Video Mesh 用導入ガイド

初版：2017 年 7 月 18 日

最終更新：2023 年 8 月 31 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目 次

新機能および変更された機能に関する情報

この表で、新機能、既存コンテンツの変更、『導入ガイド』で修正された主なエラーについて説明します。

Webex Video Mesh ノード ソフトウェアの更新の詳細については、https://help.webex.com/en-us/article/jgobq2/Webex-Video-Mesh-release-notes を参照してください。

日付	変更内容
2023 年 8 月 31 日	• 構造を更新し、「*Video Mesh* ノード *API*」に新しく導入された API に関する情報を追加。 • *Video Mesh* の *Call Control* およびミーティング統合要件から注記とワンボタン機能（OBTP）情報を削除。 • 「コンソールでの *Video Mesh* ノードのネットワーク構成を設定する」 および 「*Video Mesh* ノードの *Web* インターフェイスからネットワーク設定を構成する」に、フェールオーバーのポーリング間隔に関する注記を追加。 • サポートされる VMware ESXi のバージョンを更新。
2023 年 7 月 31 日	• 「*Video Mesh* アラートのウェブフック」を追加。
2023 年 7 月 28 日	• 「*Video Mesh* ノード *API*」を追加。

新機能および変更された機能に関する情報

日付	変更内容
2023 年 6 月 15 日	• 「Webex アプリアプリ」から「Webex アプリ」に用語を更新。 • 「*Webex Video Mesh*の概要」を更新し、E2EE ミーティングが Video Mesh でサポートされるようになったことを記載。 • 「*Webex Video Mesh* の概要」の古い情報を削除し、注記を更新。 • 「*Video Mesh* ノードを使用するクライアントとデバイス」 更新して、Web クライアントが Video Mesh でサポートされるようになったことを記載し、古い情報を削除。 • 「*Video Mesh* ノードソフトウェアのシステムおよびプラットフォーム要件」に、デモ環境がシスコ TAC でサポートされていないことを示す注記を追加。 • 「オンプレミスとクラウドコール」 セクションの情報を更新。 • 「*250 ms* 以上の *STUN* ラウンドトリップ遅延に基づくオーバーフローのためのクラウドクラスタの選択」の注記を削除。 • 「*Webex Meetings* トラフィック用のポートとプロトコル」の情報を更新。 • 「*Webex* クラウドに *Video Mesh* ノードを登録する」および「プライベートミーティングのサポートと制限事項」から古い情報を削除。 • 「*Webex* サイトの *Video Mesh* を有効にする」から手順を更新し、古い情報を削除。 • 「*Video Mesh* を非アクティブにする」の情報を更新。

新機能および変更された機能に関する情報

日付	変更内容
2023 年 5 月 16 日	• Video Mesh で使用される最新のポートとプロトコルを反映するように、「管理用のポートとプロトコル」、「*Video Mesh* のトラフィック署名（*Quality of Service* 有効）」、および「*Video Mesh* のトラフィック署名（*Quality of Service* 無効）」を更新。変更の影響を受けるイメージを更新。 • 「*Video Mesh* のプロキシサポートの要件」、「管理のポートとプロトコル」、「プロキシ統合のための *Video Mesh* ノードを設定する」、および「プロキシ統合のための *Video Mesh* ノードを設定する」から 444 のポート参照を削除。 • 「*Video Mesh* ノードのサービス品質」、「*Video Mesh* ノードのサービス品質（*QoS*）を有効にする」、および「*Webex Meetings* トラフィックのポートとプロトコル」のポート範囲を更新。 • 「即時テストを実行する」および「定期テストを設定する」に、テストの失敗のモニタリングに関する注記を追加。 • 「*Video Mesh* ノードソフトウェアをインストールおよび設定する」で、展開に最新のソフトウェアパッケージ（OVA）を使用することを強く推奨する注記を追加し、注意を更新。 • 「*Web* インターフェイスから *Video Mesh* ノードを管理する」および「コンソールから *Video Mesh* ノードを管理する」で、メンテナンスモードになっているノードに関する注意を更新。 • 最新の UI の変更を反映するように「*Video Mesh* 分析」セクションを更新。
2023 年 3 月 27 日	• *Video Mesh* ノードソフトウェアのシステムとプラットフォームの要件を最新のハードウェア設定で更新し、帯域幅の要件を追加しました。
2023 年 3 月 2 日	• 「*Video Mesh* のモニタリングツール」でモニタリングツールが実行するテストに関する情報を追加。 • 「即時テストを実行する」および「定期テストを設定する」のモニタリングツールの概要ページにアクセスする手順を変更。 • 「即時テストを実行する」および「定期テストを設定する」に結果の表示とフィルタリングに関する情報を追加。 • 「*Webex* サイトの *Video Mesh* を有効にする」を更新。

新機能および変更された機能に関する情報

日付	変更内容
2022 年 7 月 7 日	• *Video Mesh* ノードのキャパシティのキャパシティ見積もりを更新しました。 • 廃止された MM410v サーバーに関する記述を全体的に削除しました。
2022 年 6 月 30 日	https://github.com/CiscoDevNet/webex-video-mesh-node-provisioning で、新しい一括プロビジョニングスクリプトに関する情報を追加しました。
2022 年 6 月 14 日	*Unified CM Video Mesh* ノード間の交換証明書チェーンに、ECDSA 証明書を含めるように証明書チェーンを交換する手順を変更しました
2022 年 5 月 18 日	Reflector Tool のダウンロードサイトを https://github.com/CiscoDevNet/webex-video-mesh-reflector-client に変更しました。
2022 年 4 月 29 日	すべての外部 *Webex* ミーティングの *Video Mesh* にメディアを保持するに新機能に関する情報を追加しました。
2022 年 3 月 25 日	管理用のポートとプロトコルでポートの使用方法を更新しました。
2021 年 12 月 10 日	*Video Mesh* ノードソフトウェアのシステムおよびプラットフォームの要件に、CMS 2000 および古い CMS 1000 を ESXi 7 にアップグレードする場合のアップグレードの問題の注記を追加しました。
2021 年 8 月 30 日	送信元の国が正しいことを確認に、Webex の展開で正しい送信元の国が設定されていることを確認するための情報を追加しました。
2021 年 8 月 27 日	プライベートミーティングのサポートと制限に、分析レポートの表示に関する注記を追加しました。
2021 年 8 月 13 日	新しいプライベートミーティング機能に関する情報が次の場所に追加されました。 • *Video Mesh* のクラスタ • プライベート ミーティング コール • プライベート ミーティング
2021 年 7 月 22 日	システムでコールの送信元の場所が正しいことを確認する方法に関する情報を追加しました。正しい送信元の場所は、効率的なルーティングに役立ちます。送信元の国が正しいことを確認を参照してください。
2021 年 6 月 25 日	Webex アプリのフル機能の Webex エクスペリエンス機能は、*Video Mesh* ノードを使用するクライアントとデバイスの Video Mesh と互換性がないことを注記しました。

新機能および変更された機能に関する情報

日付	変更内容
2021 年 3 月 7 日	*Video Mesh* クラスタの展開に関するガイドラインで推奨されるクラスタサイズを 100 に修正しました。
2021 年 4 月 12 日	DNS ゾーンではなく Webex ゾーンを使用するように、*Video Mesh* 用の *Expressway TCP SIP* トラフィックルーティングの設定を更新しました。
2021 年 2 月 9 日	• ウェブインターフェイスからの *Webex Video Mesh* ノードのアクセスの概要に、Control Hub の新しい **[ノードに移動（Go to Node）]** に関する情報を追加しました。 • 新しい機能を説明するために、ウェブインターフェイスからのローカル管理者アカウントの無効化または再有効化セクションを追加しました。 • ノードのウェブインターフェイスを使用する各セクションで、Control Hub からインターフェイスにアクセスする方法を示す手順を更新しました。 • セキュリティ証明書のアップロードを追加しました。 • *Syslog* サーバーへの外部ロギングの設定を追加しました。
2020 年 12 月 11 日	• *DNS* キャッシュの有効化または無効化で、DNS キャッシュの消去に関する情報を追加しました。
2020 年 10 月 22 日	• *Webex Meetings* トラフィックのポートとプロトコルで、SIP シグナリングポートの要件が追加されました。
2020 年 10 月 19 日	• サービスで使用されなくなった cloudfront.net への参照を削除しました。
2020 年 9 月 18 日	• Webex Video Mesh ノードの内部使用のために予約されている IP アドレスの範囲を、元の 172.17.0.0 ～ 172.17.255.255（65,536 アドレス）から **172.17.42.0 ～ 172.17.42.63**（64 アドレス）に減らしました。
2020 年 8 月 26 日	• *Video Mesh* の概要に Webex Events のサポートを追加しました。 • 新しいセクション*DNS* キャッシュの有効化または無効化を追加しました。

新機能および変更された機能に関する情報

日付	変更内容
20208 年 8 月 4 日	• 短いビデオアドレスのサポートについて、以下のセクションを更新しました。 • 呼制御タスクフローと *Video Mesh* の統合 • *Video Mesh* 用の *Unified CM Secure TLS SIP* トラフィックルーティングの設定 • *Video Mesh* 用の *Unified CM TCP SIP* トラフィックルーティングの設定 • *Video Mesh* 用の *Expressway TCP SIP* トラフィックルーティングの設定 • *Video Mesh* ノードプラットフォームのコールキャパシティの「VMNLite コール キャパシティ ベンチマーク」セクションを更新しました。
2020 年 7 月 9 日	• 新セクションネットワーク インターフェイスの *MTU* サイズの設定を追加しました。
2020 年 6 月 26 日	• 次の場所で、新しい VMNLite 展開オプションに関する情報を追加しました。 • *Video Mesh* ノードプラットフォームのコール キャパシティ • *Video Mesh* ノードソフトウェアのシステムおよびプラットフォームの要件 • *Video Mesh* ノードソフトウェアのインストールと設定 • OVA にデフォルトの NTP サーバー値がなくなったため、デフォルトの NTP サーバーに関する情報を削除しました。 • サポート用の *Webex Video Mesh* パケットキャプチャの生成を更新して新しいフィルタリングオプションを記載しました。
2020 年 6 月 9 日	• 次の場所で、新しい週次の自動ソフトウェアアップグレードスケジュールオプションに関する情報を追加しました。 • *Webex* クラウドへの *Video Mesh* ノードの登録 • *Video Mesh* クラスタのアップグレード スケジュールの設定
2020 年 5 月 21 日	管理用のポートとプロトコルおよび *Video Mesh* のプロキシサポートの要件を更新しました。

新機能および変更された機能に関する情報

日付	変更内容
2020 年 5 月 15 日	*Video Mesh* の概要を更新しました。

2020 年 4 月 25 日	• 「ウェブインターフェイスからの Webex Video Mesh ノードの管理」に新しいセクションを追加しました。
	  • *Video Mesh* ノード ウェブ インターフェイスからの外部ネットワーク インターフェイスの設定
	  • 内部ルーティングルールと外部ルーティングルールを追加する
	  • *Webex Video Mesh* ノードウェブインターフェイスからのコンテナネットワークの構成
	• 「Webex Video Mesh へのアクセス、フィルタ処理、および保存のトラブルシューティング」における横軸のきめ細かさの誤りを修正しました（この値は、**[過去 7 日間（Last 7 Days）]** と **[過去 24 時間（Last 24 Hours）]** オプションに切り替えられました）。

2020 年 1 月 22 日	• 新しいセクション「ウェブインターフェイスからの Webex Video Mesh ノードの工場出荷時状態へのリセット」を追加しました。 • 「ウェブインターフェイスからの Webex Video Mesh ノードの管理」セクションで、接続チェックの詳細を追加しました。 • 「Webex Video Mesh ノードを使用するクライアントとデバイス」セクションに室内ワイヤレス共有を追加しました。
2019 年 12 月 12 日	• 「管理とトラブルシューティング」の章の「ウェブインターフェイスからの Webex Video Mesh ノードの管理」セクションに、パスフレーズとパスフレーズの失効手順の変更を追加しました。

新機能および変更された機能に関する情報

日付	変更内容
2019年12月10日	• トラフィックシグニチャの表に次の情報とポート範囲を追加しました（QoS が有効である場合と無効である場合）。 • 送信元 IP アドレス：Video Mesh ノード • 接続先 IP アドレス：Webex クラウドメディアサービス • 送信元 UDP ポート：35000 ～ 52499 • 接続先 UDP ポート：5004 • ネイティブ DSCP マーキング：AF41 • メディアタイプ：テスト STUN パケット • 「帯域幅のガイドライン」セクションの名前を「ビデオ品質とスケーリング」に変更し、推奨アーキテクチャのドキュメントへのリンクを追加しました。 • Unified CM TLS の設定において、このガイドでは、Webex クラウドフェールオーバー用のセキュアでない SIP トランクを設定すると誤って記載していました。SIP トランクを作成するという旨の文に修正しました（セキュアまたは非セキュアのいずれかとして設定できます）。
2019 年 11 月 4 日	• 古い分析コンテンツを廃止し、新しいセクションを追加しました。 • 「証明書の交換」セクションで [サブジェクト代替名（Subject Alternative Name(s)）] フィールドに関する情報を追加し、「はじめる前に」セクションで「セキュリティ上の理由から、ノードのデフォルトの自己署名証明書の代わりに、Video Mesh ノードで CA 署名付き証明書を使用することをお勧めします。」という文言を追加しました。
2019 年 10 月 18 日	• 1080p Control Hub 設定の説明を更新し、この設定がコールキャパシティに影響し、オンプレミスの SIP に登録済みのデバイスにのみ適用される点を明確化しました。詳細については、*Video Mesh* ノードミーティングにおけるオンプレミス *SIP* デバイス用の *1080p HD* ビデオの有効化を参照してください。 • サポートされているデバイスとエンドポイントの表を更新し、テスト済みのクラウドに登録されたデバイスの一覧のみを表示するようにしました。

新機能および変更された機能に関する情報

日付	変更内容
2019 年 9 月 26 日	• 新セクション *Video Mesh* ノード ウェブ インターフェイスからのネットワーク設定の構成を追加しました。 • リソース使用率レポートの説明を修正しました。現在は、「Video Mesh クラスタで使用されるメディアマイクロサービスの平均リソース使用率」と記載されています。 • キャパシティのセクションに「低いコールボリュームにおけるオーバーフロー（特にオンプレミスで発生した SIP コール）は、真にスケールを反映するものではありません。Video Mesh 分析（**Control Hub > [リソース（Resources）] > [コールアクティビティ（Call Activity）]**）は、オンプレミスで発生したコールレッグを示します。これらは、メディア処理のために Video Mesh ノードへのカスケードを通過したコールストリームを指定しません。ミーティングにおけるリモート参加者の数が増えれば、結果として生じるカスケードが増加し、Video Mesh ノード上のオンプレミスのメディア リソースが消費されます。」という文を追加しました。
2019 年 9 月 13 日	• *Video Mesh* ノード ソフトウェアのインストールと設定を更新して、**[テンプレートのカスタマイズ（Customize template）]** ページに表示されるネットワーク構成手順を記載しました。 • *Video Mesh* ノードソフトウェアのシステムおよびプラットフォームの要件を更新して、仕様に基づく構成用の 72vCPU（CMS 1000 と同等）を記載しました。

2019 年 8 月 29 日	• 明示的なプロキシ設定（認証なし、基本、ダイジェスト、NTLM）用の明示的なプロキシとサポートされている認証タイプを追加しました。
	  • *Edge Video Mesh* のプロキシサポート
	  • *Video Mesh* のプロキシサポートの要件
	  • プロキシ統合用の *Webex Video Mesh* ノードの設定
	• *Video Mesh* でサポートされる解像度とフレームレートを追加しました。
	• *Video Mesh* ノードを使用するクライアントとデバイスを更新して、Webex クラウドに登録されたビデオデバイスに接続する Webex *Call My Video System* が Video Mesh ノードを使用している旨を記載しました。

新機能および変更された機能に関する情報

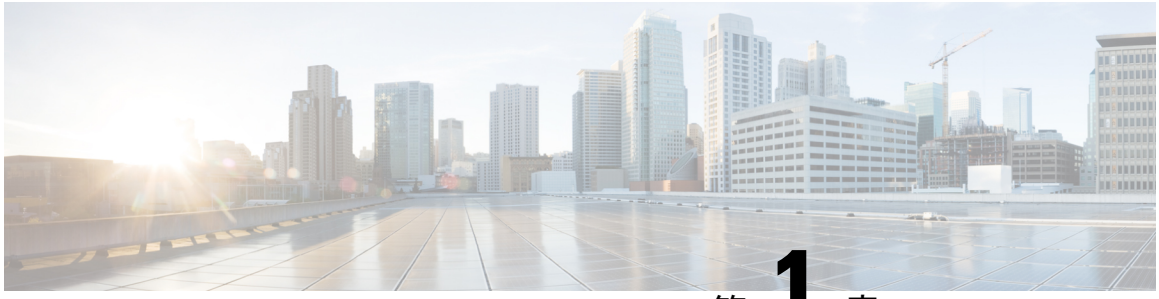
日付	変更内容

2019 年 7 月 24 日	• ウェブインターフェイスからの *Webex Video Mesh* ノードの管理セクションで、次の更新を行いました。
	  • Ping テスト、トレースルートテスト、NTP サーバーテスト、リフレクタツール、およびデバッグ ユーザーアカウントについての新しいセクションを追加しました。
	  • 「概要」セクションを更新しました。スクリーンショットからカスケードを削除し、OS のバージョンを追加しました。
	• 「コンソールからの Webex Video Mesh ノードの管理」の内容をガイドの付録に移動しました。
	• 「Webex Video Meshの管理」という章の名前を「Webex Video Meshの管理とトラブルシューティング」に変更し、登録のトラブルシューティングの内容をその章に移動しました。

2019 年 7 月 9 日	• *Video Mesh* の呼制御とミーティング統合の要件で 、Unified CM、Expressway、およびWebexサイト用にサポートされている最小バージョンを更新しました。 • *Video Mesh* ノードを使用するクライアントとデバイスで、Jabber VDI および Webex VDI のサポートされているバージョン（SIP クライアント）を追加しました。また、テストの免責事項も追加しました。

2019 年 5 月 24 日	• トラブルシューティング機能の新しいセクションを追加し、Video Mesh ノードウェブインターフェイスの概要画面を更新しました。
	  • サポート用の *Webex Video Mesh* ログの生成
	  • サポート用の *Webex Video Mesh* パケットキャプチャの生成
	  • ウェブインターフェイスからの *Webex Video Mesh* ノードのアクセスの概要

2019 年 4 月 25 日	• *Webex Video Mesh* の管理とトラブルシューティングを更新して、Video Mesh ノードでメンテナンスを実行する前に、Control Hub のメンテナンスモードが必要である旨を記載しました。
2019 年 4 月 11 日	• 帯域幅の要件から古くなった情報を削除しました。内容と図を更新し、セクション名を *Video Mesh* のビデオ品質とスケーリングに変更しました。



第 1 章

Webex Video Mesh の概要

Webex Video Mesh 概要

Webex Video Meshは、オンプレミスとクラウドの会議リソースの最適な組み合わせを動的に探します。十分なローカルリソースがある場合は、オンプレミスの会議はオンプレミスで実行されます。ローカルのリソースがすべて使用されている場合は、会議はクラウドに拡張されます。

Video Mesh ノードは、オンプレミスのシスコ UCS サーバーにインストールされ、クラウドに登録され、Control Hub で管理されるソフトウェアです。Webex ミーティングやイベント、Webex パーソナル ミーティング ルーム、Webex Space ミーティング、および 2 者間の Webex アプリコールはローカルのオンネットVideo Mesh ノードにルーティングできます。Video Mesh は利用可能なリソースを使用するための最も効率的な方法を選択します。

Video Mesh には次の利点があります。

- コールをオンプレミスで維持できるため、品質が向上し、遅延が減少します。
- オンプレミスのリソースが限界に達しているか、利用不可能な場合に、コールを透過的にクラウドに拡張することができます。
- 単一の管理インターフェイスである Control Hub（https://admin.webex.com）を使用して、クラウドから Video Mesh クラスタを管理できます。
- リソースを最適化し、必要に応じてキャパシティを拡張できます。
- クラウドとオンプレミス会議の機能を 1 つのシームレスなユーザーエクスペリエンスとして統合することができます。

- 追加の会議リソースが必要な場合にいつでもクラウドを利用できるため、キャパシティに関する心配が少なくなります。最悪のシナリオを考慮してキャパシティを計画する必要がありません。
- https://admin.webex.com のキャパシティと使用量およびトラブルシューティングレポートのデータに関する高度な分析を提供します。
- オンプレミスの標準ベースの SIP エンドポイントとクライアントからユーザーが、 Webex ミーティングにダイヤルインするときに、ローカルメディアの処理を使用します。
  - オンプレミスの呼制御（Cisco Unified Communications Manager または Expressway）に登録され、Cisco Webex ミーティングに発信する SIP ベースのエンドポイントとクライアント（シスコエンドポイント、Jabber、サードパーティの SIP）。
  - Webex ミーティングに参加する Webex アプリ（名前の逆引きルックアップとのペアを含む）。
  - Webex ミーティングに直接参加する Webex ルームおよびデスクデバイス。
- オンネット SIP エンドポイントとクライアントに対して、最適化された音声およびビデオによる自動音声応答（IVR）を提供します。
- H.323、IP ダイヤルイン、Skype for Business（S4B）エンドポイントは、引き続きクラウドからミーティングに参加します。
- 1080p をサポートするミーティング参加者が、ローカルオンプレミスの Video Mesh ノードを介してホストされている場合は、高画質の 1080p 30fps ビデオをミーティング用のオプションとしてサポートします。（参加者がクラウドから進行中のミーティングに参加した場合、オンプレミスのユーザーはサポートされているエンドポイントで引き続き 1080p 30fps の高画質を利用できます）。
- Quality of Service（QoS）マーキングの強化と差別化：オーディオ（EF）とビデオ（AF41）の分離。

Note 現時点では、Webex Video Meshは Webex ウェビナーをサポートしていません。

- エンドツーエンド暗号化会議（E2EE 会議）をサポートしています。お客様が Video Mesh を展開し、E2EE ミーティングタイプを選択すると、セキュリティレイヤが追加され、データ（メディア、ファイル、ホワイトボード、注釈）の安全性が確保され、第三者によるアクセスや変更がブロックされます。詳細については、「ゼロトラストミーティングを展開する」を参照してください。

Note プライベートミーティングは現在、エンドツーエンド暗号化をサポートしていません。

Video Mesh ノードを使用するクライアントとデバイス

Video Mesh が、関連するクライアントおよびデバイスタイプとの相互運用性を持つように取り組んでいます。すべてのシナリオをテストすることはできませんが、このデータが基づくテストは、リストされているエンドポイントとインフラストラクチャの最も一般的な機能を対象に含めています。デバイスまたはクライアントがリストに存在しない場合、テストは未実施であり、シスコによる公式なサポートが提供されていないことを示唆しています。

Table 1: 使用するクライアントとデバイス***Video Mesh*** ノード

クライアントまたはデバイスの種類	ポイントツーポイントコールでの Video Mesh ノード のを使用	Multiparty Meeting での Video Mesh ノードの使用
Webex アプリ（デスクトップとモバイル）	はい	はい
Webex デバイス（ルームデバイスおよび Webex Board を含む）。（完全なリストについては、「エンドポイントと Webex アプリ の要件, on page 10」のセクションを参照してください。）	はい	はい
Webex アプリ とサポートされている Room デバイス、Desk デバイス、および Board デバイス間でのルーム内ワイヤレス共有。	はい	はい
Webex スケジュール済みまたは Webex Personal Room ミーティングにコールする、Unified CM に登録されたデバイス（IX エンドポイントを含む）とクライアント（Jabber VDI 12.6 以降および Webex VDI 39.3 以降を含む）。*	いいえ	はい
Webex スケジュール済み、または Webex Personal Room ミーティングにコールする VCS/Expressway 登録済みデバイス。*	いいえ	はい
Webex クラウドに登録されたビデオデバイスへの Webex *Call My Video System*	N/A	はい
Webex アプリ Web クライアント（https://web.webex.com）	はい	はい
Cisco Webex コール に登録された電話機	いいえ	いいえ
オンプレミスに登録された SIP デバイスへの Webex *Call My Video System*	N/A	いいえ

* すべてのオンプレミスデバイスとクライアントが Video Mesh ーションでテスト済みであることを保証することはできません。

フル機能の Webex エクスペリエンスとの Video Mesh の非互換性

Webex アプリのフル機能の Webex エクスペリエンスを有効にすると、Webex アプリは Video Mesh ノードでサポートされません。この機能は現在、シグナリングとメディアを Webex に直接送信します。将来のリリースでは、Webex アプリと Video Mesh が互換性を持つようになります。デフォルトでは、Video Mesh を使用しているお客様に対してはこの機能が有効になっていません。

Video Mesh とフル機能の Webex エクスペリエンスに問題がある可能性があります。

- その機能の導入後に展開に Video Mesh を追加した場合。
- Video Mesh への影響を知らずにその機能を有効にした場合。

問題に気付いた場合は、シスコアカウントチームに連絡して、フル機能の Webex エクスペリエンスの切り替えを無効にしてください。

Video Mesh ノードの Quality of Service（QoS）

Video Mesh ノードは推奨される Quality of Service（QoS）のベストプラクティスに従っているため、ポート範囲を有効にすると、オーディオおよびビデオストリームと値リストコレクション作成者の間のすべてのフローを区別することができます。この変更により、QoS ポリシーを作成し、値リストコレクション作成者との間で効率的にトラフィックを注釈することができるようになります。

これらのポートの変更には、QoS の変更が付随しています。Video Mesh ノードは、オーディオ（EF）とビデオ（AF41）の両方について、メディアトラフィックを、適切なサービスクラスと個別に SIP 登録済みエンドポイント（オンプレミスの Unified CM または登録済み VCS Expressway）にマークし、特定のメディアタイプに対して既知のポート範囲を使用します。

オンプレミスの登録済みエンドポイントからの発信元トラフィックは、必ず、呼制御の構成（Unified CM または VCS Expressway）によって決定されます。

詳細については、Video Mesh で使用されるポートとプロトコル （32 ページ） の QoS 表および の 有効または無効な QoS の手順を参照してくださいVideo Mesh 導入タスクのフロー （51 ページ）

Webex アプリ は、共有ポート 5004 経由で引き続き Video Mesh ノードに接続します。これらのポートは、Video Mesh ノードへの STUN 到達可能性テストのために、Webex アプリ とエンドポイントによっても使用されます。カスケードの Video Mesh ノードから Video Mesh ノードは、宛て先ポート範囲 10000 ～ 40000 を使用します。

Video Mesh のプロキシサポート

Video Mesh は、明示的かつ透過的な検査プロキシと非検査プロキシがサポートされています。これらのプロキシを Video Mesh の展開に関連付けることで、企業からクラウドへのトラフィックを保護およびモニタリングできます。この機能は、シグナリングと管理の https ベースのトラフィックをプロキシに送信します。透過的なプロキシの場合、Video Mesh ノードからのネットワーク要求は、エンタープライズネットワークルーティングルールを介して特定のプロキシに転送されます。ノードにプロキシを実装した後、Video Mesh 管理インターフェイスを使用して証明書を管理し、全体的な接続ステータスを確認することができます。

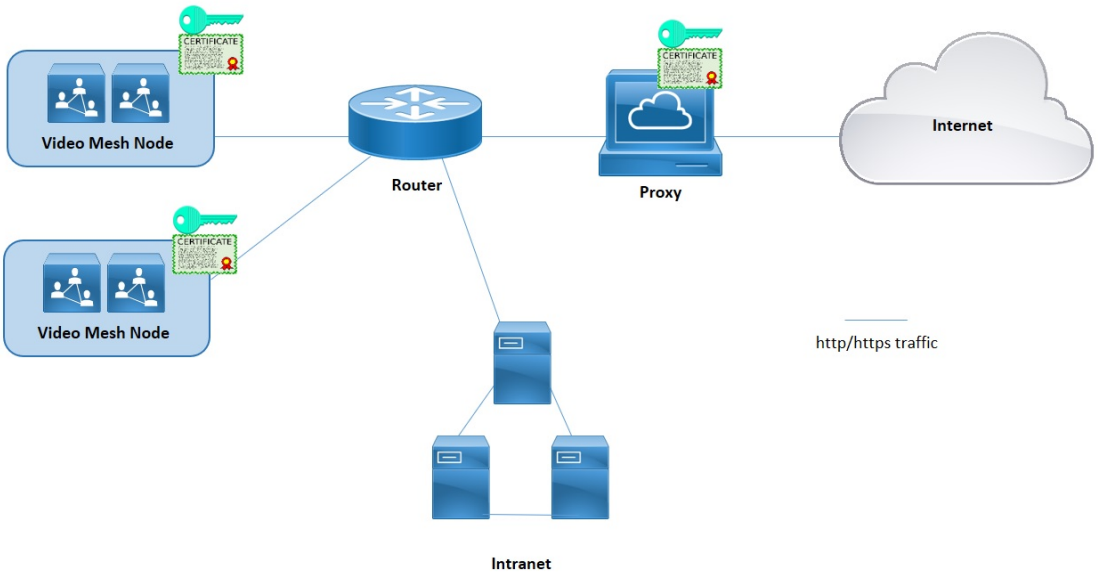
Note メディアはプロキシを通過しません。メディアストリームがクラウドに直接到達するために必要なポートを開く必要があります。「管理用のポートとプロトコル, on page 33」を参照してください。

Video Mesh では、次のプロキシ タイプがサポートされています。

- 明示的なプロキシ（Explicit Proxy）（検査または非検査）：明示的なプロキシを使用する場合、プロキシサーバーが使用するクライアント（Video Mesh ノード）を指定します。このオプションは、次のいずれかの認証タイプをサポートします。
  - なし（None）：これ以上の認証は必要ありません。（明示的な HTTP または HTTPS プロキシの場合。）
  - 基本（Basic）：HTTP ユーザーエージェントが要求を行う際にユーザー名とパスワードを入力するために使用され、Base64 エンコーディングを使用します。（明示的な HTTP または HTTPS プロキシの場合。）
  - ダイジェスト（Digest）：機密情報を送信する前にアカウントのアイデンティティを確認するために使用され、ネットワークを介して送信する前にユーザー名とパスワードにハッシュ機能を適用します。（明示的な HTTPS プロキシの場合）。
  - NTLM：[ダイジェスト（Digest）] と同様に、NTLM は、機密情報を送信する前にアカウントのアイデンティティを確認するために使用されます。ユーザー名とパスワードではなく、Windows ログイン情報を使用します。この認証方式では、複数回の情報交換が必要になります。（明示的な HTTP プロキシの場合。）
- 透過的なプロキシ（非検査）（Transparent Proxy（non-inspecting））：Video Mesh ノードは特定のプロキシサーバーアドレスを使用するように設定されないため、非検査プロキシと連動するための変更は必要ありません。
- 透過的なプロキシ（検査）（Transparent Proxy（inspecting））：Video Mesh ノードは特定のプロキシサーバーアドレスを使用するように設定されません。Video Mesh では http(s) 設定の変更は必要ありませんが、Video Mesh ノードにはプロキシを信頼するためのルート証明書が必要です通常、IT は検査プロキシを使用して、アクセス可能な Web サイトおよび

許可されないコンテンツのタイプに関するポリシーを適用します。このタイプのプロキシは、すべてのトラフィックを（https も）復号します。

Figure 1: Video Mesh ノードおよびプロキシの例



Video Meshでサポートされる解像度とフレームレート

この表は、Video Mesh ノードでホストされるミーティングで、送信者と受信者の観点からサポートされている解像度とフレームレートを示しています。送信者クライアント（アプリまたはデバイス）は表の一番上の行に記載されており、受信者クライアントは表の左側の列に記載されています。2 人の参加者が交差する位置にあるセルは、ネゴシエートされるコンテンツの解像度、セクションごとのフレーム、および音声の送信元を示しています。

（注） 解像度は、任意の Video Mesh ノードのコールキャパシティに影響します。詳細については、「Video Mesh ノードのキャパシティ （16 ページ）」を参照してください。

解像度とフレームレート値は XXXpYY として組み合わされます（たとえば、720p10 は 10 フレーム/秒で 720p を意味します）。

送信者行および受信者列の定義の略語（SD、HD、およびFHD）は、クライアントまたはデバイスの高い解像度を示しています。

- SD—標準画質（576p）

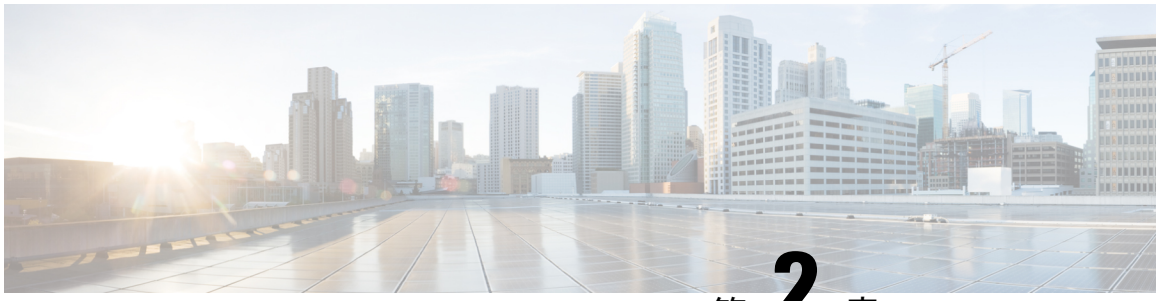
- HD—高解像度（720p）
- FHD—フル HD（1080p）

表 *2 : Video Mesh*でサポートされる解像度とフレームレート

受信者	送信者						
	Webex アプリ	Webex モバイルアプリ	SIP 登録済みデバイス（HD）	SIP 登録済みデバイス（FHD）	Webex 登録済みデバイス（SD）	Webex 登録済みデバイス（HD）	Webex 登録済みデバイス（FHD）
Webex デスクトップアプリ	720p10 混合音声*	720p10 混合音声	720p30 混合音声	720p30 混合音声	576p15 コンテンツの音声**	720p30 混合音声	720p30 混合音声
Webex モバイルアプリ	—	—	—	—	—	—	—
SIP 登録済みデバイス（HD）	720p30 コンテンツの音声	720p15 混合音声	1080p15 混合音声	1080p15 混合音声	576p15 混合音声	1080p15 混合音声	1080p15 混合音声
SIP 登録済みデバイス（FHD）	1080p30 混合音声	720p15 混合音声	1080p15 混合音声	1080p30 混合音声	576p15 混合音声	1080p15 混合音声	1080p30 混合音声
Webex 登録済みデバイス（SD）	1080p15 混合音声	720p15 混合音声	1080p15 混合音声	1080p15 混合音声	576p15 混合音声	1080p15 混合音声	1080p15 混合音声
Webex 登録済みデバイス（FHD）	1080p30 混合音声	720p15 混合音声	1080p15 混合音声	1080p30 混合音声	576p15 混合音声	1080p15 混合音声	1080p30 混合音声

* コンテンツの音声とは、共有されている特定のコンテンツ（ストリーミングビデオなど）から再生される音声をいいます。このオーディオストリームは、通常のミーティングの音声とは別個のものです。

** 混合音声とは、ミーティング参加者の音声とコンテンツ共有からの音声が混合しているものをいいます。



第 2 章

環境の準備

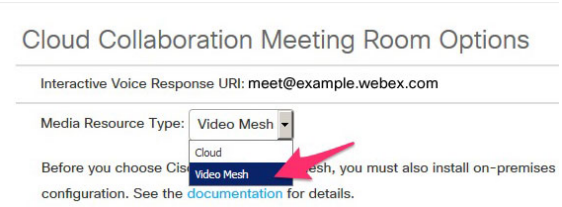
Video Mesh の要件

Video Meshは、ハイブリッドサービスのライセンス要件に記載されている機能とともに使用できます。

Video Mesh の呼制御とミーティングの統合の要件

呼制御と既存のミーティングのインフラストラクチャには Video Mesh を使用する必要はありませんが、この2つを統合することができます。呼制御およびミーティングのインフラストラクチャに Video Mesh を統合する場合は、環境が次の表に示す最低限の条件を満たしていることを確認してください。

表 *3*: の呼制御とミーティング要件 *Video Mesh*

コンポーネントの目的	サポートされている最小バージョン
オンプレミスの呼制御	Cisco Unified Communications Manager、リリース 11.5(1) SU3 またはそれ以降。（最新の SU リリースをお勧めします。） Cisco Expressway-C または E、リリース X8.11.4 またはそれ以降。（詳細については、『Expressway のリリースノート』の「重要な情報」セクションを参照してください。）
ミーティングのインフラストラクチャ	Webex WBS33 以降のミーティング。（メディアリソースの種類リストが Cloud Collaboration Meeting Room サイトオプションにある場合、Webex サイトが正しいプラットフォームにあることを確認できます。）  Video Mesh に対してサイトの準備ができていることを確認するには、カスタマーサクセスマネージャ（CSM）またはパートナーに問い合わせてください。
フェールオーバー処理	Cisco Expressway-C または E、リリース X8.11.4 またはそれ以降。（詳細については、『Expressway のリリースノート』の「重要な情報」セクションを参照してください。）

エンドポイントと Webex アプリ の要件

表 *4*: *Video Mesh*のエンドポイントとアプリの要件

コンポーネントの目的	詳細
サポートされるエンドポイント	「Webex ビデオの互換性とサポート」を参照してください。
Webex アプリ のサポートされるバージョン	Video Meshデスクトップ（Windows、Mac）およびモバイル（Android、iPhone、および iPad）について Webex アプリ をサポートしています。サポートされているプラットフォーム用のアプリをダウンロードするには、https://www.webex.com/downloads.html にアクセスしてください。

コンポーネントの目的	詳細
サポートされるコーデック	サポートされているオーディオおよびビデオコーデックについては、「通話と会議の Webex ビデオ仕様」を参照してください。Video Mesh の注意点を次に示します。 • ビデオ品質に関して、Video Mesh は、特定のシナリオで最大 1080p をサポートします。この構成は、https://admin.webex.com で変更することができます。 • SIP ビデオシステムの場合、Video Mesh は、デュアルトーンマルチ周波数（DTMF）の音声トーンを処理する SIP クライアントをサポートします。このサービスは、キーパッドマークアップ言語（KPML）もサポートします。 • クラウドに登録されている Windows および Mac、ならびに Room、Desk、および Board デバイス用の Webex Teams は、コンテンツ音声を使用して最大 1080p、30fps をサポートします。 • H.323 クライアントは、データシートには記載されていますが、クラウドにのみアクセスします。
サポートされる Webex に登録済みの Room、Desk、および Board デバイス	以下のデバイスは、Video Mesh ノードで動作することがテストおよび確認されています。 • Cisco DX70 • Cisco Webex DX80 • Cisco Webex Board 55 • Cisco Webex Room Kit • Cisco Webex Room Kit Mini • Cisco Webex Room Kit Plus • Cisco Webex Room Kit Plus Precision 60 • Cisco Webex Room Kit Pro • Cisco TelePresence SX10 Quick Set • Cisco TelePresence SX20 Quick Set • Cisco TelePresence SX80 Codec • Cisco TelePresence MX200 G2 • Cisco TelePresence MX300 G2 • Cisco TelePresence MX700 • Cisco TelePresence MX800

Video Mesh ノード ソフトウェアのシステム要件とプラットフォーム要件

実稼働環境

実稼働の展開では、特定のハードウェア構成に Video Mesh ノード ソフトウェアを展開するには、次の 2 つの方法があります。

- 各サーバーを単一の仮想マシンとしてセットアップすることができます。これは、多くの SIP エンドポイントを含む展開に最適です。
- VMNLite オプションを使用すると、各サーバーに複数の小さな仮想マシンを設定できます。VMNLite は、クライアントとデバイスの大部分が Webex アプリと Webex 登録エンドポイントである展開に最適です。

以下の要件は、すべての設定に共通です。

- VMware ESXi 6.5、6.7、または 7、vSphere 6.5、6.7、または 7
- 有効なハイパースレッディング

プラットフォーム ハードウェアに依存せずに実行される Video Mesh ノードには、専用の vCPU と RAM が必要です。他のアプリケーションとのリソースの共有はサポートされていません。これは、Video Mesh ソフトウェアのすべてのイメージに適用されます。

CMS プラットフォームの Video Mesh Lite（VMNLite）イメージの場合、VMNLite イメージの使用のみがサポートされます。VMNLite ソフトウェアを使用する CMS ハードウェア上に、他の Video Mesh イメージまたは非 Video Mesh アプリケーションを配置することはできません。

Table 5: 実稼働環境での ***Video Mesh*** ノード ソフトウェアに関するシステムおよびプラットフォームの要件

ハードウェア構成	単一の仮想マシンとしての実稼働の展開	VMNLite VM を使用した実稼働の展開	注意事項
Cisco Meeting Server 1000（CMS 1000）	• 72vCPUs（Video Mesh ノードの場合は 70、ESXi の場合は 2） • メインメモリ 60 GB • 80 GB のローカルのハードディスク容量	それぞれが以下を備えた **3** つの同一の仮想マシンインスタンスとして展開します。 • 23 vCPU • メインメモリ 20 GB • 80 GB のローカルのハードディスク容量	このプラットフォームは、Video Mesh ノードで使用することを推奨します。 **Caution** 300 GB のハードドライブを備えた CMS 1000 に VMNLite を展開すると、ESXi 7 にアップグレードするときに領域が不足する可能性があります。VMware をアップグレードする前に、500 GB 以上のハードドライブにアップグレードすることをお勧めします。

ハードウェア構成	単一の仮想マシンとしての実稼働の展開	VMNLite VM を使用した実稼働の展開	注意事項
仕様に基づいた構成 （2.6 GHz インテル Xeon E5-2600v3 またはそれ以降のプロセッサが必要です）	• 72vCPUs（Video Mesh ノードの場合は 70、ESXi の場合は 2） • メインメモリ 60 GB • 80 GB のローカルのハードディスク容量 または 80 GB の NFS ストレージ	それぞれが以下を備えた **3** つの同一の仮想マシンインスタンスとして展開します。 • 23 vCPU • メインメモリ 20 GB • 80 GB のローカルのハードディスク容量 または 80 GB の NFS ストレージ	各 Video Mesh 仮想マシンには、CPU、RAM、およびハードドライブが専用に予約されている必要があります。 構成中は、**CMS1000** または **VMNLite** オプションのいずれかを使用します。 NFS ストレージのピーク IOPS（1 秒あたりの入出力操作）は 300 IOPS です。
Cisco Meeting Server 2000（CMS 2000）	それぞれが以下を備えた **8** つの同一の仮想マシンインスタンスとして展開します。 • 72vCPUs（Video Mesh ノードの場合は 70、ESXi の場合は 2） • メインメモリ 60 GB • 80 GB のローカルのハードディスク容量 または 80 GB の NFS ストレージ	それぞれが以下を備えた **24** つの同一の仮想マシンインスタンスとして展開します。 • 23 vCPU • メインメモリ 20 GB • 80 GB のローカルのハードディスク容量 または 80 GB の NFS ストレージ	このプラットフォームは、Video Mesh ノードで使用することを推奨します。 各ブレードは、ブレードごとに予約済みの CPU、RAM、およびハードドライブを備えた完全な Cisco Meeting Server 1000 である必要があります。 NFS ストレージのピーク IOP は 300 IOPS です。

デモ環境

基本的なデモの目的で、次の最小要件を満たした、仕様に基づくハードウェア構成を使用できます。

- 14vCPUs（12 の場合は Video Mesh ノード、ESXi の場合は 2）
- メイン メモリ 8 GB
- 20 GB のローカルのハードディスク容量
- 2.6 GHz インテル Xeon E5-2600v3 またはそれ以降のプロセッサ

