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.

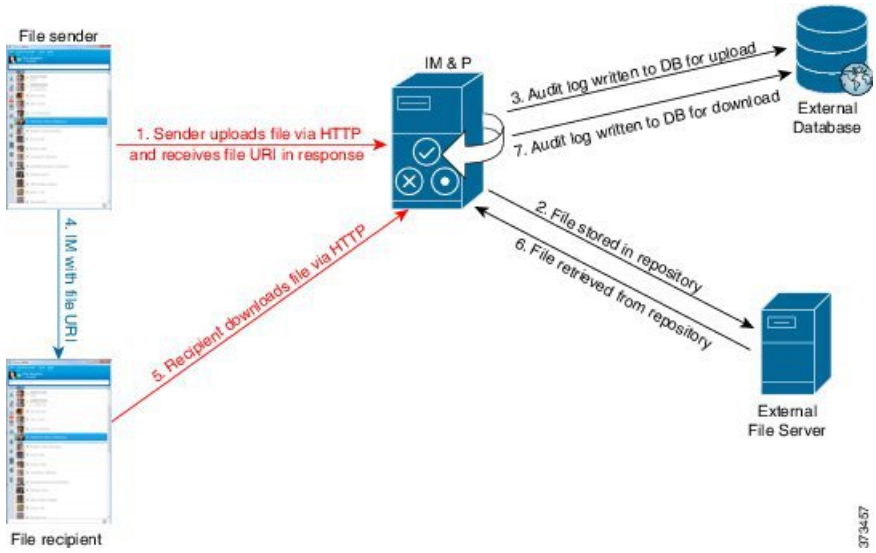
관리되는 파일 전송 기능을 구축하려면 다음 서버도 구축해야 합니다.

- 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, 2 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 구성을 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, 3 페이지
- 외부 파일 서버 요구 사항, 3 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, 10 페이지	IM and Presence 서비스에서 외부 데이터베이스에 대한 연결을 구성합니다.
단계 **2**	외부 파일 서버 설정, 11 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, 12 페이지	외부 파일 서버에 대한 사용자를 설정합니다.
단계 **4**	외부 파일 서버용 디렉터리 설정, 13 페이지	외부 파일 서버의 최상위 디렉터리 구조를 설정합니다.
단계 **5**	외부 파일 서버 공개 키 얻기, 14 페이지	외부 파일 서버 공개 키를 얻습니다.
단계 **6**	IM and Presence 서비스에서 외부 파일 서버 프로비저닝, 15 페이지	다음 외부 파일 서버 정보를 확인합니다.

	명령 또는 동작	목적
단계 **7**	Cisco XCP 파일 전송 관리자 활성화 확인, 17 페이지	관리되는 파일 전송을 활성화할 각 노드에서 Cisco XCP 파일 전송 관리자 서비스가 활성 상태여야 합니다.
단계 **8**	관리되는 파일 전송 활성화, 18 페이지	IM and Presence 서비스에서 관리되는 파일 전송을 활성화합니다.
단계 **9**	외부 서버 상태 확인, 20 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, 3 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, 12 페이지

외부 파일 서버에 대한 사용자 만들기

외부 파일 서버에 대한 사용자를 설정합니다.

시작하기 전에

외부 파일 서버 설정, 11 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, 13 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, 12 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, 14 페이지

외부 파일 서버 공개 키 얻기

외부 파일 서버 공개 키를 얻습니다.

시작하기 전에

외부 파일 서버용 디렉터리 설정, 13 페이지

프로시저

단계 **1** 파일 서버의 공개 키를 검색하려면 다음을 입력합니다.

```
$ ssh-keyscan -t rsa host
```

여기서 `호스트`는 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, 20 페이지의 내용을 참조하십시오.

다음에 수행할 작업

IM and Presence 서비스에서 외부 파일 서버 프로비저닝, 15 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, 14 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, 16 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, 17 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, 15 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, 18 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, 19 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, 20 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, 18 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.