TFTP サーバの設定

プロキシ TFTP 導入の概要

ネットワークのエンドポイントが必要とするダイヤル計画、呼出音ファイル、デバイス設定ファイルなどを提供するために、プロキシ Trivial File Transfer Protocol（TFTP）サーバを使用します。TFTP サーバは、導入する任意のクラスタに設置でき、複数のクラスタのエンドポイントから要求を処理できます。DHCP スコープでは、設定ファイルを取得するためにプロキシ TFTP サーバの IP アドレスを指定します。

冗長とピア プロキシ TFTP サーバ

単一クラスタ導入では、クラスタは、少なくとも 1 つのプロキシ TFTP サーバが必要です。別のプロキシ TFTP サーバを冗長性のためのクラスタに追加できます。2 番目のプロキシ TFTP サーバは、IPv4 のオプション 150 に追加されます。IPv6 では、DHCP スコープの TFTP サーバアドレスのサブオプションのタイプ 1 に 2 番目のプロキシ TFTP サーバを追加します。

複数のクラスタを導入する場合、プライマリ プロキシ TFTP サーバのピア クラスタとして、最大 3 台のリモート プロキシ TFTP サーバを指定できます。これは、多数の DHCP スコープに対してプロキシ TFTP サーバを 1 台だけ設定する場合に便利です。プライマリ プロキシ TFTP サーバは、ネットワークのすべての電話やデバイスに設定ファイルを提供します。

それぞれのリモート プロキシ TFTP サーバとプライマリ プロキシ TFTP サーバとの間のピア関係を作成する必要があります。

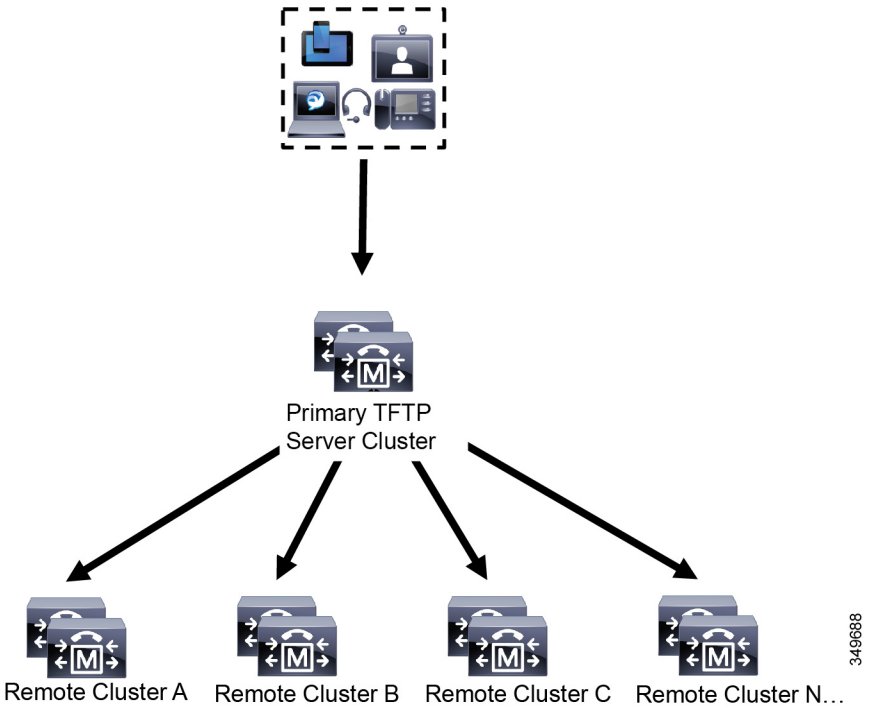
ヒント ネットワークのリモート プロキシ TFTP サーバ間のピア関係を設定する際、階層的な関係を保つようにします。ループを回避するために、リモート クラスタのピア プロキシ TFTP サーバが相互に指しあわないことを確認します。たとえば、プライマリ ノード A が、ノード B、ノード C とピア関係にあると、ノード B とノード C の間のピア関係を作成してはいけません。作成すると、ループ関係ができます。