Note Video Mesh のこの設定は、Cisco TAC でサポートされていません。

デモソフトウェアの詳細については、Video Mesh ノード デモ用ソフトウェア, on page 173 を参照 してください。

帯域幅の要件

アップロードとダウンロードの両方が正常に機能するには、Video Mesh ノードのインターネット帯域幅が 10 Mbps 以上である必要があります。

Video Mesh のプロキシサポートの要件

- Video Mesh ノードに統合できるものとして公式にサポートされているのは、次のプロキシソリューションです。
  - Cisco Web セキュリティアプライアンス（WSA）（透過的なプロキシ向け）
  - Squid（明示的なプロキシ）
- 検査する（トラフィックを復号する）明示的なプロキシまたは透過的な検査プロキシの場合、ウェブインターフェイスの Video Mesh ノード信頼ストアにアップロードする必要があるプロキシのルート証明書のコピーが必要です。
- 以下の明示的なプロキシおよび認証タイプの組み合わせをサポートしています。
  - 認証なし（http および https）
  - 基本認証（http および https）
  - ダイジェスト認証（https のみ）
  - NTLM 認証（http のみ）
- 透過的なプロキシの場合、HTTPS/443 トラフィックを強制的にプロキシに送信するには、ルーター/スイッチを使用する必要があります。WebSocket を強制的にプロキシに送信することもできます。（WebSocket は https を使用します。）

（注） Video Mesh には、ノードが正常に機能するように、クラウドサービスへの WebSocket 接続が必要です。明示的な検査および透過的な検査プロキシでは、http ヘッダーが適切な WebSocket 接続に必要です。変更された場合、WebSocket 接続は失敗します。

WebSocket 接続がポート 443 で発生する場合（透過的な検査プロキシが有効な場合）、Control Hub での登録後の警告（「Webex Video Mesh SIP コールが正しく動作していません」）が表示されます。プロキシが有効になっていない場合は、他の理由で同じアラームが発生する可能性があります。ポート 443 で WebSocket ヘッダーがブロックされている場合、メディアはアプリと SIP クライアントの間でフローしません。

これは、メディアがフローしていない場合において、ポート 443 経由でノードからの https トラフィックが失敗したときに、頻繁に発生します。

- ポート 443 のトラフィックはプロキシによって許可されますが、これは検査用プロキシであり、WebSocket を破損しています。

これらの問題を解決するには、ポート 443 で *.wbx2.com および *.ciscospark.com に「バイパス」または「スプライス」（検査を無効）する必要がある場合があります。

Video Mesh ノードのキャパシティ

Video Mesh はソフトウェアベースのメディア製品であるため、Video Mesh ノードのキャパシティはさまざまです。特に、Webex クラウドのミーティング参加者は、ノードにより大きな負荷をかけます。Webex クラウドへのカスケードが増えると、キャパシティが少なくなります。キャパシティに影響を与えるその他の要因は次のとおりです。

- デバイスやクライアントの種類
- ビデオ解像度
- ネットワーク品質
- ピーク負荷
- 導入モデル

（注） Video Mesh の使用は、Webex のライセンス数に影響しません。

一般に、クラスタにノードを追加してもキャパシティが 2 倍になることはありません。これは、カスケードの設定によるオーバーヘッドが原因です。これらの数値を一般的な指針として使用します。推奨事項は次のとおりです。

- 展開のための一般的なミーティングシナリオをテストします。
- Control Hub の分析を使用して、展開状況の変化を確認し、必要に応じてキャパシティを追加します。

（注） 低いコールボリュームにおけるオーバーフロー（特にオンプレミスで発生した SIP コール）は、真にスケールを反映するものではありません。Video Mesh 分析（**Control Hub > [リソース（Resources）] > [コール アクティビティ（Call Activity）]** の下）は、オンプレミスで発信されたコール レッグを示します。メディア処理のために、カスケード経由で Video Mesh ノードに着信したコールストリームは指定しません。ミーティングにおけるリモート参加者の数が増えれば、カスケードが増加し、Video Mesh ノード上のオンプレミスのメディアリソースが消費されます。

次の表は、通常の Video Mesh ノード上のさまざまに混在する参加者とエンドポイントのキャパシティ範囲を示しています。テストには、すべての参加者がローカルノード上にいるミーティングと、ローカルとクラウドの参加者が混在するミーティングが含まれていました。Webex クラウドに参加者が増えると、キャパシティが範囲の下限に達することが予想されます。

表 *6 :* 通常の *Video Mesh* ノードのキャパシティ

シナリオ	解像度	参加可能人数
Webex アプリの参加者のみとのミーティング	720p	100 ～ 130
	1080p	90 ～ 100
Webex アプリの参加者のみとのミーティングと 1 対 1 の通話	720p	60 ～ 100
	1080p	90 ～ 100
SIP 参加者のみとのミーティング	720p	70 ～ 80
SIP 参加者のみとのミーティング	1080p	30 ～ 40
Webex アプリおよび SIP 参加者とのミーティング	720p	75 ～ 110

（注）
- Webex アプリの基本解像度は 720p です。ただし、共有すると、参加者のサムネイルは 180p になります。
- これらのパフォーマンスの数値は、推奨されるすべてのポートが有効になっていることを前提としています。

VMNLite のキャパシティ

Webex アプリとクラウドに登録されたエンドポイントを主に含む展開の場合、VMNLite をお勧めします。これらの展開では、ノードのスイッチングは標準構成よりも多く、トランスコーディングリソースは標準構成よりも少なくなっています。このシナリオでは、ホスト上で複数の小規模な仮想マシンを展開することで、リソースが最適化されます。

次の表は、さまざまに混在する参加者とエンドポイントのキャパシティ範囲を示しています。テストには、すべての参加者がローカルノード上にいるミーティングと、ローカルとクラウドの参加者が混在するミーティングが含まれていました。Webex クラウドに参加者が増えると、キャパシティが範囲の下限に達することが予想されます。

表 *7: VMNLite* ノードのキャパシティ

シナリオ	解像度	サーバー上に 3 つの VMNLite ノードを持つ参加者のキャパシティ
Webex アプリの参加者のみとのミーティング	720p	250 ～ 300
	1080p	230 ～ 240
Webex アプリの参加者のみとのミーティングと 1 対 1 の通話	720p	175 ～ 275
	1080p	230 ～ 240

（注） Webex アプリミーティングの基本解像度は 720p です。ただし、共有すると、参加者のサムネイルは 180p になります。

Video Mesh のクラスタ

Video Mesh ノードをクラスタに展開します。クラスタは、ネットワークの近接性など、同様の属性を持つ Video Mesh ノードを定義します。参加者は、次の条件に応じて、特定のクラスタまたはクラウドを使用します。

- オンプレミスのクラスタに到達可能な企業のネットワークのクライアントは、そのクラスタに接続されます。これは、企業のネットワークのクライアントに対する優先設定です。
- Video Mesh のプライベートミーティングに参加するクライアントは、オンプレミスのクラスタにのみ接続します。これらのプライベートミーティング専用に別個のクラスタを作成できます。
- オンプレミスのクラスタに到達できないクライアントは、クラウドに接続されます。このケースには、企業のネットワークに接続していないモバイルデバイスが該当します。

- 選択されるクラスタには、場所だけでなく、遅延も影響します。たとえば、Video Mesh クラスタよりも低い STUN ラウンドトリップ（SRT）遅延が発生しているクラウドクラスタは、ミーティングに適しています。このロジックにより、SRT 遅延が大きく、地理的に遠いクラスタをユーザーが使用することを回避します。

各クラスタには、Video Mesh プライベートミーティングを除いて、必要に応じて他のクラウドミーティング クラスタにミーティングをカスケードするロジックが含まれています。カスケードによって、ミーティング中にクライアント間でメディアを転送するデータパスが提供されます。ミーティングは複数のノードに分散されます。クライアントは、ネットワークトポロジ、WAN リンク、リソース使用率などの要素に従って、地理的に最も近く最も効率的なノードを使用します。

メディアノードに対するクライアントの ping 機能によって到達可能性が決まります。実際のコールでは、UDP や TCP などのさまざまな接続メカニズムが使用されます。コールの前に、Webex デバイス（Room、Desk、Board、および Webex アプリ）は Webex クラウドに登録され、そのコールのクラスタ候補のリストを提供します。

（注） Video Mesh クラスタ内のノードは、互いにスムーズな通信が必要です。また、他のすべての Video Mesh クラスタ内のノードとのスムーズな通信も必要です。ファイアウォールが Video Mesh ノード間のすべての通信を許可していることを確認します。

プライベートミーティング用のクラスタ

プライベートミーティング用に Video Mesh クラスタを予約できます。予約済みクラスタがいっぱいになると、プライベート ミーティング メディアが他の Video Mesh クラスタにカスケードされます。予約済みクラスタがいっぱいになると、プライベートミーティングと非プライベートミーティングは残りのクラスタのリソースを共有します。

非プライベートミーティングは予約済みクラスタを使用せず、それらのリソースをプライベートミーティング用に予約します。非プライベートミーティングでネットワーク上のリソースが不足すると、代わりに Webex クラウドにカスケードされます。

Video Mesh のプライベートミーティング機能の詳細については、「プライベートミーティング（129 ページ）」を参照してください。

重要 プライベートミーティング用にすべての Video Mesh クラスタを予約する場合、短いビデオアドレス形式（meet*@your_site*）を使用することはできません。これらのコールは現在、適切なエラーメッセージなしで失敗します。一部のクラスタを予約しないままにしておくと、短いビデオアドレス形式のコールはそれらのクラスタを介して接続できます。

Video Mesh クラスタの展開に関するガイドライン

- 典型的な企業の展開では、クラスタごとに使用するノード数を最大100個にすることをお勧めします。システムでは、100 個を超えるノードを使用するクラスタのサイズをブロックするハード制限は設定されていません。ただし、より大きなクラスタを作成する必要がある場合は、シスコアカウントチームを通じてシスコエンジニアリングとこのオプションを確認することを強く推奨します。
- リソースのネットワークプロキシミティ（アフィニティ）が似ている場合は、作成するクラスタを少なくします。
- クラスタを作成する場合は、同じ地理的なリージョンと同じデータセンター内にあるノードだけを追加します。ワイドエリアネットワーク（WAN）上でのクラスタリングはサポートされていません。
- 通常は、集中的にミーティングを頻繁にホストする企業にクラスタを展開します。クラスタの配置場所は、WAN に接続する企業内の各場所で利用できる帯域幅を考慮して計画します。時間の経過と共に測定されたユーザーパターンを基に、クラスタ単位で展開および拡張できます。
- タイムゾーンが異なるクラスタは、コールパターンのピークおよびビジー時間が異なるため、複数の地域を効果的に処理できます。
- 2 つの Video Mesh ノードが 2 つの異なるデータセンター（EU と北米など）に存在し、各データセンターを介してエンドポイントが参加している場合、各データセンター内のノードはクラウド内の1つのVideo Meshノードにカスケードします。これらのカスケードは、インターネットを介します。クラウドからの参加者がすでにいる場合（Video Mesh参加者の前に参加している）、ノードはクラウドからの参加者のメディアノードを介してカスケードされます。

異なるタイムゾーン

タイムゾーンが異なると、オフピーク時にクラスタを共有できるようになります。たとえば、「Northern California」クラスタと「New York」クラスタを設置している会社があります。これら2つの場所は、ネットワーク遅延が全体としてそれほど高くなく、地理的な理由で利用者数にずれがあります。「Northern California」クラスタでリソースの利用がピークの時、「New York」クラスタはおそらくピークではなくキャパシティに余裕があります。「New York」クラスタのピーク時間についても、「Northern California」クラスタでは同じことが当てはまります。リソースを効果的に導入するための方法は他にもありますが、主に使われている方法はこの 2 つです。

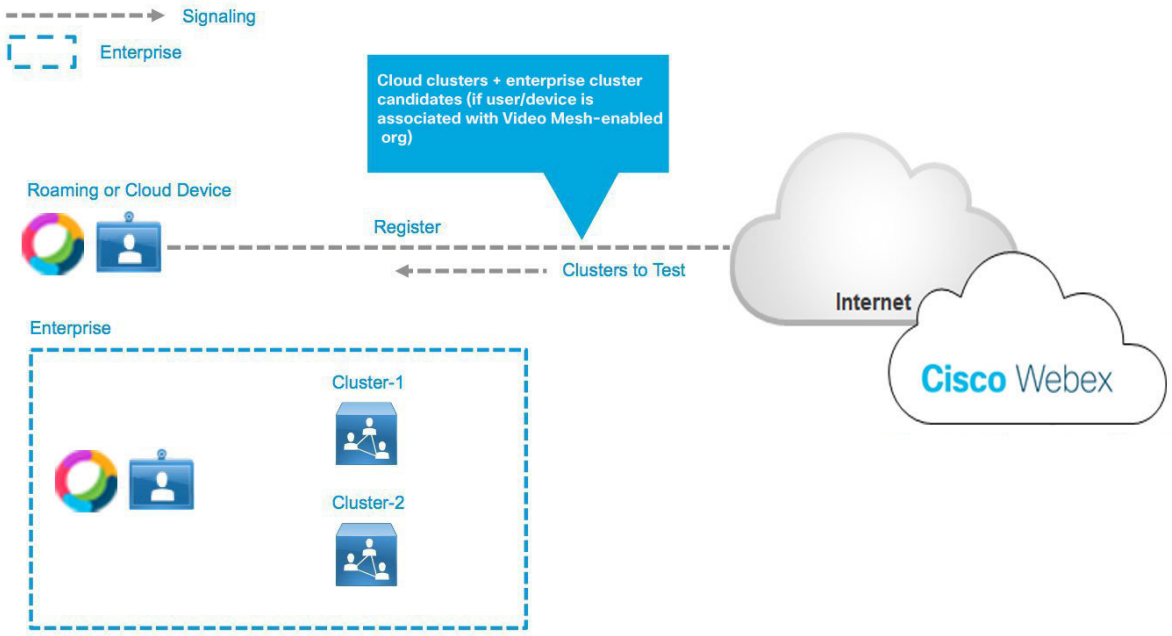
クラウドへのオーバーフロー

すべてのオンプレミスクラスタのキャパシティがいっぱいになると、オンプレミスの参加者がWebexクラウドにオーバーフローします。これは、すべてのコールがクラウドにホストされることを意味するわけではありません。Webexは、リモートの参加者、またはオンプレミスのクラスタに接続できない参加者のみをクラウドにダイレクトします。オンプレミスとクラウドの

参加者が両方いるコールでは、オンプレミスのクラスタはクラウドにブリッジし（カスケード）、すべての参加者を 1 つのコールに結合します。

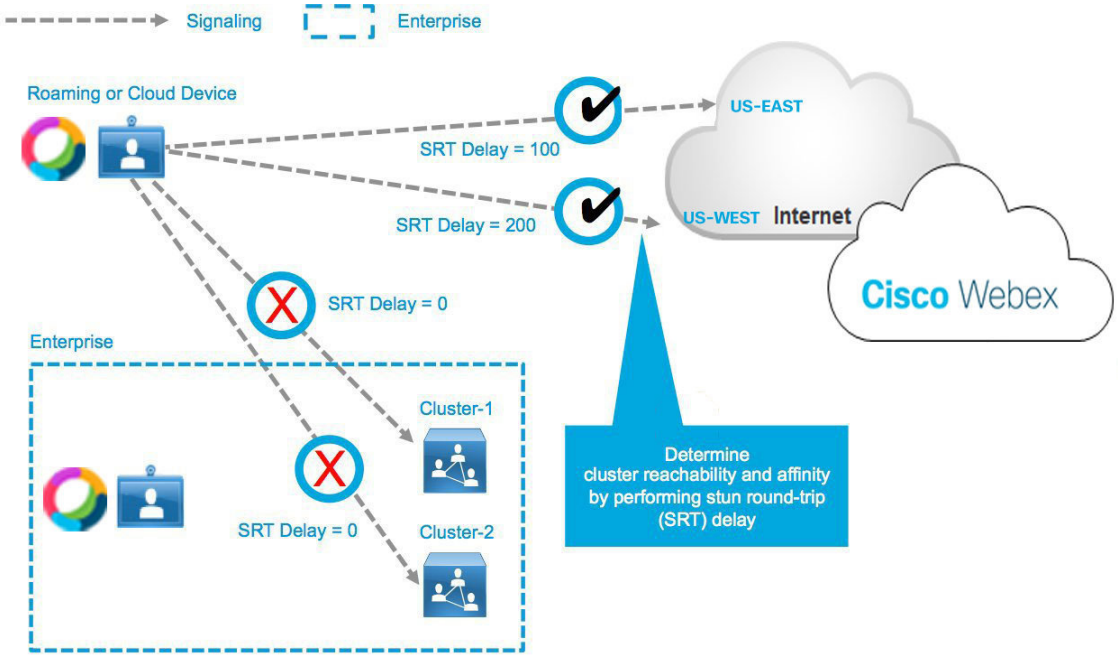
ミーティングをプライベート ミーティング タイプとして設定した場合、Webex はすべての通話をオンプレミスのクラスタに保持します。プライベートミーティングがクラウドにオーバーフローすることはありません。

Webex への Webex Device の登録

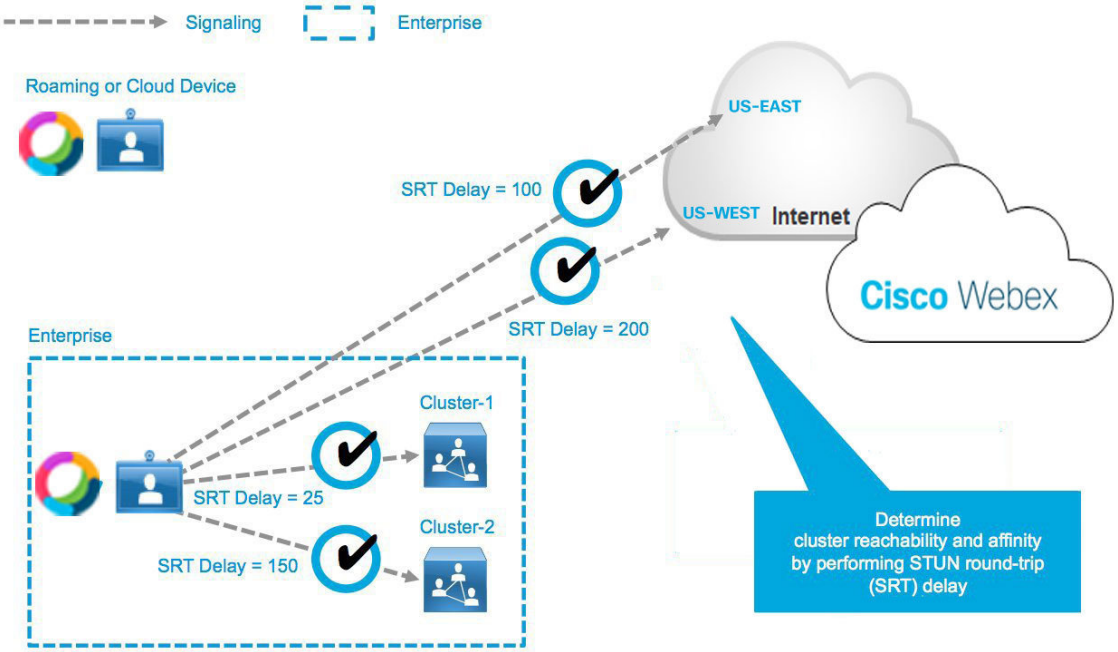


到達可能性を判定するだけでなく、クライアントは、STUN（Simple Traversal of UDP through NAT）を使用して、ラウンドトリップ遅延の定期的なテストも実行します。STUN ラウンドトリップ（SRT）遅延は、実際のコールで利用可能なリソースを選択する際に重要な要素になります。複数のクラスタが展開されている場合、第 1 の選択基準は学習した SRT 遅延に基づきます。到達可能性テストは、ネットワーク変更など多数の要因によって開始され、バックグラウンドで実行されます。到達可能性テストによって、コールの設定時間に影響するような遅延が発生することはありません。次の 2 つの例は、到達可能性テストの結果を示しています。

ラウンドトリップ遅延テスト - クラウドデバイスがオンプレミスのクラスタに到達しない



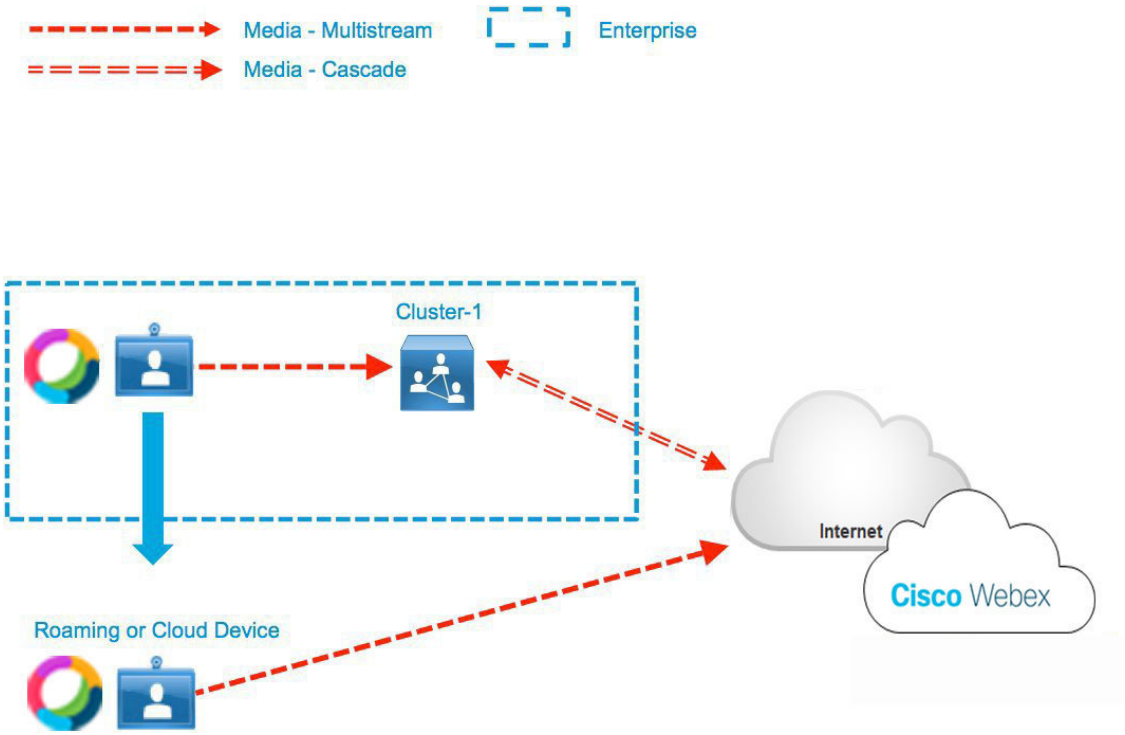
ラウンドトリップ遅延テスト - クラウドデバイスがオンプレミスのクラスタに正常に到達



コールがセットアップされるたびに、Webexクラウドに学習した到達可能性情報が提供されます。この情報により、クラウドはクライアントと利用可能なクラスタの相対的な位置やコールの種類基づいて最適なリソース（クラスタまたはクラウド）を選択できます。推奨されるクラスタに利用できるリソースがない場合は、SRT遅延に基づいてすべてのクラスタの可用性をテストします。推奨されるクラスタには、SRT遅延が最も低いクラスタが選択されます。オンプレミスで処理されるコールは、プライマリクラスタがビジーの場合、セカンダリクラスタで処理されます。ローカルの到達可能なVideo Meshリソースは、最も低いSRT遅延の順序で最初に試されます。すべてのローカルリソースが使い果たされると、参加者はクラウドに接続します。

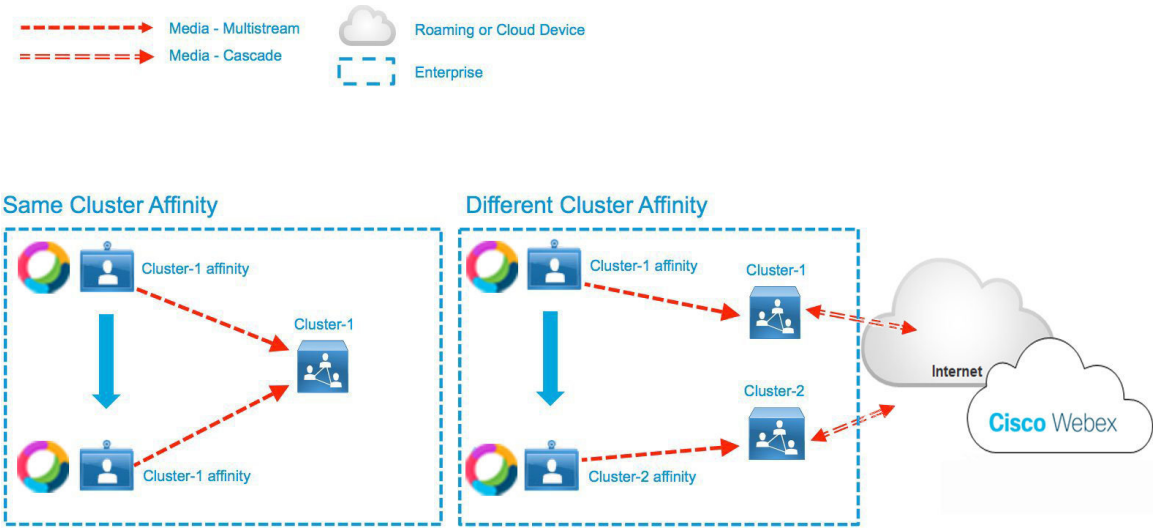
参加者が全体として優れた操作性を実感できる導入のためには、クラスタの定義と場所が極めて重要です。クライアントが位置している場所で、導入がリソースを提供することが理想です。クライアントがコールの大半を行う場所に十分なリソースを割り当てられない場合は、ユーザーを遠方のクラスタに接続することになるため、内部ネットワークの帯域幅が多く消費されます。

オンプレミスとクラウドコール



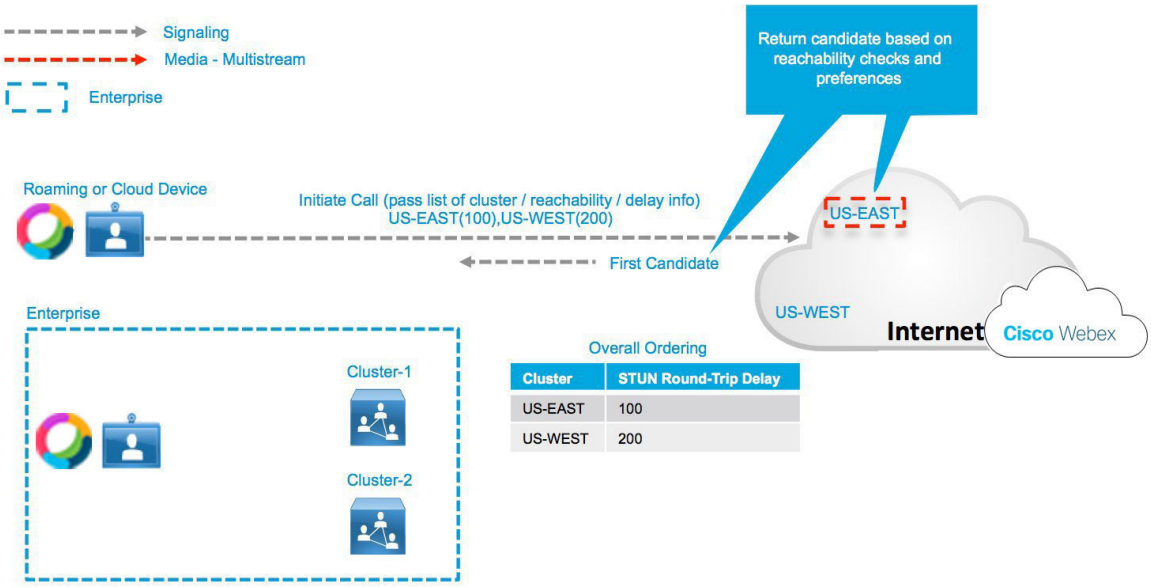
オンプレミスのWebexデバイスのうち、クラスタ アフィニティ（クラスタへの近さに基づく優先度）が同じであるデバイスは同じクラスタに接続して、コールに対応します。クラスタアフィニティが異なるオンプレミスのWebexデバイスは、異なるクラスタに接続します。これらのクラスタは、2つの環境を1つのコールに結合するため、クラウドにカスケードされます。これにより、Webexクラウドをハブとして使用するハブアンドスポーク設計が作成され、オンプレミスクラスタがミーティングのスポークとして機能します。

異なるクラスタアフィニティのオンプレミス コール

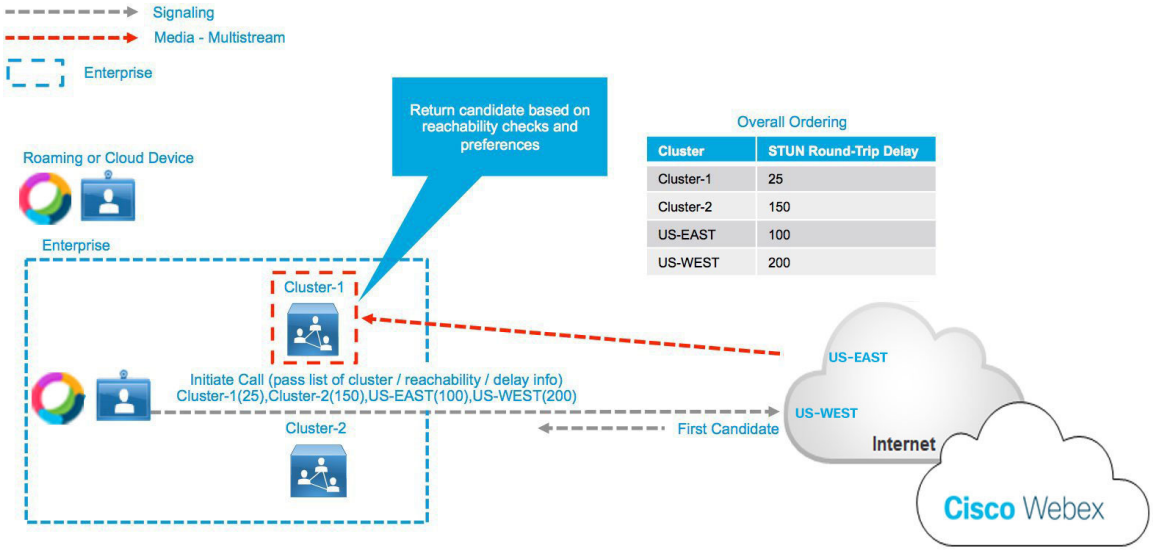


Webexデバイスは、到達可能性に応じて、オンプレミスのクラスタまたはクラウドベースのいずれかに接続されます。以下に、最も一般的なシナリオをいくつか示します。

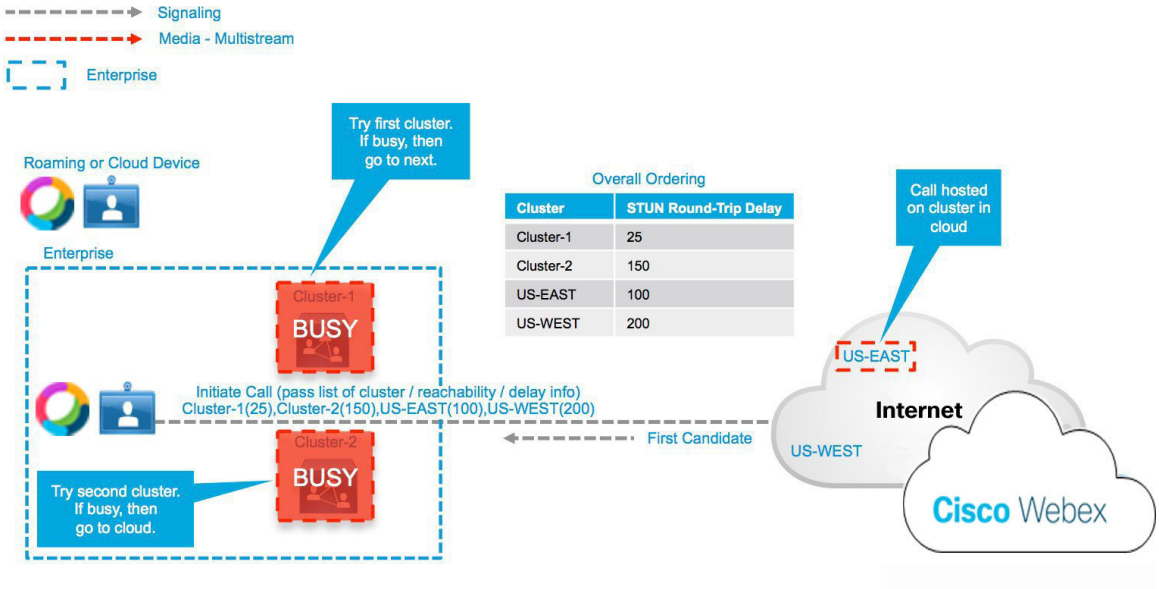
Webexクラウドに接続されているクラウドデバイス



Webexオンプレミスのクラスタに接続されるオンプレミスのデバイス



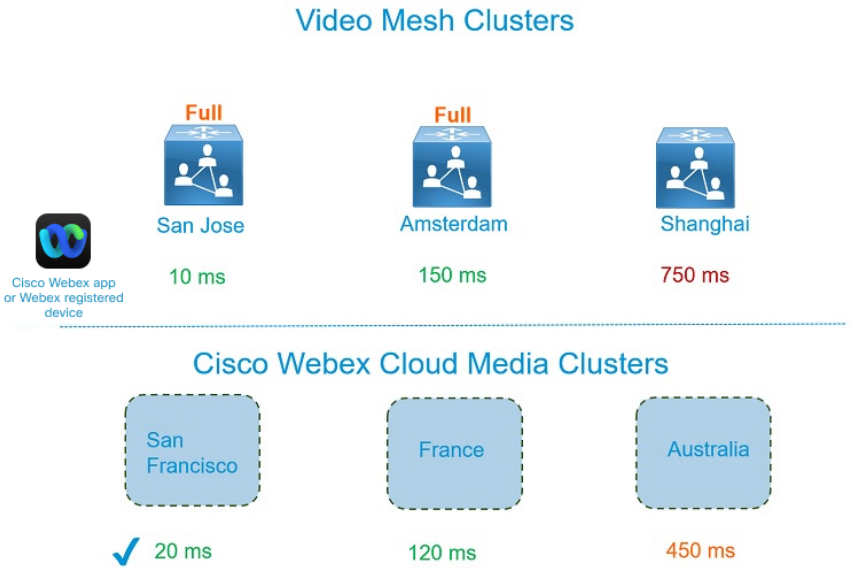
Webex クラウドに接続されるオンプレミスのデバイス



250 ms 以上の STUN ラウンドトリップ遅延に基づくオーバーフローのためのクラウドクラスタの選択

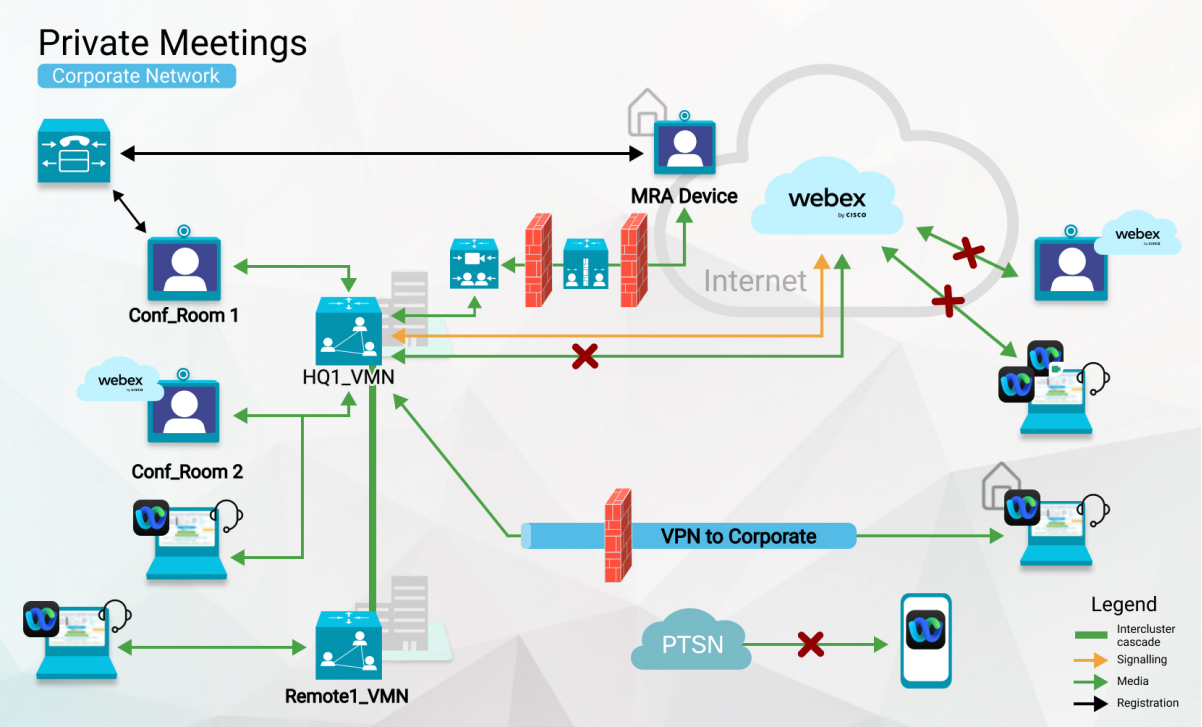
ノードの選択にはローカルに展開されている Video Mesh ノードが望ましいですが、オンプレミスの Video Mesh クラスタに対する STUN ラウンドトリップ（SRT）遅延が、許容可能なラ

ウンドトリップ遅延の250ミリ秒を超える場合（これは、通常、オンプレミスのクラスタが別の大陸で構成されている場合に発生します）、Video Mesh ノードの代わりに地理的に最も近いクラウドメディアノードが選択されるシナリオをサポートしています。



- Webex アプリ または Webex デバイスは、サンノゼ内のエンタープライズ ネットワーク上にあります。
- サンノゼ、アムステルダムのクラスタは、キャパシティをすべて使用しているか、利用できない状態です。
- 上海クラスタへの SRT 遅延は 250 ミリ秒を超え、メディア品質の問題を生じさせる可能性があります。
- SRT 遅延が最も小さいのは、サンフランシスコのクラウドクラスタです。
- 上海 Video Mesh クラスタは、検討対象から除外されます。
- 結果として、Webex アプリ はサンフランシスコのクラウドクラスタにオーバーフローします。

プライベートミーティング



プライベートミーティングでは、Video Mesh を介してすべてのメディアをネットワークに隔離します。通常のミーティングとは異なり、ローカルノードがいっぱいの場合、メディアは Webex クラウドにカスケードしません。ただし、デフォルトでは、プライベートミーティングはネットワーク上のさまざまな Video Mesh クラスタにカスケードできます。地理的な場所にまたがるプライベートミーティングの場合、Video Mesh クラスタは相互に直接接続して、図の HQ1_VMN から Remote1_VMN のようにクラスタ間カスケードを許可する必要があります。

クラスタ間のカスケードを妨げられないように、必要なポートがファイアウォールで開いていることを確認します。「管理用のポートとプロトコル （33 ページ）」を参照してください。

プライベートミーティングのすべての参加者は、ミーティングホストの Webex 組織に属している必要があります。Webex アプリまたは認証済みビデオシステム（UCM/VCS に登録された SIP エンドポイントまたは Webex 登録ビデオデバイス）を使用して参加できます。ネットワークへの VPN または MRA アクセスを持つ参加者は、プライベートミーティングに参加できます。ただし、ネットワークの外部からプライベートミーティングに参加することはできません。

Video Mesh でサポートされている展開モデル

Video Mesh 導入でサポート済み

- Video Mesh ノードは、データセンター（推奨）、または Demilitarized Zone（DMZ; 緩衝地帯）のいずれかに展開できます。詳しくは、「Video Mesh で使用されるポートとプロトコル （32 ページ）」を参照してください。
- DMZ 導入の場合は、デュアル ネットワーク インターフェイス（NIC）を使用してクラスタ内の Video Mesh ノードを構成できます。この導入によって、エンタープライズ ネットワークトラフィックを（インターボックス通信、ノードクラスタ間のカスケード、ノードの管理インターフェイスへのアクセスに使用される）外部のクラウド ネットワーク トラフィック（外部への接続に使用され、クラウドにカスケード）から分離することができます。

  デュアルNICは、Video Mesh ノードソフトウェアの完全版、VMNLite、デモバージョンで動作します。また、1:1 NAT 設定の背後に Video Mesh を展開することもできます。
- 呼制御環境と Video Mesh ノードを統合することができます。Unified CM に統合されているVideo Meshの導入例は、「Video Mesh と Cisco Unified Communications Manager の導入モデル （29 ページ）」を参照してください。
- 次のアドレス変換タイプがサポートされています。
  - IP プールを使用したダイナミック ネットワークアドレス変換（NAT）
  - ダイナミックポートアドレス変換（PAT）
  - 1 対 1 の NAT
  - その他の NAT フォームも、正しいポートとプロトコルが使用されていれば機能しますが、テストを実施していないため正式にはサポートしていません。
- IPv4
- Video Mesh ノード の静的 IP アドレス

Video Mesh 導入では未対応

- IPv6
- Video Mesh ノード 用の DHCP
- シングル NIC とデュアル NIC が混在するクラスタ
- ワイドエリアネットワーク（WAN）経由の Video Mesh ノードクラスタリング
- Video Mesh ノード を通過しない音声、ビデオ、またはメディア
  - 電話の音声

- Webex アプリ と標準規格ベースのエンドポイント間のピアツーピアコール
- Video Mesh ノード での音声終端
- Expressway C/E ペアから送信されるメディア
- Webex からのビデオコールバック

Video Mesh と Cisco Unified Communications Manager の導入モデル

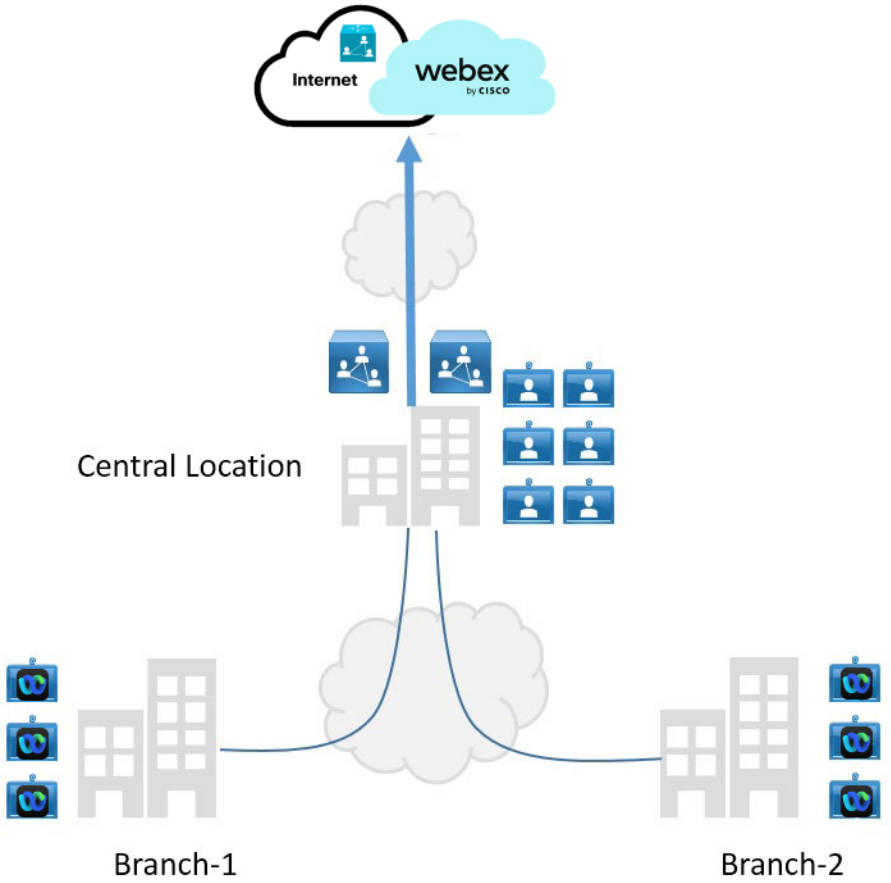
これらの例 は、一般的な Video Mesh 展開を示しており、Video Mesh クラスタがネットワークに収まる場所を理解するのに役立ちます。Video Mesh 展開は、ネットワークトポロジの要因によって異なることを念頭に置いてください。

