CTL 更新

詳細情報

CTL アップデート実行の詳細については、『*Cisco Unified Communications Manager Security Guide*』（http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html）の「Security basics」の項を参照してください。

証明書の一括管理

証明書の一括管理は、送信元ノードと宛先ノードで手動で実行する必要があります。送信元ノードと宛先ノードは、この時点で動作している必要があります。電話機は送信元ノードに登録されます。

手順

ステップ 1 Destination Cluster Publisher で、Cisco Unified Operating System Administration に移動し、**[セキュリティ（Security）] > [一括証明書管理（Bulk Certificate Management）]** を選択します。

ステップ 2 Secure File Transfer Protocol（SFTP）サーバの IP アドレス、ポート、ユーザ、パスワード、およびディレクトリを定義します。

ステップ 3 宛先クラスタから中央 SFTP サーバにすべての Trivial File Transfer Protocol（TFTP）証明書をエクスポートするには、**[エクスポート（Export）]** ボタンを使用します。

ステップ 4 Source Cluster Publisher で、Cisco Unified Operating System Administration に移動します。**[セキュリティ（Security）] > [証明書の一括管理（Bulk Certificate Management）]** を選択します。

ステップ 5 手順 2 で使用したものと同じパラメータで中央 SFTP サーバを定義します。

ステップ 6 **[Export（エクスポート）]** をクリックして、送信元クラスタから中央 SFTP サーバにすべての TFTP 証明書をエクスポートします。

ステップ 7 **[Consolidate（統合）]** をクリックして、中央 SFTP サーバ上のすべての TFTP 証明書を統合します。この手順は、[一括証明書管理（Bulk Certificate Management）] インターフェイスを使用して、送信元または宛先クラスタのいずれかで実行できます。

ステップ 8 送信元クラスタで、[一括証明書インポート（Bulk Certificate Import）] をクリックして中央 SFTP サーバから TFTP 証明書をインポートします。

ステップ 9 宛先クラスタで、**[Bulk Certificate Import（一括証明書インポート）]** をクリックして中央 SFTP サーバから TFTP 証明書をインポートします。

ステップ 10 ダイナミック ホスト コンフィギュレーション プロトコル（DHCP）オプション **150** を使用して、電話機が新しい宛先クラスタ TFTP サーバを指し示すようにします。

リセットまたは電源投入後、電話機は新規宛先クラスタ ITL ファイルをダウンロードし、新しい ITL ファイル署名を既存の ITL ファイル内の証明書で認証しようと試みます。

既存の ITL ファイル内の証明書を使用して署名を認証することはできないため、電話機は送信元クラスタ上の古い Trust Verification Service（TVS）サーバから署名者の証明書を要求します。

電話機はこの要求を TCP ポート 2445 上の送信元クラスタ TVS サービスに送信します。

手順 1 から 9 の一括証明書交換は、新規 ITL ファイルに署名した宛先クラスタ上の TFTP 証明書で、送信元クラスタ内の TVS サービスを提供します。

TVS は電話機に証明書を返し、これにより電話機は署名を認証し、古い ITL ファイルを新しくダウンロードされた ITL ファイルで交換します。

電話機は、新規宛先クラスタから署名済みの設定ファイルをダウンロードおよび認証できるようになりました。