리에서 메시징 > 외부 서버 설정 > 외부 파일 서버를 선택합니다.

b) 외부 파일 서버 상태 영역에 제공된 정보를 확인하여 연결에 문제가 없는지 확인합니다.

외부 파일 서버 공개 키 및 개인 키 문제 해결

서버 개인/공개 키 쌍이 생성되면 일반적으로 `/etc/ssh/ssh_host_rsa_key`에 개인 키가 기록됩니다.

공개 키는 `/etc/ssh/ssh_host_rsa_key.pub`에 기록됩니다.

이러한 파일이 없으면 다음 절차를 완료하십시오.

프로시저

단계 **1** 다음의 명령을 입력합니다.

```
$ ssh-keygen -t rsa -b 2048
```

단계 **2** 파일 서버의 공개 키를 복사합니다.

호스트 이름, FQDN 또는 IP 주소(예: *hostname* ssh-rsa AAAAB3NzaC1yc...)에서 공개 키에 대한 전체 텍스트 문자열을 복사해야 합니다. 대부분의 Linux 구축에서는 키에 서버의 호스트 이름 또는 FQDN이 포함되어 있습니다.

팁 `$ ssh-keygen -t rsa -b 2048` 명령의 출력에 호스트 이름이 없으면 대신 다음 명령의 출력을 사용하십시오. `$ ssh-keyscan`*hostname*

단계 **3** 이 파일 서버를 사용하도록 설정된 각 IM and Presence 서비스 노드의 경우 외부 파일 서버 설정 창의 외부 파일 서버 공개 키 필드에 공개 키를 붙여 넣습니다.

중요 관리되는 파일 전송 기능에는 암호 없는 SSH를 구성해야 합니다. 암호 없는 SSH에 대한 전체 구성 지침은 SSHD man 페이지를 참조하십시오.

참고 게시자 노드에서 가입자 노드로 상태를 확인하는 동안 정보 메시지 "이 외부 파일 서버에 대한 진단 테스트는 여기에서 실행할 수 있습니다." 가 표시됩니다.

로그에 "pingable": "-7"이 표시됩니다. 이는 외부 파일 서버가 구성되지 않은 다른 노드의 상태를 보고 있음을 의미합니다.

게시자 노드에서 외부 파일 서버를 구성하고 게시자 노드 공개 키는 외부 파일 서버의 "Authorized_key" 파일에서 공유됩니다.

관리되는 파일 전송 관리

관리되는 파일 전송을 구성한 후에는 지속적으로 기능을 관리해야 합니다. 예를 들어, 파일 서버 및 데이터베이스 증가를 관리하기 위한 시스템을 마련해야 합니다. 관리되는 파일 전송 관리 개요, 297 페이지.

20 장

다중 디바이스 메시징 구성

다중 디바이스 메시징 개요

MDM(다중 디바이스 메시징)을 사용하면 현재 로그인한 모든 디바이스에서 일대일 인스턴트 메시지(IM) 대화를 추적할 수 있습니다. 데스크톱 클라이언트와 모바일 디바이스를 사용하고 있고 둘 다 MDM이 활성화된 경우 메시지가 두 디바이스로 전송되거나 숨은 참조 처리됩니다. 대화에 참여할 때 읽기 알림도 두 디바이스에서 동기화됩니다.

MDM을 사용하면 디바이스 간에 이동하면서 IM 대화를 유지할 수 있습니다. 예를 들어, 데스크톱 컴퓨터에서 IM 대화를 시작했지만 미팅을 위해 자리를 떠나야 하는 경우 모바일 디바이스에서 IM 대화를 계속할 수 있습니다. MDM을 사용하려면 클라이언트에 로그인해야 합니다. 로그아웃한 클라이언트는 보내거나 받은 IM 또는 알림을 표시하지 않습니다.

MDM은 자동 모드를 지원하므로 모바일 디바이스의 배터리 전원을 절약할 수 있습니다. Jabber 클라이언트는 모바일 클라이언트가 사용되지 않으면 자동으로 자동 모드를 켭니다. 클라이언트가 다시 활성화되면 자동 모드가 꺼집니다.

다중 디바이스 메시징 필수 조건

인스턴트 메시징을 활성화해야 합니다. 자세한 내용은 을 참조하십시오. 그룹 채팅 및 영구 채팅 작업 흐름, 197 페이지

참고 여러 디바이스 메시징을 활성화하려는 경우 각 사용자에게 여러 Jabber 클라이언트가 있을 수 있으므로 사용자 수 대신 클라이언트 수를 기준으로 구축을 측정합니다. 예를 들어, 25,000 사용자가 있고 각 사용자에게 Jabber 클라이언트가 두 개 있는 경우, 구축에 50,000 사용자의 용량이 필요합니다.

다중 디바이스 메시징 구성

다중 디바이스 메시징은 기본적으로 활성화됩니다. 이 절차를 사용하여 기능을 비활성화하거나 비활성화한 후에 다시 활성화할 수 있습니다.

프로시저

단계 **1** **Cisco Unified CM IM and Presence** 관리에서 시스템 > 서비스 파라미터를 선택합니다.

단계 **2** 서버 드롭다운 목록 상자에서 IM and Presence 서비스 게시자 노드를 선택합니다.

단계 **3** 서비스 드롭다운 목록에서 **Cisco XCP** 라우터**(**활성**)**를 선택합니다.

단계 **4** 다중 디바이스 메시징 드롭다운 목록에서 활성화됨(기본값) 또는 비활성됨 중 하나를 선택합니다.

단계 **5** 저장을 클릭합니다.

단계 **6** Cisco XCP 라우터 서비스 다시 시작.

a) Cisco Unified IM and Presence 서비스 가용성에 로그인하고 도구 > 제어 센터 **-** 네트워크 서비스를 선택합니다.

b) 서버 드롭다운 목록 상자에서 IM and Presence 게시자 노드를 선택합니다.

c) **IM and Presence** 서비스 아래에서 **Cisco XCP** 라우터를 선택하고 다시 시작을 클릭합니다.

다중 디바이스 메시징 흐름 사용 사례

이 흐름은 사용자 Alice가 랩톱 및 모바일 디바이스에서 MDM을 활성화한 경우 메시지 및 알림을 처리하는 방법을 설명합니다.

1. Alice는 랩톱에서 Jabber 클라이언트를 열고 모바일 디바이스에서도 Jabber를 사용하고 있습니다.
2. Alice는 Bob으로부터 인스턴트 메시지(IM)를 수신합니다.

   그녀의 노트북은 알림을 수신하고 새 메시지 표시기를 표시합니다. 그녀의 모바일 디바이스는 알림없이 새 메시지를 수신합니다.

참고 IM은 항상 모든 MDM이 활성화된 클라이언트로 전송됩니다. 알림은 활성 Jabber 클라이언트에만 표시되거나 Jabber 클라이언트가 활성화되지 않은 경우 모든 Jabber 클라이언트에 알림이 전송됩니다.

3. Alice는 Bob과 20분 동안 채팅합니다.

   Alice는 모바일 디바이스에서 새 메시지를 수신하고 읽음으로 표시하는 동안 노트북을 정상적으로 사용합니다. 모바일 디바이스로는 알림이 전송되지 않습니다.

4. Alice가 세 번째 사용자인 Colin으로부터 세 개의 채팅 메시지를 수신하면 Alice의 디바이스는 2단계와 마찬가지로 작동합니다.

5. Alice는 응답하지 않고 노트북을 닫습니다. 집으로 가는 버스에서 Alice는 Bob으로부터 다른 메시지를 수신합니다.

   이 경우 노트북과 모바일 디바이스 모두 알림과 함께 새 메시지를 수신합니다.

6. Alice는 모바일 디바이스를 열고 Bob과 Colin이 보낸 새 메시지를 찾습니다. 이러한 메시지는 노트북으로도 전송되었습니다.

7. Alice는 모바일 디바이스에서 메시지를 읽으며 메시지가 랩톱과 모바일 디바이스 모두에서 읽음으로 표시됩니다.

다중 디바이스 메시징 자동 모드 사용 사례

이 흐름은 다중 디바이스 메시징이 모바일 디바이스에서 자동 모드를 활성화하는 데 사용하는 단계를 설명합니다.

1. Alice는 Jabber를 노트북에서 사용하고 모바일 디바이스에서도 사용합니다. 그녀는 Bob으로부터 온 메시지를 읽고 노트북에서 Jabber를 사용하여 응답 메시지를 보냅니다.

2. Alice는 모바일 디바이스에서 다른 애플리케이션을 사용하기 시작합니다. 그녀의 모바일 디바이스의 Jabber는 백그라운드에서 계속 작동합니다.

3. 모바일 디바이스의 Jabber가 백그라운드에서 실행 중이기 때문에 자동 모드가 자동으로 활성화됩니다.

4. Bob이 Alice에게 또 다른 메시지를 전송합니다. 자동 모드에서는 Alice의 Jabber가 모바일 디바이스에 있기 때문에 메시지가 전달되지 않습니다. Alice에게 보낸 Bob의 응답 메시지는 버퍼링됩니다.

5. 메시지 버퍼링은 다음 트리거 이벤트 중 하나가 발생할 때까지 계속됩니다.

   - `<iq>` stanza가 수신됩니다.
   - `<message>` stanza는 Alice가 현재 다른 디바이스에서 작동 중인 다른 활성 클라이언트가 없을 때 수신됩니다.

참고 활성 클라이언트는 이전 5분 동안 사용 가능한 프레즌스 상태 또는 인스턴트 메시지를 보낸 마지막 클라이언트입니다.

   - 버퍼링 제한에 도달합니다.

6. Alice가 모바일 디바이스의 Jabber로 돌아오면 다시 활성화됩니다. 버퍼링된 Bob의 메시지가 전달되고 Alice는 이 메시지를 볼 수 있습니다.

다중 디바이스 메시징 상호 작용 및 제한 사항

다음 표는 다중 디바이스 메시징(MDM) 기능의 상호 작용 및 제한 사항을 요약한 것입니다.

표 *25:* 다중 디바이스 메시징 상호 작용 및 제한 사항

기능	상호 작용 및 제한 사항
Cisco Jabber 클라이언트	MDM은 버전 11.7 이상의 모든 Jabber 클라이언트에서 지원됩니다.
그룹 채팅	모든 장치에서 로그인한 모든 MDM 사용자는 그룹 채팅을 사용할 수 있습니다.
메시지 아카이버	MDM은 메시지 아카이버 기능과 호환됩니다.
관리되는 파일 전송	모든 장치에서 로그인한 모든 MDM 사용자는 파일 전송을 사용할 수 있습니다.
Expressway를 통한 모바일 및 원격 액세스	Cisco Expressway를 통해 IM and Presence 서비스에 연결하는 모바일 및 원격 액세스 클라이언트의 경우 MDM을 사용하려면 최소 Expressway X8.8 이상을 실행해야 합니다.
서버 복구 매니저	다중 디바이스 메시징 기능은 장애 조치가 발생할 경우 IM and Presence 서비스에서 서버 복구를 지연시킵니다. 다중 디바이스 메시징이 구성된 시스템에서 서버 장애 조치가 발생하면 일반적으로 장애 조치 시간은 **Cisco** 서버 복구 매니저 서비스 파라미터로 지정된 시간의 두 배가 됩니다.
타사 클라이언트	MDM은 이 기능을 지원하지 않는 타사 클라이언트와 호환됩니다.

다중 디바이스 메시징용 카운터

MDM(다중 디바이스 메시징)은 Cisco XCP MDM 카운터 그룹의 다음 카운터를 사용합니다.

카운터 이름	설명
MDMSessions	현재 활성화된 MDM 세션 수입니다.
MDMSilentModeSessions	무음 모드에서 현재 세션 수입니다.
MDMQuietModeSessions	자동 모드에서 현재 세션 수입니다.

카운터 이름	설명
MDMBufferFlushes	MDM 버퍼 플러시의 총 수입니다.
MDMBufferFlushesLimitReached	전체 버퍼 크기 제한에 도달한 MDM 버퍼 플러시의 총 수입니다.
MDMBufferFlushPacketCount	마지막 타임 슬라이스에 플러시된 패킷의 수입니다.
MDMBufferAvgQueuedTime	MDM 버퍼가 플러시되기 전의 평균 시간(초)입니다.

디바이스 용량 모니터링

여러 디바이스에서 로그인한 각 사용자가 다중 디바이스 메시징(MDM)을 활성화하면 IM and Presence 서버에 트래픽 로드가 추가됩니다. 활성 로그인한 사용자 수가 특정 제한에 도달하면 리소스 부족(메모리 소비, CPU 사용률) 및 예기치 않은 성능 문제 및 실패가 발생합니다.

디바이스 용량 모니터링 기능을 사용하면 노드에 생성된 세션 수를 모니터링하는 데 도움이 되는 추가 카운터를 구현하여 이러한 문제를 해결할 수 있습니다.

다음 JSM(Jabber Session Manager) 세션이 IM&P 노드에 생성됩니다.

- 구성된 JSM 세션 — 사용자가 노드에 할당될 때 생성됩니다.
- Active JSM 세션
  - 온프레미스 사용자 로그인.
  - 오프프레미스 사용자 로그인.
- Phantom JSM 세션 — HA 페일오버 사용 사례를 처리하는 활성화된 사용자 푸시용.
- Spark Interop JSM 세션 — 하이브리드 사용자용.

JSM 세션을 모니터링하기 위해 다음 카운터가가 도입되었습니다.

- **JsmClientSessionsActive**
- **JsmPhantomSessionsActive**
- **JsmHybridSessionsActive**

또한 JSM 세션 카운터 및 OVA 크기를 기반으로 계산되는 JSM 임계값 제한을 모니터링하기 위해 새 카운터 **JSMSessionsExceedsThreshold**가 도입되었습니다.

이 카운터의 임계값 한도가 10분 동안 기본값 80%를 초과하는 경우 RTMT(실시간 모니터링 도구)에서 "**JSMSessionsExceedsThreshold**" 알림이 발생합니다.

RTMT를 사용하여 알림 값 구성

이 절차를 사용하여 RTMT를 사용하여 **JSMSessionsExceedsThreshold** 알림 값을 구성할 수 있습니다.

프로시저

단계 **1** **RTMT(**실시간 모니터링 도구**)**에 로그인하여 시스템 > 도구 > 알림 센터를 선택합니다.
단계 **2** **IM and Presence**를 클릭하고 **JSMSessionsExceedsThreshold** 알림 이름을 선택합니다.
단계 **3** **JSMSessionsExceedsThreshold**를 마우스 오른쪽 버튼으로 클릭하고 알림/속성 설정을 선택합니다.
단계 **4** 알림을 활성화하려면 알림 활성화 확인란을 선택합니다.
단계 **5** JSM 세션 임계값 초과 수 값에 대한 백분율 제한을 설정합니다. 기본적으로 이 값은 80%입니다.
단계 **6** 저장을 클릭합니다.
단계 **7** 알림의 빈도 및 일정을 설정합니다. 기본적으로 알림은 10분 마다 트리거됩니다.
단계 **8** 다음을 클릭합니다.
단계 **9** 저장을 클릭합니다.

노드당 **JSM** 세션 지원

다음 표에서는 테스트에 따라 노드당 지원될 수 있는 JSM 세션의 총 수를 보여줍니다.

OVA 크기	**JSM** 세션 수는 **OVA** 용량의 **1.5**배입니다**.**
5K OVA	7.5K
15K OVA	22.5K
25K OVA	37.5K

참고 고가용성이 활성화되어 있고 두 노드가 모두 활성-활성 구성인 경우:

1. 노드당 지원할 수 있는 JSM 세션의 총 수는 사용자 정의 알림에는 노드당만 구성할 수 있다는 제한이 있기 때문에 위에서 언급한 용량의 50%가 됩니다.
2. HA 구성을 기반으로 **JSMSessionsExceedsThreshold** 카운터 값을 수정해야 합니다.

제안된 조치**:**

사용자 정의 알림이 발생하면 특정 노드의 RTMT 도구에서 메모리 및 CPU 사용량 카운터를 확인합니다. 메모리 및 CPU 사용량 카운터 값이 임계값 제한을 초과하는 경우 IM&P 노드 사이에 사용자의 부하를 분산시키는 것이 좋습니다. 현재 IM&P에는 자동으로 노드 간에 사용자의 부하를 분산하는 메커니즘이 없습니다.

디바이스 용량 모니터링에 대한 사용자 세션 보고서

이 절차를 사용하여 사용자 세션 보고서를 봅니다. 이 보고서를 사용하면 클러스터, 하위 클러스터 및 노드 수준에서 여러 디바이스에 로그인한 활성 사용자의 세부 정보를 볼 수 있습니다.

프로시저

단계 **1** **Cisco Unified IM and Presence** 보고에 로그인합니다.

단계 **2** 시스템 보고서 > **IM and Presence** 사용자 세션 보고서를 선택합니다.

단계 **3** 보고서 창에서 보고서 생성(막대 차트)] 아이콘을 선택하여 현재 시간에 대한 사용자 세션 보고서를 생성합니다.

단계 **4** 확인을 클릭합니다.

단계 **5** 열 보고서 이름 아래에서 **IM and Presence** 사용자 세션 보고서를 클릭합니다.

참고
- 이 보고서 생성에는 약 2분 이상 걸릴 수 있습니다.
- 이 보고서에는 생성된 보고서의 날짜 및 타임스탬프와 함께, 프레즌스 이중화 그룹, 노드 이름, 하나 이상의 디바이스에서 로그인한 사용자 수, 클러스터의 총 세션 수, 하위 클러스터 및 노드 수준이 표시됩니다.

단계 **6** 보고서 창의 오른쪽에 있는 다운로드(녹색 화살표) 아이콘을 클릭하여 클러스터, 하위 클러스터 및 노드 수준에 대한 사용자 세션 보고서를 CSV 형식으로 다운로드합니다.

단계 **7** 하나 이상의 디바이스에서 로그인한 사용자의 수 열에 나열된 값을 클릭하여 특정 노드에 대한 세부 사용자 기반 보고서를 생성합니다.

단계 **8** 보고서 창의 오른쪽에 있는 다운로드(녹색 화살표) 아이콘을 클릭하여 노드당 세부 사용자 수준 정보를 CSV 형식으로 다운로드합니다.

참고 세션 수 열에 마우스를 올리면 도구 설명 디바이스 유형에 사용자가 로그인한 디바이스 유형이 표시됩니다.

예를 들어, 디바이스 유형은 데스크톱, iPad, iPhone일 수 있습니다.

21 장

엔터프라이즈 그룹 구성

엔터프라이즈 그룹 개요

엔터프라이즈 그룹이 구성되면 Cisco Unified Communications Manager는 데이터베이스를 외부 LDAP 디렉터리와 동기화할 때 사용자 그룹을 포함합니다. Cisco Unified CM 관리에서 사용자 그룹 창에서 동기화된 그룹을 볼 수 있습니다.

관리자는 이 기능을 사용하여 다음을 수행할 수 있습니다.

- 기능의 의견 세트(예: 영업 및 회계 팀)와 유사한 특성을 가진 사용자를 프로비전합니다.
- 특정 그룹의 모든 사용자를 대상으로 한 메시지를 보냅니다.
- 특정 그룹의 모든 구성원에 대해 동일한 액세스 구성

또한 이 기능은 Cisco Jabber 사용자가 공통된 특징을 공유하는 사용자의 연락처 목록을 신속하게 구축하는 데 도움이 됩니다. Cisco Jabber 사용자는 외부 LDAP 디렉터리에서 사용자 그룹을 검색한 다음 연락처 목록에 추가할 수 있습니다. 예를 들어, Jabber 사용자는 외부 LDAP 디렉터리를 검색하고 영업 그룹을 연락처 목록에 추가하여 모든 영업 팀원을 연락처 목록에 추가할 수 있습니다. 그룹이 외부 디렉터리에서 업데이트되면 사용자의 연락처 목록이 자동으로 업데이트됩니다.

엔터프라이즈 그룹은 외부 LDAP 디렉터리처럼 Windows의 Microsoft Active Directory에서 지원됩니다.

참고 관리자가 엔터프라이즈 그룹 기능을 비활성화하면 Cisco Jabber 사용자가 엔터프라이즈 그룹을 검색하거나 연락처 목록에 이미 추가한 그룹을 볼 수 없습니다. 관리자가 기능을 비활성화할 때 사용자가 이미 로그인되어 있으면 사용자가 로그아웃할 때까지 해당 그룹이 표시됩니다. 사용자가 다시 로그인하면 해당 그룹이 표시되지 않습니다.

보안 그룹

보안 그룹은 엔터프라이즈 그룹의 하위 기능입니다. Cisco Jabber 사용자는 보안 그룹을 검색하고 연락처 목록에 추가할 수도 있습니다. 이 기능을 설정하려면 관리자는 사용자 정의 LDAP 필터를 구성하고 구성된 LDAP 디렉터리 동기화에 적용해야 합니다. 보안 그룹은 Microsoft Active Directory에서만 지원됩니다.

허용되는 최대 항목 수

엔터프라이즈 그룹을 구성할 때 그룹을 처리하는 연락처 목록 최대 값을 구성해야 합니다

- 연락처 목록에 허용되는 최대 항목 수는 연락처 목록에 있는 항목 수와 연락처 목록에 이미 추가된 그룹의 항목 수를 합한 개수입니다.
- 연락처 목록의 최대 항목 수 = (연락처 목록의 항목 수) + (그룹의 항목 수)
- 엔터프라이즈 그룹 기능이 활성화되면 연락처 목록의 항목 수가 허용되는 최대 항목 수보다 작은 경우 Cisco Jabber 사용자가 연락처 목록에 그룹을 추가할 수 있습니다. 이 기능이 비활성화되어 있을 때 허용되는 최대 항목 수를 초과하면 기능이 활성화될 때까지 사용자가 제한되지 않습니다. 기능이 활성화된 후에도 사용자가 계속 로그인되어 있으면 오류 메시지가 표시되지 않습니다. 사용자가 로그아웃했다가 다시 로그인하면 초과된 항목을 지우라는 오류 메시지가 표시됩니다.

엔터프라이즈 그룹 필수 조건

이 기능은 아래 조건으로 구성된 LDAP 디렉터리 동기화 일정이 이미 있다고 가정합니다. LDAP 디렉터리 동기화를 구성하는 방법에 대한 자세한 내용은 *Cisco Unified Communications Manager* 시스템 구성 설명서의 "LDAP 디렉터리에서 사용자 가져오기" 장을 참조하십시오.

- Cisco DirSync 서비스를 활성화해야 합니다.
- LDAP 디렉터리 동기화는 사용자와 그룹을 모두 포함해야 합니다.
- **LDAP** 디렉터리 동기화 일정으로 구성된 대로 일반 LDAP 디렉토리 동기화를 예약해야 합니다.

지원되는 **LDAP** 디렉터리

Microsoft Active Directory만 엔터프라이즈 그룹에서 지원됩니다.

LDAP 디렉터리	엔터프라이즈 그룹 지원
Microsoft Active Directory	엔터프라이즈 그룹 및 보안 그룹 모두 지원됩니다.
OpenLDAP	Windows에서는 OpenLDAP가 다음과 같이 지원됩니다. • `GroupOfNames` 개체 클래스만 지원됩니다. • 보안 그룹은 OpenLDAP에서 지원되지 않습니다. • 최소 버전은 2.4.42입니다. • Linux에서는 OpenLDAP가 지원되지 않습니다.
다른 LDAP 디렉터리	지원되지 않음

엔터프라이즈 그룹 구성 작업 흐름

엔터프라이즈 그룹 기능을 구성하려면 다음 작업을 완료하십시오.

프로시저

	명령 또는 동작	목적
단계 **1**	LDAP 디렉터리에서 그룹 동기화 확인, 255 페이지	LDAP 디렉터리 동기화에 사용자와 그룹이 모두 포함되어 있는지 확인하십시오.
단계 **2**	엔터프라이즈 그룹 활성화, 256 페이지	Cisco Jabber는 Microsoft Active Directory에서 엔터프라이즈 그룹을 검색하여 연락처 목록에 추가할 수 있습니다.
단계 **3**	OpenLDAP 구성 파일 업데이트, 256 페이지	(OpenLDAP 전용) Windows의 OpenLDAP 디렉터리에있는 `slapd.conf` 설정 파일을 편집합니다.
단계 **4**	보안 그룹 활성화, 257 페이지	(선택 사항) Cisco Jabber 사용자가 연락처 목록을 검색하여 보안 그룹을 해당 연락처 목록에 추가할 수있게하려면 이 작업 흐름을 완료하십시오.
단계 **5**	사용자 그룹 보기, 259 페이지	(선택 사항) Cisco Unified Communications Manager 데이터베이스와 동기화되는 엔터프라이즈 그룹 및 보안 그룹을 봅니다.

LDAP 디렉터리에서 그룹 동기화 확인

이 절차를 사용하여 LDAP 디렉터리 동기화에 사용자 및 그룹이 포함되어 있는지 확인합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 다음 메뉴를 선택합니다.서버 > **LDAP** > **LDAP** 디렉터리

단계 **2** 찾기를 클릭하고 엔터프라이즈 그룹을 동기화하는 LDAP 디렉터리를 선택합니다.

단계 **3** 동기화 필드에 사용자 및 그룹이 선택되었는지 확인합니다.

단계 **4** LDAP 디렉터리 구성 창의 나머지 필드를 완료합니다. 필드 및 해당 설정에 대한 도움이 필요한 경우 온라인 도움말을 참조하십시오.

단계 **5** 저장을 클릭합니다.

엔터프라이즈 그룹 활성화

LDAP 디렉터리 동기화에 엔터프라이즈 그룹을 포함하도록 시스템을 구성합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 시스템 > 엔터프라이즈 매개 변수를 선택합니다.

단계 **2** 사용자 관리 파라미터 아래에서 **Cisco IM and Presence**에 대한 디렉터리 그룹 작업 파라미터를 활성화됨으로 설정합니다.

단계 **3** 프레즌스 정보를 사용할 수 있는 최대 엔터프라이즈 그룹 크기 파라미터에 대한 값을 입력합니다. 허용되는 범위는 1 ~ 200 사용자이며 기본값은 100 사용자입니다.

단계 **4** 엔터프라이즈 그룹의 동기화 모드 드롭다운 목록에서 정기적으로 수행할 LDAP 동기화(없음, 차등 동기화, 전체 동기화)를 구성합니다.

참고 이러한 필드 구성에 대한 추가 지원은 엔터프라이즈 매개 변수 도움말을 참조하십시오.

단계 **5** 저장을 클릭합니다.

OpenLDAP 구성 파일 업데이트

Windows에서 OpenLDAP를 통해 엔터프라이즈 그룹을 구성하는 경우 OpenLDAP 디렉터리에서 `slapd.conf` 파일을 업데이트해야 합니다.

프로시저

단계 **1** Windows의 OpenLDAP 파일 디렉터리에서 `slapd.conf` 파일을 찾습니다.

단계 **2** 텍스트 편집기에서 파일을 엽니다.

단계 **3** 다음 텍스트를 파일에 추가합니다.

```
moduleload memberof.la
overlay memberof
memberof-group-oc groupOfNames
memberof-member-ad member
memberof-memberof-ad memberof
memberof-refint TRUE
cachesize 160000
```

단계 **4** 파일을 저장하십시오.

단계 **5** OpenLDAP 디렉터리를 다시 시작합니다.

보안 그룹 활성화

Cisco Jabber 사용자가 해당 연락처 목록에 보안 그룹을 추가할 수 있도록하려면 이러한 옵션 작업을 완료하여 보안 그룹을 LDAP 디렉토리 동기화에 포함합니다.

참고 보안 그룹 동기화는 Microsoft Active Directory에서만 지원됩니다.

참고 초기 동기화가 이미 발생한 경우 Cisco 통합 커뮤니케이션 매니저의 기존 LDAP 디렉토리 구성에 새 구성을 추가할 수 없습니다.

프로시저

	명령 또는 동작	목적
단계 **1**	보안 그룹 필터 생성, 257 페이지	디렉토리 그룹 및 보안 그룹을 모두 필터링하는 LDAP 필터를 생성합니다.
단계 **2**	LDAP 디렉토리에서 보안 그룹 동기화, 258 페이지	새 LDAP 필터를 LDAP 디렉토리 동기화에 추가합니다.
단계 **3**	보안 그룹에 대한 Cisco Jabber 구성, 259 페이지	기존 서비스 프로필을 업데이트하여 연결된 Cisco Jabber 사용자에게 보안 그룹을 검색하고 추가하도록 해당 서비스 프로필 액세스 권한을 부여합니다.

보안 그룹 필터 생성

보안 그룹을 필터링하는 LDAP 필터를 생성합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 다음 메뉴를 선택합니다.시스템 > **LDAP** > **LDAP** 필터.

단계 **2** 새로 추가를 클릭합니다.

단계 **3** 고유한 필터 이름을 입력합니다. 예를 들어 `syncSecurityGroups`합입다.

단계 **4** 필터: `(&(objectClass=group)(CN=*))`를 입력합니다.

단계 **5** 저장을 클릭합니다.

LDAP 디렉토리에서 보안 그룹 동기화

LDAP 디렉토리 동기화에 보안 그룹 필터를 추가하고 동기화를 완료합니다.

참고 초기 LDAP 동기화가 이미 발생한 경우 Cisco 통합 커뮤니케이션 매니저의 기존 LDAP 디렉토리 구성에 새 구성을 추가할 수 없습니다.

참고 새 LDAP 디렉토리 동기화를 설정하는 방법에 대한 자세한 내용은 *Cisco* 통합 커뮤니케이션 매니저 시스템 구성 설명서의 "최종 사용자 구성" 부분을 참조하십시오.

시작하기 전에

보안 그룹 필터 생성, 257 페이지

프로시저

단계 **1** Cisco Unified CM 관리에서 시스템 > **LDAP** > **LDAP** 디렉토리를 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 새로 추가를 클릭하여 새 LDAP 디렉토리를 만듭니다.
- 찾기를 클릭하고 보안 그룹을 동기화할 LDAP 디렉토리를 선택합니다.

단계 **3** 그룹에 대한 **LDAP** 사용자 정의 필터 드롭다운 목록에서 사용자가 생성한 보안 그룹 필터를 선택합니다.

단계 **4** 저장을 클릭합니다.

단계 **5** **LDAP** 디렉토리 구성 창의 나머지 필드를 구성합니다. 필드 및 관련 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

단계 **6** 지금 전체 동기화 수행을 클릭하여 즉시 동기화합니다. 그렇지 않으면 다음 예약된 LDAP 동기화가 발생할 때 보안 그룹이 동기화됩니다.

보안 그룹에 대한 **Cisco Jabber** 구성

해당 서비스 프로필에 연결된 Cisco Jabber 사용자가 LDAP 디렉토리의 보안 그룹을 해당 연락처 목록에 추가할 수 있도록 기존 서비스 프로필을 업데이트합니다.

참고 새 서비스 프로필을 설정하고 Cisco Jabber 사용자에게 할당하는 방법에 대한 자세한 내용은 *Cisco* 통합 커뮤니케이션 매니저 시스템 구성 설명서의 "서비스 프로필 구성" 장을 참조하십시오.

시작하기 전에

LDAP 디렉토리에서 보안 그룹 동기화, 258 페이지

프로시저

단계 **1** 서비스 프로필 구성 창의 나머지 필드를 완료합니다. 필드 및 해당 설정에 대한 도움이 필요한 경우 온라인 도움말을 참조하십시오.

단계 **2** 찾기를 클릭하고 Jabber 사용자가 사용하는 서비스 프로필을 선택합니다.

단계 **3** 디렉토리 프로필 아래에서 **Jabber**에서 보안 그룹 검색 및 추가 허용 확인란을 선택합니다.

단계 **4** 저장을 클릭합니다.
이 서비스 프로필에 연결된 Cisco Jabber 사용자는 이제 보안 그룹을 검색하고 추가할 수 있습니다.

단계 **5** Cisco Jabber 사용자가 사용하는 모든 서비스 프로필에 대해 이 절차를 반복합니다.

사용자 그룹 보기

다음 단계에 따라 Cisco 통합 커뮤니케이션 매니저 데이터베이스와 동기화되는 엔터프라이즈 그룹 및 보안 그룹을 확인할 수 있습니다.

프로시저

단계 **1** [Cisco Unified CM 관리]에서 사용자 관리 > 사용자 설정 > 사용자 그룹을 선택합니다.
사용자 그룹 찾기 및 나열 창이 표시됩니다.

단계 **2** 검색 기준을 입력하고 찾기를 클릭합니다.
검색 기준과 일치하는 사용자 그룹 목록이 표시됩니다.

단계 **3** 사용자 그룹에 속하는 사용자의 목록을 보려면 해당 사용자 그룹을 클릭합니다.
사용자 그룹 구성 창이 나타납니다.

단계 **4** 검색 기준을 입력하고 찾기를 클릭합니다.
검색 기준과 일치하는 사용자 목록이 표시됩니다.

목록에서 사용자를 클릭하면 최종 사용자 구성 창이 표시됩니다.

다음에 수행할 작업

(선택 사항) 보안 그룹 활성화, 257 페이지

엔터프라이즈 그룹 구축 모델 (Active Directory)

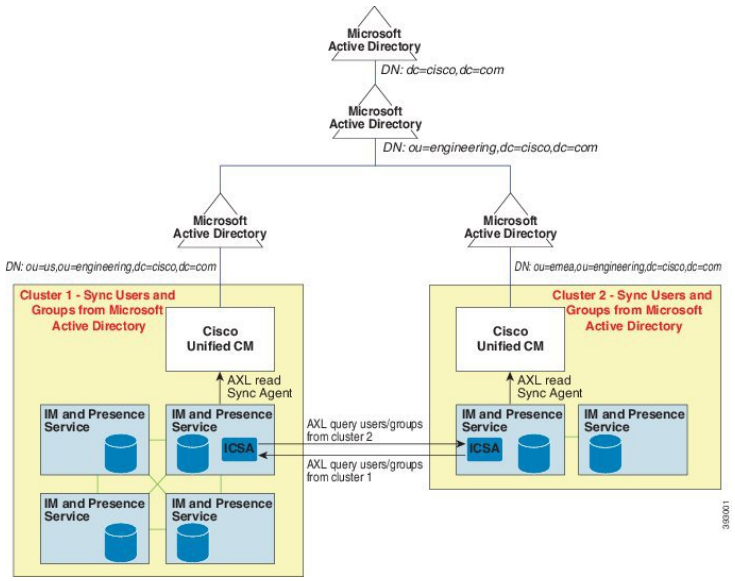
엔터프라이즈 그룹 기능은 Active Directory에 대해 두 가지 구축 옵션을 제공합니다.

중요 Cisco 클러스터 간 동기화 에이전트 서비스를 통해 데이터를 동기화하기 전에 클러스터 1과 클러스터 2에 고유한 UserGroup, UserGroupMember 및 UserGroupWatcherList 레코드 집합이 있는지 확인하십시오. 두 클러스터에 모두 고유한 레코드 세트가 있는 경우, 두 클러스터 모두 동기화 후 모든 레코드의 수퍼 세트를 갖게 됩니다.

엔터프라이즈 그룹 구축 모델 1

이 구축 모델에서 클러스터 1과 클러스터 2는 Microsoft Active Directory의 사용자 및 그룹의 서로 다른 하위 집합을 동기화합니다. Cisco 클러스터 간 동기화 에이전트 서비스는 클러스터 2의 데이터를 클러스터 1로 복제하여 사용자 및 그룹의 전체 데이터베이스를 구축합니다.

그림 *8:* 엔터프라이즈 그룹 구축 모델 *1*



엔터프라이즈 그룹 구축 모델 **2**

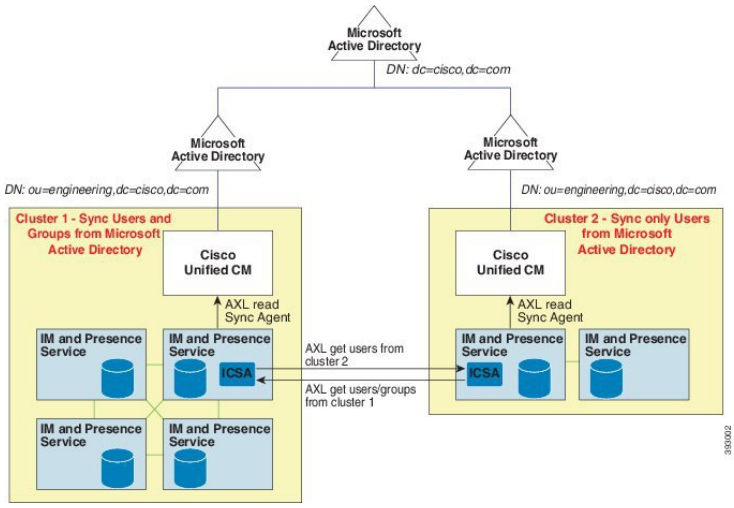
이 구축 모델에서 클러스터 1은 Microsoft Active Directory의 모든 사용자 및 그룹을 동기화합니다. 클러스터 2는 Microsoft Active Directory의 사용자만 동기화합니다. Cisco 클러스터 간 동기화 에이전트 서비스는 클러스터 1의 그룹 정보를 클러스터 2로 복제합니다.

주의 이 구축 모델을 사용하는 경우 하나의 클러스터에서만 그룹 데이터를 동기화하십시오. 엔터프라이즈 그룹 기능은 실패하는 경우 예상대로 작동하지 않습니다.

Cisco Unified CM IM and Presence 관리 > 프레즌스 > 클러스터링 간 창에서 설정을 확인할 수 있습니다.

클러스터 간 피어 테이블에서 엔터프라이즈 그룹 **LDAP** 설정 파라미터의 상태를 확인합니다. 충돌 없음은 피어 간에 잘못된 구성이 없음을 의미합니다. 충돌이 발견되면 Enterprise GroupConflicts 링크를 클릭하고 나타나는 세부 정보 버튼을 클릭합니다. 세부 보고서에 대한 보고 창이 열립니다.

그림 ***9:*** 엔터프라이즈 그룹 구축 모델 ***2***



엔터프라이즈 그룹 제한 사항

표 ***26:*** 엔터프라이즈 그룹 제한 사항

제한 사항	설명
모든 사용자 차단	Cisco Jabber 사용자가 Cisco Jabber 정책 설정에서 "모든 사용자 차단" 기능을 활성화하면 차단은 차단 사용자의 연락처 목록에 연락처로 나열되지 않은 한 다른 Jabber 사용자가 IM and Presence를 차단 사용자와 함께 보거나 교환할 수 없습니다. 예를 들어 Cisco Jabber 사용자(Andy)는 개인 Jabber 설정 내에서 모든 사용자 차단을 활성화했습니다. 다음 목록은 Andy의 차단이 Andy의 개인 연락처 목록에 포함되거나 포함되지 않을 수있는 다른 Jabber 사용자에게 미치는 영향을 보여줍니다. 차단 외에도 Andy는 다음과 같은 개인 연락처 목록을 가지고 있습니다. • Bob 포함 - Bob은 Andy의 개인 연락처 목록에 있기 때문에 차단에도 불구하고 그는 여전히 IM을 보내고 Andy의 프레즌스를 볼 수 있습니다. • Carol 생략 - Carol은 Andy의 프레즌스를 볼 수 없거나 차단으로 인해 IM을 보낼 수 없습니다. • 개인 연락처로 Deborah를 생략합니다. 그러나 Deborah의 멤버인 Andy 연락처로 나열가 엔터프라이즈 그룹 — Deborah Andy의 프레 즌 스 보거나 Andy Im을 보내기 차단 됩니다. Deborah는 Andy의 연락처 목록에 있는 엔터프라이즈 그룹의 구성원 임에도 불구하고 Andy의 프레즌스를 보거나 IM을 Andy에게 보내는 것이 차단됩니다. 엔터프라이즈 그룹 연락처 동작에 대한 자세한 내용은 CSCvg48001을 참조하십시오.
10.x 클러스터의 인터클러스터 피어링	엔터프라이즈 그룹은 릴리스 11.0(1) 이상에서 지원됩니다. 동기화된 그룹에 10.x 인터클러스터 피어의 그룹 구성원이 포함되어 있는 경우 상위 클러스터의 사용자가 10.x 클러스터에서 동기화된 구성원을 볼 수 없습니다. 이는 엔터프라이즈 그룹 동기화를 위해 11.0(1)에서 도입된 데이터베이스 업데이트로 인한 것입니다. 이 업데이트는 10.x 릴리즈의 일부가 아닙니다. 상위 클러스터에 있는 사용자가 10.x 클러스터에 있는 그룹 구성원의 프레즌스를 확인할 수 있도록하려면 상위 클러스터의 사용자가 10.x 사용자를 수동으로 자신의 연락처 목록에 추가해야 합니다. 수동으로 추가된 사용자에게는 프레즌스 문제가 없습니다.
멀티 레벨 그룹화	멀티 레벨 그룹화는 그룹 동기화에 허용되지 않습니다.

제한 사항	설명
그룹만 동기화	사용자 그룹과 사용자가 동일한 검색 기반에 있으면 그룹 전용 동기화가 허용되지 않습니다. 대신 사용자 그룹과 사용자는 동기화됩니다.
최대 사용자 그룹 수	Microsoft Active Directory 서버의 최대 15000개의 사용자 그룹을 Unified Communications Manager 데이터베이스와 동기화할 수 있습니다. 각 사용자 그룹에 1 ~ 200명의 사용자를 포함할 수 있습니다.**Cisco Unified CM IM and Presence** 관리 > 시스템 > 서비스 파라미터 창에서 정확한 수를 설정할 수 있습니다. 데이터베이스에서 최대 사용자 계정 수는 160,000을 초과할 수 없습니다.
사용자 그룹 마이그레이션	사용자 그룹을 한 조직 단위에서 다른 조직 단위로 이동하는 경우 원래 단위에서 전체 동기화를 수행한 후에 새 단위에서 전체 동기화를 수행해야 합니다.
로컬 그룹	로컬 그룹은 지원되지 않습니다. Microsoft Active Directory에서 동기화된 그룹만 지원됩니다.
IM and Presence 서비스 노드에 할당되지 않은 그룹 구성원	IM and Presence 서비스 노드에 할당되지 않은 그룹 구성원은 연락처 목록에 프레즌스 풍선이 회색으로 표시됩니다. 그러나 연락처 목록에 허용된 최대 사용자 수를 계산할 때 이 구성원이 고려됩니다.
Microsoft Office Communication Server에서 마이그레이션	Microsoft Office Communication Server에서 마이그레이션하는 동안 사용자가 IM and Presence 서비스 노드로 완전히 마이그레이션되어야 엔터프라이즈 그룹 기능이 지원됩니다.
LDAP 동기화	동기화가 진행되는 동안 **LDAP** 디렉터리 구성 창에서 동기화 옵션을 변경하면 기존 동기화는 영향을 받지 않습니다. 예를 들어 동기화가 진행 중일 때 동기화 옵션을 사용자 및 그룹에서 사용자로만으로 변경하면 사용자와 그룹 동기화가 계속됩니다.
Edge를 통한 그룹 검색 기능	이 릴리스에서는 Edge를 통한 그룹 검색 기능이 제공되지만 완전히 테스트되지 않았습니다. 따라서 Edge를 통한 그룹 검색을 완벽하게 지원할 수는 없습니다. 향후 릴리스에서는 완벽한 지원이 제공될 것으로 예상됩니다.
Cisco 클러스터 간 동기화 에이전트 서비스 주기적 동기화	그룹 이름이나 그룹 구성원 이름이 외부 LDAP 디렉터리에서 업데이트되면 주기적 Cisco Intercluster 동기화 에이전트 서비스 동기화 후에만 Cisco Jabber 연락처 목록에서 업데이트됩니다. 일반적으로 Cisco 클러스터 간 동기화 에이전트 서비스 동기화는 30분마다 발생합니다.

제한 사항	설명
LDAP 구성에서 다른 동기화 계약을 통해 사용자와 사용자 그룹 동기화	사용자 및 사용자 그룹이 동일한 동기화 계약의 일부로 Cisco Unified Communications Manager 데이터베이스에 동기화된 경우 동기화 후 Cisco Unified Communications Manager 데이터베이스에서 사용자 및 그룹 연결이 예정대로 업데이트됩니다. 그러나 사용자 및 사용자 그룹이 다른 동기화 계약의 일부로 동기화된 경우 첫 번째 동기화 후 사용자와 그룹이 데이터베이스에 연결되지 않을 수 있습니다. 데이터베이스의 사용자 및 그룹 연결은 동기화 계약이 처리되는 순서에 따라 다릅니다. 사용자가 그룹보다 먼저 동기화되는 경우 그룹이 연결을 위해 데이터베이스에서 사용 가능하지 않을 수 있습니다. 이 경우 그룹과의 동기화 계약이 사용자와의 동기화 계약 이전에 예약되도록 해야 합니다. 그렇지 않으면 그룹이 데이터베이스와 동기화된 후 사용자는 사용자 및 그룹으로 설정된 동기화 유형을 통해 다음 수동 또는 정기 동기화 후에 그룹과 연결됩니다. 계약 동기화 유형이 사용자 및 그룹으로 설정된 경우에만 사용자 및 해당 그룹 정보가 매핑됩니다. .
엔터프라이즈 그룹에 대한 테스트된 OVA 정보	테스트된 시나리오 두 클러스터인 클러스터 A와 클러스터 B를 포함한 interCluster 구축에서: 클러스터 A는 Active Directory에서 동기화된 160K의 사용자 중 IM and Presence 서비스에 대해 15K OVA와 15K 사용자가 활성화됩니다. 15K OVA 클러스터의 사용자당 테스트 및 지원되는 평균 기업 그룹 수는 13개의 엔터프라이즈 그룹입니다. 클러스터 B는 Active Directory에서 동기화된 160K의 사용자 중 IM and Presence 서비스에 대해 25K OVA와 25K 사용자가 활성화됩니다. 25K OVA 클러스터의 사용자당 테스트 및 지원되는 평균 기업 그룹 수는 8개의 엔터프라이즈 그룹입니다. 사용자 등록 명부에 있는 사용자의 개인 연락처와 사용자 등록 명부에 있는 기업 그룹의 연락처의 테스트되고 지원되는 합계는 200보다 작거나 같습니다. 참고 클러스터가 2개 이상인 환경에서는 이러한 번호가 지원되지 않습니다.
연락처 목록 내보내기	벌크 관리 > 연락처 목록 > 연락처 목록 내보내기를 사용하여 사용자의 연락처 목록을 내보낼 경우 연락처 목록 CSV 파일에는 Jabber 클라이언트에 있던 엔터프라이즈 그룹의 세부 정보는 포함되지 않습니다.

22 장

브랜딩 사용자 지정

브랜드 개요

브랜딩 기능을 사용하면 IM and Presence 서비스에 대해 사용자 지정 브랜딩을 적용할 수 있습니다. 브랜딩 사용자 지정은 Cisco Unified CM IM and Presence 관리 로그인 및 구성 창에 표시됩니다. 추가하거나 수정할 수 있는 항목에는 다음이 포함됩니다.

- 회사 로고
- 배경색
- 테두리 색상
- 글꼴 색

브랜드 필수 조건

지정된 폴더 구조 및 파일로 브랜딩 zip 파일을 만들어야 합니다. 자세한 내용은 브랜딩 파일 요구 사항, 267 페이지를 참조하십시오.

브랜딩 활성화

이 절차를 사용하여 IM and Presence 서비스 클러스터에 대해 브랜딩 사용자 지정을 활성화합니다. SAML SSO를 활성화한 경우에도 브랜딩 업데이트가 표시됩니다.

참고 브랜딩을 활성화하려면 권한 수준 4 액세스 권한이 있는 기본 관리자 계정을 사용해야 합니다. 이는 설치 중에 생성되는 기본 관리자 계정입니다.

참고 브랜드를 활성화하거나 비활성화하려면 GUI와 CLI 중 하나만 사용해야 합니다. 예를 들어, GUI 인터페이스를 사용하여 브랜딩을 활성화하는 경우 GUI 인터페이스 자체를 사용하여 브랜딩을 비활성화해야 합니다. 그렇지 않으면 제대로 작동하지 않습니다.

시작하기 전에

IM and Presence 서비스가 액세스 할 수 있는 위치에 IM and Presence 사용자 지정이 포함된 `branding.zip` 파일을 저장합니다.

프로시저

단계 **1** Cisco Unified IM and Presence OS 관리에 로그인합니다.

단계 **2** 소프트웨어 업그레이드 > 브랜딩을 선택합니다.

단계 **3** 원격 서버로 이동하고 `branding.zip` 파일을 선택합니다.

단계 **4** 파일 업로드를 클릭합니다.

단계 **5** 브랜딩 활성화를 클릭합니다.

참고 **utils branding enable** CLI 명령을 실행하여 브랜딩을 활성화할 수도 있습니다.

단계 **6** 브라우저를 새로 고침하여 변경 내용을 확인합니다.

단계 **7** 모든 IM and Presence 서비스 클러스터 노드에서 이 절차를 반복합니다.

브랜딩 비활성화

이 절차를 사용하여 IM and Presence 서비스 클러스터에서 브랜딩을 비활성화합니다.

참고 브랜딩을 비활성화하려면 권한 수준 4 액세스 권한이 있는 마스터 관리자 계정을 사용해야 합니다. 이는 설치 중에 생성되는 기본 관리자 계정입니다.

참고 브랜드를 활성화하거나 비활성화하려면 GUI와 CLI 중 하나만 사용해야 합니다. 예를 들어, GUI 인터페이스를 사용하여 브랜딩을 활성화하는 경우 GUI 인터페이스 자체를 사용하여 브랜딩을 비활성화해야 합니다. 그렇지 않으면 제대로 작동하지 않습니다.

프로시저

단계 **1** Cisco Unified IM and Presence OS 관리에 로그인합니다.

단계 **2** 소프트웨어 업그레이드 > 브랜딩을 선택합니다.

단계 **3** 브랜딩 비활성화를 클릭합니다.

참고 **utils branding disable** CLI 명령을 실행하여 브랜딩을 비활성화할 수도 있습니다.

단계 **4** 브라우저를 새로 고침하여 변경 내용을 확인합니다.

단계 **5** 모든 IM and Presence 서비스 클러스터 노드에서 이 절차를 반복합니다.

브랜딩 파일 요구 사항

사용자 지정 브랜딩을 시스템에 적용하기 전에 사양에 따라 `branding.zip` 파일을 만듭니다. 원격 서버에서 브랜딩 폴더를 만들고 지정된 내용으로 폴더를 채웁니다. 모든 이미지 파일과 하위 폴더를 추가했으면 전체 폴더를 압축하여 파일을 `branding.zip`으로 저장합니다.

헤더에 대해 단일 이미지를 사용할지 아니면 여섯 개의 이미지 조합을 사용하여 헤더에 대해 단계별 효과를 만들지 여부에 따라 폴더 구조에는 두 가지 옵션이 있습니다.

표 ***27:*** 폴더 구조 옵션

브랜딩 옵션	폴더 구조

단일 헤더 옵션	헤더 배경(설명선 항목 3)에 대해 단일 이미지를 원하는 경우 브랜딩 폴더에 다음 하위 폴더 및 이미지 파일이 있어야합니다.
	
	`Branding (folder)`
	`  cup (folder)`
	`  BrandingProperties.properties (properties file)`
	`  brandingHeader.gif (652*1 pixel)`
	`  ciscoLogo12pxMargin.gif (44*44 pixel)`

브랜딩 옵션	폴더 구조
단계별 헤더 옵션	헤더 배경(설명선 항목 3, 4, 5)의 단계별 이미지를 만들려면 단계별 효과를 만들기 위해 6 개의 별도 이미지 파일이 필요합니다. 브랜딩 폴더에는 이러한 하위 폴더 및 파일이 있어야합니다. Branding(folder) cup (folder) BrandingProperties.properties (file) brandingHeaderBegLTR.gif (652*1 pixel image) brandingHeaderBegRTR.gif (652*1 pixel image) brandingHeaderEndLTR.gif (652*1 pixel image) brandingHeaderEndRTR.gif (652*1 pixel image) brandingHeaderMidLTR.gif (652*1 pixel image) brandingHeaderMidRTR.gif (652*1 pixel image) ciscoLogo12pxMargin.gif (44*44 pixel image)

사용자 인터페이스 브랜딩 옵션

다음 이미지는 Cisco Unified CM IM and Presence 관리 사용자 인터페이스의 브랜딩 옵션을 표시합니다.

그림 ***10:*** 관리 로그인 화면의 브랜딩 옵션

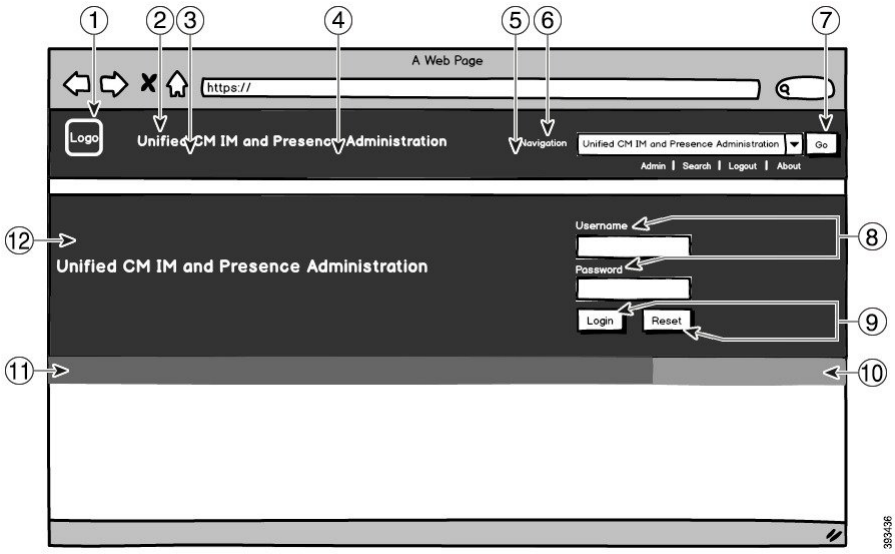
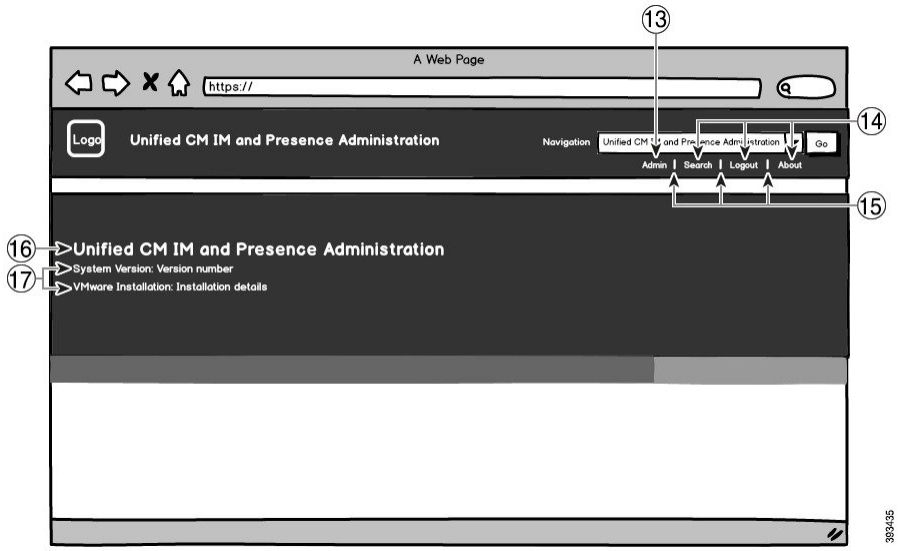


그림 ***11:*** 관리 로그인 화면의 브랜딩 옵션



다음 표에서는 위의 화면 캡처에서 설명선 항목을 사용자 지정할 수 있는 방법을 설명합니다.

표 ***28:*** 사용자 인터페이스 브랜딩 옵션

항목	설명	브랜딩 편집
로그인 화면 이미지		
1	회사 로고	IM and Presence 서비스 인터페이스에 로고를 추가하려면 회사 로고를 다음 파일 이름의 44x44 픽셀 이미지로 저장합니다. `ciscoLogo12pxMargin.gif` (44*44 픽셀)
2	헤더의 Unified CM IM and Presence 관리 텍스트	header.heading.color
3	머리글 배경(단계별 옵션 - 왼쪽)	헤더 이미지에 단계별 효과를 적용하려면 왼쪽에 다음 이미지를 사용합니다. • `brandingHeaderBegLTR.gif` (652 x 1 픽셀) • `brandingHeaderBegLTR.gif` (652 x 1 픽셀)

항목	설명	브랜딩 편집
4	헤더 배경	헤더에 단일 이미지를 사용하려면: • `brandingHeader.gif` (652 x 1 픽셀) 그렇지 않고 단계별 효과가 적용된 헤더를 만들려면 다음 이미지를 사용합니다. • `brandingHeaderMidLTR.gif` (652 x 1 픽셀) • `brandingHeaderMidRTR.gif` (652 x 1 픽셀)
5	머리글 배경(단계별 옵션 - 오른쪽)	헤더에 단계별 효과를 사용하려면 오른쪽 헤더에 다음 이미지를 사용합니다. • `brandingHeaderEndLTR` (652 x 1 픽셀) • `brandingHeaderEndRTR` (652 x 1 픽셀)
6	탐색 텍스트	header.navigation.color
7	이동 버튼	header.go.font.color header.go.background.color
8	사용자 이름 및 암호 텍스트	splash.loginfield.color
9	로그인 및 재설정 버튼	splash.button.text.color splash.button.color
10	아래 배경색 – 오른쪽	splash.hex.code.3
11	아래 배경색 – 왼쪽	splash.hex.code.2
12	배너	splash.hex.code.1
로그인 이미지 게시		
13	로그인한 사용자 텍스트(예: '관리' 사용자)	header.text.bold.color
14	검색, 정보, 로그아웃 링크	header.link.color
15	링크 구분선	header.divider.color

항목	설명	브랜딩 편집
16	배너의 Unified CM IM and Presence 관리 텍스트(로그인 후)	splash.login.text.color
17	시스템 버전 및 VMware 설치 텍스트	splash.version.color

브랜딩 속성 편집 예

브랜딩 속성은 속성 파일에 16진 코드를 추가하여 편집할 수 있습니다 (`BrandingProperties.properties`). 특성 파일은 HTML 기반 16진 코드를 사용합니다. 예를 들어 탐색 텍스트 항목(설명선 항목 6번)의 색상을 빨간색으로 변경하려면 속성 파일에 다음 코드를 추가합니다.

```
header.navigation.color="#FF0000"
```

이 코드에서 `header.navigation.color`는 편집하려는 브랜딩 속성이고 `"#FF0000"`은 새 설정(빨간색)입니다.