- データセンターの位置
- 拠点の場所と規模
- インターネットアクセスの場所とキャパシティ

通常は、Video Mesh ノードを Unified CM または Session Management Edition（SME）クラスタに関連付けます。ベストプラクティスとして、ノードはできる限りローカルブランチに集中するようにします。

Video Mesh は、Session Management Edition（SME）をサポートしています。Unified CM クラスタは、SME を介して接続することができます。その後、Video Mesh ノードに接続する SME トランクを作成する必要があり ます。

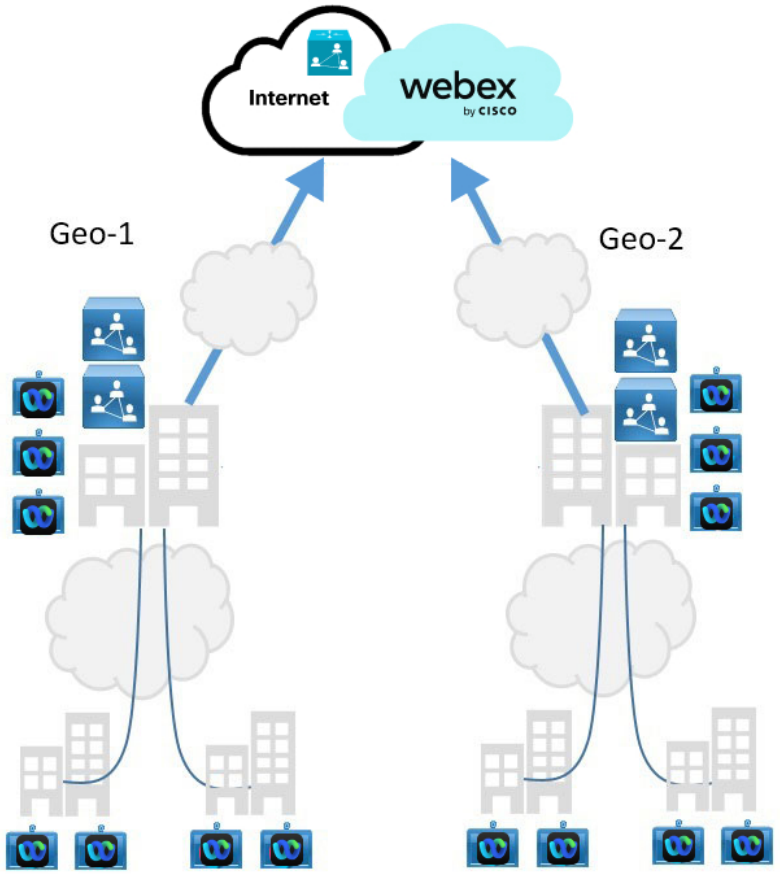
ハブおよびスポークアーキテクチャ



この導入モデルは、集中管理型ネットワーキングとインターネットアクセスが含まれています。通常、集中管理型の場所には多数の従業員が集中します。この場合、メディア処理の最適化のために Video Mesh クラスタが中央に配置されます。

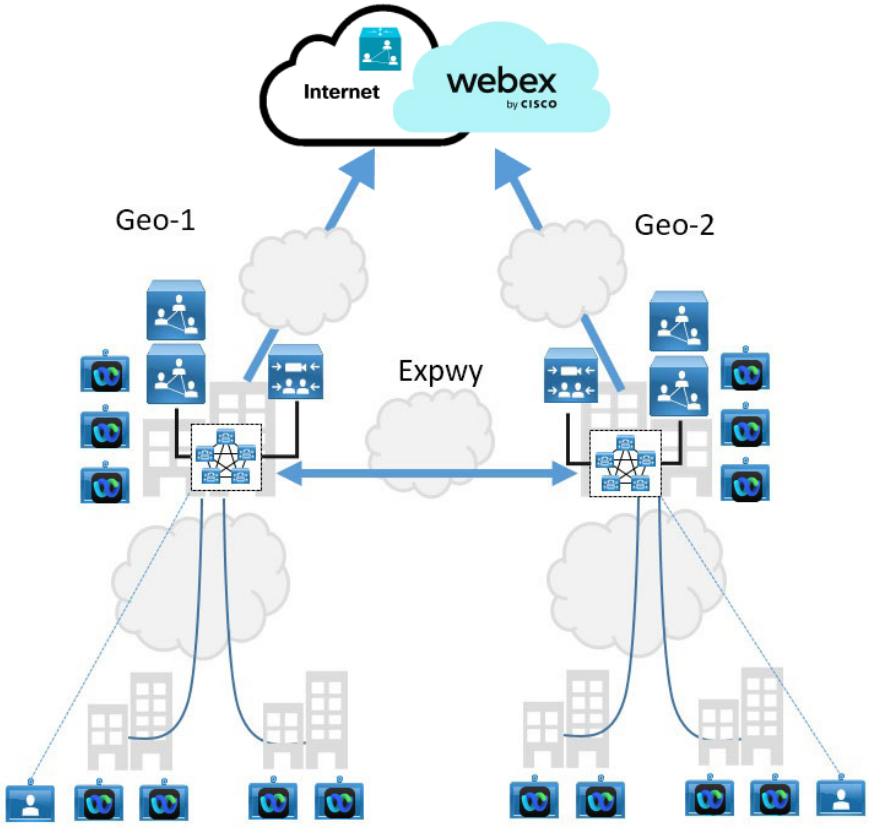
ブランチの場所にクラスタを配置しても、短期的には何の利点も得られず、最適ではないルーティングが行われることもあります。ブランチには、ブランチ間の通信が頻繁な場合のみクラスタを展開することをお勧めします。

地理的な分布



導入を地理的に分散させた場合はインターコネクトしますが、地域間に無視できない遅延が見られることがあります。各地域のユーザー間でミーティングが行われる場合にリソースが不足していると、短期的に最適ではないカスケードが設定される可能性があります。このモデルでは、地域のインターネットアクセスに近い Video Mesh ノードを割り当てることを推奨します。

SIP ダイヤルを利用する地理的な分布



この導入モデルでは、地域ごとの Unified CM クラスタが含まれます。各クラスタには、ローカル Video Mesh クラスタ内のリソースを選択するための SIP トランクを含めることができます。リソースが制限される場合、2 番目のトランクは、Expressway にフェールオーバーパスを提供できます。

Video Mesh で使用されるポートとプロトコル

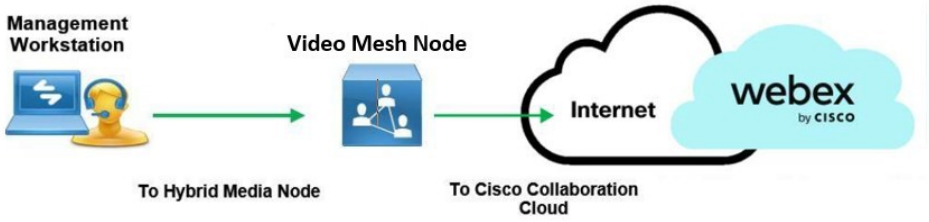
Video Mesh の正常な導入を実行し、Video Mesh ノードの問題の無い運用を行うには、ファイアウォール上の次のポートを使用して、プロトコルを使用します。

- Webex Teams の全体的なネットワーク要件を理解するには、「Webex サービスのネットワーク要件」を参照してください。
- Webex サービスに対するファイアウォールとネットワーク プラクティスの詳細については、「ファイアウォール トラバーサル ホワイトペーパー」を参照してください。
- 潜在的な DNS クエリの問題を軽減するには、企業のファイアウォールを構成する際に「DNS のベストプラクティス、ネットワーク保護および攻撃の識別」に関するドキュメントに従ってください。

- 設計情報の詳細については、「ハイブリッドサービス（CVD）の推奨アーキテクチャ」を参照してください。

管理用のポートとプロトコル

図 *2 :* 管理用のポートとプロトコル



（注） Video Mesh クラスタ内のノードは、互いにスムーズな通信が必要です。また、他のすべての Video Mesh クラスタ内のノードとのスムーズな通信も必要です。ファイアウォールが Video Mesh ノード間のすべての通信を許可していることを確認します。

クラスタ内の Video Mesh ノードは、同じ VLAN またはサブネットマスク内に存在する必要があります。

目的	送信元	送信先	送信元 IP	送信元ポート	トランスポート プロトコル	宛先 IP	宛先ポート
管理	管理コンピュータ	Video Mesh ノード	必要に応じて入力	すべて	TCP、HTTPS	Video Mesh ノード	443
Video Mesh 管理コンソールにアクセスするための SSH	管理コンピュータ	Video Mesh ノード	必要に応じて入力	すべて	TCP	Video Mesh ノード	22
クラスタ間通信	Video Mesh ノード	Video Mesh ノード	クラスタ内の他の Video Mesh ノードの IP アドレス	任意	TCP	Video Mesh ノード	8443

目的	送信元	送信先	送信元 IP	送信元ポート	トランスポート プロトコル	宛先 IP	宛先ポート
管理	Video Mesh ノード	Webex クラウド	必要に応じて入力	すべて	UDP、NTP UDP、DNS TCP、HTTPS（Websocket）	いずれか（Any）	123* 53*
カスケード シグナリング	Video Mesh ノード	Webex クラウド	すべて	すべて	TCP	すべて	443
カスケード メディア	Video Mesh ノード	Webex クラウド	Video Mesh ノード	任意***	UDP	任意 特定のアドレス範囲については、Webex サービスのネットワーク要件の「Webex メディアサービスの IP サブネット」セクションを参照してください。	5004 50000 ～ 53000 詳細については、Webex サービスのネットワーク要件の「Webex サービス – ポート番号とプロトコル」セクションを参照してください。
カスケード シグナリング	Video Mesh クラスタ（1）	Video Mesh クラスタ（2）	すべて	すべて	TCP	すべて	443
カスケード メディア	Video Mesh クラスタ（1）	Video Mesh クラスタ（2）	Video Mesh クラスタ（1）	任意***	UDP	任意	5004 50000 ～ 53000
管理	Video Mesh ノード	Webex クラウド	必要に応じて入力	すべて	TCP、HTTPS	すべて**	443

目的	送信元	送信先	送信元 IP	送信元ポート	トランスポート プロトコル	宛先 IP	宛先ポート
管理	Video Mesh ノード（1）	Video Mesh ノード（2）	Video Mesh ノード（1）	いずれか（Any）	TCP、HTTPS（Websocket）	Video Meshノード（2）	443
社内連絡	Video Mesh ノード	他のすべての Video Mesh ノード	Video Mesh ノード	任意	UDP	任意	10000 ～ 40000

* OVA のデフォルト設定は、NTP と DNS に対して設定されます。OVA にあるこれらのアウトバウンドポートをインターネットに対してオープンする必要があります。ローカルの NTP と DNS サーバーを設定する場合、ポート 53 と 123 をファイアウォール経由でオープンする必要はありません。

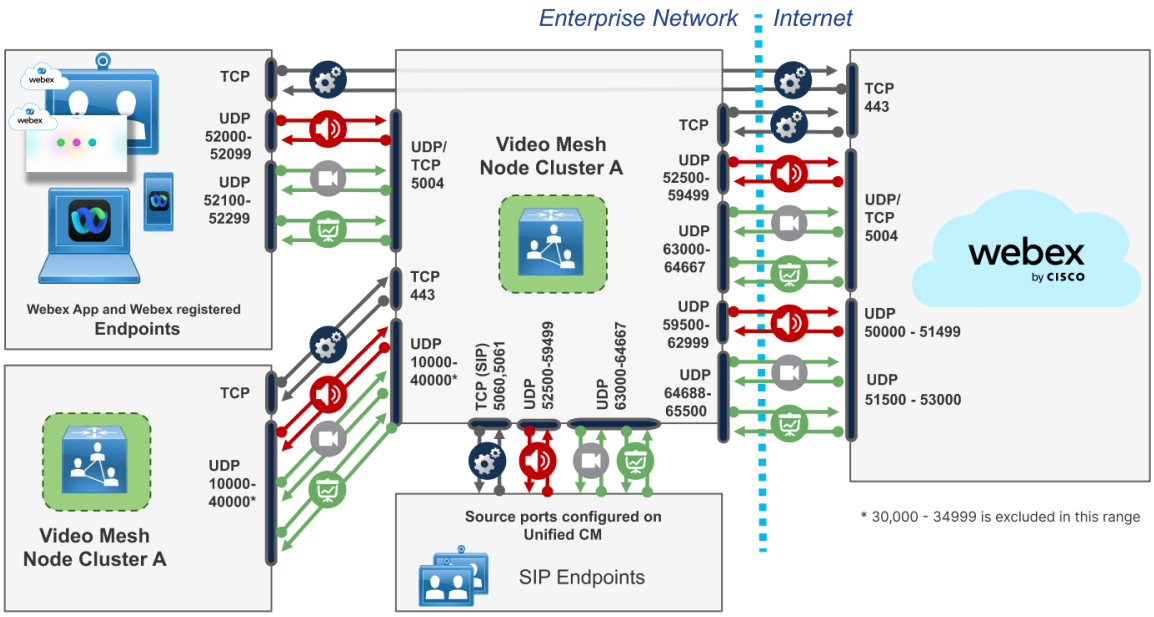
** 一部のクラウドサービス URL は警告なしに変更される可能性があるため、問題を発生しない Video Mesh ノードの操作には「すべて」を宛先として推奨します。URL に基づいてトラフィックをフィルタ処理する場合の詳細については、Webex Services のネットワーク要件の「ハイブリッドサービス の Webex Teams URL」 セクションを参照してください。

***ポートは、QoS を有効にするかどうかによって異なります。QoS が有効になっている場合、ポートは 52500 ～ 59499、63000 ～ 64667、59500 ～ 62999、および 64688 ～ 65500 です。QoS をオフにすると、ポートは 34,000 ～ 34,999 になります。

Video Meshのトラフィック署名（有効なQuality of Service（QoS））

値リストコレクション作成者がDMZの企業側またはファイアウォール内に存在する展開では、Webex Control Hub に値リストコレクション作成者構成が設定されているため、管理者は QoS ネットワークマーキングのための値リストコレクション作成者で使用されるポート範囲を最適化できます。この Quality of Service（QoS）設定がデフォルトで有効になっている場合、オーディオ、ビデオ、およびコンテンツ共有に使用されるソースポートがこのテーブルの値に変更されます。この設定では、UDP ポートの範囲に基づいた QoS マーキングポリシーを設定して、ビデオまたはコンテンツの共有の音声を区別し、推奨値 EF のすべての音声、推奨値 AF41 のビデオおよびコンテンツ共有にすることができます。

図 *3 : Video Mesh*のトラフィック署名（有効な*Quality of Service*（*QoS*））



表と図は、QoS ネットワーク構成の主要な焦点である、オーディオストリームとビデオストリームに使用される UDP ポートを示しています。UDP 経由のメディアに関するネットワーク QoS マーキングポリシーは、次の表に焦点をあてていますが、Webex Video Mesh ノードも、一時ポート 52500 ～ 65500 を使用して、Webex アプリのプレゼンテーションとコンテンツ共有用の TCP トラフィックを終了します。Video Mesh ノードと Webex アプリの間にファイアウォールが存在する場合、これらの TCP ポートも適切に機能するようにする必要があります。

（注） 値リストコレクション作成者は、トラフィックをネイティブにマークします。このネイティブマーキングは、一部のフローでは非対称であり、送信元ポートが共有ポート（さまざまな宛先と宛先ポートへの複数のフロー用の 5004 のような単一ポート）であるか、あるいは存在しない（ポートが範囲内にあるが、ポートが特定の双方向セッションに固有）かによって異なります。

値リストコレクション作成者でのネイティブのマーキングを理解するために、値リストコレクション作成者が、5004 ポートを送信元ポートとして使用していない場合、そのオーディオ EF がマークされる注意してください。Video Mesh から Video Mesh カスケードまたは Video Mesh から Webex アプリのような一部の双方向フローは、非対称的にマークされます。これは、ネットワークを使用する理由として、指定された UDP ポート範囲に基づいてトラフィックをリマークすることが挙げられます。

送信元 IP アドレス	宛先IPアドレス	送信元 UDP ポート	宛先 UDP ポート	ネイティブ DSCP マーキング	メディア タイプ

Video Mesh ノード	Webex クラウド メディア サービス	35000 ～ 52499	5004	AF41	Test STUN パケット
Video Mesh ノード	Webex クラウド メディア サービス	52500 ～ 59499	5004	EF	音声
Video Mesh ノード	Webex クラウド メディア サービス	63000 ～ 64667	5004	AF41	ビデオ
Video Mesh ノード	Webex クラウド メディア サービス	52500 ～ 62999	50000 ～ 51499	EF	音声
Video Mesh ノード	Webex クラウド メディア サービス	64668 ～ 65500	51500 ～ 53000	AF41	ビデオ
Video Mesh ノード	Video Mesh ノード	10000 ～ 40000	10000 ～ 40000	—	音声
Video Mesh ノード	Video Mesh ノード	10000 ～ 40000	10000 ～ 40000	—	ビデオ
Video Mesh ノード	Unified CM SIP エンドポイント	52500 ～ 59499	Unified CM SIP プロファイル	EF	音声
Video Mesh ノード	Unified CM SIP エンドポイント	63000 ～ 64667	Unified CM SIP プロファイル	AF41	ビデオ
Video Mesh クラスタ	Video Mesh クラスタ	52500 ～ 59499	5004	EF	音声
Video Mesh クラスタ	Video Mesh クラスタ	63000 ～ 64667	5004	AF41	ビデオ
Video Mesh クラスタ	Video Mesh クラスタ	52500 ～ 62999	50000 ～ 51499	EF	音声
Video Mesh クラスタ	Video Mesh クラスタ	64668 ～ 65500	51500 ～ 53000	AF41	ビデオ
Video Mesh ノード	Webex Teams アプリケーションまたはエンドポイント*	5004	52000 ～ 52099	AF41	音声

Video Mesh ノード	Webex Teams アプリケーションまたはエンドポイント	5004	52100 ～ 52299	AF41	ビデオ

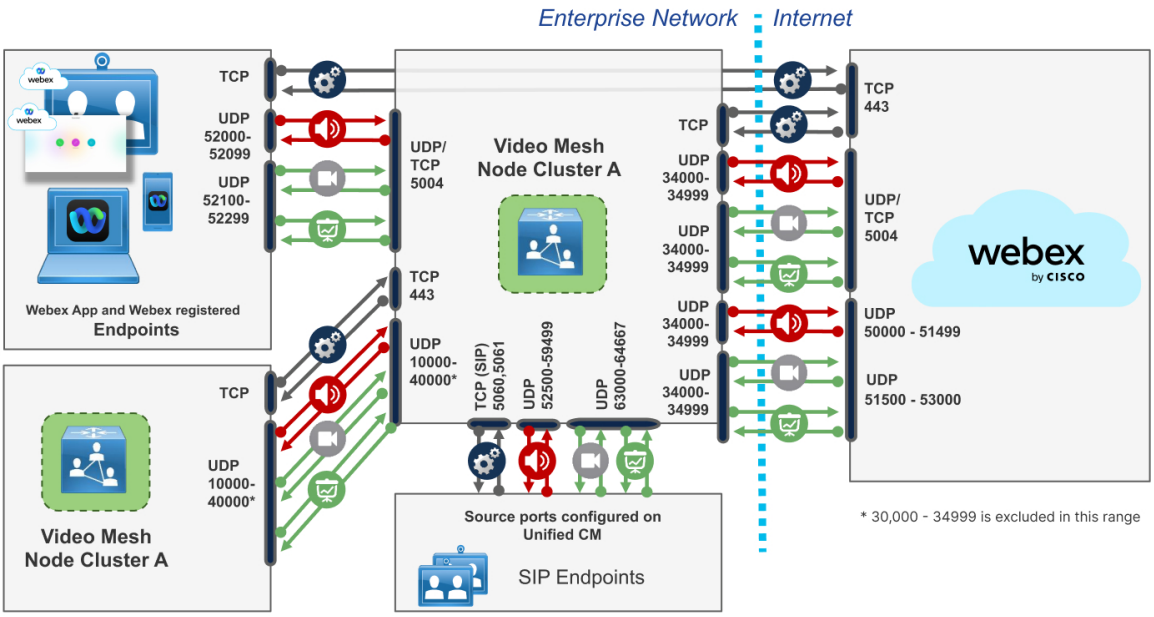
* メディアトラフィックの方向によって、DSCP マーキングが決定されます。送信元ポートが値リストコレクション作成者からのものである場合（値リストコレクション作成者から Webex Teams アプリまで）、トラフィックは AF41 のみでマークされます。Webex Teams アプリまたは Webex エンドポイントから送信されるメディアトラフィックには、個別の DSCP マーキングがありますが、値リストコレクション作成者の共有ポートからのリターントラフィックはありません。

（注） UDP Source Port Differentiation（Windows Webex アプリクライアント）：組織で UDP Source Port Differentiation を有効にする場合は、ローカルアカウントチームにお問い合わせください。これが有効になっていない場合、オーディオとビデオの共有を Windows OS で区別することはできません。送信元ポートは、Windows デバイスのオーディオ、ビデオ、およびコンテンツ共有で同じです。

Video Meshのトラフィック署名（無効なQuality of Service（QoS））

値リストコレクション作成者 が DMZ 内に配置されている導入では、値リストコレクション作成者が使用するポート範囲を最適化することが許可されている Webex Control Hub の値リストコレクション作成者構成の設定があります。Quality of Service 設定は、無効（デフォルトでは有効になっています）にした場合、オーディオ、ビデオ、およびコンテンツの共有に使用される送信元ポートを値リストコレクション作成者から 34000 ～ 34999の範囲に変更します。ビ値リストコレクション作成者は、すべての音声、ビデオ、およびコンテンツの共有を、ネイティブに 1 つの DSCP AF41 にマークします。

（注） 送信元ポートは、宛先に関係なくすべてのメディアに対して同じであるため、この設定が無効になっている場合は、ビデオまたはコンテンツ共有のオーディオをポート範囲に基づいて区別することはできません。この設定では、メディアのファイアウォール ピン ホールをより簡単に構成できるようにするため、Quality of Service（QoS）を向上させることができます。



表と図は、QoS が無効になっているときにオーディオおよびビデオストリームに使用される UDP ポートを示しています。

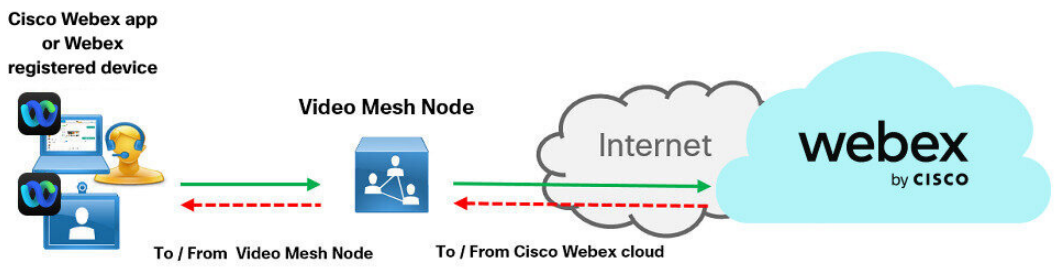
表 *8 : Video Meshのトラフィック署名（無効なQuality of Service（QoS））*

送信元 IP アドレス	宛先IPアドレス	送信元 UDP ポート	宛先 UDP ポート	ネイティブ DSCP マーキング	メディアタイプ
Video Mesh ノード	Webex クラウド メディア サービス	34000 ～ 34999	5004	AF41	音声
Video Mesh ノード	Webex クラウド メディア サービス	34000 ～ 34999	5004	AF41	ビデオ
Video Mesh ノード	Webex クラウド メディア サービス	34000 ～ 34999	50000 ～ 51499	AF41	音声
Video Mesh ノード	Webex クラウド メディア サービス	34000 ～ 34999	51500 ～ 53000	AF41	ビデオ
Video Mesh ノード	Video Mesh ノード	10000 ～ 40000	10000 ～ 40000	AF41	音声
Video Mesh ノード	Video Mesh ノード	10000 ～ 40000	10000 ～ 40000	AF41	ビデオ
Video Mesh クラスタ	Video Mesh クラスタ	34000 ～ 34999	5004	AF41	音声

Video Mesh クラスタ	Video Mesh クラスタ	34000 ～ 34999	5004	AF41	ビデオ
Video Mesh クラスタ	Video Mesh クラスタ	34000 ～ 34999	50000 ～ 51499	AF41	音声
Video Mesh クラスタ	Video Mesh クラスタ	34000 ～ 34999	51500 ～ 53000	AF41	ビデオ
Video Mesh ノード	Unified CM SIP エンドポイント	52500 ～ 59499	Unified CM SIP プロファイル	AF41	音声
Video Mesh ノード	Unified CM SIP エンドポイント	63000 ～ 64667	Unified CM SIP プロファイル	AF41	ビデオ
Video Mesh ノード	Webex クラウド メディア サービス	35000 ～ 52499	5004	AF41	Test STUN パケット
Video Mesh ノード	Webex Teams アプリケーションまたはエンドポイント	5004	52000 ～ 52099	AF41	音声
Video Mesh ノード	Webex Teams アプリケーションまたはエンドポイント	5004	52100 ～ 52299	AF41	ビデオ

Webex Meetings トラフィック用のポートとプロトコル

図 *4 : Webex* ミーティング用のポートとプロトコル



目的	送信元	送信先	送信元 IP	送信元ポート	トランスポート プロトコル	宛先 IP	宛先ポート
ミーティングへのコール	アプリ（Webex アプリ デスクトップおよびモバイル アプリ） Webex 登録済みデバイス	Video Meshノード	必要に応じて入力	すべて	UDP および TCP（Webex アプリで使用） SRTP（すべて）	すべて**	5004
ミーティングにコールする SIP デバイス（SIP シグナリング）	Unified CM または Cisco Expressway 呼制御	Video Meshノード	必要に応じて入力	エフェメラル（>=1024）	TCP または TLS	すべて**	5060 または 5061
カスケード	Video Meshノード	Webex クラウド	必要に応じて入力	34000 ～ 34999	UDP、SRTP（すべて）*	すべて**	5004 50000 ～ 53000***
カスケード	Video Meshノード	Video Meshノード	必要に応じて入力	34000 ～ 34999	UDP、SRTP（すべて）*	すべて**	5004

（注） ポート 5004 は、すべてのクラウドメディアとオンプレミスの Video Mesh ノードで使用されます。

Webex アプリ は、共有ポート 5004 経由で引き続き Video Mesh ノードに接続します。これらのポートは、Video Mesh ノードへの STUN テストのために、Webex アプリ と Webex で登録されたエンドポイントによっても使用されます。カスケードの Video Mesh ノードから Video Mesh ノードは、宛て先ポート範囲 10000 ～ 40000 を使用します。* TCP もサポートされますが、メディアの品質に影響を与えるために推奨されません。

** IP アドレスで制限する場合は、「Webex サービスのネットワーク要件」に記載されている IP アドレスの範囲を参照してください。

*** Expressway はすでに Webex クラウドにこのポート範囲を使用しています。したがって、ほとんどの展開では、Video Mesh のこの新しい要件に対応するための更新は必要ありません。ただし、展開にさらに厳しいファイアウォールルールがある場合は、ファイアウォール構成を更新して、Video Mesh 用にこれらのポートを開く必要がある場合があります。

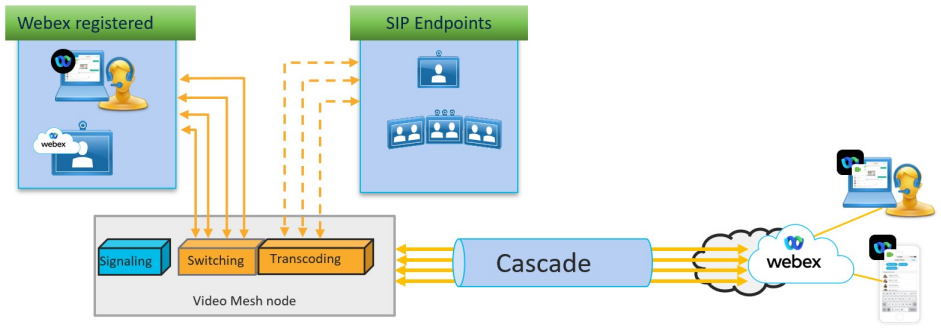
組織で Webex を使用する最適なエクスペリエンスを実現するために、ファイアウォールを設定して、ポート 5004 宛てのすべてのアウトバウンド TCP および UDP トラフィックと、そのトラフィックに対するすべてのインバウンド応答を許可します。上記のポート要件は、Video Mesh ノードが LAN（推奨）または DMZ に展開されていて、Webex アプリ が LAN 内にあることを前提としています。

Video Mesh のビデオ品質とスケーリング

以下は、カスケードが作成される場合における、いくつかの一般的なミーティングのシナリオです。利用可能な帯域幅に応じて Video Mesh が適応可能となり、それに応じてリソースを分散します。Video Mesh ノードを使用するミーティングのデバイスでは、カスケードリンクによって平均帯域幅を削減し、ユーザーのミーティングエクスペリエンスを改善できるという利点があります。

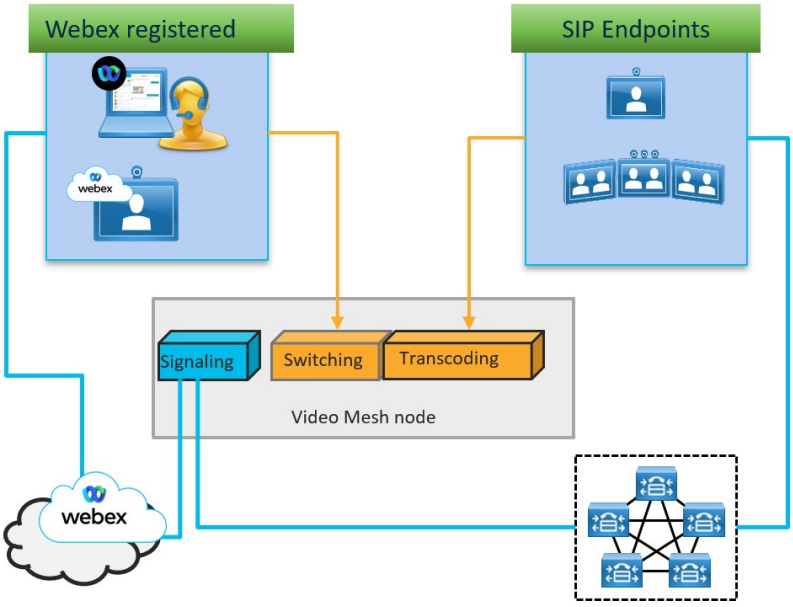
（注） 帯域幅のプロビジョニングとキャパシティの計画に関するガイドラインについては、『推奨アーキテクチャのドキュメント』を参照してください。

ミーティングでアクティブになっているスピーカーに基づいて、カスケードリンクが確立されます。各カスケードには最大 6 つのストリームを含めることができ、カスケードの参加者は 6 名に制限されます（Webex アプリ/SIP から Webex クラウドへの方向は 6 名、逆方向は 5 名）。各メディアリソース（クラウドと Video Mesh）は、カスケード全体におけるすべてのリモート参加者のローカルエンドポイントの要件を満たすのに必要なストリームをリモート側に要求します。



柔軟なユーザーエクスペリエンスを提供するために、Webex プラットフォームはミーティング参加者に対してマルチストリームビデオを実行できます。これと同じ機能は、Video Mesh ノードとクラウド間のカスケードリンクにも適用されます。このアーキテクチャでは、帯域幅の要件は、エンドポイントのレイアウトなど、さまざまな要因によって異なります。

アーキテクチャ



このアーキテクチャでは、Cisco Webex に登録されたエンドポイントがシグナリングをクラウドに送信し、メディアをスイッチングサービスに送信します。オンプレミスの SIP エンドポイントは、シグナリングを呼制御環境（Unified CM または Expressway）に送信します。その後、呼制御環境はシグナリングを Video Mesh ノードに送信します。メディアはトランスコーディング サービスに送信されます。

クラウドとオンプレミスの参加者

Video Mesh ノードにおけるオンプレミスのローカルの参加者は、レイアウトの要件に基づいて目的のストリームを要求します。これらのストリームは、ローカルデバイスレンダリングのために Video Mesh ノードからエンドポイントに転送されます。

各クラウドおよび Video Mesh ノードは、クラウドに登録されたデバイスまたは Webex アプリであるすべての参加者に HD および SD の解像度を要求します。エンドポイントに応じて、最大 4 つの解像度（通常は 1080p、720p、360p、および 180p）を送信します。

カスケード

ほとんどのシスコエンドポイントは、1 つの送信元から 3 つまたは 4 つのストリームを 1080p ～ 180p の解像度の範囲で送信できます。エンドポイントのレイアウトによって、カスケードの相手先で必要となるストリームの要件が決まります。アクティブプレゼンスの場合、メインのビデオストリームは 1080p または 720p、ビデオペイン（PiPS）は 180p です。等価ビューについては、ほとんどの場合、すべての参加者の解像度は 480p または 360p です。Video Mesh ノードとクラウド間に作成されたカスケードは、720p、360p、および 180p も両方向に送信し

ます。コンテンツは単一ストリームとして送信され、音声は複数のストリームとして送信されます。

クラスタ単位の測定を提供するカスケード帯域幅グラフは、Webex Control Hub の [分析（Analytics）] メニューで使用できます。Control Hub では、ミーティングごとにカスケードの帯域幅を設定することはできません。

（注） ミーティングごとにネゴシエートされたカスケードの最大帯域幅は、すべての送信元と送信できる複数のメインビデオストリームのメインビデオで 20 Mbps です。この最大値には、コンテンツチャネルや音声は含まれません。

複数のレイアウトを使用したメインビデオの例

次の図は、ミーティングのシナリオの例と、複数の要因が発生した場合に帯域幅に及ぶ影響を示しています。この例では、すべての Webex アプリおよび Webex に登録されているデバイスは、1x720p、1x360p、および 1x180p のストリームを Video Mesh に送信しています。カスケード上では、720p、360p、および 180p のストリームが両方向に送信されます。これは、カスケードの両側に 720p、360p、および 180p を受信している Webex アプリおよび Webex に登録されたデバイスがあるためです。

（注） 図では、データの送受信のための帯域幅の数値は、例示のみを目的としています。これらは、可能性のあるあらゆるミーティングとそれに伴う帯域幅の要件を網羅するものではありません。さまざまなミーティングシナリオ（参加者、デバイス機能、ミーティング内でのコンテンツ共有、ミーティング中の特定の時点におけるアクティビティ）により、帯域幅レベルは異なります。

図 *5:* ミーティング時に複数のレイアウトを使用するメインビデオ

この図は、クラウドおよびオンプレミスに登録されたエンドポイントとアクティブなスピーカーを使用するミーティングを示しています。

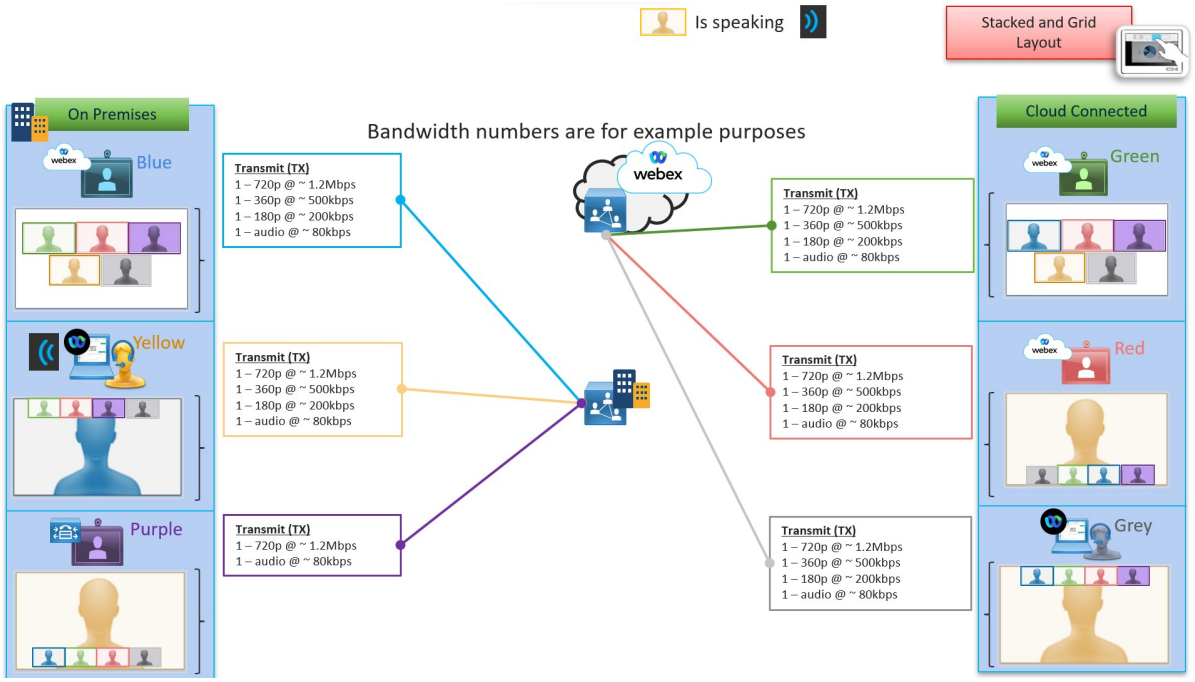


図 *6 : Video Mesh* ノードからクラウドへのカスケード

この図は、同じミーティングにおける、Video Mesh ノードとクラウド間で作成された両方向のカスケードの例を示しています。

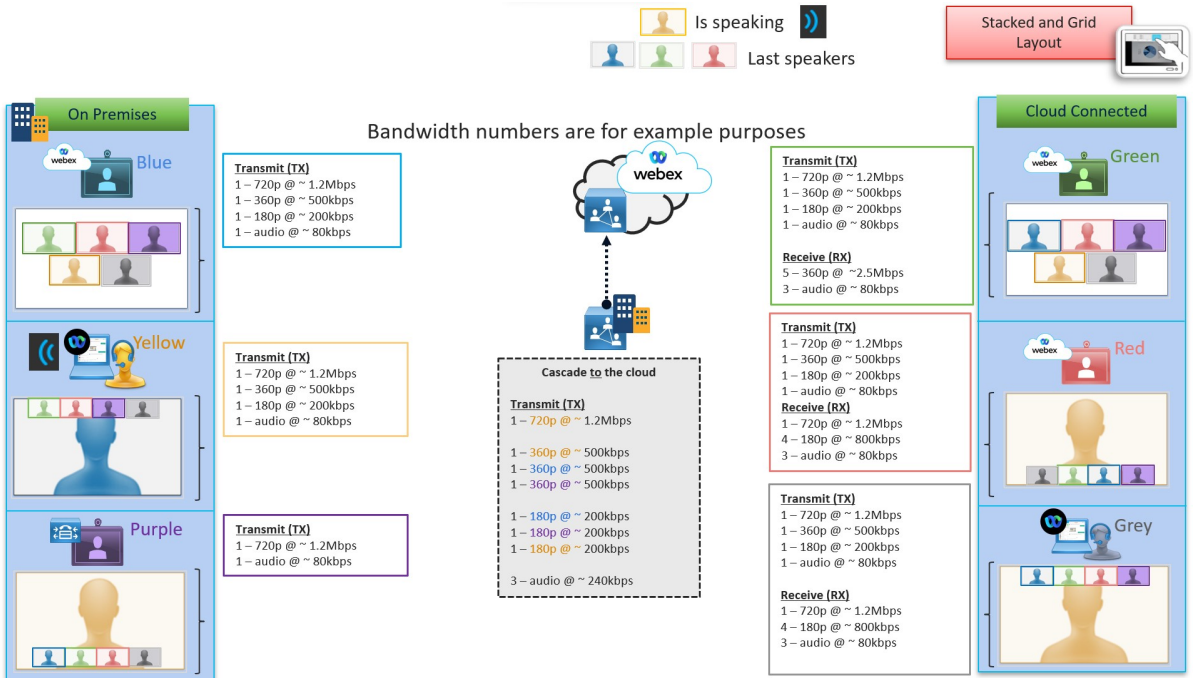


図 *7 :* クラウドからのカスケード

この図は、同じミーティングにおける、クラウドからのカスケードの例を示しています。

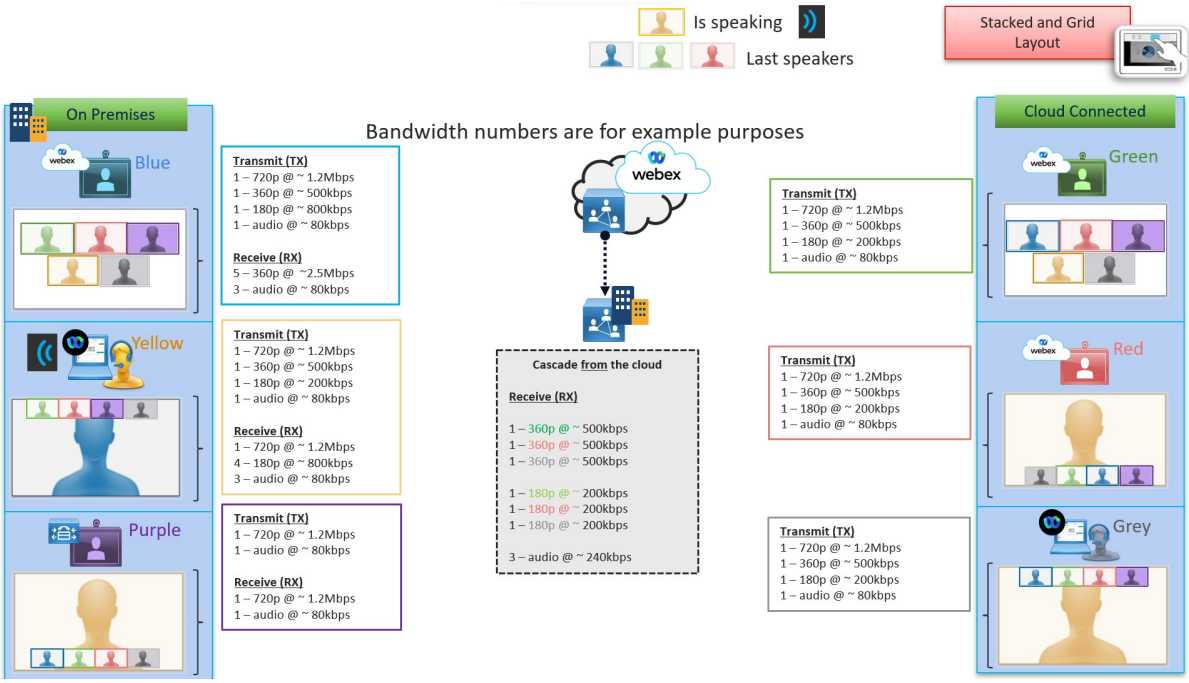
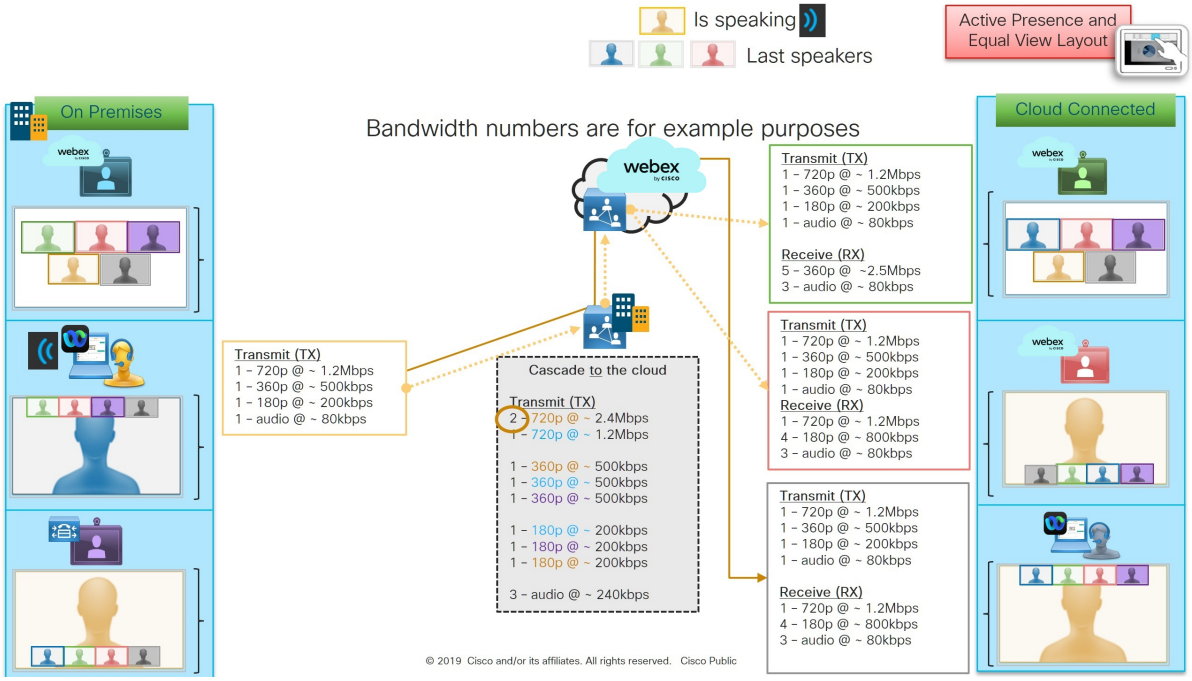