プロキシ TFTP

マルチクラスタ システムでは、プロキシ TFTP サービスは、1 つのプライマリ TFTP サーバを介して複数のクラスタから TFTP ファイルを提供できます。単一のサブネットまたは VLAN に複数のクラスタからの電話機が含まれている場合や、複数のクラスタが同じ DHCP TFTP オプション（150）を共有している場合、プロキシ TFTP はそれらの状況に対する単一の TFTP 参照として機能できます。

プロキシ TFTP サービスは、図に示すように、単一レベルの階層として機能します。より複雑な複数レベル階層はサポートされません。

図 *1:* プロキシ *TFTP* のシングル レベル階層



この図では、デバイスのグループがプライマリ TFTP サーバと通信して、それぞれの設定ファイルを要求します。デバイスからの TFTP の要求を受信すると、プライマリ TFTP がローカル キャッシュでそれらの設定ファイルを調べるほかに、リモート クラスタ A、B、C、N（設定されているそれ以外の任意のリモート クラスタ）などリモートで設定された他のクラスタも調べます。

プライマリ TFTP サーバには任意の数のリモート クラスタを設定できます。ただし、個々のリモート クラスタに含めることができる TFTP IP アドレスは最大 3 個までです。冗長性を考慮した推奨設計は、クラスタごとに 2 台の TFTP サーバを使用することです。したがって、プライマリ TFTP サーバで、リモート クラスタあたり 2 個の IP アドレスを使用して冗長性を確保します。

IPv4 および IPv6 デバイスの TFTP サポート

TFTP サーバの IP アドレスを検出するために、IPv4 電話とゲートウェイの DHCP カスタム オプション 150 の使用を有効にすることをお勧めします。ゲートウェイと電話はオプション 150 を使用して TFTP サーバの IP アドレスを検出します。詳細については、デバイスに付属のドキュメントを参照してください。

IPv6 ネットワークでは、シスコ ベンダー固有の DHCPv6 情報を使用して、TFTP サーバの IPv6 アドレスをエンドポイントに渡すことをお勧めします。この方法では、TFTP サーバの IP アドレスをオプション値として設定します。

IPv4 を使用するエンドポイントと IPv6 を使用するエンドポイントがある場合は、IPv4 用に DHCP カスタム オプション 150 を使用し、IPv6 用にシスコ ベンダー固有の情報オプションである TFTP サーバ アドレス サブオプション タイプ 1 を使用することをお勧めします。エンドポイントが IPv6 アドレスを取得して TFTP サーバに要求を送信する一方、TFTP サーバが IPv4 を使用して要求を処理している場合、TFTP サーバは IPv6 スタック上で要求をリスニングしていないため、要求を受信しません。この場合、エンドポイントは、Cisco Unified Communications Manager に登録できません。

TFTP サーバの IP アドレスを検出するために、IPv4 および IPv6 デバイスで使用できる代替手段があります。たとえば、IPv4 デバイスでは DHCP オプション 066 または CiscoCM1 を使用できます。IPv6 デバイスでは、その他の方法として、TFTP サービス サブオプション タイプ 2 の使用や、エンドポイントでの TFTP サーバの IP アドレスの設定が含まれます。これらの代替手段は推奨されません。代替手段を使用する前に、シスコのサービス プロバイダーに問い合わせてください。

TFTP 導入でのエンドポイントと設定ファイル

SCCP 電話機、SIP 電話およびゲートウェイは、初期化時に設定ファイルを要求します。デバイス設定を変更すると常に、更新された設定ファイルがエンドポイントに送信されます。