23 장

고급 기능 구성

스트림 관리

IM and Presence 서비스는 인스턴트 메시징을 위한 스트림 관리를 지원합니다. 스트림 관리는 stanza 확인 및 스트림 재개 기능을 포함하여 두 XMPP 엔티티 사이의 XML 스트림을 능동적으로 관리하기 위한 XMPP(Extensible Messaging and Presence Protocol) 확장을 정의하는 XEP-0198 사양을 사용하여 구현됩니다. XEP-0198에 대한 자세한 내용은 다음의 사양을 참조하십시오. http://xmpp.org/extensions/xep-0198.html

IM and Presence 서비스와 Cisco Jabber 간의 통신이 일시적으로 끊어지면 스트림 관리를 통해 통신 중단 중에 전송되는 인스턴트 메시지가 손 되지 않도록 합니다. 구성 가능한 시간 제한 기간에 따라 메시지가 처리되는 방법이 결정됩니다.

- Cisco Jabber가 시간 초과 기간 내에 IM and Presence 서비스와의 통신을 재설정하는 경우 메시지가 재전송됩니다.
- Cisco Jabber가 시간 초과 기간 내에 IM and Presence 서비스와의 통신을 재설정하지 않으면 메시지가 송신자에게 반환됩니다.
- 시간 초과 기간 경과된 이후에 전송되는 메시지는 오프라인으로 저장되고 Cisco Jabber가 IM and Presence 서비스와의 통신을 재개할 때 전달됩니다.

스트림 관리는 기본적으로 클러스터 수준에서 활성화됩니다. 그러나 스트림 관리 서비스 파라미터를 사용하여 기능을 구성할 수 있습니다.

스트림 관리 구성

이 절차를 사용하여 IM and Presence 서비스에서 스트림 관리(XEP-0198)를 구성합니다.

프로시저

단계 **1** Cisco Unified CM IM and Presence 관리에서 시스템 > 서비스 파라미터를 선택합니다.

단계 **2** 서버 드롭다운 목록에서 IM and Presence 노드를 선택합니다.

단계 **3** 서비스 드롭다운에서 **Cisco XCP** 라우터를 선택합니다.

단계 **4** 스트림 관리 활성화 서비스 파라미터를 활성화됨으로 설정합니다.

단계 **5** 스트림 관리 파라미터**(**클러스터 수준**)** 아래에서 스트림 관리 파라미터를 구성합니다.

표 ***29:*** 스트림 관리 서비스 파라미터

서비스 파라미터	설명
스트림 관리 활성화	스트림 관리 클러스터 수준을 활성화 또는 비활성화합니다. 기본 설정은 활성화입니다.
스트림 관리 시간 초과	시간 초과는 (연결이 끊긴) 세션이 포기하기 전에 다시 시작할 수 있는 시간(초)을 제어합니다. 클라이언트가 더 긴 시간 초과를 협상하려고 하는 경우(또는 원하는 시간 초과를 지정하지 않은 경우) 이 최대값이 적용됩니다. 이 시간 초과가 끝난 후, IM and Presence 서비스를 사용하여 Cisco Jabber에 다시 로그인하기 전에 전송되는 모든 메시지는 오프라인으로 저장되고 다시 로그인한 후 재전송됩니다. 범위는 30초~90초입니다. 기본값은 60초입니다.
스트림 관리 버퍼	스트림 관리를 사용하는 세션에 대해 버퍼에 유지될 최대 패킷(패킷 기록) 수를 정의합니다. 클라이언트에 버퍼에서 사용할 수 있는 것 보다 많은 기록이 필요한 경우에는 스트림 재시작에 실패합니다. 범위는 5~150개의 패킷이며, 기본값은 100 패킷입니다 .
승인 요청 비율	클라이언트가 마지막으로 수신한 stanza 수를 제공하도록 요청하기 전에 서버가 보내는 stanzas 수를 정의합니다. 숫자가 작을수록 네트워크 트래픽이 더 많이 사용되지만 서버에서 stanza 기록 버퍼를 정리하고 사용 하는 메모리를 줄일 수 있습니다. 범위는 1~64 stanzas이며, 기본값은 5입니다. 참고 승인 요청 속도가 작을수록 네트워크 트래픽이 증가되지만, 메모리 사용량은 감소합니다.

단계 **6** 저장을 클릭합니다.

Microsoft Outlook과 일정 통합

이 기능을 사용하면 Microsoft Outlook의 일정 및 모임 상태를 IM and Presence 서비스 서버의 현재 상태에 통합할 수 있습니다. 사용자가 미팅 중인 경우 해당 상태는 사용자의 프레즌스 상태의 일부로 표시됩니다. 이 기능은 IM and Presence 서비스를 온프레미스 Microsoft Exchange Server 또는 호스팅된 Office 365 Server에 연결하여 구성할 수 있습니다.

Microsoft Outlook과 일정 통합을 구성하는 방법에 대한 자세한 내용은 http://www.cisco.com/c/en/us/support/unified-communications/unified-presence/products-installation-and-configuration-guides-list.html에서 *M and Presence* 서비스를 위한 *Microsoft Outlook* 일정 통합을 참조하십시오.

연합

IM and Presence 서비스에서 IM and Presence 서비스가 관리하는 도메인 내에서 페더레이션된 네트워크를 만들 수 있습니다. 페더레이션 구축에는 두 가지 주요 유형이 있습니다.

- 도메인 간 페더레이션 - 이 통합을 통해 IM and Presence 서비스에서 관리하는 도메인 내 사용자가 외부 도메인의 사용자와 가용성 정보 및 인스턴트 메시징(IM)을 교환할 수 있습니다. 외부 도메인은 Microsoft, Google, IBM 또는 AOL 서버에서 관리할 수 있습니다. IM and Presence 서비스는 외부 도메인에 있는 서버와 통신하는 다양한 프로토콜을 사용할 수 있습니다.
- 분할된 도메인 간 페더레이션 - 이 통합을 통해 IM and Presence 서비스와 Microsoft 서버(예: Microsoft Lync)는 공통 도메인 또는 도메인 집합을 호스팅합니다. 이 통합을 통해 IM and Presence 서비스 클라이언트 사용자와 단일 엔터프라이즈 내의 Microsoft Lync 사용자는 인스턴트 메시징 및 가용성을 교환할 수 있습니다.
- SIP 오픈 페더레이션 - Cisco IM and Presence 서비스는 Cisco Jabber 클라이언트용 SIP 오픈 페더레이션을 지원합니다. 관리자는 Cisco Jabber 사용자가 사용 가능한 모든 도메인의 사용자와 원활하게 페더레이션할 수 있도록 SIP 오픈 페더레이션을 구성할 수 있습니다. 단일 고정 경로를 사용하는 모든 도메인에 대해 오픈 페더레이션을 구성할 수 있습니다. 정적 경로를 통해 Cisco Jabber가 외부 도메인과 페더레이션할 수 있습니다. 더 중요한 것은 개별 도메인에 대한 SIP 페더레이션을 구성하고 유지 관리하는 시간을 크게 줄여줍니다.

구성 정보는 http://www.cisco.com/c/en/us/support/unified-communications/unified-presence/products-installation-and-configuration-guides-list.html에서 *Cisco Unified Communications Manager*의 *IM and Presence* 서비스용 도메인 간 페더레이션 또는 *Cisco Unified Communications Manager*의 *IM and Presence* 서비스용 분할된 도메인 내 페더레이션을 참조하십시오.

메시지 아카이버

많은 업계에서는 인스턴트 메시지가 다른 모든 비즈니스 레코드와 동일한 규정 준수 가이드라인을 준수하도록 요구합니다. 이러한 규정을 준수하려면 시스템이 모든 비즈니스 레코드를 기록하고 보관해야 하며 보관된 기록을 검색할 수 있어야 합니다.

IM and Presence 서비스는 단일 클러스터, 클러스터 간 또는 페더레이션 네트워크 구성에서 다음 IM 활동에 대한 데이터를 수집하여 인스턴트 메시징(IM) 준수를 지원합니다.

- 포인트-투-포인트 메시지.
- 그룹 채팅 - 특별 또는 임시 채팅 메시지 및 영구 채팅 메시지가 포함됩니다.
- IM 규정 준수 구성 요소
- IM 규정 준수에 대한 샘플 토폴로지 및 메시지 흐름

IM 규정 준수 구성에 대한 자세한 내용은 http://www.cisco.com/c/en/us/support/unified-communications/unified-presence/products-installation-and-configuration-guides-list.html에서 *Cisco Unified Communications Manager*의 *IM and Presence* 서비스에 대한 인스턴트 메시징 준수를 참조하십시오.

IV 부

시스템 관리

24 장

채팅 관리

채팅 관리 개요

IM and Presence 서비스는 채팅방을 관리하고 액세스할 수 있는 사용자를 제어하는 데 사용할 수 있는 설정을 제공합니다. 여기에는 다음 기능이 포함됩니다.

- 새 룸을 만들고, 만든 룸의 구성원과 구성을 관리합니다.
- 해당 룸의 구성원만 액세스할 수 있도록 영구 채팅방에 대한 액세스를 제어합니다.
- 채팅방에 관리자를 할당합니다.
- 다른 사용자를 룸으로 초대합니다.
- 룸 내에 표시되는 구성원의 프레즌스 상태를 확인합니다. 방에 표시되는 프레즌스 상태는 구성원의 방 참여 여부를 확인하지만, 전반적인 프레즌스 상태를 반영하지는 않을 수 있습니다.

또한 IM and Presence 서비스를 통해 채팅 노드 별칭을 관리할 수 있습니다. 채팅 노드 별칭을 사용하면 사용자가 특정 노드에서 특정 채팅방을 검색하고 해당 채팅방에 참가할 수 있습니다.

또한 IM and Presence 서비스는 대화 내용을 보관하고 채팅방에 참가한 구성원을 포함하여 룸 구성원들에게 이 채팅방 기록을 제공합니다. 신규 및 기존 구성원이 사용할 수 있는 기존 아카이브의 양을 구성할 수 있습니다. .

채팅 노드 별칭 개요

시스템의 각 채팅 노드에는 고유한 별칭이 있습니다. 도메인 사용자가 특정 노드에서 특정 채팅 방을 검색하여 참가할 수 있도록, 채팅 노드 별칭은 각 채팅 노드에 대해 고유한 주소를 생성합니다. 채팅 노드 별칭은 해당 노드에서 생성되는 각 채팅방의 고유 ID의 일부를 형성합니다. 예를 들어, 별칭

conference-3-mycup.cisco.com은 해당 노드에서 생성된 채팅방 roomjid@conference-3-mycup.cisco.com의 이름을 지정하는 데 사용됩니다.

채팅 노드 별칭을 할당하는 모드는 두 가지가 있습니다.

- 시스템 생성 - 시스템이 각 채팅 노드에 고유한 별칭을 자동으로 할당합니다. 기본적으로 시스템은 다음 이름 지정 규칙을 사용하여 채팅 노드별로 하나의 별칭을 자동으로 생성합니다. conference-x-clusterid.domain, 여기서:
  - conference는 하드코딩된 키워드
  - x는 노드 ID를 나타내는 고유한 정수 값
  - clusterid는 구성된 엔터프라이즈 파라미터
  - domain은 구성된 도메인

  예를 들어 시스템은 다음을 할당할 수 있습니다: conference-3-mycup.cisco.com
- 수동 - 채팅 노드 별칭을 수동으로 할당하려면 시스템에서 생성한 별칭을 비활성화해야합니다. 수동으로 할당된 별칭을 사용할 경우 특정 요구 사항에 맞는 별칭을 사용하여 원하는 대로 채팅 노드의 이름을 지정할 수 있습니다. 예를 들어 congerence-x-clusterid.domain 명명 규칙이 구축 요구 사항에 맞지 않는 경우 이 작업을 수행할 수 있습니다.

노드당 여러 별칭 할당

노드 기반으로, 각 채팅 노드에 둘 이상의 별칭을 연결할 수 있습니다. 노드당 여러 별칭을 사용하는 경우 사용자는 이러한 별칭으로 추가 채팅 방을 만들 수 있습니다. 이 기능은 시스템 생성 별칭과 수동으로 생성된 별칭 모두에 적용됩니다.

채팅 관리 필수 조건

영구 채팅이 활성화되었는지 확인합니다.

채팅 관리 작업 흐름

프로시저

	명령 또는 동작	목적
단계 **1**	채팅방 소유자가 채팅방 설정을 편집할 수 있도록 활성화, 282 페이지	채팅방 소유자가 채팅방 설정을 편집할 수 있도록 허용할지 여부를 구성합니다. 그렇지 않으면 관리자만 채팅방 설정을 편집할 수 있습니다.

	명령 또는 동작	목적
단계 **2**	클라이언트의 인스턴트 메시지 내역 기록 허용, 282 페이지	사용자가 자신의 컴퓨터에 인스턴트 메시지 내역을 로컬로 기록하도록 허용할지 여부를 구성합니다.
단계 **3**	영구 채팅방 생성을 홈 클러스터로 제한, 283 페이지	이 절차를 사용하여 Cisco Jabber 사용자 홈 클러스터 내에서 영구 채팅방 생성을 제한할 수 있습니다.
단계 **4**	외부 데이터베이스 텍스트 전화회의 보고서 보기, 284 페이지	이 절차를 사용하면 영구 채팅방의 세부 정보를 볼 수 있는 외부 데이터베이스 텍스트 전화회의 보고서를 볼 수 있습니다.
단계 **5**	영구 채팅방의 소유권 전환, 284 페이지	홈 클러스터에 속하는 영구 채팅방의 소유권을 다른 기존의 구성원으로 전환하려면 이 절차를 사용합니다.
단계 **6**	영구 채팅 별칭 보고서, 285 페이지	이 절차를 사용하여 외부 데이터베이스에 있는 자체 및 피어 클러스터 별칭에 대한 채팅방 수를 봅니다.
단계 **7**	채팅방 설정을 편집합니다. 순서에 상관 없이 다음 작업 중 하나를 완료하여 채팅방 설정을 업데이트합니다. • 채팅 방 수 설정, 286 페이지 • 채팅방 구성원 설정 구성, 286 페이지 • 가용성 설정 구성, 287 페이지 • 점유율 설정 구성, 289 페이지 • 채팅 메시지 설정 구성, 289 페이지 • 조정된 방 설정 구성, 290 페이지 • 기록 설정 구성, 290 페이지	참고 영구 채팅 설정을 업데이트하는 경우 Cisco Unified IM and Presence 서비스 가용성에서 도구 > 제어 센터 - 기능 서비스를 선택하여 Cisco XCP 텍스트 전화회의 관리자 서비스를 다시 시작합니다.
단계 **8**	채팅방을 시스템 기본값으로 재설정, 291 페이지	채팅 구성을 시스템 기본값으로 재설정하려면 이 선택적 작업을 완료하십시오. 임시 채팅은 기본적으로 활성화되어 있지만 영구 채팅은 기본적으로 비활성화되어 있습니다. 이 작업을 완료하면 영구 채팅이 비활성화됩니다.
단계 **9**	채팅 노드 별칭 관리, 291 페이지	도메인 사용자가 특정 노드에서 특정 채팅방을 검색하여 참가할 수 있도록, 별칭은 각 채팅 노드에 대해 고유한 주소를 생성합니다. 시스템의 각 채팅 노드에는 고유한 별칭이 있습니다.

	명령 또는 동작	목적
단계 **10**	영구 채팅을 위한 외부 데이터베이스 정리, 294 페이지	(선택 사항) 외부 데이터베이스 정리 유틸리티를 사용하여 외부 데이터베이스를 모니터링하고 만료된 레코드를 삭제하는 작업을 구성합니다. 이렇게 하면 항상 새로운 레코드를 위한 충분한 디스크 공간이 확보됩니다.

채팅방 소유자가 채팅방 설정을 편집할 수 있도록 활성화

채팅방 소유자가 채팅방 설정을 편집할 수 있도록 허용하려는 경우 이 절차를 사용합니다.

참고 클라이언트에서 이러한 설정을 구성할 수 있는지는 클라이언트 구현에 따라 다르며, 클라이언트에서 이러한 설정을 구성할 인터페이스를 제공하는지 여부에 따라서도 다릅니다.

프로시저

단계 **1** **Cisco Unified CM IM and Presence** 관리에서 메시징 > 그룹 채팅 및 영구 채팅을 선택합니다.

단계 **2** 룸 소유자는 룸을 구성원 전용으로 할지 여부를 변경할 수 있습니다**.** 확인란의 값을 구성합니다.

- 선택 - 채팅방 소유자는 채팅방 설정을 편집할 관리 권한이 있습니다.
- 선택 취소 - 관리자만 채팅방 설정을 편집할 수 있습니다.

단계 **3** 저장을 클릭합니다.

단계 **4** **Cisco Unified IM and Presence Service** 가용성에서 도구 > 제어 센터 - 기능 서비스를 선택합니다.

단계 **5** Cisco XCP 텍스트 전화회의 관리자 서비스 다시 시작

클라이언트의 인스턴트 메시지 내역 기록 허용

사용자가 자신의 컴퓨터에 인스턴트 메시지 내역을 기록하도록 허용하거나 허용하지 않을 수 있습니다. 클라이언트 측에서는 애플리케이션이 이 기능을 지원해야 하며, 인스턴트 메시지 기록 차단을 적용해야 합니다.

프로시저

단계 **1** **Cisco Unified CM IM and Presence** 관리에서 메시징 > 설정을 선택합니다.

단계 **2** 인스턴트 메시지 내역 기록의 설정을 다음과 같이 구성합니다.

- 클라이언트 애플리케이션 사용자가 IM and Presence 서비스에서 인스턴트 메시지 내역을 기록하도록 허용하려면 고객이 인스턴트 메시징 기록을 기록하도록 허용(지원되는 고객의 경우)을 선택합니다.
- 클라이언트 애플리케이션 사용자가 IM and Presence 서비스에서 인스턴트 메시지 내역을 기록하지 못하게 하려면 고객이 인스턴트 메시징 기록을 기록하도록 허용(지원되는 고객의 경우)을 선택 취소합니다.

단계 **3** 저장을 클릭합니다.

영구 채팅방 생성을 홈 클러스터로 제한

중요 이 기능은 릴리스 14 SU1부터 적용할 수 있습니다.

이 절차를 사용하여 Cisco Jabber 사용자 홈 클러스터 내에서 영구 채팅방 생성을 제한할 수 있습니다. 이 기능은 클러스터 간 트래픽을 줄이고 시스템 대역폭을 증가시킵니다.

IM and Presence 서비스 관리자는 홈 클러스터의 사용자가 만든 모든 채팅방을 관리합니다. 다른 클러스터의 유지 보수 활동은 홈 클러스터의 사용자가 만든 채팅방에 영향을 주지 않습니다.

시작하기 전에

중요 릴리스 14SU1부터 지원됩니다.

- 영구 채팅이 활성화되었는지 확인합니다.
- 이 기능을 활성화하기 전에 그룹 채팅 및 **Persistent Chat** 설정 창에서 별칭 보고서를 선택합니다. 자세한 내용은 영구 채팅 별칭 보고서, 285 페이지를 참조하십시오.
- 이 기능을 지원하기 위해서는 Cisco Jabber 14.1 버전 이상이 필요합니다.

프로시저

단계 **1** 데이터베이스 퍼블리셔 노드에서 **Cisco Unified CM IM and Presence Service** 관리에 로그인합니다.

단계 **2** 메시징 > 그룹 채팅 및 영구 채팅을 선택합니다.

단계 **3** 영구 채팅 활성화에서 채팅방 생성을 홈 클러스터로 제한 확인란을 선택합니다.

다음에 수행할 작업

홈 클러스터의 모든 노드에서 **Cisco XCP** 텍스트 전화회의 관리자 서비스를 다시 시작합니다.

외부 데이터베이스 텍스트 전화회의 보고서 보기

외부 데이터베이스 텍스트 전화회의 보고서를 보려면 이 절차를 사용하십시오. 이 보고서를 통해 구축에서 영구 채팅방과 임시 채팅방에 대한 세부 정보를 볼 수 있습니다.

프로시저

단계 **1** **Cisco Unified CM IM and Presence** 관리에 로그인합니다.

단계 **2** 메시징 > 그룹 채팅 및 영구 채팅을 선택합니다.

단계 **3** 영구 채팅 데이터베이스 할당 아래에서 회의실 보고서 버튼을 클릭합니다.

단계 **4** 특정 기준을 충족하는 룸으로 선택을 제한하려면 필터 도구를 사용합니다.

단계 **5** 찾기를 클릭합니다.

단계 **6** 해당 룸의 세부 정보를 보려면 특정 채팅방을 선택합니다.

참고 데이터베이스에서 가져온 레코드 수는 "가져온 페치" 드롭다운 목록에서 선택한 값에 따라 달라집니다.

영구 채팅방의 소유권 전환

중요 이 기능은 릴리스 14 SU1부터 적용할 수 있습니다.

GUI에 액세스할 수 있는 IM and Presence 서비스 관리자의 경우 이 절차를 사용하여 영구 채팅방의 소유권을 양도합니다.

예를 들어, John은 영구 채팅방을 생성하고 몇 명의 구성원을 추가했고, 나중에 조직을 떠납니다.

John이 유일한 영구 채팅방 소유자이고 지정된 룸에 룸 소유자 기능이 여전히 필요한 경우, IM and Presence 서비스 관리자는 한 명 이상의 현재 룸 구성원을 새로운 룸 소유자로 선택할 수 있습니다.

소유자 **ID**를 업데이트하는 동안 다음 사항을 고려하십시오.

- 채팅방의 소유권은 이전 소유자와 동일한 홈 클러스터에 속하는 채팅방에 있는 구성원으로 변경할 수 있습니다.
- 소유자 **ID**는 사용자 **ID**가 아니라 사용자 **JID**여야 합니다.
- IM and Presence 서비스 노드 데이터베이스에 대해 입력 소유자 **ID**의 유효성을 검사합니다.
- 관리자는 채팅방 작성자의 ID를 채팅방에 대한 새 소유자 ID로 설정할 수 없습니다.

채팅방의 소유권을 변경하려면 다음 단계를 수행하십시오.

시작하기 전에

중요 릴리스 14SU1부터 지원됩니다.

소유자 **ID**를 업데이트하기 전에 홈 클러스터(HC)의 모든 IM and Presence 서비스 노드에서 **Cisco XCP** 텍스트 전화회의 관리자 서비스를 중지합니다.

프로시저

단계 **1** 데이터베이스 퍼블리셔 노드에서 **Cisco Unified Communications Manager IM and Presence Service** 관리에 로그인합니다.

단계 **2** 메시징 > 그룹 채팅 및 영구 채팅을 선택합니다.

단계 **3** 영구 채팅 데이터베이스 할당 아래에서 회의실 보고서 버튼을 클릭합니다.

단계 **4** 특정 기준을 충족하는 회의실로 선택을 제한하려면 필터 도구를 사용하고 찾기를 클릭합니다.

단계 **5** (선택 사항) 회의실 **JID**를 클릭하여 소유자 목록, 구성원 목록, 마지막 메시지 날짜 등 PChat 회의실의 필드를 봅니다. 필드에 대한 자세한 내용과 설명은 온라인 도움말을 참조하십시오.

단계 **6** 소유자 **ID** 필드를 편집하려면 회의실 **JID** 확인란을 선택합니다.

참고 소유자 **ID** 열은 홈 클러스터에 속하는 영구 채팅방의 경우에만 편집할 수 있습니다.

단계 **7** 새 소유자로 만들려는 채팅방 구성원의 이메일 형식으로 소유자 **ID**를 입력합니다.

단계 **8** 소유자 **ID** 업데이트를 클릭합니다.
이렇게 하면 하나 이상의 선택한 영구 채팅방 소유자가 동일한 소유자 **ID**로 업데이트됩니다.

다음에 수행할 작업

홈 클러스터의 모든 노드에서 **Cisco XCP** 텍스트 전화회의 관리자 서비스를 시작합니다.

영구 채팅 별칭 보고서

이 절차를 사용하여 외부 데이터베이스에 있는 채팅 방 수와 홈 및 피어 클러스터 별칭을 볼 수 있는 외부 데이터베이스 영구 채팅 별칭 보고서를 볼 수 있습니다.

프로시저

단계 **1** 데이터베이스 퍼블리셔 노드에서 **Cisco Unified CM IM and Presence** 서비스 관리에 로그인합니다.

단계 **2** 메시징 > 그룹 채팅 및 영구 채팅을 선택합니다.

단계 **3** 영구 채팅 데이터베이스 할당 아래의 드롭다운 목록에서 외부 데이터베이스를 선택합니다.

단계 **4** 별칭 보고서 버튼을 클릭합니다. 필드 설명은 온라인 도움말을 참조하십시오.

채팅방 설정 구성

채팅 방 수 설정

방 설정을 사용하면 사용자가 만들 수 있는 방의 수를 제한할 수 있습니다. 채팅 방 수 제한은 시스템 성능에 도움이 되며, 확장도 가능합니다. 또한 잠재적인 서비스 수준 공격의 완화에도 도움이 될 수 있습니다.

프로시저

단계 **1** **Cisco Unified CM IM and Presence** 관리에서 메시징 > 그룹 채팅 및 영구 채팅을 선택합니다.

단계 **2** 허용되는 최대 채팅 방 수를 변경하려면 허용되는 최대 방 수의 필드에 값을 입력합니다. 기본은 5500으로 설정됩니다.

단계 **3** 저장을 클릭합니다.

채팅방 구성원 설정 구성

구성원 설정을 이용하면 채팅 방의 구성원 자격을 제어할 수 있습니다. 그러한 제어는 구성원 자격 제한으로 차단할 수 있는 서비스 수준 공격을 완화하려는 사용자에게 유용합니다. 필요에 따라 구성원 설정을 구성하십시오.

프로시저

단계 **1** **Cisco Unified CM IM and Presence** 관리에서 메시징 > 그룹 채팅 및 영구 채팅을 선택합니다.

단계 **2** 룸 구성원 설정에 설명된 대로 룸 구성원 설정을 구성합니다.

단계 **3** 저장을 클릭합니다.

단계 **4** **Cisco Unified IM and Presence Service** 가용성에서 도구 > 제어 센터 **-** 기능 서비스를 선택합니다.

단계 **5** Cisco XCP 텍스트 전화회의 관리자 서비스 다시 시작

룸 구성원 설정

참고 영구 채팅방은 룸을 만들 때 해당 설정을 상속합니다. 이후 변경 사항은 기존 룸에 적용되지 않습니다. 이러한 변경 사항은 변경 사항이 적용된 후에 만들어진 룸에만 적용됩니다.

표 ***30:***

필드	설명
방은 기본적으로 구성원 전용임	방을 기본적으로 구성원 전용 방으로 만들려면 이 확인란을 선택합니다. 구성원 전용 룸에는 룸 소유자나 관리자가 구성한 허용 목록의 사용자만 액세스할 수 있습니다. 이 확인란은 기본적으로 선택되어 있지 않습니다. 참고 허용 목록에는 룸에 대한 액세스가 허용된 구성원의 목록이 포함되어 있습니다. 구성원 전용 방의 소유자 또는 관리자가 화이트리스트를 만듭니다.
중재자만 구성원 전용 방에 사람들을 초대할 수 있습니다.	중재자만 룸에 사용자를 초대할 수 있도록 룸을 구성하려면 이 확인란을 선택합니다. 이 확인란이 선택되어 있지 않으면 구성원이 다른 사용자를 방으로 초대할 수 있습니다. 이 확인란은 기본적으로 선택되어 있습니다.
방 소유자는 방을 구성원 전용으로 할지 여부를 변경할 수 있습니다.	룸 소유자가 구성원 전용룸인지 여부를 변경할 수 있도록 룸을 구성하려면 이 확인란을 선택합니다. 이 확인란은 기본적으로 선택되어 있습니다. 참고 방 소유자는 방을 만드는 사용자이거나, 방 생성자나 소유자가 소유자 상태를 보유하도록 지정한 사용자입니다(허용되는 경우). 방 소유자는 모든 관리자 기능을 가지고 있는 것은 물론, 방 구성을 변경하거나 방을 없앨 수도 있습니다.
방 소유자는 중재자만 구성원 전용 방에 사람들을 초대할 수 있는지 여부를 변경할 수 있습니다.	룸 소유자는 구성원이 룸에 다른 사용자를 초대할 수 있도록 룸을 구성하려면 이 확인란을 선택합니다. 이 확인란은 기본적으로 선택되어 있습니다.
사용자는 자신을 방에 구성원으로 추가할 수 있음	모든 사용자가 언제든지 룸에 가입을 요청할 수 있도록 룸을 구성하려면 이 확인란을 선택합니다. 이 확인란을 선택하면 방은 구성원 자격이 개방된 상태가 됩니다. 이 확인란은 기본적으로 선택되어 있지 않습니다.
방 소유자는 사용자가 자신을 구성원으로 방에 추가할 수 있는지 여부를 변경할 수 있습니다.	룸 소유자가 언제든 5단계에 나와 있는 설정을 변경할 수 있도록 룸을 구성하려면 이 확인란을 선택합니다. 이 확인란은 기본적으로 선택되어 있지 않습니다.

가용성 설정 구성

가용성 설정은 방 내 사용자의 가시성을 결정합니다.

프로시저

단계 **1** **Cisco Unified CM IM and Presence** 관리에서 메시징 > 그룹 채팅 및 영구 채팅을 선택합니다.
단계 **2** 가용성 설정에 설명된 대로 가용성 구성원 설정을 구성합니다.
단계 **3** 저장을 클릭합니다.
단계 **4** **Cisco Unified IM and Presence** 서비스 가용성에서 도구 > 제어 센터 - 기능 서비스를 선택합니다.
단계 **5** Cisco XCP 텍스트 전화회의 관리자 서비스 다시 시작

가용성 설정

필드	설명
방에 없는 구성원 및 관리자는 방에 계속 표시됩니다.	현재 오프라인인 경우에도 룸 명부에 사용자를 유지하려면 이 확인란을 선택합니다. 이 확인란은 기본적으로 선택되어 있습니다. 참고 관리자가 채팅방에서 나가도 관리자의 사용자 id는 채팅방에 표시됩니다. 사용자 목록을 새로 고치려면 사용자가 채팅방을 닫았다가 다시 열어야 합니다.
방 소유자는 방에 없는 구성원 및 관리자를 방에 계속 표시할지 여부를 변경할 수 있습니다.	룸 소유자가 구성원 또는 관리자의 가시성을 변경할 수 있도록 하려면 이 확인란을 선택합니다. 이 확인란은 기본적으로 선택되어 있습니다.
룸은 다른 클라이언트와 역호환됨	서비스가 이전 Group Chat 1.0 클라이언트와 제대로 작동하도록 하려면 이 확인란을 선택합니다. 이 확인란은 기본적으로 선택되어 있지 않습니다.
방 소유자는 방이 이전 클라이언트와 역호환되는지 여부를 변경할 수 있습니다	룸 소유자가 채팅방의 역호환성을 제어할 수 있도록 하려면 이 확인란을 선택합니다. 이 확인란은 기본적으로 선택되어 있지 않습니다.
방은 기본적으로 익명입니다.	룸에 사용자 별칭만 표시하고 Jabber ID를 유지하려는 경우 이 확인란을 선택합니다. 이 확인란은 기본적으로 선택되어 있지 않습니다.
방 소유자는 방을 익명으로 할지 여부를 변경할 수 있습니다.	룸 소유자가 사용자의 Jabber ID의 익명성 수준을 제어할 수 있도록 하려면 이 확인란을 선택합니다. 이 확인란은 기본적으로 선택되어 있지 않습니다.

점유율 설정 구성

점유율 설정은 주어진 시간에 채팅방에 수용할 수 있는 사용자 수를 결정합니다.

프로시저

단계 **1** 방에 허용되는 시스템 최대 사용자 수를 변경하려면 동시에 방에 있을 수 있는 사용자 수의 필드에 값을 입력합니다. 기본값은 1000입니다.

참고 방의 총 사용자 수는 설정한 값을 초과할 수 없습니다. 방의 총 사용자 수에는 일반 사용자와 숨은 사용자가 모두 포함됩니다.

단계 **2** 방에 허용되는 숨은 사용자 수를 변경하려면 동시에 방에 있을 수 있는 숨은 사용자 수의 필드에 값을 입력합니다. 숨은 사용자는 다른 사용자에게 보이지 않으며, 방에 메시지를 보낼 수 없으며, 프레즌스 업데이트를 전송하지 않습니다. 숨은 사용자는 방의 모든 메시지를 볼 수 있으며 다른 사용자의 프레즌스 업데이트를 받을 수 있습니다. 기본값은 1000입니다.

단계 **3** 방에 허용되는 기본 최대 사용자 수를 변경하려면 방에 대한 기본 최대 점유율의 필드에 값을 입력합니다. 기본값은 50으로 설정되며, 1단계에서 설정한 값보다 클 수 없습니다.

단계 **4** 방 소유자가 기본 최대 방 점유율을 변경하도록 허용하려면 방 소유자는 방에 대한 기본 최대 점유율을 변경할 수 있습니다를 선택합니다. 이 확인란은 기본적으로 선택되어 있습니다.

단계 **5** 저장을 클릭합니다.

채팅 메시지 설정 구성

역할을 기반으로 사용자에게 권한을 부여하려면 채팅 메시지 설정을 사용하십시오. 대부분의 경우 역할은 방문자-중재자 계층 구조로 존재합니다. 예를 들어, 참가자는 방문자가 할 수 있는 모든 것을 할 수 있으며 중재자는 참가자가 할 수 있는 모든 것을 할 수 있습니다.

이 확인란은 기본적으로 선택되어 있습니다.

프로시저

단계 **1** 사용자가 방 내에서 개인 메시지를 보내기 위해 가질 수 있는 최저 참가 수준의 드롭다운 목록에서 다음 중 하나를 선택합니다.

- 방문자 - 방문자, 참가자 및 중재자가 방의 다른 사용자에게 개인 메시지를 보낼 수 있습니다. 이 값이 기본 설정입니다.
- 참가자 - 참가자 및 중재자가 방의 다른 사용자에게 개인 메시지를 보낼 수 있습니다.
- 중재자 - 중재자만 방의 다른 사용자에게 개인 메시지를 보낼 수 있습니다.

단계 **2** 방 소유자가 개인 메시지에 대한 최소 참가 수준을 변경하도록 허용하려면 방 소유자는 사용자가 방 내에서 개인 메시지를 보내기 위해 가질 수 있는 최저 참가 수준을 변경할 수 있습니다를 선택합니다. 이 확인란은 기본적으로 선택되어 있습니다.

단계 **3** 사용자가 방 주제를 변경하기 위해 가질 수 있는 최저 참가 수준 드롭다운 목록에서 다음 중 하나를 선택합니다.

a) 참가자 - 참가자와 중재자가 방 주제를 변경할 수 있습니다. 이 값이 기본 설정입니다.

b) 중재자 - 중재자만 방 주제를 변경할 수 있습니다.

방문자는 방 주제를 변경할 수 없습니다.

단계 **4** 방 소유자가 방 주제 업데이트를 위한 최소 참가 수준을 변경하도록 허용하려면 방 소유자는 사용자가 방 주제를 변경하기 위해 가질 수 있는 최저 참가 수준을 변경할 수 있습니다를 선택합니다.

단계 **5** 메시지에서 모든 XHTML(Extensible Hypertext Markup Language)을 제거하려면 메시지에서 모든 **XHTML** 서식 지정 제거를 선택합니다. 이 확인란은 기본적으로 선택되어 있지 않습니다.

단계 **6** 방 소유자가 XHTML 서식 지정 설정을 변경하도록 허용하려면 방 소유자는 **XHTML** 서식 지정 설정을 변경할 수 있습니다를 선택합니다. 이 확인란은 기본적으로 선택되어 있지 않습니다.

단계 **7** 저장을 클릭합니다.

조정된 방 설정 구성

조정된 방은 중재자가 방 내 음성 권한을 허가 및 취소할 수 있는 기능을 제공합니다(그룹 채팅 컨텍스트에서 음성은 방에 채팅 메시지를 전송할 수 있는 기능을 의미함). 방문자는 조정된 방에서 인스턴트 메시지를 전송할 수 없습니다.

프로시저

단계 **1** 방에서 중재자의 역할을 강제로 적용하려면 방은 기본적으로 조정됩니다를 선택합니다. 이 확인란은 기본적으로 선택되어 있지 않습니다.

단계 **2** 방 소유자가 방의 조정 여부를 변경하도록 허용하려면 방 소유자는 방이 기본으로 조정되는지 여부를 변경할 수 있습니다를 선택합니다. 이 확인란은 기본적으로 선택되어 있습니다.

단계 **3** 저장을 클릭합니다.

기록 설정 구성

채팅 방에서 검색 및 표시되는 메시지의 기본값과 최대값을 설정하고 기록 쿼리를 통해 검색할 수 있는 메시지 수를 제어하려면 기록 설정을 사용합니다. 사용자가 채팅 방에 참가하면, 채팅 방의 메시지 기록이 사용자에게 전송됩니다. 기록 설정은 사용자에게 전송되는 이전 메시지의 수를 결정합니다.

프로시저

단계 **1** 사용자가 아카이브에서 검색할 수 있는 최대 메시지 수를 변경하려면 아카이브에서 검색할 수 있는 최대 메시지 수의 필드에 값을 입력합니다. 기본값은 100로 설정되어 있습니다. 이것은 다음 설정에 대해 한계 역할을 합니다.

단계 **2** 사용자가 채팅 방에 참가할 때 표시되는 이전 메시지의 수를 변경하려면 기본적으로 표시되는 채팅 기록의 메시지 수의 필드에 값을 입력합니다. 기본값은 15로 설정되며, 1단계에서 설정한 값보다 클 수 없습니다.

단계 **3** 사용자가 채팅 방에 참가할 때 표시할 이전 메시지 수를 방 소유자가 변경하도록 허용하려면 방 소유자는 채팅 기록에 표시되는 메시지 수를 변경할 수 있습니다를 선택합니다. 이 확인란은 기본적으로 선택되어 있지 않습니다.

단계 **4** 저장을 클릭합니다.

채팅방을 시스템 기본값으로 재설정

특별 및 영구 채팅방의 그룹 채팅 설정을 시스템 기본값으로 재설정하려면 이 절차를 사용하십시오.

참고 임시 채팅은 기본적으로 활성화되어 있지만 영구 채팅은 기본적으로 비활성화되어 있습니다. 이 작업을 완료하면 영구 채팅이 비활성화됩니다.

프로시저

단계 **1** **Cisco Unified CM IM and Presence** 관리에서 메시징 > 설정을 선택합니다.

단계 **2** 기본값으로 설정을 클릭합니다.

단계 **3** 저장을 클릭합니다.

채팅 노드 별칭 관리

채팅 노드 별칭 관리

클러스터의 채팅 노드 별칭을 관리하려면 다음 작업을 완료하십시오. 시스템에서 별칭을 자동으로 관리하게 하거나 직접 별칭을 업데이트할 수 있습니다.

프로시저

	명령 또는 동작	목적
단계 **1**	채팅 별칭 관리를 위한 할당 모드 , 292 페이지	시스템에서 채팅 노드 별칭을 관리할지 또는 수동으로 수행할지 여부를 지정합니다.
단계 **2**	수동으로 채팅 노드 별칭 추가, 292 페이지	클러스터의 채팅 노드 별칭을 추가, 편집 또는 삭제합니다.

채팅 별칭 관리를 위한 할당 모드

시스템에서 `conference-x-clusterid.domain` 명명 규칙을 사용하여 자동으로 채팅 노드 별칭을 할당할지 여부 또는 수동으로 할당할지 여부를 구성합니다.

시작하기 전에

채팅 노드 별칭에 대한 자세한 내용은 채팅 노드 별칭 개요, 279 페이지의 내용을 참조하십시오.

프로시저

단계 **1** **Cisco Unified CM IM and Presence** 관리에서 메시징 > 그룹 채팅 및 영구 채팅을 선택합니다.

단계 **2** 시스템 생성 별칭을 활성화 또는 비활성화합니다.

- 시스템에서 채팅 노드 별칭을 자동으로 할당하려면 시스템에서 기본 그룹 채팅 서버 별칭을 자동으로 관리합니다.를 선택합니다.

  팁 시스템 생성 별칭이 기본 그룹 채팅 서버 별칭 아래에 나열되는지 확인하려면 메시징 > 그룹 채팅 서버 별칭 매핑을 선택합니다.

- 채팅 노드 별칭을 수동으로 할당하려면 시스템에서 기본 그룹 채팅 서버 별칭을 자동으로 관리합니다.를 선택 취소합니다.

다음에 수행할 작업

- 채팅 노드에 대한 시스템 생성 별칭을 구성하더라도 필요한 경우 노드에 둘 이상의 별칭을 연결할 수 있습니다.
- 제휴된 외부 도메인이 있는 경우, 별칭이 변경되었고 새 별칭을 사용할 수 있음을 제휴된 측에 알리고자 할 수 있습니다. 모든 별칭을 외부에 광고하려면 DNS를 구성하고 별칭을 DNS 레코드로서 게시하십시오.
- 시스템 생성 별칭 구성을 업데이트하는 경우 다음 작업 중 하나를 수행합니다. Cisco XCP 텍스트 전화회의 관리자 다시 시작.
- 채팅 노드 별칭을 추가, 편집 또는 삭제하려면 수동으로 채팅 노드 별칭 추가, 292 페이지.

수동으로 채팅 노드 별칭 추가

채팅 노드 별칭을 수동으로 추가, 편집 또는 삭제하려면 이 절차를 사용하십시오. 채팅 노드 별칭을 수동으로 관리하려면 시스템 생성 별칭을 사용하는 기본 설정을 해제해야 합니다. 시스템 생성 별칭을 해제하면 기존 별칭(`conference-x-clusterid.domain`)이 Conference Server Aliases 아래에 나열된 편집 가능한 표준 별칭으로 복구됩니다. 이렇게 하여 이전 별칭 및 이와 연결된 채팅 방 주소가 유지 관리됩니다.

채팅 노드에 여러 별칭을 수동으로 할당할 수 있습니다. 채팅 노드에 대한 시스템 생성 별칭이 이미 있더라도 해당 노드에 추가 별칭을 수동으로 연결할 수 있습니다.

수동 관리 별칭의 경우, 클러스터 ID 또는 도메인이 변경되면 관리자가 별칭 목록을 수동으로 업데이트해야 합니다. 시스템 생성 별칭은 변경된 값을 자동으로 처리합니다.

참고 의무 사항은 아니지만, 노드에 새 채팅 노드 별칭을 할당할 때에는 항상 도메인을 포함하는 것이 좋습니다. 추가 별칭 newalias.proxydomain에 대해 이 규칙 사용 **Cisco Unified CM IM and Presence** 관리 > 프레즌스 설정 > 고급 설정을 선택하여 도메인을 봅니다.

시작하기 전에

채팅 별칭 관리를 위한 할당 모드 , 292 페이지

프로시저

단계 **1** **Cisco Unified CM IM and Presence** 관리에서 메시징 > 그룹 채팅 서버 별칭 매핑을 선택합니다.

단계 **2** 찾기를 클릭합니다.

그룹 채팅 서버 별칭 창에 기존 노드 별칭이 표시됩니다.

단계 **3** 새 별칭을 추가하려면:

a) 새로 추가를 클릭합니다.
b) 그룹 채팅 서버 별칭 필드에 새 별칭을 입력합니다.
c) 서버 이름 드롭다운 목록 상자에서 별칭을 할당할 서버를 선택합니다.
d) 저장을 클릭합니다.

단계 **4** 기존 별칭을 편집하려면:

a) 별칭을 선택합니다.
b) 업데이트를 입력하고 저장을 클릭합니다.

단계 **5** 별칭을 삭제하려면 별칭을 선택하고 선택한 항목 삭제를 클릭합니다.

다음에 수행할 작업

- Cisco XCP 텍스트 전화회의 관리자를 켭니다.

채팅 노드 별칭 문제 해결 팁

- 모든 채팅 노드 별칭은 고유해야 합니다. 시스템에서는 사용자가 클러스터 전체에서 중복된 채팅 노드 별칭을 만들지 못하게 합니다.
- 채팅 노드 별칭 이름은 IM and Presence 도메인 이름과 일치할 수 없습니다.

- 더 이상 이전 별칭으로 채팅 방 주소를 유지 관리할 필요가 없는 경우에만 이전 별칭을 삭제하십시오.
- 제휴된 외부 도메인이 있는 경우, 별칭이 변경되었고 새 별칭을 사용할 수 있음을 제휴된 측에 알리고자 할 수 있습니다. 모든 별칭을 외부에 광고하려면 DNS를 구성하고 별칭을 DNS 레코드로서 게시하십시오.
- 채팅 노드 별칭 구성을 업데이트하는 경우 Cisco XCP 텍스트 전화회의 관리자를 다시 시작하십시오.

영구 채팅을 위한 외부 데이터베이스 정리

외부 데이터베이스를 모니터링하고 만료된 레코드를 삭제하는 작업을 구성합니다. 이렇게 하면 항상 새로운 레코드를 위한 충분한 디스크 공간이 확보됩니다.

Persistent Chat용 데이터베이스 테이블을 정리하려면 기능 테이블에서 텍스트 전화회의**(TC)** 기능을 선택해야 합니다.

프로시저

단계 **1** 데이터베이스 퍼블리셔 노드에서 Cisco Unified CM IM and Presence 관리에 로그인합니다.

단계 **2** 메시징 > 외부 서버 설정 > 외부 데이터베이스 작업을 선택합니다.

단계 **3** 외부 **DB** 지우기를 클릭합니다.

단계 **4** 다음 중 하나를 수행합니다.

- 퍼블리셔 노드에 연결하는 외부 데이터베이스를 수동으로 정리하려면 **SameCup** 노드를 선택합니다.
- 퍼블리셔 노드에 연결하는 외부 데이터베이스를 수동으로 정리하려면 기타 **CupNode**를 선택한 다음 외부 데이터베이스 세부 정보를 선택합니다.
- 외부 데이터베이스를 자동으로 모니터링하고 지우도록 시스템을 구성하는 경우 자동 정리 라디오 버튼을 선택합니다.

참고 자동 정리를 설정하기 전에 수동 정리를 실행하는 것이 좋습니다.

단계 **5** 파일 삭제를 되돌릴 일 수를 설정합니다. 예를 들어 90을 입력하면 시스템은 90일 이상된 레코드를 삭제합니다.

단계 **6** 데이터베이스의 색인과 저장 프로시저를 만들려면 스키마 업데이트를 클릭합니다.

참고 작업을 처음 실행할 때만 스키마를 업데이트해야 합니다.

단계 **7** 파일 삭제를 되돌릴 일 수를 설정합니다. 예를 들어 **90**을 입력하면 시스템은 90일 이상된 레코드를 삭제합니다.

단계 **8** 기능 표 섹션에서 레코드를 정리할 각 기능을 선택합니다.

- 텍스트 전화회의**(TC)** - 영구 채팅 기능의 데이터베이스 테이블을 정리하려면 이 옵션을 선택합니다.

- 메시지 보관**(MA)** - 메시지 보관 기능의 데이터베이스 테이블을 정리하려면 이 옵션을 선택합니다.
- 관리되는 파일 전송**(MFT)** - 관리되는 파일 전송 기능의 데이터베이스 테이블을 정리하려면 이 옵션을 선택합니다.

단계 **9** 정리 작업 제출을 클릭합니다.

참고 자동 옵션이 활성화된 상태에서 자동 옵션을 사용하지 않으려면 자동 정리 작업 비활성화 버튼을 클릭합니다.

채팅 상호 작용 관리

채팅 노드 별칭을 변경하면 데이터베이스에서 채팅 방의 주소를 지정하지 못하게 되므로 사용자들이 기존의 채팅 방을 찾지 못할 수 있습니다.

별칭 또는 다른 노드 종속성을 구성하는 부분을 변경하기 전에 이러한 점에 유의해야 합니다.

- 클러스터 ID - 이 값은 FQDN(정규화된 도메인 이름)의 일부입니다. 클러스터 ID를 변경하면(시스템 > 프레즌스 토폴로지: 설정 선택) 클러스터 전체에서 자동으로 변경되도록 FQDN은 새 값과 시스템 관리 별칭을 통합합니다. 수동 관리 별칭의 경우, 클러스터 ID가 변경되면 관리자가 별칭 목록을 수동으로 업데이트해야 합니다.
- 도메인 - 이 값은 FQDN의 일부입니다. 도메인을 변경하면(프레즌스 > 프레즌스 설정 선택) 클러스터 전체에서 자동으로 변경되도록 FQDN은 새 값과 시스템 관리 별칭을 통합합니다. 수동 관리 별칭의 경우, 도메인이 변경되면 관리자가 별칭 목록을 수동으로 업데이트해야 합니다.
- 채팅 노드와 외부 데이터베이스 간 연결 - 영구 채팅이 활성화된 상태에서 외부 데이터베이스와 올바른 연결을 유지 관리하지 못하면 채팅 노드가 시작되지 않습니다.
- 채팅 노드 삭제 - 프레즌스 토폴로지에서 기존 별칭과 연결된 노드를 삭제하면, 추가 조치를 취하지 않는 한 이전 별칭으로 만든 채팅 방에 주소가 지정되지 않을 수 있습니다.

변경에 따른 영향을 포괄적으로 고려하지 않은 상태에서 기존 별칭을 변경하는 것은 바람직하지 않습니다.

- 사용자가 필요 시 이전 별칭을 통해 기존 채팅 방을 찾을 수 있도록 데이터베이스에서 이전 채팅 노드의 주소를 유지 관리해야 합니다.
- 외부 도메인과의 페더레이션이 있는 경우, 해당 도메인의 사용자에게 별칭이 변경되었고 새 주소를 이용할 수 있음을 알리려면 DNS에 별칭을 게시해야 할 수 있습니다. 이는 모든 별칭을 외부에 광고할지에 따라 다릅니다.

25 장

관리되는 파일 전송 관리

관리되는 파일 전송 관리 개요

IM and Presence 서비스 관리자는 관리되는 파일 전송 기능의 파일 저장 및 디스크 사용을 관리해야 합니다. 이 장을 사용하여 파일 저장 및 디스크 사용 레벨을 모니터링하고 레벨이 정의된 임계 값을 초과할 때 알려주는 카운터 및 경고를 설정합니다.

외부 파일 서버 및 데이터베이스 서버 관리

외부 데이터베이스 크기를 관리할 때 사양에 따라 파일이 데이터베이스에서 자동으로 제거되도록 셸 스크립팅과 쿼리를 결합할 수 있습니다. 쿼리를 만들려면 파일 전송 메타데이터를 사용합니다. 여기에는 전송 유형, 파일 형식, 타임스탬프, 파일 서버에서 파일의 절대 경로 및 기타 정보를 포함합니다.

IM 및 그룹 채팅 내에서 파일 전송을 다루는 방법을 선택할 때에는, 일대일 IM 및 그룹 채팅이 일시적이어서 전송된 파일이 즉시 삭제될 수 있음을 고려해야 합니다. 그러나 다음에 유의하십시오.

- 오프라인 사용자에게 전달되는 IM은 파일에 대한 요청 지연을 트리거할 수 있습니다.
- 영구 채팅 전송은 좀 더 길게 유지해야 할 수 있습니다.

참고

- 현재 UTC 시간 중에 생성된 파일은 삭제하지 마십시오.
- 파일 서버가 할당된 후, 파일 서버 자체가 아니라 파일 서버 구성의 이름을 변경할 수 있습니다.
- 관리되는 파일 전송을 구성한 상태에서 설정을 변경하는 경우 Cisco XCP Router 서비스를 다시 시작하면 관리되는 파일 전송 기능도 다시 시작됩니다.
- 파일 서버 자체에서 변경하지 않은 채 설정을 변경하면 파일 전송 작동이 중지되며, Cisco XCP Router 서비스를 다시 시작한다는 알림이 전송됩니다.
- 데이터베이스 또는 파일 서버 오류가 발생하면 이를 알리는 메시지가 생성됩니다. 그러나 오류 응답에서는 데이터베이스, 파일 서버 또는 기타 내부 오류 간에 구분이 되지 않습니다. 실시간 모니터링 도구는 데이터베이스 또는 파일 서버에 장애가 발생하면 경보를 생성합니다. 이 경고는 파일 전송 발생 여부와 관련이 없습니다.

관리되는 파일 전송 관리 필수 조건

관리되는 파일 전송 기능을 구성합니다.

관리되는 파일 전송 관리 작업 흐름

프로시저

	명령 또는 동작	목적
단계 **1**	AFT_LOG 테이블 예제 쿼리 및 출력 , 299 페이지	다음 절차는 `AFT_LOG` 테이블에서 실행할 수 있는 쿼리의 예와 출력을 사용하여 파일 서버에서 원하지 않는 파일을 제거하는 방법을 제공합니다.
단계 **2**	서비스 파라미터 임계값 설정, 300 페이지	관리되는 파일 전송 서비스 파라미터를 구성하여 외부 파일 서버 디스크 공간에 대해 RTMT 경보가 생성되는 임계값을 정의합니다.
단계 **3**	XCP 파일 전송 관리자 알람 구성, 301 페이지	정의된 임계값에 도달한 시점을 알려주는 관리되는 파일 전송에 대한 경보를 구성합니다.
단계 **4**	관리되는 파일 전송을 위한 외부 데이터베이스 정리, 303 페이지	(선택 사항) 외부 데이터베이스 정리 유틸리티를 사용하여 외부 데이터베이스를 모니터링하고 만료된 레코드를 삭제하는 작업을 구성합니다. 이렇게 하면 항상 새로운 레코드를 위한 충분한 디스크 공간이 확보됩니다.

AFT_LOG 테이블 예제 쿼리 및 출력

다음 절차는 AFT_LOG 테이블에서 실행할 수 있는 쿼리의 예와 출력을 사용하여 파일 서버에서 원하지 않는 파일을 제거하는 방법을 제공합니다.

이 쿼리는 지정된 날짜 이후에 업로드된 모든 파일에 대한 레코드를 반환합니다.

참고 샘플 SQL 명령은 외부 데이터베이스 디스크 사용, 299 페이지의 내용을 참조하십시오.

프로시저

단계 **1** 외부 데이터베이스에 다음 명령을 입력합니다.

```
SELECT file_path
aft_log
여기서 method='Post' AND timestampvalue > '2014-12-18 11:58:39';
```

명령은 다음 출력을 생성합니다.

```
/opt/mftFileStore/node_1/files/im/20140811/15/file_name1
/opt/mftFileStore/node_1/files/im/20140811/15/file_name2
/opt/mftFileStore/node_1/files/im/20140811/15/file_name3
/opt/mftFileStore/node_1/files/im/20140811/15/file_name4
...
/opt/mftFileStore/node_1/files/im/20140811/15/file_name99
/opt/mftFileStore/node_1/files/im/20140811/15/file_name100
```

단계 **2** rm 명령과 이 출력을 사용하여 외부 파일 서버에서 위의 파일을 제거하는 스크립트를 작성합니다. 샘플 SQL 쿼리는 *Cisco Unified Communications Manager*의 *IM and Presence* 서비스에 대한 데이터베이스 설정을 참조하십시오.

참고 외부 파일 서버에서 제거되지 않은 파일은 해당 파일과 관련된 레코드가 외부 데이터베이스에서 삭제된 경우에도 계속 액세스하거나 다운로드할 수 있습니다.

다음에 수행할 작업

서비스 파라미터 임계값 설정, 300 페이지

외부 데이터베이스 디스크 사용

디스크나 테이블 공간이 가득 차지 않도록 해야 합니다. 그렇지 않으면 관리되는 파일 전송 기능이 작동하지 않을 수 있습니다. 다음은 외부 데이터베이스에서 레코드를 제거하는 데 사용할 수 있는 샘

플 SQL 명령입니다. 추가 쿼리는 *Cisco Unified Communications Manager*의 *IM and Presence* 서비스에 대한 데이터베이스 설정을 참조하십시오.

참고 외부 파일 서버에서 제거되지 않은 파일은 해당 파일과 관련된 레코드가 외부 데이터베이스에서 삭제된 경우에도 계속 액세스하거나 다운로드할 수 있습니다.