図 *8 : Webex Meetings* 参加者の追加

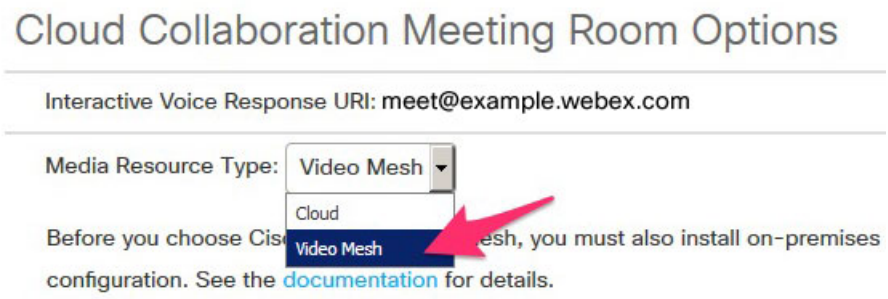
この図は、Webex Meetings クライアントと併せて、上記と同じデバイスを使用するミーティングを示しています。Video Mesh ノードは現時点で Webex Meetings をサポートしていないため、システムは、Webex Meeting クライアント用のアクティブスピーカーの追加 HD ストリームとともに、アクティブスピーカーと最後のアクティブスピーカーを高解像度で送信します。



Webex サービスの要件

パートナー、カスタマーサクセスマネージャ（CSM）、またはトライアル担当者と協力して、Cisco Webex サイトと Video Mesh に対する Webex サービスを適切にプロビジョニングします。

1. Webex サービスの有料サブスクリプションに登録している Webex 組織が必要です。
2. Video Mesh のすべてのメリットを利用するには、Webex サイトがビデオ プラットフォーム バージョン 2.0 上にあることを確認してください。（メディアリソースの種類リストが Cloud Collaboration Meeting Room サイトオプションにある場合、サイトがビデオ プラットフォーム バージョン 2.0 にあることを証明できます。）



3. ユーザープロファイルの下で、Webex サイトの CMR を有効にする必要があります。（この操作は、一括更新 CSV で SupportCMR 属性を使用して実行できます）。

詳細については、付録の「Collaboration Meeting Room Hybrid から Video Mesh への移行パスと機能比較 （184 ページ）」を参照してください。

関連トピック

カスタマー サクセス マネージャ（CSM）とどのように連絡が取れますか。

送信元の国が正しいことを確認する

Video Mesh は、Webex のグローバルに分散されたメディア（GDM）機能を使用して、より優れたメディアルーティングを実現します。最適な接続を実現するために、Webex は、Webex への Video Mesh カスケードを実行する際、企業に最も近いクラウドメディアノードを選択します。その後、トラフィックは Webex バックボーンを通過して、ミーティングの Webex マイクロサービスとやり取りします。このルーティングにより、遅延が最小限に抑えられ、ほとんどのトラフィックが Webex バックボーン上に維持されインターネットから離れた状態に保たれます。

GDM をサポートするために、このプロセスの GeoIP ロケーションプロバイダーとして MaxMind を使用します。効率的なルーティングを確保するために、MaxMind がパブリック IP アドレスの場所を正しく識別していることを確認します。

手順

ステップ 1 Web ブラウザで、Expressway またはエンドポイントのパブリック IP アドレスを最後に付けて、この URL を入力します。

例：

```
https://ds.ciscospark.com/v1/region/<public IP address>
```

次のような応答を受け取ります。

```
attribution: "This product includes GeoLite2 data created by MaxMind, available from
http://www.maxmind.com"
clientAddress: "<public IP address>"
clientRegion: "US-WEST"
countryCode: "US"
disclaimer: "This service is intended for use by Webex Team only. Unauthorized use is
prohibitted."
regionCode: "US-WEST"
timezone: "America/Chicago"
```

ステップ 2 `countryCode` が Expressway またはエンドポイントの場所に適していることを確認します。

ステップ 3 場所が正しくない場合は、パブリック IP アドレスの場所を修正するリクエストを MaxMind（https://support.maxmind.com/geoip-data-correction-request/correct-a-geoip-location）に送信します。

Video Mesh の前提条件の実行

次のチェックリストを使用して、Video Mesh ノードのインストールと設定および Webex サイトの Video Mesh との統合を行う準備が整っていることを確認します。

手順

ステップ 1 次のことを確認します。

- Video Mesh の要件 （9 ページ） に記載されている最小のシステム要件を満たし、「ハイブリッドサービスのライセンス要件」を満たします。
- Video Mesh ノードのキャパシティ （16 ページ） に記載されているコールキャパシティの例を理解します。
- Video Mesh でサポートされている展開モデル （28 ページ） で説明されているサポートされている導入モデルを理解します。
- ネットワークがポート上の接続を許可し、で説明されているプロトコルを使用していることを確認します。Video Mesh で使用されるポートとプロトコル （32 ページ）
- ネットワークが、で説明されている帯域幅要件をサポートしていることを確認します。Video Mesh のビデオ品質とスケーリング （42 ページ）

ステップ 2 パートナー、カスタマー サクセス マネージャ、またはトライアル担当者と協力して、Webex 環境を準備し、Video Mesh に接続できるようにします。詳細については、Webex サービスの要件 （47 ページ）を参照してください。

ステップ 3 Video Mesh ノードに割り当てる次のネットワーク情報を記録してください。

- IP アドレス（推奨）
- ネットワークマスク
- ゲートウェイIPアドレス
- DNS サーバー
- NTP サーバー
- Video Mesh ノードのホスト名、および必要に応じてドメイン名。（オプション）

（注） Video Mesh 用の IP アドレスを使用することを推奨します。FQDN を使用してノードを設定する場合は、FQDN 値が、ノード上に設定されている DNS サーバーリスト内のすべてのエントリを使用して解決可能である必要があります。また、DNS 設定では、正引き DNS と逆引き DNS の両方（A レコードと PTR レコード）を作成する必要もあります。

ステップ 4 インストールを開始する前に、Webex 組織が Video Mesh に対応していることを確認してください。このサービスは、「Cisco Webex ハイブリッドサービスのライセンス要件」に記載されている特定の有料 Webex サービスのサブスクリプションに登録している組織で使用できます。詳細については、シスコパートナーまたはアカウントマネージャにお問い合わせください。

ステップ 5 Video Mesh ノード ソフトウェアのシステム要件とプラットフォーム要件 （12 ページ） の説明に従って、Video Mesh ノードに対してサポートされているハードウェアまたは仕様に基づく構成を選択します。

ステップ 6 サーバーでVMware ESXi 6.5、6.7、7、およびvSphere 6.5、6.7、7が稼動し、VMホストが動作していることを確認します。

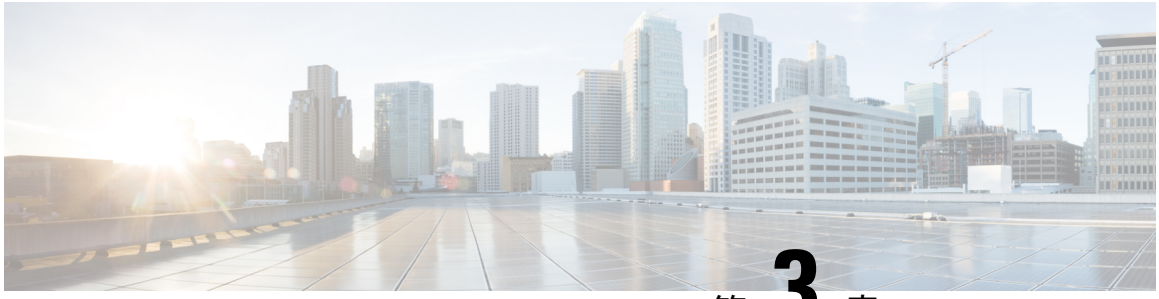
ステップ 7 Video Mesh を Unified CM 呼制御環境に統合し、ミーティングプラットフォーム全体で参加者リストを一貫性のあるものにする場合は、Unified CM クラスタセキュリティモードが混合モードに設定され、TLS で暗号化されたトラフィックがサポートされるようにします。この機能を動作させるには、エンドツーエンドの暗号化トラフィックが必要です。

Unified CM 環境を混合モードに切り替える方法の詳細については、『Cisco Unified Communications Manager セキュリティガイド』の「TLS セットアップ」の章を参照してください。機能の詳細およびエンドツーエンドの暗号化のセットアップ方法については、『Active Control ソリューションガイド』を参照してください。

ステップ 8 プロキシ（明示的、透過的な検査、または透過非検査）を Video Mesh と統合する場合は、「Video Mesh のプロキシサポートの要件 （15 ページ）」に記載されている要件に従う必要があります。

次のタスク

Video Mesh ノード ソフトウェアのインストールと設定 （55 ページ）



第 3 章

Video Mesh の導入

Video Mesh 導入タスクのフロー

始める前に

環境の準備 （9 ページ）

手順

	コマンドまたはアクション	目的
ステップ 1	Video Mesh ノード ソフトウェアのインストールと設定 （55 ページ）	VMware ESXi または vCenter を実行しているホストサーバーに Video Mesh ノードを展開するには、次の手順に従います。ソフトウェアをオンプレミスでインストールするとノードが作成されます。その後、ネットワーク設定などの初期設定を実行します。それを後からクラウドに登録します。
ステップ 2	Video Mesh ノード コンソールへのログイン （59 ページ）	コンソールに初回サインインします。Video Mesh ノード ソフトウェアには、デフォルトのパスワードが設定されています。ノードを設定する前に、この値を変更する必要があります。
ステップ 3	コンソールでの Video Mesh ノードのネットワーク構成の設定 （60 ページ）	仮想マシン上のノードのセットアップ時に設定しなかった場合に、Video Mesh ノードのネットワーク設定を構成するには、この手順を使用します。静的 IP アドレスを設定し、FQDN/ホスト名と NTP サーバーを変更します。DHCP は現在サポートされていません。
ステップ 4	デュアルネットワークインターフェイス（デュアル NIC）展開用に外部インターフェイスを設定するには、次の手順を使用します。 • Video Mesh ノードの外部ネットワークインターフェイスの設定 （62 ページ） • 内部ルーティングルールと外部ルーティングルールを追加する （82 ページ）	ノードがオンラインに戻り、内部ネットワーク構成を確認した後、ネットワークの DMZ 内で Video Mesh ノードを展開している場合は、外部ネットワークインターフェイスを設定して、企業（内部）トラフィックを外部トラフィックから分離することができます。 また、例外を作成したり、デフォルトのルーティングルールに上書きしたりすることもできます。
ステップ 5	Webex クラウドへの Video Mesh ノードの登録 （83 ページ）	次の手順を使用して、Video Mesh ノードを Webex クラウドに登録し、追加の構成を完了します。ノードの登録に Control Hub を使用する場合は、ノードを割り当てるクラスタを作成します。クラスタには 1 つまたは複数のメディアノードがあり、それぞれ特定の地理的地域のユーザーが利用します。登録

	コマンドまたはアクション	目的
		手順では、SIP コール設定の構成、アップグレードスケジュールの設定、および電子メール通知の登録も行います。
ステップ 6	次のタスクを使用して Quality of Service（QoS）の有効化と検証を行います。 • Video Mesh ノード の Quality of Service（QoS）の有効化 （88 ページ） • ウェブインターフェイスのリフレクタツールを使用した Video Mesh ノードのポート範囲の確認 （89 ページ）	適切なサービスクラスおよび特定のメディアタイプに対する既知のポート範囲で、Video Mesh ノードが、オーディオ（EF）およびビデオ（AF41）の両方に対して個別に自動で SIP トラフィック（オンプレミス SIP 登録済みエンドポイント）をマークする場合は、QoS を有効にします。この変更により、QoS ポリシーを作成し、必要に応じてクラウドからのリターントラフィックを効果的に注釈できます。 リフレクタツールの手順を使用して、ファイアウォール上で適切なポートが開かれていることを確認します。
ステップ 7	プロキシ統合のための Video Mesh ノードの構成 （91 ページ）	Video Mesh と統合するプロキシのタイプを指定するには、次の手順を使用します。透過的なプロキシを選択した場合、ノードのインターフェイスを使用してルート証明書をアップロードおよびインストールし、プロキシを確認し、考え得る問題をトラブルシュートします。
ステップ 8	呼制御タスクフローと Video Mesh の統合 （93 ページ） に従って、呼制御、セキュリティ要件、および Video Mesh を呼制御環境と統合するかどうかに応じて、次のいずれかを選択します。 • Unified CM セキュア TLS SIP トラフィックルーティングの設定 - Video Mesh （96 ページ） （TLS） • Video Mesh 用の Unified CM TCP SIP トラフィックルーティングの設定 （100 ページ） （TCP） • Video Mesh 用の Expressway TCP SIP トラフィックルーティングの設定 （105 ページ） （TCP）	SIP デバイスは、直接到達可能性をサポートしないため、Unified CM または VCS Expressway 構成を使用して、オンプレミス登録 SIP デバイスおよび Video Mesh クラスタ間の関連性を確立する必要があります。 必要なのは、呼制御環境に応じて、Unified CM または VCS Expressway を Video Mesh ノードにトランクすることだけです。

	コマンドまたはアクション	目的
ステップ 9	Unified CM と Video Mesh ノード間での証明書チェーンの交換 （108 ページ）	このタスクでは、Unified CM および Video Mesh インターフェイスから証明書をダウンロード し、1 つを他方にアップロードします。この手順では、2 つの製品間で安全な信頼を確立し、セキュアトランクの構成と併用することで、組織内の暗号化された SIP トラフィックおよびSRTP メディアが Video Mesh ノードに定着できるようにします。
ステップ 10	組織およびVideo Meshクラスタのメディア暗号化の有効化 （111 ページ）	組織および個々のVideo Mesh クラスタのメディア暗号化をオンにする場合は、次の手順を実行します。この設定では、エンドツーエンドの TLS セットアップが強制的に実行され、Video Mesh ノードをポイントするセキュアな TLS SIP トランクが Unified CM に配置されている必要があります。
ステップ 11	Webex サイトの Video Mesh の有効化（112 ページ）	Webex ミーティングの Video Mesh ノードに最適化されたメディアを使用して、すべての Webex アプリとデバイスに参加するには、この設定を Webex サイトで有効にする必要があります。この設定を有効化することによって、クラウドで Video Mesh およびミーティングインスタンスが一緒にリンクされ、カスケードが Video Mesh ノードで発生できるようになります。この設定が有効になっていない場合、Webex アプリとデバイスは Webex ミーティングに Video Mesh ノードを使用しません。
ステップ 12	Webex アプリ ユーザーへの Collaboration Meeting Rooms の割り当て（113 ページ）	
ステップ 13	セキュアなエンドポイントでのミーティングエクスペリエンスの確認 （114 ページ）	エンドツーエンドの TLS セットアップでメディア暗号化を使用する場合は、次の手順を使用して、エンドポイントが安全に登録され、正しいミーティングエクスペリエンスが表示されていることを確認します。

Video Mesh の一括プロビジョニングスクリプト

Video Mesh 展開で多くのノードを展開する必要がある場合、プロセスには時間がかかります。https://github.com/CiscoDevNet/webex-video-mesh-node-provisioning にあるこのスクリプトを使用して、VMWare ESXi サーバーに Video Mesh ノードをすばやく展開できます。スクリプトの使用方法については、readme ファイルを参照してください。

Video Mesh ノード ソフトウェアのインストールと設定

VMware ESXi または vCenter を実行しているホストサーバーに Video Mesh ノード を展開するには、次の手順に従います。ソフトウェアをオンプレミスでインストールするとノードが作成されます。その後、ネットワーク設定などの初期設定を実行します。それを後からクラウドに登録します。

前にダウンロードしたバージョンを使用するのではなく、Control Hub（https://admin.webex.com）からソフトウェアパッケージ（OVA）をダウンロードする必要があります。この OVA は Cisco 証明書によって署名されており、カスタマー管理者のログイン情報を使用して Control Hub にサインインした後にダウンロードできます。

始める前に

- サポートされているハードウェアプラットフォームおよび Video Mesh ノード の仕様要件については、「Video Mesh ノード ソフトウェアのシステム要件とプラットフォーム要件（12 ページ）」を参照してください。
- 次のものを用意します。
  - 以下を備えたコンピュータ
    - VMware vSphere クライアント 6.5、6.7、または 7。

      サポートされているオペレーティングシステムの一覧は、VMware のドキュメントを参照してください。
    - Video Mesh のダウンロードされたソフトウェア OVA ファイル。

      前にダウンロードしたバージョンを使用するのではなく、Control Hub から最新の Video Mesh ソフトウェアをダウンロードします。また、このリンクからソフトウェアにアクセスすることもできます。（ファイルは約 1.5 GB です。）

（注） ソフトウェアパッケージ（OVA）の古いバージョンは、最新の Video Mesh アップグレードと互換性がありません。これにより、アプリケーションのアップグレード中に問題が発生する可能性があります。必ずこのリンクから OVA の最新バージョンをダウンロードしてください。

- VMware ESXi または vCenter 6.5、6.7、または 7 をインストールして実行しているサポート対象サーバー
- 仮想マシンのバックアップとライブマイグレーションを無効にします。Video Mesh ノードクラスタはリアルタイムシステムです。仮想マシンの一時停止によって、これらのシステムが不安定になる可能性があります。（Video Mesh ノード でメンテナンス作業を実行する場合は、Control Hub のメンテナンス モードを使用します）。

手順

ステップ 1 お使いのコンピュータから、VMware vSphere クライアントを開き、サーバー上の vCenter または ESXi システムにサインインします。

ステップ 2 **[アクション（Actions）] > [OVF テンプレートの展開（Deploy OVF Template）]** に移動します。

ステップ 3 **[OVF テンプレートの選択（Select an OVF template）]** ページで、**[ローカルファイル（Local File）]** をクリックし、**[ファイルを選択（Choose Files）]** をクリックします。**videomesh.ova** ファイルがある場所に移動し、ファイルを選択して **[次へ（Next）]** をクリックします。

注意 Video Mesh ノード のインストールを実行するたびに、前にダウンロードしたバージョンを使用するのではなく、OVA を再ダウンロードすることをお勧めします。古い OVA を展開しようとすると、Video Mesh ノード は正常に動作しないか、クラウドに登録できない場合があります。古い OVA も、アップグレード中に潜在的な問題につながります。

必ずこのリンクから OVA の新しいコピーをダウンロードしてください。

ステップ 4 **[名前とフォルダの選択（Select a name and folder）]** ページで、Video Mesh ノード の **[仮想マシン名（Virtual machine name）]**を入力し（たとえば、「Video_Mesh_Node_1」）、仮想マシンノードの展開先となる場所を選択して、**[次へ（Next）]** をクリックします。

検証チェックが実行されます。完了すると、テンプレートの詳細が表示されます。

ステップ 5 テンプレートの詳細を確認して、[次へ（Next）]をクリックします。

ステップ 6 **[設定（Configuration）]** ページで、展開設定の種類を選択し、**[次へ（Next）]** をクリックします。

- VMNLite（デフォルト）
- CMS 1000

オプションは、リソース要件の増加順にリストされています。

（注） VMNLite オプションを選択した場合は、手順を繰り返して同じホスト上で他のインスタンスを展開し、その度に同じオプションを選択する必要があります。VMNLite インスタンスと非 VMNLite インスタンスの共存はテストされておらず、サポートされていません。

ステップ 7 **[ストレージの選択（Select storage）]** ページで、デフォルトのディスク形式である **[シックプロビジョニング（Lazy Zeroed）（Thick Provision Lazy Zeroed）]** と **[データストアのデフォルト（Datastore Default）]** の VM ストレージポリシーが選択されていることを確認してから、**[次へ（Next）]** をクリックします。

ステップ 8 [ネットワークの選択（Select network）] ページで、VM に必要な接続を提供するエントリの一覧からネットワークを選択します。

- **[内部インターフェイスネットワーク（Internal Interface Network）]** については、ノードの内部 IP アドレスを選択します。
- **外部 InterfaceNetwork** の場合は、パブリックネットワークに接している外部 IP アドレスを選択します。デュアル NIC 展開を使用しない場合は、このオプションを無視します。

（注） 内部インターフェイス（トラフィックのデフォルトインターフェイス）は、CLI、SIP トランク、SIP トラフィック、およびノード管理に使用されます。外部（external）インターフェイスは、ノードからミーティングへのカスケードトラフィックとともに、HTTPS および WebSocket が Webex クラウドと通信するためのものです。

DMZ 展開の場合は、デュアル ネットワーク インターフェイス（NIC）を使用して Video Mesh ノードをセットアップできます。この導入によって、エンタープライズネットワークトラフィックを（インターボックス通信、ノードクラスタ間のカスケード、ノードの管理インターフェイスへのアクセスに使用される）外部のクラウド ネットワーク トラフィック（外部への接続に使用され、Webex にカスケード）から分離することができます。クラスタ内のすべてのノードがデュアル NIC モードになっている必要があります。シングル NIC とデュアル NIC の混在はサポートされていません。

（注） Video Mesh ノード ソフトウェアの既存のインストールでは、単一の NIC からデュアル NIC の構成にアップグレードすることはできません。この場合は、Video Mesh ノード の新規インストールを実行する必要があります。

ステップ 9 [テンプレートのカスタマイズ（Customize template）]ページで、次のネットワーク設定を行います。

- [**ホスト名（hostname**）]（オプション）：ノードの FQDN（ホスト名とドメイン）または 1 つの単語のホスト名を入力します。

  （注）
  - クラウドに問題なく登録できるように、Video Mesh ノード に設定する FQDN またはホスト名には小文字のみを使用してください。現時点では、大文字と小文字はサポートされていません。
  - FQDN またはホスト名を使用または設定する場合は、有効で解決可能なドメインを入力する必要があります。FQDN の長さは、64 文字以下にする必要があります。

- **IP アドレス**：ノードの内部インターフェイスの IP アドレスを入力します。
- **マスク**：ドット区切りの 10 進表記でサブネットを入力します。たとえば、*255.255.255.0* と入力します。

- **ゲートウェイ**：ゲートウェイの IP アドレスを入力します。ゲートウェイは、他のネットワークへの入口として機能するネットワーク ノードを表します。
- **][DNS サーバー（DNS Servers）**：ドメイン名を数値 IP アドレスに変換する処理を行う DNS サーバーのカンマ区切りのリストを入力します。（最大 4 つの DNS エントリが許可されます）。
- **[NTP サーバー（NTP Servers）]**：組織の NTP サーバまたは組織で使用可能な別の外部 NTP サーバーを入力します。また、カンマ区切りリストを使用して複数の NTP サーバーを入力することもできます。
- Video Mesh ノードは、内部 IP アドレスと解決可能な DNS 名を持っている必要があります。ノード IP アドレスは、Video Mesh ノード内部使用のために予約されている IP アドレスの範囲に属していてはなりません。デフォルトの予約済み IP アドレスの範囲は 172.17.42.0 ～ 172.17.42.63 で、後で **[診断（Diagnostic）]** メニューで設定できます。この IP アドレスの範囲は、Video Mesh ノード内、およびノードのさまざまなコンポーネント（SIP インターフェイスやメディアトランスコーディングなど）を保持するソフトウェアコンテナ間における通信のためのものです。
- すべてのノードを同じサブネットまたは VLAN に展開します。これにより、クラスタ内のすべてのノードは、ネットワーク内のクライアントのどこからでも到達可能になります。
- デュアル NIC DMZ を展開する場合は、後で、内部ネットワーク構成を保存してノードをリブートした後、ノードコンソールで外部 IP アドレスを設定することができます。

必要に応じて、ネットワーク設定の構成をスキップして、ノードにサインインした後の「コンソールでの Video Mesh ノード のネットワーク構成の設定 （60 ページ）」の手順に従うことができます。

ステップ 10 **[準備完了（Ready to Complete）]**ページで、入力したすべての設定がこの手順のガイドラインと一致していることを確認してから **[完了（Finish）]** をクリックします。

OVA の導入が完了すると、VM のリストに Video Mesh ノード が表示されます。

ステップ 11 Video Mesh ノード VM を右クリックし、**[電源（Power）] > [電源をオン（Power On）]** の順に選択します。

Video Mesh ノード ソフトウェアは、VM ホストでゲストとしてインストールされます。これで、コンソールにサインインして Video Mesh ノード を設定する準備が整いました。

トラブルシューティングのヒント

ノードコンテナが起動するまでに、数分の遅延が発生する可能性があります。最初の起動時にコンソールにブリッジファイアウォールのメッセージが表示されます。このとき、サインインはできません。

次のタスク

Video Mesh ノード コンソールへのログイン （59 ページ）

Video Mesh ノード コンソールへのログイン

コンソールに初回サインインします。Video Mesh ノード ソフトウェアには、デフォルトのパスワードが設定されています。ノードを設定する前に、この値を変更する必要があります。

手順

ステップ 1 VMware vSphere クライアントから、Video Mesh ノード VM に移動 して、**[コンソール（Console）]** を選択し ます。

Video Mesh ノード VM が起動し、ログインプロンプトが表示されます。ログインプロンプトが表示されない場合は、**Enter** キーを押します。システムの初期化が行われていることを示す簡単なメッセージが表示される可能性があります。

ステップ 2 次のデフォルトのユーザー名とパスワードを使用して、ログインします。

a) ログイン：**admin**

b) パスワード：**cisco**

Video Mesh ノード への初回ログインであるため、管理者のパスフレーズ（パスワード）を変更する必要があります。

ステップ 3 （現在の）パスワードとして、デフォルトのパスワード（上記）を入力し、**Enter** キーを押します。

ステップ 4 [新しいパスワード（New password）]に新しいパスフレーズを入力し、**Enter** キーを押します。

ステップ 5 新しいパスワードを再入力するように求められたら、新しいパスフレーズを再入力し、**Enter** キーを押します。

「パスワードを正常に変更できました」というメッセージが表示され、最初の Video Mesh ノード 画面に、不正アクセスが禁止されたことを通知するメッセージが表示されます。

ステップ 6 **Enter** キーを押してメインメニューをロードします。

次のタスク

コンソールでの Video Mesh ノード のネットワーク構成の設定 （60 ページ）

コンソールでの Video Mesh ノードのネットワーク構成の設定

仮想マシン上のノードのセットアップ時に設定しなかった場合に、Video Mesh ノードのネットワーク設定を構成するには、この手順を使用します。静的 IP アドレスを設定し、FQDN/ホスト名と NTP サーバーを変更します。DHCP は現在サポートされていません。

OVA の展開時にネットワーク設定を構成しなかった場合、これらの手順は必須です。

（注） 内部インターフェイス（トラフィックのデフォルトインターフェイス）は、CLI、SIP トランク、SIP トラフィック、およびノード管理に使用されます。外の（外部）インターフェイスは、ノードから Webex へのカスケードトラフィックとともに、HTTPS および WebSocket が Webex クラウドと通信するためのものです。

手順

ステップ 1 VMware vSphere クライアントを通じてノードコンソールのインターフェイスを開き、管理者のログイン情報を使用してサインインします。

初めてネットワーク設定をセットアップした後、Video Meshが到達可能である場合は、セキュアシェル（SSH）を通じてノードインターフェイスにアクセスできます。

ステップ 2 Video Mesh ノードコンソールのメインメニューで、**[2 構成の編集（2 Edit Configuration）]** のオプションを選択し、**[選択（Select）]** をクリックします。

ステップ 3 Video Mesh ノードでのコールの終了を求めるプロンプトを読み、**[はい（Yes）]** をクリックします。

ステップ 4 **[静的（Static）]** をクリックして、内部インターフェイスの **[IP アドレス（IP address）]**、ネットワークの、**[マスク（Mask）]**、**[ゲートウェイ（Gateway）]**、**[DNS]** の各値を入力します。

- Video Mesh ノードは、内部 IP アドレスと解決可能な DNS 名を持っている必要があります。ノード IP アドレスは、Video Mesh ノード内部使用のために予約されている IP アドレスの範囲に属していてはなりません。デフォルトの予約済み IP アドレスの範囲は 172.17.42.0 ～ 172.17.42.63 で、**[診断（Diagnostic）]** メニューで設定できます。この IP アドレスの範囲は、Video Mesh ノード内、およびノードのさまざまなコンポーネント（SIP インターフェイスやメディアトランスコーディングなど）を保持するソフトウェアコンテナ間における通信のためのものです。
- すべてのノードを同じサブネットまたは VLAN に展開します。これにより、クラスタ内のすべてのノードは、ネットワーク内のクライアントのどこからでも到達可能になります。

- デュアル NIC DMZ を導入する場合は、内部ネットワーク構成を保存してノードをリブートした後、次の手順で外部 IP アドレスを設定することができます。

ステップ 5 組織の NTP サーバーまたは組織で使用可能な別の外部 NTP サーバーを入力します。

NTP サーバーを設定し、ネットワーク設定を保存した後は、「コンソールからの Video Mesh ノードの正常性チェック （179 ページ）」の手順に従って、指定された NTP サーバーを介して時刻が正しく同期されていることを確認できます。

（注） 複数の NTP サーバーを設定する場合、フェールオーバーのポーリング間隔は 40 秒です。

ステップ 6 （オプション）必要に応じて、ホスト名またはドメインを変更します。

（注）
- クラウドに問題なく登録できるように、Video Mesh ノード に設定するホスト名は小文字のみを使用します。現時点では、大文字と小文字はサポートされていません。
- FQDN またはホスト名を使用または設定する場合は、有効で解決可能なドメインを入力する必要があります。FQDN の長さは、64 文字以下にする必要があります。

ステップ 7 **[保存（Save）]** をクリックし、**[変更を保存して再起動（Save Changes & Reboot）]** の順に選択します。

ドメインを指定した場合は、保存中に DNS の検証が行われます。指定された DNS サーバーアドレスを使用して FQDN（ホスト名とドメイン）を解決できない場合、警告が表示されます。警告を無視して保存を選択できますが、ノードに設定されている DNS で FQDN を解決できるまで、コールは機能しません。Video Mesh ノード リブート後、ネットワーク構成の変更が有効になります。

次のタスク

ネットワーク設定（IP アドレス、DNS、NTP など）でソフトウェアイメージをインストール、構成し、エンタープライズネットワークでアクセス可能にすると、その次の手順に移行して、セキュリティで保護されているクラウドに登録することができます。Video Mesh ノード に設定されている IP アドレスに は、エンタープライズネットワークからのみアクセスできます。セキュリティの観点からは、ノードは、カスタマーの管理者だけがノードインターフェイスにアクセスして構成を実行できるようになっています。

Video Mesh ノード の外部ネットワークインターフェイスの設定 （62 ページ）

Video Mesh ノードの外部ネットワークインターフェイスの設定

ノードがオンラインに戻り、内部ネットワーク構成を確認した後、ネットワークの DMZ 内で Video Mesh ノードを展開している場合は、外部ネットワーク インターフェイスを設定して、企業（内部）トラフィックを外部トラフィックから分離することができます。

手順

ステップ 1 Video Mesh ノード コンソールのメインメニュー で、**[5 外部 IP 構成（5 External IP Configuration）]** のオプションを選択し、**[選択（Select）]** をクリックします。

ステップ 2 **[1 有効化/無効化（1 Enable/Disable）]**、**[選択（Select）]** の順に選択したら、**[はい（Yes）]** を選択して、ノードで外部 IP アドレスオプションを有効化します。

ステップ 3 初期ネットワーク構成で行ったように、**[IP アドレス（IP Address）]**（外部）、**[マスク（Mask）]**、および **[ゲートウェイ（Gateway）]** の値を入力します。

（注） **[インターフェイス（Interface）]** フィールドには、ノードの外部インターフェイスの名前が表示されます。

ステップ 4 **[保存して再起動（Save and restart）]** をクリックします。

デュアル IP アドレスを有効にするためノードを再度リブートすると、基本的な静的ルーティングルールが自動的に設定されます。これらのルールは、プライベートクラス IP アドレス間のトラフィックが、内部インターフェイスを使用することを決定します。パブリッククラスの IP アドレス間のトラフィックには、外部インターフェイスが使用されます。後で、独自のルーティングルールを作成することができます。たとえば、内部インターフェイスからの上書きを設定し、外部ドメインへのアクセスを許可する必要がある場合などです。

（注） 特定の状況においては、既存の SSH 接続が終了する場合があります。パブリック範囲の IP アドレスを使用する組織の場合、Video Mesh ノードのパブリック IP アドレスへの SSH 接続を再確立する必要があります。

ステップ 5 内部 IP アドレスと外部 IP アドレス設定を確認するには、コンソールのメインメニューから **[4 診断（4 Diagnostics）]** に移動し て、**[Ping]** を選択し ます。

ステップ 6 **[Ping]** フィールドに、外部の宛先または内部 IP アドレスなどテストする宛先アドレスを入力し、**[OK]** をクリックします。

- cisco.com などの外部宛先をテストします。成功した場合は、外部インターフェイスから宛先にアクセスしたことが結果に示されます。
- 内部 IP アドレスをテストします。成功した場合は、内部インターフェイスからアドレスにアクセスされたことが結果に示されます。

次のタスク

Webex クラウドへの Video Mesh ノードの登録 （83 ページ）

Video Mesh ノード API

Video Mesh ノード API を使用すると、組織管理者は、Video Mesh ノードに関連するパスワード、内部および外部ネットワーク設定、メンテナンスモード、およびサーバー証明書を管理できます。これらの API は、Postman などの API ツールを介して呼び出すことも、独自のスクリプトを作成して呼び出すこともできます。ユーザーは、以下に示す情報に従って、適切なエンドポイント（ノード IP または FQDN のいずれかを使用できます）、メソッド、本文、ヘッダー、承認などを使用して API を呼び出し、希望するアクションを実行し、適切なレスポンスを取得する必要があります。

VMN 管理 API

Video Mesh 管理 API を使用すると、組織管理者はVideo Mesh ノードのメンテナンスモードと管理者アカウントパスワードを管理できます。

メンテナンスモードのステータスを受け取る

現在のメンテナンスモードのステータスを取得します（予期されるステータス：オン、オフ、保留中、またはリクエスト済み）。

[GET] https://<node_ip> /api/v1/external/maintenanceMode

許可：Video Mesh のユーザー名（「admin」）とパスワードを使用する基本認証。

サンプルレスポンス：

サンプルレスポンス 1：

```
{
    "status": {
        "code": 200,
        "message": "Success"
    },
    "result": {
        "isRegistered": true,
        "maintenanceMode": "pending/requested/on/off",
        "maintenanceModeLastUpdated": 1691135731847
    }
}
```

サンプルレスポンス 2：

```
{
    "status": {
        "code": 401,
        "message": "login failed: incorrect password or username"
    }
}
```

サンプルレスポンス 3：

```
{
    "status": {
        "code": 429,
        "message": "Too Many Requests"
    }
}
```

メンテナンスモードを有効または無効にする

Video Mesh ノードをメンテナンスモードにすると、コールサービスのグレースフルシャットダウンを実行します（新しいコールの受け入れを停止し、既存のコールが完了するまで最大2時間待機します）。

[PUT] https://<node_ip> /api/v1/external/maintenanceMode

（注） アクティブなコールがない場合にのみ、この API を呼び出します。

許可：Video Mesh のユーザー名（「admin」）とパスワードを使用する基本認証。

本文：

```
{
      "maintenanceMode": "on"
}
```

- maintenanceMode：設定するメンテナンスモードのステータス（「on」または「off」）。

リクエストヘッダー：

「コンテンツ タイプ」：「application/json」

サンプルレスポンス：

サンプルレスポンス 1：

```
{
        "status": {
            "code": 200,
           "message": "Your request to enable/disable maintenance mode was successful."

    }
}
```

サンプルレスポンス 2：

```
{
      "status": {
          "code": 409,
          "message": "Maintenance Mode is already on/off"
    }
}
```

サンプルレスポンス 3：

```
{
      "status": {
          "code": 400,
          "message": "Bad Request - wrong input"
```

```
    }
}
```

admin パスワードを変更する

管理者ユーザーのパスワードを変更します。

[PUT] https://<node_ip> /api/v1/external/password

許可：Video Mesh のユーザー名（「admin」）とパスワードを使用する基本認証。

本文：

```
{
  "newPassword": "new"
}
```

- newPassword：Video Mesh ノードの「admin」アカウントに設定する新しいパスワード。

リクエストヘッダー：

「コンテンツ タイプ」：「application/json」

サンプルレスポンス：

サンプルレスポンス 1：

```
{
    "status": {
        "code": 200,
        "message": "Successfully set the new passphrase for user admin."
    }
}
```

サンプルレスポンス 2：

```
{
    "status": {
        "code": 400,
        "message": "Enter a new passphrase that wasn't used for one of the previous 3
passphrases."
    }
}
```

VMN ネットワーク API

Video Mesh ネットワーク API を使用すると、組織管理者は内部および外部のネットワーク設定を管理できます。

外部ネットワーク設定を取得する

外部ネットワークが有効か無効かを検出します。外部ネットワークが有効になっている場合は、外部 IP アドレス、外部サブネットマスク、および外部ゲートウェイも取得します。

[GET] https://<node_ip> /api/v1/external/externalNetwork

許可：Video Mesh のユーザー名（「admin」）とパスワードを使用する基本認証。

サンプルレスポンス：

サンプルレスポンス 1：

```
{
    "status": {
        "code": 200,
        "message": "Successfully fetched external network configuration."
    },
    "result": {
        "ip": "1.1.1.1",
        "mask": "2.2.2.2",
        "gateway": "3.3.3.3"
    }
}
```

サンプルレスポンス 2：

```
{
    "status": {
        "code": 200,
        "message": "External network not enabled."
    }
}
```

サンプルレスポンス 3：

```
{
    "status": {
        "code": 500,
        "message": "Failed to get external network configuration."
    }
}
```

外部ネットワーク設定を編集する

外部ネットワークの設定を変更します。このAPIを使用して、外部IPアドレス、外部サブネットマスク、および外部ゲートウェイを使用して外部ネットワークインターフェイスを設定または編集するとともに、外部ネットワークを有効にすることができます。また、外部ネットワークを無効にするためにも使用できます。外部ネットワーク設定を変更すると、ノードが再起動して変更が適用されます。

[PUT] https://<node_ip> /api/v1/external/externalNetwork

（注） これは、デフォルトの管理者パスワードが変更された、新しく展開された Video Mesh ノードに対してのみ設定できます。ノードを組織に登録した後は、この API を使用しないでください。

許可：Video Mesh のユーザー名（「admin」）とパスワードを使用する基本認証。

本文：

外部ネットワークの有効化：

```
{
  "externalNetworkEnabled": true,
  "externalIp": "1.1.1.1",
  "externalMask": "2.2.2.2",
```

```
  "externalGateway": "3.3.3.3"
}
```

外部ネットワークの無効化：

```
{
  "externalNetworkEnabled": false
}
```

- externalNetworkEnabled：外部ネットワークを有効または無効にするブール値（true または false）
- externalIp：追加する外部 IP
- externalMask：外部ネットワークのネットマスク
- externalGateway：外部ネットワークのゲートウェイ

リクエストヘッダー：

「コンテンツ タイプ」：「application/json」

サンプルレスポンス：

サンプルレスポンス 1：

```
{
    "status": {
        "code": 200,
        "message": "Successfully saved the external network configuration. This node
will reboot soon to apply the changes. Please wait for a minute and relogin to the node
 to verify that all changes were applied."
    }
}
```

サンプルレスポンス 2：

```
{
    "status": {
        "code": 200,
        "message": "Successfully disabled the external network. This node will reboot
soon to apply the changes. Please wait for a minute and relogin to the node to verify
that all changes were applied."
    }
}
```

サンプルレスポンス 3：

```
{
    "status": {
        "code": 400,
        "message": "One or more errors in the input: Value should be boolean for
'externalNetworkEnabled'"
    }
}
```

サンプルレスポンス 4：

```
{
    "status": {
        "code": 400,
       "message": "External network configuration has not changed; skipping save of the
 external network configuration."
```

```
    }
}
```

内部ネットワークの詳細を取得する

ネットワークモード、IPアドレス、サブネットマスク、ゲートウェイ、DNSキャッシングの詳細、DNSサーバー、NTPサーバー、内部インターフェイスMTU、ホスト名、ドメインを含む内部ネットワーク設定の詳細を取得します。

[GET] https://<node_ip> /api/v1/external/internalNetwork

許可：Video Mesh のユーザー名（「admin」）とパスワードを使用する基本認証。

サンプルレスポンス：

サンプルレスポンス 1：

```
{
    "status": {
        "code": 200,
        "message": "Successfully fetched internal network details"
    },
    "result": {
        "dhcp": false,
        "ip": "1.1.1.1",
        "mask": "2.2.2.2",
        "gateway": "3.3.3.3",
        "dnsCaching": false,
        "dnsServers": [
            "4.4.4.4",
            "5.5.5.5"
        ],
        "mtu": 1500,
        "ntpServers": [
            "6.6.6.6"
        ],
        "hostName": "test-vmn",
        "domain": ""
    }
}
```

サンプルレスポンス 2：

```
{
      "status": {
          "code": 500,
          "message": "Failed to get Network details."
    }
}
```

サンプルレスポンス 3：

```
{
      "status": {
          "code": 500,
          "message": "Failed to get host details."
    }
}
```

DNS サーバーを編集する

新しい DNS サーバーで DNS サーバーを更新します。

[PUT] https://<node_ip> /api/v1/external/internalNetwork/dns

（注） この変更を行う前に、ノードをメンテナンスモードにします。ノードをメンテナンスモードに移行する方法の詳細については、「メンテナンスモードを有効または無効にする （64 ページ）」を参照してください。

許可：Video Mesh のユーザー名（「admin」）とパスワードを使用する基本認証。

本文：

```
{
    "dnsServers": "1.1.1.1 2.2.2.2"
}
```

- dnsServers：更新する DNS サーバー。スペースで区切られた複数の DNS サーバーを使用できます。

リクエストヘッダー：

「コンテンツ タイプ」：「application/json」

サンプルレスポンス：

サンプルレスポンス 1：

```
{
    "status": {
        "code": 200,
        "message": "Successfully saved DNS servers"
    }
}
```

サンプルレスポンス 2：

```
{
    "status": {
        "code": 409,
        "message": "Requested DNS server(s) already exist."
    }
}
```

サンプルレスポンス 3：

```
{
    "status": {
        "code": 424,
        "message": "Maintenance Mode is not enabled. Kindly enable Maintenance Mode and
 try again for this node."
    }
}
```

NTP サーバーを編集する

NTP サーバーを新しいサーバーで更新します。

[PUT] https://<node_ip> /api/v1/external/internalNetwork/ntp

（注） この変更を行う前に、ノードをメンテナンスモードにします。ノードをメンテナンスモードに移行する方法の詳細については、「メンテナンスモードを有効または無効にする （64 ページ）」を参照してください。

