TFTP 서버 구성

프록시 TFTP 구축 개요

프록시 TFTP(Trivial File Transfer Protocol) 서버를 사용하여 네트워크의 엔드포인트에 필요한 구성 파일(예: 다이얼 플랜, 벨소리 파일 및 디바이스 구성 파일)을 제공합니다. TFTP 서버는 구축 시 모든 클러스터에 설치될 수 있으며 여러 클러스터의 엔드포인트에서 요청을 진행할 수 있습니다. DHCP 범위는 구성 파일을 가져오기 위해 사용할 프록시 TFTP 서버의 IP 주소를 지정합니다.

리던던트 및 피어 프록시 TFTP 서버

단일 클러스터 구축의 경우 클러스터에 하나 이상의 프록시 TFTP 서버가 있어야 합니다. 리던던시를 위해 다른 프록시 TFTP 서버를 클러스터에 추가할 수 있습니다. 두 번째 프록시 TFTP 서버는 IPv4에 대한 옵션 150에 추가됩니다. IPv6의 경우, 두 번째 프록시 TFTP 서버를 DHCP 범위에 있는 TFTP 서버 주소 하위 옵션 1에 추가합니다.

다중 클러스터 구축 시에, 최대 3대의 원격 프록시 TFTP 서버를 기본 프록시 TFTP 서버의 피어 클러스터로 지정할 수 있습니다. 이 기능은 많은 DHCP 범위에 대해 한 대의 프록시 TFTP 서버만 구성하거나 하나의 DHCP 범위만 포함하려는 경우에 유용합니다. 기본 프록시 TFTP 서버는 네트워크의 모든 전화기 및 디바이스에 구성 파일을 제공합니다.

각 원격 프록시 TFTP 서버와 기본 프록시 TFTP 서버 간에 피어 관계를 생성해야 합니다.

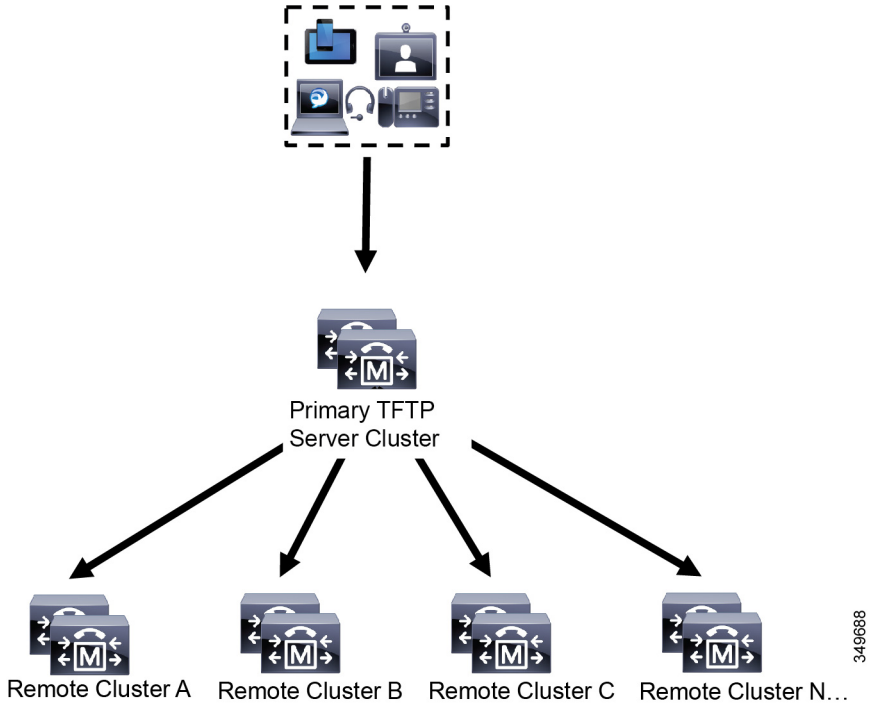
팁 네트워크의 원격 프록시 TFTP 서버 간에 피어 관계를 구성할 경우, 관계 계층 구조를 유지합니다. 루프 생성을 막기 위해 원격 클러스터의 피어 TFTP 서버가 서로를 가리키고 있지 않은지 확인하십시오. 예를 들어, 기본 노드 A가 노드 B 및 C와 피어 관계를 갖는 경우 노드 B와 C 사이에는 피어 관계를 생성하지 말아야 합니다. 이렇게 하면 루프가 생성됩니다.