동작	샘플 명령
업로드된 파일의 모든 레코드를 제거합니다.	`DELETE` *`aft_log`* 여기서 *`method`* = `'Post';`
특정 사용자가 다운로드한 모든 파일의 레코드를 제거합니다.	`DELETE` *`aft_log`* 여기서 *`jid`* `LIKE '<userid>@<domain>%' AND` *`method`* = `'Get';`
특정 시간 후에 업로드한 모든 파일의 레코드를 제거합니다.	`DELETE` *`aft_log`* 여기서 *`method`* = `'Post' AND` *`timestampvalue > '2014-12-18 11:58:39';`*

또한 데이터베이스 디스크 사용을 관리하는 데 도움이 되는 카운터 및 경보가 있습니다. 자세한 내용은 관리되는 파일 전송에 대한 알람 및 카운터, 301 페이지를 참조하십시오.

서비스 파라미터 임계값 설정

관리되는 파일 전송 서비스 파라미터를 구성하여 외부 파일 서버 디스크 공간에 대해 RTMT 경보가 생성되는 임계값을 정의합니다.

프로시저

단계 **1** Cisco Unified CM IM and Presence 관리에서 시스템 > 서비스 파라미터를 선택합니다.

단계 **2** 노드에 대한 **Cisco XCP** 파일 전송 관리자 서비스를 선택합니다.

단계 **3** 다음 서비스 파라미터의 값을 입력합니다.

- 외부 파일 서버의 사용 가능한 공간 하한 임계값 - 외부 파일 서버 파티션의 사용 가능한 공간 비율이 이 값 이하이면 XcpMFTExtFsFreeSpaceWarn 경고가 발생합니다. 기본값은 10%입니다.
- 외부 파일 서버의 사용 가능한 공간 상한 임계값 - 외부 파일 서버 파티션의 사용 가능한 공간 비율이 이 값에 도달하거나 초과하면 XcpMFTExtFsFreeSpaceWarn 경고가 해제됩니다. 기본값은 15%입니다.

참고 하한 임계값이 상한 임계값보다 커지도록 구성하지 마십시오. 그렇지 않으면 Cisco XCP 라우터 서비스를 다시 시작한 후에 Cisco XCP 파일 전송 관리자 서비스가 시작되지 않습니다.

단계 **4** 저장을 클릭합니다.

단계 **5** Cisco XCP 라우터 서비스 다시 시작.

a) Cisco Unified IM and Presence 서비스 가용성에서 도구 > 제어 센터 - 네트워크 서비스를 선택합니다.

b) 서버 드롭다운에서 IM and Presence 게시자 노드를 선택하고 이동을 클릭합니다.

c) **IM and Presence** 서비스 아래에서 **Cisco XCP** 라우터를 선택하고 다시 시작을 클릭합니다.

다음에 수행할 작업

XCP 파일 전송 관리자 알람 구성, 301 페이지

XCP 파일 전송 관리자 알람 구성

정의된 임계값에 도달한 시점을 알려주는 관리되는 파일 전송에 대한 경보를 구성합니다.

프로시저

단계 **1** **Cisco Unified IM and Presence** 서비스 가용성에 로그인합니다.

단계 **2** 알람 > 구성을 선택합니다.

단계 **3** 서버 드롭다운 목록에서 서버(노드)를 선택하고 이동을 클릭합니다.

단계 **4** 서비스 그룹 드롭다운 목록에서 **IM and Presence** 서비스를 선택하고 이동을 클릭합니다.

단계 **5** 서비스 드롭다운 목록에서 **Cisco XCP** 파일 전송 관리자**(**활성**)**를 선택하고 이동을 클릭합니다.

단계 **6** 원하는 대로 알람 설정을 구성합니다. 필드 및 해당 설정에 대한 도움이 필요한 경우 온라인 도움말을 참조하십시오.

단계 **7** 저장을 클릭합니다.

다음에 수행할 작업

사용 가능한 알람 및 카운터에 대한 자세한 내용은 다음을 참조하십시오. 관리되는 파일 전송에 대한 알람 및 카운터, 301 페이지

관리되는 파일 전송에 대한 알람 및 카운터

관리되는 파일 전송을 사용하면 전송된 파일이 사용자에게 전달되려면 먼저 해당 파일이 외부 파일 서버에 성공적으로 아카이브되고 파일 메타데이터가 외부 데이터베이스에 기록되어야 합니다. 외부

파일 서버 또는 외부 데이터베이스에 대해 IM and Presence 서비스 노드의 연결이 끊어지면 IM and Presence 서비스는 파일을 수신자에게 전달하지 못합니다.

관리되는 파일 전송에 대한 알람

연결이 끊어질 때 알림을 받으려면 실시간 모니터링 도구에서 다음 알람이 올바르게 구성되었는지 확인합니다.

참고 외부 파일 서버에 대한 연결이 손실되기 전 업로드된 모든 파일 및 수신자에게 다운로드되고 있던 모든 파일은 다운로드할 수 없게 됩니다. 그러나 실패한 전송의 기록이 외부 데이터베이스에 있습니다. 해당 파일에 대해서는 외부 데이터베이스 필드 file_size 및 bytes_transferred가 일치하지 않습니다.

표 ***31:*** 관리되는 파일 전송에 대한 알람

Alarm	문제	해결 방법
XcpMFTExtFsMountError	Cisco XCP 파일 전송 관리자와 외부 파일 서버의 연결이 끊어졌습니다.	자세한 내용은 외부 파일 서버 문제 해결 프로그램을 확인하십시오. 외부 파일 서버가 올바르게 실행 중인지 확인하십시오. 외부 파일 서버에 대한 네트워크 연결에 문제가 있는지 확인하십시오.
XcpMFTExtFsFreeSpaceWarn	Cisco XCP 파일 전송 관리자에서 외부 파일 서버의 사용 가능 디스크가 부족하다는 것을 감지했습니다.	파일 전송에 사용할 파티션에서 불필요한 파일을 삭제하여 외부 파일 서버의 공간을 확보하십시오.
XcpMFTDBConnectError	Cisco XCP 데이터 액세스 레이어가 데이터베이스에 연결할 수 없습니다.	자세한 내용은 문제 해결 프로그램을 확인하십시오. 외부 데이터베이스가 정상적으로 실행되는지, 외부 데이터베이스 서버와의 네트워크 연결에 문제가 없는지 확인하십시오.
XcpMFTDBFullError	Cisco XCP 파일 전송 관리자는 디스크나 테이블스페이스가 가득 차서 외부 데이터베이스의 데이터를 삽입하거나 수정할 수 없습니다.	데이터베이스를 확인하고 디스크 공간을 확보하거나 복구할 수 있는지 평가합니다. 추가 데이터베이스 용량을 추가하는 것을 고려하십시오.

관리되는 파일 전송에 대한 카운터

관리되는 파일 전송을 관리하는 데 도움이 되도록 실시간 모니터링 도구를 통해 다음 카운터를 모니터링할 수 있습니다. 이러한 카운터는 Cisco XCP MFT Counters 폴더에 저장됩니다.

표 ***32:*** 관리되는 파일 전송에 대한 카운터

카운터	설명
MFTBytesDownloadedLastTimeslice	마지막 보고 기간(일반적으로 60초)에 다운로드된 바이트 수를 나타냅니다.
MFTBytesUpoadedLastTimeslice	마지막 보고 기간(일반적으로 60초)에 업로드된 바이트 수를 나타냅니다.
MFTFilesDownloaded	다운로드된 총 파일 수를 나타냅니다.
MFTFilesDownloadedLastTimeslice	마지막 보고 기간(일반적으로 60초)에 다운로드된 파일 수를 나타냅니다.
MFTFilesUploaded	업로드된 총 파일 수를 나타냅니다.
MFTFilesUploadedLastTimeslice	마지막 보고 기간(일반적으로 60초)에 업로드된 파일 수를 나타냅니다.

관리되는 파일 전송을 위한 외부 데이터베이스 정리

외부 데이터베이스를 모니터링하고 만료된 레코드를 삭제하는 작업을 구성합니다. 이렇게 하면 항상 새로운 레코드를 위한 충분한 디스크 공간이 확보됩니다.

관리형 파일 전송용 데이터베이스 테이블을 정리하려면 기능 테이블에서 관리되는 파일 전송**(MFT)** 기능을 선택해야 합니다.

프로시저

단계 **1** 데이터베이스 퍼블리셔 노드에서 Cisco Unified CM IM and Presence 관리에 로그인합니다.

단계 **2** 메시징 > 외부 서버 설정 > 외부 데이터베이스 작업을 선택합니다.

단계 **3** 외부 **DB** 지우기를 클릭합니다.

단계 **4** 다음 중 하나를 수행합니다.

- 퍼블리셔 노드에 연결하는 외부 데이터베이스를 수동으로 정리하려면 **SameCup** 노드를 선택합니다.
- 퍼블리셔 노드에 연결하는 외부 데이터베이스를 수동으로 정리하려면 기타 **CupNode**를 선택한 다음 외부 데이터베이스 세부 정보를 선택합니다.
- 외부 데이터베이스를 자동으로 모니터링하고 지우도록 시스템을 구성하는 경우 자동 정리 라디오 버튼을 선택합니다.

참고 자동 정리를 설정하기 전에 수동 정리를 실행하는 것이 좋습니다.

단계 **5** 파일 삭제를 되돌릴 일 수를 설정합니다. 예를 들어 90을 입력하면 시스템은 90일 이상된 레코드를 삭제합니다.

단계 **6** 데이터베이스의 색인과 저장 프로시저를 만들려면 스키마 업데이트를 클릭합니다.

참고 작업을 처음 실행할 때만 스키마를 업데이트해야 합니다.

단계 **7** 파일 삭제를 되돌릴 일 수를 설정합니다. 예를 들어 **90**을 입력하면 시스템은 90일 이상된 레코드를 삭제합니다.

단계 **8** 기능 표 섹션에서 레코드를 정리할 각 기능을 선택합니다.

- 텍스트 전화회의**(TC)** - 영구 채팅 기능의 데이터베이스 테이블을 정리하려면 이 옵션을 선택합니다.
- 메시지 보관**(MA)** - 메시지 보관 기능의 데이터베이스 테이블을 정리하려면 이 옵션을 선택합니다.
- 관리되는 파일 전송**(MFT)** - 관리되는 파일 전송 기능의 데이터베이스 테이블을 정리하려면 이 옵션을 선택합니다.

단계 **9** 정리 작업 제출을 클릭합니다.

참고 자동 옵션이 활성화된 상태에서 자동 옵션을 사용하지 않으려면 자동 정리 작업 비활성화 버튼을 클릭합니다.

26 장

최종 사용자 관리

최종 사용자 관리 개요

사용자를 IM and Presence 서비스 노드에 맞추고 IM and Presence 서비스에 대해 최종 사용자를 설정하는 방법에 대한 자세한 내용은 다음 설명서를 참조하십시오.

최종 사용자 관리를 위한 관리 작업의 일환으로 다음 작업을 관리해야 할 수 있습니다.

- 프레즌스 요청 권한 부여를 위한 기본 정책 구성
- 중복되거나 유효하지 않은 사용자 ID 및 디렉터리 URI에 대해 예약된 시스템 검사 구성
- 사용자 ID 및 디렉터리 URI 문제가 발생할 때 수정

최종 사용자를 가져오고 설정하는 방법에 대한 자세한 내용은 *Cisco Unified Communications Manager* 시스템 구성 설명서의 "최종 사용자 구성" 섹션을 참조하십시오.

대량 사용자 연락처 목록 가져오기 및 내보내기 완료에 대한 자세한 내용은 연락처 목록의 벌크 관리, 397 페이지의 내용을 참조하십시오.

프레즌스 권한 부여 개요

프레즌스 가입 요청에 대한 시스템 권한 부여 정책을 지정해야 합니다. 프레즌스 권한 부여 정책은 시스템 수준에서 시스템의 최종 사용자가 프레즌스가 요청된 최종 사용자의 권한을 요구하지 않고 다른 최종 사용자의 프레진스를 볼 수 있는지 여부를 결정합니다. 이 설정은 프레즌스 설정 창에서 사용자에게 승인에 대한 메시지를 표시하지 않고 다른 사용자의 사용 가능성을 확인할 수 있도록 허용 확인란을 통해 설정됩니다. 사용 가능한 설정은 구축할 프로토콜에 부분적으로 의존합니다.

- SIP 기반 클라이언트의 경우 모든 프레즌스 구독 요청을 자동으로 승인하도록 IM and Presence 서비스를 구성해야 합니다. 그렇지 않으면 프레즌스가 올바르게 작동하지 않습니다(이것이 기본 설정임). 이 옵션을 구성하면 IM and Presence 서비스는 프레즌스가 요청되는 사용자가 Cisco

Jabber 클라이언트에서 요청을 하는 사용자를 포함하여 차단 목록을 구성한 경우를 제외하고는 모든 요청을 자동으로 승인합니다. 이 경우 프레즌스 요청을 승인할 것인지 묻는 메시지가 표시됩니다.

- XMPP 기반 클라이언트의 경우 IM and Presence 서비스에서 다른 사용자의 프레즌스 요청에 권한을 부여할지 또는 이러한 프레즌스 요청을 자동으로 승인해야 하는지 여부를 묻는 메시지를 표시할지 구성할 수 있습니다.

참고 최종 사용자가 Cisco Jabber 클라이언트에서 구성할 수 있는 사용자 정책 구성을 통해 권한 부여 시스템 설정을 재정의할 수 있습니다

Jabber의 사용자 정책 설정

프레즌스 요청을 인증할 때 IM and Presence 서비스는 사용자가 Cisco Jabber 클라이언트에서 구성하는 사용자 정책을 참조합니다. 최종 사용자는 다른 사용자를 차단 목록에 추가하여 다른 사용자가 승인 없이 프레즌스를 보지 못하게 하거나 해당 사용자를 허용 목록에 추가하여 해당 사용자가 프레즌스를 볼 수 있도록 권한을 부여할 수 있습니다. 이 설정은 시스템 기본 설정보다 우선합니다.

최종 사용자는 Cisco Jabber 클라이언트에서 다음을 구성할 수 있습니다.

- 차단 목록 - 사용자는 다른 사용자(로컬 및 외부 사용자 모두)를 차단 목록에 추가할 수 있습니다. 차단된 사용자의 사용자가 해당 사용자의 프레즌스를 보는 경우 사용자의 실제 상태와 상관없이 항상 사용자의 가용성 상태가 사용 불가능으로 표시됩니다. 사용자는 전체 페더레이션 도메인을 차단할 수도 있습니다.
- 허용 목록 - 사용자는 다른 로컬 및 외부 사용자가 항상 가용성을 볼 수 있도록 허용할 수 있습니다. 전체 외부(제휴) 도메인을 허용할 수도 있습니다.
- 기본 정책 - 사용자의 기본 정책 설정입니다. 모든 사용자를 차단하거나 허용하는 정책을 설정할 수 있습니다.

사용자 ID 및 디렉터리 URI 확인

단일 클러스터 구축의 경우 동일한 클러스터 내에 중복을 할당할 수 없기 때문에 중복 사용자 ID 및 디렉터리 URI는 문제가 되지 않습니다. 그러나 클러스터 간 구축을 사용하면 실수로 다른 클러스터의 다른 사용자에게 동일한 사용자 ID 또는 디렉터리 URI 값을 할당 할 수 있습니다.

IM and Presence 서비스는 다음과 같은 유효성 검사 도구를 제공하여 중복 사용자 ID 및 중복 디렉터리 URI를 확인합니다.

- IM and Presence 데이터 모니터 서비스 - 이 서비스로 진행 중인 시스템 검사를 구성할 수 있습니다. Cisco IM and Presence 데이터 모니터 서비스는 모든 IM and Presence 서비스 클러스터 간 노드의 Active Directory 항목에서 중복 사용자 ID 및 중복 또는 비어 있는 디렉터리 URI를 확인합니다. 관리자는 경보 또는 경고를 통해 알림을 받습니다. Cisco Unified 실시간 모니터링 도구를 사용하여 경보를 모니터링하고 중복 UserID 및 DuplicateDirectoryURI 오류에 대한 전자 메일 경고를 설정할 수 있습니다.

- 시스템 문제 해결 도구 - 중복 디렉터리 URI 및 사용자 ID를 포함하여 시스템 오류를 시스템에서 일시적으로 검사하려면 시스템 문제 해결 도구를 사용하십시오. 문제 해결 도구는 최대 10명의 사용자에 대한 세부 정보만을 제공합니다. 시스템 문제 해결 도구는 Cisco Unified CM IM and Presence 관리 인터페이스(진단 > 시스템 문제 해결 도구)에서 액세스할 수 있습니다.
- 명령줄 인터페이스 - 중복 URI 및 사용자 ID에 대한 완전하고 자세한 보고서를 얻으려면 `utils users validate all` CLI 명령을 실행하십시오.

최종 사용자 관리 작업 흐름

프로시저

	명령 또는 동작	목적
단계 **1**	프레즌스 인증 정책 할당, 307 페이지	프레즌스 가입 요청에 대한 시스템 권한 부여 정책을 할당합니다.
단계 **2**	사용자 데이터에 대한 데이터 모니터 검사 구성, 308 페이지	Cisco IM and Presence 데이터 모니터 서비스가 중복 디렉터리 URI 및 사용자 ID에 대한 예약 검사를 실행하도록 구성합니다. 문제가 발견되면 시스템 알람 또는 경고가 발생합니다.
단계 **3**	시스템 문제 해결 도구를 통해 사용자 데이터 유효성 검사, 310 페이지	중복 디렉터리 URI 및 사용자 ID를 포함하여 시스템 문제에 대한 임시 검사를 실행하려면 시스템 문제 해결 도구 실행.
단계 **4**	사용자 ID 및 디렉터리 URI 확인, 311 페이지	CLI 명령을 실행하여 중복 디렉터리 URI 및 사용자 ID에 대한 자세한 보고서를 가져옵니다.
단계 **5**	사용자의 프레즌스 설정 보기, 315 페이지	IM and Presence를 활성화한 최종 사용자의 프레즌스 설정을 보려면 프레즌스 뷰어를 사용하여 해당 설정을 볼 수 있습니다.

프레즌스 인증 정책 할당

프레즌스 가입 요청에 대한 시스템 권한 부여 정책을 할당합니다.

참고 Cisco Jabber 클라이언트에서 최종 사용자는 다른 사용자가 자신의 프레즌스를 볼 수 있는지 여부를 구성할 수 있습니다. 이 사용자 정책은 시스템 권한 부여 설정을 재정의합니다.

프로시저

단계 **1** **Cisco Unified CM IM and Presence** 관리에서 프레즌스 > 설정을 선택합니다.

단계 **2** 사용자에게 승인에 대한 메시지를 표시하지 않고 다른 사용자의 사용 가능성을 볼 수 있도록 허용 확인란을 선택하거나 선택을 취소합니다.

- 선택 - IM and Presence는 로컬 엔터프라이즈에서 수신된 모든 프레즌스 가입 요청을 자동으로 승인합니다.
- 선택 취소 - IM and Presence는 프레즌스가 요청된 클라이언트에 대한 모든 프레즌스 요청을 나타냅니다. 사용자는 요청을 수락 또는 거부할 수 있습니다.

참고 SIP 기반 클라이언트를 구축하는 경우 이 확인란을 선택해야 합니다. 확인란을 선택 취소하는 경우 구축은 XMPP 클라이언트만 지원합니다.

단계 **3** 저장을 클릭합니다.

단계 **4** Cisco XCP 라우터 서비스 다시 시작.

다음에 수행할 작업

계속 진행하여 IM and Presence 서비스에서 SIP 게시 트렁크를 구성합니다.

사용자 데이터에 대한 데이터 모니터 검사 구성

예약된 간격으로 디렉터리 URI 및 사용자 ID의 유효성을 검사하도록 Cisco IM and Presence 데이터 모니터를 구성하려면 다음 작업을 완료하십시오. 오류는 Cisco Unified 실시간 모니터링 도구에 경보 또는 경고를 통해 전달됩니다.

참고 중복 디렉터리 URI 및 중복 사용자 ID 오류는 클러스터 간 구축시에만 해당되는 문제입니다.

프로시저

	명령 또는 동작	목적
단계 **1**	사용자 ID 및 디렉터리 URI 유효성 검사를 위한 예약 설정, 309 페이지	Cisco IM and Presence 데이터 모니터 검사를 위해 예약된 간격을 구성합니다. 서비스는 중복 디렉터리 URI 및 사용자 ID를 포함하여 활성 디렉터리 항목에서 오류를 검사합니다.
단계 **2**	전자 메일 경고를 위한 전자 메일 서버 설정, 309 페이지	(선택 사항) 데이터 모니터 서비스가 중복 디렉터리 URI 또는 사용자 ID를 찾을 때마다 전자 메일 경고를 받으려면 실시간 모니터링 도구를 사용하여 전자 메일 서버를 설정해야 합니다.

	명령 또는 동작	목적
단계 3	이메일 알림 활성화, 310 페이지	(선택 사항) DuplicateDirectoryURI 및 DuplicateUserid 알람에 대한 전자 메일 경고를 활성화하려면이 절차를 완료하십시오. Cisco IM and Presence 데이터 모니터 서비스가 이러한 알람 중 하나를 반환하면 전자 메일이 관리자에게 전송됩니다.

사용자 ID 및 디렉터리 URI 유효성 검사를 위한 예약 설정

Cisco IM and Presence 데이터 모니터 서비스를 위해 예약된 간격을 설정합니다. 이 서비스는 중복 디렉터리 URI 및 사용자 ID를 포함하여 데이터 오류에 대해 예약된 간격으로 시스템을 검사합니다. 이 서비스는 오류가 발견될 때마다 실시간 모니터링 도구를 통해 볼 수 있는 경보 또는 경고를 발생시킵니다.

시작하기 전에

Cisco IM and Presence 데이터 모니터 네트워크 서비스가 실행 중이어야 합니다. 기본적으로 서비스는 실행 중입니다. Cisco Unified IM and Presence 서비스 인터페이스의 제어 센터 - 네트워크 서비스 창에서 서비스가 실행 중인지 확인할 수 있습니다.

프로시저

단계 1 **Cisco Unified CM IM and Presence** 관리에서 시스템 > 서비스 파라미터를 선택합니다.

단계 2 서비스 드롭다운에서 **Cisco IM and Presence** 데이터 모니터를 선택합니다.

단계 3 사용자 확인 간격 필드에 시간 간격을 분 단위로 입력합니다. 5 ~ 1440(분) 사이의 정수를 입력할 수 있습니다. 기본값은 30분입니다.

단계 4 저장을 클릭합니다.

다음에 수행할 작업

(선택 사항) DuplicateDirectoryURI 또는 DuplicateUserid 알람이 발생할 때마다 전자 메일 경고를 설정하려면, 전자 메일 경고를 위한 전자 메일 서버 설정, 309 페이지

전자 메일 경고를 위한 전자 메일 서버 설정

데이터 모니터 유효성 검사에서 중복 디렉터리 URI 및 사용자 ID 오류를 발견할 때마다 관리자가 전자 메일 경고를 수신하도록 하는 데 도움이 될 수 있습니다. 그렇다면이 선택적 절차를 사용하여 전자 메일 경고를 위한 전자 메일 서버를 설정합니다.

프로시저

단계 **1** 실시간 모니터링 도구의 시스템 창에서 중앙 알림을 클릭합니다.
단계 **2** 시스템 > 도구 > 알림 > 이메일 서버 구성을 선택합니다.
단계 **3** 메일 서버 구성 팝업에서 메일 서버에 대한 세부 정보를 입력합니다.
단계 **4** 확인을 클릭합니다.

다음에 수행할 작업

이메일 알림 활성화, 310 페이지

이메일 알림 활성화

DuplicateUserID 또는 DuplicateDirectoryURI 시스템 경고가 발생할 때마다 관리자에게 전자 메일을 보내도록 실시간 모니터링 도구를 설정하려면 이 절차를 사용하십시오.

시작하기 전에

전자 메일 경고를 위한 전자 메일 서버 설정, 309 페이지

프로시저

단계 **1** 실시간 모니터링 도구의 시스템 영역에서 중앙 알림을 클릭합니다.
단계 **2** **IM and Presence** 탭을 클릭합니다.
단계 **3** 전자 메일 알림을 추가하려는 경고를 클릭합니다. 예를 들어 **DuplicateDirecytoryURI** 또는 **DuplicateUserid** 시스템 경고입니다.
단계 **4** 도구 > 경고 > 구성 경고 작업을 선택합니다.
단계 **5** 알림 작업 팝업에서 기본값을 선택하고 편집을 클릭합니다.
단계 **6** 알림 작업 팝업에서 수신자를 추가합니다.
단계 **7** 팝업 창에 전자 메일 알림을 보낼 주소를 입력하고 확인을 클릭합니다.
단계 **8** 알림 작업 팝업에서 수신자 아래 주소가 나타나는지, 활성화 확인란이 선택되었는지 확인합니다.
단계 **9** 확인을 클릭합니다.
단계 **10** 전자 메일 경고를 사용하려는 각 시스템 경고에 대해 이 절차를 반복합니다.

시스템 문제 해결 도구를 통해 사용자 데이터 유효성 검사

Cisco Unified CM IM and Presence 관리 GUI의 시스템 문제 해결 도구를 사용하여 중복 사용자 ID 및 중복되거나 유효하지 않은 디렉터리 URI에 대한 구축을 확인하십시오. 문제 해결 도구는 구축의 모든 노드와 클러스터를 확인합니다.

프로시저

단계 1 **Cisco Unified CM IM and Presence** 관리에서 진단 > 시스템 문제 해결 도구를 선택합니다.

단계 2 사용자 문제 해결 도구 영역에서 사용자 ID 및 디렉터리 URI의 상태를 모니터링합니다. 시스템 점검 중 문제가 감지되면 문제 열이 채워집니다.

- 모든 사용자가 고유하게 구성된 사용자 ID를 가지고 있는지 확인합니다.
- 모든 사용자가 구성된 디렉터리 URI를 가지고 있는지 확인합니다.
- 모든 사용자가 고유하게 구성된 디렉터리 URI를 가지고 있는지 확인합니다.
- 모든 사용자가 유효하게 구성된 디렉터리 URI를 가지고 있는지 확인합니다.
- 모든 사용자가 고유하게 구성된 메일 ID를 가지고 있는지 확인합니다.

참고 중복 메일 ID는 페더레이션용 전자 메일 주소 및 Exchange 일정 통합 기능에 모두 영향을 미칩니다.

단계 3 문제가 나타나는 경우 사용자 설정을 설정할 수 있는 Cisco 통합 커뮤니케이션 매니저의 최종 사용자 설정 창으로 리디렉션되는 솔루션 열의 **fix** 링크를 클릭합니다.

참고 사용자 프로파일의 사용자 ID 및 디렉터리 URI 필드를 LDAP 디렉터리로 매핑할 수 있습니다. 이 경우 LDAP 디렉터리 서버에 수정을 적용하십시오.

다음에 수행할 작업

문제가 발생하면 Cisco Unified Communications Manager의 최종 사용자 구성 창에서 사용자 설정을 편집합니다. 사용자가 LDAP 디렉터리에서 동기화된 경우 LDAP 디렉터리에서 편집해야 합니다.

더 자세한 보고서가 필요한 경우 사용자 ID 및 디렉터리 URI 확인, 311 페이지.

사용자 ID 및 디렉터리 URI 확인

명령줄 인터페이스를 사용하여 중복 사용자 ID 및 중복 디렉터리 URI에 대한 구축을 자세히 검사하십시오.

프로시저

단계 1 명령줄 인터페이스에 로그인합니다.

단계 2 다음 명령 중 하나를 실행합니다.

- `utils users validate all` - 중복 사용자 ID와 중복 디렉터리 URI가 있는지 시스템을 확인합니다.
- `utils users validate userid` - 중복 사용자 ID가 있는지 시스템을 확인합니다.
- `utils users validate uri` - 중복 디렉터리 URI가 있는지 시스템을 확인합니다.

CLI는 중복 디렉터리 URI 및/또는 사용자 ID의 보고서를 반환합니다. 샘플 보고서는 다음을 참조하십시오. 사용자 ID 및 디렉터리 URI CLI 검증 예, 312 페이지

다음에 수행할 작업

문제가 발생하면 Cisco Unified Communications Manager의 최종 사용자 구성 창에서 사용자 설정을 편집합니다. 사용자가 LDAP 디렉터리에서 동기화된 경우 LDAP 디렉터리에서 편집해야 합니다.

사용자 ID 및 디렉터리 URI CLI 검증 예

중복 사용자 ID 및 중복(또는 잘못된) 디렉터리 URI를 가지고 있는 사용자 식별을 위해 IM and Presence 서비스 사용자를 검증하는 CLI 명령은 utils users validate { all | userid | uri }입니다.

디렉터리 URI는 각 사용자에 대해 고유해야 합니다. 대/소문자 구분과 관계 없이 여러 사용자에 대해 동일한 디렉터리 URI를 사용할 수 없습니다. 예를 들어,대/소문자를 구분하더라도 `aaa@bbb.ccc` 및 `AAA@BBB.CCC`와 같은 두 개의 서로 다른 디렉터리 URI를 사용할 수 없습니다.

CLI 사용 및 명령 설명에 대한 자세한 내용은 *Cisco Unified Communications Solutions*용 명령줄 인터페이스 설명서를 참조하십시오.

사용자 ID 오류를 보여주는 CLI 출력 예

```
Users with Duplicate User IDs
---------------------------------------------
 User ID: user3
  Node Name
  cucm-imp-1
  cucm-imp-2
```

디렉터리 URI 오류를 보여주는 CLI 출력 예

```
Users with No Directory URI Configured
-----------------------------------------------------
 Node Name: cucm-imp-2
 User ID
 user4

Users with Invalid Directory URI Configured
-----------------------------------------------------
 Node Name: cucm-imp-2
 User ID   Directory URI
 user1     asdf@ASDF@asdf@ADSF@cisco

Users with Duplicate Directory URIs
-----------------------------------------------------
Directory URI: user1@cisco.com
 Node Name   User ID
 cucm-imp-1  user4
 cucm-imp-2  user3
```

사용자 ID 및 디렉터리 URI 오류

Cisco IM and Presence 데이터 모니터 서비스는 모든 IM and Presence 서비스 클러스터 간 노드의 Active Directory 항목에서 중복 사용자 ID 및 빈/중복 디렉터리 URI를 확인합니다. 한 클러스터 내에서는 중복 사용자 ID 또는 디렉터리 URI가 있을 수 없습니다. 그러나 클러스터 간 구축에서는 의도하지 않게 서로 다른 클러스터의 사용자에게 동일한 사용자 ID 또는 디렉터리 URI 값을 할당할 수 있습니다.

다음 목록은 발견될 수있는 가능한 오류를 표시합니다. 실시간 모니터링 도구에서 이러한 오류를 볼 수 있으며, 이들 각각에 대해 경고 또는 경고가 발생합니다.

DuplicateDirectoryURI

이 알림은 디렉터리 URI IM 주소 체계를 구성할 때 클러스터 간 배포 내에서 사용자 여러 명에게 동일한 디렉터리 URI 값이 할당되었음을 나타냅니다.

DuplicateDirectoryURIWarning

이 경고는 `userID@Default_Domain` IM 주소 체계를 구성할 때 클러스터 간 구축 내에서 사용자 여러 명에게 동일한 디렉터리 URI 값이 할당되었음을 나타냅니다.

DuplicateUserid

이 경고는 클러스터 간 구축 내의 서로 다른 클러스터에서 한 명 이상의 사용자에게 중복 사용자 ID가 할당되었음을 나타냅니다.

InvalidDirectoryURI

이 경고는 디렉터리 URI IM 주소 체계를 구성할 때 클러스터 간 구축 내에서 한 명 이상의 사용자에게 빈/잘못된 디렉터리 URL 값이 할당되었음을 나타냅니다.

InvalidDirectoryURIWarning

이 경고는 `userID@Default_Domain` IM 주소 체계를 구성할 때 클러스터 간 구축 내에서 한 명 이상의 사용자에게 빈/잘못된 디렉터리 URL 값이 할당되었음을 나타냅니다.

어떤 사용자가 이러한 알람 상태에 있는지에 대한 특정 정보를 수집하려면 전체 목록을 표시하는 명령줄 인터페이스를 사용하십시오. 시스템 알람은 영향받는 사용자에 대한 상세정보를 제공하지 않으며, 시스템 문제 해결 도구는 최대 10명의 사용자에 대한 상세정보만 표시합니다. 알람을 일으키는 사용자에 대한 정보를 수집하려면 명령줄 인터페이스를 사용하여 사용자를 검증하십시오. 자세한 내용은 *Cisco Unified Communications Solutions*용 명령줄 인터페이스 설명서를 참조하십시오.

주의 영향받는 사용자의 통신 중단을 피할 수 있도록 중복 사용자 ID 및 중복(또는 잘못된) 디렉터리 URI 문제를 해결하려면 적절한 작업을 수행하십시오. 사용자 연락처 정보 수정에 대한 자세한 내용은 *Cisco Unified Communications Manager* 관리 설명서를 참조하십시오.

오류 및 제안 조치

다음 표에서는 클러스터 간 구축 시 시스템에서 중복 사용자 ID 및 중복(또는 잘못된) 디렉터리 URI를 확인할 때 발생할 수 있는 사용자 ID 및 디렉터리 URI 오류 조건에 대해 설명합니다. 발생하는 알람은 물론 오류 수정을 위한 제안 작업도 나열되어 있습니다.

표 33: 사용자 ID 및 디렉터리 URI 오류 조건 및 제안 조치

오류 조건	설명	제안 작업
중복 사용자 ID	클러스터 간 구축의 서로 다른 클러스터에서 한 명 이상의 사용자에게 중복 사용자 ID가 할당되었습니다. 영향을 받는 사용자는 클러스터 간 피어에 포함될 수 있습니다. 관련 알람: DuplicateUserid	DuplicateUserid 경고가 발생하면 즉시 작업을 수행하여 문제를 해결하십시오. 클러스터 간 구축 내 각 사용자에게는 고유한 사용자 ID가 필요합니다.
중복 디렉터리 URI	클러스터 간 구축 내 여러 사용자에게 동일한 디렉터리 URI 값이 할당되었습니다. 영향을 받는 사용자는 클러스터 간 피어에 포함될 수 있습니다. 관련 알람: • DuplicateDirectoryURI • DuplicateDirectoryURIWarning	시스템이 디렉터리 URI 메신저 주소 체계를 사용하도록 구성되어 있고 DuplicateDirectoryURI 경고가 발생하면 즉시 조치를 취하여 문제를 해결하십시오. 각 사용자에게 고유한 디렉터리 URI를 할당해야 합니다. 시스템이 *userID@Default_Domain* IM 주소 체계를 사용하도록 구성되어 있고 중복 디렉터리 URI가 감지되면 DuplicateDirectoryURIWarning 경고가 발생하고 즉각적인 조치가 필요하지 않습니다. 그러나 문제를 해결하는 것이 좋습니다.
잘못된 디렉터리 URI	구축 내 한 명 이상의 사용자에게 잘못된 또는 빈 디렉터리 URI 값이 할당되었습니다. *user@domain* 형식이 아닌 URI는 잘못된 디렉터리 URI입니다. 영향을 받는 사용자는 클러스터 간 피어에 포함될 수 있습니다. 관련 알람: • InvalidDirectoryURI • InvalidDirectoryURIWarning	시스템이 디렉터리 URI 메신저 주소 체계를 사용하도록 구성되어 있고 :InvalidDirectoryURI 경고가 발생하면 즉시 조치를 취하여 문제를 해결하십시오. 시스템이 *userID@Default_Domain* IM 주소 체계를 사용하도록 구성되어 있고 잘못된 디렉터리 URI가 감지되면 InvalidDirectoryURIWarning 경고가 발생하고 즉각적인 조치가 필요하지 않습니다. 그러나 문제를 해결하는 것이 좋습니다.

사용자의 프레즌스 설정 보기

프레즌스 뷰어를 사용하여 IM and Presence의 최종 사용자에 대한 프레즌스 설정 요약 보기를 가져옵니다. Presence 뷰어는 프레즌스 서버 할당, 연락처 및 감시자와 같은 정보를 제공합니다.

시작하기 전에

Cisco Unified 서비스 가용성에서 **Cisco AXL** 웹 서비스, **Cisco SIP Proxy** 서비스 및 **Cisco Presence** 엔진 서비스를 실행해야 합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 사용자 관리 > 최종 사용자를 선택합니다.

단계 **2** 찾기를 클릭하고 프레즌스 설정을 보려는 최종 사용자를 선택합니다.

단계 **3** 서비스 설정 아래에서 사용자에 대한 프레즌스 뷰어를 클릭하여 프레즌스 뷰어를 엽니다. 보기를 사용자 지정하려면 다음 표를 참조하십시오.

표 ***34:*** 최종 사용자 프레즌스 뷰어 필드

프레즌스 설정	설명
사용자 상태	다음을 포함하여 사용자의 사용 가능성 상태를 나타냅니다. • 사용 가능 • 자리 비움 • DND(Do Not Disturb) • 사용할 수 없음 • 사용자 정의
사용자 ID	선택된 사용자 ID를 나타냅니다. 해당 사용자의 사진을 사용할 수 있으면 사용자 사진이 표시됩니다. 제출을 클릭하여 다른 사용자 ID를 선택합니다.
보는 관점	사용자가 사용자 관점에서 사용 가능성 상태를 보도록 지정합니다. 이를 통해 지정된 사용자의 사용 가능성 상태가 다른 사용자(감시자)에게 표시되는 방법을 결정할 수 있습니다. 이 기능은 디버깅 시나리오에서 유용합니다(예: 사용자가 프라이버시 정책을 구성한 경우). 최대 128자가 허용됩니다.

프레즌스 설정	설명
연락처	이 사용자에 대한 연락처 목록에 있는 연락처 수를 표시합니다. 연락처 및 감시자 목록 영역의 연락처 제목 옆에 있는 화살표를 클릭하여 특정 사용자 연락처의 사용 가능성 상태를 확인합니다. 그룹 이름 옆에 있는 화살표를 클릭하여 해당 그룹 내에서 연락처 목록을 확장합니다. 그룹에 포함되지 않은 연락처(그룹 없는 연락처)는 연락처 그룹 목록 아래에 표시됩니다. 한 연락처가 여러 그룹에 속할 수 있지만 해당 사용자의 연락처 목록 크기에 대해 한 번만 계산됩니다. 최종 사용자에 대해 구성된 최대 연락처 수를 초과하면 경고 메시지가 나타납니다. IM and Presence 서비스 구성 및 최대 연락처 설정에 대한 자세한 내용은 *IM and Presence* 관리 온라인 도움말을 참조하십시오.
감시자	연락처 목록에서 이 사용자의 사용 가능성 상태를 확인하려고 가입한 감시자라는 사용자 목록을 표시합니다. 연락처 및 감시자 목록 영역의 감시자 제목 옆에 있는 화살표를 클릭하여 특정 감시자의 사용 가능성 상태를 확인합니다. 그룹 이름 옆에 있는 화살표를 클릭하여 해당 그룹 내에서 감시자 목록을 확장합니다. 한 감시자가 여러 그룹에 속할 수 있지만 해당 사용자의 감시자 목록 크기에 대해 한 번만 계산됩니다. 최종 사용자에 대해 구성된 최대 감시자 수를 초과하면 경고 메시지가 나타납니다. IM and Presence 서비스 구성 및 최대 감시자 설정에 대한 자세한 내용은 *IM and Presence* 관리 온라인 도움말을 참조하십시오.
프레즌스 서버 할당	사용자가 할당될 IM and Presence 서비스 서버를 나타냅니다. 하이퍼링크를 통해 세부 정보에 대한 서버 구성 페이지로 직접 이동할 수 있습니다.
액세스가능한프레즌스 아이콘 활성화	이 최종 사용자에 대해 프레즌스 액세스 가능성 아이콘을 활성화하려면 이 확인란을 선택합니다.
전송	프레즌스 뷰어를 실행하려면 선택합니다. 유용한 프레즌스 정보를 사용할 수 있게 하려면 IM and Presence 노드에 사용자를 할당해야 합니다. 이 작업이 작동하려면 AXL, 프레즌스 엔진 및 프록시 서비스는 모두 IM and Presence 서버에서 실행되어야 합니다.

프레즌스 권한 부여 상호 작용 및 제한 사항

기능	제한 사항
자동 프레즌스 인증 해제	프레즌스 요청의 자동 권한 부여를 해제하는 경우 IM and Presence 서비스는 다른 사용자의 연락처 목록에 있는 사용자의 가입 요청을 자동으로 승인합니다. 이는 동일한 도메인의 사용자는 물론 다른 도메인의 사용자(제휴 사용자)에게도 적용됩니다. 예: • 사용자 A는 사용자 B의 가용성 상태를 보기 위해 가입합니다. IM and Presence 서비스에서는 자동 승인이 해제되어 있으며 사용자 A의 허용 또는 차단 목록에 사용자 B가 없습니다. • IM and Presence 서비스는 사용자 B의 클라이언트 애플리케이션에 프레즌스 가입 요청을 전송하며, 클라이언트 애플리케이션은 사용자 B에게 가입을 허가하거나 거절할 프롬프트를 표시합니다. • 사용자 B가 프레즌스 가입 요청을 허가하면 사용자 B가 사용자 A의 연락처 목록에 추가됩니다. • 사용자 A는 프레즌스 가입의 인증을 요청하는 프롬프트 없이 사용자 B의 연락처 목록에 자동으로 추가됩니다. 이는 사용자 B에 대한 정책이 외부 도메인을 차단하거나 사용자 B가 사용자 프로파일에 "ask me"를 구성한 경우에도 발생합니다.
도메인 간 페더레이션 - 외부 도메인에서 수신한 프레즌스 요청	IM and Presence 는 현재 상태가 요청된 사용자의 사용자 정책 설정에만 의존합니다. 사용자가 자신의 사용자 정책에서 "ask me"를 선택하고 외부 연락처 또는 도메인에 대해 허용 또는 차단 목록을 추가하지 않은 경우 IM and Presence는 승인할 최종 사용자에게 프레즌스 요청을 보냅니다.

27 장

중앙 집중식 구축으로 사용자 마이그레이션

중앙 집중식 구축 사용자 마이그레이션 개요

이 장에는 기존의 IM and Presence 서비스 사용자를 표준 분산 IM and Presence 구축(Cisco Unified Communications Manager의 IM and Presence 서비스)에서 중앙 집중식 구축으로 마이그레이션하는 절차가 포함되어 있습니다. 중앙 집중식 구축에서는 IM and Presence 구축과 전화 통신 구축이 별도의 클러스터에 있습니다.

중앙 클러스터 마이그레이션을 위한 필수 작업

모든 사용자가 기존의 분산 클러스터에서 마이그레이션하는 새로운 IM and Presence 중앙 클러스터를 설정하는 경우 마이그레이션을 위해 클러스터를 설정하려면 다음과 같은 필수 조건 단계를 완료하십시오.

참고 마이그레이션에 포함되지 않은 새 사용자를 추가하는 경우 중앙 집중식 구축 구성, 107 페이지의 지침에 따라 새 사용자로 중앙 클러스터를 설정할 수 있습니다. 구성 작업이 확실한 경우에만 기존 사용자를 중앙 클러스터로 마이그레이션합니다.

표 ***35:*** 마이그레이션 전 작업

	마이그레이션 전 작업
1단계	새 중앙 클러스터를 마이그레이션 중인 클러스터에 연결합니다. **1.** IM and Presence 서비스 중앙 집중식 클러스터에서 데이터베이스 게시자 노드에 로그인합니다. **2.** Cisco Unified CM IM and Presence 관리에서 시스템 > 중앙 집중식 구축을 선택합니다. **3.** 찾기를 클릭하고 다음 중 하나를 수행합니다. • 기존 클러스터를 선택하고 선택 항목 수정을 클릭합니다. • 새로 추가를 클릭하여 마이그레이션 중인 클러스터를 추가합니다. **4.** 각 마이그레이션 중인 클러스터에 대해 다음 필드를 완료합니다. • 피어 주소 - 원격 전화 통신 게시자 노드의 FQDN, 호스트 이름, IPv4 주소 또는 IPv6 주소입니다. • **AXL** 사용자 이름 - 원격 전화 통신 클러스터에 있는 AXL 계정에 대한 로그인 사용자 이름입니다. • **AXL** 암호 - 원격 클러스터에 있는 AXL 계정에 대한 암호입니다. **5.** 저장을 클릭합니다.
2단계	새 중앙 클러스터가 IM and Presence 터클러스터 간 네트워크의 일부인 경우 중앙 클러스터와 마이그레이션의 일부가 아닌 IM and Presence 피어 클러스터 간에 인터클러스터 피어를 구성합니다. 다음 지침이 적용됩니다. • 중앙 클러스터와 마이그레이션 중인 클러스터 간에 인터클러스터 피어를 구성할 필요는 없습니다. 그러나 마이그레이션 중인 클러스터가 마이그레이션 시점에 여러 비 마이그레이션 클러스터와 함께 구성된 경우에는 마이그레이션 전에 중앙 클러스터에서 이러한 인터클러스터 피어 연결을 구성해야 합니다. 그렇지 않으면 마이그레이션이 작동하지 않습니다. • 인터클러스터 피어를 구성한 후 인터클러스터 피어 상태를 확인하여 구성이 적절하게 작동하는지 확인하십시오. 자세한 내용은 인터클러스터 피어 구성, 169 페이지를 참조하십시오.

중앙 클러스터로 마이그레이션 작업 흐름

분산된 클러스터(Cisco Unified Communications Manager의 IM and Presence 서비스)에서 중앙 집중식 IM and Presence 클러스터로 기존 사용자를 마이그레이션하려면 다음 작업을 완료하십시오. 이 작업 흐름에서:

- **IM and Presence** 중앙 클러스터는 사용자를 마이그레이션하는 클러스터를 말합니다. 마이그레이션 후 이 클러스터는 IM and Presence만 처리합니다.
- 마이그레이션 클러스터는 IM and Presence 사용자가 마이그레이션되는 클러스터를 나타냅니다. 마이그레이션 후 이 클러스터는 전화 통신만 처리합니다.

시작하기 전에

IM and Presence 중앙 클러스터가 새로 설치된 클러스터이고 아직 사용자가 없는 경우 사용자를 마이그레이션하기 전에 중앙 클러스터 마이그레이션을 위한 필수 작업, 319 페이지을 완료하십시오.

표 ***36:*** 중앙 클러스터로 마이그레이션 작업 흐름

	IM and Presence 중앙 클러스터	클러스터 마이그레이션	목적
1단계		마이그레이션 클러스터에서 연락처 목록 내보내기, 323 페이지	마이그레이션 클러스터의 사용자 연락처 목록을 csv 파일로 내보냅니다.
2단계		마이그레이션 클러스터에서 고가용성 비활성화, 324 페이지	마이그레이션 클러스터의 모든 프레즌스 이중화 그룹(하위 클러스터)에 대해 고가용성을 비활성화합니다.
3단계		IM and Presence에 대해 UC 서비스 구성, 325 페이지	마이그레이션 클러스터에서 IM and Presence 중앙 클러스터를 가리키는 IM and Presence UC 서비스를 구성합니다.
4단계		IM and Presence의 서비스 프로파일 만들기, 325 페이지	마이그레이션 클러스터에서 사용자가 설정한 IM and Presence UC 서비스를 사용하는 서비스 프로파일을 만듭니다.
5단계		전화 통신 클러스터에서 프레즌스 사용자 비활성화, 326 페이지	마이그레이션 클러스터에서 벌크 관리를 사용하여 사용자에 대한 IM and Presence를 비활성화합니다.

	IM and Presence 중앙 클러스터	클러스터 마이그레이션	목적
6단계		중앙 클러스터에 대한 OAuth 인증 활성화, 327 페이지	(선택 사항) 마이그레이션 클러스터에서 OAuth 새로 고침 로그인을 활성화합니다. 이렇게 하면 중앙 클러스터에서도 이 기능이 활성화됩니다.
7단계	중앙 클러스터에서 고가용성 비활성화, 327 페이지		IM and Presence 중앙 클러스터의 모든 프레즌스 중복 그룹(하위 클러스터)에서 고가용성을 비활성화합니다.
8단계	중앙 및 마이그레이션 중인 클러스터에 대한 피어 관계 삭제, 328 페이지		중앙 클러스터와 마이그레이션 중인 클러스터 사이에 인터클러스터 피어가 존재하는 경우 두 클러스터에서 피어 연결을 삭제합니다.
9단계	Cisco 클러스터 간 동기화 에이전트 중지, 329 페이지		IM and Presence 중앙 클러스터에서 Cisco 클러스터 간 동기화 에이전트를 중지합니다.
10단계	기능 그룹 템플릿을 통한 IM and Presence 활성화, 329 페이지		중앙 클러스터에서 IM and Presence 서비스를 활성화하는 기능 그룹 템플릿을 구성합니다.
11단계	중앙 클러스터에서 LDAP 동기화 완료, 330 페이지		기능 그룹 템플릿을 LDAP 디렉터리 동기화에 추가합니다. 동기화를 사용하여 마이그레이션 클러스터의 사용자를 추가합니다.
12단계	홈 클러스터로 연락처 목록 가져오기, 332 페이지		앞에서 생성한 벌크 관리 및 csv 내보내기 파일을 사용하여 연락처 목록을 중앙 클러스터로 가져옵니다.
13단계	Cisco 클러스터 간 동기화 에이전트 시작, 333 페이지		중앙 클러스터에서 Cisco 클러스터 간 동기화 에이전트를 시작합니다.
14단계	중앙 클러스터에서 고가용성 활성화, 333 페이지		중앙 클러스터의 모든 프레즌스 중복 그룹에서 고가용성을 활성화합니다.

	IM and Presence 중앙 클러스터	클러스터 마이그레이션	목적
15단계	마이그레이션 중인 클러스터에 대한 나머지 피어 삭제, 333 페이지		마이그레이션 중인 클러스터(현재 전화 통신 클러스터)와 기타 피어 클러스터 간의 나머지 인터클러스터 피어 연결을 삭제합니다.

마이그레이션 클러스터에서 연락처 목록 내보내기

분산 IM and Presence 구축에서 중앙 집중식 구축으로 마이그레이션하는 경우에만 이 절차를 사용하십시오. 마이그레이션 클러스터에서 사용자의 연락처 목록을 나중에 중앙 클러스터로 가져올 수있는 CSV 파일로 내보냅니다. 두 가지 유형의 연락처 목록을 내보낼 수 있습니다.

- 연락처 목록 -이 목록은 IM and Presence 연락처로 구성됩니다. IM 주소가 없는 연락처는 이 목록과 함께 내보내지 않습니다(비 프레즌스 연락처 목록을 내보내야 함).
- 비 프레즌스 연락처 목록 - 이 목록은 IM 주소가 없는 연락처로 구성됩니다.

프로시저

단계 **1** 이전 클러스터(전화 통신 클러스터)의 Cisco Unified CM IM and Presence 관리에 로그인합니다.

단계 **2** 내보내려는 연락처 목록의 유형에 따라 다음 옵션 중 하나를 선택합니다.

- 연락처 목록 내보내기의 경우 벌크 관리 > 연락처 목록 > 연락처 목록 내보내기를 선택합니다.
- 비 프레즌스 연락처 목록 내보내기의 경우 벌크 관리 > 비 프레즌스 연락처 목록 > 비 프레전스 연락처 목록 내보내기를 선택하고 다음 단계로 건너 뜁니다.

단계 **3** 연락처 목록만. 연락처 목록을 내보낼 사용자를 선택합니다.

a) 연락처 목록 내보내기 옵션에서 연락처 목록을 내보낼 사용자 범주를 선택합니다. 기본 옵션은 클러스터의 모든 사용자입니다.
b) 찾기를 클릭하여 사용자 목록을 표시한 후 다음을 클릭합니다.

단계 **4** 파일 이름을 입력합니다.

단계 **5** 작업 정보 아래에서 이 작업을 실행할 시기를 구성합니다.

- 즉시 실행 - 연락처 목록을 즉시 내보내면 이 버튼을 선택합니다.
- 나중에 실행 - 작업을 실행할 시간을 예약하려면 이 버튼을 선택합니다.

단계 **6** 제출을 클릭합니다.

참고 즉시 실행을 선택한 경우 내보내기 파일이 즉시 생성됩니다. 나중에 실행을 선택하는 경우 (벌크 관리 > 작업 스케줄러)에서 작업 스케줄러를 사용하여 이 작업을 실행할 시간을 예약해야 합니다.

단계 **7** 내보내기 파일이 생성된 후 csv 파일을 다운로드합니다.

a) 벌크 관리 > 파일 업로드/다운로드를 선택합니다.
b) 찾기를 클릭합니다.
c) 다운로드하려는 내보내기 파일을 선택하고 선택한 항목 다운로드를 클릭합니다.
d) 파일을 안전한 위치에 저장합니다.

단계 **8** 다른 csv 내보내기 파일을 생성하려면 이 절차를 반복합니다. 예를 들어 연락처 목록에 대한 내보내기 파일을 만드는 경우 비 프레즌스 연락처 목록에 대해 다른 파일을 만들 수 있습니다.

다음에 수행할 작업

마이그레이션 클러스터에서 고가용성 비활성화, 324 페이지

마이그레이션 클러스터에서 고가용성 비활성화

중앙 집중식 구축으로 마이그레이션하는 경우 마이그레이션하는 전화 통신 클러스터의 각 프레즌스 이중화 그룹(하위 클러스터)에서 고가용성을 비활성화합니다.

참고 프레즌스 이중화 그룹 세부 정보 페이지는 클러스터에서 고가용성을 비활성화한 경우에도 모든 활성 JSM 세션을 보여줍니다.

프로시저

단계 **1** 이전 클러스터의 Cisco Unified Communications Manager 게시자 노드에 로그인합니다.

단계 **2** Cisco Unified CM 관리에서 시스템 > 프레즌스 이중화 그룹을 선택합니다.

단계 **3** 찾기클릭하여 하위 클러스터를 선택합니다.

단계 **4** 고가용성 활성화 확인란을 선택 취소합니다.

단계 **5** 저장을 클릭합니다.

단계 **6** 각 하위 클러스터에 대해 이 절차를 반복합니다.

참고 모든 하위 클러스터에 대해 이 절차를 완료한 후 이 클러스터에서 추가 구성을 완료하기 전에 2분 이상 기다립니다.

다음에 수행할 작업

IM and Presence에 대해 UC 서비스 구성, 325 페이지

IM and Presence에 대해 UC 서비스 구성

원격 전화 통신 클러스터에서 이 절차를 사용하여 IM and Presence 서비스 중앙 클러스터를 가리키는 UC 서비스를 구성합니다. 전화 통신 클러스터의 사용자는 IM and Presence 중앙 클러스터에서 IM and Presence 서비스를 받게 됩니다.

프로시저

단계 **1** 전화 통신 클러스터의 Cisco Unified CM 관리 인터페이스에 로그인합니다.

단계 **2** 사용자 관리 > 사용자 설정 > **UC** 서비스를 선택합니다.

단계 **3** 다음 중 하나를 수행합니다.

a) 찾기를 클릭하고 편집할 기존 서비스를 선택합니다.

b) 새로 추가를 클릭하여 새 UC 서비스를 만듭니다.

단계 **4** **UC** 서비스 유형 드롭다운 목록에서 **IM and Presence**를 선택하고 다음을 클릭합니다.

단계 **5** 제품 유형 드롭다운 목록 상자에서 **IM and Presence** 서비스를 선택합니다.

단계 **6** 클러스터의 고유한 이름을 입력합니다. 호스트 이름일 필요는 없습니다.

단계 **7** 호스트 이름**/IP** 주소에서 IM and Presence 중앙 클러스터 데이터베이스 게시자 노드의 호스트 이름, IPv4 주소 또는 IPv6 주소를 입력합니다.

단계 **8** 저장을 클릭합니다.

단계 **9** 권장 사항. 호스트 이름**/IP** 주소 필드가 중앙 클러스터의 구독자 노드를 가리키는 두 번째 IM and Presence 서비스를 만들려면 이 절차를 반복하십시오.

다음에 수행할 작업

IM and Presence의 서비스 프로파일 만들기, 325 페이지

IM and Presence의 서비스 프로파일 만들기

원격 전화 통신 클러스터에서 이 절차를 사용하여 IM and Presence 중앙 클러스터를 가리키는 서비스 프로파일을 만듭니다. 전화 통신 클러스터의 사용자는 이 서비스 프로파일을 사용하여 중앙 클러스터에서 IM and Presence 서비스를 받게 됩니다.

프로시저

단계 **1** [Cisco Unified CM 관리]에서 사용자 관리 > 사용자 설정 > 서비스 프로파일을 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

a) 찾기를 클릭하고 편집할 기존 서비스 프로파일을 선택합니다.

b) 새로 추가를 클릭하여 새 서비스 프로파일을 만듭니다.

단계 **3** **IM and Presence** 프로파일 섹션에서 이전 작업에서 구성한 IM and Presence 서비스를 구성합니다.

a) 기본 드롭다운에서 데이터베이스 게시자 노드 서비스를 선택합니다.
b) 보조 드롭다운에서 가입자 노드 서비스를 선택합니다.

단계 **4** 저장을 클릭합니다.

다음에 수행할 작업

전화 통신 클러스터에서 프레즌스 사용자 비활성화, 326 페이지

전화 통신 클러스터에서 프레즌스 사용자 비활성화

전화 통신 구축에서 이미 LDAP 동기화를 완료한 경우 벌크 관리 도구를 사용하여 IM and Presence 사용자에 대한 전화 통신 클러스터의 사용자 설정을 편집합니다. 이 구성은 프레즌스 사용자가 IM and Presence 서비스의 중앙 집중식 클러스터를 가리 키도록 합니다.