許可：Video Mesh のユーザー名（「admin」）とパスワードを使用する基本認証。

本文：

```
{
    "ntpServers": "1.1.1.1 2.2.2.2"
}
```

- ntpServers：更新する NTP サーバー。スペースで区切られた複数の NTP サーバーを使用できます。

リクエストヘッダー：

「コンテンツ タイプ」：「application/json」

サンプルレスポンス：

サンプルレスポンス 1：

```
{
    "status": {
        "code": 200,
        "message": "Successfully saved the NTP servers."
    }
}
```

サンプルレスポンス 2：

```
{
    "status": {
        "code": 409,
        "message": "Requested NTP server(s) already exist."
    }
}
```

サンプルレスポンス 3：

```
{
    "status": {
        "code": 424,
        "message": "Maintenance Mode is not enabled. Kindly enable Maintenance Mode and
 try again for this node."
    }
}
```

ホスト名とドメインを編集する

Video Mesh ノードのホスト名とドメインを更新します。

[PUT] https://<node_ip> /api/v1/external/internalNetwork/host

（注） この変更を行う前に、ノードをメンテナンスモードにします。ノードが再起動し、変更が適用されます。ノードをメンテナンスモードに移行する方法の詳細については、「メンテナンスモードを有効または無効にする （64 ページ）」を参照してください。

許可：Video Mesh のユーザー名（「admin」）とパスワードを使用する基本認証。

本文：

```
{
    "hostName": "test-vmn",
    "domain": "abc.com"
}
```

- hostName：ノードの新しいホスト名。
- domain：ノードのホスト名の新しいドメイン（オプション）。

リクエストヘッダー：

「コンテンツ タイプ」：「application/json」

サンプルレスポンス：

サンプルレスポンス 1：

```
{
    "status": {
        "code": 200,
       "message": "Successfully saved the host FQDN. This node will reboot soon to apply
 the changes. Please wait for a minute and relogin to the node to verify that all changes
 were applied."
    }
}
```

サンプルレスポンス 2：

```
{
    "status": {
        "code": 400,
        "message": "Unable to resolve FQDN"
    }
}
```

サンプルレスポンス 3：

```
{
    "status": {
        "code": 409,
        "message": "Entered hostname and domain already set to same."
    }
}
```

DNS キャッシングを有効または無効にする

DNS キャッシングの有効または無効にします。DNS チェックの解決に 750 ミリ秒以上かかることが多い場合、またはシスコサポートで推奨されている場合は、キャッシングを有効にすることを検討してください。

[PUT] https://<node_ip> /api/v1/external/internalNetwork/dnsCaching

（注） この変更を行う前に、ノードをメンテナンスモードにします。ノードが再起動し、変更が適用されます。ノードをメンテナンスモードに移行する方法の詳細については、「メンテナンスモードを有効または無効にする （64 ページ）」を参照してください。

許可：Video Mesh のユーザー名（「admin」）とパスワードを使用する基本認証。

本文：

```
{
    "dnsCaching": true
}
```

- dnsCaching：DNS キャッシング設定。ブール値（true または false）を受け入れます。

リクエストヘッダー：

「コンテンツ タイプ」：「application/json」

サンプルレスポンス：

サンプルレスポンス 1：

```
{
    "status": {
        "code": 200,
        "message": "Successfully saved DNS settings changes. This node will reboot soon
 to apply the changes. Please wait for a minute and relogin to the node to verify that
all changes were applied."
    }
}
```

サンプルレスポンス 2：

```
{
    "status": {
        "code": 400,
        "message": "One or more errors in the input: 'dnsCaching' field value should be
 a boolean"
    }
}
```

サンプルレスポンス 3：

```
{
    "status": {
        "code": 409,
        "message": "dnsCaching is already set to false"
    }
}
```

インターフェイス MTU を編集する

ノードのネットワーク インターフェイスの最大伝送ユニット（MTU）をデフォルト値の 1500 から変更します。1280 ～ 9000 の値を使用できます。

[PUT] https://<node_ip> /api/v1/external/internalNetwork/mtu

（注） この変更を行う前に、ノードをメンテナンスモードにします。ノードが再起動し、変更が適用されます。ノードをメンテナンスモードに移行する方法の詳細については、「メンテナンスモードを有効または無効にする （64 ページ）」を参照してください。

許可：Video Mesh のユーザー名（「admin」）とパスワードを使用する基本認証。

本文：

```
{
    "internalInterfaceMtu": 1500
}
```

- internalInterfaceMtu：ノードのネットワーク インターフェイスの最大伝送ユニット。値は 1280 ～ 9000 である必要があります。

リクエストヘッダー：

「コンテンツ タイプ」：「application/json」

サンプルレスポンス：

サンプルレスポンス 1：

```
{
    "status": {
        "code": 200,
        "message": "Successfully saved the internal interface MTU settings. This node
will reboot soon to apply the changes. Please wait for a minute and relogin to the node
 to verify that all changes were applied."
    }
}
```

サンプルレスポンス 2：

```
{
    "status": {
        "code": 400,
        "message": "One or more errors in the input: 'internalInterfaceMtu' field value
 should be a number"
    }
}
```

サンプルレスポンス 3：

```
{
    "status": {
        "code": 400,
        "message": "Please enter a number between 1280 and 9000."
    }
}
```

VMN サーバー証明書 API

Video Mesh サーバー証明書 API を使用すると、組織管理者は Video Mesh ノードに関連する証明書を作成、更新、ダウンロード、および削除できます。詳細については、「Unified CM と Video Mesh ノード間での証明書チェーンの交換 （108 ページ）」を参照してください。

CSR 証明書を作成する

指定された詳細に基づいて、CSR（証明書署名要求）証明書と秘密キーを生成します。

[POST] https://<node_ip> /api/v1/externalCertManager/generateCsr

許可：Video Mesh のユーザー名（「admin」）とパスワードを使用する基本認証。

本文：

```
{
    "csrInfo":
    {
         "commonName": "1.2.3.4",
         "emailAddress": "abc@xyz.com",
         "altNames": "1.1.1.1 2.2.2.2",
         "organization": "VMN",
         "organizationUnit": "IT",
         "locality": "BLR",
         "state": "KA",
         "country": "IN",
         "passphrase": "",
         "keyBitSize": 2048
    }
}
```

- commonName：共通名として指定された Video Mesh ノードの IP/FQDN。（必須）
- emailAddress：ユーザーの電子メールアドレス。（オプション）。
- altNames：サブジェクト代替名（オプション）。複数のスペースで区切られた FQDN を使用できます。指定する場合は、共通名を含める必要があります。altNames が指定されていない場合は、altNames の値として commonName を使用します。
- organization：組織/会社の名前。（オプション）。
- organizationUnit：組織単位、部署、グループ名など（任意）
- locality：市区町村。（オプション）。
- state：州/都道府県。（オプション）。
- country：国/地域。2 文字の略語。2 文字を超えて入力しないでください。（オプション）。
- passphrase：秘密キーのパスフレーズ。（オプション）。
- keyBitSize：秘密キーのビットサイズ。許容値は、デフォルトの 2048 または 4096 です。（オプション）。

リクエストヘッダー：

「コンテンツ タイプ」：「application/json」

サンプルレスポンス：

サンプルレスポンス 1：


```
{
    "status": {
        "code": 200,
        "message": "Successfully generated CSR"
    },
    "result": {
        "caCert": {},
        "caKey": {
            "fileName": "VideoMeshGeneratedPrivate.key",
            "localFileName": "CaPrivateKey.key",
            "fileLastModified": "Fri Jul 21 2023 08:12:25 GMT+0000 (Coordinated
Universal Time)",
            "uploadDate": 1689927145422,
            "size": 1678,
            "type": "application/pkcs8",
            "modulus": "S4MP1EM0DULU2"
        },
        "certInstallRequestPending": false,
        "certInstallStarted": null,
        "certInstallCompleted": null,
        "isRegistered": true,
        "caCertsInstalled": false,
        "csr": {
            "keyBitsize": 2048,
            "commonName": "1.2.3.4",
            "organization": "VMN",
            "organizationUnit": "IT",
            "locality": "BLR",
            "state": "KA",
            "country": "IN",
            "emailAddress": "abc@xyz.com",
            "altNames": [
                "1.1.1.1",
                "2.2.2.2"
            ],
            "csrContent": "-----BEGIN CERTIFICATE
REQUEST-----\nS4MP1E_C3RT_C0NT3NT\n-----END CERTIFICATE REQUEST-----"
        },
        "encryptedPassphrase": null
    }
}
```


サンプルレスポンス 2：


```
{
    "status": {
        "code": 400,
        "message": "Private key already exists. Delete it before generating new CSR."

    }
}
```


サンプルレスポンス 3：

```
{
    "status": {
        "code": 400,
        "message": "CSR certificate already exists. Delete it before generating new
CSR."
    }
}
```

サンプルレスポンス 4：

```
{
    "status": {
        "code": 400,
        "message": "CSR certificate and private key already exist. Delete them before
 generating new CSR."
    }
}
```

サンプルレスポンス 5：

```
{
    "status": {
        "code": 400,
        "message": "There were one or more errors while generating the CSR: The
\"Country\" field must contain exactly two A-Z characters."
    }
}
```

CSR 証明書をダウンロードする

生成された CSR 証明書をダウンロードします。

[GET] https://<node_ip> /api/v1/externalCertManager/csr

[送信とダウンロード（Send and Download）] オプションを使用してファイルをダウンロードすることもできます。

許可：Video Mesh のユーザー名（「admin」）とパスワードを使用する基本認証。

サンプルレスポンス：

サンプルレスポンス 1：

```
-----BEGIN CERTIFICATE REQUEST-----
S4MP1E_C3RT_C0NT3NT
-----END CERTIFICATE REQUEST-----
```

サンプルレスポンス 2：

```
{
    "status": {
        "code": 404,
        "message": "Could not download, CSR certificate does not exist."
    }
}
```

秘密キーをダウンロードする

CSR 証明書とともに生成された秘密キーをダウンロードします。

[GET] https://<node_ip> /api/v1/externalCertManager/key

[送信とダウンロード（Send and Download）] オプションを使用してファイルをダウンロードすることもできます。

許可：Video Mesh のユーザー名（「admin」）とパスワードを使用する基本認証。

サンプルレスポンス：

サンプルレスポンス 1：

```
-----BEGIN RSA PRIVATE KEY-----
S4MP1E_PR1V4T3_K3Y
-----END RSA PRIVATE KEY-----
```

サンプルレスポンス 2：

```
{
    "status": {
        "code": 404,
        "message": "Could not download, private key does not exist."
    }
}
```

CSR 証明書を削除する

既存の CSR 証明書を削除します。

[DELETE] https://<node_ip> /api/v1/externalCertManager/csr

許可：Video Mesh のユーザー名（「admin」）とパスワードを使用する基本認証。

サンプルレスポンス：

サンプルレスポンス 1：

```
{
    "status": {
        "code": 200,
        "message": "Successfully deleted the CSR certificate"
    }
}
```

サンプルレスポンス 2：

```
{
    "status": {
        "code": 404,
        "message": "CSR certificate does not exist."
    }
}
```

秘密キーを削除する

既存の秘密キーを削除します。

[DELETE] https://<node_ip> /api/v1/externalCertManager/key

許可：Video Mesh のユーザー名（「admin」）とパスワードを使用する基本認証。

サンプルレスポンス：

サンプルレスポンス 1：

```
{
    "status": {
        "code": 200,
        "message": "Successfully deleted the private key"
    }
}
```

サンプルレスポンス 2：

```
{
    "status": {
        "code": 404,
        "message": "Private key does not exist."
    }
}
```

CA 署名付き証明書と秘密キーをインストールする

提供された CA 署名付き証明書と秘密キーを Video Mesh ノードにアップロードし、ノードに証明書をインストールします。

[POST] https://<node_ip> /api/v1/externalCertManager/uploadInstallCaCert

許可：Video Mesh のユーザー名（「admin」）とパスワードを使用する基本認証。

本文：

「form-data」を使用して、次のファイルをアップロードします。

- 「crtFile」というキーを持つ CA 署名付き証明書（.crt）ファイル。
- 「keyFile」というキーを持つ秘密キー（.key）ファイル。

リクエストヘッダー：

Content-Type：「multipart/form-data」

サンプルレスポンス：

サンプルレスポンス 1：

```
{
    "status": {
        "code": 200,
        "message": "Successfully installed certificate and key. It might take a few
seconds to reflect on the node."
```

```
},
"result": {
    "caCert": {
        "fileName": "videoMeshCsr.crt",
        "localFileName": "CaCert.crt",
        "fileLastModified": 1689931788598,
        "uploadDate": 1689931788605,
        "size": 1549,
        "type": "application/x-x509-ca-cert",
        "certStats": {
            "version": 0,
            "subject": {
                "countryName": "IN",
                "stateOrProvinceName": "KA",
                "localityName": "BLR",
                "organizationName": "VMN",
                "organizationalUnitName": "IT",
                "emailAddress": "abc@xyz.com",
                "commonName": "1.2.3.4"
            },
            "issuer": {
                "countryName": "AU",
                "stateOrProvinceName": "Some-State",
                "organizationName": "ABC"
            },
            "serial": "3X4MPL3",
            "notBefore": "2023-07-21T09:28:19.000Z",
            "notAfter": "2024-12-02T09:28:19.000Z",
            "signatureAlgorithm": "sha256WithRsaEncryption",
            "fingerPrint": "11:22:33:44:AA:BB:CC:DD",
            "publicKey": {
                "algorithm": "rsaEncryption",
                "e": 65537,
                "n": "3X4MPL3",
                "bitSize": 2048
            },
            "altNames": [],
            "extensions": {}
        }
    },
    "caKey": {
        "fileName": "VideoMeshGeneratedPrivate.key",
        "localFileName": "CaPrivateKey.key",
        "fileLastModified": 1689931788629,
        "uploadDate": 1689931788642,
        "size": 1678,
        "type": "application/pkcs8",
        "modulus": "S4MP1EM0DULU2"
    },
    "certInstallRequestPending": true,
    "certInstallStarted": null,
    "certInstallCompleted": null,
    "isRegistered": true,
    "caCertsInstalled": false,
    "csr": {
        "keyBitsize": 2048,
        "commonName": "1.2.3.4",
        "organization": "VMN",
        "organizationUnit": "IT",
        "locality": "BLR",
        "state": "KA",
        "country": "IN",
        "emailAddress": "abc@xyz.com",
```

```
            "altNames": [
                "1.1.1.1",
                "2.2.2.2"
            ],
            "csrContent": "-----BEGIN CERTIFICATE
REQUEST-----\nS4MP1E_C3RT_C0NT3NT\n-----END CERTIFICATE REQUEST-----"
        },
        "encryptedPassphrase": null
    }
}
```

サンプルレスポンス 2：

```
{
    "status": {
        "code": 400,
        "message": "Could not parse the certificate file. Make sure it is a properly
 formatted certificate and try again."
    }
}
```

サンプルレスポンス 3：

```
{
    "status": {
        "code": 400,
        "message": "Private Key does not match Certificate (different modulus)"
    }
}
```

サンプルレスポンス 4：

```
{
    "status": {
        "code": 202,
        "message": "Certificate and private key PENDING installation. It might take
a few seconds to reflect on the node. If the node is in maintenance mode, it will get
 installed once it is disabled."
    }
}
```

CA 署名付き証明書をダウンロードする

ノードにインストールされている CA 署名付き証明書をダウンロードします。

[GET] https://<node_ip> /api/v1/externalCertManager/caCert

[送信とダウンロード（Send and Download）] オプションを使用してファイルをダウンロードすることもできます。

許可：Video Mesh のユーザー名（「admin」）とパスワードを使用する基本認証。

サンプルレスポンス：

サンプルレスポンス 1：

```
-----BEGIN CERTIFICATE-----
S4MP1E_C3RT_C0NT3NT
-----END CERTIFICATE-----
```

サンプルレスポンス 2：

```
{
    "status": {
        "code": 404,
        "message": "Could not download, CA certificate does not exist."
    }
}
```

CA 署名付き証明書を削除する

ノードにインストールされている CA 署名付き証明書を削除します。

[DELETE] https://<node_ip> /api/v1/externalCertManager/caCert

許可：Video Mesh のユーザー名（「admin」）とパスワードを使用する基本認証。

サンプルレスポンス：

サンプルレスポンス 1：

```
{
    "status": {
        "code": 200,
        "message": "Successfully deleted the CA certificate."
    }
}
```

サンプルレスポンス 2：

```
{
    "status": {
        "code": 404,
        "message": "CA certificate does not exist."
    }
}
```

共通 API レスポンス

上記の API のいずれかを使用しているときに発生する可能性のあるレスポンスの例を以下に示します。

レスポンス例 1：基本認証で提供されたログイン情報が正しくありません。

```
{
    "status": {
        "code": 401,
        "message": "login failed: incorrect password or username"
    }
}
```

レスポンス例 2：VMN は、これらの API をサポートする必要なバージョンにアップグレードされていません。

```
{
    "status": {
        "code": 421,
        "message": "Misdirected Request 1:[undefined]"
    }
}
```

レスポンス例 3：ヘッダーに誤ったリファラーが入力されました（ヘッダーが予期されなかった場合）。

```
{
    "status": {
        "code": 421,
        "message": "Misdirected Request 2:[https://x.x.x.x/setup]"
    }
}
```

レスポンス例 4：レート制限を超えています。しばらくしてから再試行してください。

```
{
    "status": {
        "code": 429,
        "message": "Too Many Requests"
    }
}
```

内部ルーティングルールと外部ルーティングルールを追加する

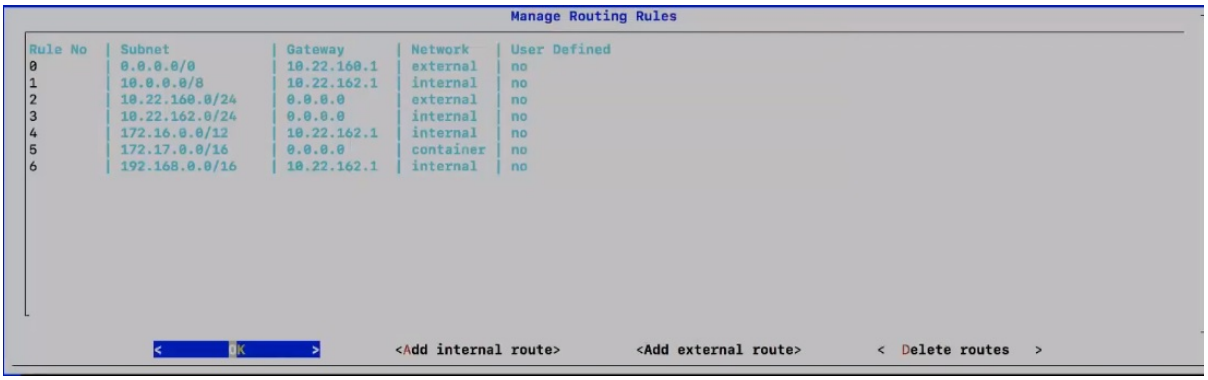
デュアルネットワークインターフェイス（NIC）の展開では、外部インターフェイスと内部インターフェイスのユーザー定義ルートルールを追加することによって、値リストコレクション作成者のルーティングを微調整することができます。デフォルトルートはノードに追加されますが、たとえば、外部サブネットまたは内部インターフェイスを介してアクセスする必要があるホストアドレス、あるいは外部インターフェイスからアクセスする必要がある内部サブネットまたはホストアドレスなど、例外を作成することができます。必要に応じて、次の手順を実行します。

手順

ステップ 1 値リストコレクション作成者インターフェイスから **[5 外部 IP 構成（5 External IP Configuration）]** を選択し、**[選択（Select）]** をクリックします。

ステップ 2 **[3 ルーティングルールの管理（3 Manage Routing Rules）]** を選択し、**[選択（Select）]** をクリックします。

このページを初めて開いたときは、デフォルトのシステムルーティングルールがリストに表示されます。デフォルトでは、すべての内部トラフィックは内部インターフェイスを通過し、外部トラフィックは外部インターフェイスを通過します。



これらのルールに手動オーバーライドを追加するには、次の手順を実行します。

ステップ 3 必要に応じて次の手順を実行します。

- **[外部ルートの追加（Add external route）]** をクリックして、外部ルートに使用する内部サブネットまたはホスト IP アドレスを入力します。
- **[内部ルートの追加（Add internal route）]** をクリックして、内部ルートに使用する内部サブネットまたはホスト IP アドレスを入力します。

各ルールを追加すると、そのルールはルーティングルールの一覧に表示され、ユーザー定義ルールとして分類されます。

（注） デフォルトルートを削除することはできませんが、設定した任意のユーザー定義オーバーライドを削除することはできます。

⚠

注意 カスタムルーティングルールは、他のルーティングと競合する可能性があります。たとえば、Video Mesh ノード インターフェイスへの SSH 接続をフリーズするルールを定義できます。このような場合は、次のいずれかを実行して、ルーティングルールを削除または変更します。

- Video Mesh ノード のパブリック IP アドレスへの SSH 接続を開きます。
- ESXi コンソールからの Video Mesh ノード へのアクセス

Webex クラウドへの Video Mesh ノードの登録

次の手順を使用して、Video Mesh ノードを Webex クラウドに登録し、追加の構成を完了します。ノードの登録に Control Hub を使用する場合は、ノードを割り当てるクラスタを作成します。クラスタには1つまたは複数のメディアノードがあり、それぞれ特定の地理的地域のユーザーが利用します。登録手順では、SIP コール設定の構成、アップグレードスケジュールの設定、および電子メール通知の登録も行います。

Before you begin

- ノードの登録を開始したら、60 分以内に登録を完了する必要があります。そうでないと、最初からやり直さなければなりません。
- ブラウザ内のポップアップブロックが無効になっていないか、または https://admin.webex.com の例外を許可しているかどうかを確認します。
- できるだけ問題が生じないように、クラスタのすべてのノードを同じデータセンターに展開します。ノードの動作とベストプラクティスについては、「Video Mesh のクラスタ , on page 18」を参照してください。
- Video Mesh ノードをクラウドに登録するホストまたはマシンから、Webex クラウドと登録される Video Mesh IP アドレスに接続できる必要があります（デュアル NIC 環境内（特に Video Mesh ノードの内部 IP アドレスを含む））。

Procedure

ステップ 1 [Control Hub] にサインインします。

管理者のログイン情報を使用して Control Hub にサインインします。Control Hub 管理者機能は、Control Hub で管理者として定義されているユーザーのみが使用できます。詳細については、「顧客アカウントの役割」を参照してください。

ステップ 2 **[サービス（Services）]** > **[ハイブリッド（Hybrid）]** に移動し、次のいずれかを選択します。

- **セットアップ（Set up）**：これが登録する最初の Video Mesh ノード である場合は、このオプションを選択し、**[次へ（Next）]** をクリックします。

  Note 詳細については、「Video Mesh の前提条件の実行, on page 48」を参照してください。

- **すべて表示（View all）**：すでに 1 つ以上の Video Mesh ノード を登録している場合は、このオプションを選択し、**[リソースの追加（Add Resource）]** をクリックします。

ステップ 3 Video Mesh ノード をインストールして設定していることを確認します。**[はい、登録する準備ができています（Yes, I'm ready to register...）]** をクリックし、**[次へ（Next）]** をクリックします。

ステップ 4 **[新規作成（Create a new）]** または **[クラスタの選択（select a cluster）]** で以下のいずれかを選択します。

- 新しいクラスタの場合は、Video Mesh ノードを割り当てるクラスタの名前を入力します。
- 既存のクラスタの場合は、フィールドをクリックして、新しいノードを追加する既存のクラスタを選択します。

Note クラスタには、クラスタのノードの地理的な配置場所に応じた名前を付けることを推奨します。たとえば、「San Francisco」と入力します。

ステップ 5 **[FQDN] または [IP アドレス（IP addres）]** で、Video Mesh ノードの完全修飾ドメイン名（FQDN）または内部 IP アドレスを入力して、**[次へ（Next）]** をクリックします。

- FQDN を使用する場合は、DNS によって解決できるドメインを入力します。
- IP アドレスを使用する場合は、コンソールからノードを設定するために使用したのと同じ内部 IP アドレスを入力します。

FQDN は、IP アドレスに対して直接解決する必要があります。FQDN の検証を実行して、入力ミスや一致しない構成を除外します。

Note デュアル ネットワーク インターフェイスでは、外部 IP アドレスの FQDN の指定がサポートされていません。FQDN は、内部 IP アドレスが入力されている画面でのみ追加できます。これは、同じ画面上で指定された DNS サーバーを使用するために、FQDN が解決する必要があることを示しています。

ステップ 6 **[アップグレードスケジュール（Upgrade Schedule）]** で、時間、頻度、およびタイムゾーンを選択します。

デフォルトは毎日のアップグレードスケジュールです。毎週の特定の日のスケジュールに変更できます。アップグレードが利用可能な場合は、選択した時間に Video Mesh ノード ソフトウェアが自動的にアップグレードされます。

Note アップグレードが利用可能な場合は、**[今すぐアップグレード（Upgrade Now）]** を使用して次のメンテナンスウィンドウの前にアップグレードを開始するか、**[延期（Postpone）]** して以降のウィンドウまで延期できます。

ステップ 7 **[電子メール通知（Email Notifications）]** で、管理者の電子メールアドレスを追加して、サービスアラームやソフトウェアのアップグレードに関する通知を登録します。

管理者の電子メールアドレスは自動的に追加されます。必要に応じて削除できます。

ステップ 8 **ビデオ品質**設定のオン/オフを切り替えて、1080p 30fps のビデオを有効にします。

この設定により、企業のネットワーク内に存在し、高画質の対応可能なデバイスを使用している場合、Video Mesh ノード でホストされたミーティングに参加している SIP 参加者は 1080p 30fps のビデオを使用できます。この設定は、ノードのすべてのクラスタに適用されます。

Note
- この設定がオフの場合、デフォルトは 720p です。
- Webex アプリ がサポートするビデオ解像度については、「通話とミーティングのビデオ仕様」参照してください。

ステップ 9 *[登録完了（Complete Registration）]* に表示される情報を読み、**[ノードに移動（Go to node）]** をクリックしてノードを Webex クラウドに登録します。

ノードを確認するために、ブラウザで新しいタブが開きます。この手順は、ノードの IP アドレス を使用して Video Mesh ノード をセーフリストに追加します。登録プロセス中に、Control Hub は、Video Mesh ノード にリダイレクトします。IP アドレスをセーフリストに追加する必要があります。そうでない場合、登録は失敗します。登録プロセスは、ノードがインストールされているエンタープライズ ネットワークから完了する必要があります。

ステップ 10 **[Webex Video Mesh ノードへのアクセスを許可（Allow Access to the Webex Video Mesh Node）]** をオンにして、**[続行（Continue）]** をクリックします。

ステップ 11 **[許可（Allowed）]** をクリックします。

アカウントが検証されると、Video Mesh ノードが登録され、**「登録が完了しました」**というメッセージが表示されます。これで、Video Mesh ノードが Webex に登録されました。

Video Mesh ノードは、組織の権限に基づいてマシンのログイン情報を取得します。生成されたマシンのログイン情報は定期的に期限切れになり、更新されます。

ステップ 12 ポータルリンクをクリックするか、タブを閉じて [Video Mesh] ページに戻ります。

[Video Mesh] ページに、登録した Video Mesh ノードが含まれる新しいクラスタが表示されます。

- クラスタに移動すると、新しい Video Mesh ノードが表示されます。これは最初に **[登録中（Registering）]** のステータスを示します。Webex 組織での使用準備が完了すると、ノードが **[実行中（Running）]** に変わります。
- このソフトウェアはクラウドインフラストラクチャからのサービスを含むコンテナであるため、クラウドから更新を取得してクラウドサービスと同期されるようになります。必要な更新は、ノードをクラウドに登録した後すぐにインストールされる場合があります。また、自動アップグレードスケジュールを変更することもできます。詳細については、「ハイブリッド サービス リソースの自動アップグレード」を参照してください。
- 登録したノードにデモイメージをインストールした場合は、“デモモード”の黄色ステータスのアラームが表示されます。このアラームは正常ですが、デモイメージの 90 日の猶予期間が満了する前に、完全なソフトウェアイメージをインストールすることを推奨します。

この時点で、Video Mesh ノードは、認証用に発行されたトークンを使用して、セキュリティで保護されたチャネルを介して Cisco Cloud サービスと通信する準備ができています。Video Mesh ノードは、Docker Hub（docker.com、docker.io）とも通信します。Docker は、世界中のさまざまな Video Mesh ノードに配布するためのコンテナを格納するために Video Mesh ノードによって使用されます。Docker Hub に書き込むためのログイン情報を持っているのは Cisco だけです。Video Mesh ノードは、読み取り専用のログイン情報を使用して Docker Hub に接続し、アップグレード用のコンテナをダウンロードできます。

Note イメージは、プロビジョニングデータの一部としてノードに送信されるチェックサムに基づいてダウンロードされます。Docker pull の機能の詳細については、本ドキュメントを参照してください。https://docs.docker.com/v17.09/engine/userguide/storagedriver/imagesandcontainers/#sharing-promotes-smaller-images

留意点

Video Mesh ノードに関する次の情報および Webex 組織に登録した後、どのように動作するかに注意してください。

- 新しい Video Mesh ノードを展開時、Webex アプリ および Webex の登録は、最大 2 時間、新しいノードを認識しません。クライアントは、スタートアップ時にノードの到達可能性、ネットワークの変更、キャッシュの有効期限を確認します。2 時間の待機または、回避策として、Webex アプリ の再起動または Webex ルームまたはデスクデバイスの再起動ができます。後で、コールアクティビティが Control Hub の Video Mesh レポートにキャプチャされます。
- Video Mesh ノードは、1 つの Webex 組織に対する登録であり、マルチテナントデバイスではありません。
- Video Mesh ノードを使用するものと使用しないものを理解するには、Video Mesh ノードを使用するクライアントとデバイスの表を参照してください。
- Video Mesh ノードは、お使いの Webex サイトまたは他のカスタマーまたはパートナーの Webex サイトに接続できます。たとえば、サイト A が Video Mesh ノード クラスタを展開して、それを example1.webex.com ドメインに登録したとします。サイト A のユーザーが mymeeting@example1.webex.com にダイヤルインした場合は、Video Mesh ノードを使用し、カスケードが作成できます。サイト A 内のユーザーが、yourmeeting@example2.webex.com にダイヤルする場合、サイト A のユーザーが自身のローカル Video Mesh ノードを使用して、サイト B の Webex 組織のミーティングに接続します。

What to do next

- 追加ノードを登録するには、これらの手順を繰り返します。
- アップグレードが利用可能な場合は、できるだけ早く適用することを推奨します。アップグレードするには、次の手順を実行します。

1. プロビジョニングデータは、セキュリティで保護されたチャネルを介して、Cisco 開発チームによって Webex クラウドにプッシュされます。プロビジョニングデータは署名されています。コンテナの場合、プロビジョニングデータには名前、チェックサム、バージョンなどが含まれます。また、Video Mesh ノードは、セキュリティで保護されたチャネルを介して Webex クラウドからプロビジョニングデータを取得します。
2. Video Mesh ノードによってプロビジョニングデータがいったん取得されると、ノードは読み取り専用のログイン情報で認証され、コンテナを特定のチェックサムと名前でダウンロードし、システムをアップグレードします。Video Mesh ノードで実行される各コンテナには、イメージ名とチェックサムが含まれています。これらの属性は、セキュリティで保護されたチャネルを使用して Webex クラウドにアップロードされます。

Video Mesh ノードの Quality of Service（QoS）の有効化

始める前に

- 図と表に記載されている、必要なファイアウォールポートの変更を行います。「Video Mesh で使用されるポートとプロトコル （32 ページ）」を参照してください。
- 値リストコレクション作成者をQoSに対して有効にするには、ノードがオンラインになっている必要があります。この設定を有効にすると、メンテナンスモードまたはオフライン状態のノードは除外されます。

手順

ステップ 1 https://admin.webex.com のカスタマービューで、**[サービス（Services）]** > **[ハイブリッド（Hybrid）]** に移動し、Video Mesh カードの **[設定の編集（Edit settings）]** をクリックします。

ステップ 2 **[サービスの品質（Quality of Service）]** までスクロールし、**[有効にする（Enable）]** をクリックします。

有効にすると、オンプレミスのSIPクライアント/エンドポイントおよび一意のDSCPマーキングがあるクラスタ間のカスケードの音声とビデオに使用される大規模な個別のポート範囲（オンプレミスの 呼制御構成によって決定）が取得されます。

- オーディオ：52500 ～ 59499 および 59500 ～ 62999 DSCP EF（Expedited Forwarding（EF; 完全優先転送））
- ビデオ/コンテンツ：63000 ～ 64667 および 64668 ～ 65500 DSCP AF41

値リストコレクション作成者からのすべてのSIPおよびカスケードトラフィックは、オーディオは、EF、ビデオは、AF41 とマークされています。個別のポート範囲は、カスケードメディアのソースポートとして、他の値リストコレクション作成者、クラウドメディアノード、さらに、SIP クライアントメディアの発信元と宛先のポートとして使用されます。Webex Teams アプリとカスケードメディアは、5004 の接続先共有ポートとポート範囲 50000 ～ 53000 を引き続き使用します。

（注） 共有ポートからのすべての Video Mesh リターン トラフィック（音声、ビデオ、コンテンツ）は、AF41 とマークされます。音声トラフィックは、発信元ポート番号に基づいて、ネットワーク内で EF と再マークされる必要があります。

QoS ポートの範囲に対して 1 つのノードがひとつづつ有効になっているかを示すステータスメッセージが表示されます。**[保留中ノードの確認（Review Pending Nodes）]** をクリックすると、QoSに対して保留状態になっているノードのリストが表示されます。ノードのコールトラフィックによっては、この設定を有効にするのに最大 2 時間かかることがあります。

ステップ 3 QoSが2時間以内に完全に有効になっていない場合は、さらなる調査を行うため、サポートに対してケースを開きます。

ノードがリブートし、新しいポートの範囲で更新されます。

この設定を無効にすると、音声とビデオ（34000–34999）の両方に使用される狭く整理したポート範囲を取得します。値リストコレクション作成者からのすべてのトラフィック（SIP、カスケード、クラウドトラフィックなど）は、1 つの AF41 のマーキングを取得します。

ウェブインターフェイスのリフレクタツールを使用した Video Mesh ノードのポート範囲の確認

必要な TCP/UDP ポートが Video Mesh ノードから開かれているかどうかを確認するため、リフレクタツール（Video Mesh ノードとクライアント上の Python スクリプトを使用したサーバーの組み合わせ）が使用されます。

始める前に

- https://github.com/CiscoDevNet/webex-video-mesh-reflector-client から Reflector ツールクライアント（Python スクリプト）のコピーをダウンロードします。
- スクリプトを正常に動作させるには、使用している環境で Python 2.7.10 またはそれ以降を実行していることを確認してください。
- 現在、このツールでは、Video Mesh ノードおよびクラスタ内検証に SIP エンドポイントをサポートしています。

手順

ステップ 1 https://admin.webex.com のカスタマービューで、値リストコレクション作成者のメンテナンスノードを有効にするには、次の手順に従います。

ステップ 2 ノードが Control Hub で [メンテナンス可能（Ready for maintenance）] ステータスを表示するまで待機します。

ステップ 3 Webex Video Mesh ノードインターフェイスを開きます。

この説明については、「ウェブインターフェイスからの Video Mesh ノードの管理 （144 ページ）」を参照してください。

ステップ 4 **[リフレクタツール（Reflector Tool）]** までスクロールし、使用するプロトコルに応じて **[TCP リフレクタサーバー（TCP Reflector Server）]** または **[UDP リフレクタサーバー（UDP Reflector Server）]** のいずれかを起動します。

ステップ 5 **[リフレクタサーバーの起動（Start Reflector Server）]** をクリックし、サーバーが正常に起動するまで待機します。

サーバーの起動時に通知が表示されます。

ステップ 6 Video Mesh ノードの到達先とするネットワーク上のシステム（PC など）から、次のコマンドでスクリプトを実行します。

```
$ python <local_path_to_client_script>/reflectorClient.py --ip <ip address of the server>
 --protocol <tcp or udp>
```

実行の終了時に、必要なすべてのポートが開かれている場合、クライアントは成功メッセージを表示します。

```
$ python reflectorClient.py --ip 10.22.162.102 --protocol tcp
Please wait while verifying tcp for ports: ['5004', '5060-5061'] ...
 [----------------------------->] 100.00%  Success/Failed/Total: 3/0/3

############################
No ports are blocked for tcp in ['5004', '5060-5061']
############################
Exiting Reflector Client tool...
$
```

必要なポートが開いていない場合、クライアントは、失敗した旨を通知するメッセージを示します。

```
$ python reflectorClient.py --ip 10.22.162.102 --protocol tcp --start-port 5060 --end-port 5062
Please wait while verifying tcp for port range: 5060 - 5062 ...
 [----------------------------->] 100.00%  Success/Failed/Total: 2/1/3

Failed ports in the first try:  ['5062']
Retrying(4 times) the above failed ports:
Retry number 1:
   Verifying port -> 5062
Retry number 2:
   Verifying port -> 5062
Retry number 3:
   Verifying port -> 5062
Retry number 4:
   Verifying port -> 5062
############################
Ports which are not open for tcp are: ['5062']
############################
Exiting Reflector Client tool...
```

ステップ 7 ファイアウォール上のポートの問題を解決してから、上記の手順を再実行します。

ステップ 8 詳細については、**--help** を使用してクライアントを実行してください。

```
$ python reflectorClient.py --help
Usage:
      --ip and --protocol are mandatory.
      If start-port is specified, end-port is considered mandatory. If no starting port is specified, default ports are verified for connectivity.
      By default, tool checks for QoS ports unless --non-qos option is specified.
      Default QoS ports include: TCP - 5004, 5060, 5061 and UDP - 5004, 52500-59499 and 63000-64667.
      Default non QoS ports include: TCP - 5004, 5060, 5061 and UDP - 5004, 34000-34999.
      To verify single port, both start and end port should be the required port to verify.
      Examples:
      Below run is to verify non-qos ports using an input port range:
        python reflectorClient.py --ip <hmn-ip-address> --protocol <udp/tcp> --start-port 52000 --end-port 52501 --non-qos
      Below run in to verify default qos ports:
        python reflectorClient.py --ip <> --protocol <udp/tcp>
$
```

プロキシ統合のための Video Mesh ノードの構成

Video Mesh と統合するプロキシのタイプを指定するには、次の手順を使用します。透過的な検査プロキシまたは明示的なプロキシを選択した場合、ノードのインターフェイスを使用してルート証明書をアップロードおよびインストールし、プロキシ接続を確認し、考え得る問題をトラブルシュートします。

始める前に

- サポートされているプロキシオプションの概要については、「Video Mesh のプロキシサポート （5 ページ）」を参照してください。
- Video Mesh のプロキシサポートの要件 （15 ページ）

手順

ステップ 1 Web ブラウザで Video Mesh セットアップ URL `https://[IP または FQDN/setup` を入力し、ノード用にセットアップした管理者のログイン情報を入力して、**[サインイン（Sign In）]** をクリックし ます。

ステップ 2 [信頼ストアとプロキシ（Trust Store & Proxy）] に移動して、次のオプションを選択します。

- **プロキシなし（No proxy）**：プロキシを統合する前のデフォルトオプション。証明書の更新は必要ありません。
- **透過的な非検査プロキシ（Transparent Non-Inspecting Proxy）**：Video Mesh ノードは特定のプロキシサーバーアドレスを使用するように設定されないため、非検査プロキシと連動するための変更は必要ありません。証明書の更新は必要ありません。
- **透過的な検査プロキシ（Transparent Inspecting Proxy）**：Video Mesh ノードは特定のプロキシサーバーアドレスを使用するように設定されません。Video Mesh では http(s) 設定の変更は必要ありませんが、Video Mesh ノードにはプロキシを信頼するためのルート証明書が必要です。通常、IT は検査プロキシを使用して、アクセス可能な Web サイトおよび許可されないコンテンツのタイプに関するポリシーを適用します。このタイプのプロキシは、すべてのトラフィックを（https も）復号します。
- **明示的なプロキシ（Explicit Proxy）**：明示的なプロキシを使用する場合、プロキシサーバーが使用するクライアント（Video Mesh ノード）を指定します。このオプションは複数の認証タイプをサポートします。このオプションを選択した場合、以下の情報を入力する必要があります。

  1. **プロキシ IP/FQDN（Proxy IP/FQDN）**：プロキシ マシンに到達可能なアドレス。
  2. **プロキシポート（Proxy Port）**：プロキシがプロキシ経由のトラフィックをリッスンするために使用するポート番号。
  3. **プロキシプロトコル（Proxy Protocol）**：**http**（Video Mesh は、http プロキシ経由で https トラフィックをトンネル接続します）または **https**（Video Mesh ノードからプロ

キシへのトラフィックは、https プロトコルを使用します）を選択します。プロキシサーバーのサポート対象に応じてオプションを選択します。

4. プロキシ環境に応じて、次の認証タイプの中から選択します。

オプション	使用方法
なし（**None**）	認証方式がない HTTP または HTTPS の明示的なプロキシを選択します。
基本（**Basic**）	HTTP または HTTPS の明示的なプロキシで使用できます。 HTTP ユーザーエージェントが要求を行う際にユーザー名とパスワードを入力するために使用され、Base64 エンコーディングを使用します。
ダイジェスト（**Digest**）	HTTPS の明示的なプロキシでのみ使用できます。 機密情報を送信する前にアカウントを確認するために使用され、ネットワークを介して送信する前にユーザー名とパスワードにハッシュ機能を適用します。
NTLM	HTTP の明示的なプロキシでのみ使用できます。 ダイジェストと同様に、機密情報を送信する前にアカウントを確認するために使用されます。ユーザー名とパスワードではなく、Windows ログイン情報を使用します。 このオプションを選択する場合は、プロキシが **[NTLM ドメイン（NTLM Domain）]** フィールドで認証のために使用する Active Directory ドメインを入力します。**[NTLM ワークステーション（NTLM Workstation）]** フィールドで、指定された NTLM ドメイン内のプロキシワークステーション（ワークステーション アカウントまたはマシン アカウントとも呼ばれます）の名前を入力します。

透過的な検査または明示的なプロキシについては、次の手順に従います。

ステップ 3 **[ルート証明書またはエンドエンティティ証明書のアップロード（Upload a Root Certificate or End Entity Certificate）]** をクリックし、明示的または透過的な検査プロキシのルート証明書を見つけて選択します。

証明書はアップロードされますが、証明書をインストールするためにノードを再起動する必要があるため、まだインストールされません。詳細を確認するには、証明書発行者名の近くにある矢印をクリックします。または、誤りがあったために証明書を再アップロードする場合は、[**削除（Delete）**] をクリックします。

ステップ 4 透過的な検査または明示的なプロキシについては、**[プロキシ接続の確認（Check Proxy Connection）]** をクリックして、Video Mesh ノードとプロキシ間のネットワーク接続をテストします。

接続テストが失敗した場合は、失敗した理由とその問題を解決する方法を説明するエラーメッセージが表示されます。

ステップ 5 明示的なプロキシの場合、接続テストが成功した後、トグルを **[このノードからポート 443 へのすべての HTTPS リクエストを明示的なプロキシ経由でルーティングする（Route all port 443 https requests from this node through the explicit proxy）]** に切り替えます。この設定は適用されるまでに 15 秒かかります。

ステップ 6 **[すべての証明書を信頼ストアにインストール（Install All Certificates Into the Trust Store）]**（プロキシのセットアップ中にルート証明書が追加された場合は常に表示されます）または **[再起動（Reboot）]**（ルート証明書が追加されない場合は表示されます）をクリックし、プロンプトを読み、準備ができたら **[インストール（Install）]** をクリックします。

ノードは数分以内に再起動します。

ステップ 7 ノードが再起動したら、必要に応じて再度サインインして **[概要（Overview）]** ページを開き、接続チェックのステータスがすべて緑色になっていることを確認します。

プロキシ接続チェックでは、webex.com のサブドメインだけがテストされます。接続の問題がある場合、一般的な原因は、インストール手順に記載されているクラウドドメインの一部がプロキシでブロックされていることです。

呼制御タスクフローと Video Mesh の統合

Video Mesh に SIP ダイヤルインをルーティングするように、SIP トランクを設定します。SIP デバイスは、直接到達可能性をサポートしないため、Unified CM または VCS Expressway 設定を使用して、オンプレミス SIP デバイスおよび Video Mesh クラスタ間の関係を確立する必要があります。

