ハイブリッドサービス 展開に関する重要項目

ハイブリッドサービス 展開に関する重要項目

このセクションでは、ハイブリッドサービスに関連する主要な設定項目に関する追加のコンテキストについて説明します。

これらのポイントは、ハイブリッド コール を Webex デバイスに正常に展開する場合に重要です。特にこれらの項目に焦点を当てる理由は次のとおりです。

- ハイブリッド展開での各項目の役割を理解して確信が得られるように説明します。
- これらは、クラウドとオンプレミス環境間の安全な展開を保証する必須の前提条件です。
- 稼働前に行う必要があるアクティビティとみなしてください。ユーザインターフェイスでの通常の設定よりも、完了までにかかる時間が若干長くなるため、これらの項目が整うまでの時間を考慮する必要があります。
- これらの項目が環境内で対処されれば、残りの ハイブリッドサービス の設定はスムーズに進行します。

サポートされている認証局

がWebexデバイスコネクタ機能Webexするためハイブリッドコールには、と通信する必要があります。

Webex デバイスコネクタ 内部ネットワークに導入されており、クラウドとの通信はアウトバウンド HTTPS 接続を通じて行われます。これは、Web サーバに接続するブラウザで使用されるのと同じ方法です。

クラウドへのWebex通信では TLS が使用されます。Webex デバイスコネクタ tls クライアントであり、 Webexクラウドは tls サーバです。そのため、Webex デバイスコネクタ はサーバ証明書を確認します。

認証局は、独自の秘密キーを使用してサーバ証明書に署名します。公開キーを持つ任意のユーザは、その署名を復号化し、同じ認証局がその証明書に署名したことを証明できます。

Webex デバイスコネクタ がクラウドから提供された証明書を検証する必要がある場合、その証明書に署名した認証局の公開キーを使用して署名をデコードする必要があります。公開キーは、認証局の証明書に含まれています。クラウドで使用されている認証局との信頼を構築するには、これらの信頼された認証局の証明書のリストを Webex デバイスコネクタ の信頼ストアに格納する必要があります。

デバイスと通信する場合、このツールは提供する信頼できるものを使用します。現在の方法は、`[ホームフォルダ]/.devicestool/certs`に配置する方法です。

トラバーサルペアの Expressway-E には、認証局の証明書のリストも必要です。Expressway-E は、相互認証によって適用された SIP と TLS を使用して Webex Cloud と通信します。Expressway-E は、TLS 接続設定時にクラウドによって提示された証明書の CN または SAN が Expressway-E の DNS ゾーンに設定されたサブジェクト名（「callservice.webex.com」）と一致する場合にのみ、クラウドに対して発着信するコールを信頼します。認証局は、アイデンティティ確認が終了してから、証明書をリリースします。証明書に署名を得るには、callservice.webex.com ドメインの所有権を証明する必要があります。シスコはそのドメインを所有しているため、リモートピアが本当に Webex であることを DNS 名の「callservice.webex.com」が直接証明します。

関連トピック

Webex でサポートされている認証局

Exchange 偽装アカウント

カレンダー コネクタ は、偽装アカウントを通じて、 Webex と Microsoft Exchange 2013、2016、2019、または Office 365 を統合します。Exchange のアプリケーション偽装管理ロールにより、アプリケーションは組織内のユーザを偽装してユーザの代わりにタスクを実行できます。アプリケーション偽装ロールは、Exchange で設定する必要があり、Expressway-C インターフェイスで行う Exchange の設定の一部として カレンダー コネクタ で使用されます。

Exchange の偽装アカウントは、このタスクで Microsoft が推奨する方法です 。パスワードは Exchange の管理者によって Expressway-C インターフェイスに入力することができるため、Expressway-C の管理者がパスワードを知る必要はありません。パスワードは、Expressway-C 管理者が Expressway-C ボックスへのルートアクセス権がある場合でも、明示されません。パスワードは、Expressway-C 上の他のパスワードと同じログイン情報暗号化メカニズムを使用して暗号化され、保存されます。

セキュリティを強化するには、Microsoft Exchange 向けの Expressway カレンダーコネクタの展開の手順に従って、回線上で EWS 接続を保護するために TLS を有効にします。

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。