참고 이 절차에서는 전화 통신 클러스터에서 LDAP 동기화를 이미 완료했다고 가정합니다. 그러나 아직 초기 LDAP 동기화를 완료하지 않은 경우 프레즌스 사용자의 중앙 구축 설정을 초기 동기화에 추가할 수 있습니다. 이 경우 전화 통신 클러스터에서 다음을 수행합니다.

- 방금 설정한 서비스 프로파일이 포함된 기능 그룹 템플릿을 구성합니다. 홈 클러스터 옵션을 선택하고 **Unified CM IM and Presence**에 대한 사용자 활성화 옵션을 선택 취소합니다.
- **LDAP** 디렉터리 구성에서 기능 그룹 템플릿을 LDAP 디렉터리 동기화에 추가합니다.
- 초기 동기화를 완료합니다.

기능 그룹 템플릿 및 LDAP 디렉터리 구성에 대한 자세한 내용은 *Cisco Unified Communications Manager* 시스템 구성 설명서의 "최종 사용자 구성" 부분을 참조하십시오.

프로시저

단계 **1** Cisco Unified CM 관리에서 쿼리 > 벌크 관리 > 사용자 > 사용자 업데이트 > 쿼리를 선택합니다.

단계 **2** 필터에서 홈 클러스터가 활성화됨을 선택하고 찾기를 클릭합니다. 이 창에는 자신의 홈 클러스터인 모든 최종 사용자가 표시됩니다.

단계 **3** 다음을 클릭합니다.
사용자 업데이트 구성 창에서 맨 왼쪽의 확인란은 이 쿼리로 이 설정을 편집할지 여부를 나타냅니다. 왼쪽 확인란을 선택하지 않으면 쿼리가 해당 필드를 업데이트하지 않습니다. 오른쪽 필드는 이 필드에 대한 새로운 설정을 나타냅니다. 두 확인란이 나타나는 경우 왼쪽의 확인란을 선택하여 필드를 업데이트하고 오른쪽 확인란에서 새 설정을 입력해야 합니다.

단계 **4** 서비스 설정에서 다음 각 필드의 맨 왼쪽 확인란을 선택하여 이러한 필드를 업데이트할 것을 나타낸 후 다음과 같이 인접한 설정을 편집합니다.

- 홈 클러스터 - 전화 통신 클러스터를 홈 클러스터로 사용하려면 오른쪽 확인란을 선택합니다.

- **Unified CM IM and Presence**에 대한 사용자 활성화 - 오른쪽 확인란을 선택하지 않습니다. 이 설정은 전화 통신 클러스터를 IM and Presence의 공급자로 사용하지 않도록 설정합니다.
- **UC** 서비스 프로파일 - 드롭다운에서 이전 작업에서 구성한 서비스 프로파일을 선택합니다. 이 설정은 IM and Presence 서비스의 공급자가 될 IM and Presence 중앙 클러스터를 사용자에게 알려줍니다.

참고 Expressway 모바일 및 원격 액세스 구성의 경우 https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-and-configuration-guides-list.html 에서 *Cisco Expressway*를 통한 모바일 및 원격 액세스 구축 설명서를 참조하십시오.

단계 **5** 나머지 필드를 완료합니다. 필드 및 해당 설정에 대한 도움이 필요한 경우 온라인 도움말을 참조하십시오.

단계 **6** 작업 정보 아래에서 즉시 실행을 선택합니다.

단계 **7** 제출을 클릭합니다.

다음에 수행할 작업

중앙 클러스터에 대한 OAuth 인증 활성화, 327 페이지

중앙 클러스터에 대한 **OAuth** 인증 활성화

전화 통신 클러스터에서 OAuth 인증을 활성화하려면 이 절차를 사용하십시오. 또한 IM and Presence 중앙 클러스터에서 OAuth 인증을 사용할 수 있습니다.

프로시저

단계 **1** 전화 통신 클러스터의 Cisco Unified CM 관리에 로그인합니다.

단계 **2** 시스템 > 엔터프라이즈 파라미터를 선택합니다.

단계 **3** **SSO** 및 **OAuth** 구성 아래에서 새로 고침 로그인을 사용한 **OAuth** 엔터프라이즈 파라미터를 활성화됨으로 설정합니다.

단계 **4** 파라미터 설정을 편집한 경우 저장을 클릭합니다.

중앙 클러스터에서 고가용성 비활성화

IM and Presence 중앙 클러스터의 각 프레즌스 이중화 그룹(하위 클러스터)에서 고가용성이 비활성화되었는지 확인하십시오. 구성을 적용하거나 사용자를 마이그레이션하기 전에 이 작업을 수행해야 합니다.

참고 프레즌스 이중화 그룹 세부 정보 페이지는 클러스터에서 고가용성을 비활성화한 경우에도 모든 활성 JSM 세션을 보여줍니다.

프로시저

단계 **1** 중앙 클러스터의 Cisco Unified CM 관리 인스턴스에 로그인합니다.
단계 **2** 시스템 > 프레즌스 이중화 그룹을 선택합니다.
단계 **3** 찾기를 클릭하여 기존 하위 클러스터를 선택합니다.
단계 **4** 고가용성 활성화 확인란을 선택 취소합니다.
단계 **5** 저장을 클릭합니다.
단계 **6** 각 하위 클러스터에 대해 이 단계를 반복합니다.

다음에 수행할 작업

Cisco 클러스터 간 동기화 에이전트 중지, 329 페이지

중앙 및 마이그레이션 중인 클러스터에 대한 피어 관계 삭제

IM and Presence 중앙 클러스터와 마이그레이션 중인 클러스터 사이에 인터클러스터 피어가 있는 경우 해당 피어 관계를 삭제합니다.

프로시저

단계 **1** IM and Presence 서비스 중앙 클러스터의 데이터베이스 퍼블리셔 노드에 로그인합니다.
단계 **2** Cisco Unified CM IM and Presence 관리에서 프레즌스 > 클러스터 간을 선택합니다.
단계 **3** 찾기클릭하여 마이그레이션 중인 클러스터를 선택합니다.
단계 **4** 삭제를 클릭합니다.
단계 **5** **Cisco XCP** 라우터를 다시 시작합니다.
a) Unified IM and Presence 서비스 가용성에 로그인하고 도구 > 제어 센터 - 네트워크 서비스를 선택합니다.
b) 서버 목록에서 데이터베이스 퍼블리셔 노드를 선택하고 이동을 클릭합니다.
c) **IM and Presence** 서비스 아래에서 **Cisco XCP** 라우터를 선택하고 다시 시작을 클릭합니다.
단계 **6** 마이그레이션 중인 클러스터에서 이 단계를 반복합니다.

Cisco 클러스터 간 동기화 에이전트 중지

IM and Presence 중앙 클러스터를 구성하기 전에 중앙 클러스터에서 **Cisco** 클러스터 간 동기화 에이전트 서비스가 중지되었는지 확인하십시오.

프로시저

단계 **1** Cisco Unified IM and Presence 서비스 가용성에서 도구 > 제어 센터 - 네트워크 서비스를 선택합니다.

단계 **2** 서버 드롭다운에서 중앙 클러스터 데이터베이스 게시자 노드를 선택하고 이동을 클릭합니다.

단계 **3** **Cisco** 클러스터 간 동기화 에이전트 서비스의 상태를 확인합니다. 서비스가 실행 중이거나 활성화된 경우 옆의 라디오 버튼을 선택하고 중지를 클릭합니다.

다음에 수행할 작업

기능 그룹 템플릿을 통한 IM and Presence 활성화, 329 페이지

기능 그룹 템플릿을 통한 IM and Presence 활성화

중앙 클러스터에 대한 IM and Presence 설정을 사용하여 기능 그룹 템플릿을 구성하려면 이 절차를 사용하십시오. 기능 그룹 템플릿을 LDAP 디렉터리 구성에 추가하여 동기화된 사용자에 대해 IM and Presence를 구성할 수 있습니다.

참고 초기 동기화가 아직 수행되지 않은 LDAP 디렉터리 구성에만 기능 그룹 템플릿을 적용할 수 있습니다. 중앙 클러스터에서 LDAP 구성을 동기화하면 Cisco Unified Communications Manager의 LDAP 구성에 편집을 적용할 수 없습니다. 이미 디렉터리를 동기화한 경우 벌크 관리를 사용하여 사용자에 대한 IM and Presence를 구성해야 합니다. 자세한 내용은 벌크 관리자를 통해 IM and Presence에 대해 사용자 활성화, 116 페이지를 참조하십시오.

프로시저

단계 **1** IM and Presence 중앙 집중식 클러스터의 Cisco Unified CM 관리 인터페이스에 로그인합니다. 이 서버에는 전화 통신이 구성되어 있지 않아야 합니다.

단계 **2** 사용자 관리 > 사용자 전화기/추가 > 기능 그룹 템플릿을 선택합니다.

단계 **3** 다음 중 하나를 수행합니다.

- 찾기를 클릭하고 기존 템플릿을 선택합니다.
- 새로 추가를 클릭하여 새 템플릿을 만듭니다.

단계 **4** 다음 두 확인란을 모두 선택합니다.

- 홈 클러스터

- **Unified CM IM and Presence**에 대한 사용자 활성화

단계 **5** 기능 그룹 템플릿 구성 창에서 나머지 필드를 완성합니다. 필드 및 해당 설정에 대한 도움이 필요한 경우 온라인 도움말을 참조하십시오.

단계 **6** 저장을 클릭합니다.

다음에 수행할 작업

설정을 사용자에게 전파하려면 초기 동기화가 아직 수행되지 않은 LDAP 디렉터리 구성에 기능 그룹 템플릿을 추가한 다음 초기 동기화를 완료해야 합니다.

중앙 클러스터에서 LDAP 동기화 완료, 330 페이지

중앙 클러스터에서 **LDAP** 동기화 완료

원격 Cisco Unified Communications Manager 전화 통신 클러스터에서 이 절차를 사용하여 LDAP 동기화를 사용하여 Cisco Unified Communications Manager 구축에 중앙 집중식 IM and Presence 설정을 구축합니다.

참고 LDAP 디렉터리 동기화를 설정하는 방법에 대한 추가 정보는 *Cisco Unified Communications Manager* 시스템 구성 설명서의 "최종 사용자 구성" 부분을 참조하십시오.

프로시저

단계 **1** Cisco Unified CM 관리에서 시스템 > **LDAP** > **LDAP** 디렉터리를 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 찾기를 클릭하고 기존 LDAP 디렉터리 동기화를 선택합니다.
- 새로 추가를 클릭하여 새 LDAP 디렉터리 동기화를 만듭니다.

단계 **3** 기능 그룹 템플릿 드롭 다운 목록 상자에서 이전 작업에서 만든 기능 그룹 템플릿을 선택합니다. 이 템플릿에서 IM and Presence를 비활성화해야 합니다.

단계 **4** **LDAP** 디렉터리 창에서 나머지 필드를 완료합니다. 필드 및 해당 설정에 대한 도움이 필요한 경우 온라인 도움말을 참조하십시오.

단계 **5** 저장을 클릭합니다.

단계 **6** 전체 동기화 수행을 클릭합니다.
Cisco Unified Communications Manager는 데이터베이스를 LDAP 디렉터리와 동기화하고 업데이트된 IM and Presence 설정을 할당합니다.

다음에 수행할 작업

홈 클러스터로 연락처 목록 가져오기, 332 페이지

벌크 관리자를 통해 IM and Presence에 대해 사용자 활성화

사용자를 이미 중앙 클러스터에 동기화하고 해당 사용자가 IM and Presence 서비스를 활성화하지 않은 경우 벌크 관리의 사용자 업데이트 기능을 사용하여 IM and Presence 서비스에 대해 해당 사용자를 활성화합니다.

참고 또한 벌크 관리의 사용자 가져오기 또는 사용자 삽입 기능을 사용하여 CSV 파일을 통해 새 사용자를 가져올 수 있습니다. 절차는 *Cisco Unified Communications Manager* 벌크 관리 설명서를 참조하십시오. 가져온 사용자에게 아래 옵션이 선택되어 있는지 확인합니다.

- 홈 클러스터
- Unified CM IM and Presence에 대한 사용자 활성화

프로시저

단계 **1** Cisco Unified CM 관리에서 벌크 관리 > 사용자 > 사용자 업데이트 > 쿼리를 선택합니다.

단계 **2** 필터에서 홈 클러스터가 활성화됨을 선택하고 찾기를 클릭합니다. 이 창에는 자신의 홈 클러스터인 모든 최종 사용자가 표시됩니다.

단계 **3** 다음을 클릭합니다.
사용자 업데이트 구성 창에서 맨 왼쪽의 확인란은 이 쿼리로 이 설정을 편집할지 여부를 나타냅니다. 왼쪽 확인란을 선택하지 않으면 쿼리가 해당 필드를 업데이트하지 않습니다. 오른쪽 필드는 이 필드에 대한 새로운 설정을 나타냅니다. 두 확인란이 나타나는 경우 왼쪽의 확인란을 선택하여 필드를 업데이트하고 오른쪽 확인란에서 새 설정을 입력해야 합니다.

단계 **4** 서비스 설정에서 다음 각 필드의 왼쪽 확인란을 선택하여 이러한 필드를 업데이트할 것을 나타낸 후 다음과 같이 인접한 설정을 편집합니다.

- 홈 클러스터 - 이 클러스터를 홈 클러스터로 사용하려면 오른쪽 확인란을 선택합니다.
- **Unified CM IM and Presence**에 대한 사용자 활성화 - 오른쪽 확인란을 선택합니다. 이 설정을 사용하면 중앙 클러스터를 이러한 사용자의 IM and Presence 서비스 공급자로 사용할 수 있습니다.

단계 **5** 업데이트하려는 나머지 필드를 완성합니다. 필드 및 해당 설정에 대한 도움이 필요한 경우 온라인 도움말을 참조하십시오.

단계 **6** 작업 정보 아래에서 즉시 실행을 선택합니다.

단계 **7** 제출을 클릭합니다.

홈 클러스터로 연락처 목록 가져오기

사용자를 IM and Presence 중앙 클러스터로 마이그레이션한 경우 이 절차를 사용하여 사용자의 연락처 목록을 IM and Presence 중앙 클러스터로 가져올 수 있습니다. 다음 유형의 연락처 목록 중 하나를 가져올 수 있습니다.

- 연락처 목록 - 이 목록에는 IM and Presence 연락처가 포함됩니다.
- 비 프레즌스 연락처 목록 - 이 목록에는 IM 주소가 없는 연락처가 포함됩니다.

시작하기 전에

이전 클러스터(전화 통신 클러스터)에서 내보낸 연락처 목록 csv 파일이 필요합니다.

프로시저

단계 **1** IM and Presence 중앙 클러스터에서 Cisco Unified CM IM and Presence 관리에 로그인합니다.

단계 **2** 전화 통신 클러스터에서 내보낸 csv 파일을 업로드합니다.

a) 벌크 관리 > 파일 업로드/다운로드를 선택합니다.
b) 새로 추가를 클릭합니다.
c) 파일 선택을 클릭하여 가져올 csv 파일을 선택합니다.
d) 대상 선택 드롭다운에서 가져올 연락처 목록 유형에 따라 연락처 목록 또는 비 프레즌스 연락처 목록 중 하나를 선택합니다.
e) 트랜잭션 유형 선택에서 가져오기 작업을 선택합니다.
f) 저장을 클릭합니다.

단계 **3** csv 정보를 중앙 클러스터로 가져옵니다.

a) Cisco Unified CM IM and Presence 관리에서 다음 중 하나를 수행합니다.
   - 연락처 목록 가져오기의 경우 벌크 관리 > 연락처 목록 > 연락처 목록 업데이트를 선택합니다.
   - 비 프레즌스 연락처 목록 가져오기의 경우 벌크 관리 > 비 프레즌스 연락처 목록 > 비 프레전스 연락처 목록 가져오기를 선택합니다.

b) 파일 이름 드롭다운에서 업로드한 csv 파일을 선택합니다.
c) 작업 정보 아래에서 작업이 실행하려는 시기에 따라 즉시 실행 또는 나중에 실행 중 하나를 선택합니다.
d) 제출을 클릭합니다. 즉시 실행을 선택한 경우 연락처 목록을 즉시 가져옵니다

   참고 . 나중에 실행을 선택하는 경우 벌크 관리 > 작업 스케줄러로 이동하여 실행할 작업 일정을 선택할 수 있습니다.

단계 **4** 가져올 두 번째 csv 파일이 있는 경우 이 절차를 반복합니다.

다음에 수행할 작업

Cisco 클러스터 간 동기화 에이전트 시작, 333 페이지

Cisco 클러스터 간 동기화 에이전트 시작

구성 또는 마이그레이션이 완료되면 IM and Presence 중앙 클러스터에서 **Cisco** 클러스터 간 동기화 에이전트를 시작합니다. 이 서비스는 인터클러스터 피어링을 사용하는 경우 필요합니다.

프로시저

단계 **1** Cisco Unified IM and Presence 서비스 가용성에서 도구 > 제어 센터 - 네트워크 서비스를 선택합니다.

단계 **2** 서버 드롭다운에서 IM and Presence 데이터베이스 게시자 노드를 선택하고 이동을 클릭합니다.

단계 **3** **IM and Presence** 서비스 아래에서 **Cisco** 클러스터 간 동기화 에이전트를 선택하고 시작을 클릭합니다.

다음에 수행할 작업

중앙 클러스터에서 고가용성 활성화, 333 페이지

중앙 클러스터에서 고가용성 활성화

구성 또는 사용자 마이그레이션이 완료되면 IM and Presence 중앙 클러스터의 프레즌스 이중화 그룹(하위 클러스터)에서 고가용성을 활성화합니다.

프로시저

단계 **1** IM and Presence 중앙 클러스터에서 Cisco Unified CM 관리 인스턴스에 로그인합니다.

단계 **2** 시스템 > 프레즌스 이중화 그룹을 선택합니다.

단계 **3** 찾기를 클릭하여 기존 하위 클러스터를 선택합니다.

단계 **4** 고가용성 활성화 확인란을 선택합니다.

단계 **5** 저장을 클릭합니다.

단계 **6** IM and Presence 중앙 클러스터의 각 하위 클러스터에 대해 이 절차를 반복합니다.

마이그레이션 중인 클러스터에 대한 나머지 피어 삭제

마이그레이션 중인 클러스터(현재 전화 통신 클러스터)와 나머지 IM and Presence 서비스 피어 클러스터 간의 인터클러스터 피어 관계를 삭제합니다.

참고 클러스터 간 연결 제거는 전체 메시의 Cisco XCP 라우터 재시작 가능 여부에 따라 나중에 연기될 수 있습니다. 전화 통신 클러스터와 피어 클러스터 수 간에 기존 클러스터 간 연결이 있는 한, 현재 실행 중인 Cisco XCP 라우터 서비스를 전화 통신 클러스터에서 실행 중 상태로 유지해야 합니다.

프로시저

단계 **1** 마이그레이션 중인 클러스터의 IM and Presence 데이터베이스 퍼블리셔 노드에 로그인합니다.

단계 **2** Cisco Unified CM IM and Presence 관리에서 프레즌스 > 클러스터 간을 선택합니다.

단계 **3** 찾기클릭하여 피어 클러스터를 선택합니다.

단계 **4** 삭제를 클릭합니다.

단계 **5** **Cisco XCP** 라우터를 다시 시작합니다.

a) Unified IM and Presence 서비스 가용성에 로그인하고 도구 > 제어 센터 - 네트워크 서비스를 선택합니다.
b) 서버 목록에서 데이터베이스 퍼블리셔 노드를 선택하고 이동을 클릭합니다.
c) **IM and Presence** 서비스 아래에서 **Cisco XCP** 라우터를 선택하고 다시 시작을 클릭합니다.

단계 **6** IM and Presence 서비스 피어 클러스터에서 이 단계를 반복합니다.

참고 마이그레이션 중인 클러스터가 여러 클러스터에 대한 인터클러스터 피어 연결을 가지고 있는 경우 클러스터 간 네트워크에 유지되는 각 피어 클러스터에 대해 이 절차를 반복해야 합니다. 즉, 마이그레이션 중인 클러스터에서는 끊어진 피어 클러스터 연결이 있으므로 끊긴 횟수만큼 **Cisco XCP** 라우터가 다시 시작됩니다.

28 장

사용자 마이그레이션

사용자 마이그레이션 개요

이 섹션에서는 IM and Presence 서비스 클러스터 간 사용자 마이그레이션 방법에 대해 설명합니다.

사용자 마이그레이션 필수 조건

- 현재 클러스터와 대상 클러스터 모두의 전체 백업을 실행합니다. 자세한 내용은 백업 작업 흐름, 370 페이지를 참조하십시오.
- 마이그레이션할 사용자에게 현재 홈 클러스터에만 IM and Presence 서비스 또는 Cisco Jabber에 대한 라이센스가 있는지 확인하십시오. 이러한 사용자가 사전 마이그레이션 클러스터 이외의 클러스터에서 라이센스를 얻은 경우 마이그레이션 작업을 진행하기 전에 라이센스를 완전히 해제해야 합니다.

사용자 마이그레이션 작업 흐름

이 작업을 완료하여 IM and Presence 사용자를 새 클러스터로 마이그레이션합니다.

프로시저

	명령 또는 동작	목적
단계 **1**	부실 항목 제거, 336 페이지	사용자를 마이그레이션하기 전에 모든 부실 등록 명부, 그룹 항목 및 비 프레즌스 계약 레코드를 제거합니다.

	명령 또는 동작	목적
단계 **2**	마이그레이션을 위한 필수 서비스 시작, 338 페이지	마이그레이션하기 전에 다음 서비스가 실행 중인지 확인하십시오. • Cisco AXL 웹 서비스 • Cisco Sync Agent • Cisco 클러스터 간 동기화 에이전트
단계 **3**	클러스터 간 동기화 오류 확인, 338 페이지	시스템 문제 해결 도구를 실행하고 클러스터 간 동기화 문제가 없는지 확인합니다.
단계 **4**	마이그레이션을 위해 표준 프레즌스 구성, 338 페이지	사용자를 마이그레이션하기 전에 이러한 표준 프레즌스 설정을 구성합니다.
단계 **5**	사용자 연락처 목록 내보내기, 339 페이지	현재 클러스터에서 마이그레이션 사용자의 연락처 목록을 내보내려면 다음 절차를 완료하십시오.
단계 **6**	다음과 같은 간단한 작업 흐름 중 하나를 완료하여 사용자를 새 클러스터로 이동합니다. • LDAP 통해 사용자 마이그레이션, 340 페이지 • 사용자를 새 클러스터로 수동으로 이동, 342 페이지 • 벌크 관리를 통해 사용자 마이그레이션, 344 페이지	사용자를 새 클러스터로 이동합니다. LDAP를 사용하여 새 클러스터에서 사용자를 프로비저닝하거나, 사용자를 수동으로 이동하거나, 벌크 관리를 사용하여 사용자를 새 클러스터로 마이그레이션할 수 있습니다.
단계 **7**	홈 클러스터에서 연락처 목록 가져오기, 348 페이지	사용자를 새 클러스터로 마이그레이션한 후 연락처 목록을 가져와서 마이그레이션된 사용자의 연락처 데이터를 복원합니다.
단계 **8**	기존 클러스터에서 사용자 업데이트, 349 페이지	새 클러스터에서 모든 것이 정상적으로 작동할 때까지 이전 클러스터에서 사용자를 제거하지 않을 수 있습니다. 벌크 관리의 사용자 업데이트 기능을 사용하여 이전 클러스터에서 IM and Presence 기능을 제거하려면 이 절차를 사용하십시오.

부실 항목 제거

사용자를 마이그레이션하기 전에 부실 등록 명부, 그룹 항목 및 비 프레즌스 연락처 레코드를 제거합니다. 이 작업은 사용자 프레즌스가 비활성 상태였던 게시자 IM&P 노드에서 수행해야 합니다.

참고 2000개 배치에서는 필요에 따라 이 단계들을 반복합니다. CLI를 통해 많은 양의 부실 항목을 제거하는 데 시간이 너무 많이 소요되는 경우에는 TAC 케이스를 열어 이 섹션의 끝 부분에 있는 루트 액세스를 필요로 하는 부실 등록 명부 스크립트를 활용하십시오.

프로시저

단계 **1** CLI 세션을 시작합니다. CLI 세션을 시작하는 방법에 대한 자세한 내용은 *Cisco Unified Communications* 솔루션용 명령줄 인터페이스 참조 설명서의 "CLI 세션 시작" 섹션을 참조하십시오.

단계 **2** 부실 등록 명부 항목을 확인하고 제거합니다. 이렇게 하려면 다음 쿼리를 실행합니다.

a) 부실 등록 명부 항목을 확인합니다.

```
run sql select count(*) from rosters where user_id in (select xcp_user_id from enduser
where primarynodeid is NULL)
```

b) 부실 등록 명부 항목을 제거합니다.

```
run sql delete from rosters where pkid in (select * from (select first 2000 pkid from
rosters where user_id in (select xcp_user_id from enduser where primarynodeid is NULL)))
```

단계 **3** 부실 그룹 레코드를 확인하고 제거합니다. 이렇게 하려면 다음 쿼리를 실행합니다.

a) 부실 그룹 레코드를 확인합니다.

```
run sql select count(*) from groups where user_id in (select xcp_user_id from enduser
where primarynodeid is NULL)
```

b) 부실 그룹 레코드를 제거합니다.

```
run sql delete from groups where pkid in (select * from (select first 2000 pkid from
groups where user_id in (select xcp_user_id from enduser where primarynodeid is NULL)))
```

단계 **4** 부실 비 연락처 레코드를 확인하고 제거합니다(순서대로). 이렇게 하려면 다음 쿼리를 실행합니다.

a) 부실 비 연락처 레코드를 확인합니다(순서대로).

```
run sql select count(*) from nonpresencecontacts where fkenduser in (select pkid from
enduser where primarynodeid is null)
```

b) 부실 비 연락처 레코드를 제거합니다(순서대로).

```
run sql delete from nonpresencecontacts where pkid in (select * from (select first 2000
 pkid from nonpresencecontacts where fkenduser in (select pkid from enduser where
primarynodeid is null)))
```

c) 루트 액세스 권한이 있는 경우 다음 쿼리를 사용합니다.

```
run sql delete from epascontactaddinfo where pkid in (select * from (select first 2000
pkid from epascontactaddinfo where pkid not in (select fkepascontactaddinfo from
nonpresencecontacts)))
```

마이그레이션을 위해 표준 프레즌스 구성

사용자를 마이그레이션하기 전에 이러한 프레즌스 설정을 구성합니다.

프로시저

단계 **1** Cisco Unified CM IM and Presence 관리에서 프레즌스 > 설정 > 표준 구성을 선택합니다.

단계 **2** 사용자에게 승인에 대한 메시지를 표시하지 않고 다른 사용자의 사용 가능성을 볼 수 있도록 허용 확인란을 선택합니다.

단계 **3** 최대 연락처 목록 크기(사용자별) 설정의 경우 제한 없음 확인란을 선택합니다.

단계 **4** 최대 관찰자 수(사용자당) 설정의 경우 제한 없음 확인란을 선택합니다.

단계 **5** 저장을 클릭합니다.

다음에 수행할 작업

클러스터 간 동기화 오류 확인, 338 페이지

클러스터 간 동기화 오류 확인

마이그레이션하기 전에 클러스터 간 동기화 오류가 없는지 확인합니다.

프로시저

단계 **1** Cisco Unified CM IM and Presence 관리에서 진단 > 시스템 문제 해결 도구를 선택합니다.

단계 **2** 클러스터 간 동기화 오류가 없는지 확인합니다. 오류가 있는 경우 계속하기 전에 오류를 수정합니다.

다음에 수행할 작업

마이그레이션을 위한 필수 서비스 시작, 338 페이지

마이그레이션을 위한 필수 서비스 시작

Cisco Unified IM and Presence 서비스 가용성에서 다음과 같은 마이그레이션을 위한 필수 서비스가 실행 중인지 확인합니다.

- Cisco AXL 웹 서비스
- Cisco Sync Agent
- Cisco 클러스터 간 동기화 에이전트

프로시저

단계 **1** Cisco Unified IM and Presence 서비스 가용성에서 도구 > 제어 센터 - 기능 서비스를 선택합니다.

단계 **2** 서버 드롭다운에서 IM and Presence 노드를 선택하고 이동을 클릭합니다.

단계 **3** 데이터베이스 및 관리 서비스에서 **Cisco AXL** 웹 서비스가 시작되었는지 확인합니다. 서비스가 실행 중이 아니면(기본 설정이 실행되고 있지 않음) 서비스를 선택하고 시작을 클릭합니다.

단계 **4** 도구제어 센터 > - 네트워크 서비스를 선택합니다.

단계 **5** 서버 드롭다운에서 IM and Presence 노드를 선택하고 이동을 클릭합니다.

단계 **6** **IM and Presence** 서비스에서 **Cisco** 동기화 에이전트 및 **Cisco** 클러스터 간 동기화 에이전트 서비스가 모두 실행되고 있는지 확인합니다. 실행되지 않고 있는 경우 시작하십시오.

다음에 수행할 작업

사용자 연락처 목록 내보내기, 339 페이지

사용자 연락처 목록 내보내기

현재 클러스터에서 마이그레이션 사용자의 연락처 목록을 내보내려면 다음 절차를 완료하십시오.

프로시저

단계 **1** 현재의 홈 클러스터에서 마이그레이션 사용자의 연락처 목록을 내보냅니다.

a) **Cisco Unified CM IM and Presence** 관리에서 벌크 관리 > 연락처 목록 > 내보내기를 선택합니다.
b) 클러스터의 모든 미할당 사용자를 선택하고 찾기를 클릭합니다.
c) 결과를 검토하고 필요에 따라 **AND/OR** 필터를 사용하여 검색 결과를 필터링합니다.
d) 목록이 완료되면 다음을 클릭합니다.
e) 내보낸 연락처 목록 데이터의 파일 이름을 선택합니다.
f) 선택적으로 작업 설명을 업데이트합니다.
g) 지금 실행을 클릭하거나, 나중에 실행하려면 작업을 예약합니다.

단계 **2** 연락처 목록 내보내기 작업의 상태를 모니터링합니다.

a) **Cisco Unified CM IM and Presence** 관리에서 벌크 관리 > 작업 스케줄러를 선택합니다.
b) 모든 BAT 작업을 나열하려면 찾기를 클릭합니다.
c) 연락처 목록 내보내기 작업을 찾아보고 완료된 것으로 보고되면 작업을 선택합니다.
d) 연락처 목록 내보내기 파일의 내용을 보려면 CSV 파일 이름 링크를 선택합니다. 파일 이름에 타임스탬프가 추가되었는지 확인합니다.
e) 작업 결과 섹션에서 로그 파일을 선택하여 업로드된 내용의 요약을 확인합니다. 로그 파일에는 작업의 시작 및 종료 시간과 결과 요약이 포함됩니다.

단계 **3** 사용자 마이그레이션이 완료될 때 사용할 수 있도록 연락처 목록 내보내기 파일을 다운로드하여 저장합니다.

a) **Cisco Unified CM IM and Presence** 관리에서 벌크 관리 > 파일 업로드/다운로드를 선택합니다.
b) 찾기를 클릭합니다.
c) 연락처 목록 내보내기 파일을 선택하고 선택한 항목 다운로드를 클릭합니다.
d) 절차의 뒷부분에 업로드할 수 있도록 CSV 파일을 로컬에 저장합니다.

다음에 수행할 작업

다음 작업 흐름 중 하나로 이동하여 새 클러스터에 사용자를 할당합니다.

- LDAP 통해 사용자 마이그레이션, 340 페이지
- 사용자를 새 클러스터로 수동으로 이동, 342 페이지

LDAP 통해 사용자 마이그레이션

사용자가 LDAP 디렉터리와 동기화되고 새 클러스터로 마이그레이션하려는 경우 이러한 작업을 완료하십시오.

참고 LDAP 디렉터리 구성을 새 클러스터에 추가해야 합니다. 여기에는 모든 서비스 프로파일, 사용자 프로파일 및 기능 그룹 템플릿이 포함됩니다. 기능 그룹 템플릿 구성에 **Unified CM IM and Presence**에 대한 사용자 활성화 확인란이 선택되어 있는지 확인합니다.

프로시저

	명령 또는 동작	목적
단계 **1**	외부 LDAP 디렉터리 업데이트, 341 페이지	구축에서 각 클러스터에 별도의 LDAP 구조를 사용하고 사용자가 홈 클러스터에만 동기화되는 경우 외부 LDAP 디렉터리를 업데이트해야 할 수도 있습니다.
단계 **2**	새 클러스터에서 LDAP 구성, 341 페이지	Cisco Unified Communications Manager에서 LDAP가 활성화된 경우 새 클러스터를 업데이트된 LDAP 디렉터리와 동기화하여 사용자를 새 클러스터로 가져옵니다.

다음에 수행할 작업

홈 클러스터에서 연락처 목록 가져오기, 348 페이지

외부 LDAP 디렉터리 업데이트

구축에서 각 클러스터에 별도의 LDAP 구조를 사용하고 사용자가 홈 클러스터에만 동기화되는 경우 외부 LDAP 디렉터리를 업데이트해야 할 수도 있습니다.

참고 모든 사용자가 모든 Cisco Unified Communications Manager 및 IM and Presence 서비스 클러스터(사용자가 하나의 클러스터만 사용하도록 허가됨)에 대해 동기화되는 평면 LDAP 구조의 구축에서는 사용자를 이동할 필요가 없습니다.

참고 이전 및 새 클러스터에서 LDAP 디렉터리 동기화를 구성한 방법에 따라 외부 LDAP 디렉터리에서 사용자를 이동하면 다음 동기화가 발생할 때 해당 사용자를 새 IM and Presence 서비스 클러스터로 자동으로 마이그레이션할 수 있습니다.

프로시저

단계 **1** 외부 LDAP 디렉터리에서 사용자 업데이트

단계 **2** 사용자를 이동한 후에는 이전 LDAP 클러스터에서 LDAP 항목을 삭제합니다.

다음에 수행할 작업

새 클러스터에서 LDAP 구성, 341 페이지

새 클러스터에서 LDAP 구성

시작하기 전에

새 클러스터에서 LDAP 디렉터리를 프로비저닝합니다. LDAP 디렉터리 동기화에 범용 회선 및 디바이스 템플릿과 기능 그룹 템플릿이 포함되어 있는 경우 새 클러스터에서 이 템플릿을 구성해야 합니다. 기능 그룹 템플릿에 다음 옵션이 선택되어 있는지 확인합니다.

- 홈 클러스터
- Unified CM IM and Presence에 대한 사용자 활성화

LDAP 디렉터리 동기화를 구성하는 방법에 대한 자세한 내용은 *Cisco Unified Communications Manager* 시스템 구성 설명서의 "최종 사용자 구성" 섹션을 참조하십시오.

프로시저

단계 **1** Cisco Unified CM 관리에서 시스템 > **LDAP** > **LDAP** 디렉터리를 선택합니다.

단계 **2** 찾기를 클릭하고 구성된 LDAP 디렉터리를 선택합니다.
단계 **3** 지금 전체 동기화 수행을 클릭합니다.

다음에 수행할 작업

홈 클러스터에서 연락처 목록 가져오기, 348 페이지

사용자를 새 클러스터로 수동으로 이동

사용자를 수동으로 새 클러스터로 이동하려면 이 작업을 완료하십시오.

참고 많은 사용자가 있는 경우 Cisco Unified Communications Manager의 벌크 관리 도구를 사용하여 csv 파일을 통해 많은 수의 사용자를 업데이트할 수 있습니다. 자세한 내용은 *Cisco Unified Communications Manager* 벌크 관리 설명서를 참조하십시오.

프로시저

	명령 또는 동작	목적
단계 **1**	사용자를 위해 IM and Presence 수동으로 비활성화, 342 페이지	현재 홈 클러스터에서 IM and Presence 서비스 및 Cisco Jabber에 대한 마이그레이션 사용자를 비활성화합니다.
단계 **2**	사용자 수동으로 가져오기, 343 페이지	새 클러스터에 LDAP 동기화가 구성되어 있지 않은 경우 사용자를 새 Cisco Unified Communications Manager 클러스터에 수동으로 프로비저닝합니다.
단계 **3**	새 클러스터에서 IM and Presence 서비스에 대해 사용자 활성화, 343 페이지	새로운 홈 클러스터에서 사용자가 동기화되었거나 수동으로 프로비저닝된 경우, IM and Presence 서비스 및 Cisco Jabber에 대해 사용자를 활성화해야 합니다.

다음에 수행할 작업

홈 클러스터에서 연락처 목록 가져오기, 348 페이지

사용자를 위해 **IM and Presence** 수동으로 비활성화

다음 절차는 현재의 홈 클러스터에서 마이그레이션 사용자에 대해 IM and Presence 서비스 및 Cisco Jabber를 비활성화하는 방법에 대해 설명합니다.

참고 한 번에 많은 수의 사용자를 마이그레이션하는 경우 Cisco Unified Communications Manager에서 벌크 관리 도구를 사용할 수 있습니다. 자세한 내용은 *Cisco Unified Communications Manager* 벌크 관리 설명서를 참조하십시오.

시작하기 전에

사용자 연락처 목록 내보내기, 339 페이지

프로시저

단계 **1** **Cisco Unified CM** 관리에서 사용자 관리 > 최종 사용자를 선택합니다.
단계 **2** 필터를 사용하여 IM and Presence 서비스에 대해 비활성화할 사용자를 찾습니다.
단계 **3** 최종 사용자 구성 화면에서 **Unified CM IM and Presence**에 대한 사용자 활성화를 선택 취소합니다.
단계 **4** 저장을 클릭합니다.

다음에 수행할 작업

사용자 수동으로 가져오기, 343 페이지

사용자 수동으로 가져오기

새 클러스터에 LDAP 동기화가 구성되어 있지 않은 경우 사용자를 새 Cisco Unified Communications Manager 클러스터에 수동으로 가져옵니다.

자세한 내용은 사용자 설정 구성, 73 페이지를 참조하십시오.

다음에 수행할 작업

새 클러스터에서 IM and Presence 서비스에 대해 사용자 활성화, 343 페이지

새 클러스터에서 **IM and Presence** 서비스에 대해 사용자 활성화

새로운 홈 클러스터에서 사용자가 동기화되었거나 수동으로 프로비저닝된 경우, IM and Presence 서비스 및 Cisco Jabber에 대해 사용자를 활성화해야 합니다.

프로시저

단계 **1** **Cisco Unified CM** 관리에서 사용자 관리 > 최종 사용자를 선택합니다.
단계 **2** 필터를 사용하여 IM and Presence 서비스에 대해 활성화할 사용자를 찾습니다.
단계 **3** 최종 사용자 구성 화면에서 **Unified CM IM and Presence**에 대한 사용자 활성화를 선택합니다.
단계 **4** 저장을 클릭합니다.

단계 **5** Cisco Unified Communications Manager에서 전화기 및 CSF에 대해 사용자를 프로비저닝합니다. 자세한 내용은 *Cisco Unified Communications Manager* 관리 설명서를 참조하십시오.

다음에 수행할 작업

홈 클러스터에서 연락처 목록 가져오기, 348 페이지

벌크 관리를 통해 사용자 마이그레이션

벌크 관리 도구(예: 클러스터 1에서 클러스터 2로 마이그레이션)를 통해 사용자를 새 클러스터로 이동합니다.

시작하기 전에

Cisco Bulk Provisioning 서비스는 두 클러스터 모두에서 실행 중이어야 합니다.

참고 IM and Presence 클러스터의 소스에서 대상으로 이동할 사용자 수가 100보다 작으면 Cisco 클러스터 간 동기화 에이전트 서비스를 시작하거나 중지하지 마십시오.

소스/대상 클러스터에서 100에서 1000 사용자를 이동하는 경우 소스 및 대상 클러스터 모두에서 클러스터 간 동기화 에이전트 서비스를 중지하여 아래 단계를 수행합니다.

이동할 사용자 수가 1000보다 많은 경우, 예를 들어, 16K 사용자를 이동해야 하는 경우에는 먼저 다음 단계를 수행하여 8K 사용자를 이동하고 클러스터 간 동기화 에이전트 서비스를 중지하고 1K 사용자 청크로 사용자를 이동합니다. 나중에, 다음 8K를 1K 사용자의 청크로 분산하여 직렬 시퀀스로 이동합니다.

사용자가 소스에서 이동 중인 **IM and Presence** 클러스터에서**:**

1단계 IM and Presence 게시자의 프레즌스 이중화 그룹(PRG) 쌍의 연결된 구독자 노드에서 클러스터 간 동기화 에이전트 서비스를 중지합니다.

2단계 게시자 IM and Presence 프레즌스 이중화 그룹 쌍의 게시자 노드에서 클러스터 간 동기화 에이전트 서비스를 중지합니다.

사용자가 대상에서 이동 중인 **IM and Presence** 클러스터에서**:**

3단계 게시자 프레즌스 이중화 그룹 쌍의 두 번째 노드에서 클러스터 간 동기화 에이전트 서비스를 중지합니다.

4단계 게시자 프레즌스 이중화 그룹 쌍의 게시자 노드에서 클러스터 간 동기화 에이전트 서비스를 중지합니다.

참고 클러스터 간 동기화 에이전트 서비스를 중지해야 하는 다른 클러스터 노드가 없습니다.

5단계 벌크 관리를 통한 사용자 마이그레이션에 언급된 단계를 수행합니다.

6단계 대상 및 소스 클러스터 모두에서 IM and Presence 게시자 및 가입자 노드에서 클러스터 간 동기화 에이전트 서비스를 시작합니다.

7단계 다른 모든 클러스터에서 대상 클러스터와의 동기화를 완료하는 데 최대 30분이 걸릴 수 있습니다.

프로시저

	명령 또는 동작	목적
단계 1	CSV 파일로 사용자 내보내기, 345 페이지	원래 클러스터(클러스터 1)에서 마이그레이션 사용자를 CSV 파일로 내보냅니다.
단계 2	CSV 내보내기 파일 다운로드, 346 페이지	CSV 내보내기 파일을 다운로드합니다.
단계 3	CSV 내보내기 파일을 새 클러스터로 업로드, 346 페이지	CSV 파일을 대상 클러스터(클러스터 2)로 업로드합니다.
단계 4	사용자 템플릿 구성, 347 페이지	대상 클러스터에서 사용자 설정을 사용하여 사용자 템플릿을 구성합니다.
단계 5	새 클러스터로 사용자 가져오기, 347 페이지	벌크 관리의 사용자 삽입 메뉴를 사용하여 CSV 파일에서 사용자를 가져옵니다.
단계 6	벌크 관리를 통해 사용자 마이그레이션 확인, 348 페이지	벌크 관리를 통한 사용자 마이그레이션을 확인합니다.

CSV 파일로 사용자 내보내기

원래 클러스터에서 벌크 관리 도구를 사용하여 마이그레이션할 사용자를 CSV 파일로 내보냅니다.

참고: 작업이 실행된 후 작업 스케줄러로 이동하여 작업 상태를 확인하고 파일이 작성되었는지 확인할 수 있습니다. 나중에 실행을 선택한 경우, 작업 스케줄러를 사용하여 작업 실행 시간을 설정할 수 있습니다.

프로시저

단계 1 Cisco Unified CM 관리에서 벌크 관리 > 사용자 > 사용자 내보내기를 선택합니다.

단계 2 검색할 필터 도구를 사용하여 마이그레이션 할 사용자를 선택하고 찾기를 클릭합니다.

단계 3 다음을 클릭합니다.

단계 4 파일의 파일 이름을 입력합니다.
도구는 파일 끝에 `.txt` 확장명을 추가합니다. 예: `<csvfilename>.txt`.

단계 5 파일 형식 드롭다운에서 내보내기 파일의 형식을 선택합니다.

단계 6 작업을 즉시 실행하려면 즉시 실행을 선택하고 전송을 클릭합니다.

다음에 수행할 작업

작업이 실행된 후 작업 스케줄러로 이동하여 작업 상태를 확인하고 파일이 작성되었는지 확인할 수 있습니다. 나중에 실행을 선택한 경우, 작업 스케줄러를 사용하여 작업 실행 시간을 설정할 수 있습니다.

파일이 생성되었는지 확인한 후, CSV 내보내기 파일 다운로드, 346 페이지.

CSV 내보내기 파일 다운로드

내보내기 파일이 생성되었는지 확인한 후, 파일을 다운로드합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 벌크 관리 > 파일 업로드/다운로드를 선택합니다.

단계 **2** 찾기를 클릭합니다.

단계 **3** 생성된 파일을 선택하고 선택한 항목 다운로드를 클릭합니다.

단계 **4** 파일을 다운로드합니다.

다음에 수행할 작업

CSV 내보내기 파일을 새 클러스터로 업로드, 346 페이지

CSV 내보내기 파일을 새 클러스터로 업로드

대상 클러스터(클러스터 2)에서 클러스터 1에서 내보낸 csv 파일을 업로드합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 벌크 관리 > 파일 업로드/다운로드를 선택합니다.

단계 **2** 새로 추가를 클릭합니다.

단계 **3** 파일 선택을 클릭합니다. 다른 시스템에서 내보내기 파일을 찾아 선택합니다.

단계 **4** 대상 드롭다운에서 파일 내용을 가져오는 데 사용할 벌크 관리 메뉴를 선택합니다. 예를 들어, 사용자 또는 전화기 및 사용자.

단계 **5** 트랜잭션 유형 드롭다운에서 파일 내용을 가져오는 데 사용할 하위 메뉴를 선택합니다. 예를 들어 사용자 삽입 또는 전화기/사용자 삽입.

단계 **6** 저장을 클릭합니다.

다음에 수행할 작업

사용자 템플릿 구성, 347 페이지

사용자 템플릿 구성

대상 클러스터에서 가져온 사용자에게 적용할 설정으로 사용자 템플릿을 구성합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 벌크 관리 > 사용자 > 사용자 템플릿을 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 찾기를 클릭하고 기존 템플릿을 선택합니다.
- 새로 추가를 클릭하여 새 템플릿을 만듭니다.

단계 **3** 가져온 사용자에게 적용할 사용자 설정을 구성합니다. 예를 들어, 다음 필드가 선택되어 있는지 확인하십시오.

- 홈 클러스터
- **Unified CM IM and Presence**에 대한 사용자 활성화

단계 **4** 사용자가 Microsoft Outlook과 일정을 통합할 수있도록 하려면 프레즌스에 회의 정보 포함 확인란을 선택합니다을 선택합니다.

단계 **5** 나머지 필드를 구성합니다.

단계 **6** 저장을 클릭합니다.

다음에 수행할 작업

새 클러스터로 사용자 가져오기, 347 페이지

새 클러스터로 사용자 가져오기

벌크 관리의 사용자 삽입 메뉴를 사용하여 내보낸 사용자를 새 클러스터로 가져옵니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 벌크 관리 > 사용자 > 사용자 삽입을 선택합니다.

단계 **2** 파일 이름에서 다른 시스템에서 내보낸 파일을 선택합니다.

단계 **3** 사용자 템플릿 이름에서 위에서 만든 사용자 템플릿을 선택합니다.

단계 **4** 사용자 내보내기로 생성된 파일 확인란을 선택합니다.

단계 **5** 즉시 실행을 클릭하고 제출을 클릭합니다.

다음에 수행할 작업

홈 클러스터에서 연락처 목록 가져오기, 348 페이지

벌크 관리를 통해 사용자 마이그레이션 확인

벌크 관리를 통해 사용자를 마이그레이션하고 소스 및 대상 클러스터에서 Cisco 클러스터 간 동기화 에이전트 서비스를 시작한 후, 소스 및 대상 클러스터와는 다른 클러스터가 사용자 이동이 발생했다는 알림을 받았는지 확인해야 합니다.

다른 모든 클러스터에서 대상 클러스터와의 동기화를 완료하는 데 최대 30분이 걸릴 수 있습니다. 대기하는 동안, CiscoSyslogs를 모니터링하기 위해 변경 사항(소스 또는 대상)의 일부가 아닌 병렬 게시자를 병렬로 샘플링하는 터미널 세션을 열 수 있습니다.

프로시저

단계 **1** 벌크 관리를 통해 사용자를 마이그레이션하고, 소스 및 대상 클러스터에서 Cisco 클러스터 간 동기화 에이전트 서비스를 시작하여 샘플 IMP 퍼블리셔 노드가 이미 동기화를 완료했는지 확인하려면 아래 명령을 실행합니다. 이 순간의 타임스탬프에 알립니다. 다음 예제 구문에서 대상 클러스터 이름은 dst-name입니다. 이 이름을 해당 대상 클러스터 이름으로 대체합니다.

```
admin:file search activelog syslog/CiscoSyslog ".*InterClusterSyncAgentStatus:.*dst-name.*"
```

단계 **2** ICSA 상태의 타임스탬프가 기록된 타임스탬프보다 최근이 아닌 경우에는 최대 30분 동안 다음 명령을 사용하여 동기화를 성공적으로 수행합니다.

```
admin:file tail activelog syslog/CiscoSyslog regexp
".*InterClusterSyncAgentStatus:.*dst-name.*"
```

선택한 샘플 클러스터/노드에서 ICSA 실패 동기화 상태 알람이 표시되는 경우 성공적인 동기화 상태 알람이 발생하면 5-10분 동안 기다립니다. ICSA는 5분마다 재시도합니다. 동기화 알람이 없거나 계속 동기화가 실패하는 경우에는 TAC 케이스를 엽니다.

이 시점에, 벌크 관리를 통해 사용자를 마이그레이션하고, 소스 및 대상 클러스터에서 Cisco 클러스터 간 동기화 에이전트 서비스를 시작한 후 기록된 타임스탬프 보다 현재 시간이 30분 늦은 경우 5개의 원격 샘플 클러스터를 확인한 것입니다. 이제 다음 이동 프로세스를 진행하거나 다른 이동이 없는 경우 작업이 완료됩니다.

홈 클러스터에서 연락처 목록 가져오기

사용자를 새 클러스터로 마이그레이션한 후 연락처 목록을 가져와서 마이그레이션된 사용자의 연락처 데이터를 복원합니다.

프로시저

단계 **1** 전에 내보낸 연락처 목록 CSV 파일을 업로드합니다.

a) **Cisco Unified CM IM and Presence** 관리에서 벌크 관리 > 파일 업로드/다운로드를 선택합니다.
b) 새로 추가를 클릭합니다.
c) 찾아보기를 클릭하고 연락처 목록 CSV 파일을 찾아 선택합니다.

d) 대상으로 연락처 목록을 선택합니다.
e) 트랜잭션 유형으로 사용자 연락처 가져오기 - 사용자 정의 파일을 선택합니다.
f) 선택적으로 파일이 있으면 덮어씁니다를 선택합니다.
g) 저장을 클릭하여 파일을 업로드합니다.
h) 저장을 클릭하여 파일을 업로드합니다.

단계 **2** 연락처 목록 가져오기 작업을 실행합니다.

a) **Cisco Unified CM IM and Presence** 관리에서 벌크 관리 > 연락처 목록 > 업데이트를 선택합니다.
b) 1단계에서 업로드한 CSV 파일을 선택합니다.
c) 선택적으로 작업 설명을 업데이트합니다.
d) 지금 작업을 실행하려면 즉시 실행을 클릭합니다. 업데이트 일정을 예약하려면 나중에 실행을 클릭합니다.
e) 제출을 클릭합니다.

단계 **3** 연락처 목록 가져오기 상태를 모니터링합니다.

a) **Cisco Unified CM IM and Presence** 관리에서 벌크 관리 > 연락처 목록 > 작업 스케줄러를 선택합니다.
b) 모든 BAT 작업을 나열하려면 찾기를 클릭합니다.
c) 완료된 것으로 상태가 보고되면 연락처 목록 가져오기 작업의 작업 ID를 선택합니다.
d) 연락처 목록 파일의 내용을 보려면 **CSV** 파일 이름에 나열된 파일을 선택합니다.
e) 로그를 열려면 로그 파일 이름 링크를 클릭합니다.

작업의 시작 시간과 끝 시간이 나열되고, 결과 요약이 표시됩니다.

기존 클러스터에서 사용자 업데이트

새 클러스터에서 모든 것이 정상적으로 작동할 때까지 이전 클러스터에서 사용자를 제거하지 않을 수 있습니다. 벌크 관리의 사용자 업데이트 기능을 사용하여 이전 클러스터에서 IM and Presence 기능을 제거하려면 이 절차를 사용하십시오.

프로시저

단계 **1** Cisco Unified CM 관리에서 벌크 관리 > 사용자 > 사용자 업데이트 > 쿼리를 선택합니다.
단계 **2** 필터 도구를 사용하여 마이그레이션 사용자를 검색합니다. 예를 들어, **IM and Presence**가 활성화됨 조건을 충족하는 모든 사용자를 검색 할 수 있습니다.
단계 **3** 다음을 클릭합니다.
단계 **4** 다음 두 필드 각각에 대해 맨 왼쪽 상자를 선택하고 오른쪽 옆의 상자를 선택하지 마십시오. 왼쪽 상자는 필드를 업데이트하려는 것을 나타내고 오른쪽 상자는 새 설정을 나타냅니다: 선택 취소.

- 홈 클러스터
- **Unified CM IM and Presence**에 대한 사용자 활성화

단계 **5** 작업 정보 아래에서 즉시 실행을 선택합니다.

단계 **6** 제출을 클릭합니다.

다음에 수행할 작업

마이그레이션이 성공적으로 수행되고 모든 사용자가 새 클러스터에서 올바르게 구성되었다고 확신하면 이전 클러스터에서 마이그레이션된 사용자를 삭제할 수 있습니다.

29 장

로캘 관리

로캘 관리 개요

여러 언어를 지원하려면 Cisco Unified Communications Manager 및 IM and Presence 서비스를 구성할 수 있습니다. 설치할 수 있는 지원되는 언어의 수에는 제한이 없습니다.

Cisco Unified Communications Manager 로캘 설치 관리자 및 IM and Presence 서비스 로캘 설치 관리자의 로캘별 버전을 www.cisco.com에서 다운로드할 수 있습니다. 시스템 관리자가 로캘 설치 관리자를 설치하면, 사용자는 지원되는 인터페이스로 작업할 때 해당되는 경우 선택한 번역된 텍스트/신호음을 보거나 받을 수 있습니다.

Cisco Unified Communications Manager 또는 IM & Presence 서비스를 업그레이드 한 후에는 모든 로캘을 다시 설치해야 합니다. Cisco Unified Communications Manager 노드 또는 IM and Presence 서비스 노드의 major.minor 버전 번호와 일치하는 최신 버전의 로캘을 설치합니다.

클러스터의 모든 노드에 Cisco Unified Communications Manager를 설치하고 데이터베이스를 설정한 후 로캘을 설치하십시오. IM and Presence 서비스 노드에 특정 로캘을 설치하려면 먼저 Cisco Unified Communications Manager 클러스터에 동일한 국가의 Cisco Unified Communications Manager 로캘 파일을 설치해야 합니다.

소프트웨어 업그레이드를 완료한 후 Cisco Unified Communications Manager 노드 및 IM and Presence 서비스 노드에 로캘을 설치하려면 다음 섹션의 정보를 사용하십시오.

사용자 로캘

사용자 로캘 파일에는 특정 언어 및 국가에 대한 언어 정보가 포함되어 있습니다. 사용자 로캘 파일은 사용자가 선택하는 로캘로 전화기 디스플레이, 사용자 애플리케이션, 사용자 웹 페이지에 대한 번역 텍스트 및 음성 프롬프트(해당되는 경우)를 제공합니다. 사용자 로캘 파일의 명명 규칙은 다음과 같습니다.

- cm-locale-language-country-version.cop(Cisco Unified Communications Manager)

- ps-locale-language_country-version.cop(IM and Presence 서비스)

시스템에 사용자 로캘만 필요한 경우 CUCM 로캘을 설치한 후 설치합니다.

네트워크 로캘

네트워크 로캘 파일은 전화기 신호음, 알림 디바이스, 게이트웨이 신호음 등 다양한 네트워크 항목에 대한 국가별 파일을 제공합니다. 결합된 네트워크 로캘 파일의 명명 규칙은 다음과 같습니다.

- cm-locale-combinednetworklocale-version.cop(Cisco Unified Communications Manager)

Cisco에서는 여러 네트워크 로캘을 단일 로캘 설치 관리자에 결합할 수 있습니다.

참고 Cisco에서 승인하고 고객이 제공하는 서버에서 Cisco Unified Communications Manager와 IM and Presence 서비스는 여러 로캘을 지원할 수 있습니다. 여러 로캘 설치 관리자를 설치하면 사용자가 여러 로캘 중에서 선택할 수 있습니다.

소프트웨어 업그레이드 설치와 동일한 프로세스를 통해 로컬 또는 원격 소스에서 로캘 파일을 설치할 수 있습니다. 클러스터의 각 노드에 둘 이상의 로캘 파일을 설치할 수 있습니다. 클러스터의 각 노드를 재부팅할 때까지는 변경 사항이 적용되지 않습니다. 클러스터의 모든 노드에 모든 로캘을 설치한 후에 노드를 재부팅하는 것이 좋습니다. 정규 근무 시간 후 노드를 재부팅하여 통화 프로세싱 중단을 최소화하십시오.