프록시 TFTP

다중 클러스터 시스템에서 프록시 TFTP 서비스는 단일 기본 TFTP 서버를 통해 여러 클러스터의 TFTP 파일을 제공할 수 있습니다. 프록시 TFTP는 단일 서브넷 또는 VLAN에 여러 클러스터의 전화 또는 여러 클러스터가 동일한 DHCP TFTP 옵션 (150)을 공유하는 시나리오가 포함된 경우, 단일 TFTP 참조로 사용할 수 있습니다.

프록시 TFTP 서비스는 설명한 것처럼 단일 수준 계층 구조로 작동합니다. 더 복잡한 다중 레벨 계층 구조는 지원되지 않습니다.

그림 *1:* 프록시 ***TFTP*** 단일 수준 계층 구조



위 그림에서 디바이스 그룹은 구성 파일에 대해 기본 TFTP 서버에 연결합니다. 디바이스에서 TFTP에 대한 요청을 받으면, 기본 TFTP는 구성 파일 및 원격 클러스터 A, B, C 또는 N(구성된 다른 모든 원격 클러스터)과 같은 원격으로 구성된 모든 클러스터에 대해 자체 로컬 캐시를 조사합니다.

기본 TFTP 서버에 원하는 수의 원격 클러스터를 구성할 수 있습니다. 그러나 각 원격 클러스터에는 최대 3 개의 TFTP IP 주소만 포함될 수 있습니다. 리던던시를 위해 권장되는 설계는 클러스터 당 2개의 TFTP 서버이므로, 리던던시를 위해 주 TFTP 서버의 원격 클러스터 당 2개의 IP 주소입니다.

사용 사례 계획 모범 사례

프록시 TFTP 사용 방법 및 구현 모범 사례를 자세히 설명하고 있는 다음 시나리오를 고려하십시오.

1. 클러스터는 다른 용도로 사용되지 않을 경우 프록시 TFTP 클러스터 역할을 할 수 있습니다. 이 경우 클러스터는 다른 클러스터와 관계가 없으며 통화를 처리하지 않습니다. 이 시나리오에서는 원격 클러스터 TFTP가 수동으로 정의되고 8.0 이전으로의 롤백이 권장됩니다.

참고 이 시나리오에서는 자동 등록이 작동되지 않습니다.

2. 해당 클러스터는 원격 클러스터에 대한 프록시 TFTP 서버 역할을 하기도 하는 원격 클러스터입니다. 원격 클러스터는 수동으로 정의되므로 자동 등록을 활성화하지 않아야 합니다.

IPv4 및 IPv6 디바이스에 대한 TFTP 지원

DHCP 사용자 지정 옵션 150을 사용하도록 IPv4 전화기 및 게이트웨이를 활성화하여 TFTP 서버 IP 주소를 검색하는 것이 좋습니다. 옵션 150을 사용하여 게이트웨이 및 전화기에서 TFTP 서버 IP 주소를 검색합니다. 자세한 내용은 디바이스와 함께 제공되는 설명서를 참조하십시오.

IPv6 네트워크에서 Cisco 공급업체별 DHCPv6 정보를 사용하여 TFTP 서버 IPv6 주소를 엔드포인트에 전달하는 것이 좋습니다. 이런 방식으로 TFTP 서버 IP 주소를 옵션 값으로 구성합니다.