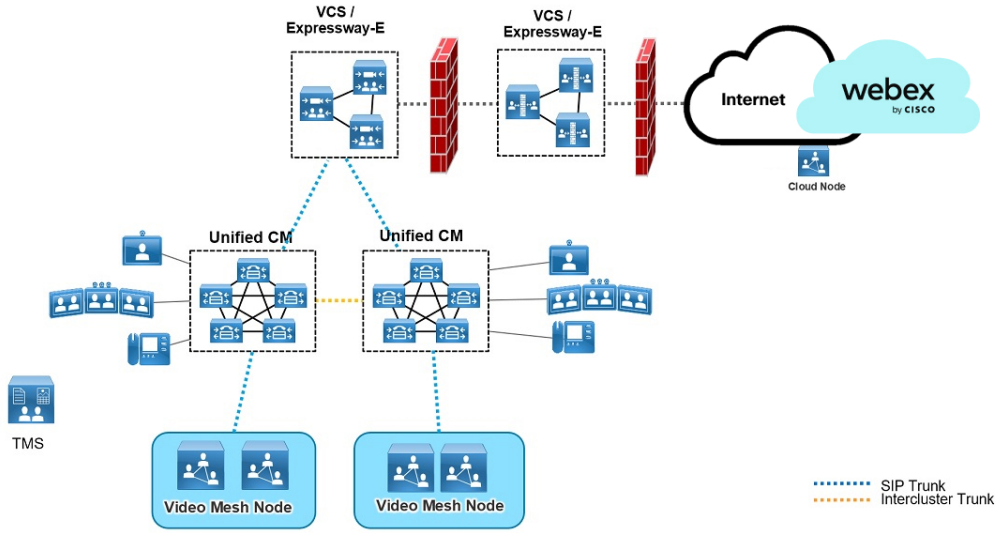
始める前に

- 一般的な導入例については、「Video Mesh と Cisco Unified Communications Manager の導入モデル （29 ページ）」を参照してください。

- Video Mesh は、Unified CM と SIP シグナリング間の TCP または TLS のいずれかをサポートします。SIP TLS は VCS Expressway 向けにサポートされていません。
- Unified CM では、各 SIP トランクが最大 16 の Video Mesh 接続先（IP アドレス）をサポートできます。
- Unified CM では、SIP トランクセキュリティプロファイルの受信ポートは、デフォルト（非セキュア SIP トランクプロファイル）にできます。
- Video Mesh では、**webex.com**（短いビデオアドレス向け）、**sitename.webex.com**、および **meet.ciscospark.com** の 3 つのルートパターンがサポートされています。他のルートパターンはサポートされていません。

（注） 短いビデオアドレス形式（**meet@webex.com**）を使用する場合、Video Mesh ノードは常にコールを処理します。Video Mesh が有効になっていないサイトに対するコールの場合でも、ノードはコールを処理します。

図 *9*：分散 ***Unified CM*** を使用した ***Video Mesh*** の導入例



手順

	コマンドまたはアクション	目的
ステップ 1	呼制御環境とセキュリティ要件に応じて、次のオプションのいずれかを選択します。 • Unified CM セキュア TLS SIP トラフィックルーティングの設定 - Video Mesh （96 ページ） • Video Mesh 用の Unified CM TCP SIP トラフィックルーティングの設定（100 ページ） • Video Mesh 用の Expressway TCP SIP トラフィックルーティングの設定（105 ページ）（TCP のみ）	**Unified CM に登録されている SIP デバイス（TLS または TCP）** TLS 暗号化トラフィックまたは TCP SIP トラフィックのいずれかを使用して、Video Mesh を使用して Unified CM を設定します。高い可用性を備え、デバイス障害に対応できる、クラスタ設定を反映したトランクルーティングポリシーを作成できます。Unified CM Session Management Edition（SME）を使用している場合、Session Management クラスタ内の Unified CM サーバー間でインバウンドコールとアウトバウンドコールが均等に分散されるよう、Unified CM SME とリーフシステムにトランクを設定します。 通常各サイトには、関連付けられている専用の Unified CM クラスタがあります。これらのクラスタは、クラスタ間 SIP トランクを介して接続されます。各クラスタには、Video Mesh ノードのローカルサイトへのコールイントランクが含まれます。 障害やオーバーフロー状態に対応できるように設定することもできます。この構成は、停止が発生した場合や Video Mesh クラスタがキャパシティに達した場合に役立ちます。クラスタとの間で SIP 会議またはコールを確立できない場合、会議/コールはオーバーフローします。 **VCS または Expressway に登録されている SIP デバイス（TCP のみ）** ネイバーゾーンと検索ルールを設定して、Webex Meetings から Video Mesh クラスタへ SIP ダイヤルインおよびダイヤルアウトをルートします。VCS Control または Expressway-C に登録されている SIP デバイスは、

	コマンドまたはアクション	目的
		直接到達可能性をサポートしないため、TCP ベースの Expressway 設定を使用して、オンプレミス SIP デバイスおよび Video Mesh クラスタ間の関係を確立する必要があります。 障害やオーバーフロー状態に対応できるように設定することもできます。この構成は、停止が発生した場合や Video Mesh クラスタがキャパシティに達した場合に役立ちます。クラスタとの間で確立できない SIP ミーティングやコールは、VCS Control/Expressway-C または Expressway-C/E ペアを介してクラウドにオーバーフローします。

Unified CM セキュア TLS SIP トラフィックルーティングの設定 - Video Mesh

手順

ステップ 1 Video Mesh クラスタに SIP プロファイルを作成するには、次のようにします。

a) Cisco Unified CM Administration から、**[デバイス（Device）] > [デバイスの設定（Device Settings）] > [SIPプロファイル（SIP Profile）]** の順に選択し、**[検索（Find）]** をクリックします。

b) **[Cisco VCS用の標準SIPプロファイル（Standard SIP Profile For Cisco VCS）]** を選択し、さらに **[コピー（Copy）]** をクリックします。

c) 新しいプロファイルの名前を入力します。たとえば、「**`Video Mesh SIP プロファイル`**」と入力します。

d) **[トランク固有の構成（Trunk Specific Configuration）]** で、**[音声コールとビデオ コールに対する早期オファー サポート（Early Offer support for voice and video calls）]** を**[ベストエフォート（Best Effort）]**（MTP は挿入しない）にセットします。

この設定は、（Webex サイト用に外部ドメインによってルーティングされた）Webex クラウドへの新しい SIP トランクに適用できます。この設定は、既存の SIP トランキングやコールルーティングには影響を与えません。

e) **[サービスタイプのトランクの接続先ステータスをモニタするために OPTIONS Ping を有効にする（Enable OPTIONS Ping to monitor destination status for Trunks with Service Type）]** がオンになっていることを確認します。

f) その他のフィールドはデフォルト値のままにして変更を保存します。

ステップ 2 Video Mesh クラスタの新しい SIP トランク セキュリティ プロファイルを追加します。

a) Cisco Unified CM Administration から、**[システム（System）] > [セキュリティ（Security）] > [SIPトランクセキュリティプロファイル（SIP Trunk Security Profile）]** の順に選択し、さらに **[新規追加（Add New）]** をクリックします。

b) 「**`Video Mesh Secure SIP Trunk Security Profile`**」 などのわかりやすい名前を入力します。

c) 次の設定を確認します。

フィールド	値
デバイスセキュリティモード（Device Security Mode）	**暗号化（Encrypted）**
着信転送タイプ（Incoming Transport Type）	**TLS**
発信転送タイプ（Outgoing Transport Type）	**TLS**
X.509 のサブジェクト名（X.509 Subject Name） 安全な証明書の件名またはサブジェクトの別名	Video Mesh ノード証明書の共通名を入力します。
着信ポート（Incoming Port）	**5061**
SIP V.150アウトバウンドSDPオファーのフィルタリング（SIP V.150 Outbound SDP Offer Filtering）	**デフォルトのフィルタを使用（Use Default Filter）**

d) その他のフィールドはデフォルト値のままにして変更を保存します。

ステップ 3 Video Mesh クラスタをポイントする新しい SIP トランクを追加します。

- Unified CM のみの導入では、トランクを 1 つ追加します。
- SME の導入では、通常、Unified CM と SME の間にトランクが存在します。SME と Video Mesh ノードの間に別のトランクを追加します。いずれのトランクにも以下の同じ内容を設定します。

a) Cisco Unified CM Administration で、**[デバイス（Device）] > [トランク（Trunk）]** の順に選択し、さらに **[新規追加（Add New）]** をクリックします。

b) トランク タイプに **[SIP トランク（SIP Trunk）]** を選択し、他の値はそのままにして **[次へ（Next）]** をクリックします。

c) 「**`Video_Mesh_SIP_Trunk_UCMtoVMN`**」 などのわかりやすい名前を入力します。

d) **[SRTP Allowed（SRTP を許可する）]** チェックボックスをオンにします。

e) **[発呼側および接続側情報フォーマット（Calling and Connecting Party Info Format）]** として、**[接続側にのみ URI および DN を配信（使用可能な場合）（Deliver URI and DN in connected party, if available）]** をオンにします。この設定により、混合アイデンティティが有効になります。これにより、SIP トランクが企業側のパーティのディレクトリ URI を Webex に送信できるようになります。

f) **[すべてのアクティブな Unified CM ノードで実行（Run on All Active Unified CM Nodes）]** をオンにします。

g) **[SIP 情報 - 宛先（SIP Information - Destination）]** で、各 Video Mesh ノードに対して IP アドレスまたは完全修飾ドメイン名（FQDN）を入力します。

h) **[宛先ポート（Destination Port）]** に**「5061」**と入力します。

i) **SIP トランク セキュリティ プロファイル**の場合は、前の手順で作成した**「Video Mesh トランク セキュリティ プロファイル」**を選択します。（「**`Video Mesh Secure SIP Trunk Security Profile`**」 はその一例です。）

j) **SIP プロファイル**の場合は、前の手順で作成した**「Video Mesh SIP プロファイル」**を選択します。（たとえば、「**`Video Mesh SIP プロファイル`**」など）。

k) その他のフィールドはデフォルト値のままにして変更を保存します。

（注） Video Mesh コールまたは会議では、SIP コールを終了するノードだけでなく、クラスタ内の任意のノードにメディアを割り当てることができます。

ステップ 4 Webex クラウドフェールオーバー用の Expressway をポイントする SIP トランクを作成します。

注意 既存の Unified CM と Expressway の導入にすでにある SIP トランクを使用できます。別のトランクを作成し、それら Expressway で Mobile Remote Access（MRA）も実行する場合は、MRA が中断されることがあります。

a) Cisco Unified CM Administration で、**[デバイス（Device）] > [トランク（Trunk）]** の順に選択し、さらに **[新規追加（Add New）]** をクリックします。

b) トランク タイプに **[SIP トランク（SIP Trunk）]** を選択し、他の値はそのままにして **[次へ（Next）]** をクリックします。

c) 「**`Video_Mesh_VCS_Trunk`**」 などのわかりやすい名前を入力します。

d) **[発呼側および接続側情報フォーマット（Calling and Connecting Party Info Format）]** として、**[接続側にのみ URI および DN を配信（使用可能な場合）（Deliver URI and DN in connected party, if available）]** をオンにします。この設定により、混合アイデンティティが有効になります。これにより、SIP トランクが企業側のパーティのディレクトリ URI を Webex に送信できるようになります。

e) **[SIP 情報 - 宛先（SIP Information - Destination）]** で、各 Expressway の IP アドレス、または完全修飾ドメイン名（FQDN）を入力します。**[ポート（Port）]** に対して、**「5060」**を入力します。

f) **[SIP プロファイル（SIP Profile）]** には、**[Cisco VCS 用の標準 SIP プロファイル（Standard SIP Profile For Cisco VCS）]** を選択します。

ステップ 5 Video Mesh クラスタへのコール用の新しいルートグループを作成します。

a) Cisco Unified CM Administration で、**[コールルーティング（Call Routing）] > [ルート/ハント（Route/Hunt）] > [ルートグループ（Route Group）]** の順に選択し、**[新規追加（Add New）]** をクリックします。
b) 「**Video Mesh Node Route Group**」 などの、わかりやすい名前を入力します。
c) **分散アルゴリズム**を**トップダウン方式**に変更します。
d) **[ルートグループメンバー情報]** セクションで、**Video Mesh**と名前が付いているデバイスを見つけます。
e) **[ルートグループに追加（Add to Route Group）]** をクリックし、「**Video_Mesh_SIP_Trunk_UCMtoVMN**」 を追加します。
f) 変更を保存します。

ステップ 6 クラウドにオーバーフローできるように、コールを Expressway に渡す新しいルートグループを作成します。

a) Cisco Unified CM Administration で、**[コールルーティング（Call Routing）] > [ルート/ハント（Route/Hunt）] > [ルートグループ（Route Group）]** の順に選択し、**[新規追加（Add New）]** をクリックします。
b) 「**Video Mesh Expressway Route Group**」 などの、わかりやすい名前を入力します。
c) **分散アルゴリズム**を**トップダウン方式**に変更します。
d) **[ルートグループメンバー情報]** セクションで、**Video Mesh** と名前が付いているデバイスを見つけます。
e) **[ルートグループに追加（Add to Route Group）]** をクリックし、**「Video_Mesh_VCS_Trunk」**を追加します。
f) 変更を保存します。

ステップ 7 Video Mesh クラスタおよびExpressway にコールするための新しいルートリストを作成 します。

a) Cisco Unified CM Administration で、**[コールルーティング（Call Routing）] > [ルート/ハント（Route/Hunt）] > [ルートリスト（Route List）]** の順に選択し、**[新規追加（Add New）]** をクリックします。
b) 「**Video Mesh Node Route List**」 などの、わかりやすい名前を入力します。
c) **[Cisco Unified Communications Manager グループ（Cisco Unified Communications Manager Group）]** を **[デフォルト（Default）]** に設定するか、構成に合わせて別の値を設定します。
d) 変更を保存します。
e) **[ルートリストメンバー情報]** セクションで、**[ルートグループの追加（Add Route Group）]** をクリックして、**「Video Mesh ルート グループ」**を選択します。
f) その他の設定はデフォルトのままにし、変更内容を保存します。
g) **[ルートリストメンバー情報]** セクションで、**[ルートグループの追加（Add Route Group）]** をクリックして、**「Video Mesh エクスプレスウェイ ルート グループ」**を選択します。
h) その他の設定はデフォルトのままにし、変更内容を保存します。

ステップ 8 Webex ミーティング向けに、短いビデオアドレスのダイヤリング形式の SIP ルートパターンを作成します。

a) **[コールルーティング（Call Routing）] > [SIP ルートパターン（SIP Route Pattern）]** で、**[新規追加（Add New）]** をクリックし、「**Video Mesh Route Pattern for Webex Short URIs**」 という名前を入力します。
b) **[Pv4 パターン（IPv4 pattern）]** で、ドメインとして **webex.com** と入力します。
c) **[SIP トランク/ルートリスト（SIP Trunk/Route List）]**の場合は、Video Mesh に対して作成された [ルートリスト（Route List）] を選択します。例：「**Video Mesh ルート リスト**」など。
d) その他のフィールドはデフォルト値のままにして変更を保存します。

短いビデオアドレスダイヤリング機能により、ユーザーは、ビデオシステムを使用して Webex ミーティングまたはイベントに参加するために Webex サイト名を記憶しておく必要がなくなりました。知っておく必要があるのはミーティングまたはイベントの番号のみであるため、ミーティングにより迅速に参加できます。

ステップ 9 Webex サイトの SIP ルートパターンを作成します。

a) **[コールルーティング（Call Routing）] > [SIP ルートパターン（SIP Route Pattern）]** で、**[新規追加（Add New）]** をクリックし、「**Video Mesh Route Pattern for Webex Sites**」 という名前を入力します。
b) **[Pv4 パターン（IPv4 pattern）]** で、メディアを最適化する Webex サイト（例：「**examplesitename.webex.com**」）を入力します。
c) **[SIP トランク/ルートリスト（SIP Trunk/Route List）]**の場合は、Video Mesh に対して作成された [ルートリスト（Route List）] を選択します。例：「**Video Mesh ルート リスト**」など。
d) その他のフィールドはデフォルト値のままにして変更を保存します。

ステップ 10 Webex アプリ ミーティング用の SIP ルートパターンを作成し ます（下位互換性）。

a) **[コールルーティング（Call Routing）] > [SIP ルートパターン（SIP Route Pattern）]** で、**[新規追加（Add New）]** をクリックし、「**Video Mesh Route Pattern for Teams Meetings**」 という名前を入力します。
b) **[Pv4 パターン（IPv4 pattern）]** に、**meet.ciscospark.com** と入力します。
c) **[SIP トランク/ルートリスト（SIP Trunk/Route List）]**の場合は、Video Mesh に対して作成された [ルートリスト（Route List）] を選択します。例：「**Video Mesh ルート リスト**」など。
d) その他のフィールドはデフォルト値のままにして変更を保存します。

Video Mesh 用の Unified CM TCP SIP トラフィックルーティングの設定

Procedure

ステップ 1 Video Mesh クラスタに SIP プロファイルを作成するには、次のようにします。

a) Cisco Unified CM Administration から、**[デバイス（Device）] > [デバイスの設定（Device Settings）] > [SIPプロファイル（SIP Profile）]** の順に選択し、**[検索（Find）]** をクリックします。
b) **[Cisco VCS用の標準SIPプロファイル（Standard SIP Profile For Cisco VCS）]** を選択し、さらに **[コピー（Copy）]** をクリックします。
c) 新しいプロファイルの名前を入力します。たとえば、"**`Video Mesh SIP プロファイル`**" と入力します。
d) **[トランク固有の構成（Trunk Specific Configuration）]** で、**[音声コールとビデオ コールに対する早期オファー サポート（Early Offer support for voice and video calls）]** を**[ベストエフォート（Best Effort）]**（MTP は挿入しない）にセットします。

この設定は、（Webex サイト用に外部ドメインによってルーティングされた）Webex への新しい SIP トランクに適用できます。この設定は、既存の SIP トランキングやコールルーティングには影響を与えません。

e) **[サービスタイプのトランクの接続先ステータスをモニタするために OPTIONS Ping を有効にする（Enable OPTIONS Ping to monitor destination status for Trunks with Service Type）]** がオンになっていることを確認します。
f) その他のフィールドはデフォルト値のままにして変更を保存します。

ステップ 2 Video Mesh クラスタの新しい SIP トランク セキュリティ プロファイルを追加します。

a) Cisco Unified CM Administration から、**[システム（System）] > [セキュリティ（Security）] > [SIPトランクセキュリティプロファイル（SIP Trunk Security Profile）]** の順に選択し、さらに **[新規追加（Add New）]** をクリックします。
b) "**`Video Mesh Trunk Security Profile`**" などの、わかりやすい名前を入力します。
c) 次の設定を確認します。

フィールド	値
デバイスセキュリティモード（Device Security Mode）	**非セキュア（Non Secure）**
着信転送タイプ（Incoming Transport Type）	**TCP+UDP**
発信転送タイプ（Outgoing Transport Type）	**TCP**
着信ポート（Incoming Port）	**5060**
SIP V.150アウトバウンドSDPオファーのフィルタリング（SIP V.150 Outbound SDP Offer Filtering）	**デフォルトのフィルタを使用（Use Default Filter）**

d) その他のフィールドはデフォルト値のままにして変更を保存します。

ステップ 3 Video Mesh クラスタをポイントする新しい SIP トランクを追加します。

- Unified CM のみの導入では、トランクを 1 つ追加します。
- SME の導入では、通常、Unified CM と SME の間にトランクが存在します。SME と Video Mesh ノードの間に別のトランクを追加します。いずれのトランクにも以下の同じ内容を設定します。

a) Cisco Unified CM Administration で、**[デバイス（Device）] > [トランク（Trunk）]** の順に選択し、さらに **[新規追加（Add New）]** をクリックします。

b) トランク タイプに **[SIP トランク（SIP Trunk）]** を選択し、他の値はそのままにして **[次へ（Next）]** をクリックします。

c) **“Video_Mesh_SIP_Trunk_UCMtoVMN”** などのわかりやすい名前を入力します。

d) **[発呼側および接続側情報フォーマット（Calling and Connecting Party Info Format）]** として、**[接続側にのみ URI および DN を配信（使用可能な場合）（Deliver URI and DN in connected party, if available）]** をオンにします。この設定により、混合アイデンティティが有効になります。これにより、SIP トランクが企業側のパーティのディレクトリ URI を Webex に送信できるようになります。

e) **[すべてのアクティブな Unified CM ノードで実行（Run on All Active Unified CM Nodes）]** をオンにします。

f) **[SIP 情報 - 宛先（SIP Information - Destination）]** で、各 Video Mesh ノードに対して IP アドレスまたは完全修飾ドメイン名（FQDN）を入力します。

g) **[宛先ポート（Destination Port）]** に**「5060」**と入力します。

h) **SIP トランク セキュリティ プロファイル**の場合は、前の手順で作成した**「Video Mesh トランク セキュリティ プロファイル」**を選択します。（たとえば、“**Video Mesh トランク セキュリティ プロファイル**”など）。

i) **SIP プロファイル**の場合は、前の手順で作成した**「Video Mesh SIP プロファイル」**を選択します。（たとえば、“**Video Mesh SIP プロファイル**”など）。

j) その他のフィールドはデフォルト値のままにして変更を保存します。

Note Video Mesh コールまたは会議では、SIP コールを終了するノードだけでなく、クラスタ内の任意のノードにメディアを割り当てることができます。

ステップ 4 Expressway をポイントする新しい SIP トランクを作成します。

Caution 既存の Unified CM と Expressway の導入にすでにある SIP トランクを使用できます。別のトランクを作成し、それら Expressway で Mobile Remote Access（MRA）も実行する場合は、MRA が中断されることがあります。

a) Cisco Unified CM Administration で、**[デバイス（Device）] > [トランク（Trunk）]** の順に選択し、さらに **[新規追加（Add New）]** をクリックします。

b) トランク タイプに **[SIP トランク（SIP Trunk）]** を選択し、他の値はそのままにして **[次へ（Next）]** をクリックします。

c) “**Video_Mesh_VCS_Trunk**” などのわかりやすい名前を入力します。

d) **[発呼側および接続側情報フォーマット（Calling and Connecting Party Info Format）]** として、**[接続側にのみ URI および DN を配信（使用可能な場合）（Deliver URI and DN in connected party, if available）]** をオンにします。この設定により、混合アイデンティティ

が有効になります。これにより、SIP トランクが企業側のパーティのディレクトリ URI を Webex に送信できるようになります。

e) **[SIP 情報 - 宛先（SIP Information - Destination）]** で、各 Expressway の IP アドレス、または完全修飾ドメイン名（FQDN）を入力します。**[ポート（Port）]** に対して、**「5060」**を入力します。

f) **[SIP プロファイル（SIP Profile）]** には、**[Cisco VCS 用の標準 SIP プロファイル（Standard SIP Profile For Cisco VCS）]** を選択します。

ステップ 5 Video Mesh クラスタへのコール用の新しいルートグループを作成します。

a) Cisco Unified CM Administration で、**[コールルーティング（Call Routing）] > [ルート/ハント（Route/Hunt）] > [ルートグループ（Route Group）]** の順に選択し、**[新規追加（Add New）]** をクリックします。

b) "**`Video Mesh Node Route Group`**" などの、わかりやすい名前を入力します。

c) **分散アルゴリズム**を**トップダウン方式**に変更します。

d) **[ルートグループメンバー情報]** セクションで、**Video Mesh** と名前が付いているデバイスを見つけます。

e) **[ルートグループに追加（Add to Route Group）]** をクリックし、"**`Video_Mesh_SIP_Trunk_UCMtoVMN`**" を追加します。

f) 変更を保存します。

ステップ 6 クラウドにオーバーフローできるように、コールを Expressway に渡す新しいルートグループを作成します。

a) Cisco Unified CM Administration で、**[コールルーティング（Call Routing）] > [ルート/ハント（Route/Hunt）] > [ルートグループ（Route Group）]** の順に選択し、**[新規追加（Add New）]** をクリックします。

b) "**`Video Mesh Expressway Route Group`**" などの、わかりやすい名前を入力します。

c) **分散アルゴリズム**を**トップダウン方式**に変更します。

d) **[ルートグループメンバー情報]** セクションで、**Video Mesh** と名前が付いているデバイスを見つけます。

e) **[ルートグループに追加（Add to Route Group）]** をクリックし、"Video_Mesh_VCS_Trunk" を追加します。

f) 変更を保存します。

ステップ 7 Video Mesh クラスタおよび Expressway にコールするための新しいルートリストを作成 します。

a) Cisco Unified CM Administration で、**[コールルーティング（Call Routing）] > [ルート/ハント（Route/Hunt）] > [ルートリスト（Route List）]** の順に選択し、**[新規追加（Add New）]** をクリックします。

b) "**`Video Mesh Node Route List`**" などの、わかりやすい名前を入力します。

c) **[Cisco Unified Communications Manager グループ（Cisco Unified Communications Manager Group）]** を **[デフォルト（Default）]** に設定するか、構成に合わせて別の値を設定します。

d) 変更を保存します。

e) **[ルートリストメンバー情報]** セクションで、**[ルートグループの追加（Add Route Group）]** をクリックして、**「Video Mesh ルート グループ」**を選択します。

f) その他の設定はデフォルトのままにし、変更内容を保存します。

g) **[ルートリストメンバー情報]**セクションで、**[ルートグループの追加（Add Route Group）]** をクリックして、**「Video Mesh エクスプレスウェイ ルート グループ」**を選択します。
h) その他の設定はデフォルトのままにし、変更内容を保存します。

ステップ 8 Webex ミーティング向けに、短いビデオアドレスのダイヤリング形式の SIP ルートパターンを作成します。

a) **[コールルーティング（Call Routing）] > [SIP ルートパターン（SIP Route Pattern）]** で、**[新規追加（Add New）]** をクリックし、“**`Video Mesh Route Pattern for Webex Short URIs`**” という名前を入力します。
b) **[Pv4 パターン（IPv4 pattern）]** で、ドメインとして **webex.com** と入力します。
c) **[SIP トランク/ルートリスト（SIP Trunk/Route List）]**の場合は、Video Mesh に対して作成された [ルートリスト（Route List）] を選択します。例：“**Video Mesh ルートリスト**”など。
d) その他のフィールドはデフォルト値のままにして変更を保存します。

短いビデオアドレスダイヤリング機能により、ユーザーは、ビデオシステムを使用して Webex ミーティングまたはイベントに参加するために Webex サイト名を記憶しておく必要がなくなりました。知っておく必要があるのはミーティングまたはイベントの番号のみであるため、ミーティングにより迅速に参加できます。

ステップ 9 Webex サイトの SIP ルートパターンを作成します。

a) **[コールルーティング（Call Routing）] > [SIP ルートパターン（SIP Route Pattern）]** で、**[新規追加（Add New）]** をクリックし、“**`Video Mesh Route Pattern for Webex Sites`**” という名前を入力します。
b) **[IPv4 パターン（IPv4 pattern）]**で、メディアを最適化する Webex サイトを入力します。たとえば、“**examplesitename.webex.com**” です（**examplesitename** は実際の Webex サイトの名前）。
c) **[SIP トランク/ルートリスト（SIP Trunk/Route List）]**の場合は、Video Mesh に対して作成された [ルートリスト（Route List）] を選択します。例：“**Video Mesh ルートリスト**”など。
d) その他のフィールドはデフォルト値のままにして変更を保存します。

ステップ 10 Webex アプリ ミーティング用の SIP ルートパターンを作成します。

a) **[コールルーティング（Call Routing）] > [SIP ルートパターン（SIP Route Pattern）]** で、**[新規追加（Add New）]** をクリックし、“**`Video Mesh Route Pattern for Teams Meetings`**” という名前を入力します。
b) **[Pv4 パターン（IPv4 pattern）]** に、**meet.ciscospark.com** と入力します。
c) **[SIP トランク/ルートリスト（SIP Trunk/Route List）]**の場合は、Video Mesh に対して作成された [ルートリスト（Route List）] を選択します。例：“**Video Mesh ルートリスト**”など。
d) その他のフィールドはデフォルト値のままにして変更を保存します。

Video Mesh 用の Expressway TCP SIP トラフィックルーティングの設定

Procedure

ステップ 1 Video Mesh クラスタをポイントするゾーンを作成します。

a) VCS Control または Expressway-C から、**[設定（Configuration）]** > **[ゾーン（Zones）]** > **[ゾーン（Zones）]** に移動し、**[新規（New）]** をクリックします。

b) 次のフィールドを設定します。

フィールド名	値
名前（Name）	**WebexVideoMeshZone** などゾーンを容易に識別するための名前を入力します。
タイプ（Type）	**ネイバー（Neighbor）**
H.323	
モード（Mode）	**オフ（Off）**
SIP	
モード（Mode）	**オン（On）**
ポート（Port）	**5060**
転送	**TCP**
ロケーション（Location）	
次の方法でピアを検索する（Look up peers by）	**アドレス（Address）**
ピア [n] アドレス	各 Video Mesh ノードの IP アドレスを入力します。

c) その他のフィールドはデフォルト設定のままにし、変更を保存します。

ステップ 2 Webex サイトの Video Mesh クラスタ用のダイヤルパターンを作成します。

a) Expressway-C から、**[設定（Configuration）]** > **[ダイヤル プラン（Dial Plan）]** > **[検索ルール（Search rules）]** に移動し、**[新規（New）]** をクリックします。

b) Webex サイト検索ルール用に次のフィールドを設定します。

フィールド名	値
ルール名（Rule Name）	検索ルールを簡単に識別するためのルール名（たとえば、**WebexVideoMesh-YourSite**）を入力します。

フィールド名	値
優先度（Priority）	デフォルトは**100**です。この数値がクラウドのフォールバックルールおよびB2Bルールよりも低いことを確認してください。
プロトコル（Protocol）	**SIP**
モード（Mode）	**エイリアスのパターンマッチ（Alias pattern match）**
パターンタイプ（Pattern type）	**Regex**
パターン文字列（Pattern string）	`.*@(YourSite\.)?webex\.com.*` **Note** このパターンは、**yoursite.webex.com** と **webex.com**（短いビデオアドレス向け）の両方の形式と一致します。短いビデオ アドレス ダイヤリング機能により、ユーザーは、ビデオシステムを使用して Webex ミーティングまたはイベントに参加するために Webex サイト名を記憶しておく必要がなくなりました。知っておく必要があるのはミーティングまたはイベントの番号のみであるため、ミーティングにより迅速に参加できます。
パターン動作（Pattern behavior）	**変更なし（Leave）**
正常に一致する場合（On successful match）	**続行（Continue）**
ターゲット（Target）	**WebexVideoMeshZone** など、作成した Video Mesh ゾーンを選択します。

c) その他のフィールドはデフォルト設定のままにし、変更を保存します。

ステップ 3 フェールオーバーのためのクラウド Expressway をポイントするトラバーサルクライアントとゾーンのペアを作成します。

a) トラバーサルクライアントとゾーンペアを作成する手順については、『*Expressway* 基本設定ガイド』を参照してください。

ステップ 4 Expressway-E をリードするトラバーサル クライアント ゾーンにフォールバック検索ルールを作成します。

a) Expressway-C から、**[設定（Configuration）]** > **[ダイヤル プラン（Dial Plan）]** > **[検索ルール（Search rules）]** に移動し、**[新規（New）]** をクリックします。

b) 次のフィールドを設定します。

フィールド名	値
ルール名（Rule Name）	検索ルールを簡単に識別するためのルール名（たとえば、**WebexVideoMesh-Failover**）を入力します。
優先度（Priority）	100 がデフォルトです。Video Mesh のダイヤルパターンおよびB2Bルールより高い数値を入力して、優先順位が低いことを確認します。
プロトコル（Protocol）	**SIP**
モード（Mode）	**Any Alias**
パターン動作（Pattern behavior）	**変更なし（Leave）**
正常に一致する場合（On successful match）	**続行（Continue）**
ターゲット（Target）	Expressway-E をリードするトラバース クライアント ゾーンを選択します。

c) その他のフィールドはデフォルト設定のままにし、変更を保存します。

ステップ 5 Expressway-E から、**[設定（Configuration）] > [ゾーン（Zones）] > [ゾーン（Zones）]** に移動します。**[新規（New）]** をクリックして、Webex Zone を追加します。

X8.11 より前のバージョンでは、この目的のために新しい DNS ゾーンを作成しました。

ステップ 6 クラウド Expressway のダイヤルパターンを作成します。

a) Expressway-E から、**[設定（Configuration）] > [ダイヤル プラン（Dial Plan）] > [検索ルール（Search rules）]** に移動し、**[新規（New）]** をクリックします。

b) 次のフィールドを設定します。

フィールド名	値
ルール名（Rule Name）	検索ルールを簡単に識別するためのルール名（たとえば、**WebexVideoMesh-toCloud**）を入力します。
優先度（Priority）	ローカルの Video Mesh ノードのルールより大きい値を入力してください。ノードが 100 に設定されている場合、この値を **101** に設定します。また、その値が Expressway のすべてのB2Bルールより低いことも確認する必要があります。
プロトコル（Protocol）	**SIP**
ソース（Source）	**指定（Named）**
ソース名（Source Name）	**WebexVideoMeshZone** などのセキュア トラバーサル サーバー ゾーンを選択します。

フィールド名	値
モード（Mode）	**エイリアスのパターンマッチ（Alias pattern match）**
パターンタイプ（Pattern type）	**Regex**
パターン文字列（Pattern string）	**.*@(YourSite\.)?webex\.com.***
パターン動作（Pattern behavior）	**変更なし（Leave）**
正常に一致する場合（On successful match）	**停止（Stop）**
ターゲット（Target）	Webex Zone または DNS ゾーンを選択します。

ステップ 7 Expressway-C に登録されている SIP デバイスの場合、ブラウザでデバイスの IP アドレスを入力し、**[セットアップ（Setup）]** に移動し、**[SIP]** にスクロールして、**[タイプ（Type）]** ドロップダウンから **[標準（Standards）]** を選択します。

Unified CM と Video Mesh ノード間での証明書チェーンの交換

証明書交換を完了して、Unified CM と Video Mesh インターフェイス間の双方向の信頼を確立します。証明書は、安全なトランク設定を使用し、組織内の暗号化された SIP トラフィックと SRTP メディアが、信頼できる Unified CM から信頼できる Video Mesh ノードに到達することを許可します。

（注） クラスタ化された環境では、CA とサーバー証明書を各ノードにインストールする必要があります。

始める前に

セキュリティ上の理由から、ノードのデフォルトの自己署名証明書の代わりに、Video Mesh ノードで CA 署名付き証明書を使用することをお勧めします。

手順

ステップ 1 Web ブラウザで Video Mesh ノードインターフェイス（IP アドレス/セットアップ、例：`https://192.0.2.0/setup`）を開き、そのノードの管理者ログイン情報でサインインします。

ステップ 2 **[サーバー証明書（Server Certificates）]** に移動し、必要に応じて証明書とキーのペアをリクエストおよびアップロードします。

a) （オプション）認定プロバイダーから発行された証明書が必要な場合は、**[証明書署名要求の作成（Create a Certificate Signing Request）]** をクリックします。必要な情報（共通名を含む必要がある FQDN である**サブジェクト代替名**を含む）を入力し、リクエストを作成します。CSR をダウンロードし、リクエストをプロバイダーに送信します。（リクエストは複数可能です。これらは、認証局（CA）の署名付き証明書（CSR の作成中にすでに生成された秘密キー）を返します

（注） 共通名は URL ではありません。プロトコル（http:// や https:// など）、ポート番号、またはパス名は含まれません。X.509 証明書仕様の `commonName` フィールドは、共通名を表します。`https://www.example.com` の場合、正しい値は `example.com` です。

秘密キーは、CSR を生成したときにすでに配置されています。CSR の作成手順を使用しない場合、秘密キーをアップロードする必要があります。

b) 証明書とキーを有している場合、**[サーバー証明書のアップロード（.crt または .pem ファイル）（Upload a Server Certificate（.crt or .pem file））]** をクリックし、証明書ファイルを選択して、**[秘密キーのアップロード（.key ファイル）（Upload a Private Key（.key file））]** をクリックし、パスフレーズがある場合はパスフレーズを入力します。

c) 証明書を取得したら、クラスタ内の最初の Video Mesh ノードに移動し、**[サーバー証明書のインストール（Install Server Certificate）]** をクリックし、プロンプトを読み、**[インストール（Install）]** をクリックして **[OK]** をクリックします。

クラウドに登録された Video Mesh ノードは正常にシャットダウンし、通話が終了するまで最大 2 時間待機します。その後、ノードは証明書のインストールを完了します。サーバー証明書がインストールされると、プロンプトが表示されます。その後、ページをリロードして、新しい証明書とキーエントリを表示できます。

d) 証明書とキーファイルの横にある **[ダウンロード（Download）]** をクリックして、ローカルコピーを保存します。

ファイルを覚えやすい場所に保存し、ブラウザタブで、Video Mesh インスタンスを開いたままにしておきます。

e) クラスタ内の次の Video Mesh ノードに移動し、パスフレーズを入力して、秘密キーファイルをアップロードします。その後、**[サーバー証明書のアップロード（Upload a Server Certificate）]** をクリックし、**[サーバー証明書のインストール（Install Server Certificate）]** を選択し、プロンプトを読み、**[インストール（Install）]** をクリックして **[OK]** をクリックします。

f) 同じクラスタ内の Video Mesh ノードについて、この手順を繰り返します。

ステップ 3 別のブラウザタブで、Cisco Unified OS の管理から、**[セキュリティ（Security）]** > **[証明書の管理（Certificate Management）]** に移動します。検索条件を入力して **[検索（Find）]** をクリックし、証明書または証明書信頼リスト(CTL)のファイル名を選択して **[ダウンロード（Download）]** をクリックします。

Unified CM ファイルを覚えやすい場所に保存し、ブラウザタブで、 Unified CM インスタンスは開いたままにしておきます。

ステップ 4 Video Mesh [ノードインターフェイス（Node Interface）] タブに戻り、**[信頼ストアおよびプロキシ（Trust Store & Proxy）]** をクリックして、オプションを選択します。

- Unified CM がよく知られた組織によって署名された CA 証明書を使用する場合、Video Mesh ノードはそれを自動的に信頼します。信頼は、定期的に更新される VMN ノードのホスト OS からのルート証明書のリストに基づいています。
- Unified CM が内部の企業 CA ルート証明書で署名された CA 証明書を使用する場合、そのルート証明書をノードに追加します。このルート証明書は企業内から入手できますが、Unified CM からダウンロードできない場合があります。
- Unified CM が外部要求を処理するために使用する ECDSA 証明書と RSA 証明書の両方を追加します。これらの証明書は、自己署名証明書または CA 証明書です。
- 1 つの証明書をダウンロードした場合は、**[ルート証明書またはエンドエンティティ証明書のアップロード（.crt または .pem ファイル）（Upload a Root Certificate or End Entity Certificate（.crt or .pem file））]** をクリックし、ダウンロードした CallManager.pem 証明書ファイルを選択します。**[すべての証明書を信頼ストアにインストール（Install All Certificates into the Trust Store）]** をクリックし、プロンプトを読み、**[インストール（Install）]** をクリックして、ノードを再起動します。
- 証明書チェーンをダウンロードした場合は、ルート CA 証明書と中間 CA 証明書をアップロードし、**[すべての証明書を信頼ストアにインストール（Install All Certificates into the Trust Store）]** をクリックし、プロンプトを読んで **[インストール（Install）]** をクリックします。

クラウドに登録された Video Mesh ノードは正常にシャットダウンし、通話が終了するまで最大 2 時間待機します。CallManager.pem 証明書をインストールするには、ノードが自動的に再起動します。オンラインに戻ると、CallManager.pem 証明書が Video Mesh ノードにインストールされている場合にはプロンプトが表示されます。その後、ページをリロードして新しい証明書を表示できます。

ステップ 5 [Cisco Unified OS の管理（Cisco Unified OS Administration）] タブに戻り、**[証明書/証明書チェーンのアップロード（Upload Certificate/Certificate Chain）]** をクリックします。**[証明書の目的（Certificate Purpose）]** ドロップダウンリストから証明書名を選択し、Video Mesh ノードインターフェイスからダウンロードしたファイルを参照して、**[開く（Open）]** をクリックします。

ステップ 6 ファイルをサーバーにアップロードするには、[ファイルのアップロード（Upload File）] をクリックします。

証明書チェーンをアップロードしている場合は、チェーン内のすべての証明書をアップロードする必要があります。

（注） 証明書をアップロードしたら、影響を受けるサービスを再起動します。サーバーが再起動したら、CCMAdmin または CCMUser GUI にアクセスして、新しく追加した証明書が使用されていることを確認できます。

（注） API を使用してサーバー証明書をインストールおよび管理できます。詳細については、「VMN サーバー証明書 API （74 ページ）」を参照してください。

組織およびVideo Meshクラスタのメディア暗号化の有効化

組織および個々のVideo Mesh クラスタのメディア暗号化をオンにする場合は、次の手順を実行します。この設定では、エンドツーエンドの TLS セットアップが強制的に実行され、Video Mesh ノードをポイントするセキュアな TLS SIP トランクが Unified CM に配置されている必要があります。

設定	結果
Unified CM は安全なトランクで設定されており、このVideo Mesh Control Hub 設定は有効になっていません。	コールが失敗します。
Unified CM は安全なトランクで設定されておらず、このVideo Mesh Control Hub 設定は有効になっています。	コールは失敗しませんが、非セキュアモードにフォールバックします。

注意 シスコのエンドポイントには、エンドツーエンドの暗号化が動作するように、セキュリティプロファイルと TLS ネゴシエーションを設定する必要があります。この設定を行わない場合、TLS を使用して設定されていないエンドポイントからクラウドにコールがオーバーフローします。すべてのエンドポイントが TLS を使用するように設定できる場合にのみ、この機能を有効にすることをお勧めします。

始める前に

- Unified CM セキュア TLS SIP トラフィックルーティングの設定 - Video Mesh （96 ページ）
- Unified CM と Video Mesh ノード間での証明書チェーンの交換 （108 ページ）

手順

ステップ 1 https://admin.webex.com のカスタマービューで、**[サービス（Services）]** > **[ハイブリッド（Hybrid）]** に移動し、Video Mesh カードの **[設定（Settings）]** をクリックします。

ステップ 2 **[メディア暗号化（Media Encryption）]** までスクロールし、設定をオンに切り替えます。

この設定により、組織内の Video Mesh ノードを通過するすべてのメディアチャネルで暗号化が強制されます。コールが失敗する可能性がある状況や、エンドツーエンドの暗号化が動作するために必要な要件については、前の表および注意を参照してください。

ステップ 3 **[すべて表示（Show all）]** をクリックし、セキュアな SIP トラフィックを有効にする各 Video Mesh クラスタで、次の手順を繰り返します。

a) リストにある Video Mesh クラスタエントリを選択して、**[クラスタ設定の編集（Edit cluster settings）]** をクリックします。

b) **[SIP コール（SIP Calls）]** までスクロールし、チェックボックスをオンにします。

c) **[信頼済み SIP 送信元（Trusted SIP sources）]** で、Unified CM 証明書のサブジェクト代替名（通常は Unified CM の FQDN）に存在する共通名（CN）または FQDN を入力します。

これらのエントリは信頼済み SIP 送信元として識別され、セキュアな SIP コールを Webex Video Mesh に送信することが許可されます。

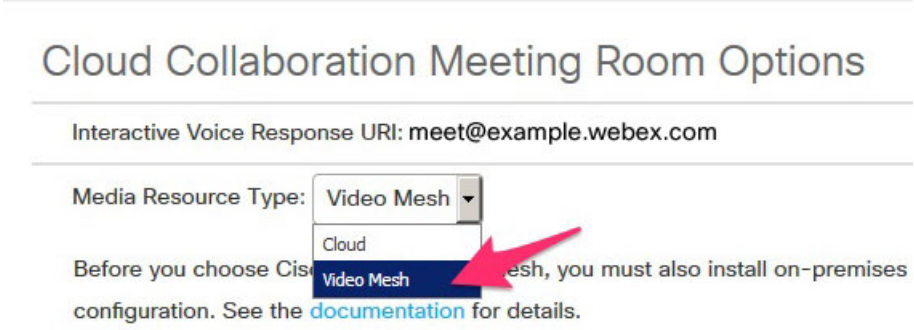
Webex サイトの Video Mesh の有効化

Webex ミーティングの Video Mesh ノードに最適化されたメディアを使用して、すべての Webex アプリとデバイスに参加するには、この設定を Webex サイトで有効にする必要があります。この設定を有効化することによって、クラウドで Video Mesh およびミーティングインスタンスが一緒にリンクされ、カスケードが Video Mesh ノードで発生できるようになります。この設定が有効になっていない場合、Webex アプリとデバイスは Webex ミーティングに Video Mesh ノードを使用しません。