로캘 관리 필수 조건

로캘 설치 고려 사항

- 로캘을 설치하기 전에 모든 Cisco Unified Communications Manager 및 IM and Presence 서비스 클러스터 노드를 설치하고 데이터베이스를 설정합니다.
- IM and Presence 서비스 노드에 특정 로캘을 설치하려면 먼저 Cisco Unified Communications Manager 클러스터에 동일한 국가의 Cisco Unified Communications Manager 로캘 파일을 설치해야 합니다.
- 클러스터의 각 노드에 둘 이상의 로캘 파일을 설치할 수 있습니다. 새 로캘을 활성화하려면 설치 후 클러스터의 각 노드를 다시 시작해야 합니다.
- 소프트웨어 업그레이드 설치와 동일한 프로세스를 통해 로컬 또는 원격 소스에서 로캘 파일을 설치할 수 있습니다. 로컬 또는 원격 소스에서 업그레이드하는 방법에 대한 자세한 내용은 *Cisco Unified Communications Manager*용 업그레이드 설명서를 참조하십시오.

IM and Presence 서비스에 로캘 설치 관리자 설치

- IM and Presence 서비스에 대한 로캘을 설치하기 전에 Cisco Unified Communications Manager에 로캘 설치 프로그램을 설치합니다. 영어 외의 로캘을 사용하려면 Cisco Unified Communications Manager 및 IM and Presence 서비스에 모두 해당 언어 설치 관리자를 설치해야 합니다.
- IM and Presence 서비스 클러스터에 노드가 둘 이상 있는 경우 클러스터의 각 노드에 로캘 설치 관리자가 설치되었는지 확인합니다(가입자 노드 전에 IM and Presence 데이터베이스 게시자 노드에서 설치).
- 모든 로캘 설치 관리자가 두 시스템에 모두 로드되기 전에 사용자 로캘을 설정해서는 안 됩니다. 로캘 설치 관리자가 Cisco Unified Communications Manager에서는 로드되었지만 IM and Presence 서비스에서는 아직 로드되지 않았을 때 실수로 사용자 로캘을 설정하면 문제가 발생할 수 있습니다. 문제가 보고되면, Cisco Unified Communications 셀프 케어 포털에 로그인하는 각 사용자에게 현재 설정에서 영어로 로캘을 변경한 후 다시 해당 언어로 변경하도록 안내할 수 있습니다. 또한 BAT 도구를 사용하여 사용자 로캘을 해당 언어로 동기화할 수도 있습니다.

프로시저

단계 **1** `cisco.com`으로 이동하여 각자의 IM and Presence 서비스 버전에 맞는 로캘 설치 관리자를 선택합니다. http://software.cisco.com/download/navigator.html?mdfid=285971059

단계 **2** 현재의 작업 환경에 맞는 IM and Presence 로캘 설치 관리자 버전을 클릭합니다.

단계 **3** 파일을 다운로드한 후 하드 드라이브에 저장하고, 저장된 파일의 위치를 적어둡니다.

단계 **4** SFTP를 지원하는 서버로 이 파일을 복사합니다.

단계 **5** 관리자 계정 및 암호를 사용하여 Cisco Unified IM and Presence Operating System 관리에 로그인합니다.

단계 **6** 소프트웨어 업그레이드 > 설치/업그레이드를 선택합니다.

단계 **7** 소프트웨어 위치 소스로 원격 파일 시스템을 선택합니다.

단계 **8** 디렉터리 필드에 파일 위치(예: `/tmp`)를 입력합니다.

단계 **9** 서버 필드에 IM and Presence 서비스 서버 이름을 입력합니다.

단계 **10** 사용자 이름 및 사용자 암호 필드에 사용자 이름과 암호 자격 증명을 입력합니다.

단계 **11** 전송 프로토콜로 SFTP를 선택합니다.

단계 **12** 다음을 클릭합니다.

단계 **13** 검색 결과 목록에서 IM and Presence 서비스 로캘 설치 관리자를 선택합니다.

단계 **14** 다음을 클릭하여 설치 관리자 파일을 로드 및 검증합니다.

단계 **15** 로캘 설치를 완료한 후 클러스터의 각 서버를 다시 시작합니다.

단계 **16** 설치된 로캘의 기본 설정은 "English, United States"입니다. IM and Presence 서비스 노드가 다시 시작되는 동안 필요한 경우 다운로드한 설치 관리자의 로캘과 일치하도록 브라우저의 언어를 변경합니다.

단계 **17** 지원되는 제품에 대해 사용자가 로캘을 선택할 수 있는지 확인합니다.

팁 클러스터의 모든 서버에 동일한 구성 요소를 설치해야 합니다.

오류 메시지 로캘 참조

다음 표에서는 로캘 설치 관리자 활성화 중 발생할 수 있는 메시지에 대해 설명합니다. 오류가 발생하면 설치 로그에서 메시지를 볼 수 있습니다.

표 ***37:*** 로캘 설치 관리자 메시지 및 설명

메시지	설명
[LOCALE] 파일을 찾을 수 없음: <language>_<country>_user_locale.csv, 사용자 로컬이 데이터베이스에 추가되지 않았습니다.	이 오류는 시스템이 데이터베이스에 추가할 사용자 로캘 정보가 포함된 CSV 파일을 찾을 수 없을 때 발생하며, 빌드 프로세스의 오류를 나타냅니다.
[LOCALE] 파일을 찾을 수 없음: <country>_network_locale.csv, 네트워크 로케일이 데이터베이스에 추가되지 않았습니다.	이 오류는 시스템이 데이터베이스에 추가할 네트워크 로캘 정보가 포함된 CSV 파일을 찾을 수 없을 때 발생하며, 빌드 프로세스의 오류를 나타냅니다.
[LOCALE] CSV 파일 설치 관리자 installdb가 없거나 이 파일을 실행할 수 없음	installdb라는 애플리케이션이 있는지 확인해야 합니다. 이 애플리케이션은 CSV 파일에 포함된 정보를 읽고 대상 애플리케이션에 정확히 적용합니다. 이 애플리케이션이 없다면 Cisco Unified Communications 애플리케이션과 함께 설치되지 않았거나(거의 가능성 없음), 삭제되었거나(좀 더 가능성 있음), 노드에 Cisco Unified Communications Manager나 IM and Presence 서비스 등의 Cisco Unified Communications 애플리케이션이 설치되지 않은 것입니다(가장 가능성 높음). 데이터베이스의 올바른 레코드 없이는 로캘이 작동하지 않으므로 로캘의 설치가 종료됩니다.

메시지	설명
[LOCALE] /usr/local/cm/application_locale/cmservices/ipma/com/cisco/ipma/client/locales/maDialogs_<ll>_<CC>.properties.Checksum을 만들지 못했습니다. [LOCALE] /usr/local/cm/application_locale/cmservices/ipma/com/cisco/ipma/client/locales/maMessages_<ll>_<CC>.properties.Checksum을 만들지 못했습니다. [LOCALE] /usr/local/cm/application_locale/cmservices/ipma/com/cisco/ipma/client/locales/maGlobalUI_<ll>_<CC>.properties.Checksum을 만들지 못했습니다. [LOCALE] /usr/local/cm/application_locale/cmservices/ipma/LocaleMasterVersion.txt.Checksum을 만들 수 없음.	이러한 오류는 시스템이 체크섬 파일(Java 실행 파일이 없는 경우 /usr/local/thirdparty/java/j2sdk/jre/bin/java), Java 아카이브 파일 없거나 손상된 경우 /usr/local/cm/jar/cmutil.jar 또는 Java 클래스가 없거나 손상된 경우 com.cisco.ccm.util.Zipper)을 만들지 못할 때 발생합니다. 이러한 오류가 발생해도 로캘은 계속 올바르게 작동합니다. 단, 지역화된 Cisco Unified Communications Manager Assistant 파일의 변경 사항을 감지할 수 없는 Cisco Unified Communications Manager Assistant는 예외입니다.
[LOCALE] Unified CM Assistant 로캘 정보 업데이트를 위한 /usr/local/cm/application_locale/cmservices/ipma/LocaleMasterVersion.txt를 찾을 수 없음	시스템이 올바른 위치에서 파일을 찾을 수 없을 때 이 오류가 발생하는데, 빌드 프로세스의 오류 때문일 가능성이 높습니다.
[LOCALE] <locale-installer-file-name>을 데이터베이스에 추가하지 못했습니다.	로캘이 설치되는 동안 발생하는 모든 실패 때문에 이 오류가 발생하며, 터미널 상태를 나타냅니다.
[LOCALE] <locale-installer-file-name>을 찾지 못했습니다.	업그레이드 중에 시스템이 이 로캘을 마이그레이션하지 않습니다. 다운로드된 로캘 설치 관리자 파일이 다운로드 위치에 있지 않습니다. 플랫폼이 이 파일을 이동 또는 삭제했을 수 있습니다. 중요하지 않은 이 오류는 Cisco Unified Communications 애플리케이션이 업그레이드된 후 로캘 설치 관리자를 다시 적용하거나 새 로캘 설치 관리자를 적용해야 함을 나타냅니다.
[LOCALE] <locale-installer-file-name>을 마이그레이션 경로에 복사하지 못했습니다. 이 로캘은 업그레이드 중 마이그레이션되지 않습니다!	다운로드된 로캘 설치 관리자 파일을 마이그레이션 경로로 복사할 수 없습니다. 중요하지 않은 이 오류는 Cisco Unified Communications 애플리케이션이 업그레이드된 후 로캘 설치 관리자를 다시 적용하거나 새 로캘 설치 관리자를 적용해야 함을 나타냅니다.

메시지	설명
[LOCALE] DRS 등록 취소 실패	로캘 설치 관리자를 재해 복구 시스템에서 등록 취소할 수 없습니다. 백업 또는 복원 레코드에 로캘 설치 관리자가 포함되지 않습니다. 설치 로그를 기록하고 Cisco TAC에 문의하십시오.
[LOCALE] 백업 실패!	재해 복구 시스템이 다운로드된 로캘 설치 관리자 파일에서 tarball을 만들 수 없습니다. 백업을 시도하기 전에 로캘 설치 관리자를 다시 적용하십시오. 참고 시스템 복원 후 로캘을 수동으로 다시 설치해도 동일한 결과를 얻을 수 있습니다.
[LOCALE] 복원된 tarball에 COP 파일이 없음!	백업 파일이 손상되면 로캘 설치 관리자 파일을 성공적으로 추출하지 못할 수 있습니다. 참고 로캘 설치 관리자를 수동으로 다시 적용하면 로캘이 완전히 복원됩니다.
[LOCALE] COP 파일을 성공적으로 다시 설치하지 못함!	백업 파일이 손상되면 로캘 설치 관리자 파일도 손상될 수 있습니다. 참고 로캘 설치 관리자를 수동으로 다시 적용하면 로캘이 완전히 복원됩니다.
[LOCALE] COP 파일을 다시 설치하기 위한 스크립트를 빌드하지 못함!	플랫폼이 로캘을 다시 설치하는 데 사용되는 스크립트를 동적으로 생성할 수 없습니다. 참고 로캘 설치 관리자를 수동으로 다시 적용하면 로캘이 완전히 복원됩니다. 설치 로그를 기록하고 TAC에 문의하십시오.

지역화된 애플리케이션

IM and Presence 서비스 애플리케이션은 다양한 언어를 지원합니다. 지역화된 애플리케이션 및 사용 가능한 언어 목록은 다음 표를 참조하십시오.

표 ***38:*** 지역화된 애플리케이션 및 사용 가능한 언어 목록

인터페이스	지원되는 언어
관리 애플리케이션	

인터페이스	지원되는 언어
Cisco Unified CM IM and Presence 관리	중국어(중국), 영어, 일본어(일본), 한국어(대한민국)
Cisco Unified IM and Presence 운영 체제	중국어(중국), 영어, 일본어(일본), 한국어(대한민국)

30 장

서버 관리

서버 관리 개요

이 장에는 구축된 시스템의 서버 세부 정보를 편집하는 방법에 대한 정보가 들어 있습니다. 여기에는 클러스터에 새 노드를 할당하고, 클러스터에서 노드를 제거하고, 프레즌스를보고 서버 주소 세부 사항을 변경하는 작업이 포함됩니다.

서버 주소 변경

실행 중인 시스템이 있고 서버 주소 지정을 다음과 같이 변경해야 하는 경우 https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html에서 문서 *Cisco Unified Communications Manager* 및 *IM and Presence* 서비스의 *IP* 주소 및 호스트 이름 변경의 절차를 참조하십시오.

이는 다음과 같은 주소 변경 유형에 적용됩니다.

- 서버 IP 주소 변경
- 서버 호스트 이름 변경
- 노드 이름 변경(예를 들어, IP 주소를 사용하여 노드 이름을 정의하고 대신 호스트 이름을 사용하려는 경우).
- IM and Presence 서비스의 기본 도메인 변경

클러스터에서 IM and Presence 노드 삭제

IM and Presence Service 노드를 해당 프레즌스 이중화 그룹 및 클러스터에서 안전하게 제거해야 하는 경우 이 절차를 수행합니다.

주의 노드를 제거하면 프레즌스 이중화 그룹에 있는 나머지 노드의 사용자에 대한 서비스가 중단됩니다. 이 절차는 유지 보수 기간 동안에만 수행해야 합니다.

프로시저

단계 **1** **Cisco Unified CM** 관리 > 시스템 > 프레즌스 이중화 그룹페이지에서 고가용성이 활성화되어 있는 경우 이를 비활성화합니다.

단계 **2** **Cisco Unified CM** 관리 > 사용자 관리 > **Presence** 사용자 할당 페이지에서 제거할 노드의 모든 사용자를 할당 해제하거나 이동합니다.

단계 **3** 해당 프레즌스 이중화 그룹에서 노드를 제거하려면 프레즌스 이중화 그룹의 프레즌스 이중화 그룹 설정 페이지에 있는 Presence Server 드롭다운 목록에서 선택되지 않음을 선택합니다. 경고 대화 상자에 노드 할당 해제로 인해 프레즌스 이중화 그룹의 서비스가 다시 시작된다는 내용이 표시되면 확인을 선택합니다.

참고 프레즌스 이중화 그룹에서 퍼블리셔 노드를 직접 삭제할 수 없습니다. 퍼블리셔 노드를 삭제하려면 먼저 퍼블리셔 노드에서 사용자 할당을 해제하고 프레즌스 이중화 그룹을 완전히 삭제합니다.

그러나 삭제된 IM and Presence 노드를 클러스터에 다시 추가할 수 있습니다. 삭제된 노드를 추가하는 방법에 대한 자세한 내용은 삭제된 서버를 클러스터에 다시 추가, 360 페이지의 내용을 참조하십시오. 이 시나리오에서는 삭제된 퍼블리셔 노드가 Cisco Unified CM 관리 콘솔의 시스템 > 서버 화면에서 서버에 다시 추가될 때 **DefaultCUPSubcluster**가 자동으로 생성됩니다.

단계 **4** Cisco Unified CM 관리에서 시스템 > 서버에서 할당 해제된 노드를 삭제합니다. 경고 대화 상자에 이 작업을 실행 취소할 수 없다는 내용이 표시되면 확인을 클릭합니다.

단계 **5** 할당 해제한 노드의 호스트 VM 또는 서버를 종료합니다.

단계 **6** 모든 노드에서 **Cisco XCP** 라우터를 다시 시작합니다.

삭제된 서버를 클러스터에 다시 추가

Cisco Unified Communications Manager 관리에서 후속 노드(가입자)를 삭제한 후 클러스터에 다시 추가하려면 다음 절차를 수행합니다.

프로시저

단계 **1** Cisco Unified Communications Manager 관리에서 시스템 > 서버를 선택하여 서버를 추가합니다.

단계 **2** Cisco Unified Communications Manager 관리에 후속 노드를 추가한 후 해당 버전용 소프트웨어 키트에 제공된 디스크를 사용하여 서버에 설치합니다.

팁 설치하는 버전이 게시자 노드에서 실행되는 버전과 일치하는지 확인하십시오. 게시자에서 실행 중인 버전이 설치 파일과 일치하지 않는 경우 설치 프로세스 동안 설치 중 업그레이드 옵션을 선택합니다. 자세한 내용은 *Cisco Unified Communications Manager* 및 *IM and Presence Service* 설치 설명서를 참조하십시오.

단계 **3** Cisco Unified CM을 설치한 후에는 해당 Cisco Unified CM 버전을 지원하는 설치 설명서에 설명된 대로 후속 노드를 구성합니다.

단계 **4** Cisco Unified Reporting, RTMT 또는 CLI에 액세스하여 기존 노드 사이에서 데이터베이스 복제가 발생하는지 확인합니다. 필요한 경우 노드 간 데이터베이스 복제를 복구합니다.

설치 전 클러스터에 노드 추가

노드 설치 전에 [Cisco Unified Communications Manager 관리]를 사용하여 클러스터에 새 노드를 추가합니다. 노드를 추가할 때 선택하는 서버 유형과 설치하는 서버 유형이 일치해야 합니다.

새 노드를 설치하기 전에 첫 번째 노드에서 [Cisco Unified Communications Manager 관리]를 사용하여 새 노드를 구성해야 합니다. 클러스터에 노드를 설치하려면 *Cisco Unified Communications Manager* 설치 설명서를 참조하십시오.

Cisco Unified Communications Manager 비디오/음성 서버의 경우 Cisco Unified Communications Manager 소프트웨어의 초기 설치 중 추가하는 첫 번째 서버가 게시자 노드로 지정됩니다. 이후 설치 또는 추가되는 서버는 모두 가입자 노드로 지정됩니다. 클러스터에 추가하는 첫 번째 Cisco Unified Communications Manager IM and Presence 노드는 IM and Presence Service 데이터베이스 게시자 노드로 지정됩니다.

참고 서버가 추가된 후에는 [Cisco Unified Communications Manager 관리]를 사용하여 서버 유형을 변경할 수 없습니다. 기존 서버 인스턴스를 삭제한 다음 새 서버를 다시 추가하고 서버 유형 설정을 올바로 선택해야 합니다.

프로시저

단계 **1** 시스템 > 서버를 선택합니다.

서버 찾기 및 나열 창이 표시됩니다.

단계 **2** 새로 추가를 클릭합니다.

서버 구성 - 서버 추가 창이 표시됩니다.

단계 **3** 서버 유형 드롭다운 목록 상자에서 추가할 서버를 선택한 후 다음을 클릭합니다.

- CUCM 비디오/음성
- CUCM IM and Presence

단계 **4** 서버 구성 창에서 서버 설정을 적절히 입력합니다.

서버 구성 필드에 대한 설명은 서버 설정을 참조하십시오.

단계 **5** 저장을 클릭합니다.

Presence 서버 상태 보기

Cisco Unified Communications Manager 관리를 사용하여 IM and Presence Service 노드의 중요 서비스 및 셀프 진단 테스트 결과에 대한 상태를 확인합니다.

프로시저

단계 **1** 시스템 > 서버를 선택합니다.

서버 찾기 및 나열 창이 나타납니다.

단계 **2** 서버 검색 파라미터를 선택한 다음 찾기를 클릭합니다.

일치하는 레코드가 나타납니다.

단계 **3** 서버 찾기 및 나열 창에 나열되는 IM and Presence 서버를 선택합니다.

서버 구성 창이 나타납니다.

단계 **4** 서버 구성 창의 [IM and Presence 서버 정보] 섹션에서 [Presence 서버 상태] 링크를 클릭합니다.

서버에 대한 노드 세부 정보 창이 표시됩니다.

고가용성으로 서비스 다시 시작

고가용성을 비활성화한 다음 Cisco XCP 라우터, Cisco Presence 엔진 또는 서버 자체를 다시 시작해야 하는 시스템 구성 변경 또는 시스템 업그레이드를 수행하는 경우 고가용성을 활성화하기 전에 Cisco Jabber 세션을 재작성할 충분한 시간을 허용해야 합니다. 그렇지 않으면 세션이 생성되지 않은 Jabber 클라이언트에서 프레즌스가 작동하지 않습니다.

이 프로세스를 수행해야 합니다.

프로시저

단계 **1** 변경하기 전에 Cisco Unified CM IM and Presence 관리 창의 프레즌스 토폴로지 창(시스템 > 프레즌스 토폴로지)을 확인하십시오. 각 프레즌스 이중화 그룹에서 각 노드에 할당된 사용자 수를 기록합니다.

단계 **2** 각 프레즌스 이중화 그룹에서 고가용성을 비활성화하고 새 HA 설정이 동기화되도록 2분 이상 기다립니다.

단계 **3** 업데이트를 위해 다음 중 필요한 작업을 수행하십시오.

- Cisco XCP 라우터 다시 시작
- Cisco Presence 엔진을 다시 시작
- 서버 다시 시작

단계 **4** 다시 시작한 후 모든 노드의 활성 세션 수를 모니터링합니다.

단계 **5** 각 노드에 대해 `show perf query counter "Cisco Presence Engine" ActiveJsmSessions` CLI 명령을 각 노드에서 실행하여 각 노드에서 활성 세션 수를 확인합니다. 활성 세션 수는 할당된 사용자에 대해 1단계에서 기록한 번호와 일치해야 합니다. 모든 세션을 다시 시작하는 데 15분 이상 걸리지 않습니다.

단계 **6** 모든 세션이 만들어지면 프레즌스 이중화 그룹 내에서 고가용성을 활성화할 수 있습니다.

참고 30분이 경과하고 활성 세션이 아직 생성되지 않은 경우 Cisco Presence 엔진을 다시 시작합니다. 그래도 문제가 해결되지 않으면 해결해야 할 더 큰 시스템 문제가 있습니다.

참고 Cisco XCP 라우터 및/또는 Cisco Presence 엔진을 연속적으로 다시 시작하지 않는 것이 좋습니다. 그러나 다시 시작해야 할 경우: 첫 번째 서비스를 다시 시작하고 모든 JSM 세션을 다시 만들 때까지 기다립니다. 모든 JSM 세션이 만들어지면 두 번째 다시 시작합니다.

호스트 이름 구성

다음 표에는 통합 커뮤니케이션 매니저 서버의 호스트네임을 설정할 수 있는 위치, 호스트네임에 허용되는 문자 수, 호스트네임에 권장되는 첫 번째 문자와 마지막 문자가 열거되어 있습니다. 호스트네임을 정확히 설정하지 않을 경우 운영체제, 데이터베이스, 설치 등을 포함해 통합 커뮤니케이션 매니저의 일부 설정요소가 예상대로 작동하지 않을 수 있다는 점에 유의하십시오.

표 ***39: Cisco Unified Communications Manager***에서 호스트 이름 구성

호스트 이름 위치	허용되는 구성	허용되는 문자 수	호스트 이름에 권장되는 첫 번째 문자	호스트 이름에 권장되는 마지막 문자
호스트 이름/IP 주소 필드 Cisco Unified Communications Manager Administration의 시스템 > 서버	클러스터에서 서버의 호스트 이름을 추가 또는 변경할 수 있습니다.	2-63	영문자	영숫자
호스트 이름 필드 Cisco Unified Communications Manager 설치 마법사	클러스터에서 서버의 호스트 이름을 추가할 수 있습니다.	1-63	영문자	영숫자
호스트 이름 필드 Cisco Unified Communications 운영 체제의 설정 > **IP** > 이더넷	클러스터에서 서버의 호스트 이름을 변경할 수 있으며 추가할 수는 없습니다.	1-63	영문자	영숫자
set network hostname hostname 명령줄 인터페이스	클러스터에서 서버의 호스트 이름을 변경할 수 있으며 추가할 수는 없습니다.	1-63	영문자	영숫자

팁 호스트 이름은 ARPANET 호스트 이름에 대한 규칙을 따라야 합니다. 호스트 이름의 첫 번째 문자와 마지막 문자 사이에 영숫자와 하이픈을 입력할 수 있습니다.

모든 위치에서 호스트 이름을 구성하기 전에 다음 정보를 검토합니다.

- 디바이스-서버, 애플리케이션-서버 및 서버-서버 통신을 지원하는 서버 구성 창의 호스트 이름/IP 주소 필드를 사용하면 점으로 구분된 형식의 IPv4주소 또는 호스트 이름을 입력할 수 있습니다.

  Unified Communications Manager 게시자 노드를 설치한 후에 게시자의 호스트 이름이 이 필드에 자동으로 표시됩니다. Unified Communications Manager 가입자 노드를 설치하기 전에 Unified Communications Manager 게시자 노드에서 이 필드에 가입자 노드의 IP 주소 또는 호스트 이름을 입력합니다.

  이 필드에 Unified Communications Manager가 DNS 서버에 액세스하여 IP 주소에 대한 호스트 이름을 확인할 수 있는 경우에만 호스트 이름을 구성합니다. 반드시 DNS 서버에서 Cisco Unified Communications Manager 이름과 주소 정보를 구성해야 합니다.

팁 DNS 서버에서 Unified Communications Manager 정보를 구성하는 것 외에도 Cisco Unified Communications Manager를 설치하는 동안 DNS 정보를 입력합니다.

- Unified Communications Manager 게시자 노드를 설치하는 동안 정적 네트워킹을 사용하려는 경우 필수인 호스트 이름과 게시자 노드의 IP 주소를 입력하여 네트워크 정보를 구성합니다.

  통합 커뮤니케이션 매니저 가입자 노드를 설치할 때 통합 커뮤니케이션 매니저 퍼블리셔 노드의 호스트네임과 IP 주소를 입력해야만 통합 커뮤니케이션 매니저가 네트워크 연결 및 퍼블리셔-가입자의 유효성을 확인할 수 있습니다. 뿐만 아니라, 가입자 노드에 대한 호스트 이름 및 IP 주소를 입력해야 합니다. Unified Communications Manager 설치 프로그램에서 가입자 서버의 호스트 이름을 묻는 메시지를 표시하는 경우 호스트 이름/IP 주소 필드에 가입자 서버의 호스트 이름을 구성했으면 Cisco Unified Communications Manager 관리의 서버 구성 창에 표시되는 값을 입력합니다.

31 장

시스템 백업

백업 개요

일반 백업을 수행하는 것이 좋습니다. 재난 복구 시스템(DRS)을 사용하여 클러스터의 모든 서버에 대해 전체 데이터 백업을 수행할 수 있습니다. 언제든지 자동 백업을 설정하거나 백업을 호출할 수 있습니다.

재해 복구 시스템은 클러스터 수준 백업을 수행하며 중앙 위치로 Cisco Unified Communications Manager 클러스터의 모든 서버에 대한 백업을 수집하고 백업 데이터를 물리적 저장 장치에 보관합니다. 백업 파일은 암호화되고 시스템 소프트웨어에서만 열 수 있습니다.

DRS은 플랫폼 백업/복원의 일환으로 자체 설정(백업 디바이스 설정 및 예약 설정)을 복원합니다. DRS는 drfDevice.xml 및 drfSchedule.xml 파일을 백업 및 복원합니다. 이러한 파일로 서버가 복원되면 DRS 백업 디바이스 및 일정을 다시 구성할 필요가 없습니다.

시스템 데이터 복원을 수행하면 복원할 클러스터의 노드를 선택할 수 있습니다.

재해 복구 시스템에는 다음과 같은 기능이 포함됩니다.

- 백업 및 복원 작업을 수행하기 위한 사용자 인터페이스.
- 백업 기능을 수행하기 위해 분산된 시스템 아키텍처.
- 예약된 백업 또는 (사용자가 호출한) 수동 백업.
- 원격 sftp 서버에 백업을 보관합니다.

이 테이블에는 재난 복구 시스템에서 백업하고 복원할 수 있는 기능 및 구성 요소가 표시되어 있습니다. 선택하는 각 기능에 대해 시스템이 그 모든 구성 요소를 자동으로 백업합니다.

표 ***40: Cisco Unified CM*** 기능 및 구성 요소

기능	구성 요소
CCM - 통합 커뮤니케이션 매니저	통합 커뮤니케이션 매니저 데이터베이스
	플랫폼
	서비스 가용성
	음악 대기(MOH)
	Cisco Emergency Responder
	벌크 도구(BAT)
	기본 설정
	전화기 파일(TFTP)
	syslogagt(SNMP syslog 에이전트)
	cdpagent(SNMP cdp 에이전트)
	tct(추적 모음 도구)
	CDR(Call Detail Record)
	CDR 보고 및 분석(CAR)

표 ***41: IM and Presence*** 기능 및 구성 요소

기능	구성 요소
IM and Presence Service	IM and Presence 데이터베이스
	syslogagt(SNMP syslog 에이전트)
	cdpagent(SNMP cdp 에이전트)
	플랫폼
	보고자(서비스 가용성 보고자)
	CUP SIP 프록시
	XCP
	CLM
	벌크 도구(BAT)
	기본 설정
	tct(추적 모음 도구)

필수 구성 요소 백업

- 버전 요구 사항을 충족하는지 확인하십시오.
  - 모든 Cisco Unified Communications Manager 클러스터 노드는 동일한 버전의 Cisco Unified Communications Manager 애플리케이션을 실행하고 있어야 합니다.
  - 모든 IM and Presence Service 클러스터 노드는 동일한 버전의 IM and Presence 애플리케이션을 실행하고 있어야 합니다.
  - 백업 파일에 저장된 소프트웨어 버전은 클러스터 노드에서 실행되는 버전과 일치해야 합니다.

  전체 버전 문자열이 일치해야 합니다. 예를 들어, IM and Presence 데이타베이스 게시자 노드의 버전이 11.5.1.10000-1인 경우 모든 IM and Presence는 11.5.1.10000-1이어야 하며 백업 파일도 11.5.1.10000-1이어야 합니다. 현재 버전과 일치하지 않는 백업 파일에서 시스템을 복원하려고 하면 복원이 실패합니다. 백업 파일에 저장된 버전이 클러스터 노드에서 실행되는 버전과 일치하도록 소프트웨어 버전을 업그레이드할 때마다 시스템을 백업해야 합니다.
- DRS 암호화는 클러스터 보안 암호에 따라 달라집니다. 백업을 실행할 때 DRS은 암호화를 위해 임의의 암호를 생성한 다음, 임의의 암호를 클러스터 보안 암호로 암호화합니다. 백업하고 복원하는 사이에 클러스터 보안 암호가 변경된 경우 시스템을 복원하기 위해 해당 백업 파일을 사용

하려면 백업 당시의 암호가 무엇인지 알고 있거나 보안 암호를 변경/재설정한 후 즉시 백업해야 합니다.

- 원격 디바이스로 백업하려는 경우 SFTP 서버를 설정했는지 확인하십시오. 사용 가능한 SFTP 서버에 관한 자세한 내용은 다음을 참조하십시오. 원격 백업용 SFTP 서버 , 376 페이지

백업 작업 흐름

백업을 구성하고 실행하려면 이러한 작업을 수행합니다. 백업이 실행되는 동안에는 OS 관리 작업을 수행하지 마십시오. 그 이유는 재난 복구 시스템이 플랫폼 API를 잠가 모든 OS 관리 요청을 차단하기 때문입니다. 그러나 CLI 기반 업그레이드 명령만 플랫폼 API 잠금 패키지를 사용 하기 때문에 재난 복구 시스템은 대부분의 CLI 명령을 차단하지 않습니다.

프로시저

	명령 또는 동작	목적
단계 **1**	백업 디바이스 구성, 370 페이지	데이터를 백업할 디바이스를 지정합니다.
단계 **2**	백업 파일의 크기 계산, 371 페이지	SFTP 디바이스에 만들어지는 백업 파일의 크기를 예상합니다.
단계 **3**	다음 옵션 중 하나를 선택합니다. • 예약 백업 구성, 372 페이지 • 수동 백업 시작, 373 페이지	일정에 따라 데이터를 백업하는 백업 일정을 만듭니다. 필요한 경우 수동 백업을 실행합니다.
단계 **4**	현재 백업 상태 보기, 374 페이지	(선택 사항) 백업의 상태를 확인합니다. 백업이 실행되는 동안 현재 백업 작업의 상태를 확인할 수 있습니다.
단계 **5**	백업 기록 보기, 375 페이지	(선택 사항) 백업 기록 보기

백업 디바이스 구성

최대 10개의 백업 디바이스를 구성할 수 있습니다. 백업 파일을 저장할 위치를 구성하려면 다음 단계를 수행합니다.

시작하기 전에

- 백업 파일을 저장할 SFTP 서버의 디렉터리 경로에 대한 쓰기 권한이 있는지 확인합니다.
- DRS 마스터 상담원이 백업 디바이스 구성의 유효성을 검사하므로 사용자 이름, 암호, 서버 이름 및 디렉터리 경로가 유효한지 확인합니다.

참고 네트워크 트래픽이 덜할 것으로 예상되는 기간 동안 백업을 예약합니다.

프로시저

단계 **1** 재난 복구 시스템에서 백업 > 백업 디바이스를 선택합니다.

단계 **2** 백업 디바이스 목록 창에서 다음 중 하나를 수행합니다.

- 새 디바이스를 구성하려면 새로 추가를 클릭합니다.
- 기존 백업 디바이스를 편집하려면 검색 조건을 입력하고 [찾기]를 클릭하고 선택한 항목 편집을 클릭합니다.
- 백업 디바이스를 삭제하려면 백업 디바이스 목록에서 디바이스를 선택하고 선택한 항목 삭제를 클릭합니다.

백업 일정에서 백업 디바이스로 구성된 백업 디바이스는 삭제할 수 없습니다.

단계 **3** 백업 디바이스 이름 필드에 백업 이름을 입력합니다.

백업 디바이스 이름은 영숫자, 공백( ), 대시(-) 및 밑줄(_)만 포함합니다. 다른 문자는 사용하지 마십시오.

단계 **4** 대상 선택 영역의 네트워크 디렉터리에서 다음을 수행합니다.

- 호스트 이름/**IP** 주소 필드에 네트워크 서버의 호스트 이름 또는 IP 주소를 입력합니다.
- 경로 이름 필드에 백업 파일을 저장하려는 디렉터리 경로를 입력합니다.
- 사용자 이름 필드에 유효한 사용자 이름을 입력합니다.
- 암호 필드에 유효한 암호를 입력합니다.
- 네트워크 디렉터리에 저장할 백업 수 드롭다운 목록에서 필요한 백업 수를 선택합니다.

단계 **5** 저장을 클릭합니다.

다음에 수행할 작업

백업 파일의 크기 계산, 371 페이지

백업 파일의 크기 계산

하나 이상의 선택된 기능에 대한 백업 기록이 있는 경우에만 Cisco Unified Communications Manager는 백업 tar의 크기를 계산합니다.

계산된 크기는 정확한 값이 아니라 백업 tar의 예상 크기입니다. 크기는 이전의 성공적인 백업의 실제 백업 크기에 따라 계산되고, 마지막으로 백업한 이후 구성을 구성이 변경된 경우 다를 수 있습니다.

처음으로 시스템을 백업할 때가 아닌 및 이전 백업이 존재하는 경우에만 이 절차를 사용할 수 있습니다.

이 절차에 따라 SFTP 디바이스에 저장된 백업 tar의 크기를 예상합니다.

프로시저

단계 **1** 재난 복구 시스템에서 백업 > 수동 백업을 선택합니다.

단계 **2** 기능 선택 영역에서 백업할 기능을 선택합니다.

단계 **3** 예상 크기를 클릭하여 선택한 기능에 대한 백업의 예상 크기를 볼 수 있습니다.

다음에 수행할 작업

다음 절차 중 하나를 수행하여 시스템을 백업합니다.

- 예약 백업 구성, 372 페이지
- 수동 백업 시작, 373 페이지

예약 백업 구성

백업 예약을 최대 10개까지 만들 수 있습니다. 각 백업 일정에 자동 백업 일정, 백업할 기능 집합 및 저장 위치를 포함하여 자체 속성 집합이 있는 경우.

백업 .tar 파일이 임의로 생성되는 암호로 암호화되었는지 확인하십시오. 이 암호는 클러스터 보안 암호를 사용하여 암호화되고 백업 .tar 파일이 함께 저장됩니다. 이 보안 암호를 기억하고 있거나 보안 암호를 변경 또는 재설정한 후 즉시 백업을 수행해야 합니다.

주의 통화 처리 중단을 방지하고 서비스에 영향을 주지 않으려면 사용량이 적은 시간 동안 백업을 예약합니다.

시작하기 전에

백업 디바이스 구성, 370 페이지

프로시저

단계 **1** 재난 복구 시스템에서 백업스케줄러를 선택합니다.

단계 **2** 일정 목록 창에서 다음 단계 중 하나를 수행하여 새 일정을 추가하거나 기존 일정을 편집합니다.

- 새 일정을 만들려면 새로 추가를 클릭합니다.
- 기존 일정을 구성하려면 [일정 목록] 열에서 이름을 클릭합니다.

단계 **3** 스케줄러 창에서 일정 이름 필드에 일정 이름을 입력합니다.

참고 기본 일정의 이름은 변경할 수 없습니다.

단계 **4** 백업 디바이스 선택 영역에서 백업 디바이스를 선택합니다.

단계 **5** 기능 선택 영역에서 백업할 기능을 선택합니다. 하나 이상의 기능을 선택해야 합니다.

단계 **6** 백업 시작 영역에서 백업을 시작할 날짜 및 시간을 선택합니다.

단계 **7** 빈도 영역에서 백업이 발생하도록 하려는 빈도를 선택합니다. 빈도는 매일 한 번, 주별 및 월별로 설정할 수 있습니다. 주별을 선택하는 경우 백업이 발생할 요일을 선택할 수도 있습니다.

팁 백업 빈도를 화요일부터 토요일까지 발생하는 주별로 설정하려면 기본 설정을 클릭합니다.

단계 **8** 이러한 설정을 업데이트하려면 저장을 클릭합니다.

단계 **9** 다음 옵션 중 하나를 선택합니다.

- 선택한 일정을 활성화하려면 선택한 일정 활성화를 클릭합니다.
- 선택한 일정을 비활성화하려면 선택한 일정 비활성화를 클릭합니다.
- 선택한 일정을 삭제하려면 선택한 항목 삭제를 클릭합니다.

단계 **10** 일정을 활성화하려면 일정 활성화를 클릭합니다.

다음 백업은 설정한 시간에 자동으로 발생합니다.

참고 클러스터의 모든 서버에서 동일한 버전의 Cisco Unified Communications Manager 또는 Cisco IM and Presence Service를 실행 중이고 네트워크를 통해 연결할 수 있는지 확인합니다. 예약 백업 실행 시 연결할 수 없는 서버는 백업되지 않습니다.

다음에 수행할 작업

다음 절차를 수행합니다.

- 백업 파일의 크기 계산, 371 페이지
- (선택 사항) 현재 백업 상태 보기, 374 페이지

수동 백업 시작

시작하기 전에

- 백업 파일에 대한 저장 위치로 네트워크 디바이스를 사용하는지 확인합니다. Unified Communications Manager의 가상화된 구축은 백업 파일을 저장할 테이프 드라이브 사용을 지원하지 않습니다.
- 모든 클러스터 노드에 동일한 버전의 Cisco Unified Communications Manager 또는 IM and Presence Service가 설치되었는지 확인하십시오.

- 백업 프로세스는 원격 서버의 사용 가능한 공간 부족 또는 네트워크 연결 중단으로 인해 실패할 수 있습니다. 백업이 실패한 원인이 되는 문제를 해결한 후 새로운 백업 시작해야 합니다.
- 네트워크 중단이 없는지 확인하십시오.
- 백업 디바이스 구성, 370 페이지
- 백업 파일의 크기 계산, 371 페이지
- 클러스터 보안 암호에 대한 기록이 있는지 확인합니다. 이 백업을 완료한 후 클러스터 보안 암호가 변경되는 경우 암호를 알고 있어야 합니다. 그렇지 않으면 백업 파일을 사용하여 시스템을 복원할 수 없습니다.

참고 백업이 실행되는 동안 재난 복구 시스템이 플랫폼 API를 잠가 모든 요청을 차단하기 때문에 Cisco Unified OS 관리 또는 Cisco Unified IM and Presence OS 관리에서 작업을 수행할 수 없습니다. 그러나 CLI 기반 업그레이드 명령만 플랫폼 API 잠금 패키지를 사용하기 때문에 재난 복구 시스템은 대부분의 CLI 명령을 차단하지 않습니다.

프로시저

단계 **1** 재난 복구 시스템에서 백업 > 수동 백업을 선택합니다.
단계 **2** 수동 백업 창의 백업 디바이스 이름 영역에서 백업 디바이스를 선택합니다.
단계 **3** 기능 선택 영역에서 기능을 선택합니다.
단계 **4** 백업 시작을 클릭합니다.

다음에 수행할 작업

(선택 사항) 현재 백업 상태 보기, 374 페이지

현재 백업 상태 보기

현재 백업 작업의 상태를 확인하려면 다음 단계를 수행합니다.

주의 원격 서버에 대한 백업이 20시간 내에 완료되지 않을 경우 백업 세션 시간이 초과되고 새로 백업을 시작해야 합니다.

프로시저

단계 **1** 재난 복구 시스템에서 백업 > 현재 상태를 선택합니다.

단계 **2** 백업 로그 파일을 보려면 로그 파일 이름 링크를 클릭합니다.

단계 **3** 현재 백업을 취소하려면 백업 취소를 클릭합니다.

참고 현재 구성 요소가 백업 작업을 완료한 후에 백업을 취소합니다.

다음에 수행할 작업

백업 기록 보기, 375 페이지

백업 기록 보기

백업 기록을 보려면 다음 단계를 수행합니다.

프로시저

단계 **1** 재난 복구 시스템에서 백업 > 기록을 선택합니다.

단계 **2** 백업 기록 창에서 파일 이름, 백업 디바이스, 완료 날짜, 결과, 버전, 백업된 기능 및 실패한 기능을 포함하여 수행한 백업을 볼 수 있습니다.

참고 백업 기록 창에는 마지막 20개 백업 작업만 표시됩니다.

백업 상호 작용 및 제한 사항

- 백업 제한 사항 , 375 페이지

백업 제한 사항

백업에 다음과 같은 제한 사항이 적용됩니다.

표 ***42:*** 백업 제한 사항

제한 사항	설명
클러스터 보안 암호	클러스터 보안 암호를 변경할 때마다 백업을 실행하는 것이 좋습니다. 백업 암호화는 클러스터 보안 암호를 사용하여 백업 파일의 데이터를 암호화합니다. 백업 파일을 만든 후 클러스터 보안 암호를 편집하는 경우 기존 암호가 기억나지 않으면 해당 백업 파일을 사용하여 데이터를 복원할 수 없습니다.

제한 사항	설명
인증서 관리	재난 복구 시스템(DRS)은 Cisco Unified Communications Manager 클러스터 노드 사이에 인증 및 데이터 암호화를 위해 마스터 상담원과 로컬 상담원 간에 SSL 기반 통신을 사용합니다. DRS은 공개/개인 키 암호화를 위해 IPsec 인증서를 사용합니다. 인증서 관리 페이지에서 IPSEC truststore(hostname.pem) 파일을 삭제하는 경우 DRS는 예상대로 작동하지 않습니다. IPSEC-trust 파일을 수동으로 삭제하는 경우 IPSEC 인증서를 IPSEC-trust로 업로드해야 합니다. 자세한 내용은 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html에서 *Cisco Unified Communications Manager* 보안 설명서의 "인증서 관리" 섹션을 참조하십시오.

원격 백업용 SFTP 서버

데이터를 네트워크의 원격 디바이스에 백업하려면 SFTP 서버를 구성해야 합니다. 내부 테스트의 경우 Cisco는 Cisco에서 제공하고 Cisco TAC에서 지원하는 Cisco Prime Collaboration Deployment(PCD)의 SFTP 서버를 사용합니다. SFTP 서버 옵션에 대한 요약은 다음 표를 참조하십시오.

다음 표에 있는 정보를 사용하여 시스템에서 사용하는 SFTP 서버 솔루션을 확인합니다.

표 ***43: SFTP*** 서버 정보

SFTP 서버	정보
Cisco Prime Collaboration Deployment의 SFTP 서버	이 서버는 Cisco에서 제공 및 테스트하고 Cisco TAC에서 완벽하게 지원하는 유일한 SFTP 서버입니다. 버전 호환성은 Unified Communications Manager 및 Cisco Prime Collaboration Deployment 버전에 따라 달라집니다. 버전(SFTP) 또는 Unified Communications Manager를 업그레이드하기 전에 버전이 호환되는지 확인하기 위해 *Cisco Prime Collaboration Deployment* 관리 설명서를 참조하십시오.
기술 파트너의 SFTP 서버	이러한 서버는 타사에서 제공하고 타사에서 테스트했습니다. 버전 호환성은 타사 테스트에 따라 다릅니다. SFTP 제품을 업그레이드하거나 Unified Communications Manager를 업그레이드할 경우 기술 파트너가 페이지에서 버전 호환성 여부를 참조하십시오. https://marketplace.cisco.com

SFTP 서버	정보
다른 타사의 SFTP 서버	이러한 서버는 타사에서 제공하고 Cisco TAC에서 공식 지원하지 않습니다. 버전 호환성은 SFTP 버전 및 Unified Communications Manager 버전의 호환성을 위해 최대한 노력합니다. 참고 이러한 제품은 Cisco에서 테스트하지 않았으므로 기능을 보증할 수 없습니다. Cisco TAC는 이러한 제품을 지원하지 않습니다. SFTP 솔루션을 완벽하게 테스트하고 지원하기 위해 Cisco Prime Collaboration Deployment 또는 기술 파트너를 이용합니다.

암호화 지원

Unified Communications Manager 11.5의 경우 Unified Communications Manager는 SFTP 연결에 대해 다음 CBC 암호화를 광고합니다.

- aes128-cbc
- 3des-cbc
- aes128-ctr
- aes192-ctr
- aes256-ctr

참고 백업 SFTP 서버가 이러한 암호화 중 하나를 지원하여 Unified Communications Manager와 통신하는지 확인하십시오.

Unified Communications Manager 12.0 릴리스부터는 CBC 암호화가 지원되지 않습니다. Unified Communications Manager는 다음 CTR 암호화만 지원하고 광고합니다.

- aes256-ctr
- aes128-ctr
- aes192-ctr

참고 백업 SFTP 서버가 이러한 CTR 암호화 중 하나를 지원하여 Unified Communications Manager와 통신하는지 확인하십시오.

32 장

시스템 복원

복원 개요

재난 복구 시스템(DRS)은 시스템 복원 프로세스를 안내하는 마법사를 제공합니다.

백업 파일은 암호화되어 있으며 DRS 시스템만 데이터를 열어 복원할 수 있습니다. 재해 복구 시스템에는 다음과 같은 기능이 포함됩니다.

- 복원 작업을 수행하기 위한 사용자 인터페이스.
- 복원 기능을 수행하기 위해 분산된 시스템 아키텍처.

마스터 상담원

시스템이 클러스터의 각 노드에서 마스터 에이전트 서비스를 자동으로 시작하지만 마스터 에이전트는 게시자 노드에서만 작동합니다. 가입자 노드의 마스터 에이전트는 모든 기능을 수행하지는 않습니다.

로컬 에이전트

서버에 백업 및 복원 기능을 수행하는 로컬 에이전트가 있습니다.

마스터 에이전트가 포함된 노드를 포함하여 Cisco Unified Communications Manager 클러스터의 각 노드에 백업 및 복원 기능을 수행할 자체 로컬 에이전트가 있어야합니다.

참고 기본적으로 로컬 상담원이 IM and Presence 노드를 포함하여 클러스터의 각 노드에서 자동으로 시작됩니다.

필수 구성 요소 복원

- 버전 요구 사항을 충족하는지 확인하십시오.
  - 모든 Cisco Unified Communications Manager 클러스터 노드는 동일한 버전의 Cisco Unified Communications Manager 애플리케이션을 실행하고 있어야 합니다.
  - 모든 IM and Presence Service 클러스터 노드는 동일한 버전의 IM and Presence 애플리케이션을 실행하고 있어야 합니다.
  - 백업 파일에 저장된 버전은 클러스터 노드에서 실행되는 버전과 일치해야 합니다.

  전체 버전 문자열이 일치해야 합니다. 예를 들어, IM and Presence 데이타베이스 게시자 노드의 버전이 11.5.1.10000-1인 경우 모든 IM and Presence는 11.5.1.10000-1이어야 하며 백업 파일도 11.5.1.10000-1이어야 합니다. 현재 버전과 일치하지 않는 백업 파일에서 시스템을 복원하려고 하면 복원이 실패합니다.
- IP 주소, 호스트 이름, DNS 구성 및 서버의 구축 유형이 백업 파일에 저장된 IP 주소, 호스트 이름, DNS 구성 및 서버의 구축 유형과 일치하는지 확인하십시오.
- 백업을 실행한 후 클러스터 보안 암호를 변경한 경우 기존 암호에 대한 기록이 있어야 합니다. 그렇지 않으면 복원이 실패합니다.
- 클러스터에서 IPsec 정책이 활성화된 경우 복원 작업을 시작하기 전에 이 정책을 비활성화해야 합니다.

복원 후 **SAML SSO** 다시 활성화

중요 이 섹션은 릴리스 12.5(1)SU7에만 해당됩니다.

DRS을 사용하여 시스템을 복원한 후에는 클러스터의 임의 노드에서 간헐적으로 SAML SSO를 비활성화할 수 있습니다. 영향을 받는 노드에서 SAML SSO를 다시 활성화하려면 다음을 수행해야 합니다.

1. Cisco Unified CM 관리에서 시스템 > **SAML** 싱글 사인-온을 선택합니다.
2. 비활성화된 모든 서버 수정을 클릭합니다.

   SAML 싱글 사인-온 설정 창이 표시되면 다음을 클릭합니다.
3. **SSO** 테스트 실행을 클릭합니다.

4. "SSO 테스트가 성공 했습니다!"라는 메시지가 표시되면 브라우저 창을 닫고 마침을 클릭합니다.

참고 SAML SSO 재활성화 프로세스 중에 Cisco Tomcat이 다시 시작됩니다. SAML SSO가 이미 활성화된 노드에는 영향이 가지 않습니다.

작업 흐름 복원

복원 과정에서 Cisco Unified Communications Manager OS 관리 또는 Cisco Unified IM and Presence OS 관리를 사용하여 작업을 수행하지 마십시오.

프로시저

	명령 또는 동작	목적
단계 1	첫 번째 노드만 복원, 382 페이지	(선택 사항) 클러스터의 첫 번째 게시자 노드를 복원하는 경우에만 이 절차를 사용합니다.
단계 2	후속 클러스터 노드 복원, 384 페이지	(선택 사항) 클러스터의 가입자 노드를 복원하려면 이 절차를 사용합니다.
단계 3	게시자를 다시 빌드한 후 한 번에 클러스터 복원, 385 페이지	(선택 사항) 게시자가 이미 다시 빌드된 경우 한 번에 전체 클러스터를 복원하려면 이 절차를 수행합니다.
단계 4	전체 클러스터 복원, 386 페이지	(선택 사항) 게시자 노드를 포함하여 클러스터의 모든 노드를 복원하는 경우 이 절차를 사용합니다. 주요 하드 드라이브 고장 또는 업그레이드 오류가 발생하거나 하드 드라이브를 마이그레이션하는 경우 클러스터의 모든 노드를 다시 빌드해야 할 수 있습니다.
단계 5	마지막으로 성공한 구성으로 노드 또는 클러스터 복원, 388 페이지	(선택 사항) 노드를 마지막으로 성공한 구성으로 복원하는 경우 이 절차를 사용합니다. 하드 드라이브 고장 또는 기타 하드웨어 고장이 발생한 후에는 이 절차를 사용하지 마십시오.
단계 6	노드 다시 시작, 388 페이지	노드를 다시 시작하려면 이 절차를 사용합니다.
단계 7	복원 작업 상태 확인, 389 페이지	(선택 사항) 복원 작업 상태를 확인하려면 이 절차를 사용합니다.
단계 8	복원 기록 보기, 390 페이지	(선택 사항) 복원 기록을 보려면 이 절차를 사용합니다.

첫 번째 노드만 복원

다시 빌드한 후에 첫 번째 노드에 복원하는 경우 백업 디바이스를 구성해야 합니다.

이 절차는 Cisco Unified Communications Manager 첫 번째 노드(게시자 노드라고도 함)에 적용됩니다. 다른 Cisco Unified Communications Manager 노드 및 모든 IM and Presence Service 노드는 보조 노드 또는 가입자로 간주됩니다.

시작하기 전에

클러스터에 IM and Presence Service 노드가 있는 경우 첫 번째 노드를 복원할 때 실행 중이고 액세스할 수 있는지 확인합니다. 이는 절차를 수행하는 동안 유효한 백업 파일을 찾을 수 있도록 하는데 필요합니다.

프로시저

단계 **1** 재난 복구 시스템에서 복원 > 복원 마법사를 선택합니다.

단계 **2** 복원 마법사 **1**단계 창의 백업 디바이스 선택 영역에서 복원할 적절한 백업 디바이스를 선택합니다.

단계 **3** 다음을 클릭합니다.

단계 **4** 복원 마법사 **2**단계 창에서 복원하려는 백업 파일을 선택합니다.

참고 백업 파일 이름은 백업 파일을 만든 날짜와 시간을 나타냅니다.

단계 **5** 다음을 클릭합니다.

단계 **6** 복원 마법사 **3**단계 창에서 다음을 클릭합니다.

단계 **7** 복원할 기능을 선택합니다.

참고 백업을 위해 선택한 기능이 표시됩니다.

단계 **8** 다음을 클릭합니다. 복원 마법사 4단계 창이 표시됩니다.

단계 **9** 파일 무결성 확인을 실행하려면 SHA1 메시지 다이제스트를 사용하여 파일 무결성 확인 수행 확인란을 선택합니다.

참고 파일 무결성 확인은 선택 사항이며 SFTP 백업의 경우에만 필요합니다.

파일 무결성 확인 프로세스는 상당한 양의 CPU 및 네트워크 대역폭을 사용하므로 복원 프로세스가 느려집니다.

FIPS 모드에서는 메시지 다이제스트 확인에 대해서도 SHA-1을 사용할 수 있습니다. SHA-1은 디지털 서명에 사용되지 않는 HMAC 및 임의 비트 생성과 같은 해시 함수 애플리케이션의 모든 비 디지털 서명 용도에 사용할 수 있습니다. 예를 들어, SHA-1은 여전히 체크섬을 계산하는 데 사용될 수 있습니다. 서명 생성 및 확인의 경우에만 SHA-1을 사용할 수 없습니다.

단계 **10** 복원할 노드를 선택합니다.

단계 **11** 복원을 클릭하여 데이터를 복원합니다.

단계 **12** 다음을 클릭합니다.

단계 **13** 복원할 노드를 선택하라는 메시지가 표시되면 첫 번째 노드(게시자)만 선택합니다.

주의 복원 시도가 실패하므로 이 조건에서는 후속(가입자) 노드를 선택하지 마십시오.

단계 **14** (선택 사항) 서버 이름 선택 드롭다운 목록에서 게시자 데이터베이스를 복원하려는 가입자 노드를 선택합니다. 선택한 가입자 노드가 서비스 중이고 클러스터에 연결되었는지 확인합니다.
재난 복구 시스템은 백업 파일에서 모든 비 데이터베이스 정보를 복원하고 선택한 가입자 노드에서 최신 데이터베이스를 가져옵니다.

참고 이 옵션은 사용자가 선택한 백업 파일에 CCMDB database 구성 요소가 포함된 경우에 나타납니다. 처음에는 게시자 노드만 완전히 복원되지만 14단계를 수행하고 후속 클러스터 노드를 다시 시작하면 재난 복구 시스템은 데이터베이스 복제를 수행하고 모든 클러스터 노드 데이터베이스를 완벽하게 동기화합니다. 이렇게하면 모든 클러스터 노드가 최신 데이터를 사용하게 됩니다.

단계 **15** 복원을 클릭합니다.

단계 **16** 데이터가 게시자 노드에 복원됩니다. 데이터베이스 크기 및 복원하려고 선택한 구성 요소에 따라 복원하는 데 몇 시간이 필요할 수 있습니다.

참고 첫 번째 노드를 복원하면 전체 Cisco Unified Communications Manager 데이터베이스가 클러스터에 복원됩니다. 복원 중인 해당 데이터베이스의 노드 수와 크기에 따라 여러 시간이 걸릴 수 있습니다. 데이터베이스 크기 및 복원하려고 선택한 구성 요소에 따라 복원하는 데 몇 시간이 필요할 수 있습니다.

단계 **17** 복원 상태 창의 완료율 필드에 100%가 표시되면 서버를 다시 시작합니다. 첫 번째 노드만 복원하는 경우 클러스터의 모든 노드를 다시 시작해야 합니다. 후속 노드를 다시 시작하기 전에 첫 번째 노드를 다시 시작해야 합니다. 서버를 다시 시작하는 방법에 대한 자세한 내용은 다음에 할 일 섹션을 참조하십시오.

참고 Cisco Unified Communications Manager 노드만 복원하는 경우 Cisco Unified Communications Manager 및 IM and Presence Service 클러스터를 다시 시작해야 합니다.

IM and Presence Service 게시자 노드만 복원하는 경우 IM and Presence Service 클러스터를 다시 시작해야 합니다.

다음에 수행할 작업

- (선택 사항) 복원 상태를 보려면 다음을 참조하십시오. 복원 작업 상태 확인, 389 페이지
- 노드를 다시 시작하려면 다음을 참조하십시오. 노드 다시 시작, 388 페이지

후속 클러스터 노드 복원

이 절차는 Cisco Unified Communications Manager 가입자(후속) 가입자 노드에 적용됩니다. 설치된 첫 번째 Cisco Unified Communications Manager 노드가 게시자 노드입니다. 다른 모든 Cisco Unified Communications Manager 노드 및 모든 IM and Presence Service 노드는 가입자 노드입니다.

클러스터에 있는 하나 이상의 Cisco Unified Communications Manager 가입자 노드를 복원하려면 이 절차를 수행합니다.