IPv4를 사용하는 일부 엔드포인트 및 IPv6을 사용하는 일부 엔드포인트가 있는 경우, IPv4에 대해 DHCP 사용자 지정 옵션 150을 사용하고 IPv6에 대해 TFTP 서버 주소 하위 옵션 유형 1, Cisco 공급업체별 정보 옵션을 사용하는 것이 좋습니다. TFTP 서버에서 IPv4를 사용하여 요청을 처리하는 동안 엔드포인트에서 IPv6 주소를 얻고 요청을 TFTP 서버에 보내는 경우, TFTP 서버는 IPv6 스택에서 요청을 수신하지 않기 때문에 TFTP 서버에서 요청을 받지 않습니다. 이 경우 엔드포인트를 Cisco Unified Communications Manager에 등록할 수 없습니다.

IPv4 및 IPv6 디바이스에서 TFTP 서버의 IP 주소를 검색하기 위해 사용할 수 있는 다른 방법이 있습니다. 예를 들어, IPv4 디바이스에 대해 DHCP 옵션 066 또는 CiscoCM1를 사용할 수 있습니다. IPv6 디바이스의 경우, 다른 방법으로 TFTP 서비스 하위 옵션 유형 2를 사용하는 것이나 엔드포인트에서 TFTP 서버의 IP 주소를 구성하는 것이 있습니다 이러한 대체 방법은 사용하지 않는 것이 좋습니다. 먼저 Cisco 서비스 제공자에게 문의한 다음 대체 방법을 사용하십시오.

TFTP 구축을 위한 엔드포인트 및 구성 파일

SCCP 전화기, SIP 전화기 및 게이트웨이는 초기화될 때 구성 파일을 요청합니다. 디바이스 구성을 변경할 때마다 업데이트된 구성 파일이 엔드포인트로 전송됩니다.

구성 파일에는 Unified Communications Manager 노드의 우선 순위 목록과 같은 정보, 이러한 노드에 연결하는 데 사용되는 TCP 포트, 기타 실행 파일이 포함되어 있습니다. 일부 엔드포인트의 경우, 구성 파일에 메시지, 디렉터리, 서비스 및 정보와 같은 전화기 버튼에 대한 로캘 정보와 URL이 들어 있습니다. 게이트웨이에 대한 구성 파일에는 디바이스에 필요한 모든 구성 정보가 포함되어 있습니다.

프록시 TFTP의 보안 고려 사항

Cisco 프록시 TFTP 서버는 서명된 또는 서명되지 않은 요청을 모두 처리하며, 비보안 모드 또는 혼합 모드에서 실행됩니다. 프록시 TFTP 서버에서는 전화기에서 파일을 요청할 경우 로컬 파일 시스템이나 데이터베이스를 검색하며, 검색 결과가 없을 경우 원격 클러스터에 요청을 전송합니다. 전화기에서 `ringlist.xml.sgn`, `locale file` 등과 같은 이름을 갖는 공통 파일에 대한 서버를 요청할 경우, 해당 서버는 전화기의 홈 클러스터에서 자체 파일 대신 파일의 로컬 사본을 전송합니다.

프록시 TFTP에서 파일을 수신할 때, 파일의 프록시 서버 서명이 전화기의 ITL(Initial Trust List)과 일치하지 않아 서명 검증이 실패로 돌아가 전화기에서 파일을 거부합니다. 이 문제를 해소하기 위해, 전화기의 SBD(Security by Default)를 비활성화하거나 프록시 TFTP의 CallManager 인증서를 새로운(원격/홈) 클러스터 phone-sast-trust로 가져올 수 있습니다. 그런 다음 전화기를 TVS(Trust Verification Service)에 문의하여 프록시 TFTP 인증서를 신뢰합니다. EMCC가 구축 시 활성화되어 있으면 벌크 인증서 교환이 필요합니다

보안(기본값)을 비활성화하려면 "Cisco Unified IP Phone에 대한 ITL 파일 업데이트" 섹션 Cisco 통합 커뮤니케이션 매니저 보안 설명서의 내용을 참조하십시오.

혼합 모드의 프록시 TFTP

혼합 모드로 실행 중인 원격 클러스터의 TFTP 서버에서 기본 프록시 TFTP 서버 인증서를 Cisco CTL(Certificate Trust List) 파일에 추가해야만 합니다. 그렇지 않으면 보안이 활성화되어 있는 클러스터에 등록하는 엔드포인트가 필요한 파일을 다운로드할 수 없습니다. 이를 위해, 인증서 벌크 가져오기-내보내기를 수행한 이후 CTL 파일을 업데이트합니다.

