TFTP サーバの設定

プロキシ TFTP 展開の概要

プロキシ簡易ファイル転送プロトコル (TFTP) サーバを使用して、ネットワークのエンドポイントに必要な設定ファイル(ダイヤルプラン、着信音ファイル、デバイス設定ファイルなど)を指定します。 展開内の任意のクラスタに TFTP サーバをインストールして、複数クラスタのエンドポイントからの要求を処理することができます。 DHCP スコープは、設定ファイルを取得するために使用するプロキシ TFTP サーバの IP アドレスを指定します。

冗長およびピア プロキシ TFTP サーバ

単一クラスタの導入では、クラスタは少なくとも 1 つのプロキシ TFTP サーバを備えている必要があります。 冗長性を確保するために、クラスタに別のプロキシ TFTP サーバを追加することができます。 2 台目のプロキシ TFTP サーバは、IPv4 のオプション 150 に追加されます。 IPv6 の場合、第 2 TFTP サーバを、DHCP スコープの TFTP サーバ アドレスサブオプションタイプ 1 に追加します。

複数のクラスタ展開では、最大 3 台のリモートプロキシ TFTP サーバをプライマリプロキシ TFTP サーバのピアクラスタとして指定できます。 これは、複数の DHCP スコープに対して 1 台のプロキシ TFTP サーバだけを設定する場合、または 1 つの DHCP スコープのみを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、ネットワーク内のすべての電話機とデバイスに設定ファイルを提供します。

各リモートプロキシ TFTP サーバとプライマリプロキシ TFTP サーバの間にピア関係を作成する必要があります。

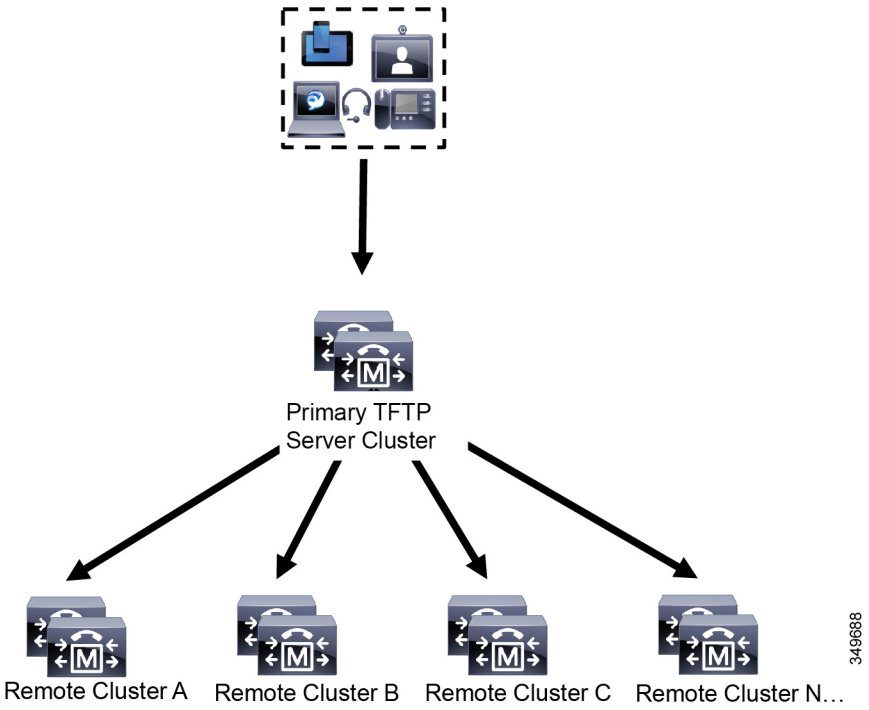
ヒント　ネットワーク内のリモートプロキシ TFTP サーバ間にピア関係を設定する場合は、関係を階層構造にしておきます。 ループの発生を回避するために、リモートクラスタ上のピアプロキシ TFTP サーバが相互にポイントしないようにします。 たとえば、プライマリノード A にノード B と C のピアリレーションシップがあるとします。ノード B と C の間にピア関係を作成しないでください。作成すると、ループが作成されます。

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



上の図では、デバイスのグループが構成ファイルのプライマリ TFTP サーバと通信します。デバイスから TFTP の要求を受信すると、プライマリ TFTP は、設定ファイルだけでなく、リモートクラスタ A、B、C、N(構成されている他のリモートクラスタ)などリモートで構成された他のクラスタについて、それぞれ自身のローカルキャッシュを検索します。

プライマリ TFTP サーバ上では、任意の数のリモートクラスタを設定できます。ただし、各リモートクラスタには最大 3 個の TFTP IP アドレスしか含めることができません。 冗長性を確保するための推奨設計は、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 サーバ上のリモートクラスタあたり 2 つの IP アドレスを使用して冗長性を確保できます。

使用例とベスト プラクティス

実装でのプロキシ TFTP の使用方法とベストプラクティスを詳細に示す次のシナリオを検討します。

1. クラスタは、他の目的がない単なるプロキシ TFTP クラスタとして機能できます。 この場合、クラスタには他のクラスタとの関係がなく、コールを処理しません。 このシナリオでは、リモート クラスタ TFTP が手動で定義され、8.0 よりも前へのロールバックが推奨されます。