시작하기 전에

복원 작업을 수행하기 전에 복원의 호스트 이름, IP 주소, DNS 구성 및 구축 유형이 복원하려는 백업 파일의 호스트 이름, IP 주소, DNS 구성 및 구축 유형과 일치하는지 확인합니다. 재난 복구 시스템은 다른 호스트 이름, IP 주소, DNS 구성 및 구축 유형을 복원하지 않습니다.

서버에 설치된 소프트웨어 버전이 복원하려는 백업 파일의 버전과 일치하는지 확인하십시오. 재난 복구 시스템은 복원 작업의 경우 일치하는 소프트웨어 버전만 지원합니다. 다시 빌드한 이후 후속 노드를 복원하는 경우 백업 장치를 구성해야 합니다.

프로시저

단계 **1** 재난 복구 시스템에서 복원 > 복원 마법사를 선택합니다.

단계 **2** 복원 마법사 **1**단계 창의 백업 디바이스 선택 영역에서 복원을 시작할 백업 디바이스를 선택합니다.

단계 **3** 다음을 클릭합니다.

단계 **4** 복원 마법사 **2**단계 창에서 복원하려는 백업 파일을 선택합니다.

단계 **5** 다음을 클릭합니다.

단계 **6** 복원 마법사 **3**단계 창에서 복원하려는 기능을 선택합니다.

참고 사용자가 선택한 파일로 백업한 기능만 표시됩니다.

단계 **7** 다음을 클릭합니다. 복원 마법사 4단계 창이 표시됩니다.

단계 **8** 복원 마법사 **4**단계 창에서 복원할 노드를 선택하라는 메시지가 표시되면 후속 노드만 선택합니다.

단계 **9** 복원을 클릭합니다.

단계 **10** 데이터가 후속 노드에 복원됩니다. 복원 상태를 보는 방법에 대한 자세한 내용은 다음에 할 일 섹션을 참조하십시오.

참고 복원 과정에서 Cisco Unified Communications Manager 관리 또는 사용자 옵션을 사용하여 작업을 수행하지 마십시오.

단계 **11** 복원 상태 창의 완료율 필드에 100%가 표시되면 방금 복원한 보조 서버를 다시 시작합니다. 첫 번째 노드만 복원하는 경우 클러스터의 모든 노드를 다시 시작해야 합니다. 후속 노드를 다시 시작하기 전에 첫 번째 노드를 다시 시작해야 합니다. 서버를 다시 시작하는 방법에 대한 자세한 내용은 다음에 할 일 섹션을 참조하십시오.

참고 IM and Presence Service 첫 번째 노드가 복원된 경우. IM and Presence Service 후속 노드를 다시 시작하기 전에 IM and Presence Service 첫 번째 노드를 다시 시작해야 합니다.

다음에 수행할 작업

- (선택 사항) 복원 상태를 보려면 다음을 참조하십시오. 복원 작업 상태 확인, 389 페이지
- 노드를 다시 시작하려면 다음을 참조하십시오. 노드 다시 시작, 388 페이지

게시자를 다시 빌드한 후 한 번에 클러스터 복원

데이터베이스 크기 및 복원하려고 선택한 구성 요소에 따라 복원하는 데 몇 시간이 필요할 수 있습니다. 게시자가 이미 다시 빌드되었거나 새로 설치한 경우 한 번에 전체 클러스터를 복원하려면 이 절차를 수행합니다.

프로시저

단계 **1** 재난 복구 시스템에서 복원 > 복원 마법사를 선택합니다.

단계 **2** 복원 마법사 **1**단계 창의 백업 디바이스 선택 영역에서 복원을 시작할 백업 디바이스를 선택합니다.

단계 **3** 다음을 클릭합니다.

단계 **4** 복원 마법사 **2**단계 창에서 복원하려는 백업 파일을 선택합니다.

백업 파일 이름은 백업 파일을 만든 날짜와 시간을 나타냅니다.

전체 클러스터를 복원하려는 클러스터의 백업 파일만 선택합니다.

단계 **5** 다음을 클릭합니다.

단계 **6** 복원 마법사 **3**단계 창에서 복원하려는 기능을 선택합니다.

화면에 백업 파일에 저장된 기능만 표시됩니다.

단계 **7** 다음을 클릭합니다.

단계 **8** 복원 마법사 **4**단계 창에서 **1** 단계 복원을 클릭합니다.

이 옵션은 복원을 위해 선택한 백업 파일이 클러스터의 백업 파일이고 복원을 위해 선택한 기능에 게시자 및 가입자 노드에 등록된 기능이 포함된 경우에만 복원 마법사 **4**단계 창에 나타납니다. 자세한 내용은 첫 번째 노드만 복원, 382 페이지 및 후속 클러스터 노드 복원, 384 페이지를 참조하십시오.

참고 상태 메시지에 게시자가 클러스터를 인식하는 데 실패했습니다. *1*단계 복원을 시작할 수 없습니다가 표시되면 퍼블리셔 노드를 복원한 다음, 가입자 노드를 복원해야 합니다. 자세한 내용은 관련 항목을 참조하십시오.

이 옵션을 사용하면 게시자가 클러스터를 인식할 수 있으며 이렇게 하는 데 5분 정도 걸립니다. 이 옵션을 클릭하면 "게시자가 클러스터를 인식할 때까지 5분간 기다리고 이 기간 동안에는 백업 또는 복원 활동을 시작하지 마십시오"라는 상태 메시지가 표시됩니다.

이 지연이 끝난 후 "게시자가 클러스터를 인식하게 되면 게시자가 클러스터를 인식했습니다. 서버를 선택하고 복원을 클릭하여 전체 클러스터의 복원을 시작하십시오.라는 상태 메시지가 표시됩니다".

이 지연이 끝난 후 게시자가 클러스터를 인식하지 못하는 경우 "게시자가 클러스터를 인식하는 데 실패했습니다. 1단계 복원을 시작할 수 없습니다. 계속해서 일반 2단계 복원을 수행하십시오."라는 상태 메시지가 표시됩니다. 2단계(게시자, 그런 다음 가입자)로 전체 클러스터를 복원하려면 첫 번째 노드만 복원, 382 페이지 및 후속 클러스터 노드 복원, 384 페이지에서 설명하는 단계를 수행합니다.

단계 **9** 복원하려면 노드를 선택하라는 메시지가 표시되면 클러스터의 모든 노드를 선택합니다.

재난 복구 시스템은 첫 번째 노드를 복원할 때 후속 노드에서 Cisco Unified Communications Manager 데이터베이스(CCMDB)를 자동으로 복원합니다. 복원 중인 해당 데이터베이스의 노드 수와 크기에 따라 여러 시간이 걸릴 수 있습니다.

단계 **10** 복원을 클릭합니다.
데이터는 클러스터의 모든 노드에 복원됩니다.

단계 **11** 복원 상태 창의 완료율 필드에 100%가 표시되면 서버를 다시 시작합니다. 첫 번째 노드만 복원하는 경우 클러스터의 모든 노드를 다시 시작해야 합니다. 후속 노드를 다시 시작하기 전에 첫 번째 노드를 다시 시작해야 합니다. 서버를 다시 시작하는 방법에 대한 자세한 내용은 다음에 할 일 섹션을 참조하십시오.

다음에 수행할 작업

- (선택 사항) 복원 상태를 보려면 다음을 참조하십시오. 복원 작업 상태 확인, 389 페이지
- 노드를 다시 시작하려면 다음을 참조하십시오. 노드 다시 시작, 388 페이지

전체 클러스터 복원

주요 하드 드라이브 고장 또는 업그레이드 오류가 발생하거나 하드 드라이브를 마이그레이션하는 경우 클러스터의 모든 노드를 다시 빌드해야 합니다. 전체 클러스터 복원하려면 다음 단계를 수행합니다.

네트워크 카드 바꾸거나 메모리를 추가하는 등 대부분의 다른 유형의 하드웨어 업그레이드를 수행하는 경우 이 절차를 수행할 필요가 없습니다.

프로시저

단계 **1** 재난 복구 시스템에서 복원 > 복원 마법사를 선택합니다.

단계 **2** 백업 디바이스 선택 영역에서 복원할 적절한 디바이스를 선택합니다.

단계 **3** 다음을 클릭합니다.

단계 **4** 복원 마법사 **2**단계 창에서 복원하려는 백업 파일을 선택합니다.

참고 백업 파일 이름은 백업 파일을 만든 날짜와 시간을 나타냅니다.

단계 **5** 다음을 클릭합니다.

단계 **6** 복원 마법사 **3**단계 창에서 다음을 클릭합니다.

단계 **7** 복원 마법사 **4**단계 창에서 복원 노드를 선택하라는 메시지가 표시될 때 모든 노드를 선택합니다.

단계 **8** 복원을 클릭하여 데이터를 복원합니다.

재해 복구 시스템은 첫 번째 노드를 복원할 때 후속 노드에서 Cisco Unified Communications Manager 데이터베이스(CCMDB)를 자동으로 복원합니다. 해당 데이터베이스의 노드 수와 크기에 따라 여러 시간이 걸릴 수 있습니다.

데이터가 모든 노드에서 복원됩니다.

참고 복원 과정에서 Cisco Unified Communications Manager 관리 또는 사용자 옵션을 사용하여 작업을 수행하지 마십시오.

데이터베이스 크기 및 복원하려고 선택한 구성 요소에 따라 복원하는 데 몇 시간이 필요할 수 있습니다.

단계 **9** 복원 프로세스가 완료되면 서버를 다시 시작합니다. 서버를 다시 시작하는 방법에 대한 자세한 내용은 다음에 할 일 섹션을 참조하십시오.

참고 후속 노드를 다시 시작하기 전에 첫 번째 노드를 다시 시작해야 합니다.

첫 번째 노드가 다시 시작되고 Cisco Unified Communications Manager의 복원된 버전을 실행한 후에 후속 노드를 다시 시작합니다.

단계 **10** 클러스터를 재부팅하면 복제가 자동으로 설정됩니다. *Cisco* 통합 커뮤니케이션 솔루션용 명령줄 인터페이스 설명서에 설명된 대로 "utils dbreplication runtimestate" CLI 명령어를 사용하여 모든 노드에서 복제 상태 값을 확인합니다. 각 노드의 값은 2가되어야합니다.

참고 후속 노드의 데이터베이스 복제는 클러스터의 크기에 따라 후속 노드를 다시 시작한 후 완료하는 데 많은 시간이 걸릴 수 있습니다.

팁 복제가 제대로 설정되지 않은 경우 *Cisco Unified Communications Solutions*용 명령줄 인터페이스 설명서에 설명된 대로 "utils dbreplication rebuild" CLI 명령을 사용합니다.

다음에 수행할 작업

- (선택 사항) 복원 상태를 보려면 다음을 참조하십시오. 복원 작업 상태 확인, 389 페이지
- 노드를 다시 시작하려면 다음을 참조하십시오. 노드 다시 시작, 388 페이지

마지막으로 성공한 구성으로 노드 또는 클러스터 복원

이 절차에 따라 마지막으로 성공한 구성으로 노드 또는 클러스터를 복원합니다.

시작하기 전에

- 복원 파일에 호스트 이름, IP 주소, DNS 구성 및 백업 파일에 구성된 구축 유형이 포함되어 있는지 확인하십시오.
- 서버에 설치된 Cisco Unified Communications Manager 버전이 복원하려는 백업 파일의 버전과 일치하는지 확인하십시오.
- 이 절차는 마지막으로 성공한 구성으로 노드를 복원하는 데만 사용해야 합니다.

프로시저

단계 **1** 재난 복구 시스템에서 복원 > 복원 마법사를 선택합니다.

단계 **2** 백업 디바이스 선택 영역에서 복원할 적절한 디바이스를 선택합니다.

단계 **3** 다음을 클릭합니다.

단계 **4** 복원 마법사 **2**단계 창에서 복원하려는 백업 파일을 선택합니다.

참고 백업 파일 이름은 백업 파일을 만든 날짜와 시간을 나타냅니다.

단계 **5** 다음을 클릭합니다.

단계 **6** 복원 마법사 **3**단계 창에서 다음을 클릭합니다.

단계 **7** 복원 노드를 선택하라는 메시지가 표시되면 해당 노드를 선택합니다.
데이터가 선택한 노드에서 복원됩니다.

단계 **8** 클러스터의 모든 노드를 다시 시작합니다. 첫 번째 Cisco Unified Communications Manager 노드를 다시 시작한 후에 이후의 Cisco Unified Communications Manager 노드를 다시 시작합니다. 클러스터에도 Cisco IM and Presence 노드가 있는 경우 첫 번째 Cisco IM and Presence 노드를 다시 시작한 후에 이후의 IM and Presence 노드를 다시 시작합니다. 자세한 내용은 다음에 할 일 섹션을 참조하십시오.

노드 다시 시작

데이터 복원 후 노드를 다시 시작해야 합니다.

게시자 노드(첫 번째 노드)를 복원하는 경우 먼저 게시자 노드를 다시 시작해야 합니다. 게시자 노드를 다시 시작하고 및 소프트웨어의 복원된 버전을 성공적으로 실행한 후에만 가입자 노드를 다시 시작합니다.

참고 CUCM 퍼블리셔 노드가 오프라인인 경우 IM and Presence 가입자 노드를 다시 시작하지 마십시오. 이러한 경우에는 가입자 노드가 CUCM 퍼블리셔에 연결할 수 없으므로 노드 서비스가 시작되지 않습니다.

주의 이 절차로 인해 시스템이 다시 시작되고 일시적으로 서비스를 사용할 수 없게 됩니다.

다시 시작해야 하는 클러스터의 모든 노드에서 이 절차를 수행합니다.

프로시저

단계 **1** Cisco Unified OS 관리에서 설정 > 버전을 선택합니다.

단계 **2** 노드를 다시 시작하려면 다시 시작을 클릭합니다.

단계 **3** 클러스터를 재부팅하면 복제가 자동으로 설정됩니다. **utils dbreplication runtimestate** CLI 명령을 사용하여 모든 노드에서 복제 상태 값을 확인합니다. 각 노드의 값은 2가 되어야 합니다. CLI 명령에 대한 자세한 내용은 Cisco Unified Communications (CallManager) 명령 참조를 참조하십시오.

복제가 제대로 설정되지 않은 경우 *Cisco Unified Communications Solutions*용 명령줄 인터페이스 설명서에 설명된 대로 **utils dbreplication reset** CLI 명령을 사용합니다.

참고 후속 노드의 데이터베이스 복제는 클러스터의 크기에 따라 후속 노드를 다시 시작한 후 완료하는 데 여러 시간이 걸릴 수 있습니다.

다음에 수행할 작업

(선택 사항) 복원 상태를 보려면 복원 작업 상태 확인, 389 페이지을 참조하십시오.

복원 작업 상태 확인

복원 작업 상태를 확인하려면 이 절차를 수행합니다.

프로시저

단계 **1** 재난 복구 시스템에서 복원 > 현재 상태를 선택합니다.

단계 **2** 복원 상태 창에서 복원 상태를 보려는 로그 파일 이름 링크를 클릭합니다.

복원 기록 보기

복원 기록을 보려면 다음 단계를 수행합니다.

프로시저

단계 **1** 재난 복구 시스템에서 복원 > 기록을 선택합니다.

단계 **2** 복원 기록 창에서 파일 이름, 백업 디바이스, 완료 날짜, 결과, 버전, 복원된 기능 및 실패한 기능을 포함하여 수행한 복원을 볼 수 있습니다.

복원 기록 창에는 마지막 20개 복원 작업만 표시됩니다.

데이터 인증

추적 파일

다음 추적 파일 위치는 문제를 해결하는 동안 또는 로그를 수집하는 동안 사용됩니다.

마스터 에이전트, GUI, 각 로컬 상담원 및 JSch 라이브러리에 대한 추적 파일은 다음 위치에 기록됩니다.

- 마스터 에이전트의 경우 추적 파일 위치: platform/drf/trace/drfMA0*
- 각 로컬 에이전트의 경우 추적 파일 위치: platform/drf/trace/drfLA0*
- GUI의 경우 추적 파일 위치: platform/drf/trace/drfConfLib0*
- JSch의 경우 추적 파일 위치: platform/drf/trace/drfJSch*

자세한 내용은 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-command-reference-list.html에서 *Cisco Unified Communications Solutions*용 명령줄 인터페이스 설명서를 참조하십시오.

명령줄 인터페이스

또한 재해 복구 시스템은 다음 표에 표시된 대로 백업 및 복원 기능의 하위 집합에 대한 명령줄 액세스를 제공합니다. 이러한 명령 및 이 명령줄 인터페이스 사용에 대한 자세한 내용은 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-command-reference-list.html에서 Cisco Unified Communications Solutions용 명령줄 인터페이스 설명서를 참조하십시오.

표 **44:** 재해 복구 시스템 명령줄 인터페이스

명령	설명
utils disaster_recovery estimate_tar_size	SFTP/로컬 디바이스에서 백업 tar의 예상 크기를 표시하고 기능 목록에 대해 하나의 매개 변수가 필요
utils disaster_recovery backup	재해 복구 시스템 인터페이스에 구성된 기능을 사용하여 수동 백업 시작
utils disaster_recovery jschLogs	JSch 라이브러리 로깅 활성화 또는 비활성화
utils disaster_recovery restore	복원을 시작하고 백업 위치, 파일 이름, 기능 및 복원할 노드에 대한 매개 변수가 필요
utils disaster_recovery status	진행 중인 백업 또는 복원 작업의 상태 표시
utils disaster_recovery show_backupfiles	기존 백업 파일 표시
utils disaster_recovery cancel_backup	진행 중인 백업 작업 취소
utils disaster_recovery show_registration	현재 구성된 등록 표시
utils disaster_recovery device add	네트워크 디바이스 추가
utils disaster_recovery device delete	디바이스 삭제
utils disaster_recovery device list	모든 디바이스 나열
utils disaster_recovery schedule add	일정 추가
utils disaster_recovery schedule delete	일정 삭제
utils disaster_recovery schedule disable	일정 비활성화
utils disaster_recovery schedule enable	일정 활성화
utils disaster_recovery schedule list	모든 일정 나열
utils disaster_recovery backup	재해 복구 시스템 인터페이스에 구성된 기능을 사용하여 수동 백업 시작
utils disaster_recovery restore	복원을 시작하고 백업 위치, 파일 이름, 기능 및 복원할 노드에 대한 매개 변수가 필요

명령	설명
utils disaster_recovery status	진행 중인 백업 또는 복원 작업의 상태 표시
utils disaster_recovery show_backupfiles	기존 백업 파일 표시
utils disaster_recovery cancel_backup	진행 중인 백업 작업 취소
utils disaster_recovery show_registration	현재 구성된 등록 표시

알람 및 메시지

알람 및 메시지

재해 복구 시스템 문제는 백업 또는 복원 절차 동안 발생할 수 있는 다양한 오류에 대해 알람을 제공합니다. 다음 표에서는 Cisco 재해 복구 시스템 알람 목록을 제공합니다.

표 ***45:*** 재해 복구 시스템 알람 및 메시지

알람 이름	설명	설명
DRFBackupDeviceError	DRF 백업 프로세스가 디바이스에 액세스하는 데 문제가 있습니다.	디바이스에 액세스하는 동안 D 프로세스에 오류가 발생했습니
DRFBackupFailure	Cisco DRF 백업 프로세스가 실패했습니다.	DRS 백업 프로세스에 오류가 니다.
DRFBackupInProgress	다른 백업을 실행 중에는 새 백업을 시작할 수 없습니다.	다른 백업을 실행 중에는 DRS 업을 시작할 수 없습니다.
DRFInternalProcessFailure	DRF 내부 프로세스에 오류가 발생했습니다.	DRS 내부 프로세스에 오류가 니다.
DRFLA2MAFailure	DRF 로컬 에이전트가 마스터 에이전트에 연결할 수 없습니다.	DRS 로컬 에이전트가 마스터 에 연결할 수 없습니다.
DRFLocalAgentStartFailure	DRF 로컬 에이전트가 시작되지 않습니다.	DRS 로컬 에이전트가 종료될 다.
DRFMA2LAFailure	DRF 마스터 에이전트가 로컬 에이전트에 연결할 수 없습니다.	DRS 마스터 에이전트가 로컬 에 연결할 수 없습니다.

알람 이름	설명	설명
DRFMABackupComponentFailure	DRF가 하나 이상의 구성 요소를 백업할 수 없습니다.	DRS가 데이터를 백업할 구 청했습니다.하지만 백업 프 오류가 발생했으며 구성 요 지 않았습니다.
DRFMABackupNodeDisconnect	백업 중인 노드가 완전히 백업되기 전에 마스터 에이전트에서 연결이 끊어졌습니다.	DRS 마스터 에이전트가 C Communications Manager 노 작업을 실행하는 동안 백업 되기 전에 노드 연결이 끊어
DRFMARestoreComponentFailure	DRF가 하나 이상의 구성 요소를 복원할 수 없습니다.	DRS가 데이터를 복원할 구 청했습니다.하지만 복원 프 오류가 발생했으며 구성 요 지 않았습니다.
DRFMARestoreNodeDisconnect	복원 중인 노드가 완전히 복원되기 전에 마스터 에이전트에서 연결이 끊어졌습니다.	DRS 마스터 에이전트가 C Communications Manager 노 작업을 실행하는 동안 복원 되기 전에 노드 연결이 끊어
DRFMasterAgentStartFailure	DRF 마스터 에이전트가 시작되지 않았습니다.	DRS 마스터 에이전트가 종 니다.
DRFNoRegisteredComponent	등록된 구성 요소를 사용할 수 없으므로 백업에 실패했습니다.	등록된 구성 요소를 사용할 DRS 백업에 실패했습니다
DRFNoRegisteredFeature	백업을 위한 기능을 선택하지 않았습니다.	백업을 위한 기능을 선택하 다.
DRFRestoreDeviceError	DRF 복원 프로세스가 디바이스에 액세스하는 데 문제가 있습니다.	디바이스에서 DRS 복원 프 수 없습니다.
DRFRestoreFailure	DRF 복원 프로세스가 실패했습니다.	DRS 복원 프로세스에 오류 니다.
DRFSftpFailure	DRF SFTP 작업에 오류가 발생했습니다.	DRS SFTP 작업에서 오류가 다.
DRFSecurityViolation	DRF 시스템이 보안 위반이 발생할 수 있는 악의적인 패턴을 발견했습니다.	DRF 네트워크 메시지에 코 디렉터리 통과 같은 보안 위 수 있는 악의적인 패턴이 포 니다. DRF 네트워크 메시지 습니다.

알람 이름	설명	설명
DRFTruststoreMissing	IPsec truststore가 노드에 누락되어 있습니다.	IPsec truststore가 노드에 누락되 니다. DRF 로컬 에이전트가 마 이전트에 연결할 수 없습니다.
DRFUnknownClient	Pub의 DRF 마스터 에이전트가 클러스터 외부의 알 수 없는 서버로부터 클라이언트 연결 요청을 받았습니다. 요청이 거부되었습니다.	Pub의 DRF 마스터 에이전트가 터 외부의 알 수 없는 서버로부 이언트 연결 요청을 받았습니다 거부되었습니다.
DRFBackupCompleted	DRF 백업이 성공적으로 완료되었습니다.	DRF 백업이 성공적으로 완료되 다.
DRFRestoreCompleted	DRF 복원이 성공적으로 완료되었습니다.	DRF 복원이 성공적으로 완료되 다.
DRFNoBackupTaken	DRF가 현재 시스템의 유효한 백업을 찾지 못했습니다.	DRF가 업그레이드/마이그레이 새로 설치 후 현재 시스템의 유 업을 찾지 못했습니다.
DRFComponentRegistered	DRF가 요청된 구성 요소를 성공적으로 등록했습니다.	DRF가 요청된 구성 요소를 성 등록했습니다.
DRFRegistrationFailure	DRF를 등록하지 못했습니다.	일부 내부 오류로 인해 구성 요 한 DRF 등록 작업이 실패했습
DRFComponentDeRegistered	DRF가 요청된 구성 요소를 성공적으로 등록 해제했습니다.	DRF가 요청된 구성 요소를 성 등록 해제했습니다.
DRFDeRegistrationFailure	구성 요소에 대한 DRF 등록 해제 요청이 실패했습니다.	구성 요소에 대한 DRF 등록 해 이 실패했습니다.
DRFFailure	DRF 백업 또는 복원 프로세스가 실패했습니다.	DRF 백업 또는 복원 프로세스 발생했습니다.
DRFRestoreInternalError	DRF 복원 작업에 오류가 발생했습니다. 복원이 내부적으로 취소되었습니다.	DRF 복원 작업에 오류가 발생 복원이 내부적으로 취소되었
DRFLogDirAccessFailure	DRF가 로그 디렉터리에 액세스할 수 없습니다.	DRF가 로그 디렉터리에 액세 습니다.
DRFDeRegisteredServer	DRF가 서버에 대한 모든 구성 요소를 자동으로 등록 해제했습니다.	서버가 Unified Communications 클러스터에서 연결이 끊어졌
DRFSchedulerDisabled	백업에 사용할 수 있는 기능이 구성되지 않아 DRF 스케줄러가 비활성화되었습니다.	백업에 사용할 수 있는 기능이 않아 DRF 스케줄러가 비활성 니다.

알람 이름	설명	설명
DRFSchedulerUpdated	기능 등록 해제로 인해 DRF 일정 백업 구성이 자동으로 업데이트되었습니다.	기능 등록 해제로 인해 DR 구성이 자동으로 업데이트

복원 상호 작용 및 제한 사항

복원 제한 사항

다음 제한 사항은 재난 복구 시스템을 사용하여 Cisco Unified Communications Manager 또는 IM and Presence Service를 복원하는 데 적용됩니다.

표 ***46:*** 복원 제한 사항

제한 사항	설명
수출 제한	제한된 버전에서 제한된 버전으로만 DRS 백업을 복원할 수 있으며 무제한 버전의 백업은 무제한 버전에만 복원할 수 있습니다. Cisco Unified Communications Manager의 미국 수출 무제한 버전으로 업그레이드하는 경우 나중에 이 소프트웨어의 미국 수출 제한 버전으로 업그레이드하거나 새로 설치를 수행할 수 없습니다.
플랫폼 마이그레이션	재난 복구 시스템을 사용하여 플랫폼 간에 데이터를 마이그레이션할 수 없습니다(예를 들어, Windows에서 Linux로 또는 Linux에서 Windows로). 복원은 백업과 동일한 제품 버전에서 실행해야 합니다. Windows 기반 플랫폼에서 Linux 기반 플랫폼으로 데이터 마이그레이션에 대한 자세한 내용은 *Data Migration Assistant* 사용 설명서를 참조하십시오.
하드웨어 교체 및 마이그레이션	데이터를 새 서버로 마이그레이션하기 위해 DRS 복원을 수행할 때 이전 서버에서 사용한 것과 동일한 IP 주소 및 호스트 이름을 새 서버에 할당해야 합니다. 또한 백업을 수행할 때 DNS가 구성된 경우 복원을 수행하기 전에 동일한 DN 구성이 있어야합니다. 서버를 교체하는 방법에 대한 자세한 내용은 *Cisco Unified Communications Manager* 단일 서버 또는 클러스터 교체 설명서를 참조하십시오. 뿐만 아니라, 하드웨어 교체 후 인증서 신뢰 목록(CTL) 클라이언트를 실행해야 합니다. 후속 노드(가입자) 서버를 복원하지 않은 경우 CTL 클라이언트를 실행해야 합니다. 다른 경우에는 DRS가 필요한 인증서를 백업합니다. 자세한 내용은 *Cisco* 통합 커뮤니케이션 매니저 보안 설명서에서 “CTL 클라이언트 설치” 및 “CTL 클라이언트 설정” 절차를 참조하십시오.
클러스터 간 Extension Mobility	백업에서 원격 클러스터에 로그인한 클러스터 간 내선 이동 사용자는 복구 후 로그인을 유지합니다.

참고 DRS 백업/복원은 CPU를 많이 사용하는 프로세스입니다. 스마트 라이센스 관리자는 백업 및 복원되는 구성 요소 중 하나입니다. 이 프로세스를 진행하는 동안 스마트 라이센스 관리자 서비스가 다시 시작됩니다. 리소스 사용률이 높게 예상되므로 유지 관리 기간 중에 프로세스를 예약하는 것이 좋습니다.

Cisco Unified Communications 서버 구성 요소를 성공적으로 복원한 후 Cisco Unified Communications Manager를 Cisco Smart Software Manager 또는 Cisco Smart Software Manager 위성을 사용하여 등록합니다. 백업을 수행하기 전에 이미 제품이 등록된 경우 라이센스 정보를 업데이트하기 위해 제품을 다시 등록합니다.

Cisco Smart Software Manager 또는 Cisco Smart Software Manager 위성에 제품을 등록하는 방법에 대한 자세한 내용은 해당 릴리스의 *Cisco Unified Communications Manager* 시스템 구성 설명서를 참조하십시오.

문제 해결

더 작은 가상 시스템으로 **DRS** 복원 실패

문제

IM and Presence Service 노드를 디스크 더 작은 VM으로 복원하는 경우 데이터베이스 복원이 실패할 수 있습니다.

원인

이 오류는 큰 디스크 크기에서 작은 디스크 크기로 마이그레이션하는 경우에 발생합니다.

해결 방법

2개의 가상 디스크가 있는 OVA 템플릿에서 복원을 위해 VM을 구축합니다.

33 장

연락처 목록의 벌크 관리

벌크 관리 개요

IM and Presence 벌크 관리 도구를 사용하면 다음을 포함하여 많은 IM and Presence 서비스 사용자에게 대량 트랜잭션을 수행할 수 있습니다.

- Microsoft 마이그레이션 프로세스에서 사용할 사용자 연락처 ID의 이름을 바꿉니다.
- 특정 노드 또는 프레즌스 이중화 그룹에 속한 사용자의 연락처 목록, 비 프레즌스 연락처 목록 및 위치 세부 정보를 CSV 데이터 파일로 내보냅니다.

참고 비 프레즌스 연락처는 IM 주소가 없고 이 절차를 통해서만 내보낼 수 있는 연락처입니다.

- 사용자가 내보낸 사용자 연락처 목록, 비 프레즌스 연락처 목록 및 사용자 위치 마이그레이션 세부 정보를 다른 클러스터에 있는 다른 노드 또는 프레즌스 이중화 그룹으로 가져올 수 있습니다. 새로운 사용자를 위한 연락처 목록을 미리 채우거나 기존 연락처 목록에 추가합니다.
- 이러한 기능을 사용하면 클러스터간에 사용자를 쉽게 마이그레이션할 수 있습니다.

벌크 관리 필수 조건

사용자 연락처 목록을 가져오기 전에:

1. Cisco Unified Communications Manager에서 사용자를 프로비저닝합니다.
2. Cisco Unified Communications Manager에서 사용자의 IM and Presence 서비스 사용이 허가되었는지 확인합니다.

참고 기본 연락처 목록 가져오기 속도는 가상 컴퓨터 구축 하드웨어 유형을 기반으로 합니다. **Cisco Unified CM IM and Presence** 관리시스템 > 서비스 파라미터 > **Cisco Bulk Provisioning Service**를 선택하여 연락처 목록 가져오기 속도를 변경할 수 있습니다. 그러나 기본 가져오기 속도를 높이면 IM and Presence 서비스의 CPU 및 메모리 사용량이 늘어납니다.

벌크 관리 작업 흐름

프로시저

	명령 또는 동작	목적
단계 **1**	사용자 연락처 ID 벌크 이름 변경, 398 페이지	CSV 파일을 업로드하고 사용자 목록에 대해 연락처 ID의 이름을 변경합니다.
단계 **2**	사용자 연락처 목록 및 비 프레즌스 연락처 목록 벌크 내보내기, 400 페이지	사용자의 연락처 목록을 CSV 파일로 내보내려면 이 절차를 사용하십시오. 그런 다음 벌크 관리를 사용하여 사용자 연락처 목록을 다른 노드 또는 클러스터로 이동할 수 있습니다.
단계 **3**	사용자 위치 세부 정보 벌크 내보내기 , 400 페이지	이 절차를 사용하여 사용자 위치 세부 정보를 CSV 파일로 내보낼 수 있습니다. 그런 다음 벌크 관리를 사용하여 사용자 위치 세부 정보 목록을 다른 노드 또는 클러스터로 이동할 수 있습니다.
단계 **4**	IM and Presence 서비스로 사용자 연락처 목록을 가져오려면 다음 작업을 수행하십시오. • 최대 연락처 목록 크기 확인, 404 페이지 • 입력 파일 업로드, 404 페이지 • 새 벌크 관리 작업 만들기, 409 페이지 • 벌크 관리 작업의 결과 확인, 410 페이지	

사용자 연락처 **ID** 벌크 이름 변경

주의 연락처 ID의 벌크 이름 변경은 Microsoft 서버(예: Lync)에서 IM and Presence 서비스로 사용자를 마이그레이션하는 경우 사용됩니다. 사용자 마이그레이션 프로세스에서 이 도구를 사용하는 방법에 대한 자세한 지침은 Cisco.com의 분할된 도메인 내 페더레이션 설명서를 참조하십시오. 다른 상황에서는 이 도구의 사용이 지원되지 않습니다.

CSV 파일을 업로드하고 사용자 목록에 대해 연락처 ID의 이름을 변경합니다.

프로시저

단계 1 모든 연락처 목록에서 이름을 변경하고자 하는 연락처 ID 목록이 포함된 CSV 파일을 업로드합니다.
a) IM and Presence 서비스 데이터베이스 게시자 노드로 이동합니다.
b) **Cisco Unified CM IM and Presence** 관리에서 벌크 관리 > 파일 업로드/다운로드를 선택합니다.
c) 새로 추가를 클릭합니다.
d) 찾아보기를 클릭하고 CSV 파일을 찾아 선택합니다. 입력 파일에 대한 자세한 내용은 사용자 연락처 ID 세부 정보 벌크 이름 변경, 399 페이지의 내용을 참조하십시오.
e) 대상으로 연락처를 선택합니다.
f) 트랜잭션 유형으로 연락처 이름 변경 - 사용자 정의 파일을 선택합니다.
g) 저장을 클릭하여 파일을 업로드합니다.

단계 2 게시자 노드의 **Cisco Unified CM IM and Presence** 관리에서 벌크 관리 > 연락처 목록 > 연락처 이름 변경을 선택합니다.

단계 3 파일 이름 필드에서 업로드한 파일을 선택합니다.

단계 4 다음 작업 중 하나를 선택합니다.
- 벌크 관리 작업을 즉시 실행하려면 즉시 실행을 클릭합니다.
- 벌크 관리 작업을 실행할 시간을 예약하려면 나중에 실행을 클릭합니다. BAT(Bulk Administration Tool)에서 작업을 예약하는 방법에 대한 자세한 내용은 Cisco Unified CM IM and Presence 관리의 온라인 도움말을 참조하십시오.

단계 5 제출을 클릭합니다.

작업을 즉시 실행하도록 선택한 경우 제출을 클릭하면 작업이 바로 실행됩니다.

다음에 수행할 작업

사용자 연락처 목록 및 비 프레즌스 연락처 목록 벌크 내보내기, 400 페이지

사용자 연락처 ID 세부 정보 벌크 이름 변경

이 작업을 실행하기 전에 업로드하는 파일은 다음 형식의 CSV 파일이어야 합니다.

<Contact ID> , <New Contact ID>

여기서 <Contact ID>는 기존 연락처 ID이며 <New Contact ID>는 연락처 ID의 새 형식입니다.

<Contact ID>는 프레즌스 토폴로지 사용자 할당 창에 나타나는 사용자의 IM 주소입니다.

다음은 항목이 하나 포함된 샘플 CSV 파일입니다.

```
Contact ID, New Contact ID
john.smith@example.com, jsmith@example.com
```

사용자 연락처 목록 및 비 프레즌스 연락처 목록 벌크 내보내기

사용자의 연락처 목록을 CSV 파일로 내보내려면 이 절차를 사용하십시오. 그런 다음 벌크 관리를 사용하여 사용자 연락처 목록을 다른 노드 또는 클러스터로 이동할 수 있습니다.

- 연락처 목록 -이 목록은 IM and Presence 연락처로 구성됩니다. IM 주소가 없는 연락처는 내보내지 않습니다(비 프레즌스 연락처 목록을 내보내야 함).
- 비 프레즌스 연락처 목록 - 이 목록은 IM 주소가 없는 연락처로 구성됩니다.

프로시저

단계 **1** Cisco Unified CM IM and Presence 관리에서 다음 중 하나를 수행합니다.

- 연락처 목록을 내보내려면 벌크 관리 > 연락처 목록 > 연락처 목록 내보내기를 선택합니다.
- 비 프레즌스 연락처 목록을 내보내려면 벌크 관리 > 비 프레즌스 연락처 목록 > 비 프레전스 연락처 목록 내보내기를 선택하고 다음 단계로 건너 뜁니다.

단계 **2** 연락처 목록만. 연락처 목록을 내보낼 사용자를 선택합니다.

a) 연락처 목록 내보내기 옵션에서 연락처 목록을 내보낼 사용자 범주를 선택합니다. 기본값은 모든 사용자의 연락처 목록을 내보내는 것입니다.
b) 찾기를 클릭하여 사용자 목록을 표시한 후 다음을 클릭합니다.

단계 **3** 파일 이름 필드에 CSV 파일의 이름을 입력합니다.

단계 **4** 작업 정보 아래에서 이 작업을 실행할 시기를 구성합니다.

- 즉시 실행 - 연락처 목록을 즉시 내보내면 이 버튼을 선택합니다.
- 나중에 실행 - 작업 시간을 예약하려면 이 버튼을 선택합니다. 이 옵션을 사용하면 벌크 관리 > 작업 스케줄러에서 작업 스케줄러 페이지를 사용하여 이 작업을 실행할 시간을 예약해야 합니다.

단계 **5** 제출을 클릭합니다.
즉시 실행을 선택하는 경우 내보내기 작업이 즉시 실행됩니다.

단계 **6** 내보내기 파일을 만든 후 내보낸 파일을 다운로드합니다.

a) Cisco Unified CM IM and Presence 관리에서 벌크 관리 > 파일 업로드/다운로드를 선택합니다.
b) 찾기를 클릭하고 내보내기 파일을 선택합니다.
c) 선택한 항목 다운로드를 클릭하고 액세스할 수있는 위치로 파일을 다운로드합니다.

사용자 위치 세부 정보 벌크 내보내기

이 절차를 사용하여 사용자 위치 세부 정보를 CSV 파일로 내보낼 수 있습니다. 그런 다음 벌크 관리를 사용하여 사용자 위치 세부 정보를 다른 노드 또는 클러스터로 이동할 수 있습니다.

프로시저

단계 **1** Cisco Unified CM IM and Presence 관리에서 벌크 관리 > 사용자 위치 마이그레이션 > 사용자 위치 세부 정보 내보내기를 선택합니다.

단계 **2** 사용자 위치 세부 정보 내보내기 아래의 파일 이름 필드에 CSV 파일의 이름을 입력합니다.

단계 **3** 작업 정보 아래에서 이 작업을 실행할 시기를 구성합니다.

- 즉시 실행 - 사용자 위치 세부 정보를 즉시 내보내려면 이 버튼을 선택합니다.
- 나중에 실행 - 작업 시간을 예약하려면 이 버튼을 선택합니다. 이 옵션을 사용하면 벌크 관리 > 작업 스케줄러에서 작업 스케줄러 페이지를 사용하여 이 작업을 실행할 시간을 예약해야 합니다.

단계 **4** 제출을 클릭합니다.
즉시 실행을 선택하면 내보내기 작업이 즉시 실행됩니다.

단계 **5** 내보내기 파일을 만든 후 내보낸 파일을 다운로드합니다.

a) Cisco Unified CM IM and Presence 관리에서 벌크 관리 > 파일 업로드/다운로드를 선택합니다.
b) 찾기를 클릭하고 내보내기 파일을 선택합니다.
c) 선택한 항목 다운로드를 클릭하고 액세스할 수있는 위치로 파일을 다운로드합니다.

내보내기 연락처 목록에 대한 파일 세부 정보

다음은 샘플 CSV 파일 항목입니다.

```
userA,example.com,userB,example.com,buddyB,General,0
```

BAT에서는 해당 연락처 목록을 내보낼 사용자를 찾아서 선택할 수 있습니다. 사용자 연락처 목록은 다음 형식의 CSV 파일로 내보낼 수 있습니다.

```
<User ID>,<User Domain>,<Contact ID>,<Contact Domain>,<Nickname>,<Group Name>,<State>
```

다음 표에서는 내보내기 파일의 파라미터에 대해 설명합니다.

파라미터	설명
사용자 ID	IM and Presence 서비스 사용자의 사용자 ID 참고 이 값은 사용자 IM 주소의 사용자 부분입니다.

파라미터	설명
사용자 도메인	IM and Presence 서비스 사용자의 프레즌스 도메인 참고 이 값은 사용자 IM 주소의 도메인 부분입니다. 예 **1:** bjones@example.com - bjones는 사용자 ID이고 example.com은 사용자 도메인입니다. 예 **2:** bjones@usa@example.com - bjones@usa는 사용자 ID이고 example.com은 사용자 도메인입니다.
연락처 ID	연락처 목록 항목의 사용자 ID.
연락처 도메인	연락처 목록 항목의 프레즌스 도메인
Nickname	연락처 목록 항목의 별칭. 사용자가 연락처의 별칭을 지정하지 않은 경우 별칭(Nickname) 파라미터는 공백이 됩니다.
그룹 이름	연락처 목록 항목이 추가되는 그룹의 이름 사용자의 연락처가 그룹으로 정렬되지 않은 경우 그룹 이름 필드에 기본 그룹 이름이 지정됩니다.
상태	등록 명부의 상태, 등록 명부 데이터베이스에서 이를 10진수 형식으로 저장합니다.

내보내기 비 프레즌스 연락처 목록의 파일 세부 정보

비 프레즌스 사용자 연락처 목록은 다음 형식의 CSV 파일로 내보낼 수 있습니다.

```
<User JID>,<Contact JID>,<Group Name>,<Content Type>,<Version>,<Info>
```

다음 표에서는 내보내기 파일의 파라미터에 대해 설명합니다.

파라미터	설명
사용자 JID	사용자 JID입니다. 사용자의 IM 주소입니다.
연락처 JID	사용 가능한 경우 연락처 목록 항목의 사용자 JID입니다. 그렇지 않으면 UUID입니다.
그룹 이름	연락처 목록 항목이 추가되는 그룹의 이름
컨텐츠 유형	정보 필드에 사용되는 textmime 유형 및 하위 유형입니다.

파라미터	설명
버전	정보 필드에 사용되는 콘텐츠 유형입니다.
정보	연락처 목록 항목의 연락처 정보는 vCard 형식입니다.

다음은 샘플 CSV 파일 항목입니다.

```
user2@cisco.com,ce463d44-02c3-4975-a37f-d4553e3f17e1,group01,text/directory,3,BEGIN:VCARD
ADR;TYPE=WORK:ADR\;WORK:\;\;123 Dublin rd\,\;Oranmore\;Galway\;\;Ireland
EMAIL;TYPE=X-CUSTOM1;X LABEL=Custom:testuser01@test.com N:test;user;;; NICKNAME:pizzaguy01
ORG:ABC TEL;TYPE=WORK,VOICE:5323534535 TITLE:QA VERSION:3.0 END:VCARD
```

사용자 위치 세부 정보 내보내기에 대한 파일 세부 정보

사용자 위치 세부 정보는 다음 형식의 CSV 파일로 내보낼 수 있습니다.

```
<User JID>,<Access Type>,<Create Time>,<Item ID>,<Resource ID>,<Message Text>
```

주의 파일 자체의 크기와 사용자 위치 정보 손상 위험이 있으므로 내보낸 CSV 파일을 수동으로 수정하지 않는 것이 좋습니다.

다음 표에서는 내보내기 파일의 파라미터에 대해 설명합니다.

파라미터	설명
사용자 JID	사용자 JID입니다. 사용자의 IM 주소입니다.
Access Type(액세스 유형)	액세스 유형은 사용자의 액세스 유형을 정의합니다. 액세스 유형에 대한 값은 다음과 같습니다. • W: 허용 목록 • R: 등록 명부 그룹 • O: 열기 참고 Jabber의 경우 'W'를 사용합니다.
시간 생성	작성 시간은 항목이 작성되거나 업데이트된 날짜 및 시간을 표시합니다.
항목 ID	항목 ID는 사용자에 대한 특정 레코드를 식별합니다.
리소스 ID	리소스 ID는 Jabber 인스턴스 ID입니다.
메시지 텍스트	메시지 텍스트는 사용자의 위치 정보입니다.

다음은 샘플 CSV 파일 항목입니다.

```
userA@example.com,W,2021-01-22
10:11:18.000001,7d0ec34c-458f-4fd2-9d15-58accac4af00,jabber_7151,

<geoloc
xmlns='http://jabber.org/protocol/geoloc'><description>newlocation104</description><street>104</street><mobile>0</mobile><enable>1</enable></geoloc>
```

사용자 연락처 목록 벌크 가져오기

최대 연락처 목록 크기 확인

IM and Presence 서비스의 최대 연락처 목록 크기 및 최대 감시자 설정을 확인하십시오. 시스템 기본값은 최대 연락처 목록 크기 200, 최대 관찰자 수 200입니다.

사용자 연락처 목록을 가져오는 동안에는 최대 연락처 목록 크기 및 최대 관찰자 수를 무제한으로 설정하는 것이 좋습니다. 이 단계는 BAT를 사용하여 연락처 목록을 가져올 때 데이터 손실 없이 최대 연락처 목록 크기를 초과하더라도 마이그레이션된 각 사용자 연락처 목록을 완전히 가져옵니다. 모든 사용자를 마이그레이션한 후 최대 연락처 목록 크기 및 최대 관찰자 수를 원하는 값으로 다시 설정할 수 있습니다.

연락처를 가져오려는 사용자가 포함된 클러스터에 대해서만 최대 연락처 목록 크기를 확인하면 됩니다. 프레즌스 설정을 변경하면 변경 사항이 클러스터의 모든 노드에 적용됩니다. 따라서 클러스터 내 IM and Presence 데이터베이스 게시자 노드에서만 이러한 설정을 변경해야 합니다.

다음에 수행할 작업

입력 파일 업로드, 404 페이지

입력 파일 업로드

다음 절차에서는 연락처 목록과 비 프레즌스 연락처 목록에 대해 BAT를 사용하여 CSV 입력 파일을 업로드하는 방법에 대해 설명합니다.

시작하기 전에

최대 연락처 목록 크기 확인, 404 페이지

프로시저

단계 **1** **Cisco Unified CM IM and Presence** 관리에서 벌크 관리 > 파일 업로드/다운로드를 선택합니다.

단계 **2** 새로 추가를 클릭합니다.

단계 **3** 찾아보기를 클릭하고 CSV 파일을 찾아 선택합니다.

단계 **4** 목표를 설정하는 경우:

- 연락처 목록에 대한 입력 파일을 업로드하려면 연락처 목록을 선택합니다. 사용자 연락처 목록 입력 파일에 대한 자세한 내용은 가져오기 연락처 목록에 대한 파일 세부 정보, 405 페이지의 내용을 참조하십시오.

- 비 프레즌스 연락처 목록에 대한 입력 파일을 업로드하려면 비 프레즌스 연락처 목록을 선택합니다. 비 프레즌스 사용자 연락처 목록 입력 파일에 대한 자세한 내용은 비 프레즌스 연락처 가져오기에 대한 파일 세부 정보, 408 페이지의 내용을 참조하십시오.
- 사용자 위치 마이그레이션 세부 정보에 대한 입력 파일을 업로드하려면 사용자 위치 마이그레이션을 선택합니다. 사용자 위치 세부 정보 입력 파일에 대한 자세한 내용은 사용자 위치 세부 정보 가져오기에 대한 파일 세부 정보, 408 페이지의 내용을 참조하십시오.

단계 **5** 트랜잭션 유형의 경우: 트랜잭션 유형으로 선택합니다.

- 연락처 목록에 대한 입력 파일을 업로드하려면 사용자 연락처 가져오기 - 파일 사용자 지정을 선택합니다.
- 비 프레즌스 연락처 목록에 대한 입력 파일을 업로드하려는 경우 사용자의 비 프레즌스 연락처 가져오기를 선택합니다.
- 사용자 위치 마이그레이션 세부 정보에 대한 입력 파일을 업로드하는 경우 사용자 위치 세부 정보 가져오기를 선택합니다.

단계 **6** 저장을 클릭하여 파일을 업로드합니다.

다음에 수행할 작업

새 벌크 관리 작업 만들기, 409 페이지

가져오기 연락처 목록에 대한 파일 세부 정보

입력 파일은 다음 형식의 CSV 파일이어야 합니다.

```
<User ID>,<User Domain>,<Contact ID>,<Contact Domain>,<Nickname>,<Group Name>,<State>
```

다음은 샘플 CSV 파일 항목입니다.

```
userA,example.com,userB,example.com,buddyB,General,0
```

다음 표에서는 가져오기 파일의 파라미터에 대해 설명합니다.

파라미터	설명
사용자 ID	필수 파라미터입니다. IM and Presence 서비스 사용자의 사용자 ID 최대 132자까지 가능합니다. 참고 • 이 값은 사용자 IM 주소의 사용자 부분입니다. • 다음 문자가 포함된 사용자 ID에 대해서는 JSM 세션이 생성되지 않습니다. º ª ² ¼ ¾ - ³ µ ¹ ½ ß ´ ¨ ¸ ¯ Æ

파라미터	설명
사용자 도메인	필수 파라미터입니다. IM and Presence 서비스 사용자의 프레즌스 도메인 최대 128자까지 가능합니다. 참고 이 값은 사용자 IM 주소의 도메인 부분입니다. 예 **1**: bjones@example.com - bjones는 사용자 ID이고 example.com은 사용자 도메인입니다. 예 **2**: bjones@usa@example.com - bjones@usa는 사용자 ID이고 example.com은 사용자 도메인입니다.
연락처 ID	필수 파라미터입니다. 연락처 목록 항목의 사용자 ID. 최대 132자까지 가능합니다.
연락처 도메인	필수 파라미터입니다. 연락처 목록 항목의 프레즌스 도메인 도메인 이름 형식에는 다음 제한이 적용됩니다. • 128자보다 작거나 같아야 합니다. • 숫자, 대/소문자 및 하이픈(-)만 사용할 수 있습니다. • 시작 또는 끝에는 하이픈(-)을 사용할 수 없습니다. • 레이블 길이는 63자 이하여야 합니다. • 최상위 도메인에는 문자만 사용할 수 있으며 2자 이상이어야 합니다.
Nickname	연락처 목록 항목의 별칭. 최대 255자까지 가능합니다.
그룹 이름	그룹 이름은 필수 파라미터입니다. 연락처 목록 항목이 추가되는 그룹의 이름 최대 255자까지 가능합니다.
상태	등록 명부의 상태, 등록 명부 데이터베이스에서 이를 10진수 형식으로 저장합니다.

비 프레즌스 연락처 가져오기에 대한 파일 세부 정보

입력 파일은 다음 형식의 CSV 파일이어야 합니다.

```
<User JID>,<Contact JID>,<Group Name>,<Content Type>,<Version>,<Info>
```

다음은 샘플 CSV 파일 항목입니다.

```
user2@cisco.com,ce463d44-02c3-4975-a37f-d4553e3f17e1,group01,text/directory,3,BEGIN:VCARD
ADR;TYPE=WORK:ADR\;WORK:\;\;123 Dublin rd\,\;Oranmore\;Galway\;\;Ireland
EMAIL;TYPE=X-CUSTOM1;X LABEL=Custom:testuser01@test.com N:test;user;;; NICKNAME:pizzaguy01
ORG:ABC TEL;TYPE=WORK,VOICE:5323534535 TITLE:QA VERSION:3.0 END:VCARD
```

주의 파일 자체의 크기와 vCard 정보 손상 위험이 있으므로 CSV 파일을 수동으로 수정하지 않는 것이 좋습니다.

다음 표에서는 비 프레즌스 연락처에 대한 입력 파일의 파라미터에 대해 설명합니다.

파라미터	설명
사용자 JID	사용자 JID입니다. 사용자의 IM 주소입니다.
연락처 JID	사용 가능한 경우 연락처 목록 항목의 사용자 JID입니다. 그렇지 않으면 UUID입니다.
그룹 이름	연락처 목록 항목이 추가되는 그룹의 이름
컨텐츠 유형	정보 필드에 사용되는 textmime 유형 및 하위 유형입니다.
버전	정보 필드에 사용되는 콘텐츠 유형입니다.
정보	연락처 목록 항목의 연락처 정보는 vCard 형식입니다.

사용자 위치 세부 정보 가져오기에 대한 파일 세부 정보

입력 파일은 다음 형식의 CSV 파일이어야 합니다.

```
<User JID>,<Access Type>,<Item ID>,<Create Time>,<Resource ID>,<Message Text>
```

다음은 샘플 CSV 파일 항목입니다.

```
userA@example.com,W,7d0ec34c-458f-4fd2-9d15-58accac4af00,2021-01-22
10:11:18.000001,jabber_7151,

<geoloc
xmlns='http://jabber.org/protocol/geoloc'><description>newlocation104</description><street>104</street><mobile>0</mobile><enable>1</enable></geoloc>
```

주의 파일 자체의 크기와 사용자 위치 정보 손상 위험이 있으므로 CSV 파일을 수동으로 수정하지 않는 것이 좋습니다.

다음 표에서는 사용자 위치 정보에 대한 입력 파일의 파라미터에 대해 설명합니다.

파라미터	설명
사용자 JID	필수 파라미터입니다. 사용자 JID는 사용자의 IM 주소입니다. 최대 255자까지 가능합니다.
Access Type(액세스 유형)	필수 파라미터입니다. 액세스 유형은 사용자의 액세스 유형을 정의합니다. 최대 128자까지 가능합니다. 액세스 유형에 대한 값은 다음과 같습니다. • W: 허용 목록 • R: 등록 명부 그룹 • O: 열기 참고 Jabber의 경우 'W'를 사용합니다.
항목 ID	필수 파라미터입니다. 항목 ID는 사용자에 대한 특정 레코드를 식별합니다. 항목 ID 값은 '무시' 또는 영숫자 값이어야 합니다. 연락처 목록 항목의 사용자 ID. 최대 50자까지 가능합니다.
시간 생성	필수 파라미터입니다. 작성 시간은 항목이 작성되거나 업데이트된 날짜 및 시간을 표시합니다. 최대 26자까지 가능합니다.
리소스 ID	필수 파라미터입니다. 리소스 ID는 Jabber 인스턴스 ID입니다. 최대 1,023자까지 가능합니다.
메시지 텍스트	필수 파라미터입니다. 메시지 텍스트는 사용자의 위치 정보입니다. 최대 30,000자까지 가능합니다.

새 벌크 관리 작업 만들기

연락처 목록 및 비 프레즌스 연락처 목록에 대한 새로운 벌크 관리 작업을 만듭니다.

시작하기 전에

입력 파일 업로드, 404 페이지

프로시저

단계 **1** **Cisco Unified CM IM and Presence** 관리에서:

- 연락처 목록에 대해 새로운 벌크 관리 작업을 만들려면 벌크 관리 > 연락처 목록 > 업데이트를 선택합니다.
- 연락처 목록에 대해 새로운 벌크 관리 작업을 만들려면 벌크 관리 > 연락처 비 프레즌스 목록 > 비 프레즌스 연락처 목록을 선택합니다.
- 사용자 위치 마이그레이션에 대한 새 벌크 관리 작업을 생성하려면 벌크 관리 > 사용자 위치 마이그레이션 > 사용자 위치 세부 정보 가져오기를 선택합니다.

단계 **2** 파일 이름 드롭다운 목록에서 가져올 파일을 선택합니다.

단계 **3** 작업 설명 필드에 이 벌크 관리 작업에 대한 설명을 입력합니다.

단계 **4** 다음 중 하나를 선택합니다.

- 벌크 관리 작업을 즉시 실행하려면 즉시 실행을 클릭합니다.
- 벌크 관리 작업을 실행할 시간을 예약하려면 나중에 실행을 클릭합니다. BAT에서 작업을 예약하는 방법에 대한 자세한 내용은 Cisco Unified CM IM and Presence 관리의 온라인 도움말을 참조하십시오.

단계 **5** 제출을 클릭합니다. 작업을 즉시 실행하도록 선택한 경우 제출을 클릭하면 작업이 바로 실행됩니다.

다음에 수행할 작업

벌크 관리 작업의 결과 확인, 410 페이지

벌크 관리 작업의 결과 확인

벌크 관리 작업이 완료되면 IM and Presence 서비스 BAT 도구는 연락처 목록 가져오기 작업의 결과를 로그 파일에 기록합니다. 로그 파일에는 다음 정보가 포함됩니다.

- 성공적으로 가져온 연락처의 수
- 연락처 가져오기를 시도하는 동안 발생한 내부 서버 오류의 수
- 가져오지 못한(무시된) 연락처의 수. 로그 파일 끝에는 무시된 각 연락처의 이유가 나열됩니다. 연락처를 가져오지 못한 이유는 다음과 같습니다.
  - 잘못된 형식 - 필수 필드가 누락되었거나 비어 있는 등 행 형식이 잘못되었습니다.
  - 잘못된 연락처 도메인 - 연락처 도메인의 형식이 잘못되었습니다. 연락처 도메인의 유효한 형식은 사용자 연락처 목록 벌크 가져오기와 관련된 항목을 참조하십시오.

