このマニュアルについて

First Published: October 29, 2007, OL-13676-01-J

はじめに

ここでは、このマニュアルの使用方法について説明します。次の項を参照してください。

対象読者と範囲

『Cisco TelePresence System Release 1.2 アドミニストレータ ガイド』は、Cisco TelePresence システムを監視し、保守するために Cisco TelePresence System Release 1.2 Administration の Web ベースのアプリケーションを使用する管理者を対象としています。

マニュアルの構成と用途

Cisco TelePresence System Release 1.2 Administration アプリケーションの使用に関する情報および手順は、次の章に示されています。

- 第 1 章「Cisco TelePresence System Administration の使用方法」
- 第 2 章「Cisco TelePresence システムの設定」
- 第 3 章「Cisco TelePresence システムのトラブルシューティング」
- 第 4 章「Cisco TelePresence システムの監視」

技術情報の入手方法、サポートの利用方法、およびセキュリティ ガイドライン

技術情報の入手、サポートの利用、技術情報に関するフィードバックの提供、セキュリティ ガイドライン、推奨するエイリアスおよび一般的なシスコのマニュアルに関する情報は、月刊の『*What's New in Cisco Product Documentation*』を参照してください。ここには、新規および改訂版のシスコの技術マニュアルもすべて記載されています。次の URL からアクセスできます。

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

このリリースの最新情報

セキュリティ

CTS Release 1.2 のセキュリティ パッケージには、次の機能が組み込まれています。

- Secure Real-Time Transport Protocol（SRTP）/Datagram Transport Layer Security（DTLS）
- Transport Layer Security
- S ディスクリプタ：暗号化されたメディアの SDP サポート
- 証明書信頼リスト（CTL）のサポート
- 署名および暗号化されたコンフィギュレーション ファイル
- 認証局プロキシ関数（CAPF）およびローカルで有効な証明書（LSC）のサポート

Secure Real-Time Transport Protocol（SRTP）/Datagram Transport Layer Security（DTLS）

TelePresence エンドポイントは、Transport Layer Security（TLS）/Secure Real-Time Transport Protocol（SRTP）を使用して SRTP キーを交換します。ただし、コールが SIP トランクを経由する場合、Cisco Unified Communications Manager（CUCM）は Session Description Protocol（SDP）内の SRTP キー フィールドを取り除き、TelePresence エンドポイントは代替メカニズムを使用して SRTP キー：Datagram Transport Layer Security（DTLS）/SRTP を交換します。

TelePresence エンドポイントが SRTP/DTLS を使用する場合は、DTLS ハンドシェイクの間に相互に証明書が送信され、その後、SRTP マスター キーが交換されます。ハンドシェイク後、メディアは生成されたセッション キーを使用して暗号化され、生成された認証キーを使用して認証されてから、ネットワーク経由で送信されます。

Transport Layer Security

現在、TelePresence エンドポイントがセキュアなデバイスとして設定され、CUCM が混合 / セキュア モードである場合、TelePresence エンドポイントは CUCM との間で SIP シグナリング メッセージを送受信するために Transport Layer Security（TLS）を使用できます。TelePresence エンドポイントと CUCM 間のすべての SIP シグナリング メッセージは暗号化できます。

S ディスクリプタ：暗号化されたメディアの SDP サポート

メディア ストリームの暗号化をサポートするために、SIP シグナリングは、7970 SIP Phone との相互運用性を確保する目的で RFC4568 を実装しています。これには、メディア暗号化キーを交換するためのメディア ストリームごとの SDP a=crypto 回線が含まれます。

証明書信頼リスト（CTL）のサポート

CUCM のみが自己署名証明書を持つため、CUCM の証明書の検証には Certificate Trust List（CTL; 証明書信頼リスト）が使用されます。CTL は、CUCM から取得し、CTL に含まれる証明書を持つ eToken ペアによって署名された信頼できるサーバの証明書のリストです。CTL は、TFTP サーバと、セキュア モードのデバイスの署名および暗号化されたコンフィギュレーション ファイルの署名を検証するためにも使用されます。

署名および暗号化されたコンフィギュレーション ファイル

現在、CTS は署名されたコンフィギュレーション ファイルをサポートしています。TelePresence エンドポイントがセキュア モードの場合は、署名付きのバージョンのコンフィギュレーション ファイルを TFTP サーバからダウンロードできます。CTS は、暗号化されたコンフィギュレーション ファイルもサポートします。TelePresence エンドポイントがセキュア モードで、TFTP Encrypted Config が有効な場合は、暗号化されたコンフィギュレーション ファイルを TFTP サーバからダウンロードできます。

認証局プロキシ関数（CAPF）およびローカルで有効な証明書（LSC）のサポート

現在、TelePresence エンドポイントには、CUCM 内の Certificate Authority Proxy Function（CAPF; 認証局プロキシ関数）サーバとやり取りし、そこから Locally Significant Certificate（LSC; ローカルで有効な証明書）を取得したり、それをアップグレードしたりする機能があります。LSC は、TLS を伴うシグナリング セキュリティ用に、Manufacturing Installed Certificate（MIC; 製造元がインストールした証明書）より優先して使用されます。CAPF では、TelePresence 公開キーを使用して、TFTP サーバによって生成された対称キーを暗号化します。その後、その対称キーを使用して、TelePresence コンフィギュレーション ファイルを暗号化します。

管理性

Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）を介してデバイスの管理性を向上させるために、次の標準 MIB がサポートされています。

- HOST-RESOURCES-MIB
- SYSAPPL-MIB
- UCD-SNMP-MIB

SIP Mid-call Re-invite

現在、CTS Release 1.2 は SIP mid-call re-invite をサポートしています。SIP mid-call re-invite は、主に 2 つの目的に使用されます。

- 帯域幅ネゴシエーション
- セキュリティの再ネゴシエーション

Call Statistics

CTS Release 1.2 では新しい Call Statistics カテゴリとして、Failed Secure Real-time Transfer Protocol (SRTP) Authentication Packets（失敗した SRTP 認証パケット）が追加されました。