벌크 인증서 내보내기를 수행하기 위해 인터클러스터에 IP 전화기를 마이그레이션할 때 자세한 내용은, Cisco 통합 커뮤니케이션 매니저 보안 설명서의 "벌크 인증서 내보내기" 섹션을 참조하십시오.

프록시 TFTP 환경에서 클러스트 간에 전화기 이동

프록시 TFTP 환경에서 하나의 원격 클러스터에서 다른 클러스터로 전화기를 이동할 때는, 다음을 수행합니다.

1. 원격 클러스터 B(대상 클러스터)에 전화기 세부 정보를 추가합니다.
2. 원격 클러스터 A(소스 클러스터)에서 전화기 세부 정보를 삭제합니다.

참고 프록시 TFTP에서 전화기 구성은 끝날 때까지 30분 걸립니다. 어떤 파일도 찾을 수 없다는 반응을 피하기 위해, 프록시 클러스터의 TFTP 서비스를 다시 시작할 수 있습니다.

3. 전화기를 재설정하여 원격 클러스터 B에서 구성 파일을 다운로드한 다음 원격 클러스터 B에 등록합니다.

TFTP 서버 구성 작업 플로우

클러스터에 대해 구성된 EMCC(Extension Mobility Cross Cluster)가 있는 경우, 시스템에서 프록시 TFTP 서버를 동적으로 구성하도록 할 수 있습니다. 그렇지 않은 경우, TFTP 서버를 설정하고 보안 모드를 수동으로 설정할 수 있습니다.

프로시저

	명령 또는 동작	목적
단계 1	다음 방법 중 하나를 사용하여 TFTP 서버를 설정합니다. • TFTP 서버 동적 구성, 5 페이지 • TFTP 서버 수동 구성, 6 페이지	ILS(Intercluster Lookup Service) 가 구성된 경우, TFTP 서버를 동적으로 설정할 수 있습니다. EMCC를 구성하지 않은 경우, TFTP 서버를 수동으로 설정합니다. 클러스터가 보안 상태인지 비보안 상태인지 나타내야만 합니다. 클러스터는 기본값으로 비보안으로 처리됩니다.
단계 2	(선택 사항) TFTP 서버에 대한 CTL 파일 업데이트, 7 페이지	CTL 클라이언트 플러그 인을 설치 하 고 혼합 모드에서 작동 하는 모든 원격 클러스터에 있는 모든 프록시 TFTP 서버의 Cisco CTL (Certificate Trust List) 파일에 기본 프록시 TFTP 서버를 추가 합니다.
단계 3	(선택 사항) 엔드포인트 디바이스를 지원하는 설명서를 참조하십시오.	프록시 TFTP 구축에 원격 클러스터가 있는 경우, 모든 원격 엔드포인트의 TVL(신뢰 확인 목록)에 프록시 TFTP 서버를 추가합니다.
단계 4	(선택 사항) TFTP 서버에 대한 비 구성 파일 수정, 8 페이지	엔드포인트가 프록시 TFTP 서버에서 요청하는 비구성 파일을 수정할 수 있습니다.
단계 5	(선택 사항) TFTP 서비스 시작 및 중지, 8 페이지	엔드포인트에 대한 수정된 비구성 파일을 업로드한 경우, 프록시 TFTP 노드에서 TFTP 서비스를 중지했다가 다시 시작합니다.
단계 6	(선택 사항) DHCP 서버를 지원하는 설명서를 참조하십시오.	다중 클러스터 구축을 위해 개별 원격 노드에 대한 DHCP 범위를 수정하여 기본 프록시 TFTP 서버의 IP 주소를 포함합니다.

TFTP 서버 동적 구성

네트워크의 ILS(Intercluster Lookup Service) 를 구성한 경우, Cisco 프록시 TFTP 서버를 동적으로 구성할 수 있습니다.