- 자신을 연락처로 추가할 수 없음 - 연락처가 사용자 자신인 경우에는 사용자의 연락처를 가져올 수 없습니다.
- 사용자 연락처 목록이 제한 초과 - 최대 연락처 목록 크기에 도달하여 해당 사용자에 대해 연락처를 더 이상 가져올 수 없습니다.
- 사용자가 로컬 노드에 할당되지 않음 - 사용자가 로컬 노드에 할당되지 않았습니다.

- BAT 작업 조기 종료의 원인이 된 오류 때문에 처리되지 않은, CSV 파일의 연락처 수. 이 오류는 거의 발생하지 않습니다.

이 로그 파일에 액세스하려면 다음 절차를 완료하십시오.

시작하기 전에

새 벌크 관리 작업 만들기, 409 페이지

프로시저

단계 **1** **Cisco Unified CM IM and Presence** 관리에서 벌크 관리 > 작업 스케줄러를 선택합니다.

단계 **2** 찾기를 클릭하고 연락처 목록 가져오기 작업의 작업 ID를 선택합니다.

단계 **3** 로그를 열려면 로그 파일 이름 링크를 클릭합니다.

34 장

시스템 문제 해결

문제 해결 개요

이 장의 절차를 사용하여 IM and Presence 구축 관련 문제를 해결하십시오. IM and Presence 서비스 구축을 통해 다음을 수행할 수 있습니다.

- 명령줄 인터페이스(CLI)를 사용하여 문제점을 확인하기 위해 점검할 수 있는 추적 로그를 빌드합니다.
- 진단을 실행하여 시스템 문제를 확인합니다.
- 시스템 상태를 확인하려면 시스템 문제 해결 도구 실행.
- 중복 디렉터리 URI 문제를 해결합니다.

시스템 문제 해결 도구 실행

IM and Presence 서비스 구축 문제를 진단하려면 문제 해결 도구를 실행하십시오. 문제 해결 도구는 구축시 다음과 같은 다양한 문제를 자동으로 확인합니다.

- 시스템 문제
- 동기화 에이전트 문제
- Presence 엔진 문제
- SIP 프록시 문제
- 일정 관리 문제

- 클러스터 간 문제
- 토폴로지 문제
- Cisco Jabber 중복 할당
- 외부 데이터베이스 항목
- 타사 준수 서버
- 타사 LDAP 연결
- LDAP 연결
- XCP 상태
- 사용자 구성

프로시저

단계 **1** Cisco Unified CM IM and Presence 관리에서 진단 > 시스템 문제 해결 도구를 선택합니다.
문제 해결 도구는 시스템에 대해 일련의 자동 검사를 실행합니다. 시스템 구성 문제 해결 도구 창에 결과가 표시됩니다.

단계 **2** 문제 해결 도구에서 강조하는 모든 문제를 해결합니다.

진단 실행

설정 하 고 작동 시스템을 관리 하는 경우 시스템의 일반 실행에 영향을 줍니다 문제가 발생할 수 있습니다. IM and Presence 진단 도구를 사용하여 이러한 문제의 근본 원인을 파악할 수 있습니다.

IM and Presence 서비스의 진단 도구에 액세스하려면 이 절차를 사용하십시오.

이 도구는 **Cisco Unified CM IM and Presence** 관리에서 진단을 클릭하고 다음 옵션 중 하나를 선택하여 액세스할 수 있습니다.

프로시저

단계 **1** **Cisco Unified CM IM and Presence** 관리에서 진단을 선택합니다.

단계 **2** 드롭다운 목록에서 사용할 진단 도구를 클릭합니다.

이러한 도구의 목적에 대한 자세한 내용은 진단 도구 개요를 참조하십시오.

진단 도구 개요

진단 도구	목적
□시스템대시보드	디바이스 수, 사용자 수, 연락처 같은 사용자별 데이터 및 기본 확장 등 이러한 시스템 구성 요소의 요약 데이터 보기를 포함하여 IM and Presence 서비스 시스템 상태의 스냅샷을 얻으려면 시스템 대시보드를 사용합니다.
시스템 구성 문제 해결 도구	초기 구성 후 또는 구성을 변경할 때마다 IM and Presence 서비스 구성을 진단하려면 시스템 구성 문제 해결 도구를 사용합니다. 문제 해결사는 문제 해결 도구는 IM and Presence 서비스 클러스터 및 Cisco Unified Communications Manager 클러스터에서 일련의 테스트를 수행하여 IM and Presence 서비스 구성의 유효성을 검사합니다. 문제 해결 도구가 테스트를 완료한 후 각 테스트에 대해 세 가지 가능한 상태 중 하나를 보고합니다. • 테스트 통과 • 테스트 실패 • 가능한 구성 문제를 나타내는 테스트 알림 각 테스트에 실패하거나 알림이 발생하는 경우 문제 해결 도구는 문제점 및 가능한 솔루션에 대한 설명을 제공합니다. 테스트 오류 또는 테스트 경고의 경우 솔루션 열에서 해결 링크를 클릭하여 문제 해결 도구가 문제를 발견한 Cisco Unified Communications Manager IM and Presence 관리 창으로 이동합니다. 발견한 구성 오류를 해결하고 문제 해결 도구로 돌아갑니다.

추적 로그를 사용하여 문제 해결

추적을 사용하여 IM and Presence 서비스 및 기능과 관련된 시스템 문제를 해결합니다. 다양한 서비스, 기능 및 시스템 구성 요소에 대해 자동화된 시스템 추적을 구성할 수 있습니다. 결과는 Cisco Unified 실시간 모니터링 도구를 사용하여 찾아보고 볼 수 있는 시스템 로그에 저장됩니다. 또는 명령줄 인터

페이스를 사용하여 시스템 로그 파일의 하위 집합을 가져와서 추가 분석을 위해 자신의 PC 또는 노트북에 업로드할 수 있습니다.

추적을 사용하려면 먼저 추적을 위해 시스템을 구성해야 합니다. 시스템 추적을 구성하는 방법에 대한 자세한 내용은 *Cisco Unified* 서비스 가용성 관리 설명서의 "추적" 장을 참조하십시오.

추적이 구성되면 다음 두 가지 방법 중 하나를 사용하여 추적 파일의 내용을 볼 수 있습니다.

- 실시간 모니터링 도구 - 실시간 모니터링 도구를 사용하면 시스템 추적의 결과로 생성 된 개별 로그 파일을 찾아보고 볼 수 있습니다. 실시간 모니터링 도구를 사용하는 방법에 대한 자세한 내용은 *Cisco Unified* 실시간 모니터링 도구 관리 설명서를 참조하십시오.
- 명령줄 인터페이스 (CLI) - 시스템 추적이 구성된 경우 CLI를 사용하여 시스템 로그에서 사용자 지정 추적을 작성합니다. CLI를 사용하여 사용자 지정 추적 파일에 포함시키려는 특정 요일을 지정할 수 있습니다. CLI는 시스템에서 관련 추적 파일을 가져와서 압축된 zip 파일에 저장합니다. 이 압축 파일을 PC 또는 랩톱에 복사하여 추가 분석을 할 수 있으므로 시스템에서 로그를 덮어 쓰지 않습니다.

  이 섹션에 나오는 후속 표와 작업에서는 CLI 명령을 사용하여 IM and Presence 서비스에 대한 추적 로그 파일을 작성하는 방법을 설명합니다.

추적을 통한 일반 IM and Presence 문제

다음 표는 IM and Presence 서비스의 일반적인 문제점과 문제를 해결하기 위해 실행할 수있는 추적을 나열합니다.

표 ***47:*** 일반 ***IM and Presence*** 문제 해결

문제...	이러한 서비스를 위한 추적 보기	추가 지침
로그인 및 인증 추적	클라이언트 프로파일 에이전트 Cisco XCP 연결 관리자 Cisco XCP 라우터 Cisco XCP 인증 서비스 Cisco Tomcat Security Log	로그 및 출력 위치를 작성하는 CLI 명령은 CLI를 통한 일반 추적, 419 페이지의 내용을 참조하십시오.
사용 가능성 상태	Cisco XCP 연결 관리자 Cisco XCP 라우터 Cisco Presence 엔진	로그 및 출력 위치를 작성하는 CLI 명령은 CLI를 통한 일반 추적, 419 페이지의 내용을 참조하십시오.
IM 보내기 및 받기	Cisco XCP 연결 관리자 Cisco XCP 라우터	로그 및 출력 위치를 작성하는 CLI 명령은 CLI를 통한 일반 추적, 419 페이지의 내용을 참조하십시오.

문제...	이러한 서비스를 위한 추적 보기	추가 지침
연락처 목록	Cisco XCP 연결 관리자 Cisco XCP 라우터 Cisco Presence 엔진	로그 및 출력 위치를 작성하는 CLI 명령은 CLI를 통한 일반 추적, 419 페이지의 내용을 참조하십시오.
채팅방	Cisco XCP 연결 관리자 Cisco XCP 라우터 Cisco XCP 텍스트 전화회의 관리자	로그 및 출력 위치를 작성하는 CLI 명령은 CLI를 통한 일반 추적, 419 페이지의 내용을 참조하십시오.
파티션된 도메인간 페더레이션	Cisco XCP 라우터 Cisco XCP SIP 페더레이션 연결 관리자 Cisco SIP Proxy Cisco Presence 엔진	로그 및 출력 위치를 작성하는 CLI 명령은 CLI를 통한 일반 추적, 419 페이지의 내용을 참조하십시오. 참고 SIP 메시지 교환을 보려면 Cisco SIP Proxy 디버그 로깅이 필요합니다.
XMPP 기반 도메인 간 페더레이션 연락처에 대한 가용성 및 IM	Cisco XCP 연결 관리자 Cisco XCP 라우터 Cisco Presence 엔진 Cisco XCP XMPP 페더레이션 연결 관리자	로그 및 출력 위치를 작성하는 CLI 명령은 CLI를 통한 일반 추적, 419 페이지의 내용을 참조하십시오. XMPP 페더레이션이 활성화된 각 IM and Presence 노드에서 이 추적을 수행하십시오.
SIP 도메인 간 페더레이션 연락처에 대한 가용성 및 IM	Cisco XCP 연결 관리자 Cisco XCP 라우터 Cisco Presence 엔진 Cisco SIP Proxy Cisco XCP SIP 페더레이션 연결 관리자	로그 및 출력 위치를 작성하는 CLI 명령은 CLI를 통한 일반 추적, 419 페이지의 내용을 참조하십시오.
일정 관리 추적	Cisco Presence 엔진	로그 및 출력 위치를 작성하는 CLI 명령은 CLI를 통한 일반 추적, 419 페이지의 내용을 참조하십시오.

문제...	이러한 서비스를 위한 추적 보기	추가 지침
클러스터 간 동기화 추적 및 클러스터 간 문제 해결 도구	Cisco 클러스터 간 동기화 에이전트 Cisco AXL 웹 서비스 Cisco Tomcat Security Log Cisco Syslog Agent	진단 > 시스템 문제 해결 도구에서 시스템 문제 해결 도구를 실행하여 클러스터 간 오류가 있는지 확인하십시오.
SIP 페더레이션 추적	Cisco SIP Proxy Cisco XCP 라우터 Cisco XCP SIP 페더레이션 연결 관리자	로그 및 파일 출력 위치를 작성하는 CLI 명령은 CLI를 통한 일반 추적, 419 페이지의 내용을 참조하십시오.
XMPP 페더레이션 추적	Cisco XCP 라우터 Cisco XCP XMPP 페더레이션 연결 관리자	로그 및 파일 출력 위치를 작성하는 CLI 명령은 CLI를 통한 일반 추적, 419 페이지의 내용을 참조하십시오.
높은 CPU 및 낮은 VM 경고 문제 해결	Cisco XCP 라우터 Cisco XCP SIP 페더레이션 연결 관리자 Cisco SIP Proxy Cisco Presence 엔진 Cisco Tomcat Security Log Cisco Syslog Agent	추가 문제 해결을 위해 다음 CLI 명령을 실행하십시오. • `show process using-most cpu` • `show process using-most memory` • `utils dbreplication runtimestate` • `utils service list` 다음 CLI를 실행하여 RIS(실시간 정보 서비스) 데이터를 가져옵니다. • `file get activelog cm/log/ris/csv` 런타임 상태 및 시스템 상태에 대한 정보를 로컬 시스템 로그에 제공하도록 Cisco Unified IM and Presence 서비스 가용성 알람을 설정할 수도 있습니다.

CLI를 통한 일반 추적

명령 줄 인터페이스를 통해 추적 로그 파일을 작성하여 시스템 문제를 해결하십시오. CLI를 사용하면 추적을 실행할 구성 요소를 선택하고 로그 파일에 포함하려는 오늘 이전의 일 수인 <duration>을 지정할 수 있습니다.

다음 두 표에는 추적 로그 파일과 로그 출력 위치를 작성하는 데 사용할 수 있는 CLI 명령이 들어 있습니다.

- IM and Presence Service
- IM and Presence 기능

참고 CLI는 Cisco Unified RTMT(실시간 모니터링 도구)로 볼 수 있는 동일한 개별 추적 파일의 하위 집합을 가져 오지만 단일의 압축된 zip 파일로 그룹화하고 저장합니다. RTMT 추적은 RTMT를 통한 일반 추적, 423 페이지의 내용을 참조하십시오.

표 ***48: CLI***를 사용한 ***IM and Presence*** 서비스에 대한 일반 추적

서비스	로그를 작성하기 위한 **CLI**	**CLI** 출력 파일
Cisco 감사 로그	file build log cisco_audit_logs <duration>	`/epas/trace/log_cisco_audit_logs_*.tar.gz`
Cisco 클라이언트 프로파일 에이전트	file build log cisco_client_profile_agent <duration>	`/epas/trace/log_cisco_client_profile_agent_*.tar.gz`
Cisco Cluster Manager	file build log cisco_config_agent <duration>	`/epas/trace/log_cisco_cluster_manager_*.tar.gz`
Cisco 구성 에이전트	file build log cisco_config_agent<duration>	`/epas/trace/log_cisco_config_agent_*.tar.gz`
Cisco Database Layer Monitor	file build log cisco_database_layer_monitor <duration>	`/epas/trace/log_cisco_database_layer_monitor_*.tar.gz`
Cisco 클러스터 간 동기화 에이전트	file build log cisco_inter_cluster_sync_agent <duration>	`/epas/trace/log_cisco_inter_cluster_sync_agent_*.tar.gz`
Cisco OAM 에이전트	file build log cisco_oam_agent <duration>	`/epas/trace/log_cisco_oam_agent_*.gz`
Cisco Presence 엔진	file build log cisco_presence_engine <duration>	`/epas/trace/log_cisco_presence_engine_*.tar.gz`

서비스	로그를 작성하기 위한 **CLI**	**CLI** 출력 파일
Cisco RIS(실시간 정보 서비스) 데이터 컬렉터	file build log cisco_ris_data_collector <duration>	/epas/trace/log_cisco_ris_data_collector_*.tar.gz
Cisco 서비스 관리	file build log cisco_service_management <duration>	/epas/trace/log_cisco_service_management_*.tar.gz
Cisco SIP Proxy	file build log cisco_sip_proxy <duration>	/epas/trace/log_cisco_sip_proxy_*.tar.gz
Cisco Sync Agent	file build log cisco_sync_agent <duration>	/epas/trace/log_cisco_sync_agent_*.tar.gz
Cisco XCP 구성 관리자	file build log cisco_xcp_config_mgr <duration>	/epas/trace/log_cisco_xcp_config_mgr_*.tar.gz
Cisco XCP 라우터	file build log cisco_xcp_router <duration>	/epas/trace/log_cisco_xcp_router_*.tar.gz

표 ***49: CLI***를 사용한 ***IM and Presence*** 기능에 대한 일반 추적

기능 이름	로그를 작성하기 위한 **CLI**	**CLI** 출력 파일
관리 GUI	file build log admin_ui <duration>	/epas/trace/log_admin_ui_*.tar.gz
벌크 관리	file build log bat <duration>	/epas/trace/log_bat_*.tar.gz
동기식 HTTP를 통한 양방향 스트림	file build log bosh <duration>	/epas/trace/log_bosh_*.tar.gz
인증서	file build log certificates <duration>	/epas/trace/log_certificates_*.tar.gz
구성 에이전트 코어	file build log cfg_agent_core <duration>	/epas/trace/log_cfg_agent_core_*.tar.gz
Customer Voice Portal	file build log cvp <duration>	/epas/trace/log_cvp_*.tar.gz
디렉토리 그룹	file build log directory_groups <duration>	/epas/trace/log_directory_groups_*.tar.gz
재해 복구	file build log disaster_recovery <duration>	/epas/trace/log_disaster_recovery_*.tar.gz
유연한 IM 주소	file build log flexable_im_address <duration>	/epas/trace/log_flexible_im_address_*.tar.gz

기능 이름	로그를 작성하기 위한 **CLI**	**CLI** 출력 파일
일반 코어	file build log general_core <duration>	/epas/trace/log_general_core_*.tar.gz
고가용성	file build log ha <duration>	/epas/trace/log_ha_*.tar.gz
높은 CPU	file build log high_cpu <duration>	/epas/trace/log_high_cpu_*.tar.gz
하이 메모리	file build log high_memory <duration>	/epas/trace/log_high_memory_*.tar.gz
인스턴트 메시징 데이터베이스 코어	file build log imdb <duration>	/epas/trace/log_imdb_core_*.tar.gz
인터클러스터 피어링	file build log inter_cluster <duration>	/epas/trace/log_inter_cluster_*.tar.gz
관리되는 파일 전송	file build log managed_file_transfer <duration>	/epas/trace/log_managed_file_transfer_*.tar.gz
Microsoft Exchange	file build log msft_exchange <duration>	/epas/trace/log_msft_exchange_*.tar.gz
메시지 아카이버	file build log msg_archiver <duration>	/epas/trace/log_msg_archiver_*.tar.gz
Presence 엔진 코어	file build log pe_core <duration>	/epas/trace/log_pe_core_*.tar.gz
Presence and IM 메시지 교환	file build log presence_im_exchange <duration>	/epas/trace/log_presence_im_exchange_*.tar.gz
SIP 로그인 문제	file build log pws <duration>	/epas/trace/log_pws_*.tar.gz
보안 취약점	file build log sec_vulnerability <duration>	/epas/trace/log_sec_vulnerability_*.tar.gz
서비스 가용성 GUI	file build log serviceability_ui <duration>	/epas/trace/log_serviceability_ui_*.tar.gz
SIP 도메인 간 페더레이션	file build log sip_inter_federation <duration>	/epas/trace/log_sip_inter_federation_*.tar.gz
SIP 파티션된 도메인간 페더레이션	file build log sip_partitioned_federation <duration>	/epas/trace/log_sip_partitioned_federation_*.tar.gz
SIP 프록시 코어	file build log sipd_core <duration>	/epas/trace/log_sipd_core_*.tar.gz

기능 이름	로그를 작성하기 위한 CLI	CLI 출력 파일
영구 채팅 고가용성	file build log tc_ha <duration>	/epas/trace/log_tc_ha_*.tar.gz
영구 채팅	file build log text_conference <duration>	/epas/trace/log_text_conference_*.tar.gz
업그레이드 문제	file build log upgrade_issues <duration>	/epas/trace/log_upgrade_issues_*.tar.gz
사용자 연결	file build log user_connectivity <duration>	/epas/trace/log_user_connectivity_*.tar.gz
등록 명부	file build log user_rosters <duration>	/epas/trace/log_user_rosters_*.tar.gz
XCP 라우터 코어	file build log xcp_core <duration>	/epas/trace/log_xcp_core_*.tar.gz
XMPP 도메인 간 페더레이션	file build log xmpp_inter_federation <duration>	/epas/trace/log_xmpp_inter_federation_*.tar.gz
구축 정보	file build log deployment_info <duration>	/epas/trace/log_deployment_info_*.tar.gz

CLI를 통한 실행 추적

명령줄 인터페이스(CLI)를 통해 사용자 지정 추적 파일을 작성하려면 이 절차를 사용하십시오. CLI를 사용하면 duration 파라미터를 통해 추적에 포함시키려는 날짜 수를 지정할 수 있습니다. CLI가 시스템 로그의 하위 집합을 가져옵니다.

참고 파일을 전송할 때만 SFTP 서버를 사용해야 합니다.

시작하기 전에

시스템에 맞게 추적을 구성해야 합니다. 추적 설정에 대한 자세한 내용은 *Cisco Unified* 서비스 가용성 관리 설명서의 "추적" 장을 참조하십시오.

실행할 수 있는 추적 목록은 CLI를 통한 일반 추적, 419 페이지의 내용을 검토하십시오.

프로시저

단계 **1** 명령줄 인터페이스에 로그인합니다.

단계 **2** 로그를 빌드하려면 `file build log <name of service> <duration>` CLI 명령어를 실행하십시오. 여기서 duration(지속 시간)은 추적에 포함할 일 수입니다.

예를 들어, 지난 주 동안 Cisco Cluster Manager 로그를 보려면 `file build log cisco_cluster_manager 7`을 사용합니다.

단계 **3** 로그를 가져오려면 `file get activelog <log filepath>` CLI 명령어를 실행하여 추적 파일을 가져옵니다.

예를 들어, **file get activelog epas/trace/log_cisco_cluster_manager__2016-09-30-09h41m37s.tar.gz**.

단계 **4** 시스템을 안정적으로 유지하려면 검색한 후에 로그를 삭제합니다. 로그를 삭제하려면 `file delete activelog <filepath>` 명령을 실행합니다.

예를 들어, `file delete activelog epas/trace/log_cisco_cluster_manager__2016-09-30-09h41m37s.tar.gz`.

RTMT를 통한 일반 추적

다음 표에는 IM and Presence 서비스 노드에서 수행할 수 있는 공통 추적 및 결과 로그 파일이 나열되어 있습니다. RTMT(실시간 모니터링 도구)를 사용하여 추적 로그 파일을 볼 수 있습니다.

참고 CLI를 사용하여 RTMT로 볼 수 있는 동일한 개별 추적 파일의 하위 집합을 가져 오지만 단일의 압축된 zip 파일로 그룹화하고 저장할 수 있습니다. CLI 추적은 CLI를 통한 일반 추적, 419 페이지의 내용을 참조하십시오.

표 ***50: IM and Presence*** 노드를 위한 공통 추적 및 로그 파일

서비스	추적 로그 파일 이름
Cisco AXL 웹 서비스	`/tomcat/logs/axl/log4j/axl*.log`
Cisco 클러스터 간 동기화 에이전트	`/epas/trace/cupicsa/log4j/icSyncAgent*.log`
Cisco Presence 엔진	`/epas/trace/epe/sdi/epe*.txt.gz`
Cisco SIP Proxy	`/epas/trace/esp/sdi/esp*.txt.gz`
Cisco Syslog Agent	`/cm/trace/syslogmib/sdi/syslogmib*.txt`
Cisco Tomcat Security Log	`/tomcat/logs/security/log4/security*.log`
Cisco XCP 인증 서비스	`/epas/trace/xcp/log/auth-svc-1*.log.gz`
Cisco XCP 구성 관리자	`/epas/trace/xcpconfigmgr/log4j/xcpconfigmgr*.log`
Cisco XCP 연결 관리자	`/epas/trace/xcp/log/client-cm-1*.log.gz`
Cisco XCP 라우터	`/epas/trace/xcp/log/rtr-jsm-1*.log.gz`

서비스	추적 로그 파일 이름
Cisco XCP SIP 페더레이션 연결 관리자	/epas/trace/xcp/log/sip-cm-3*.log
Cisco XCP 텍스트 전화회의 관리자	/epas/trace/xcp/log/txt-conf-1*.log.gz
Cisco XCP XMPP 페더레이션 연결 관리자	/epas/trace/xcp/log/xmpp-cm-4*.log
클러스터 관리자	/platform/log/clustermgr*.log
Cisco CPA(클라이언트 프로파일 에이전트)	/tomcat/logs/epassoap/log4j/EPASSoap*.log
dbmon	/cm/trace/dbl/sdi/dbmon*.txt

사용자 ID 및 디렉터리 URI 오류 문제 해결

중복 사용자 ID 오류 수신

문제 중복된 사용자 ID가 있다는 알람을 수신했으며, 해당 사용자의 연락처 정보를 수정해야 합니다.

해결 방법 다음 단계를 수행하십시오.

1. **utilsusersvalidate{ all | userid | uri }** CLI 명령어를 사용하여 전체 사용자 목록을 생성합니다. CLI 명령 사용에 대한 자세한 내용은 *Cisco Unified Communications Solutions*용 명령줄 인터페이스 설명서를 참조하십시오.

   UserID가 표시되고 그 뒤에 중복된 UserID가 있는 서버의 목록이 표시됩니다. 다음의 샘플 CLI 출력은 출력 중 UserID 오류를 보여줍니다.

   ```
   Users with Duplicate User IDs
   ---------------------------------------------
    User ID: user3
     Node Name
     cucm-imp-1
     cucm-imp-2
   ```

2. 두 개의 서로 다른 클러스터에 동일한 사용자가 할당된 경우 클러스터 중 하나에서 사용자의 할당을 취소합니다.
3. 서로 다른 클러스터의 서로 다른 사용자에게 동일한 사용자 ID가 할당된 경우 사용자 중 한 명의 UserID 값을 변경하여 중복이 발생하지 않도록 합니다.
4. 사용자 정보가 잘못되었거나 비어 있으면 Cisco Unified Communications Manager 관리 GUI를 사용하여 해당 사용자의 사용자 ID 정보를 수정합니다.

5. 최종 사용자 설정 창(사용자 관리 > 최종 사용자)를 사용하여 Cisco 통합 커뮤니케이션 매니저에서 사용자 레코드를 수정하여 모든 사용자에게 유효한 사용자 ID 또는 디렉터리 URI 값을 갖게 할 수 있습니다. 자세한 내용은 *Cisco Unified Communications Manager* 관리 설명서를 참조하십시오.

참고 사용자 프로파일의 사용자 ID 및 디렉터리 URI 필드를 LDAP 디렉터리로 매핑할 수 있습니다. 이 경우 LDAP 디렉터리 서버에 수정을 적용하십시오.

6. 중복된 사용자 ID 오류가 더 이상 표시되지 않는지 확인하기 위해 CLI 명령을 실행하여 사용자를 다시 검증합니다.

중복된 또는 잘못된 디렉터리 **URI** 오류

문제 중복된 또는 잘못된 사용자 디렉터리 URI가 있다는 알람을 수신했으며, 해당 사용자의 연락처 정보를 수정해야 합니다.

해결 방법 다음 단계를 수행하십시오.

1. **utilsusersvalidate{ all | userid | uri }** CLI 명령어를 사용하여 전체 사용자 목록을 생성합니다. CLI 명령 사용에 대한 자세한 내용은 *Cisco Unified Communications Solutions*용 명령줄 인터페이스 설명서를 참조하십시오.

   URI가 결과 집합에 입력되고 그 뒤에 중복된 UserID가 있는 서버의 목록이 표시됩니다. 다음의 샘플 CLI 출력은 유효성 확인 중 감지된 디렉터리 URI 오류를 보여줍니다.

```
Users with No Directory URI Configured
-------------------------------------------------------
 Node Name: cucm-imp-2
 User ID
 user4

Users with Invalid Directory URI Configured
-------------------------------------------------------
 Node Name: cucm-imp-2
 User ID   Directory URI
 user1     asdf@ASDF@asdf@ADSF@cisco

Users with Duplicate Directory URIs
-------------------------------------------------------
Directory URI: user1@cisco.com
 Node Name   User ID
 cucm-imp-1  user4
 cucm-imp-2  user3
```

2. 두 개의 서로 다른 클러스터에 동일한 사용자가 할당된 경우 클러스터 중 하나에서 사용자의 할당을 취소합니다.
3. 서로 다른 클러스터의 서로 다른 사용자에게 동일한 디렉터리 URI 값이 할당된 경우 사용자 중 한 명의 디렉터리 URI 값을 변경하여 중복이 발생하지 않도록 합니다.
4. 사용자 정보가 잘못되었거나 비어 있으면 사용자의 디렉터리 URI 정보를 수정합니다.

5. 최종 사용자 설정 창(사용자 관리 > 최종 사용자)를 사용하여 Cisco 통합 커뮤니케이션 매니저에서 사용자 레코드를 수정하여 모든 사용자에게 유효한 사용자 ID 또는 디렉터리 URI 값을 갖게 할 수 있습니다. 자세한 내용은 *Cisco Unified Communications Manager* 관리 설명서를 참조하십시오.

참고 사용자 프로파일의 사용자 ID 및 디렉터리 URI 필드를 LDAP 디렉터리로 매핑할 수 있습니다. 이 경우 LDAP 디렉터리 서버에 수정을 적용하십시오.

6. 중복된 또는 잘못된 사용자 URI 오류가 더 이상 표시되지 않는지 확인하기 위해 CLI 명령을 실행하여 사용자를 다시 검증합니다.

V 부

참조 정보

35 장

Cisco Unified Communications Manager TCP 및 UDP 포트 사용

이 장에서는 Cisco Unified Communications Manager가 클러스터 내 연결 및 외부 애플리케이션이나 디바이스와의 통신에 사용하는 TCP 및 UDP 포트 목록을 제공합니다. 또한 IP Communications 솔루션이 구현될 때 네트워크의 방화벽 구성, 액세스 제어 목록(ACL) 및 서비스 품질(QoS)에 대한 중요한 정보를 찾을 수 있습니다.

Cisco Unified Communications Manager TCP 및 UDP 포트 사용 개요

Cisco Unified Communications Manager TCP 및 UDP 포트는 다음 범주로 구성 됩니다.

- Cisco Unified Communications Manager 간 클러스터 간 포트
- 공통 서비스 포트
- Cisco Unified Communications Manager와 LDAP 디렉터리 간 보안 포트
- CCMAdmin 또는 CCMUser에서 Cisco Unified Communications Manager로 웹 요청
- Cisco Unified Communications Manager에서 전화기로 웹 요청
- 전화기와 Cisco Unified Communications Manager 간 신호, 미디어 및 기타 통신
- 게이트웨이와 Cisco Unified Communications Manager 간 신호, 미디어 및 기타 통신
- 애플리케이션과 Cisco Unified Communications Manager 간 통신
- CTL 클라이언트와 방화벽 간 통신
- HP 서버에 대한 특별 포트

위의 각 범주에서 포트 세부 정보는 "포트 설명"을 참조하십시오.

참고 Cisco는 이러한 포트에 대해 가능한 모든 구성 시나리오를 확인하지 않았습니다. 이 목록을 사용하여 구성 문제가 있는 경우 Cisco 기술 지원부에 지원을 요청하십시오.

포트 참조는 Cisco Unified Communications Manager에만 적용됩니다. 일부 포트는 릴리스마다 변경되며 이후 릴리스에서는 새로운 포트가 도입될 수 있습니다. 따라서 설치된 Cisco Unified Communications Manager 버전에 이 문서의 올바른 버전을 사용하고 있는지 확인하십시오.

거의 모든 프로토콜이 양방향이지만 세션 생성자 관점에서의 방향성이 가정됩니다. 경우에 따라 관리자가 수동으로 기본 포트 번호를 변경할 수 있지만 Cisco에서는 이를 권장하지 않습니다. 따라서 Cisco Unified Communications Manager는 여러 포트를 내부용으로만 엽니다.

Cisco Unified Communications Manager 소프트웨어를 설치하면 서비스 가용성을 위해 다음과 같은 네트워크 서비스가 자동으로 설치되고 기본적으로 활성화됩니다. 자세한 내용은 "Cisco Unified Communications Manager 간 클러스터 간 포트"를 참조하십시오.

- Cisco 로그 파티션 모니터링(일반 파티션을 모니터링하고 제거합니다. 사용자 지정 공통 포트를 사용하지 않습니다.)
- Cisco 추적 수집 서비스(TCTS 포트 사용)
- Cisco RIS 데이터 컬렉터(RIS 서버 포트 사용)
- Cisco AMC 서비스(AMC 포트 사용)

방화벽, ACL 또는 QoS의 구성은 토폴로지, 전화 통신 디바이스의 배치 및 전화 보안 디바이스의 배치와 관련한 서비스 및 사용 중인 애플리케이션 및 전화 통신 확장 기능에 따라 다릅니다. 또한 ACL의 형식은 디바이스와 버전에 따라 다양합니다.

참고 Cisco Unified Communications Manager에서 멀티캐스트 대기 중 음악(MOH) 포트를 구성할 수도 있습니다. 관리자가 실제 포트 값을 지정하기 때문에 멀티캐스트 MOH의 포트 값은 제공되지 않습니다.

참고 시스템의 임시 포트 범위는 32768 ~ 61000이며 전화 등록을 유지하려면 포트를 열어야합니다. 자세한 정보는 http://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/tsd-products-support-series-home.html를 참조하십시오.

참고 포트 22에 대한 연결이 열려 있고 스로틀되지 않도록 방화벽을 구성해야 합니다. IM and Presence 가입자 노드를 설치하는 동안 Cisco Unified Communications Manager 게시자 노드에 대한 여러 연결이 빠르게 연속적으로 열립니다. 이러한 연결을 조절하면 설치가 실패할 수 있습니다.

포트 설명

Cisco Unified Communications Manager 간 클러스터 간 포트

표 ***51: Cisco Unified Communications Manager*** 간 클러스터 간 포트

보낸 사람(전송자)	받는 사람(리스너)	대상 포트	목적
엔드포인트	Unified Communications Manager	514 / UDP	시스템 로깅 서비
엔드포인트	Unified Communications Manager	514 / UDP	시스템 로깅 서비
Unified Communications Manager	Unified Communications Manager	443 / TCP	이 포트는 가입자 COP 파일을 설치 입자와 게시자 간 용됩니다.
Unified Communications Manager	RTMT	1090, 1099 / TCP	RTMT 성능 모니 집, 로깅 및 경고 서비스
Unified Communications Manager(DB)	Unified Communications Manager(DB)	1500, 1501 / TCP	데이터베이스 연 TCP 는 보조 연결

보낸 사람(전송자)	받는 사람(리스너)	대상 포트	목적
Unified Communications Manager(DB)	Unified Communications Manager(DB)	1510 / TCP	CAR IDS DB. CAR I 은 클라이언트의 연 기다리면서 수신 대
Unified Communications Manager(DB)	Unified Communications Manager(DB)	1511 / TCP	CAR IDS DB. 업그레 는 동안 CAR IDS의 인스턴스를 표시하는 되는 대체 포트입니
Unified Communications Manager(DB)	Unified Communications Manager(DB)	1515 / TCP	설치 중 노드 간 데이 복제
Cisco 확장 기능(QRT)	Unified Communications Manager(DB)	2552 / TCP	가입자가 Cisco Unif Communications Mar 터베이스 변경 알림 수 있습니다.
Unified Communications Manager	Unified Communications Manager	2551 / TCP	활성/백업 결정을 위 확장 서비스 간의 클 통신
Unified Communications Manager(RIS)	Unified Communications Manager(RIS)	2555 / TCP	실시간 정보 서비스(터베이스 서버
Unified Communications Manager(RTMT/AMC/SOAP)	Unified Communications Manager(RIS)	2556 / TCP	Cisco RIS용 실시간 스(RIS) 데이터베이 언트
Unified Communications Manager(DRS)	Unified Communications Manager(DRS)	4040 / TCP	DRS 주 에이전트
Unified Communications Manager(Tomcat)	Unified Communications Manager(SOAP)	5001/TCP	이 포트는 실시간 모 비스를 위해 SOAP 서 사용됩니다.
Unified Communications Manager(Tomcat)	Unified Communications Manager(SOAP)	5002/TCP	이 포트는 성능 모니 를 위해 SOAP 모니 용됩니다.
Unified Communications Manager(Tomcat)	Unified Communications Manager(SOAP)	5003/TCP	이 포트는 제어 센터 위해 SOAP 모니터 됩니다.
Unified Communications Manager(Tomcat)	Unified Communications Manager(SOAP)	5004/TCP	이 포트는 로그 수집 위해 SOAP 모니터 됩니다.

보낸 사람(전송자)	받는 사람(리스너)	대상 포트	목적
표준 CCM 관리 사용자 / 관리자	Unified Communications Manager	5005 / TCP	이 포트는 SOAP CDROnDemand2 사용됩니다.
Unified Communications Manager(Tomcat)	Unified Communications Manager(SOAP)	5007 / TCP	SOAP 모니터
Unified Communications Manager(RTMT)	Unified Communications Manager(TCTS)	임시 / TCP	Cisco 추적 수집 - RTMT 추적 및 Central(TLC)에 서비스
Unified Communications Manager(Tomcat)	Unified Communications Manager(TCTS)	7000, 7001, 7002 / TCP	이 포트는 Cisco 구 서비스와 Cis 서블릿 간의 통신 다.
Unified Communications Manager	Certificate Manager	7070 / TCP	Certificate Manag
Unified Communications Manager(DB)	Unified Communications Manager(CDLM)	8001 / TCP	클라이언트 데이 경 알림
Unified Communications Manager(SDL)	Unified Communications Manager(SDL)	8002 / TCP	클러스터 간 통신
Unified Communications Manager(SDL)	Unified Communications Manager(SDL)	8003 / TCP	클러스터 간 통신 측)
Unified Communications Manager	CMI 관리자	8004 / TCP	Cisco Unified Co Manager와 CMI M 러스터 간 통신
Unified Communications Manager(Tomcat)	Unified Communications Manager(Tomcat)	8005 / TCP	Tomcat 종료 스크 용하는 내부 수신
Unified Communications Manager(Tomcat)	Unified Communications Manager(Tomcat)	8080 / TCP	진단 테스트에 사 간 통신
게이트웨이	Unified Communications Manager	8090	게이트웨이 레코 한 CuCM 및 GW 페이스) 간의 통 HTTP 포트.
Unified Communications Manager	게이트웨이		
Unified Communications Manager(IPSec)	Unified Communications Manager(IPSec)	8500 / TCP 및 UDP	IPSec Cluster Ma 시스템 데이터의 복제

보낸 사람(전송자)	받는 사람(리스너)	대상 포트	목적
Unified Communications Manager(RIS)	Unified Communications Manager(RIS)	8888 - 8889 / TCP	RIS 서비스 관리자 및 응답
위치 대역폭 관리자(LBM)	위치 대역폭 관리자(LBM)	9004 / TCP	LBM 간 클러스터 간
Unified Communications Manager[Dialed Number Analyzer (DNA) 초기화 서버]	JNIWrapper 서버	30000 / TCP	DNA(Dialed Number DNA 초기화를 처리 에서 사용하는 포트 JNIWrapper 기능이 서비스가 전송하는 답합니다.
Unified Communications Manager 게시자	Unified Communications Manager 가입자	22 / TCP	Cisco SFTP 서비스 가입자를 설치할 때 열어야 합니다.
Unified Communications Manager	Unified Communications Manager	8443 / TCP	노드 간에 제어 센터 네트워크 서비스에 허용합니다.

공통 서비스 포트

표 ***52:*** 공통 서비스 포트

보낸 사람(전송자)	받는 사람(리스너)	대상 포트	목적
엔드포인트	Unified Communications Manager	7	인터넷 제어 메시지 프로토콜(ICMP). 이 프로토콜 번호는 에코 관련 트래픽을 전달합니다. 열 머리글에 표시된 대로 포트를 구성하지 않습니다.
Unified Communications Manager	엔드포인트		
Unified Communications Manager(DRS, 통화 세부 정보 기록)	SFTP 서버	22 / TCP	SFTP 서버에 백업 데이터를 전송합니다. (DRS 로컬 에이전트) 통화 세부 정보 기록 데이터를 SFTP 서버로 전송합니다.

보낸 사람(전송자)	받는 사람(리스너)	대상 포트	목적
엔드포인트	Unified Communications ManagerDNS 서버)	임시 / UDP	DNS 서버 또는 DNS 클라이언트 역할을 하는 Cisco Unified Communications Manager 참고 Cisco Unified Communications Manager는 DNS 서버로 작동하지 않으며 모든 IP 전화 통신 애플리케이션 및 끝점은 호스트 이름 대신 정적 IP 주소를 사용하는 것이 좋습니다.
Unified Communications Manager	DNS Server(DNS 서버)		
엔드포인트	Unified Communications Manager(DHCP 서버)	67 / UDP	DHCP 서버 역할을 하는 Cisco Unified Communications Manager 참고 Cisco Unified Communications Manager에서 DHCP 서버를 실행하지 않는 것이 좋습니다.
Unified Communications Manager	DHCP 서버	68 / UDP	DHCP 클라이언트 역할을 하는 Cisco Unified Communications Manager 참고 Cisco Unified Communications Manager에서 DHCP 클라이언트를 실행하지 않는 것이 좋습니다. Configure Cisco Unified Communications Manager는 정적 IP 주소를 사용)
엔드포인트 또는 게이트웨이	Unified Communications Manager	69 6969, 그런 다음 임시 / UDP	전화기 및 게이트웨이에 대한 TFTP 서비스

보낸 사람(전송자)	받는 사람(리스너)	대상 포트	목적
엔드포인트 또는 게이트웨이	Unified Communications Manager	6970 / TCP	기본 서버와 프록시 서버 간 TFTP. TFTP 서버에서 전화기 및 게이트웨이로의 HTTP 서비스
Unified Communications Manager	NTP 서버	123 / UDP	NTP(Network Time Protocol)
SNMP 서버	Unified Communications Manager	161 / UDP	SNMP 서비스 응답(관리 애플리케이션에서 요청)
CUCM 서버 SNMP 주 에이전트 애플리케이션	SNMP 트랩 대상	162 / UDP	SNMP 트랩
SNMP 서버	Unified Communications Manager	199 / TCP	SMUX 지원용 기본 제공 SNMP 에이전트 수신 대기 포트
Unified Communications Manager	DHCP 서버	546 / UDP	DHCPv6. IPv6용 DHCP 포트입니다.
Unified Communications Manager 서비스 가용성	위치 대역폭 관리자(LBM)	5546 / TCP	고급 위치 기반 CAC 서비스 가용성
Unified Communications Manager	위치 대역폭 관리자(LBM)	5547 / TCP	통화 허용 요청 및 대역폭 공제
Unified Communications Manager	Unified Communications Manager	6161 / UDP	기본 에이전트 MIB 요청을 처리하기 위해 주 에이전트와 기본 에이전트 간의 통신에 사용
Unified Communications Manager	Unified Communications Manager	6162 / UDP	기본 에이전트에서 생성된 알림을 전달하기 위해 주 에이전트와 기본 에이전트 간의 통신에 사용
Unified Communications Manager	Unified Communications Manager	6666 / UDP	Netdump 서버
중앙 집중식 TFTP	대체 TFTP	6970 / TCP	중앙 집중식 TFTP 파일 로케이터 서비스
Unified Communications Manager	Unified Communications Manager	7161 / TCP	SNMP 주 에이전트와 하위 에이전트 간의 통신에 사용

보낸 사람(전송자)	받는 사람(리스너)	대상 포트	목적
SNMP 서버	Unified Communications Manager	7999 / TCP	Cisco Discovery Protocol(CDP) 에이전트가 CDP 실행 파일과 통신
엔드포인트	Unified Communications Manager	443, 8443 / TCP	Cisco 사용자 데이터 서비스(UDS) 요청에 사용
Unified Communications Manager	Unified Communications Manager	9050 / TCP	Cisco Unified Communications Manager에 있는 TAPS를 통해 서비스 CRS 요청
Unified Communications Manager	Unified Communications Manager	61441 / UDP	Cisco Unified Communications Manager 애플리케이션은 UDP를 통해 이 포트에 경보를 전송합니다. Cisco Unified Communications Manager MIB 에이전트는 이 포트를 수신하고 Cisco Unified Communications Manager MIB 정의에 따라 SNMP 트랩을 생성합니다.
Unified Communications Manager	Unified Communications Manager	5060, 5061 / TCP	트렁크 기반 SIP 서비스를 제공
Unified Communications Manager	Unified Communications Manager	7501	인증서 기반 인증을 위해 ILS(Intercluster Lookup Service)에서 사용됩니다.
Unified Communications Manager	Unified Communications Manager	7502	암호 기반 인증을 위해 ILS에서 사용됩니다.
Unified Communications Manager	Unified Communications Manager	9966	Cisco 푸시 알림 서비스는 방화벽이 활성화되어 있을 때 클러스터 노드 간 통신을 위해 이를 사용합니다.
Unified Communications Manager	Unified Communications Manager	9560	로컬 푸시 알림 서비스(LPNS)에서 사용됩니다.
--	--	8000-48200	ASR 및 ISR G3 플랫폼 기본 포트 범위입니다.
		16384-32766	ISR G2 플랫폼 기본 포트 범위입니다.

Cisco Unified Communications Manager와 LDAP 디렉터리 간 보안 포트

표 *53: Cisco Unified Communications Manager*와 *LDAP* 디렉터리 간 보안 포트

보낸 사람(전송자)	받는 사람(리스너)	대상 포트	목적
Unified Communications Manager	외부 디렉터리	389, 636, 3268, 3269 / TCP	외부 디렉터리(Netscape Directory Active Directory)에 LDAP(Lightweight Directory Access Protocol) 쿼리
외부 디렉터리	Unified Communications Manager	임시	

CCMAdmin 또는 CCMUser에서 Cisco Unified Communications Manager로 웹 요청

표 *54: CCMAdmin* 또는 *CCMUser*에서 *Cisco Unified Communications Manager*로 웹 요청

보낸 사람(전송자)	받는 사람(리스너)	대상 포트	목적
브라우저	Unified Communications Manager	80, 8080 / TCP	HTTP(Hypertext Tra Protocol)
브라우저	Unified Communications Manager	443, 8443 / TCP	HTTPS(Hypertext Tr Protocol over SSL)
브라우저	Unified Communications Manager	9463 / TCP	SSL(HTTPS)를 통한 스트 전송 프로토콜 TLS1.3만 허용합니
브라우저 또는 CLI	Unified Communications Manager	2355, 2356 / TCP	CLI 및 웹 애플리케 감사 이벤트 로그
Unified Communications Manager	Cisco License Manager	5555 / TCP	Cisco License Manag 트에서 라이센스 요 합니다.

Cisco Unified Communications Manager에서 전화기로 웹 요청

표 *55: Cisco Unified Communications Manager*에서 전화기로 웹 요청

보낸 사람(전송자)	받는 사람(리스너)	대상 포트	목적
Unified Communications Manager • QRT • RTMT • 전화기 찾기 및 나열 페이지 • 전화기 구성 페이지	전화기	80 / TCP	HTTP(Hypertext Protocol)

전화기와 Cisco Unified Communications Manager 간 신호, 미디어 및 기타 통신

표 *56:* 전화기와 *Cisco Unified Communications Manager* 간 신호, 미디어 및 기타 통신

보낸 사람(전송자)	받는 사람(리스너)	대상 포트	목적
전화기	DNS 서버	53 / TCP	SIP(Session Initiation Protocol) 전화기는 DNS(Domain Name System)를 사용하여 FQDN(정규화된 도메인 이름)을 확인합니다. 참고 기본적으로 일부 무선 액세스 지점은 TCP 53 포트를 차단하므로 FQDN을 사용하여 CUCM을 구성할 때 무선 SIP 전화기가 등록되지 않습니다.
전화기	Unified Communications Manager(TFTP)	69, 그런 다음 임시 / UDP	펌웨어 및 구성 파일을 다운로드하는 데 사용되는 TFTP(Trivial File Transfer Protocol)

보낸 사람(전송자)	받는 사람(리스너)	대상 포트	목적
전화기	Unified Communications Manager	2000 / TCP	SCCP(Skinny Client Control Protocol)
전화기	Unified Communications Manager	2443 / TCP	SCCPS(Secure Skinny Client Control Protocol)
전화기	Unified Communications Manager	2445 / TCP	엔드포인트에 신뢰 검증 서비스를 제공합니다.
전화기	Unified Communications Manager(CAPF)	3804 / TCP	IP Phone에 로컬 서명 인증서(LSC)를 발행하는 CAPF(Certificate Authority Proxy Function) 수신 포트
전화기	Unified Communications Manager	5060 / TCP 및 UDP	SIP(Session Initiation Protocol) 전화기
Unified Communications Manager	전화기		
전화기	Unified Communications Manager	TCP 5061	SIPS(Secure Session Initiation Protocol) 전화기
Unified Communications Manager	전화기		
전화기	Unified Communications Manager(TFTP)	6970 TCP	펌웨어 및 구성 파일의 HTTP 기반 다운로드
전화기	Unified Communications Manager(TFTP)	6971, 6972 / TCP	TFTP에 대한 HTTPS 인터페이스입니다. 전화기는 이 포트를 사용하여 TFTP에서 보안 구성 파일을 다운로드합니다.
전화기	Unified Communications Manager	8080 / TCP	XML 애플리케이션, 인증, 디렉터리, 서비스 등을 위한 전화기 URL 이러한 포트는 서비스 별로 구성할 수 있습니다.
전화기	Unified Communications Manager	9443 / TCP	전화기 인증된 연락처 검색에 이 포트를 사용합니다.
전화기	Unified Communications Manager	9444	전화기는 이 포트 번호를 사용하여 헤드셋 관리 기능을 사용합니다.
iPhone/iPad(Webex 앱)	Unified Communications Manager	9560/보안 WebSocket	Webex 앱은 LPNS 기능에 이 포트 번호를 사용합니다.

보낸 사람(전송자)	받는 사람(리스너)	대상 포트	목적
IP VMS	전화기	16384 - 32767 / UDP	RTP(Real-Time Protocol), SRTP(Secure Real-Time Protocol) 참고 다른 디바이스들은 전체 범위를 사용하지만 Cisco Unified Communications Manager는 24576-32767만 사용합니다.
전화기	IP VMS		

게이트웨이와 **Cisco Unified Communications Manager** 간 신호, 미디어 및 기타 통신

표 ***57:*** 게이트웨이와 ***Cisco Unified Communications Manager*** 간 신호, 미디어 및 기타 통신

보낸 사람(전송자)	받는 사람(리스너)	대상 포트	목적
게이트웨이	Unified Communications Manager	47, 50, 51	GRE(Generic Rou Encapsulation), ESP(Encapsulatin Payload), AH(Au Header). 이러한 호는 암호화된 IP 을 전달합니다. 표시된 대로 포트 않습니다.
Unified Communications Manager	게이트웨이		
게이트웨이	Unified Communications Manager	500 / UDP	IP 보안 프로토콜 을 위한 IKE(인터
Unified Communications Manager	게이트웨이		
게이트웨이	Unified Communications Manager(TFTP)	69, 그런 다음 임시 / UDP	TFTP(Trivial File Protocol)
Cisco Intercompany Media Engine(CIME) 트렁크를 사용하는 Unified Communications Manager	CIME ASA	1024-65535 / TCP	포트 매핑 서비스 CIME 경로 이탈 서만 사용됩니다

보낸 사람(전송자)	받는 사람(리스너)	대상 포트	목적
Gatekeeper	Unified Communications Manager	1719 / UDP	게이트키퍼(H.225)
게이트웨이	Unified Communications Manager	1720 / TCP	H.323 게이트웨이 및 터클러스터 트렁크) H.225 신호 서비스
Unified Communications Manager	게이트웨이		
게이트웨이	Unified Communications Manager	임시 / TCP	게이트키퍼 제어 트 한 H.225 신호 서비
Unified Communications Manager	게이트웨이		
게이트웨이	Unified Communications Manager	임시 / TCP	음성, 비디오 및 데 을 위한 H.245 신호
Unified Communications Manager	게이트웨이		참고 원격 시 사용하는 포트는 이 유형 다릅니 IOS 게 의 경우 트 범위 ~ 65535
게이트웨이	Unified Communications Manager	2000 / TCP	SCCP(Skinny Client Protocol)
게이트웨이	Unified Communications Manager	2001 / TCP	Cisco Unified Commu Manager 구축을 사용 6608 게이트웨이에 업그레이드
게이트웨이	Unified Communications Manager	2002 / TCP	Cisco Unified Commu Manager 구축을 사용 6624 게이트웨이에 업그레이드
게이트웨이	Unified Communications Manager	2427 / UDP	MGCP(Media Gatewa Protocol) 게이트웨이
게이트웨이	Unified Communications Manager	2428 / TCP	MGCP(Media Gatewa Protocol) 백홀

보낸 사람(전송자)	받는 사람(리스너)	대상 포트	목적
--	--	4000 - 4005 / TCP	이러한 포트는 C Communications M 러한 미디어에 대 을 때 오디오, 비 터 채널에 대해 지 RTP(Real-Time T Protocol) 및 RTC Transport Control 트로 사용됩니다
게이트웨이	Unified Communications Manager	5060 / TCP 및 UDP	SIP(Session Initia 게이트웨이 및 IC 스터 트렁크)
Unified Communications Manager	게이트웨이		
게이트웨이	Unified Communications Manager	5061 / TCP	SIPS(Secure Sess Protocol) 게이트 ICT(인터클러스
Unified Communications Manager	게이트웨이		
게이트웨이	Unified Communications Manager	16384 - 32767 / UDP	RTP(Real-Time P SRTP(Secure Rea Protocol) 참고 다른 은 전 사용 Unifi Comm Mana 2457 용합
Unified Communications Manager	게이트웨이		

애플리케이션과 **Cisco Unified Communications Manager** 간 통신

표 ***58:*** 애플리케이션과 ***Cisco Unified Communications Manager*** 간 통신

보낸 사람(전송자)	받는 사람(리스너)	대상 포트	목적
CTL 클라이언트	Unified Communications Manager CTL 공급자	2444 / TCP	Cisco Unified Co Manager의 인증 (CTL) 공급자 수

보낸 사람(전송자)	받는 사람(리스너)	대상 포트	목적
Cisco Unified Communications 앱	Unified Communications Manager	2748 / TCP	CTI 애플리케이션 서
Cisco Unified Communications 앱	Unified Communications Manager	2749 / TCP	CTI 애플리케이션(JT 및 CTIManager 간 T
Cisco Unified Communications 앱	Unified Communications Manager	2789 / TCP	JTAPI 애플리케이션
Unified Communications Manager Assistant 콘솔	Unified Communications Manager	2912 / TCP	Cisco Unified Commu Manager Assistant 서 에는 IPMA)
Unified Communications Manager Attendant 콘솔	Unified Communications Manager	1103 -1129 / TCP	Cisco Unified Commu Manager Attendant 콘 JAVA RMI 레지스트
Unified Communications Manager Attendant 콘솔	Unified Communications Manager	1101 / TCP	RMI 서버는 RMI 콜 를 이 포트의 클라이 송합니다.
Unified Communications Manager Attendant 콘솔	Unified Communications Manager	1102 / TCP	어텐던트 콘솔(AC) 바인드 포트 - RMI 러한 포트에서 RMI 전송합니다.
Unified Communications Manager Attendant 콘솔	Unified Communications Manager	3223 / UDP	Cisco Unified Commu Manager AC(Attenda Console) 서버 회선 는 어텐던트 콘솔 서 및 등록 메시지를 수 선 상태를 어텐던트 로 보냅니다.
Unified Communications Manager Attendant 콘솔	Unified Communications Manager	3224 / UDP	Cisco Unified Commu Manager Attendant Console(AC) 클라이 선 및 디바이스 상태 위해 AC 서버에 등록
Unified Communications ManagerAttendant 콘솔	Unified Communications Manager	4321 / UDP	Cisco Unified Commu Manager Attendant Console(AC) 클라이 화 제어를 위해 AC 록합니다.

보낸 사람(전송자)	받는 사람(리스너)	대상 포트	목적
Unified Communications Manager(SAF/CCD 포함)	SAF 이미지를 실행하는 IOS 라우터	5050 / TCP	EIGRP/SAF 프로 하는 다중 서비스
Unified Communications Manager	Cisco Intercompany Media Engine(IME) 서버	5620 / TCP Cisco는 이 포트에 5620 값을 권장하지만 Cisco IME 서버에서 add ime vapserver 또는 ime vapserver port CLI 명령을 실행하여 값을 변경할 수 있습니다.	Cisco Intercompa Engine 서버와 통 용되는 VAP 프로
Cisco Unified Communications 앱	Unified Communications Manager	8443 / TCP	결제 또는 전화 부 플리케이션과 같 사용하는 프로그 Cisco Unified Co Manager 데이터베 또는 쓰기용 AXL 입니다.

CTL 클라이언트와 방화벽 간 통신

표 *59: CTL* 클라이언트와 방화벽 간 통신

보낸 사람(전송자)	받는 사람(리스너)	대상 포트	목적
CTL 클라이언트	TLS 프록시 서버	2444 / TCP	ASA 방화벽에서 목록(CTL) 공급 스

Cisco 스마트 라이센스 서비스와 Cisco Smart Software Manager 간의 통신

Unified Communications Manager의 Cisco 스마트 라이센스 서비스는 통화 홈을 통해 Cisco Smart Software Manager와 직접 통신을 설정합니다.

표 *60: Cisco* 스마트 라이센스 서비스와 *Cisco Smart Software Manager* 간의 통신

보낸 사람(전송자)	받는 사람(리스너)	대상 포트	목적
통합 커뮤니케이션 관리자(Cisco 스마트 라이센스 서비스)	CSSM(Cisco Smart Software Manager)	443 / HTTPS	스마트 라이센스 서비스는 라이선스 사용량을 CSSM에 전송하여 Unified CM의 불만 사항 여부를 확인합니다.