手順

ステップ 1 https://admin.webex.com のカスタマービューで、**[サービス（Services）]** > **[ミーティング（Meetings）]** に移動し、ミーティングカードで Webex サイトをクリックし、**[設定（Settings）]** をクリックすると、Webex サイト設定オプションにアクセスできます。

ステップ 2 **[共通設定（Common Settings）]** にアクセスするには、**[サービス（Service）]** > **[ミーティング（Meeting）]** > 、**[サイト設定（Site Settings）]** の順にクリックします。**[共通設定（Common Settings）]** から、**[Cloud Collaboration Meeting Rooms（CMR）]** をクリックして、**[メディアリソースの種類（Media Resource Type）]** で **[Video Mesh]** を選択し、下部にある **[保存（Save）]** をクリックします。



この設定によって、クラウドで Video Mesh およびミーティングインスタンスが一緒にリンクされ、カスケードが Video Mesh ノードで発生できるようになります。この設定は、15 分後に環境全体に反映されます。 この変更が反映された後に開始される Webex ミーティングでは、新しい設定が適用されます。このフィールドをデフォルトのオプションである [クラウド（Cloud）]に設定したままにすると、クラウドでホストされているすべてのミーティングおよび Video Mesh ノードは使用されなくなります。

Webex アプリ ユーザーへの Collaboration Meeting Rooms の割り当て

手順

- Control Hub を使用してサイトを管理する場合は、次のようにします。
  a) https://admin.webex.com のカスタマー ビューから、**[ユーザー（Users）] > [ユーザーの管理（Manage Users）]** に移動します。

     複数のユーザーをまとめて割り当てるには、この文書を参照してください。

  b) **Webex Collaboration Meeting Rooms** を組織内のユーザーに割り当てます。
- サイト管理者を使用してサイトを管理する場合は、次のようになります。
  a) [サイト管理（Site Admin）]から、**[ユーザーの管理（Manage Users）]** に移動します。
  b) ユーザーアカウントを編集し、Collaboration Meeting Room をオンにします。

     複数のユーザーをまとめて割り当てるには、この文書を参照してください。

セキュアなエンドポイントでのミーティングエクスペリエンスの確認

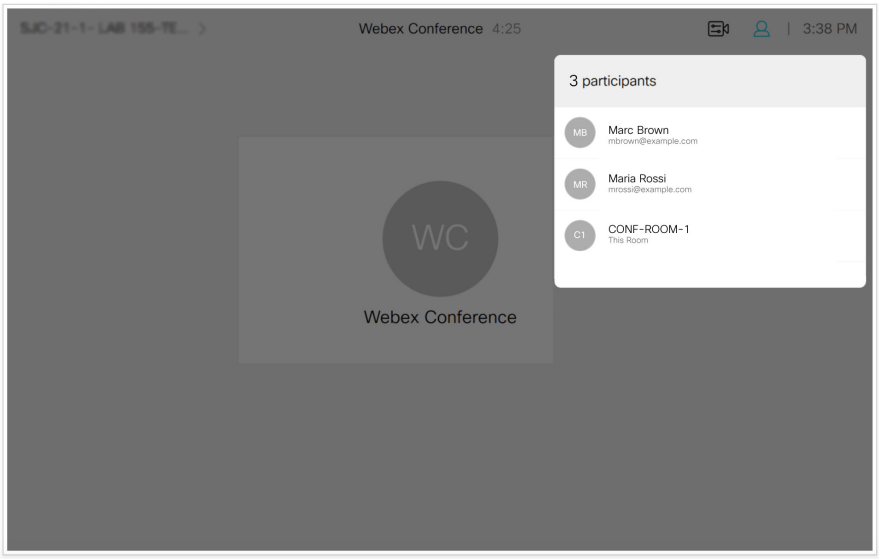
エンドポイントが安全に登録され、正しいミーティングエクスペリエンスが表示されていることを確認するには、以下の手順を実行します。

手順

ステップ 1 セキュリティ保護されたエンドポイントからミーティングに参加します。

ステップ 2 ミーティングの名簿がデバイスに表示されることを確認します。

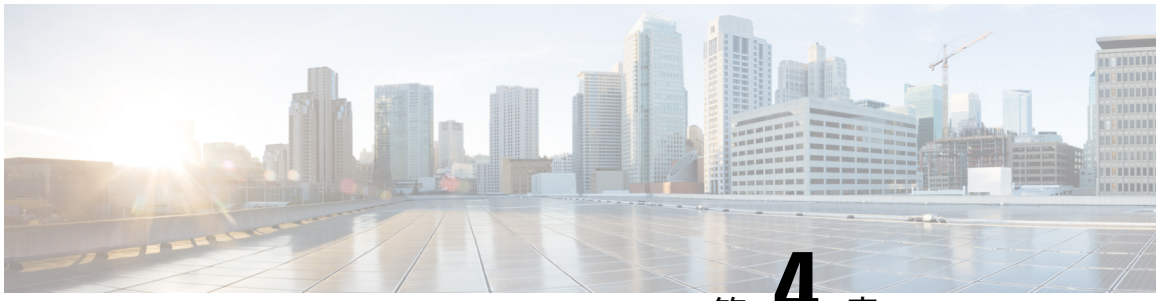
この例は、タッチパネルを使用するエンドポイントでミーティングリストがどう見えるかを示しています。



ステップ 3 ミーティング中、**[コールの詳細（Call Details）]** から Webex Conference の情報にアクセスします。

ステップ 4 [暗号化（Encryption）] セクションで、**[タイプ（Type）]** が **[AES-128]** として表示され、**[ステータス（Status）]** が **[オン（On）]** として表示されていることを確認します。


Webex Conference
Participant(s)
URL
Call rate
6000 kbps
Encryption
Type
AES-128
Status
On
Video
Transmit
Presentation
Receive
Presentation
Protocol
H264
N/A
H264
N/A
Resolution
1280x720
N/A
1280x720
N/A
Frame rate
30 fps
N/A
30 fps
N/A
Channel rate
2484 kbps
N/A
759 kbps
N/A
Total packet loss (%)
0.0%
0.0%
Current packet loss (...
0.0%
0.0%
Jitter
1 ms
3 ms
Audio
Transmit
Receive
Protocol
AACLD
Opus
Channel rate
63 kbps
64 kbps
Total packet loss (%)
0.0%
0.0%
Current packet loss (...
0.0%
0.0%
Jitter
1.00 ms
4.00 ms



第 4 章

Video Meshの管理とトラブルシューティング

Video Mesh 分析

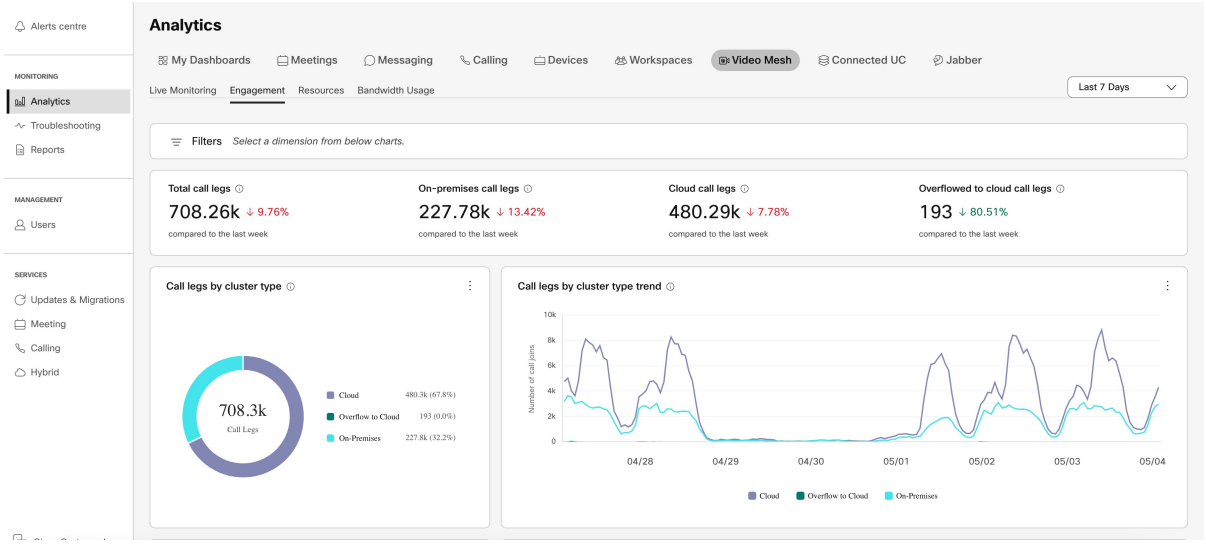
分析は、Webex 組織内でのオンプレミス Video Mesh ノードおよびクラスタの使用方法に関する情報を提供します。メトリックビューの履歴データを使用すると、オンプレミスリソースのキャパシティ、使用率、および可用性をモニタリングすることによって、Video Mesh リソースをより効果的に管理できます。この情報を使用して、クラスタへの Video Mesh ノードの追加や新しいクラスタの作成などの判断を行うことができます。Video Mesh 分析は、Control Hub の **[分析（Analytics）]** > **[Video Mesh]** で確認できます。

組織内のデータの分析に役立てるため、グラフ上のデータを拡大し、特定の期間だけを分離できます。分析のために、レポートをより多角的に分析して、さらにきめ細かな詳細を表示することもできます。

（注） Video Mesh分析およびトラブルシューティングレポートには、ローカルブラウザに設定されているタイムゾーンでデータが表示されます。

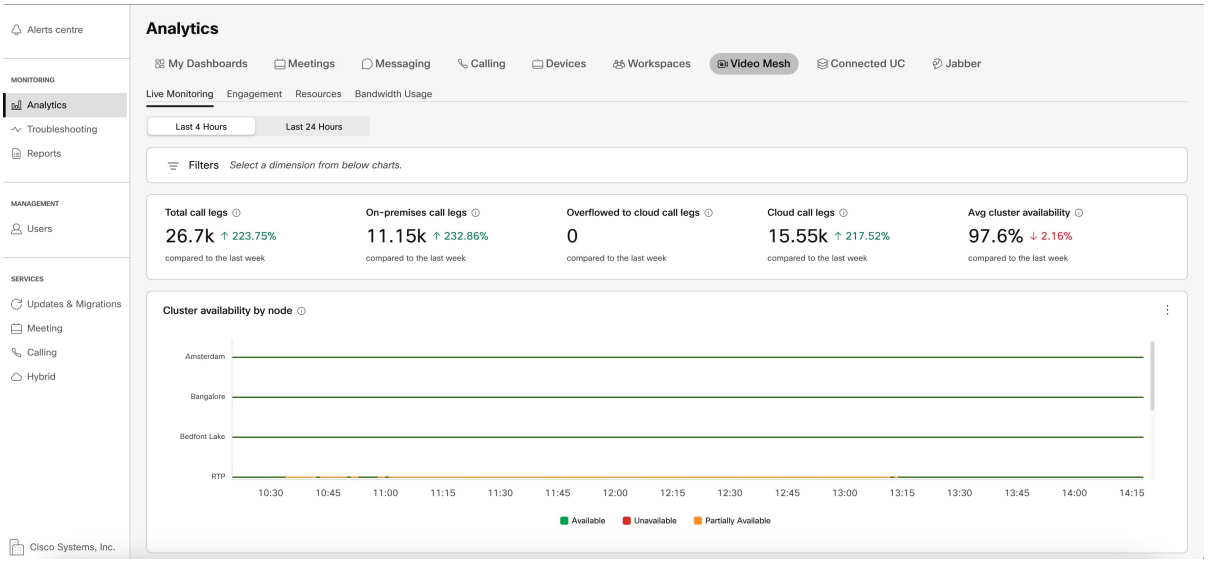
分析

Video Mesh 分析によって、関与、リソースの使用状況、および帯域幅の使用状況のカテゴリにおける長期（最大 3 ヵ月分のデータ）の傾向が示されます。



ライブ モニタリング

ライブモニタリングタブは、組織内のアクティビティについてほぼリアルタイムのビューを提供します（最大 1 分間の集約と、すべてのクラスタまたは特定のクラスタで過去 4 時間または 24 時間を表示する機能）。Control Hub のページが自動的に更新されます（過去 4 時間は 1 分ごとに、過去 24 時間は 10 分ごとに更新されます）。



Video Mesh のライブモニタリングレポートにアクセス、フィルタ処理、保存する

Video Mesh がアクティブで、少なくとも 1 つの Video Mesh ノードが登録されているクラスタがある場合、Video Mesh のライブモニタリングレポートを Control Hub（https://admin.webex.com）の [分析（Analytics）] ページで利用できます。

手順

ステップ 1 https://admin.webex.com の [カスタマー（Customer）] ビューで、**[分析（Analytics）]** を選択し、画面の右上にある **[Video Mesh]** をクリックします。

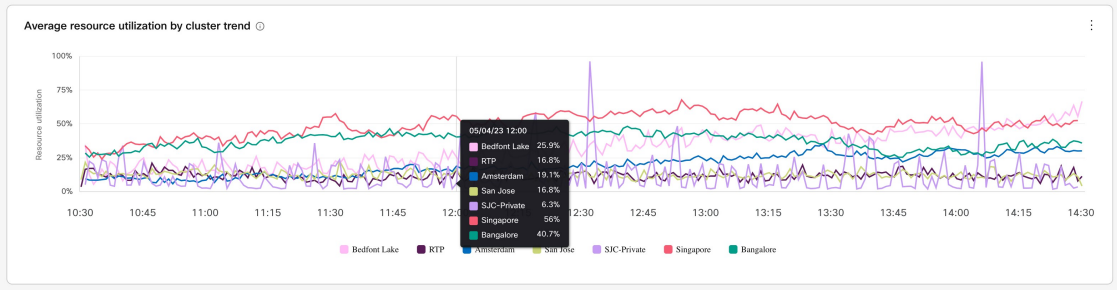
ヒント 情報 ⓘ をホバーすると、チャートの簡単な説明が表示されます。

ステップ 2 左側のトグルから、データを表示する過去の期間をフィルタ処理するオプションを選択します。

- **過去 4 時間（Last 4 Hours）**（デフォルト）—このオプションを選択すると、グラフデータは 1 分ごとに更新されます。
- **過去 24 時間（Last 24 Hours）**—このオプションを選択すると、グラフデータは 10 分ごとに更新されます。

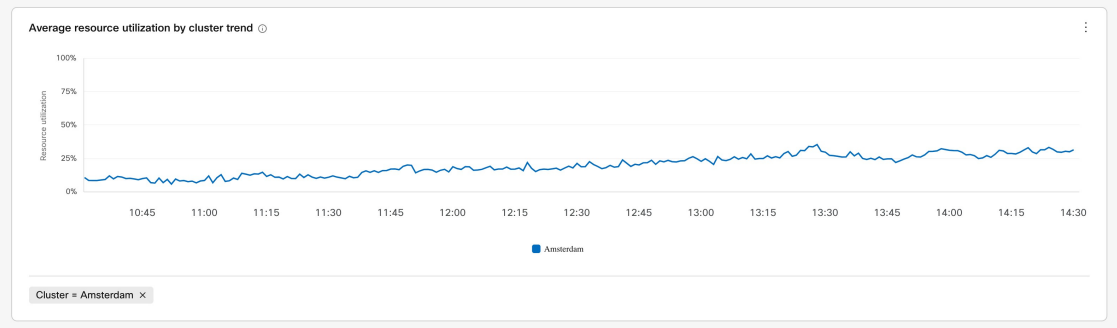
ステップ 3 必要に応じて、次のオプションを使用してチャートを操作します。

- チャートビューのセグメントの上でホバーすると、特定のデータポイントに関する情報が表示されます。

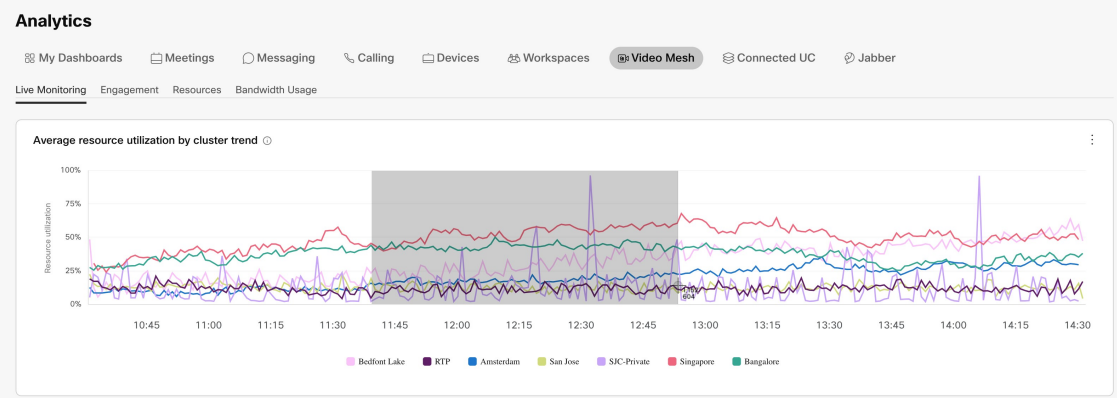


- グラフ上の凡例項目または概要をクリックし、**[適用（Apply）]** をクリックすると、その他の凡例項目のビューが更新されます。たとえば、アムステルダムの凡例項目を選択すると、折れ線グラフが更新され、その他の凡例項目を除外し、選択した項目のデータだけが含まれます。

（注） フィルタを適用すると、他のすべてのグラフとチャートが更新され、選択したフィルタのデータが表示されます。



- 時間範囲のデータを表示するグラフで、左側をクリックし、マウスを右方向にドラッグして、特定の時間範囲に絞り込みます。（このアクションは、分析ページに表示されるすべての関連データに影響します。）



ヒント ドーナツグラフ、グラフ上の折れ線、またはグラフ上のインサイトポイントのセクションをホバーすると、データの特定の時点に関する詳細が表示されます。

ステップ 4 レポートのデータをフィルタ処理した後で、さらに... をクリックし、レポートのローカルコピーを保存してオフラインで（たとえば、内部的に作成されたレポートで）使用できるよう、ファイル形式オプションを選択します。

- **PNG**
- **PDF**
- **CSV**

Video Mesh 分析へのアクセス、フィルタ処理、および保存

Video Mesh がアクティブで、少なくとも 1 つの Video Mesh ノードが登録されているクラスタがある場合、Video Mesh のメトリックレポートを Control Hub（https://admin.webex.com）の [分析（Analytics）] ページで利用できます。

手順

ステップ 1 https://admin.webex.com の [カスタマー（Customer）] ビューで、**[分析（Analytics）]** を選択し、画面の右上にある **[Video Mesh]** をクリックします。

ステップ 2 探しているデータの種類に応じて、カテゴリをクリックします。

- **エンゲージメント**
- **関連資料**
- **帯域幅使用率**

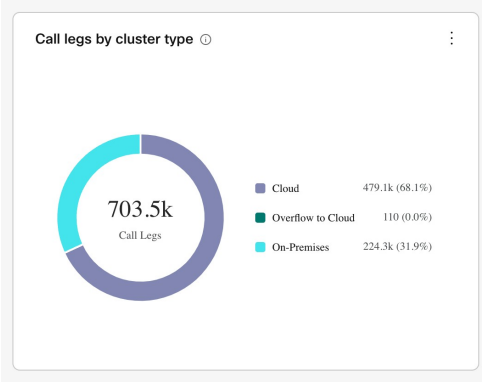
ヒント　情報 ⓘ をホバーすると、ドーナツグラフまたはチャートの簡単な説明が表示されます。

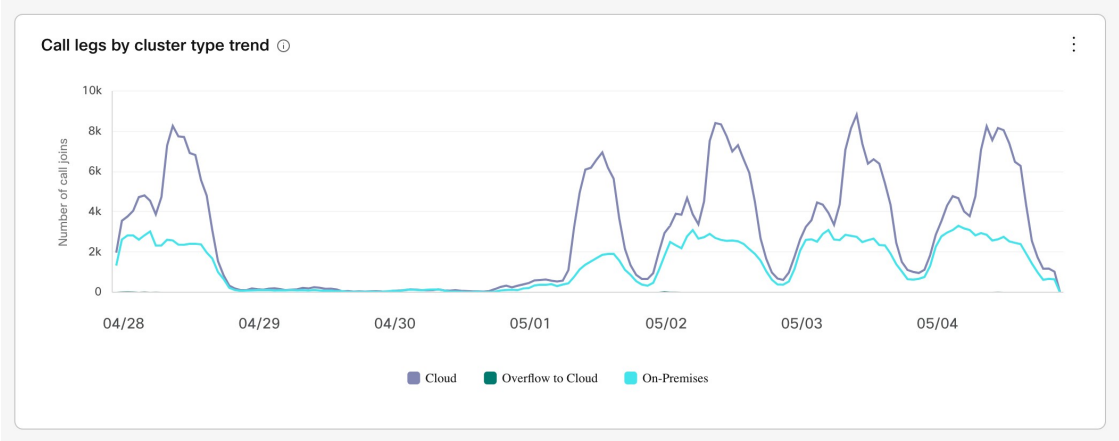
ステップ 3 右側のドロップダウンリストから、データを表示する過去の期間をフィルタ処理するオプションを選択します。

- **過去 7 日間（Last 7 Days）**（デフォルト）：横軸を 1 時間ごとに変更します。
- **過去 24 時間（Last 24 Hours）**：横軸を 10 分ごとに変更します。
- **過去 30 日間（Last 30 Days）**：横軸を 3 時間ごとに変更します。
- **過去 90 日間（Last 90 Days）**：横軸を 8 時間ごとに変更します。

ステップ 4 必要に応じて、次のオプションを使用してチャートまたはドーナツグラフを操作します。

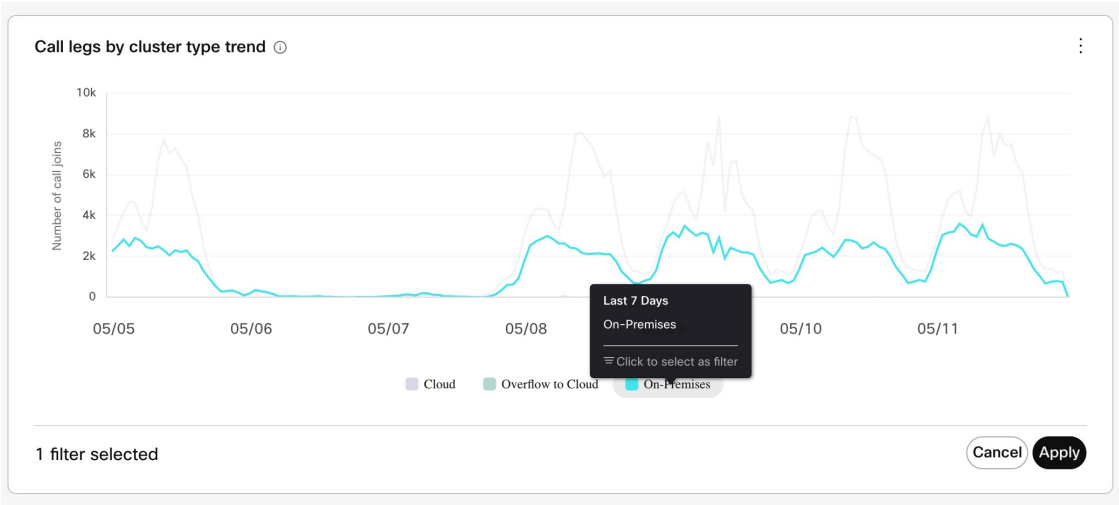
- ドーナツグラフまたはチャートビューで 1 つ以上のセグメントをクリックし、**[適用（Apply）]** をクリックして、そのドーナツビューと対応するチャートビューを更新します。

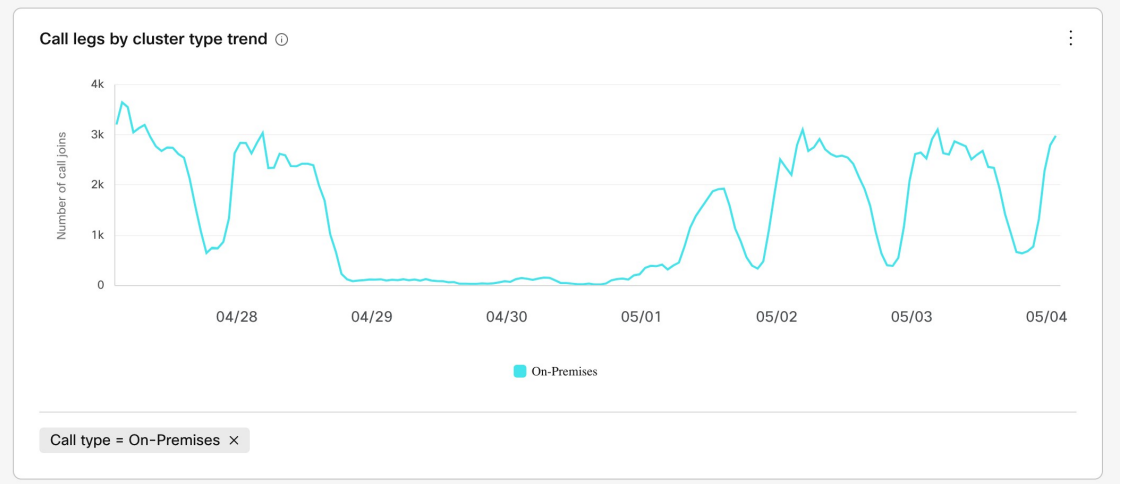




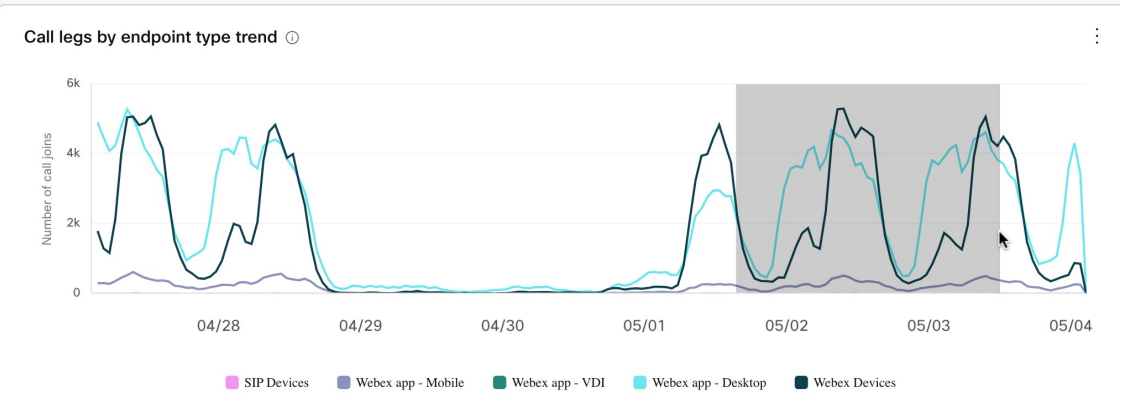
- グラフ上の凡例項目または概要を選択して、その特定の凡例項目のビューを更新し、**[適用（Apply）]**をクリックします。たとえば、[オンプレミス（On-Premises）]の凡例項目を選択すると、そのデータが強調表示された折れ線グラフが更新されます。

（注） フィルタを適用すると、他のすべてのグラフとチャートが更新され、選択したフィルタのデータが表示されます。





- 時間範囲のデータを表示するグラフで、左側をクリックし、マウスを右方向にドラッグして、希望の範囲が選択されたらその場を離れることで、特定の時間範囲に絞り込みます。（このアクションは、分析ページに表示されるすべての関連データに影響します。）

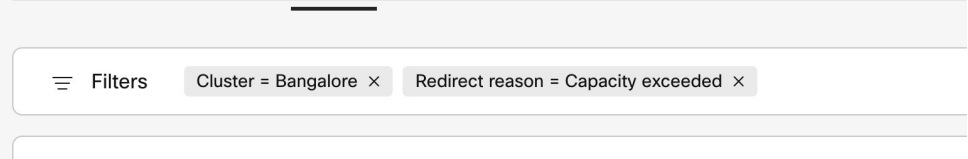


ヒント ドーナツグラフ、グラフ上の折れ線、またはグラフ上のインサイトポイントのセクションをホバーすると、データの特定の時点に関する詳細が表示されます。

（注） 同じグラフまたは概要内から最初からやり直すには、グラフの下部にある選択したフィルタの [X] をクリックします。

ステップ 5 レポートのデータをフィルタ処理した後で、さらに...をクリックし、レポートのローカルコピーを保存してオフラインで（たとえば、内部的に作成されたレポートで）使用できるよう、ファイル形式オプションを選択します。

- **PDF**
- **PNG**
- **CSV**



ステップ 6 分析ビューをリセットする場合は、フィルタバーからすべてのフィルタをクリアします。

Video Meshで利用可能な分析

Control Hub で利用可能な分析の詳細については、「クラウド コラボレーション ポートフォリオの分析」の「Video Mesh 」セクションを参照してください。

Video Mesh用のモニタリングツール

Control Hub のモニタリングツールは、組織が Video Mesh 展開の正常性をモニタリングするのに役立ちます。Video Mesh ノード、クラスタ、またはその両方で次のテストを実行して、特定のパラメータの結果を取得できます。

- **シグナリングテスト（Signaling Test）** ：Video Mesh ノードと Webex クラウドメディアサービスの間で SIP シグナリングとメディアシグナリングが発生するかどうかをテストします。
- **カスケードテスト（Cascade Test）** ：Video Mesh ノードと Webex クラウドメディアサービス間でカスケードを確立できるかどうかをテストします。
- **到達可能性テスト（Reachability Test）** ：Video Mesh ノードが Webex クラウドメディアサービスのメディアストリームの宛先ポートに到達できるかどうかをテストします。また、Video Mesh ノードがこれらのポートを介してメディアコンテナに関連付けられたクラウドクラスタと通信できるかどうかもテストします。

テストを実行すると、シミュレーションされたミーティングがツールによって作成されます。テストが終了すると、単純な合格または失敗の結果が表示され、レポートにはトラブルシューティングのヒントがインラインで含まれます。定期的なテストをスケジュール設定したり、オンデマンドでのテストをスケジュール設定したりできます。詳細については、「Video Mesh のメディアヘルスモニタリング」を参照してください。

即座のテストの実行

Control Hub 組織に登録されているクラスタ内にあるすべての Video Mesh ノードでオンデマンドのメディア ヘルス モニタリング テストと到達可能性テストを実行する場合は、この手順を使用します。結果は Control Hub でキャプチャされ、00:00 UTC から 6 時間ごとに集約されます。

手順

ステップ 1 Control Hubにログインし、**[トラブルシューティング（Troubleshooting）]** > **[Video Mesh]** に移動します。

ステップ 2 **[テストの設定（Configure Test）]** をクリックし、**[今すぐテスト（Test now）]** をクリックして、テストするノードやクラスタを確認します。

（注） チェックボックスをオフにして最後の設定を復元する場合は、**[最後のテスト設定の復元（Restore last test configuration）]** をクリックします。

ステップ 3 **[テストを実行（Run Test）]** をクリックします。

次のタスク

結果は、Control Hub のモニタリングツールの概要のページに表示されます。デフォルトでは、すべてのテストの結果がまとめて表示されます。**[シグナリング（Signaling）]**、**[カスケード（Cascade）]**、または **[到達可能性（Reachability ）]** をクリックして、特定のテストに従って結果をフィルタリングします。

スライダ付きのタイムライン上のポイントは、組織全体の集約されたテスト結果を示します。クラスタレベルのタイムラインには、各クラスタの集約結果が表示されます。

（注） タイムラインには、米国形式で日付が表示される場合があります。プロファイル設定で言語を変更して、ローカル形式で日付を表示します。

テスト結果を表示するには、タイムライン上のポイントをホバーします。各ノードのテスト結果の詳細も確認できます。クラスタレベルのタイムライン上のポイントをクリックすると、詳細な結果が表示されます。

結果はサイドパネルに表示され、シグナリング、カスケード、および到達可能性に分割されます。テストが成功したか、スキップされたか、テストが失敗したかを確認できます。修正可能なエラーコードも結果とともに表示されます。

提供されているトグルを使用して、さまざまなパラメータの成功率を表形式で表示します。

（注） スキップされたテスト、部分的な失敗、または失敗は、一定期間にわたって継続的に発生しない限り、重大ではありません。

定期テストの構成

定期的なメディア ヘルス モニタリング テストと到達可能性のテストを設定および開始するには、次の手順を使用します。これらのテストは6時間ごとにデフォルトで実行されます。これらのテストは、クラスタ全体、クラスタ固有、またはノード固有のレベルで実行できます。結果は Control Hub でキャプチャされ、00:00 UTC から 6 時間ごとに集約されます。

手順

ステップ 1 Control Hubにログインし、**[トラブルシューティング（Troubleshooting）]** > **[Video Mesh]** に移動します。

ステップ 2 **[テストの設定（Configure Test）]** をクリックし、**[定期テスト（Periodic test）]** をクリックして、テストするノードやクラスタを確認します。

ステップ 3 次のオプションを選択します。

- Control Hub 組織にあるすべての Video Mesh ノードでテストを実行する場合は、**[すべてのクラスタ（All Clusters）]** のチェックをオンにします。
- 特定のクラスタ内にあるすべての Video Mesh ノードでテストを実行する場合は、個々のクラスタ名のチェックをオンにします。チェックがオフになっているクラスタは、テストから除外されます。
- 個々のクラスタ内で、テストを実行する個々のノード名を確認します。チェックがオフになっているノードは、テストから除外されます。

ステップ 4 **[次へ（Next）]** をクリックします。

ステップ 5 定期テストを実行するクラスタとノードの一覧を確認します。問題なければ、**[設定（Configure）]** をクリックして現在の設定のスケジュールを設定します。

次のタスク

結果は、Control Hub のモニタリングツールの概要のページに表示されます。デフォルトでは、すべてのテストの結果がまとめて表示されます。**[シグナリング（Signaling）]**、**[カスケード（Cascade）]**、または **[到達可能性（Reachability ）]** をクリックして、特定のテストに従って結果をフィルタリングします。

スライダ付きのタイムライン上のポイントは、組織全体の集約されたテスト結果を示します。クラスタレベルのタイムラインには、各クラスタの集約結果が表示されます。

（注） タイムラインには、米国形式で日付が表示される場合があります。プロファイル設定で言語を変更して、ローカル形式で日付を表示します。

テスト結果を表示するには、タイムライン上のポイントをホバーします。各ノードのテスト結果の詳細も確認できます。クラスタレベルのタイムライン上のポイントをクリックすると、詳細な結果が表示されます。

結果はサイドパネルに表示され、シグナリング、カスケード、および到達可能性に分割されます。テストが成功したか、スキップされたか、テストが失敗したかを確認できます。修正可能なエラーコードも結果とともに表示されます。

提供されているトグルを使用して、さまざまなパラメータの成功率を表形式で表示します。

（注） スキップされたテスト、部分的な失敗、または失敗は、一定期間にわたって継続的に発生しない限り、重大ではありません。

Video Mesh ノードミーティングにおけるオンプレミス SIP デバイス用の 1080p HD ビデオの有効化

この設定により、組織は、オンプレミスで登録された SIP エンドポイント向けに 1080p の高解像度ビデオを利用できますが、ミーティングのキャパシティは低下します。Video Mesh ノードがミーティングをホストする必要があります。参加者は、次の条件で 1080p 30fps ビデオを使用できます。

- 全員が企業のネットワーク内にいる。
- オンプレミスの登録済み高解像度対応 SIP デバイスを使用している。

この設定は、Video Mesh ノードが含まれているすべてのクラスタに適用されます。

Note クラウドに登録されたデバイスは、この設定のオン/オフにかかわらず、引き続き 1080p ストリームを送受信します。

Procedure

ステップ 1 https://admin.webex.com のカスタマービューで、**[サービス（Services）]** > **[ハイブリッド（Hybrid）]** に移動し、Video Mesh カードの **[設定（Settings）]** をクリックします。

ステップ 2 **[ビデオ品質（Video Quality）]** をオンに切り替えます。

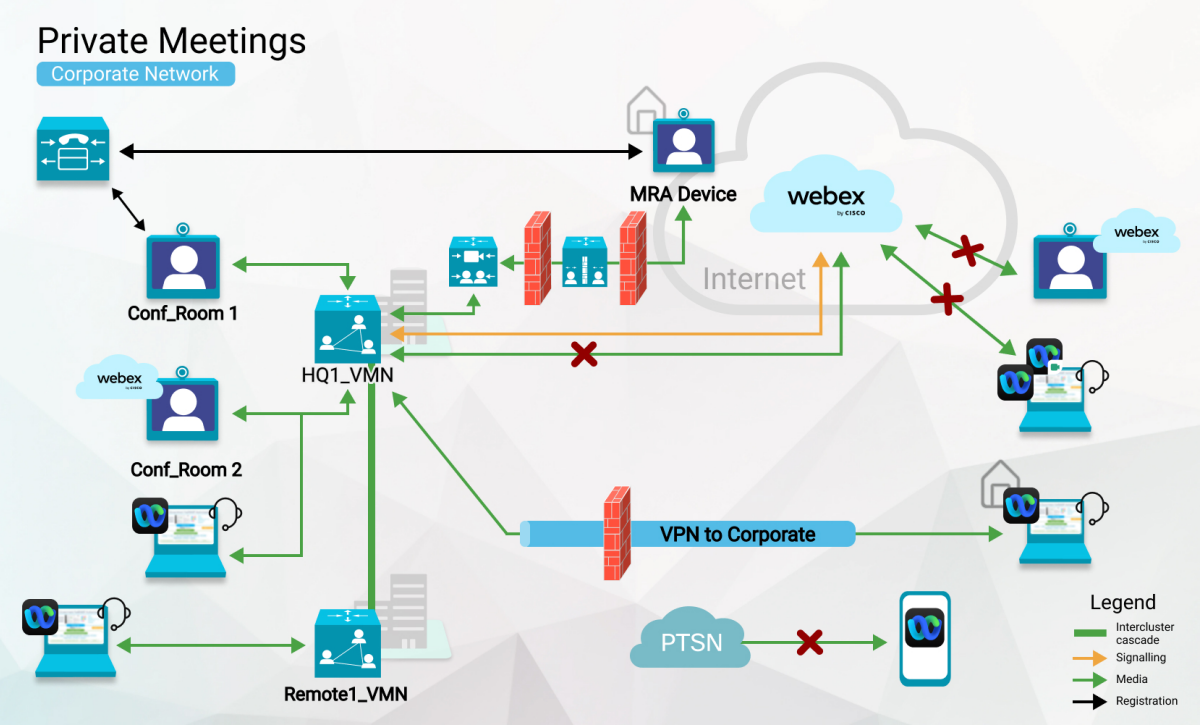
この設定がオフの場合、デフォルトは 720p です。

Webex アプリがサポートするビデオ解像度については、「通話とミーティングのビデオ仕様」を参照してください。

プライベートミーティング

プライベートミーティング機能は、お客様の社内でメディアを終端させることで会議のセキュリティを強化します。プライベート会議のスケジュールを設定すると、メディアは常にクラウドカスケードを使用しない企業のネットワーク内の Video Mesh ノードで終端します。

ここに示すように、プライベートミーティングがクラウドにメディアをカスケードすることはありません。メディアは、Video Mesh クラスタで完全に終端します。Video Mesh クラスタは、相互にのみカスケードできます。



プライベートミーティング用にVideo Meshクラスタを予約できます。予約済みクラスタがいっぱいになると、プライベート ミーティング メディアが他の Video Mesh クラスタにカスケードされます。予約済みクラスタがいっぱいになると、プライベートミーティングと非プライベートミーティングは残りのクラスタのリソースを共有します。

非プライベートミーティングでは予約済みクラスタを使用せず、それらのリソースをプライベートミーティング用に予約します。非プライベートミーティングでネットワーク上のリソースが不足すると、代わりに Webex クラウドにカスケードされます。

（注） フル機能の Webex エクスペリエンスが有効になっている Webex アプリは、Video Mesh と互換性がありません。詳細については、「Video Mesh ノードを使用するクライアントとデバイス（3 ページ）」を参照してください。

プライベート ミーティングのサポートと制限事項

Video Mesh は、次のようにプライベートミーティングをサポートします。

- プライベートミーティングは Webex バージョン 40.12 以降で利用できます。
- プライベート ミーティング タイプを使用できるのは、スケジュールされたミーティングのみです。詳細については、「Cisco Webex プライベートミーティングをスケジュールする」の項目を参照してください。

- プライベートミーティングは、Webex アプリから開始または参加したフル機能のミーティングでは利用できません。
- 現在 Video Mesh がサポートされているデバイスを使用できます。
- ノードは現在のイメージ 72vCPU および 23vCPU を使用できます。
- プライベートミーティングのロジックで、メトリックにギャップが生じることはありません。非プライベートミーティングの場合と同じメトリックを Control Hub で収集します。

（注） 一部のユーザーはこの機能を有効にしていないため、組織で 90 日間プライベートミーティングがない場合、プライベートミーティングの分析レポートは表示されません。

- プライベートミーティングは、ビデオエンドポイントからの一方向ホワイトボーディングをサポートします。

制限事項

プライベートミーティングには次の制限があります。

- プライベートミーティングは、音声の VoIP のみをサポートします。Webex Edge Audio または PSTN はサポートしていません。
- プライベートミーティングにパーソナル ミーティング ルーム（PMR）を使用することはできません。
- プライベートミーティングは、クラウド録音・録画、文字起こし、Webex Assistant など、クラウドへの接続を必要とする Webex 機能をサポートしていません。
- 認証されていないクラウド登録ビデオシステムからプライベートミーティングに参加することはできません。Webex アプリにペアリングされている場合でも同様です。

デフォルトのミーティング タイプとしてプライベート ミーティングを使用する

Control Hub では、組織の将来のスケジュールされたミーティングがプライベートミーティングになるように指定できます。

手順

ステップ 1 https://admin.webex.com のカスタマービューから、**[サービス（Services）]** > **[ハイブリッド（Hybrid）]** に移動します。

ステップ 2 **Video Mesh** カードの **[設定の編集（Edit settings）]** をクリックします。**[プライベートミーティング（Private Meetings）]** までスクロールし、設定を有効にします。

ステップ 3 変更を保存します。

この設定を有効にすると、以前にスケジュールされたものも含め、組織のすべてのミーティングに適用されます。

（オプション）プライベートミーティング用にクラスタを予約する

プライベートミーティングと非プライベートミーティングは、通常、同じ Video Mesh リソースを使用します。ただし、プライベートミーティングではメディアをローカルに保つ必要があるため、ローカルリソースが枯渇したときにクラウドへのオーバーフローを設定することはできません。その可能性を軽減するために、プライベートミーティングのみをホストするように Video Mesh クラスタを設定できます。

Control Hub で、プライベートミーティングのホスト専用にクラスタを構成します。この設定により、非プライベートミーティングがそのクラスタを使用できなくなります。プライベートミーティングでは、デフォルトでそのクラスタが使用されます。クラスタのリソースが不足すると、プライベートミーティングは他の Video Mesh クラスタにのみカスケードされます。

プライベートミーティングから予想されるピーク使用量に対処するために、プライベートクラスタをプロビジョニングすることをお勧めします。

（注） プライベートミーティング用にすべての Video Mesh クラスタを予約する場合、短いビデオアドレス形式（meet@*your_site*）を使用することはできません。これらのコールは現在、適切なエラーメッセージなしで失敗します。一部のクラスタを予約しないままにしておくと、短いビデオアドレス形式のコールはそれらのクラスタを介して接続できます。