시작하기 전에

네트워크의 EMCC를 구성합니다. 자세한 내용은 Cisco Unified Communications Manager의 기능 및 서비스 설명서를 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html에서 참조하십시오.

SIP OAuth가 활성화된 경우 오프 클러스터 Tomcat 인증서의 루트 CA 인증서를 프록시 전화기 엣지 신뢰로 복사해야 합니다.

프로시저

Cisco Unified Communications Manager 관리에서 고급 기능 > 클러스터 보기 > 지금 원격 클러스터 업데이트를 선택합니다. TFTP 서버는 클러스터에 대해 자동으로 구성됩니다.

다음에 수행할 작업

원격 프록시 TFTP 서버를 엔드포인트의 신뢰 확인 목록(TVL)으로 추가해야만 합니다. 그렇지 않으면 원격 클러스터에 있는 프록시 TFTP 서버의 구성 파일을 승인하지 않습니다. 자세한 지침은 엔드포인트 디바이스를 지원하는 설명서를 참조하십시오.

TFTP 서버 수동 구성

EMCC를 구성하지 않은 상태로 네트워크에서 TFTP를 구성하려면 수동 절차를 사용해야만 합니다.

클러스터 보기에서 기본 프록시 TFTP 서버와 기타 TFTP 서버 간에 피어 관계를 설정합니다. 최대 3개의 피어 TFTP 서버를 추가할 수 있습니다.

프록시 TFTP 구축 시 각 원격 TFTP 서버에는 기본 프록시 TFTP 서버에 대한 피어 관계가 포함되어야만 합니다. 루프 생성을 막으려면 원격 클러스터의 피어 TFTP 서버가 서로를 가리키고 있지 않은지 확인하십시오.

시작하기 전에

중요 14SU1 릴리스부터 SIP OAuth가 활성화된 경우 오프 클러스터 Tomcat 인증서의 루트 CA 인증서를 프록시 전화기 엣지 신뢰로 복사해야 합니다.

프로시저

단계 **1** 원격 클러스터를 생성합니다. 다음 작업을 수행합니다.

a) Cisco Unified CM 관리에서 고급 기능 > 클러스터 보기를 선택합니다.
b) 새로 추가를 클릭합니다. 원격 클러스터 구성 창이 나타납니다.
c) TFTP 서버에 대해 최대 50자의 클러스터 ID 및 FQDN(Fully Qualified Domain name)을 입력한 다음, 저장을 클릭합니다.

   클러스터 ID에 대한 유효한 값에는 영숫자 문자, 마침표(.), 하이픈(-)이 포함됩니다. FQDN에 대한 유효한 값에는 영숫자 문자, 마침표(.), 대시(-), 별표(*), 공백이 포함됩니다.

d) (선택 사항) 원격 클러스터 서비스 구성 창에서 최대 128자의 원격 클러스터에 대한 설명을 입력합니다.

   따옴표("), 폐쇄 또는 개방 꺾쇠 괄호(> <), 백슬래시(\), 대시(-), 앰퍼샌드(&) 또는 백분율 기호(%)를 사용하지 마십시오.

단계 2 **TFTP** 확인란에 체크 표시하여 원격 클러스터의 TFTP를 활성화합니다.

단계 3 **TFTP** 를 클릭합니다.

단계 4 원격 클러스터 서비스 수동 재정의 구성] 창에서 원격 서비스 주소 수동 구성을 선택합니다.

단계 5 TFTP 서버의 IP 주소를 입력하여 이들 TFTP 서버에 대한 피어 관계를 만듭니다.

TFTP 서버 IP 주소는 최대 3개까지 입력할 수 있습니다.

단계 6 (선택 사항) 프록시 TFTP 서버가 보안 클러스터에 구축된 경우, 클러스터가 안전하다 확인란에 체크 표시합니다.

단계 7 저장을 클릭합니다.

다음에 수행할 작업

엔드포인트의 TVL(신뢰 확인 목록, Trust Verification Lists)에 원격 TFTP 서버를 추가해야만 합니다. 그렇지 않으면, 원격 클러스터의 프록시 TFTP 서버에서 구성 파일을 승인하지 않습니다. 자세한 지침은 엔드포인트 디바이스를 지원하는 설명서를 참조하십시오.