HP 서버에 대한 특별 포트

표 61: HP 서버에 대한 특별 포트

보낸 사람(전송자)	받는 사람(리스너)	대상 포트	목적
엔드포인트	HP SIM	2301 / TCP	HP 에이전트측 HTT
엔드포인트	HP SIM	2381 / TCP	HP 에이전트측 HTT
엔드포인트	Compaq 관리 에이전트	25375, 25376, 25393 / UDP	COMPAQ 관리 에이 번호(cmaX)
엔드포인트	HP SIM	50000 - 50004 / TCP	HP SIM측 HTTPS 포

포트 참조

방화벽 애플리케이션 검사 설명서

ASA 시리즈 참조 정보

http://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/tsd-products-support-series-home.html

PIX 애플리케이션 검사 구성 설명서

http://www.cisco.com/c/en/us/support/security/pix-firewall-software/products-installation-and-configuration-guides-list.html

FWSM 3.1 애플리케이션 검사 구성 설명서

http://www-author.cisco.com/c/en/us/td/docs/security/fwsm/fwsm31/configuration/guide/fwsm_cfg/inspct_f.html

IETF UDP/TCP 포트 할당 목록

IANA(Internet Assigned Numbers Authority) IETF 할당 포트 목록

http://www.iana.org/assignments/port-numbers

IP 전화 통신 구성 및 포트 활용 설명서

Cisco CRS 4.0(IP IVR and IPCC Express) 포트 활용 설명서

http://www.cisco.com/en/US/products/sw/custcosw/ps1846/products_installation_and_configuration_guides_list.html

Cisco ICM/IPCC Enterprise 및 Hosted Editions용 포트 활용 설명서

http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products_installation_and_configuration_guides_list.html

Cisco Unified Communications Manager Express 보안 설명서(모범 사례)

http://www.cisco.com/en/US/netsol/ns340/ns394/ns165/ns391/networking_solutions_design_guidance09186a00801f8e30.html

Cisco Unity Express 보안 설명서(모범 사례)

http://www.cisco.com/en/US/netsol/ns340/ns394/ns165/ns391/networking_solutions_design_guidance09186a00801f8e31.html#wp41149

VMware 포트 할당 목록

vCenter 서버, ESX 호스트 및 기타 네트워크 구성 요소 관리 액세스를 위한 TCP 및 UDP 포트

36 장

IM and Presence 서비스를 위한 포트 사용 정보

IM and Presence 서비스 포트 사용 개요

이 문서는 IM and Presence 서비스가 클러스터 내 연결 및 외부 애플리케이션 또는 디바이스와의 통신에 사용하는 TCP 및 UDP 포트 목록을 제공합니다. 또한 IP Communications 솔루션이 구현될 때 네트워크의 방화벽 구성, 액세스 제어 목록(ACL) 및 서비스 품질(QoS)에 대한 중요한 정보를 제공합니다.

참고 Cisco는 이러한 포트에 대해 가능한 모든 구성 시나리오를 확인하지 않았습니다. 이 목록을 사용하여 구성 문제가 있는 경우 Cisco 기술 지원부에 지원을 요청하십시오.

거의 모든 프로토콜이 양방향이지만 이 문서에서는 세션 생성자 관점에서의 방향성을 제공합니다. 경우에 따라 관리자가 수동으로 기본 포트 번호를 변경할 수 있지만 Cisco에서는 이를 권장하지 않습니다. IM and Presence 서비스는 여러 포트를 내부용으로만 엽니다.

이 문서의 포트는 특히 IM and Presence 서비스에 적용됩니다. 일부 포트는 릴리스마다 변경되며 이후 릴리스에서는 새로운 포트가 도입될 수 있습니다. 따라서 설치된 IM and Presence 서비스 버전에 이 문서의 올바른 버전을 사용하고 있는지 확인하십시오.

방화벽, ACL 또는 QoS의 구성은 토폴로지, 디바이스의 배치 및 전화 보안 디바이스의 배치와 관련한 서비스 및 사용 중인 애플리케이션 및 전화 통신 확장 기능에 따라 다릅니다. 또한 ACL의 형식은 디바이스와 버전에 따라 다양합니다.

표에 정리된 정보

이 표는 이 문서의 각 표에 정리된 정보를 정의합니다.

표 ***62:*** 표 정보 정의

표 제목	설명
보낸 사람	이 포트에 요청을 전송하는 클라이언트
끝	이 포트에 대한 요청을 수신하는 클라이언트
역할	클라이언트 또는 서버 애플리케이션 또는 프로세스
프로토콜	통신 설정 및 종료에 사용되는 세션 계층 프로토콜 또는 요청 및 응답 트랜잭션에 사용되는 애플리케이션 계층 프로토콜
전송 프로토콜	연결 지향형(TCP) 또는 비연결(UDP)인 전송 계층 프로토콜
대상/리스너	요청 수신에 사용되는 포트
소스/전송자	요청을 전송하는 데 사용되는 포트

IM and Presence 서비스 포트 목록

다음 표에서는 IM and Presence 서비스가 클러스터 내 및 클러스터 간 트래픽에 사용하는 포트를 보여줍니다.

표 ***63: IM and Presence*** 서비스 포트 **-** ***SIP*** 프록시 요청

보낸 사람(전송자)	받는 사람(리스너)	프로토콜	전송 프로토콜	대상/리스너	소스/전송자	참고
SIP Gateway --- IM and Presence	IM and Presence --- SIP Gateway	SIP	TCP/UDP	5060	임시	기본 SIP 프록시 UDP 및 TCP 리스너
SIP Gateway	IM and Presence	SIP	TLS	5061	임시	TLS 서버 인증 리스너 포트
IM and Presence	IM and Presence	SIP	TLS	5062	임시	TLS 상호 인증 리스너 포트

보낸 사람(전송자)	받는 사람(리스너)	프로토콜	전송 프로토콜	대상/리스너	소스/전송자	참고
IM and Presence	IM and Presence	SIP	UDP / TCP	5049	임시	내부 포트입니다. 로컬 호스트 트래픽 전용입니다.
IM and Presence	IM and Presence	HTTP	TCP	8081	임시	구성 변경을 나타내기 위해 구성 에이전트의 HTTP 요청에 사용됩니다.
타사 클라이언트	IM and Presence	HTTP	TCP	8082	임시	기본 IM and Presence HTTP 리스너. 타사 클라이언트를 연결하는 데 사용
타사 클라이언트	IM and Presence	HTTPS	TLS / TCP	8083	임시	기본 IM and Presence HTTPS 리스너. 타사 클라이언트를 연결하는 데 사용

표 ***64: IM and Presence*** 서비스 포트 **-** 프레즌스 엔진 요청

보낸 사람(전송자)	받는 사람(리스너)	프로토콜	전송 프로토콜	대상/리스너	소스/전송자	참고
IM and Presence	IM and Presence (프레즌스 엔진)	SIP	UDP / TCP	5080	임시	기본 SIP UDP/TCP 리스너 포트
IM and Presence (프레즌스 엔진)	IM and Presence (프레즌스 엔진)	Livebus	UDP	50000	임시	내부 포트입니다. 로컬 호스트 트래픽 전용입니다. LiveBus 메시징 포트입니다. IM and Presence 서비스는 이 포트를 클러스터 통신에 사용합니다.

표 ***65: IM and Presence*** 서비스 포트 ***- Cisco Tomcat WebRequests***

보낸 사람(전송자)	받는 사람(리스너)	프로토콜	전송 프로토콜	대상/리스너	소스/전송자	참고
브라우저	IM and Presence	HTTPS	TCP	8080	임시	웹 액세스에 사용

보낸 사람(전송자)	받는 사람(리스너)	프로토콜	전송 프로토콜	대상/리스너	소스/전송자	참고
브라우저	IM and Presence	AXL / HTTPS	TLS / TCP	8443	임시	SOAP를 통해 데이터베이스 및 서비스 가용성을 제공합니다.
브라우저	IM and Presence	HTTPS	TLS / TCP	8443	임시	웹 관리에 대한 액세스를 제공합니다.
브라우저	IM and Presence	HTTPS	TLS / TCP	8443	임시	사용자 옵션 페이지에 대한 액세스를 제공합니다.
브라우저	IM and Presence	SOAP	TLS / TCP	8443	임시	SOAP를 통해 Cisco Unified Personal Communicator, Cisco Unified Mobility Advantage 및 타사 API 클라이언트에 대한 액세스를 제공합니다.
브라우저	IM and Presence	HTTPS	TCP	9463	임시	SSL(HTTPS)를 통한 하이퍼텍스트 전송 프로토콜은 v6의 TLS1.3만 허용합니다.

표 ***66: IM and Presence*** 서비스 포트 **-** 외부 회사 디렉터리 요청

보낸 사람(전송자)	받는 사람(리스너)	프로토콜	전송 프로토콜	대상/리스너	소스/전송자	참고
IM and Presence --- 외부 회사 디렉터리	외부 회사 디렉터리 --- IM and Presence	LDAP	TCP	389 / 3268	임시	디렉터리 프로토콜은 외부 회사 디렉터리와 통합하는 것을 허용합니다. LDAP 포트는 회사 디렉토리에 따라 다릅니다(기본값은 389). Netscape Directory의 경우 고객은 LDAP 트래픽을 수용할 수 있도록 다른 포트를 구성 할 수 있습니다. LDAP가 인증을 위해 IM&P와 LDAP 서버 간에 통신을 허용합니다.

보낸 사람(전송자)	받는 사람(리스너)	프로토콜	전송 프로토콜	대상/리스너	소스/전송자	참고
IM and Presence	외부 회사 디렉터리	LDAPS	TCP	636	임시	디렉터리 프로토콜은 외부 회사 디렉터리와 통합하는 것을 허용합니다. LDAP 포트는 회사 디렉토리에 따라 다릅니다(기본값은 636).

표 ***67: IM and Presence*** 서비스 포트 - 구성 요청

보낸 사람(전송자)	받는 사람(리스너)	프로토콜	전송 프로토콜	대상/리스너	소스/전송자	참고
IM and Presence (구성 에이전트)	IM and Presence (구성 에이전트)	TCP	TCP	8600	임시	구성 에이전트 하트비트 포트

표 ***68: IM and Presence*** 서비스 포트 - 인증서 관리자 요청

보낸 사람(전송자)	받는 사람(리스너)	프로토콜	전송 프로토콜	대상/리스너	소스/전송자	참고
IM and Presence	Certificate Manager	TCP	TCP	7070	임시	내부 포트 - Localhost 트래픽 전용

표 ***69: IM and Presence*** 서비스 포트 - ***IDS*** 데이터베이스 요청

보낸 사람(전송자)	받는 사람(리스너)	프로토콜	전송 프로토콜	대상/리스너	소스/전송자	참고
IM and Presence (데이터베이스)	IM and Presence (데이터베이스)	TCP	TCP	1500	임시	데이터베이스 클라이언트를 위한 내부 IDS 포트입니다. 로컬 호스트 트래픽 전용입니다.
IM and Presence (데이터베이스)	IM and Presence (데이터베이스)	TCP	TCP	1501	임시	내부 포트 - 업그레이드하는 동안 IDS의 두 번째 인스턴스를 표시하는 데 사용됩니다. 로컬 호스트 트래픽 전용입니다.
IM and Presence (데이터베이스)	IM and Presence (데이터베이스)	XML	TCP	1515	임시	내부 포트입니다. 로컬 호스트 트래픽 전용입니다. DB 복제 포트

표 *70: IM and Presence* 서비스 포트 - *IPSec* 관리자 요청

보낸 사람 (전송자)	받는 사람 (리스너)	프로토콜	전송 프로토콜	대상/리스너	소스/전송자	참고
IM and Presence (IPSec)	IM and Presence (IPSec)	Proprietary	UDP/TCP	8500	8500	내부 포트 - 플랫폼 데이터(호스트) 인증서의 클러스터 복제를 위해 ipsec_mgr 데몬에서 사용하는 클러스터 관리자 포트

표 *71: IM and Presence* 서비스 포트 - *DRF* 마스터 에이전트 서버 요청

보낸 사람(전송자)	받는 사람(리스너)	프로토콜	전송 프로토콜	대상/리스너	소스/전송자	참고
IM and Presence (DRF)	IM and Presence (DRF)	TCP	TCP	4040	임시	로컬 에이전트, GUI 및 CLI에서 연결을 허용하는 DRF 마스터 에이전트 서버 포트

표 *72: IM and Presence* 서비스 포트 - *RISDC* 요청

보낸 사람(전송자)	받는 사람(리스너)	프로토콜	전송 프로토콜	대상/리스너	소스/전송자	참고
IM and Presence (RIS)	IM and Presence (RIS)	TCP	TCP	2555	임시	실시간 정보 서비스 (RIS) 데이터베이스 서버. 클러스터의 다른 RISDC 서비스에 연결하여 클러스터 전체의 실시간 정보를 제공
IM and Presence (RTMT/AMC/ SOAP)	IM and Presence (RIS)	TCP	TCP	2556	임시	Cisco RIS용 실시간 정보 서비스(RIS) 데이터베이스클라이언트. RIS 클라이언트 연결을 통해 실시간 정보를 검색 가능
IM and Presence (RIS)	IM and Presence (RIS)	TCP	TCP	8889	8888	내부 포트입니다. 로컬 호스트 트래픽 전용입니다. RISDC(시스템 액세스)에서 서비스 상태 요청 및 응답을 위해 TCP를 통해 servM에 연결하는 데 사용

표 *73: IM and Presence* 서비스 포트 *- SNMP* 요청

보낸 사람(전송자)	받는 사람(리스너)	프로토콜	전송 프로토콜	대상/리스너	소스/전송자	참고
SNMP 서버	IM and Presence	SNMP	UDP	161, 8161	임시	SNMP 기반 관리 애플리케이션에 대한 서비스를 제공
IM and Presence	IM and Presence	SNMP	UDP	6162	임시	SNMP 마스터 에이전트가 전달한 요청을 수신하는 기본 SNMP 에이전트
IM and Presence	IM and Presence	SNMP	UDP	6161	임시	기본 SNMP 에이전트에서 트랩을 수신하고 관리 애플리케이션으로 전달하는 마스터 에이전트
SNMP 서버	IM and Presence	TCP	TCP	7999	임시	cdp 에이전트가 cdp 바이너리와 통신하기 위한 소켓으로 사용
IM and Presence	IM and Presence	TCP	TCP	7161	임시	SNMP 마스터 에이전트와 하위 에이전트 간의 통신에 사용
IM and Presence	SNMP 트랩 모니터	SNMP	UDP	162	임시	SNMP 트랩을 관리 애플리케이션으로 전송
IM and Presence	IM and Presence	SNMP	UDP	가능 설정	61441	내부 SNMP 트랩 수신기

표 *74: IM and Presence* 서비스 포트 *- Racoon* 서버 요청

보낸 사람(전송자)	받는 사람(리스너)	프로토콜	전송 프로토콜	대상/리스너	소스/전송자	참고
게이트웨이 --- IM and Presence	IM and Presence --- 게이트웨이	Ipsec	UDP	500	임시	Internet Security Association and the Key Management 프로토콜 활성화

표 *75: IM and Presence* 서비스 포트 - 시스템 서비스 요청

보낸 사람(전송자)	받는 사람(리스너)	프로토콜	전송 프로토콜	대상/리스너	소스/전송자	참고
IM and Presence (RIS)	IM and Presence (RIS)	XML	TCP	8888 및 8889	임시	내부 포트입니다. 로컬 호스트 트래픽 전용입니다. RIS Service Manager(servM)와 통신하는 클라이언트를 수신하는 데 사용됩니다.

표 *76: IM and Presence Service* 포트 - *DNS* 요청

보낸 사람(전송자)	받는 사람(리스너)	프로토콜	전송 프로토콜	대상/리스너	소스/전송자	참고
IM and Presence	DNS Server(DNS 서버)	DNS	UDP	53	임시	DNS 서버가 IM and Presence DNS 쿼리를 수신하는 포트입니다. 수신: DNS 서버 | 발신: IM and Presence

표 *77: IM and Presence* 서비스 포트 - *SSH/SFTP* 요청

보낸 사람(전송자)	받는 사람(리스너)	프로토콜	전송 프로토콜	대상/리스너	소스/전송자	참고
IM and Presence	엔드포인트	SSH / SFTP	TCP	22	임시	많은 애플리케이션에서 서버에 대한 명령줄 액세스에 사용됩니다. 또한 인증서와 기타 파일 교환을 위해 노드간에 사용됩니다(sftp).

표 *78: IM and Presence* 서비스 포트 - *ICMP* 요청

보낸 사람(전송자)	받는 사람(리스너)	프로토콜	전송 프로토콜	대상/리스너	소스/전송자	참고
IM and Presence --- Cisco Unified Communications Manager	Cisco Unified Communications Manager --- IM and Presence	ICMP	IP	해당 없음	임시	ICMP(Internet Control Message Protocol). Cisco Unified Communications Manager 서버와 통신하는 데 사용

표 *79: IM and Presence* 서비스 포트 *- NTP* 요청

보낸 사람(전송자)	받는 사람(리스너)	프로토콜	전송 프로토콜	대상/리스너	소스/전송자	참고
IM and Presence	NTP 서버	NTP	UDP	123	임시	Cisco Unified Communications Manager는 작동 중인 NTP 서버입니다. 게시자 노드와 시간을 동기화하기 위해 구독자 노드에서 사용됩니다.

표 *80: IM and Presence* 서비스 포트 *- Microsoft Exchange* 알림 요청

보낸 사람(전송자)	받는 사람(리스너)	프로토콜	전송 프로토콜	대상/리스너	소스/전송자	참고
Microsoft Exchange	IM and Presence	HTTP (HTTPu)	) WebDAV - HTTP /UDP/IP 알림 2) EWS - HTTP/TCP /IP SOAP 알림	IM and Presence 서버 포트(기본값 50020)	임시	Microsoft Exchange는 이 포트를 사용하여 달력 이벤트의 특정 구독 식별자가 변경되었음을 알리는 알림(알림 메시지 사용)을 보냅니다. 네트워크 구성에서 Exchange 서버와 통합하는 데 사용됩니다. 두 개의 포트가 생성됩니다. 전송되는 메시지의 종류는 구성된 일정 프레즌스 백엔드 게이트웨이의 유형에 따라 다릅니다.

표 *81: IM and Presence* 서비스 포트 *- SOAP* 요청 서비스

보낸 사람(전송자)	받는 사람(리스너)	프로토콜	전송 프로토콜	대상/리스너	소스/전송자	참고
IM and Presence (Tomcat)	IM and Presence (SOAP)	TCP	TCP	5007	임시	SOAP 모니터 포트

표 ***82: IM and Presence*** 서비스 포트 - ***AMC RMI*** 요청

보낸 사람(전송자)	받는 사람(리스너)	프로토콜	전송 프로토콜	대상/리스너	소스/전송자	참고
IM and Presence	RTMT	TCP	TCP	1090	임시	AMC RMI 개체 포트입니다. RTMT 성능 모니터, 데이터 수집, 로깅 및 경고용 Cisco AMC 서비스
IM and Presence	RTMT	TCP	TCP	1099	임시	AMC RMI 레지스트리 포트입니다. RTMT 성능 모니터, 데이터 수집, 로깅 및 경고용 Cisco AMC 서비스

표 ***83: IM and Presence*** 서비스 포트 - ***XCP*** 요청

보낸 사람(전송자)	받는 사람(리스너)	프로토콜	전송 프로토콜	대상/리스너	소스/전송자	참고
XMPP 클라이언트	IM and Presence	TCP	TCP	5222	임시	클라이언트 액세스 포트
IM and Presence	IM and Presence	TCP	TCP	5269	임시	서버 간 연결(S2S) 포트
타사 BOSH 클라이언트	IM and Presence	TCP	TCP	7335	임시	BOSH 타사 API 연결을 위해 XCP 웹 연결 관리자에서 사용하는 HTTP 수신 대기 포트
IM and Presence (XCP 서비스)	IM and Presence (XCP 라우터	TCP	TCP	7400	임시	XCP 라우터 마스터 수락 포트입니다. 개방 포트 구성(예: XCP 인증 구성 요소 서비스)에서 라우터에 연결하는 XCP 서비스는 일반적으로 이 포트에 연결합니다.
IM and Presence (XCP 라우터	IM and Presence (XCP 라우터	UDP	UDP	5353	임시	MDNS 포트입니다. 클러스터의 XCP 라우터는 이 포트를 사용하여 서로를 찾습니다.

보낸 사람(전송자)	받는 사람(리스너)	프로토콜	전송 프로토콜	대상/리스너	소스/전송자	참고
IM and Presence (XCP 라우터	IM and Presence (XCP 라우터	TCP	TCP	7336	HTTPS	MFT 파일 전송(온-프레미스에만 해당).

표 ***84: IM and Presence*** 서비스 포트 - 외부 데이터베이스 요청

보낸 사람(전송자)	받는 사람(리스너)	프로토콜	전송 프로토콜	대상/리스너	소스/전송자	참고
IM and Presence	PostgreSQL 데이터베이스	TCP	TCP	5432[1]	임시	PostgreSQL 데이터베이스 수신 대기 포트
IM and Presence	Oracle 데이터베이스	TCP	TCP	1521	임시	Oracle 데이터베이스 수신 대기 포트
IM and Presence	MSSQL 데이터베이스	TCP	TCP	1433	임시	MSSQL 데이터베이스 수신 대기 포트

[1] 이것은 기본 포트이지만 모든 포트에서 수신 대기하도록 PostgreSQL 데이터베이스를 구성할 수 있습니다.

표 ***85: IM and Presence*** 서비스 포트 - 고가용성 요청

보낸 사람(전송자)	받는 사람(리스너)	프로토콜	전송 프로토콜	대상/리스너	소스/전송자	참고
IM and Presence (서버 복구 매니저)	IM and Presence (서버 복구 매니저)	TCP	TCP	20075	임시	Cisco 서버 복구 매니저가 admin rpc 요청을 제공하는 데 사용하는 포트입니다.
IM and Presence (서버 복구 매니저)	IM and Presence (서버 복구 매니저)	UDP	UDP	21999	임시	Cisco 서버 복구 매니저가 피어와 통신하는 데 사용하는 포트입니다.

표 ***86: IM and Presence*** 서비스 포트 - 인 메모리 데이터베이스 복제 메시지

보낸 사람(전송자)	받는 사람(리스너)	프로토콜	전송 프로토콜	대상/리스너	소스/전송자	참고
IM and Presence	IM and Presence	Proprietary	TCP	6603*	임시	Cisco Presence 데이터 저장소

보낸 사람(전송자)	받는 사람(리스너)	프로토콜	전송 프로토콜	대상/리스너	소스/전송자	참고
IM and Presence	IM and Presence	Proprietary	TCP	6604*	임시	Cisco 로그인 데이터 저장소
IM and Presence	IM and Presence	Proprietary	TCP	6605*	임시	Cisco SIP 등록 데이터 저장소
IM and Presence	IM and Presence	Proprietary	TCP	9003	임시	Cisco 프레즌스 데이터 저장소 이중 노드 하위 클러스터 복제.
IM and Presence	IM and Presence	Proprietary	TCP	9004	임시	Cisco 로그인 데이터 저장소 이중 노드 하위 클러스터 복제.
IM and Presence	IM and Presence	Proprietary	TCP	9005	임시	Cisco SIP 등록 데이터 저장소 이중 노드 하위 클러스터 복제.

* 관리 CLI 진단 유틸리티를 실행하려면 `utils imdb_replication status` 명령을 사용하여 이러한 포트가 클러스터의 IM 및 프레즌스 서비스 노드 사이에 설정된 모든 방화벽에서 열려 있어야 합니다. 정상적인 작동에는 이 설정이 필요하지 않습니다.

표 ***87: IM and Presence*** 서비스 포트 - 인메모리 데이터베이스 ***SQL*** 메시지

보낸 사람(전송자)	받는 사람(리스너)	프로토콜	전송 프로토콜	대상/리스너	소스/전송자	참고
IM and Presence	IM and Presence	Proprietary	TCP	6603	임시	Cisco Presence 데이터 저장소 SQL 쿼리.
IM and Presence	IM and Presence	Proprietary	TCP	6604	임시	Cisco 로그인 데이터 저장소 SQL 쿼리.
IM and Presence	IM and Presence	Proprietary	TCP	6605	임시	Cisco SIP 등록 데이터 저장소 SQL 쿼리.
IM and Presence	IM and Presence	Proprietary	TCP	6606	임시	Cisco 라우트 데이터 저장소 SQL 쿼리.

표 ***88: IM and Presence*** 서비스 포트 **-** 인메모리 데이터베이스 알림 메시지

보낸 사람(전송자)	받는 사람(리스너)	프로토콜	전송 프로토콜	대상/리스너	소스/전송자	참고
IM and Presence	IM and Presence	Proprietary	TCP	6607	임시	Cisco Presence 데이터 저장소 XML 기반 변경 알림.
IM and Presence	IM and Presence	Proprietary	TCP	6608	임시	Cisco 로그인 데이터 저장소 XML 기반 변경 알림.
IM and Presence	IM and Presence	Proprietary	TCP	6609	임시	Cisco SIP 등록 데이터 저장소 XML 기반 변경 알림.
IM and Presence	IM and Presence	Proprietary	TCP	6610	임시	Cisco 라우트 데이터 저장소 XML 기반 변경 알림.

표 ***89: IM and Presence*** 서비스 포트 **-** 강제 수동 동기화***/X.509*** 인증서 업데이트 요청

보낸 사람(전송자)	받는 사람(리스너)	프로토콜	전송 프로토콜	대상/리스너	소스/전송자	참고
IM and Presence (Intercluster 동기화 에이전트)	IM and Presence (Intercluster 동기화 에이전트)	TCP	TCP	37239	임시	Cisco 클러스터 간 동기화 에이전트 서비스는 이 포트를 사용하여 명령을 처리하기 위한 소켓 연결을 설정합니다.

표 ***90: IM and Presence*** 서비스 포트 **-** ***ICMP*** 요청

보낸 사람(전송자)	받는 사람(리스너)	대상 포트	목적
엔드포인트/IM and Presence	IM and Presence	7	인터넷 제어 메시 (ICMP). 이 프로 에코 관련 트래픽 다. 열 머리글에 포트를 구성하지
IM and Presence	엔드포인트/IM and Presence		

표 *91: IM and Presence*에 사용되는 포트 - *Cisco Unified CM* 통신 및 *IM and Presence* 게시자 - 가입자 통신

보낸사람(전송자)	받는사람(리스너)	전송 프로토콜	대상/리스너	소스/전송자	참고
Cisco Unified Communications Manager	IM and Presence 게시자	TCP	1500	양방향	데이터베이스 클라이언트를 위한 내부 ID 포트입니다. 로컬 호스트 트래픽 전용입니다.
Cisco Unified Communications Manager	IM and Presence 게시자	TCP	8443	양방향	웹 관리에 대한 액세스를 제공합니다.
Cisco Unified Communications Manager	IM and Presence 게시자	TCP	1090	양방향	AMC RMI 개체 포트입니다. RTMT 성능 모니터, 데이터 수집, 로깅 및 경고용 Cisco AMC 서비스
Cisco Unified Communications Manager	IM and Presence 게시자	TCP	2555	양방향	양방향 실시간 정보 서비스(RIS) 데이터베이스 서버. 클러스터의 다른 RISDC 서비스에 연결하여 클러스터 전체의 실시간 정보를 제공
Cisco Unified Communications Manager	IM and Presence 게시자	TCP	8500	양방향	내부 포트 - 플랫폼 데이터(호스트) 인증서의 클러스터 복제를 위해 ipsec_mgr 데몬에서 사용하는 클러스터 관리자 포트
Cisco Unified Communications Manager	IM and Presence 게시자	TCP	8600	양방향	구성 에이전트 하트비트 포트
Cisco Unified Communications Manager	IM and Presence 게시자	UDP	123	양방향	시간 동기화에 사용되는 NTP(Network Time Protocol)
IM and Presence 게시자	IM and Presence 가입자	UDP	50000	양방향	내부 포트입니다. 로컬 호스트 트래픽 전용입니다. LiveBus 메시징 포트입니다. IM and Presence 서비스는 이 포트를 클러스터 통신에 사용합니다.

보낸사람(전송자)	받는사람(리스너)	전송 프로토콜	대상/리스너	소스/전송자	참고
IM and Presence 게시자	IM and Presence 가입자	UDP	21999	양방향	Cisco 서버 복구 매니저가 피어와 통신하는 데 사용하는 포트입니다.
IM and Presence 게시자	Cisco Unified Communications Manager	TCP	4040	양방향	로컬 에이전트, GUI 및 CLI에서 연결을 허용하는 DRF 마스터 에이전트 서버 포트
IM and Presence 게시자	Cisco Unified Communications Manager	TCP	8001	양방향	영구 채팅을 구성하는 중에 사용됩니다.
IM and Presence 게시자	Cisco Unified Communications Manager	TCP	6379	양방향	관리형 파일 전송(MFT)을 구성하는 동안 사용됩니다.
IM and Presence 게시자	IM and Presence 가입자	TCP	7	양방향	외부 데이터베이스(MSSQL)를 구성하는 중에 사용됩니다.
IM and Presence 게시자	IM and Presence 가입자	TCP	20075	양방향	Cisco 서버 복구 매니저가 admin RPC 요청을 제공하는 데 사용하는 포트입니다.
IM and Presence 게시자	IM and Presence 가입자	TCP	8600	양방향	구성 에이전트 하트비트 포트
IM and Presence 가입자	IM and Presence 게시자	TCP	9005	양방향	Cisco SIP 등록 데이터 저장소 이중 노드 하위 클러스터 복제.
IM and Presence 가입자	IM and Presence 게시자	TCP	9003	양방향	Cisco 프레즌스 데이터 저장소 이중 노드 하위 클러스터 복제.
IM and Presence 가입자	IM and Presence 게시자	TCP	20075	양방향	Cisco 서버 복구 매니저가 admin RPC 요청을 제공하는 데 사용하는 포트입니다.
IM and Presence 가입자	IM and Presence 게시자	TCP	9004	양방향	Cisco 로그인 데이터 저장소 이중 노드 하위 클러스터 복제.

보낸사람(전송자)	받는사람(리스너)	전송프로토콜	대상/리스너	소스/전송자	참고
Cisco Unified Communications Manager	IM and Presence 게시자	TCP	5070	양방향	통화 구성에 사용됨
IM and Presence 게시자	IM and Presence 가입자	TCP	44000	양방향	통화 구성에 사용됨

표 ***92: On-a-call_Presence***

보낸사람(전송자)	받는사람(리스너)	소스 포트	대상 포트	프로토콜	참고
Cisco Unified Communications Manager	IM and Presence 게시자	[37240 – 61000]	5070	TCP	
IM and Presence 게시자	XMPP 클라이언트(Jabber)	5222	64846	TCP	클라이언트 액세스 포트
IM and Presence 게시자	XMPP 클라이언트(Jabber)	5222	56361	TCP	클라이언트 액세스 포트

표 ***93: MS-SQL DB*** 구성

보낸 사람(전송자)	받는 사람(리스너)	소스 포트	대상 포트	프로토콜
IM and Presence 게시자	데이터베이스	[37240 – 61000]	7	TCP

표 ***94: MS-SQL*** 영구 채팅 구성

보낸 사람(전송자)	받는 사람(리스너)	소스 포트	대상 포트	프로토콜
IM and Presence 게시자	데이터베이스	37240 – 61000	1433	TCP

표 ***95:*** 관리형 파일 전송***(MFT)*** 구성

보낸 사람(전송자)	받는 사람(리스너)	소스 포트	대상 포트	프로토콜
IM and Presence 게시자	외부 파일 서버	37240 – 61000	7	TCP

보낸 사람(전송자)	받는 사람(리스너)	소스 포트	대상 포트	프로토콜
IM and Presence 게시자	외부 파일 서버	37240 – 61000	22	TCP
IM and Presence 게시자	외부 파일 서버	37240 – 61000	5432	TCP
IM and Presence 게시자	데이터베이스	54288 - 54292	5432	TCP

SNMP에 대한 자세한 내용은 *Cisco Unified Serviceability* 관리 설명서를 참조하십시오.

37 장

추가 요구 사항

고가용성 로그인 프로파일

고가용성 로그인 프로파일에 대한 중요한 참고 사항

- 프레즌스 이중화 그룹에서 클라이언트 다시 로그인의 상한값과 하한값을 구성하려면 이 섹션의 고가용성 로그인 프로파일 테이블을 사용할 수 있습니다. **Cisco Unified CM IM and Presence** 관리 시스템 > 서비스 파라미터를 선택한 다음 [서비스] 메뉴에서 **Cisco Server Recovery Manager**를 선택하여 클라이언트 다시 로그인의 상한값과 하한값을 구성합니다.
- 고가용성 클라이언트 로그인 프로파일은 단일 클러스터 구축에만 적용됩니다. 고가용성 클라이언트 로그인 프로파일은 여러 클러스터가 있는 경우 이중화 그룹에 대한 클라이언트 재로그인의 상한값과 하한값을 구성할 수 없습니다. 여러 클러스터 구축에서 고가용성 클라이언트 로그인 프로파일을 검색하려면 더 많은 테스트를 수행해야 합니다.
- Cisco XCP 라우터 서비스에 대해 디버그 로깅이 활성화된 경우에는 증가하는 CPU 사용량을 예상하고 IM and Presence 서비스에 대해 현재 지원되는 로깅 수준이 감소해야 합니다.
- 여기에서 제공하는 테이블을 기반으로 프레즌스 이중화 그룹에서 클라이언트 다시 로그인의 상한값과 하한값을 구성하면 구축 시 성능 문제 및 CPU 사용 급증 문제를 피할 수 있습니다.
- Cisco에서는 각 IM and Presence 서비스 노드 메모리 크기 및 각 고가용성 구축 유형(Active/Active 또는 Active/Standby)에 대한 고가용성 로그인 프로파일을 제공합니다.
- 고가용성 로그인 프로파일 테이블은 다음과 같은 입력을 기반으로 계산됩니다.
  - 클라이언트 다시 로그인 하한값은 서버 복구 관리자 서비스 파라미터인 "중요 서비스 중지 지연(Critical Service Down Delay)"을 기반으로 하며, 기본값은 90초입니다. 중요 서비스 중지 지연(Critical Service Down Delay)을 변경하면 하한값도 변경됩니다.

- Active/Standby 구축용 프레즌스 이중화 그룹 또는 Active/Active 구축에서 사용자 수가 가장 많은 노드의 총 사용자 수.

- 프레즌스 이중화 그룹의 두 노드에서 클라이언트 다시 로그인의 상한값과 하한값을 구성해야 합니다. 프레즌스 이중화 그룹의 두 노드에서 이 모든 값을 수동으로 구성해야 합니다.
- 클라이언트 다시 로그인의 상한값과 하한값은 프레즌스 이중화 그룹의 각 노드에서 동일해야 합니다.
- 사용자를 균형 조정하는 경우 고가용성 로그인 프로파일 테이블을 기반으로 클라이언트 다시 로그인의 상한값과 하한값을 다시 구성해야 합니다.

고가용성 로그인 프로파일 테이블 사용

다음 값을 검색하려면 고가용성 로그인 프로파일 테이블을 사용하십시오.

- 클라이언트 재로그인 하한**(Client Re-Login Lower Limit)** 서비스 파라미터 값
- 클라이언트 재로그인 상한**(Client Re-Login Upper Limit)** 서비스 파라미터 값

프로시저

단계 **1** 가상 하드웨어 구성 및 고가용성 구축 유형을 기반으로 프로파일 테이블을 선택합니다.

단계 **2** 프로파일 테이블에서 구축의 사용자 수를 선택합니다(근사치로 반올림). Active/Standby 구축에서는 사용자 수가 가장 많은 노드를 사용합니다.

단계 **3** 프레즌스 이중화 그룹에 대한 사용자 수 값을 기반으로 프로파일 테이블에서 해당 재시도 하한과 상한을 검색합니다.

단계 **4** **Cisco Unified CM IM and Presence** 관리 > 시스템 > 서비스 파라미터파라미터를 선택하고 서비스 메뉴에서 **Cisco** 서버 복구 매니저를 선택하여 IM and Presence 서비스에서 재시도 하한과 상한을 설정합니다.

단계 **5** **Cisco Unified CM IM and Presence** 관리 > 시스템 > 서비스 파라미터를 선택하고 서비스 메뉴에서 **Cisco** 서버 복구 매니저를 선택하여 중요 서비스 중지됨 지연 값을 확인합니다. 기본값은 90초입니다. 재시도 하한을 이 값으로 설정해야 합니다.

고가용성 및 로그인 구성 예

예 **1: 15000** 사용자 전체 **UC** 프로파일 **- Active/Active** 구축

프레즌스 이중화 그룹에 사용자 3000명이 있는데, 한 노드에 2000명이 있고 두 번째 노드에 1000명이 있습니다. Unbalanced Active/Active 구축에서는 사용자 수가 가장 많은 노드(이 경우에는 사용자 2000명의 노드)를 사용하는 것이 좋습니다. 사용자 15000명 전체 UC(4 vCPU 8GB) Active/Active 프로파일을 사용하면 다음의 재시도 상한값 및 하한값이 검색됩니다.

예상 Active 사용자 수	재시도 하한	재시도 상한
2000	120	253

참고 재시도 상한은 장애 조치 발생 이후 모든 클라이언트가 해당 백업 노드에 로그인하는 데 걸리는 대략적인 시간(초)입니다.

참고 하한값 120은 중요 서비스 중지 지연**(Critical Service Down Delay)** 서비스 파라미터가 120으로 설정됨을 의미합니다.

예 **2: 5000** 사용자 전체 **UC** 프로파일 **- Active/Active** 구축

에서 프레즌스 이중화 그룹의 각 노드에 사용자 4700명이 있습니다. 사용자 5000명 전체 US(4 vCPU 8GB) Active/Active 프로파일을 사용하여 사용자 수 5000을 기준으로 재시도 상한값과 하한값을 검색할 수 있도록 근사치로 반올림하는 것이 좋습니다.

예상 Active 사용자 수	재시도 하한	재시도 상한
5000	120	953

단일 클러스터 구성

사용자 **500**명 전체 **UC(1vCPU 700MHz 2GB) Active/Active** 프로파일

표 ***96:*** 표준 구축을 위한 사용자 로그인 재시도 제한**(**사용자 ***500***명 전체 ***UC Active/Active)***

예상 **Active** 사용자 수	재시도 하한	재시도 상한
전체 **UC**		
100	120	187
250	120	287

사용자 500명 전체 UC(1vCPU 700MHz 2GB) Active/Standby 프로파일

표 97: 표준 구축을 위한 사용자 로그인 재시도 제한(사용자 500명 전체 UC Active/Standby)

예상 Active 사용자 수	재시도 하한	재시도 상한
전체 UC		
100	120	187
250	120	287
500	120	453

사용자 1000명 전체 UC(1vCPU 1500MHz 2GB) Active/Active 프로파일

표 98: 표준 구축을 위한 사용자 로그인 재시도 제한(사용자 1000명 전체 UC Active/Active)

예상 Active 사용자 수	재시도 하한	재시도 상한
전체 UC		
100	120	153
250	120	203
500	120	287

사용자 1000명 전체 UC(1vCPU 1500MHz 2GB) Active/Standby 프로파일

표 99: 표준 구축을 위한 사용자 로그인 재시도 제한(사용자 1000명 전체 UC Active/Standby)

예상 Active 사용자 수	재시도 하한	재시도 상한
전체 UC		
100	120	153
250	120	203
500	120	287
750	120	370
1000	120	453

사용자 2000명 전체 UC(1vCPU 1500Mhz 4GB) Active/Active 프로파일

표 *100:* 표준 구축을 위한 사용자 로그인 재시도 제한*(*사용자 *2000*명 전체 *UC Active/Active)*

예상 **Active** 사용자 수	재시도 하한	재시도 상한
전체 **UC**		
100	120	153
500	120	287
1000	120	453

사용자 2000명 전체 UC(1vCPU 1500Mhz 4GB) Active/Standby 프로파일

표 *101:* 표준 구축을 위한 사용자 로그인 재시도 제한*(*사용자 *2000*명 전체 *UC Active/Standby)*

예상 **Active** 사용자 수	재시도 하한	재시도 상한
전체 **UC**		
100	120	153
250	120	203
500	120	287
750	120	370
1000	120	453
1250	120	537
1500	120	620
1750	120	703
2000	120	787

사용자 5000명 전체 UC(4GB 2vCPU) Active/Active 프로파일

표 *102:* 표준 구축을 위한 사용자 로그인 재시도 제한*(*사용자 *5000*명 전체 *UC Active/Active)*

예상 **Active** 사용자 수	재시도 하한	재시도 상한
전체 **UC**		
100	120	137
500	120	203

예상 **Active** 사용자 수	재시도 하한	재시도 상한
1000	120	287
1500	120	370
2000	120	453
2500	120	537

사용자 5000명 전체 UC(4GB 2vCPU) Active/Standby 프로파일

주의 사용자 5000명 규모 시스템에서 최대 클라이언트 로그인 처리량을 달성하려면 최소 2.6GHz CPU 클럭 속도를 사용하는 것이 좋습니다.

표 *103:* 표준 구축을 위한 사용자 로그인 재시도 제한*(*사용자 *5000*명 전체 *UC Active/Standby)*

예상 **Active** 사용자 수	재시도 하한	재시도 상한
전체 **UC**		
100	120	154
500	120	287
1000	120	453
1500	120	620
2000	120	787
2500	120	953
3000	120	1120
3500	120	1287
4000	120	1453
4500	120	1620
5000	120	1787

사용자 15000명 전체 UC(4 vCPU 8GB) Active/Active 프로파일

주의 사용자 15000명 규모 시스템에서 최대 클라이언트 로그인 처리량을 달성하려면 최소 2.5GHz CPU 클럭 속도를 사용하는 것이 좋습니다.

표 *104:* 표준 구축을 위한 사용자 로그인 재시도 제한*(*사용자 *15000*명 전체 *UC Active/Active)*

예상 **Active** 사용자 수	재시도 하한	재시도 상한
전체 **UC**		
100	120	127
500	120	153
1000	120	187
1500	120	220
2000	120	253
2500	120	287
3000	120	320
3500	120	353
4000	120	387
4500	120	420
5000	120	453
6000	120	520
7000	120	587
7500	120	620

사용자 15000명 전체 UC(4 vCPU 8GB) Active/Standby 프로파일

주의 사용자 15000명 규모 시스템에서 최대 클라이언트 로그인 처리량을 달성하려면 최소 2.6GHz CPU 클럭 속도를 사용하는 것이 좋습니다.

표 *105:* 표준 구축을 위한 사용자 로그인 재시도 제한*(*사용자 *15000*명 전체 *UC Active/Standby)*

예상 **Active** 사용자 수	재시도 하한	재시도 상한
전체 **UC**		
100	120	137
500	120	203

예상 **Active** 사용자 수	재시도 하한	재시도 상한
1000	120	287
1500	120	370
2000	120	453
2500	120	537
3000	120	620
3500	120	703
4000	120	787
4500	120	870
5000	120	953
6000	120	1120
7000	120	1287
8000	120	1453
9000	120	1620
10000	120	1787
11000	120	1953
12000	120	2120
13000	120	2287
14000	120	2453
15000	120	2620

사용자 25000명 전체 UC(6 vCPU 16GB) Active/Standby 프로파일

주의 사용자 25000명 규모 시스템에서 최대 클라이언트 로그인 처리량을 달성하려면 최소 2.8GHz CPU 클럭 속도를 사용하는 것이 좋습니다.

표 *106:* 활성/활성 프로파일에 대한 로그인 속도*: 9*는 *45% CPU*를 사용

예상 **Active** 사용자 수	재시도 하한	재시도 상한
100	120	131

예상 **Active** 사용자 수	재시도 하한	재시도 상한
500	120	176
1000	120	231
1500	120	287
2000	120	342
2500	120	398
3000	120	453
3500	120	509
4000	120	564
4500	120	620
5000	120	676
6000	120	787
7000	120	898
7500	120	953
8000	120	1009
9000	120	1120
10000	120	1231
11000	120	1342
12000	120	1453
12500	120	1509

사용자 25000명 전체 UC(6 vCPU 16GB) Active/Standby 프로파일

주의 사용자 25000명 규모 시스템에서 최대 클라이언트 로그인 처리량을 달성하려면 최소 2.6GHz CPU 클럭 속도를 사용하는 것이 좋습니다.

표 ***107:*** 활성/대기 프로파일에 대한 로그인 비율***: 16***명 사용자 ***80% CPU***

예상 활성 사용자 수	재시도 하한	재시도 상한
100	120	133

예상 활성 사용자 수	재시도 하한	재시도 상한
500	120	183
1000	120	245
1500	120	308
2000	120	370
2500	120	433
3000	120	495
3500	120	558
4000	120	620
4500	120	683
5000	120	745
6000	120	870
7000	120	995
8000	120	1058
9000	120	1120
10000	120	1245
11000	120	1370
12000	120	1495
13000	120	1620
14000	120	1870
15000	120	1995
16000	120	2120
17000	120	2245
18000	120	2370
19000	120	2495
20000	120	2620
21000	120	2745
22000	120	2870
23000	120	2995

예상 활성 사용자 수	재시도 하한	재시도 상한
24000	120	3120
25000	120	3245

XMPP 표준 규정 준수

IM and Presence 서비스는 다음의 XMPP 표준을 준수합니다.

- RFC 3920 XMPP(Extensible Messaging and Presence Protocol) : 코어 RFC 3921 XMPP (Extensible Messaging and Presence Protocol): 인스턴트 메시징 및 프레즌스
  - XEP-0004 Data Forms
  - XEP-0012 Last Activity
  - XEP-0013 Flexible Offline Message Retrieval
  - XEP-0016 Privacy Lists
  - XEP-0030 Service Discovery
  - XEP-0045 Multi-User Chat
  - XEP-0054 Vcard-temp
  - XEP-0055 Jabber Search
  - XEP-0060 Publish-Subscribe
  - XEP-0065 SOCKS5 Bystreams
  - XEP-0066 Out of Band Data Archive OOB requests
  - XEP-0068 Field Standardization for Data Forms
  - XEP-0071 XHTML-IM
  - XEP-0082 XMPP Date and Time Profiles
  - XEP-0092 Software Version
  - XEP-0106 JID Escaping
  - XEP-0114 Jabber Component Protocol
  - XEP-0115 Entity Capabilities
  - XEP-0124 BOSH(Bidirectional Streams over Synchronous HTTP)
  - XEP-0126 Invisibility
  - XEP-0128 Service Discovery Extensions

- XEP-0160 Best Practices for Handling Offline Messages
- XEP-0163 Personal Eventing Via PubSub
- XEP-0170 Recommended Order of Stream Feature Negotiation
- XEP-0178 Best Practices for Use of SASL EXTERNAL
- XEP-0220 Server Dialback
- XEP-0273 SIFT(Stanza Interception and Filtering Technology)

구성 변경 및 서비스 다시 시작 알림

서비스를 다시 시작해야 할 때마다 활성 알림 팝업이 나타납니다. Cisco Unified CM IM and Presence 관리 GUI 헤더의 오른쪽 위에 활성 알림 요약이 있습니다.

또한 Cisco Unified CM IM and Presence 관리 인터페이스에서 시스템 > 알림을 선택하여 활성 알림 목록에 액세스할 수 있습니다.

다시 시작해야 하는 구성 변경

많은 IM and Presence 구성 변경 및 업데이트의 경우 Cisco XCP 라우터, Cisco SIP Proxy 또는 Cisco Presence 엔진을 다시 시작해야 합니다.

다음 표에서는 이러한 서비스를 다시 시작해야 하는 구성 변경 사항을 보여줍니다. 이 목록에는 구성 변경 사항이 포함되지만 설치 또는 업그레이드와 같은 플랫폼 변경은 포함되지 않습니다.

다시 시작해야 하는 구성	이 서비스 다시 시작
애플리케이션 리스너 구성 (시스템 > 애플리케이션 리스너) 애플리케이션 리스너 편집	Cisco SIP Proxy
준수 프로파일 구성 (메시징 > 준수 > 준수 설정) (메시징 > 준수 > 준수 프로파일 타사 컴플라이언스 서버에 할당된 이벤트 설정을 편집하는 경우	Cisco XCP 라우터
그룹 채팅 시스템 관리자 (메시징 >그룹 채팅 시스템 관리자) 이 설정을 활성화하거나 비활성화하는 경우	Cisco XCP 라우터

다시 시작해야 하는 구성	이 서비스 다시 시작
외부 파일 서버 구성 (메시징 > 외부 서버 설정 > 외부 파일 서버) 호스트**/IP** 주소 설정을 편집하는 경우 외부 파일 서버 공개 키를 재생성하는 경우	Cisco XCP 라우터
그룹 채팅 및 영구 채팅 구성 (메시징 > 그룹 채팅 및 영구 채팅) 시작시 채팅 노드가 외부 DB에 연결할 수 없는 경우 Cisco XCP 텍스트 전화회의 관리자 서비스가 실행되고 있지 않습니다.	Cisco XCP 라우터
그룹 채팅 서버 별칭 매핑 (메시징 > 그룹 채팅 서버 별칭 매핑) 채팅 별칭 추가	Cisco XCP 라우터
ACL 구성 (시스템 > 보안 > 수신 ACL) (시스템 > 보안 > 발신 ACL) 수신 및 발신 ACL 구성 편집	Cisco SIP Proxy
준수 설정 메시지 보관 - 설정 편집	Cisco XCP 라우터
LDAP 서버 (애플리케이션 > 타사 클라이언트 > 타사 LDAP 설정) LDAP 검색 - LDAP 검색 편집 LDAP에서 vCards 빌드 편집 Vcard FN에 사용할 LDAP 특성 편집	Cisco XCP 라우터
메시지 설정 구성 (메시징 > 설정) 인스턴트 메시지 활성화 편집 오프라인 인스턴트 메시징 표시 안 함	Cisco XCP 라우터

다시 시작해야 하는 구성	이 서비스 다시 시작
프레즌스 게이트웨이 (프레즌스 > 게이트웨이) 프레즌스 게이트웨이 추가, 편집, 삭제 MS Exchange 인증서를 업로드 후	Cisco Presence 엔진
프레즌스 설정 구성 (프레즌스 > 설정 > 표준 구성) 가용성 공유 활성화 설정 편집 사용자에게 승인에 대한 메시지를 표시하지 않고 다른 사용자의 사용 가능성을 볼 수 있도록 허용 최대 연락처 목록 크기(사용자별) 최대 관찰자 수	Cisco Presence 엔진 Cisco XCP 라우터
프레즌스 설정 구성 (프레즌스 > 설정 > 표준 구성) 도메인 간 페더레이션에 대해 전자 메일 주소 사용 활성화 필드 편집	Cisco XCP 라우터
파티션된 도메인간 페더레이션 구성 프레즌스 > 설정 > 표준 구성(확인란) 프레즌스 > 도메인 간 페더레이션 설정(마법사) 확인란 또는 마법사를 통해 Lync/OCS/LCS를 사용하여 분할된 도메인 내 페더레이션 활성화 파티션된 도메인 간 라우팅 모드 - 표준 구성 창 또는 마법사를 통해 구성	이 설정을 편집하면 Cisco SIP Proxy가 자동으로 다시 시작됩니다. 또한 XCP 라우터를 다시 시작해야 합니다.
프록시 구성 (프레즌스 > 라우팅 > 설정) 프록시 구성 편집	Cisco SIP Proxy
보안 설정 (시스템 > 보안 > 설정) SIP 클러스터 간 프록시 간 전송 프로토콜과 같은 SIP 보안 설정 편집 XMPP 보안 설정 편집	Cisco SIP Proxy(SIP 보안 편집의 경우) Cisco XCP 라우터 (XMPP 보안 편집의 경우)
SIP 페더레이션 도메인 (프레즌스 > 도메인 간 페더레이션 > SIP 페더레이션) 이 구성 추가, 편집, 삭제	Cisco XCP 라우터

다시 시작해야 하는 구성	이 서비스 다시 시작
타사 준수 서비스 (애플리케이션 > 타사 클라이언트 > 타사 LDAP 서버) 호스트 이름/IP 주소, 포트, 암호/확인 암호 필드 편집	Cisco XCP 라우터
TLS 피어 제목 구성 (시스템 > 보안 > TLS 피어 주체) 이 페이지에서 편집	Cisco SIP Proxy
TLS 컨텍스트 (시스템 > 보안 > TLS 상황 구성) 이 페이지에서 편집	연결된 채팅 서버를 다시 시작해야 합니다.
XMPP Federation (프레즌스 > 도메인 간 페더레이션 > XMPP 페더레이션 > 설정) (프레즌스 > 도메인 간 페더레이션 > XMPP 페더레이션 > 정책) XMPP 페더레이션 편집	Cisco XCP 라우터
인터클러스터 피어링 (프레즌스 클러스터 간) 인터클러스터 피어 구성 편집	경우에 따라 Cisco XCP 라우터를 다시 시작하라는 메시지가 나타날 수도 있습니다(오른쪽 상단 창에 알림이 나타남).
이더넷 설정 (Cisco Unified IM and Presence OS OS 관리, 설정 > IP > 이더넷/이더넷 IPv6) 이더넷 설정 편집	시스템이 즉시 재시작됨
IPv6 구성 (시스템 > 엔터프라이즈 파라미터) IPv6 엔터프라이즈 파라미터 활성화 편집	Cisco XCP 라우터 Cisco SIP Proxy Cisco Presence 엔진
문제 해결 가입자가 오프라인인 동안 IM and Presence 게시자가 변경된 경우 가입자의 설정 > IP > 게시자 설정 편집	가입자 노드 다시 시작
IM and Presence 업그레이드 및 이전 버전으로 전환해야 함	시스템 다시 시작
cup 인증서 다시 생성	Cisco SIP Proxy Cisco Presence 엔진

다시 시작해야 하는 구성	이 서비스 다시 시작
Cup xmpp 다시 생성	Cisco XCP 라우터
cup-xmpp-s2s 인증서 다시 생성	Cisco XCP 라우터
새 인증서 업로드	해당 인증서의 관련 서비스를 다시 시작합니다. Cup-신뢰 인증서의 경우 Cisco SIP Proxy 다시 시작
원격 감사 로그 전송 프로토콜 utils remotesyslog set protocol * CLI 명령을 실행하는 경우	노드 다시 시작
다음 경고 중 하나가 표시되는 경우: • PEIDSQueryError • PEIDStoIMDBDatabaseSyncError • PEIDSSubscribeError • PEWebDAVInitializationFailure	Cisco Presence 엔진을 다시 시작하는 것이 좋습니다.
다음 경고 중 하나가 표시되는 경우: • • XCPConfigMgrJabberRestartRequired • XCPConfigMgrR2RPasswordEncryptionFailed • XCPConfigMgrR2RRequestTimedOut • XCPConfigMgrHostNameResolutionFailed	Cisco XCP 라우터를 다시 시작하는 것이 좋습니다.
PWSSCBInitFailed	Cisco SIP Proxy를 다시 시작하는 것이 좋습니다.

다시 시작해야 하는 구성	이 서비스 다시 시작
Exchange 서비스 파라미터 편집 • Microsoft Exchange 알림 포트 • 일정 표시 • Exchange 시간 초과(초) • Exchange 큐 • Exchange 스레드 • EWS 상태 빈도	Cisco Presence 엔진
Exchange 인증서 업로드	Cisco SIP Proxy Cisco Presence 엔진
로캘 설치	IM and Presence 서비스 다시 시작
새 MSSQL 외부 데이터베이스 만들기	Cisco XCP 라우터
외부 데이터베이스 구성 편집	Cisco XCP 라우터
외부 데이터베이스 병합	Cisco XCP 라우터
TLS 피어 주체 구성	Cisco SIP Proxy
피어 인증 TLS 상황 구성	Cisco SIP Proxy
다음 Cisco SIP Proxy 서비스 파라미터 편집: • CUCM 도메인 • 서버 이름(추가) • HTTP 포트 • 상태 저장 서버(트랜잭션 상태) • TCP 연결 유지 • 공유 메모리 크기(바이트) • 페더레이션 라우팅 IM/P FQDN • Microsoft 페더레이션 사용자-에이전트 헤더(쉼표로 구분)	Cisco SIP Proxy
라우팅 통신 유형 서비스 파라미터 편집	Cisco XCP 라우터
IM 주소 체계를 편집	Cisco XCP 라우터

다시 시작해야 하는 구성	이 서비스 다시 시작
기본 도메인 할당	Cisco XCP 라우터
클러스터에서 노드 삭제 또는 제거	Cisco XCP 라우터
Cisco XCP 라우터에 영향을 미치는 파라미터를 편집하려면 Cisco XCP 라우터를 다시 시작해야 합니다	Cisco XCP 라우터
라우팅 통신 유형 서비스 파라미터	Cisco XCP 라우터
Cisco XCP File Transfer Manager 서비스 파라미터 중 하나 편집: • 외부 파일 서버 사용 가능한 공간 하한 임계값 • 외부 파일 서버 사용 가능한 공간 상한 임계값	Cisco XCP 라우터
다중 디바이스 메시징 활성화 서비스 파라미터 편집	Cisco XCP 라우터
사용자당 로그온 세션의 최대 수 서비스 파라미터 편집	Cisco XCP 라우터
외부 데이터베이스에서 `install_dir /data/pg_hba.conf` 또는 `install_dir /data/postgresql.conf` 구성 파일 업데이트	Cisco XCP 라우터
마이그레이션 유틸리티: • 프레즌스 설정 창에서 사용자에게 승인에 대한 메시지를 표시하지 않고 다른 사용자의 사용 가능성을 볼 수 있도록 허용 설정 편집. • 프레즌스 설정 구성 창에서 최대 연락처 목록 크기(사용자별) 및 최대 관찰자 (사용자별) 설정 편집.	Cisco XCP 라우터
클러스터에서 노드를 삭제 또는 제거	Cisco XCP 라우터