設定ファイルには、Unified Communications Manager ノードの優先順位付きリスト、それらのノードとの接続に使用される TCP ポートなどの情報と、その他の実行可能ファイルが含まれます。一部のエンドポイントでは、設定ファイルにメッセージ、ディレクトリ、サービス、情報などの電話ボタンのロケール情報と URL も含まれます。ゲートウェイの設定ファイルには、デバイスが必要なすべての設定情報が含まれています。

TFTP のセキュリティに関する考慮事項

Cisco プロキシ TFTP サーバは、署名付きの要求と署名されていない要求の両方を処理でき、非セキュア モードと混在モードのいずれでも動作できます。プロキシ TFTP サーバは、ファイルをエンドポイントに送信する前に、独自の TFTP 秘密キーでファイルに署名します。

プロキシ TFTP サーバがエンドポイントのホーム クラスタに存在する単一クラスタ導入では、エンドポイントが自動的に署名付き設定ファイルを信頼します。

プロキシ TFTP 導入にリモート クラスタが含まれる場合は、プロキシ TFTP サーバをすべてのリモート エンドポイントの信頼検証リスト（TVL）に追加する必要があります。追加しない

と、エンドポイントは、リモート プロキシ TFTP サーバからの書名付きファイルを拒否します。手順については、エンドポイントデバイスをサポートするドキュメントを参照してください。

混合モードで動作しているリモート クラスタ上のすべての TFTP サーバに、プライマリ クラスタ TFTP サーバまたはクラスタ外 CTL ファイルに追加された IP アドレスが存在している必要があります。存在していない場合は、セキュリティが有効なクラスタに登録するエンドポイントが必要なファイルをダウンロードできません。

（注） プロキシ TFTP サーバでデバイスの登録をしない TFTP 導入環境では、プロキシ TFTP クラスタで [8.0以前へのロールバック用にクラスタを準備（Prepare Cluster for Rollback to Pre-8.0）] エンタープライズ パラメータを True に設定するのが最適です。

TFTP サーバの設定タスク フロー

Extension Mobility Cross Cluster（EMCC）をクラスタ用に設定している場合、システムでプロキシ TFTP サーバを動的に設定できます。EMCC を設定していない場合は、TFTP サーバを設定して、手動でセキュリティ モードを設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	次の方法のいずれかを使用して、TFTP サーバを設定します。 • TFTP サーバの動的設定 （5 ページ） • TFTP サーバの手動設定 （6 ページ）	クラスタ間検索サービス（ILS）を設定してある場合は、TFTP サーバを動的にセットアップすることができます。 EMCC を設定していない場合は、手動でTFTPサーバを設定します。クラスタがセキュアか非セキュアかを示す必要があります。デフォルトでは、クラスタは非セキュアとして処理されます。
ステップ 2	（任意） TFTP サーバの CTL ファイルの更新 （7 ページ）	CTL クライアント プラグインをインストールして、混合モードで動作するすべてのリモート クラスタ内にあるすべてのプロキシ TFTP サーバの Cisco Certificate Trust List（CTL）ファイルにプライマリ TFTPサーバを追加します。
ステップ 3	（任意） エンドポイント デバイスに対応するドキュメントを参照してください。	プロキシ TFTP の導入にリモート クラスタが含まれている場合、プロキシ TFTPサーバをすべてのリモートエンド

	コマンドまたはアクション	目的
		ポイントの信頼検証リスト（TVL）に追加します。
ステップ 4	（任意）TFTP サーバの非設定ファイルの変更 （7 ページ）	エンド ポイントがプロキシ TFTP サーバから要求する非設定ファイルを変更できます。
ステップ 5	（任意）TFTP サービスの停止および開始 （8 ページ）	エンドポイントの変更済み非設定ファイルをアップロードした場合、プロキシ TFTP ノードの TFTP サービスを停止および再起動します。
ステップ 6	（任意）DHCP サーバに対応するドキュメントを参照してください。	複数のクラスタを導入する場合、プライマリ プロキシ TFTP サーバの IP アドレスを含むように個々のリモート ノードの DHCP 範囲を変更します。