（注） 自動登録は、このシナリオでは動作しません。

2. クラスタは、リモートクラスタのプロキシ TFTP サーバとしても機能するリモートクラスタです。 リモート クラスタは手動で定義されるので、自動登録は有効にしないでください。

IPv4 および IPv6 デバイスに対する TFTP サポート

IPv4 の電話機とゲートウェイで DHCP カスタムオプション 150 を使用して、TFTP サーバの IP アドレスを検出することを推奨します。 オプション 150 を使用すると、ゲートウェイと電話機は TFTP サーバの IP アドレスを検出します。 詳細については、デバイスに同梱されているマニュアルを参照してください。

IPv6 ネットワークでは、Cisco ベンダー固有の DHCPv6 情報を使用して、TFTP サーバ IPv6 アドレスをエンドポイントに渡すことを推奨します。 この方式では、TFTP サーバの IP アドレスをオプション値として設定しています。

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 には DHCP カスタム オプション 150 を、IPv6 には Cisco ベンダー固有情報オプションである TFTP サーバアドレスの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。 TFTP サーバが IPv4 を使用して要求を処理しているときに、エンドポイントが IPv6 アドレスを取得して要求を TFTP サーバに送信した場合、TFTP サーバは IPv6 スタックで要求を受信していないため、その要求を受信しません。 この場合、エンドポイントを Cisco Unified Communications Manager に登録できません。

IPv4 および IPv6 デバイスが TFTP サーバの IP アドレスを検出するために使用できる別の方法があります。 たとえば、IPv4 デバイスに DHCP オプション 066 または CiscoCM1 を使用できます。 IPv6 デバイスの場合、他の方法として、TFTP サービスのサブオプションタイプ 2 を使用する方法と、エンドポイントで TFTP サーバの IP アドレスを設定する方法があります。 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 展開のエンドポイントおよび設定ファイル

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、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ノードの優先順位リスト、これらのノードに接続するために使用される TCP ポート、さらに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用の設定ファイルには、電話機のボタン（メッセージ、ディレクトリ、サービス、および情報）用のロケール情報および URL が保存されています。 ゲートウェイ用の設定ファイルには、デバイスが必要とする設定情報がすべて保存されています。

プロキシ TFTP のセキュリティに関する考慮事項

シスコプロキシ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、セキュアでない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、電話機がファイルをリクエストし、見つからない場合は、リモートクラスタにリクエストを送信するときに、ローカル ファイル システムまたはデータベースを検索します。 電話が `ringlist.xml.sgn`、ロケールファイルなどの名前の共通ファイルをサーバにリクエストすると、サーバは電話のホームクラスタからファイル自体ではなくファイルのローカルコピーを送信します。

プロキシ TFTP からファイルを受信すると、ファイルにプロキシサーバの署名があり、電話の初期信頼リスト（ITL）と一致しないことから、署名の検証に失敗するため、電話はファイルを拒否します。 この問題を解決するには、電話機のセキュリティ デフォルト (SBD) セキュリティを無効にするか、プロキシ TFTP の CallManager 証明書を新しい(リモート/ホーム) クラスタの phone-sast-trust にインポートします。 その後、電話機は Trust Verification Service (TVS) に到達し、プロキシ TFTP 認証を信頼できます。 導入で EMCC が有効になっている場合は、一括証明書の交換が必要です。

デフォルトでセキュリティを無効にするには、Cisco Unified Communications Manager セキュリティ ガイドの「Cisco Unified IP Phone の ITL ファイルの更新」セクションを参照してください。

混在モードのプロキシ TFTP

混在モードで実行されているリモートクラスタ上のTFTPサーバには、シスコ証明書信頼リスト (CTL) ファイルにプライマリ プロキシ TFTP サーバ証明書を追加する必要があります。 そうでない場合、セキュリティが有効になっているクラスタに登録されているエンドポイントは、必要なファイルをダウンロードできなくなります。 証明書の一括インポートエクスポートを実行した後、この更新 CTL ファイルを実現するには。

詳細については、IP電話をクラスタ間で移行して一括証明書のエクスポートを実行する場合、Cisco Unified Communications Manager セキュリティ ガイドの「一括証明書のエクスポート」セクションを参照してください。

プロキシ TFTP 環境内のクラスタ間での電話機の移動

プロキシ TFTP 環境のリモート クラスタ間で電話機を移動する場合は、次の手順を実行します。

1. リモート クラスタ B (宛先クラスタ) に電話機の詳細を追加します。
2. リモート クラスタ A (送信元クラスタ) から電話機の詳細を削除します。

（注） プロキシTFTPでの電話機の設定は、期限切れになるまで30分あります。ファイルが見つからない応答を避けるために、プロキシ クラスタの TFTP サービスを再起動します。

3. 電話機をリセットしてリモートクラスタBから設定ファイルをダウンロードし、リモートクラスタ B に登録します。

TFTP サーバの設定タスク フロー

クラスタに対して拡張モビリティクロスクラスタ (EMCC) が設定されている場合は、システムがプロキシTFTPサーバを動的に設定できます。そうしない場合は、TFTPサーバを設定して、セキュリティモードを手動で設定することができます。