TFTP 서버에 대한 CTL 파일 업데이트

혼합 모드에 있는 각 클러스터에서 `utils ctl`을 실행하여 퍼블리셔 노드의 CTL 파일을 업데이트합니다. 프록시 TFTP 서버와 모든 인터클러스터에 완전한 보안 네트워크가 확보되었는지 확인하십시오. 즉, 이는 프록시 및 원격 인터클러스터 인증서의 벌크 가져오기 및 내보내기 교환을 의미합니다.

CTLClient를 사용하는 동안 기본 TFTP 서버 또는 기본 TFTP 서버의 IP 주소를 혼합 모드로 실행 중인 원격 클러스터의 모든 TFTP 서버에 대한 Cisco CTL(Certificate Trust List) 파일에 추가해야 합니다. 이렇게 하는 이유는 보안 활성 클러스터의 엔드포인트에서 구성 파일을 성공적으로 다운로드할 수 있도록 지원하기 위해서입니다.

보안 및 Cisco CTL CLI 사용에 대한 자세한 내용은 Cisco 통합 커뮤니케이션 매니저 보안 설명서에서 "Cisco CTL 설정 정보" 섹션을 참조하십시오.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다.애플리케이션 > 플러그인.

단계 2 설치할 수 있는 모든 플러그인의 목록에 찾기를 클릭합니다.

단계 3 Cisco CTL 클라이언트에 대한 다운로드 링크를 클릭합니다.
시스템에서 TFTP 서버에 저장된 인증서를 디지털 서명한 클라이언트를 설치합니다.

단계 4 TFTP 서버를 재부팅합니다.

TFTP 서버에 대한 비 구성 파일 수정

엔드포인트가 프록시 TFTP 서버에서 요청하는 로드 파일 또는 `RingList.xml`과 같은 비구성 파일을 수정할 수 있습니다. 이 절차를 완료한 후에는 수정된 파일을 프록시 TFTP 서버의 TFTP 디렉터리에 업로드합니다.

프로시저

단계 **1** Cisco Unified Communications 운영체제 관리에서 소프트웨어 업그레이드 > **TFTP** 파일 관리를 선택합니다.
TFTP 파일 관리 창이 나타납니다.

단계 **2** 파일 업로드를 클릭합니다.
파일 업로드 팝업이 나타납니다.

단계 **3** 다음 작업 중 하나를 수행합니다.

- 찾아보기를 클릭하여 업로드할 파일의 디렉터리 위치를 찾습니다.
- 업데이트된 파일의 전체 디렉터리 경로를 디렉터리 필드에 붙여 넣습니다.

단계 **4** 파일 업로드를 클릭하거나 닫기를 클릭하여 파일을 업로드하지 않은 상태로 종료합니다.

다음에 수행할 작업

Cisco Unified Serviceability 관리를 사용하여 프록시 TFTP 노드에서 Cisco TFTP 서비스를 중지했다가 다시 시작합니다.

TFTP 서비스 시작 및 중지

다음 절차를 사용하여 프록시 TFTP 노드에서 TFTP 서비스를 중지하고 다시 시작합니다.

서비스 활성화에 대한 자세한 내용은 *Cisco Unified Serviceability* 관리 설명서를 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html에서 참조하십시오.

프로시저

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

단계 **2** 제어 센터-기능 서비스 창에서 서버 드롭다운 목록에서 프록시 TFTP 노드를 선택합니다.

단계 **3** **CM** 서비스 영역에서 TFTP 서비스를 선택하고 중지를 클릭합니다.

상태가 변경되어 업데이트된 상태가 반영됩니다.

팁 서비스의 최신 상태를 보려면 새로 고침을 클릭합니다.

단계 **4** **CM** 서비스 영역에서 TFTP 서비스를 선택한 다음 시작을 클릭합니다.

상태가 변경되어 업데이트된 상태가 반영됩니다.