TFTP サーバの動的設定

ネットワークでクラスタ間検索サービス（ILS）を設定済みである場合は、Cisco Proxy TFTP Server を動的に設定することができます。

始める前に

ネットワークの EMCC を設定します。詳細については、http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.htmlにある『*Cisco Unified Communications Manager* 機能およびサービス ガイド』を参照してください。

手順

[Cisco Unified CM Administration （Cisco Unified Communications Manager Administration）] で、**[詳細機能（Advanced Features）] > [クラスタ ビュー（Cluster View）] > [今すぐリモート クラスタを更新（Update Remote Cluster Now）]** を選択します。TFTP サーバは、自動的に該当クラスタ向けに設定されます。

次のタスク

リモート プロキシの TFTP サーバをエンドポイントの信頼検証リスト（TVL）に追加する必要があります。追加しない場合、リモート クラスタ上にあるプロキシの TFTP サーバの設定ファイルは承認されません。手順については、エンドポイント デバイスに対応しているマニュアルを参照してください。

TFTP サーバの手動設定

EMCC が設定されていない場合にネットワークで TFTP を設定するには、手動の手順を実行する必要があります。

[クラスタ ビュー（Cluster View）] で、プライマリ プロキシ TFTP サーバとその他の TFTP サーバ間のピア関係をセットアップします。最大 3 台のピア TFTP サーバを追加できます。

プロキシ TFTP 導入環境の各リモート TFTP サーバには、プライマリ プロキシ TFTP サーバとのピア関係が含まれる必要があります。ループの作成を回避するため、リモート クラスタのピア TFTP サーバが互いを指し示していないことを確認します。

手順

ステップ 1 リモート クラスタを作成します。次のアクションを実行します。

a) Cisco Unified CM Administration で、**[高度な機能（Advanced Features）] > [クラスタの表示（Cluster View）]** を選択します。

b) [Add New] をクリックします。[リモート クラスタの設定（Remote Cluster Configuration）] ウィンドウが表示されます。

c) TFTP サーバの最大 50 文字のクラスタ ID と完全修飾ドメイン名（FQDN）を入力し、[保存（Save）] をクリックします。

クラスタ ID の有効な値には、英数字、ピリオド（.）、ハイフン（-）が含まれます。FQDN の有効な値には、英数字、ピリオド（.）、ハイフン（-）、アスタリスク（*）、およびスペースが含まれます。

d) （任意）[リモート クラスタ サービスの設定（Remote Cluster Service Configuration）] ウィンドウで、リモート クラスタの最大 128 文字の説明を入力します。

二重引用符（"）、山カッコ（><）、バックスラッシュ（\）、ハイフン（-）、アンパサンド（&）、またはパーセント記号（%）は使用しないでください。

ステップ 2 リモート クラスタの TFTP を有効にするには、[TFTP] チェックボックスをオンにします。

ステップ 3 [TFTP] をクリックします。

ステップ 4 [リモート クラスタ サービスの手動上書き設定（Remote Cluster Service Manually Override Configuration）] ウィンドウで、[リモート サービス アドレスの手動設定（Manually configure remote service addresses）] を選択します。

ステップ 5 これらの TFTP サーバとピア関係を作成するには、TFTP サーバの IP アドレスを入力します。

TFTP サーバの IP アドレスは 3 つまで入力できます。

ステップ 6 （任意）プロキシ TFTP サーバがセキュアなクラスタに展開されている場合は、[クラスタは安全です（Cluster is Secure）] チェックボックスをオンにします。

ステップ 7 [保存（Save）] をクリックします。

次のタスク

エンドポイントの Trust Verification List（TVL）に、すべてのリモート TFTP サーバを追加する必要があります。追加しないと、エンドポイントがリモート クラスタにあるプロキシ TFTP サーバからの設定ファイルの受け入れが拒否されます。詳細については、お使いのエンドポイント デバイスをサポートするマニュアルを参照してください。