手順

	コマンドまたはアクション	目的
ステップ 1	次のいずれかの方法を使用して、TFTP サーバをセットアップします。 • TFTP サーバのダイナミック設定 （6 ページ） • TFTP サーバの手動設定 （7 ページ）	クラスタ間ルックアップサービス (ILS) が設定されている場合は、TFTP サーバを動的に設定することができます。 EMCCが設定されていない場合は、TFTP サーバを手動でセットアップします。クラスタがセキュアであるか、あるいは非セキュアであるかを示す必要があります。 クラスタは、デフォルトでは非セキュアとして扱われます。
ステップ 2	（任意） TFTP サーバの CTL ファイルの更新 （8 ページ）	CTL クライアントプラグインをインストールし、混在モードで動作しているすべてのリモートクラスタ内のすべてのプロキシ TFTP サーバの Cisco Certificate Trust List (CTL) ファイルにプライマリプロキシ TFTP サーバを追加します。

	コマンドまたはアクション	目的
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展開にリモートクラスタがある場合は、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。
ステップ 4	（任意） TFTPサーバの非設定ファイルの変更 （9 ページ）	プロキシTFTPサーバからエンドポイントを要求した非設定ファイルを変更できます。
ステップ 5	（任意） TFTP サービスの停止と開始 （9 ページ）	エンドポイントの変更済みの設定されていないファイルをアップロードした場合は、プロキシ TFTP ノード上で TFTP サービスを停止して再起動します。
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。	複数のクラスタに展開する場合は、プライマリプロキシ TFTP サーバの IP アドレスが含まれるように、個々のリモートノードのDHCPスコープを変更します。

TFTP サーバのダイナミック設定

ネットワークに設定されているクラスタルックアップサービス (ILS) を使用している場合は、Cisco proxy TFTP サーバ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、『*Cisco Unified Communications Manager* 機能およびサービス ガイド』（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。

SIP OAuth が有効になっている場合は、オフクラスタの Tomcat 証明書のルート CA 証明書をプロキシ電話 Edge Trust にコピーする必要があります。

手順

Cisco Unified Communications Manager の管理ページで、**[拡張機能(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 サーバはクラスタに対して自動的に設定されます。

次のタスク

エンドポイントの信頼検証リスト (TVL) にリモートプロキシ TFTP サーバを追加する必要があります。そうでない場合は、リモートクラスタ上のプロキシ TFTP サーバからの構成ファイルは受け入れられません。詳細については、お使いのエンドポイントデバイスに対応す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。

始める前に

重要 リリース 14SU1 以降、SIP OAuth が有効になっている場合は、オフクラスタの Tomcat 証明書のルート CA 証明書をプロキシ電話機のエッジ信頼にコピーする必要があります。

手順

ステップ 1 リモート クラスタを作成します。 次の操作を実行します。

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) [新規追加] 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]** 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 デバイスに対応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

混在モードの各クラスタで `utils ctl` を実行して、発行元ノードから CTL ファイルを更新します。 プロキシ TFTP サーバとすべてのクラスタ間で完全なセキュリティ ネットワークが作成され、プロキシとリモート クラスタ間の証明書の一括インポートとエクスポート交換が行なえるのを確認します。

CTLClient の使用中、混在モードで動作しているリモートクラスタ内のすべての TFTP サーバの Cisco Certificate Trust List (CTL) ファイルに、プライマリ TFTP サーバまたはプライマリ 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内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できるようにするために必要です。

セキュリティと Cisco CTL CLI の使用の詳細については、Cisco Unified Communications Manager セキュリティ ガイドの「Cisco CTL セットアップについて」のセクションを参照してください。

手順

ステップ 1 [Cisco Unified CM 管理（Cisco Unified CM Administration）] から、以下を選択します。**[アプリケーション] > [プラグイン]**

ステップ 2 **[検索]**をクリックして、インストール可能なすべてのプラグインのリストが表示します。

ステップ 3 Cisco CTL クライアントの**ダウンロード**リンクをクリックします。
システムは TFTP サーバ上に保管される証明書にデジタル署名をするクライアントをインストールします。

ステップ 4 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

ロードファイルや `RingList.xml`など、設定されていないファイルを、プロキシ TFTP サーバからのエンドポイント要求であるように変更できます。 この手順を完了したら、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] 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] 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。

- **[参照]**をクリックして、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します。
- 更新されたファイルの完全なディレクトリパスを**[ディレクトリ]**フィールドに貼り付けます。

ステップ 4 **[ファイルのアップロード]** をクリックするか、**[終了]**をクリックしてファイルをアップロードせずに終了します。

次のタスク

Cisco Unified 有用性管理を使用して、プロキシ TFTP ノード上の Cisco TFTP サービスを停止して再起動します。

TFTP サービスの停止と開始

次の手順に従って、プロキシ TFTP ノード上の TFTP サービスを停止して再開します。

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* アドミニストレーション ガイド』（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 サービスの最新の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。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。