TFTP サーバの CTL ファイルの更新

混合モードで動作しているリモート クラスタ内にあるすべての TFTP サーバに対する Cisco 証明書信頼リスト（CTL）ファイルにプライマリ TFTP サーバの IP アドレスを追加する必要があります。これは、セキュリティ対応クラスタのエンドポイントが設定ファイルを正常にダウンロードするために必要です。

プロキシ TFTP サーバに CTL クライアント プラグインをダウンロードしてインストールする必要があります。CTL クライアントは、プロキシ TFTP サーバから CTL ファイルを取得し、セキュリティ トークンを使用して CTL ファイルにデジタル署名を追加して、プロキシ TFTP サーバのファイルを更新します。

（注） セキュリティ トークンなしの CLI はサポートされていません。

セキュリティと Cisco CTL クライアントを使用する方法の詳細については、http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html にある *Cisco Unified Communications Manager* セキュリティ ガイド を参照してください。

手順

ステップ 1 Cisco Unified CM Administration で、**[アプリケーション（Application）]** > **[プラグイン（Plugins）]** を選択して、[プラグインの検索と一覧表示（Find and List Plugins）] ウィンドウで [検索（Find）] をクリックします。
インストールできるすべてのプラグインが一覧表示されます。

ステップ 2 Cisco CTL クライアントの [ダウンロード（Download）] リンクをクリックします。
TFTP サーバにある証明書にデジタル署名するクライアントをインストールします。

ステップ 3 TFTP サーバをリブートします。

TFTP サーバの非設定ファイルの変更

エンドポイントがプロキシ TFTP サーバから要求する、ロード ファイルや RingList.xml などの非設定ファイルを健康できます。この手順を完了すると、変更したファイルをプロキシ TFTP サーバの TFTP ディレクトリにアップロードします。

手順

ステップ 1 Cisco Unified Communications Operating System Administration で、**[ソフトウェア アップグレード（Software Upgrades）] > [TFTP ファイル管理（TFTP File Management）]** を選択します。
[TFTP ファイル管理（TFTP File Management）] ウィンドウが表示されます。

ステップ 2 [ファイルのアップロード（Upload File）] をクリックします。
[ファイルのアップロード（Upload File）] ポップアップが表示されます。

ステップ 3 次のいずれかの操作を実行します。

- アップロードするファイルのディレクトリの場所を参照するには、[参照（Browse）] をクリックしてください。
- [ディレクトリ（Directory）] フィールドに更新されるファイルの完全なディレクトリ パスを貼り付けます。

ステップ 4 [ファイルのアップロード（Upload File）] をクリックするか、ファイルをアップロードせずに終了するには、[閉じる（Close）] をクリックします。

次のタスク

Cisco Unified Serviceability 管理を使用して、プロキシ TFTP ノード上の Cisco TFTP サービスを停止するか、または再起動します。

TFTP サービスの停止および開始

プロキシ TFTP ノードで TFTP サービスを停止および再起動するには、次の手順を使用します。

サービスの有効化、無効化、および再起動についての詳細は、『*Cisco Unified Serviceability Administration Guide*』（http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html）を参照してください。

手順

ステップ 1 Cisco Unified Serviceability で、**[ツール（Tools）] > [コントロール センター - 機能サービス（Control Center - Feature Services）]** の順に選択します。

ステップ 2 [コントロール センター - 機能サービス（Control Center - Feature Services）] ウィンドウで、[サーバ（Server）] ドロップダウン リストからプロキシ TFTP ノードを選択します。

ステップ 3 [CM サービス（CM Services）] 領域で TFTP サービスを選択し、[停止（Stop）] をクリックします。

ステータスが変化し、更新されたステータスが反映されます。

ヒント サービスの最新ステータスを表示するには、[更新（Refresh）] をクリックします。

ステップ 4 [CM サービス（CM Services）] 領域で TFTP サービスを選択し、[開始（Start）] をクリックします。

ステータスが変化し、更新されたステータスが反映されます。