手順

ステップ 1 https://admin.webex.com のカスタマービューで、**[サービス（Services）]** > **[ハイブリッド（Hybrid）]** に移動し、Video Mesh カードの **[すべて表示（Show all）]** をクリックします。

ステップ 2 リストで Video Mesh クラスタを選択し、**[クラスタ設定の編集（Edit cluster settings）]** をクリックします。

ステップ 3 **[プライベートミーティング（Private Meetings）]** までスクロールし、設定を有効にします。

ステップ 4 変更を保存します。

プライベートミーティングのエラーメッセージ

この表は、プライベートミーティングに参加するときにユーザーに表示される可能性のあるエラーを示しています。

エラー メッセージ	ユーザアクション	理由
外部ネットワークアクセスが拒否されました プライベートミーティングに参加するには、企業ネットワークに接続している必要があります。企業ネットワークの外部にあるペアリングされた Webex デバイスは、ミーティングに参加できません。このようなシナリオでは、ラップトップ、モバイルを企業ネットワークに接続し、ペアリングされていないモードでミーティングに参加してみてください。	外部ユーザーが、VPN または MRA を使用せずに企業ネットワークの外部から参加しています。	プライベートミーティングに参加するには、外部ユーザーが VPN または MRA を介して企業ネットワークにアクセスする必要があります。
	外部ユーザーは VPN を使用していますが、認証されていないデバイスとペアになっています。	デバイスメディアが、VPN を介して企業ネットワークにトンネリングしていません。そのデバイスはプライベートミーティングに参加できません。 代わりに、VPN に接続した後、リモートユーザーはデスクトップまたはモバイルクライアントから、デバイスのペアリングされていないモードでプライベートミーティングに参加する必要があります。
利用可能なクラスタがありません このプライベートミーティングをホストしているクラスタは、キャパシティがピークに達しているか、到達不能であるか、オフラインであるか、または登録されていません。IT 管理者に連絡してサポートを依頼してください。	ユーザーは企業ネットワーク（オンプレミスまたは VPN によるリモート）にいますが、プライベートミーティングに参加できません。	Video Mesh クラスタが次のいずれかの状態です。 • キャパシティ上限 • 到達不能 • Offline • 登録されていません

エラー メッセージ	ユーザアクション	理由
認可されていません ホスト組織のメンバーではないため、このプライベートミーティングに参加する権限がありません。ミーティングの主催者に連絡してください。	ホスト組織とは異なる組織のユーザーがプライベートミーティングに参加しようとしています。	ホスト組織に属するユーザーのみがプライベートミーティングに参加できます。
	ホスト組織とは異なる組織のデバイスがプライベートミーティングに参加しようとしています。	ホスト組織に属するデバイスのみがプライベートミーティングに参加できます。

すべての外部 Webex Meetings でメディアをVideo Meshに保持する

メディアがローカル Video Mesh ノードを通過すると、パフォーマンスが向上し、使用するインターネット帯域幅が少なくなります。

以前のリリースでは、ミーティングでの Video Mesh 使用の制御は内部サイトのみでした。外部 Webex サイトでホストされているミーティングの場合、それらのサイトは、Video Mesh が Webex にカスケードできるかどうかを制御していました。外部サイトで Video Mesh のカスケードが許可されていない場合、メディアは常に Webex クラウドノードを使用していました。

[すべての外部 Webex ミーティングに Video Mesh を優先（Prefer Video Mesh for All External Webex Meetings）] 設定を使用すると、Webex サイトに使用可能な Video Mesh ノードがある場合、メディアは外部の Webex サイトでホストされたミーティングでそれらのノードを介して実行されます。次の表は、Webex ミーティングに参加する参加者の動作をまとめたものです。

設定が以下の場合...	Video Mesh カスケードが有効になっている内部 Webex サイトでのミーティング	Video Mesh カスケードが無効になっている内部 Webex サイトでのミーティング	Video Mesh カスケードが有効になっている外部 Webex サイトでのミーティング	Video Mesh カスケードが無効になっている外部 Webex サイトでのミーティング
有効（Enabled）	メディアは Video Mesh ノードを使用します。	メディアはクラウドノードを使用します。	メディアは Video Mesh ノードを使用します。	メディアは Video Mesh ノードを使用します。
無効（Disabled）	メディアは Video Mesh ノードを使用します。	メディアはクラウドノードを使用します。	メディアは Video Mesh ノードを使用します。	メディアはクラウドノードを使用します。

この設定はデフォルトでオフになっており、以前のリリースの動作を維持しています。これらのリリースでは、Video Mesh は Webex にカスケードされず、参加者は Webex クラウドノードを介して参加していました。

手順

	コマンドまたはアクション	目的
ステップ 1	https://admin.webex.com のカスタマービューで、**[サービス（Services）]** > **[ハイブリッド（Hybrid）]** に移動し、Video Mesh カードの **[すべて表示（Show all）]** をクリックします。	
ステップ 2	リストで Video Mesh クラスタを選択し、**[設定の編集（Edit settings）]** をクリックします。	
ステップ 3	**[すべての外部 Webex ミーティングに Video Mesh を優先（Prefer Video Mesh for All External Webex Meetings）]** までスクロールし、設定を有効にします。	
ステップ 4	変更を保存します。	

Video Mesh 展開の使用率を最適化する

Video Mesh クラスタにすべてのクライアントを配置して、Video Mesh によるユーザーエクスペリエンスを向上させることができます。Video Mesh クラスタのキャパシティが一時的にダウンしているか、使用率が増加している場合は、Video Mesh クラスタに到達するクライアントタイプを制御することで、Video Mesh クラスタの使用率を最適化できます。これにより、需要を満たすためにノードを追加できるようになるまで、既存のキャパシティを効果的に管理できます。

使用状況、使用率、リダイレクト、オーバーフローの傾向を理解するには、「Control Hub の分析ポータル」を参照してください。これらのトレンドに基づいて、たとえば、デスクトップクライアントまたは SIP デバイスを Video Mesh クラスタに配置し、モバイルクライアントを Webex クラウドノードに配置するように選択できます。モバイルクライアントと比較して、デスクトップクライアントと SIP デバイスはより高い解像度をサポートし、画面もより大きく、より多くの帯域幅を使用するため、これらのクライアントタイプを使用する参加者のユーザーエクスペリエンスを最適化できます。

また、最も多くのお客様が使用するクライアントタイプを Video Mesh クラスタに配置することで、クラスタのキャパシティを最適化し、ユーザーエクスペリエンスを最大化することもできます。

手順

ステップ 1 Control Hub にサインインしてから、**[サービス（Services）]** > **[ハイブリッド（Hybrid）]** > **[Video Mesh]** > **[リソース（Resources）]** > **[すべて表示（View all）]** を選択します。

または

[概要（Overview）] > **[ハイブリッドサービス（Hybrid services）]** > **[Video Mesh]** > **[設定（Settings）]** を選択します。

ステップ 2 **[クライアントタイプの包含設定（Client Type Inclusion Settings）]** では、すべてのクライアントタイプがデフォルトでオンになっています。Video Mesh クラスタの使用から除外するクライアントタイプのチェックをオフにします。これらのクラスタは、Webex クラウドノードでホストされます。

ステップ 3 **[保存（Save）]** をクリックします。

Video Mesh ノードの登録解除

Webex クラウドから Video Mesh ノードを削除するには、次の手順に従います。この手順を完了すると、ノードはクラスタから削除されて使用できなくなります。ノードの登録を解除した後、再度使用できるようにする唯一の方法は、そのノードを再登録することです。

手順

ステップ 1 https://admin.webex.com のカスタマービューから、**[サービス（Services）]** > **[ハイブリッド（Hybrid）]** に移動します。

ステップ 2 Video Mesh カードの **[すべて表示（View all）]** をクリックします。

ステップ 3 リソースのリストから、適切なクラスタに移動し、ノードを選択します。

ステップ 4 **[アクション（Action）]** > **[ノードを登録解除（Deregister node）]** をクリックします。

ノードの削除を確認するよう求めるメッセージが表示されます。

ステップ 5 メッセージを読んで理解してから、**[ノードの登録解除（Deregister Node）]** をクリックします。

Video Mesh ノードの移動

クラスタ間でノードを移動することがあります。たとえば、新しいクラスタを作成したため、ノードを配置し直す場合などが挙げられます。この手順を使用して、Video Mesh ノードを移動します。この手順を完了すると、ノードは新しいリソースでのみ利用できるようになります。

手順

ステップ 1 https://admin.webex.com のカスタマービューで、**[サービス（Services）]** > **[ハイブリッド（Hybrid）]** に移動し、Video Mesh カードの **[すべて表示（View all）]** を選択します。

ステップ 2 リストから移動するノードを選択し、**[アクション（Actions）]**（縦三点リーダー）をクリックします。

ステップ 3 **[ノードの移動（Move Node）]** を選択します。

ステップ 4 ノードを移動する場所に該当するラジオボタンを選択します。

- **既存のクラスタを選択する（Select an existing cluster）**：ドロップダウンリストから既存のクラスタを選択します。
- **新しいクラスタを作成する（Create a new cluster）**：フィールドに新しいクラスタの名前を入力します。

ステップ 5 **[ノードを移動（Move Node）]** をクリックします。
ノードが新しいクラスタに移動します。

関連トピック

ノードをメンテナンスモードに移行する

Video Mesh クラスタのアップグレードスケジュールの設定

特定のアップグレードスケジュールを設定することも、デフォルトのスケジュール（米国：アメリカ/ロサンゼルス時間の毎日午前 3:00）を適用することもできます。必要に応じて、予定されているアップグレードを延期できます。

Video Mesh のソフトウェアアップグレードはクラスタレベルで自動的に行われるため、すべてのノードが常に同じソフトウェアバージョンを実行していることが保証されます。アップグレードは、クラスタのアップグレードスケジュールに従って行われます。クラスタは、ソフトウェアアップグレードが利用できるようになった時点で、スケジュールされているアップグレード時間の前でも手動でアップグレードできます。

Before you begin

Note 緊急アップグレードは、利用可能になるとすぐに適用されます。

Procedure

ステップ 1 https://admin.webex.com のカスタマービューで、**[サービス（Services）]** > **[ハイブリッド（Hybrid）]** に移動し、Video Mesh カードの **[すべて表示（View all）]** を選択します。

ステップ 2 メディアリソースをクリックして、**[クラスタ設定の編集（Edit cluster settings）]** をクリックします。

ステップ 3 **[設定（Settings）]** ページで、**[アップグレード（Upgrade）]** までスクロールし、アップグレードスケジュールの時間、頻度、およびタイムゾーンを選択します。

Note Video Mesh ノードがアクティブコールを終了するまで待機する場合、アップグレードに数分以上かかる場合があります。アップグレードプロセスがすぐに開始されるように、自動アップグレードの時間帯は業務時間外にスケジュールすることをお勧めします。

ステップ 4 (Optional) 必要に応じて、**[延期（Postpone）]** をクリックして、後続のウィンドウまでアップグレードを 1 回延期します。

[タイムゾーン（time zone）] に、次のアップグレードの日付が表示されます。

アップグレード時の動作

1. ノードは、更新が利用可能かどうかを確認するために、クラウドに定期的に要求します。
2. クラウドは、クラスタのアップグレードの時間帯になるまでアップグレードを利用可能にしません。アップグレードの時間帯に達すると、ノードからクラウドへの次の定期的な更新リクエスト時に、更新情報が提供されます。
3. ノードは、セキュリティで保護されたチャネルを介して更新をプルします。
4. 既存のサービスはグレースフルシャットダウンを実行して、ノードへの着信コールのルーティングを停止します。グレースフルシャットダウンにより、既存の通話が完了する時間が与えられます（最長 2 時間）。
5. アップグレードをインストールします。
6. クラウドは、クラスタ内の一度にノードの一部のみのアップグレードをトリガーします。

Video Mesh クラスタの削除

Video Mesh クラスタを Webex クラウドから完全に削除することができます。この手順を完了するには、各ノードを別のクラスタに移動するか、すべてのノードの登録を解除する必要があります。クラスタのすべてのノードの登録を解除すると、それらノードは完全に削除されるた

め、利用できなくなります。登録を解除したノードを再度利用できるようにするには、再登録する必要があります。

手順

ステップ 1 https://admin.webex.com のカスタマービューで、**[サービス（Services）]** > **[ハイブリッド（Hybrid）]** に移動し、**[すべて表示（View all）]** をクリックします。

ステップ 2 リソースのリストから、削除する Video Mesh リソースまでスクロールし、**[クラスタ設定の編集（Edit Cluster Settings）]** をクリックします。

ヒント **[Video Mesh]** をクリックすると、Video Mesh リソースだけにフィルタ処理することができます。

ステップ 3 **[クラスタの削除（Delete Cluster）]** をクリックし、以下のいずれかを選択します。

- **[すべてのノードを移動（Move All Nodes）]** をクリックします。各ノードで、ドロップダウンリストから既存のリソースを選択して新しいリソースを作成するか、新しい名前を入力して **[続行（Continue）]** をクリックします。
- **[すべてのノードの登録解除（Deregister All Nodes）]** をクリックし、チェックボックスをオンにしてから **[クラスタの削除（Delete Cluster）]** をクリックします。

Video Mesh の非アクティブ化

Video Mesh を非アクティブ化することで、ミーティングでメディアをオンプレミスにする機能を削除できます。また、Video Mesh ノードを使用した進行中のすべてのミーティングは終了し、今後のミーティングはクラウドでホストされます。非アクティブ化した場合、Video Mesh を使用する唯一の方法は、始めから展開することです。

始める前に

Video Mesh を非アクティブ化する前に、すべての Video Mesh ノードを登録解除します。

手順

ステップ 1 https://admin.webex.com のカスタマービューで、**[サービス（Services）]** > **[ハイブリッド（Hybrid）]** > **[すべて表示（View all）]** に移動し、Video Mesh カードの **[設定（Settings）]** を選択します。

ステップ 2 **[非アクティブ化（Deactivate）]** をクリックします。

ステップ 3 クラスタのリストを確認し、ダイアログの免責事項を読みます。

ステップ 4 このアクションについて理解していることを確認するチェックボックスをオンにし、ダイアログで**[非アクティブ化（Deactivate）]** をクリックします。

ステップ 5 Video Mesh を非アクティブ化する準備ができたら、**[サービスの非アクティブ化（Deactivate Service）]** をクリックします。

非アクティブ化すると、すべての Video Mesh ノードとクラスタが削除されます。Video Mesh が構成されなくなります。

Video Mesh ノードの登録のトラブルシューティング

このセクションには、Video Mesh ノードを Webex クラウドに登録する際に発生する可能性のあるエラーと、それらを修正するための推奨手順が含まれています。

ドメインを解決できませんでした（The domain could not be resolved）

考えられる原因 このメッセージは、Video Mesh ノードで構成されている DNS 設定が正しくない場合に表示され ます。

解決法 Video Mesh ノードのコンソールにサインインし、DNS 設定が正しいことを確認します。

SSL 経由のポート 443 を使用してサイトに接続できませんでした（Could not connect to site using port 443 via SSL）

考えられる原因 このメッセージは、Video Mesh ノードが Webex クラウドに接続できない場合に表示され ます。

解決法 Video Mesh に必要なポートでの接続がネットワークで許可されていることを確認してください。詳細については、「Video Mesh で使用されるポートとプロトコル （32 ページ）」を参照してください。

Video Mesh アラーム

このセクションには、Video Mesh 展開のさまざまな段階で Control Hub で発生する可能性のあるアラームの包括的なリストが含まれています。

アラームタイプ（アラーム ID）	アラームタイトル	シビラティ（重大度）	詳細	
mf.coreos.dnsConfig	Video Mesh ノードの DNS 設定が無効です。	警告	アラームテキスト	理由（Reason）
			DNS アドレスの解決中にエラーが発生したため、DNS サーバー {} を照会できません。	アドレスの解決中にエラーまたは例外が発生しました。
			DNS クエリが失敗したため、DNS サーバー {} をクエリできません。	
mf.coreos.hostnameConfig	Video Mesh ノードのホスト名設定が無効です。	警告	アラームテキスト	理由（Reason）
			FQDN{} の IP が ECP IP と一致しません。	dig によって返された IP が現在のノード IP と一致しません。
			現在の DNS 設定に対して FQDN {} の IP アドレスを解決できません。	
mf.coreos.ntpConfig	Video Mesh ノードの NTP 設定が無効です。	警告またはアラート	アラームテキスト	理由（Reason）
			現在のシステム時刻を NTP サーバー {} に照会できません。	サーバーへの SNTP クエリが失敗しました。
			現在の DNS 設定に対して NTP サーバー{} の IP アドレスを解決できません。	
mf.coreos.ntpSync	Video Mesh ノードのシステム時刻が同期していない	警告または重大		
mf.callHealth.fail	コールヘルスチェックに失敗しました	警告		

アラームタイプ（アラーム ID）	アラームタイトル	シビラティ（重大度）	詳細
mf.linus.connectivityError	Cisco Webex Cloud サービスへの接続で問題が発生しました	警告	クラウドへの接続の問題により、コールが切断されています。コールスイッチングプロセスを再起動して、接続を再確立します。
mf.linus.highCpuError	少なくとも 2 分間、CPU 使用率が 95% を超えています。	警告	
mf.linus.networkError		警告	
mf.homer.connectivityError	Cisco Webex Cloud サービスへの接続で問題が発生しました	警告	
mf.l2sip.fault	Webex Video Mesh SIP コールが正しく機能していません	警告	クラウドへの接続の問題により、SIP コールが中断されました。Webex Video Mesh SIP コールが正しく機能していません。SIP コールは、クラウドにオーバーフローしたり、失敗したりする可能性があります。https://status.webex.com で、クラウドへのネットワーク接続（FQDN）と Cisco Webex のステータスを確認します。公開されたインシデントがなくてもこの問題が解決しない場合は、https://admin.webex.com にアクセスし、管理者のユーザー名をクリックし、**[フィードバック（Feedback）]** をクリックして、さらに調査するためのケースを開きます。

アラームタイプ（アラーム ID）	アラームタイトル	シビラティ（重大度）	詳細
mf.vm.insufficientCpuCores	重大バージョン：CPUコアの数が少ないため、コール処理機能をインストールできませんでした。 警告バージョン：この Webex Video Mesh ノードには X 個の CPU コアがありますが、これは必要な最小 X 個の CPUコアよりも少なくなっています。この仮想マシンを X 個以上の CPU コアに更新してください。	警告から重大	必要な最小 CPU コア数を下回っています。
mf.device.pullFailure	このノードは、アップグレードを成功させるために必要なダウンロードを完了できません。	重大	アップグレードできません。Docker ハブに到達できません。ノードがネットワーク環境から適切なクラウドリソースにアクセスできることを確認します。
mf.device.caCertExpiring-n	このノードにインストールされた CA 証明書はn日後に期限切れになります	警告から重大	CA 証明書が n 日後に期限切れになります。
mf.device.rootCertExpiring-n	ルート証明書がn日後に期限切れになります	警告から重大	ルート証明書がn日後に期限切れになります。
mf.amazonEcr.pullFailure	Cisco Cloud プロバイダーからソフトウェアイメージにアクセスできない	重大	Video Mesh ノードは、シスコのクラウドプロバイダーから必要なソフトウェアをダウンロードできませんでした。この問題は、ネットワークに関連する複数の問題が原因で発生する可能性があります。パブリックネットワーク（*.amazonaws.com）へのネットワーク接続を確認し、DNS 設定を確認します。これは、Video Mesh ノードとインターネットの間に存在するファイアウォールの変更によっても発生する可能性があります。

アラームタイプ（アラーム ID）	アラームタイトル	シビラティ（重大度）	詳細
mf.device.storageFull	デバイスストレージがほぼいっぱいです。使用済みディスク容量は X% です	重大	お客様が VM により多くのスペースを割り当てるか、ファイルのクリーンアップが必要になる場合があります。
mf.vm.lowCpuMode	この Webex Video Meshノードは、X個の vCPU のみを使用して「デモモード」で実行されています。コール処理のパフォーマンスが低下します。このノードは、最初のインストールから 90 日後に期限切れになります。」	アラート	
mf.reachability.fail	この Video Mesh ノードと別のクラスタ間の接続の問題	警告	組織内の VMN クラスタへの 1 つ以上の到達可能性テストが失敗しました。ホームノードの場合は、他のすべてのクラスタへの到達可能性チェックが実行されます。非ホームノードの場合は、ホームノードに対してのみ到達可能性チェックが実行されます。他の組織クラスタへのネットワーク接続を確認します。
mf.cloudReachability.fail	この Video Mesh ノードとクラウド間の接続の問題	警告	この Video Mesh ノードは、次のクラウドメディアサーバーに接続できませんでした：<one-or-more-cloud-servers> 。ファイアウォールルールを確認し、必要に応じて更新を行い、ポート 5004 で発信トラフィックを許可します。

ウェブインターフェイスからの Video Mesh ノードの管理

クラウドに登録されている Video Mesh ノードのネットワークを変更する前に、Control Hub を使用してノードをメンテナンスモードにする必要があります。詳細および従うべき手順については、「ノードのメンテナンスモードへの移行」を参照してください。

⚠

注意 メンテナンスモードは、特定のネットワーキング設定の変更（DNS、IP、FQDN）を行ったり、RAM やハードドライブの置き換えなどのハードウェア メンテナンスの準備を行ったりできるよう、ノードのシャットダウンまたは再起動を準備することのみを意図しています。

ノードがメンテナンスモードになっている場合、アップグレードは行われません。

ノードをメンテナンスモードにすると、コールサービスのグレースフルシャットダウンを実行します（新しいコールの受け入れを停止し、既存のコールが完了するまで最大2時間待機します）。コールサービスのグレースフルシャットダウンの目的は、コールのドロップを引き起こすことなく、ノードの再起動またはシャットダウンを可能にすることです。

Video Mesh の概要にアクセスする方法

次のいずれかの方法でウェブインターフェイスを開くことができます。

- フルアクセス権を持つ管理者であり、すでにノードをクラウドに登録している場合、Control Hub からノードにアクセスできます。

  https://admin.webex.com のカスタマービューから、**[サービス（Services）]** > **[ハイブリッド（Hybrid）]** に移動します。Video Mesh カードの **[リソース（Resources）]** で **[すべて表示（View all）]** をクリックします。クラスタをクリックし、アクセスするノードをクリックします。[ノードに進む（Go to Node）] をクリックします

  この機能を使用できるのは、Webex 組織のフルアクセス権を持つ管理者のみです。他の管理者（パートナーや外部のフルアクセス権を持つ管理者を含む）は、Video Meshリソース用に **[ノードに移動（Go To Node）]** オプションを持っている必要はありません。

- ブラウザタブで、`<IP アドレス>/setup`（たとえば、 `https://192.0.2.0/setup`）に移動します。ノード用に設定した管理者ログイン情報を入力し、**[サインイン（Sign In）]** をクリックします。

  管理者アカウントが無効になっている場合、この方法は使用できません。「ウェブインターフェイスからのローカル管理者アカウントの無効化または再有効化」セクションを参照してください。

概要はデフォルトのページで、次の情報が含まれています。

- **コール ステータス（Call Status）**：ノードを経由する進行中のコールの数を提供します。
- **ノードの詳細（Node Details）**：ノードタイプ、ソフトウェアイメージ、ソフトウェアバージョン、OS バージョン、QoS ステータス、およびメンテナンスモードのステータスを提供します。
- **ノードの正常性（Node Health）**：使用状況データ（CPU、メモリ、ディスク）、およびサービスステータス（Management Service、Messaging Service、NTP Sync）を提供します。
- **ネットワーク設定（Network Settings）**：ホスト名、インターフェイス、IP、ゲートウェイ、DNS、NTP、デュアル IP が有効かどうかというネットワーク情報を提供します。

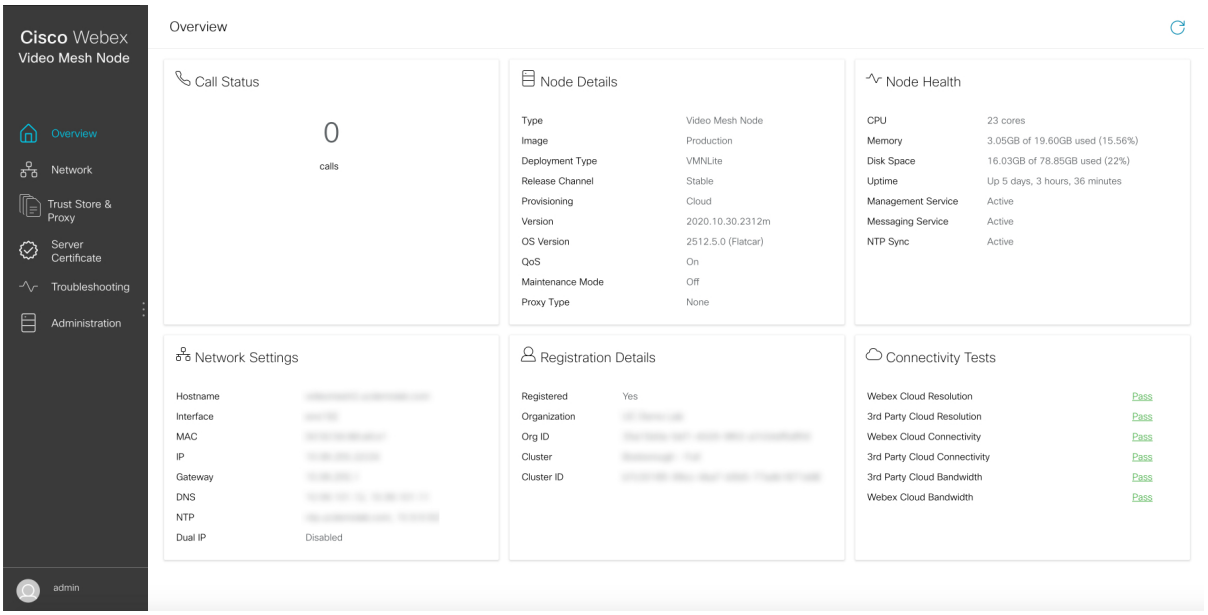
- **登録の詳細（Registration Details）**：登録ステータス、組織名、組織 ID、ノードが一部となっているクラスタ、およびクラスタ ID を提供します。
- **クラウド接続（Cloud Connectivity）**：ノードから、ノードが適切に実行するためにアクセスする必要がある Webex クラウドおよびサードパーティの接続先に対して、一連のテストを実行します。
  - DNS 解決、サーバー応答時間、および帯域幅の 3 種類のテストが実行されます。

（注）
- DNSテストは、ノードが特定のドメインを解決できるかを検証します。これらのテストでは、サーバーが 10 秒以内に応答しない場合、失敗した旨がレポートされます。応答時間が 1.5 ～ 10 秒の場合、オレンジ色の「警告色」で「合格」と表示されます。ノードでの定期的な DNS チェックでは、DNS の応答時間が 1.5 秒を超える場合にアラームが生成されます。
- 接続テストでは、ノードが特定の HTTPS URL に接続して応答を受信できること（プロキシまたはゲートウェイのエラー以外の応答が接続の証拠として受け入れられること）を検証します。
- 概要ページから実行されるテストのリストは網羅的ではなく、WebSocket テストを含むものでもありません。
- コールプロセスがクラウドへの WebSocket 接続を完了できない、またはコール関連サービスに接続できない場合、ノードはアラームを送信します。

- [合格（Pass）] または [失敗（Fail）] の結果は、各テストの横に表示されます。このテキストの上でホバーすると、テストが実行された時にチェックされた情報の詳細を確認できます。

次のスクリーンショットに示すように、ノードによってアラームが生成された場合、アラーム通知をサイドパネルに表示することもできます。これらの通知は、ノードにおける潜在的な問題を識別し、これらの問題のトラブルシュート方法または解決方法を提案します。アラームが生成されていない場合、通知パネルは表示されません。

図 *10 : Video Mesh* ノードウェブインターフェイスの *[*概要（*Overview*）*]* ページの例



Video Mesh ノード ウェブ インターフェイスからのネットワーク設定の構成

ネットワークトポロジが変更された場合は、各 Webex Video Mesh ノードのためにウェブインターフェイスを使用して、そこでネットワーク設定を変更することができます。ネットワーク設定の変更については注意が表示される場合がありますが、Webex Video Mesh ノードの設定を変更した後にネットワークに変更を加える場合は、変更を保存することができます。

手順

ステップ 1 Webex Video Mesh ノードインターフェイスを開きます。

ステップ 2 **[ネットワーク（Network）]** に移動します。

ノードの現在のネットワーク設定が表示されます。

ステップ 3 必要に応じて、**[ホストとネットワークの構成（Host and Network Configuration）]** で次の設定を変更します。

- **[ホスト名とドメインの編集（Edit Hostname and Domain）]** で、**[ホスト名（Hostname）]** と **[ドメイン（Domain）]**の値を変更します。

  FQDN（ホスト名とドメイン）に正しい形式が設定されていない場合、エラーが表示されます。

- **[ネットワークモード（Network Mode）]** で、**[DHCP の有効化（Enable DHCP）]** がリストに表示されますが、DHCP はサポートされていません。静的 IP アドレス、サブネットマスク、およびゲートウェイを設定する必要があります。
- **[ネットワーク設定の編集（Edit Network Configuration）]** で、**[IP アドレス（IP Address）]**（内部インターフェイス向け）、**[サブネットマスク（Subnet Mask）]**、**[ゲートウェイ（Gateway）]**（別のネットワークへのアクセスポイントとして機能するネットワークノード）の値を変更します。

  （注） Video Mesh ノードは、内部 IP アドレスと解決可能な DNS 名を持っている必要があります。ノード IP アドレスは、Video Mesh ノード内部使用のために予約されている IP アドレスの範囲に属していてはなりません。デフォルトの予約済み IP アドレスの範囲は 172.17.42.0 ～ 172.17.42.63 で、後でノードコンソールの **[診断（Diagnostic）]** メニューで設定できます。この IP アドレスの範囲は、Video Mesh ノード内、およびノードのさまざまなコンポーネント（SIP インターフェイスやメディアトランスコーディングなど）を保持するソフトウェアコンテナ間における通信のためのものです。

- **[DNS サーバーの編集（Edit DNS Servers）]** で、ドメイン名を数字の IP アドレスに変換する DNS サーバーエントリを変更します。最大 4 つの DNS サーバーを入力できます。

ステップ 4 **[ホストとネットワークの設定を保存（Save Host and Network Configuration）]** をクリックし、ノードのリブートが必要である旨のポップアップが表示されたら、**[保存して再起動（Save and Reboot）]** をクリックします。

保存中は、すべてのフィールドがサーバー側で検証されます。一般的に表示される警告は、サーバーが到達不可能か、クエリ時に有効な応答が返されないことを示しています（FQDN が提供された DNS サーバーのアドレスを使用して解決可能でない場合など）。警告を無視して保存を選択できますが、ノードに構成されている DNS で FQDN を解決できるまで、コールは機能しません。可能性のあるもう 1 つのエラー状態は、ゲートウェイのアドレスが IP アドレスと同じサブネット内にない場合です。Video Mesh ノードのリブート後、ネットワーク構成の変更が有効になります。

ステップ 5 必要に応じて 、**NTP サーバー**用に以下の設定を変更します。

- **[NTP サーバーの編集（Edit NTP Servers）]** で、組織内で時間をノードと同期させるために使用される NTP サーバーエントリの値を変更します。

ステップ 6 **[NTP サーバーの保存（Save NTP Servers）]** をクリックします。

（注） 複数の NTP サーバーを設定する場合、フェールオーバーのポーリング間隔は 40 秒です。

NTP サーバーが FQDN であって、かつ、解決できない場合は、警告が返されます。NTP サーバーの FQDN は解決したが、NTP 時刻について 解決済み IP をクエリできない場合は、警告が返されます。

Video Mesh ノード ウェブ インターフェイスからの外部ネットワーク インターフェイスの設定

ネットワークトポロジが変更された場合は、各 Webex Video Mesh ノードのためにウェブインターフェイスを使用して、そこでネットワーク設定を変更することができます。ネットワーク設定の変更についての注意が表示される可能性があります。ただし、Webex Video Mesh ノードの設定を変更した後にネットワークを変更する場合には、変更を保存できます。

ネットワークの DMZ 内で Video Mesh ノードを展開している場合は、外部ネットワーク インターフェイスを設定して、企業（内部）トラフィックを外部トラフィックから分離することができます。

手順

ステップ 1 Webex Video Mesh ノードインターフェイスを開きます。

ステップ 2 **[ネットワーク（Network）]** に移動します。

ノードの現在のネットワーク設定が表示されます。

ステップ 3 **[詳細設定（Advanced）]** をクリックします。

ステップ 4 ノードの外部 IP アドレスオプションを有効にするには、**[外部ネットワークの有効化（Enable External Network）]** をオンに切り替えて、**[OK]** をクリックします。

ステップ 5 **[外部 IP アドレス（External IP Address）]**、**[外部サブネットマスク（External Subnet Mask）]**、および **[外部ゲートウェイ（External Gateway）]** の値を入力します。

ステップ 6 **[外部ネットワーク設定の保存（Save External Network Configuration）]** をクリックします。

ステップ 7 **[保存して再起動（Save and Reboot）]** をクリックして変更を確認します。

デュアル IP アドレスを有効にするためにノードが再起動し、基本的な静的ルーティングルールが自動的に設定されます。これらのルールは、プライベートクラス IP アドレス間のトラフィックが、内部インターフェイスを使用することを決定します。パブリッククラスの IP アドレス間のトラフィックには、外部インターフェイスが使用されます。後で、独自のルーティングルールを作成することができます。たとえば、内部インターフェイスからの上書きを設定し、外部ドメインへのアクセスを許可する必要がある場合などです。

ステップ 8 エラーが発生した場合は、**[OK]** をクリックしてエラーダイアログボックスを閉じ、エラーを修正して、**[外部ネットワーク設定の保存（Save External Network Configuration）]** を再度クリックします。

次のタスク

内部 IP アドレスと外部 IP アドレスの設定を検証するには、「Video Mesh ノード ウェブ インターフェイスからの Ping の実行 （158 ページ）」の手順を実行します。

- cisco.com などの外部宛先をテストします。成功した場合は、外部インターフェイスから宛先にアクセスしたことが結果に示されます。
- 内部 IP アドレスをテストします。成功した場合は、内部インターフェイスからアドレスにアクセスされたことが結果に示されます。

Video Mesh ノードウェブインターフェイスからの内部および外部ルーティングルールの追加

デュアルネットワークインターフェイス（NIC）の展開では、外部インターフェイスと内部インターフェイスのユーザー定義ルートルールを追加することによって、値リストコレクション作成者のルーティングを微調整することができます。デフォルトルートはノードに追加されますが、たとえば、外部サブネットまたは内部インターフェイスを介してアクセスする必要があるホストアドレス、あるいは外部インターフェイスからアクセスする必要がある内部サブネットまたはホストアドレスなど、例外を作成することができます。必要に応じて、次の手順を実行します。

始める前に

ルーティングルールを設定するには、まず外部ネットワークインターフェイスを有効にして設定する必要があります。

手順

ステップ 1 Webex Video Mesh ノードインターフェイスを開きます。

ステップ 2 **[ネットワーク（Network）]** に移動します。

ノードの現在のネットワーク設定が表示されます。外部ネットワークを設定している場合は、[ルーティングルール（Routing Rules）] タブが表示されます。

ステップ 3 **[ルーティングルール（Routing Rules）]** タブをクリックします。

このページを初めて開いたときは、デフォルトのシステムルーティングルールがリストに表示されます。デフォルトでは、すべての内部トラフィックは内部インターフェイスを通過し、外部トラフィックは外部インターフェイスを通過します。

これらのルールに手動オーバーライドを追加するには、次の手順を実行します。

ステップ 4 ルールを追加するには、**[ルーティングルールの追加（Add Routing Rule）]** をクリックし、次のいずれかのオプションを選択します。

- **[ネットワークタイプ（Network Type）]** で **[内部（Internal）]** をクリックして、内部ルートに使用する外部サブネットまたはホスト IP アドレスを入力します。
- **[ネットワークタイプ（Network Type）]** で **[外部（External）]** をクリックして、外部ルートに使用する内部サブネットまたはホスト IP アドレスを入力します。

ステップ 5 **[ルーティングルールの追加（Add Routing Rule）]** をクリックします。

各ルールを追加すると、そのルールはルーティングルールの一覧に表示され、ユーザー定義ルールとして分類されます。

ステップ 6 1 つ以上のユーザー定義ルールを削除するには、ルールの左側にある列のチェックボックスをオンにして、**[ルーティングルールの削除（Delete Routing Rule(s)）]** をクリックします。

（注） デフォルトルートを削除することはできませんが、設定した任意のユーザー定義オーバーライドを削除することはできます。

⚠

注意 カスタムルーティングルールは、他のルーティングと競合する可能性があります。たとえば、Video Mesh ノードインターフェイスへの SSH 接続をフリーズするルールを定義できます。このような場合は、次のいずれかを実行して、ルーティングルールを削除または変更します。

- Video Mesh ノードのパブリック IP アドレスへの SSH 接続を開きます。
- ESXi コンソールから Video Mesh ノードにアクセスする

Video Mesh ノードウェブインターフェイスからのコンテナネットワークの構成

Video Mesh ノードは、ノード内での内部使用のためのサブネット範囲を予約します。デフォルトの範囲は、172.17.42.0 ～ 172.17.42.63 です。ノードは、この範囲から発信される外部から Video Mesh ノードへのトラフィックには応答しません。ネットワーク内の他のデバイスと競合しないように、コンテナのブリッジ IP アドレスを変更するためにノードコンソールを使用することもできます。

手順

ステップ 1 Webex Video Mesh ノードインターフェイスを開きます。

ステップ 2 **[ネットワーク（Network）]** に移動します。

ノードの現在のネットワーク設定が表示されます。

ステップ 3 **[詳細設定（Advanced）]** をクリックします。

ステップ 4 必要に応じて **[コンテナ IP アドレス（Container IP Address）]** と **[コンテナサブネットマスク（Container Subnet Mask）]** の値を変更し、**[コンテナネットワーク設定の保存（Save Container Network Configuration）]** をクリックします。

ステップ 5 **[保存して再起動（Save and Reboot）]** をクリックして変更を確認します。

ステップ 6 エラーが発生した場合は、**[OK]** をクリックしてエラーダイアログボックスを閉じ、エラーを修正して、**[コンテナネットワーク設定の保存（Save Container Network Configuration）]** を再度クリックします。

ネットワークインターフェイスの MTU サイズの設定

すべての Webex Video Mesh ノードは、デフォルトで有効になっているパス MTU（PMTU）検出を備えています。PMTU を使用すると、ノードは、MTU の問題を検出し、自動的に MTU サイズを調整します。ファイアウォールまたはネットワークの問題が原因で PMTU に障害が発生する場合、このノードには、パケットが MTU ドロップよりも大きいことを原因とする、クラウドへの接続に関する問題がある可能性があります。手動で MTU サイズを小さく設定することで、この問題を解決できます。

始める前に

ノードがすでに登録されている場合は、MTU設定を変更する前に、ノードをメンテナンスモードにする必要があります。

手順

ステップ 1 Webex Video Mesh ノードインターフェイスを開きます。

ステップ 2 **[ネットワーク（Network）]** に移動します。

ノードの現在のネットワーク設定が表示されます。

ステップ 3 **[詳細設定（Advanced）]** をクリックします。

ステップ 4 **[インターフェイス MTU 設定（Interface MTU Settings）] セクション**で、適切なフィールドに 1280 ～ 9000 バイトの間で MTU の値を入力します。

外部インターフェイスを有効にした場合は、内部 MTU と外部 MTU の両方のサイズを個別に設定できます。

ノードが再起動し、MTU の変更が適用されます。

次のタスク

MTU を変更するためにノードをメンテナンスモードにした場合は、メンテナンスモードをオフにします。

DNS キャッシングを有効または無効にする

Video Mesh ノードへの DNS 応答が定期的に 750 ミリ秒を超える場合、または Cisco TAC で推奨されている場合は、DNS キャッシングを有効にできます。DNS キャッシングがオンの場合、

ノードは DNS 応答をローカルにキャッシュします。キャッシュを使用すると、要求の遅延やタイムアウトが発生しにくくなり、接続アラーム、コールドロップ、またはコール品質の問題が発生する可能性があります。DNS キャッシングは、DNS インフラストラクチャの負荷の軽減にもつながる場合があります。

始める前に

ノードをメンテナンスモードに切り替えます。メンテナンスモードのステータスが**[オン（On）]**の場合（保留期間の終了時にアクティブコールが完了しているか、ドロップしている場合）、DNS キャッシングを有効または無効にできます。

手順

ステップ 1 Webex Video Mesh ノードインターフェイスを開きます。

ステップ 2 **[ネットワーク（Network）]** に移動します。

ノードの現在のネットワーク設定が表示されます。

ステップ 3 **[詳細設定（Advanced）]** をクリックします。

ステップ 4 [DNS キャッシング設定（DNS Caching Configuration）] セクションで、**[DNS キャッシングの有効化（Enable DNS Caching）]** のオンまたはオフを切り替えます。

ステップ 5 確認ダイアログで、**[保存して再起動（Save and Reboot）]** をクリックします。

ステップ 6 ノードの再起動後、Webex Video Mesh ノードインターフェイスを再度開いて、接続チェックが成功しているかを [概要（Overview）] ページで確認します。

DNS キャッシングを有効にした場合、**[DNS キャッシュ統計（DNS Cache Statistics）]** に次の統計が表示されます。

統計	説明
キャッシュエントリ	DNS キャッシュサーバーが保存している前の DNS 解決数
キャッシュ ヒット	キャッシュのリセット後、お客様の DNS サーバーを照会せずに、Video Mesh からの DNS 要求をキャッシュが処理した回数
キャッシュ ミス	キャッシュのリセット後、Video Mesh からの DNS 要求を（キャッシュを通じて処理するのではなく）お客様の DNS サーバーが処理した回数
キャッシュヒットの割合	お客様の DNS サーバーを照会せずに、キャッシュが処理した Video Mesh からの DNS 要求の割合
サーバーアウトバウンド DNS がクエリしたキャッシュ	Video Mesh DNS キャッシュサーバーがお客様の DNS サーバーに対して行った DNS クエリの数

統計	説明
サーバーインバウンドDNSがクエリしたキャッシュ	Video Mesh が内部の DNS キャッシュサーバーに対して行った DNS クエリの数
アウトバウンドクエリのインバウンドクエリに対する比率	Video Mesh がお客様の DNS サーバーに対して行った DNS クエリと、Video Mesh が内部の DNS キャッシュサーバーに対して行ったクエリの比率
インバウンドクエリ/秒	Video Mesh が内部の DNS キャッシュサーバーに対して行った 1 秒あたりの DNS クエリの平均数
アウトバウンドクエリ/秒	Video Mesh がお客様の DNS サーバーに対して行った 1 秒あたりの DNS クエリの平均数
アウトバウンド DNS 遅延 [時間範囲]	応答時間が記載された時間範囲内の、Video Mesh がお客様の DNS サーバーに対して行った DNS クエリの割合

TAC 要求時に DNS キャッシュをリセットするには、**[DNS キャッシュのワイプ（Wipe DNS Cache）]** ボタンを使用します。DNS キャッシュをワイプした後、キャッシュが補充されるのに伴って、**[アウトバウンドクエリのインバウンドクエリに対する比率（Outbound to Inbound Query Ratio）]** が大きくなります。キャッシュをワイプするためにノードをメンテナンスモードにする必要はありません。

次のタスク

ノードのメンテナンスモードを終了します。その後、変更が必要な他のノードでタスクを繰り返します。

セキュリティ証明書のアップロード

syslog サーバーなど、ノードと外部サーバー間の信頼関係を設定します。

（注） クラスタ化された環境では、CA とサーバー証明書を各ノードにインストールする必要があります。

手順

ステップ 1 Webex Video Mesh ノードインターフェイスを開きます。

ステップ 2 Syslog サーバーへの外部ロギングの設定などの別のサーバーで TLS を設定する場合、セキュリティ上の理由から、Video Mesh ノードでノードのデフォルト自己署名証明書の代わりに CA 署名付き証明書を使用することを**お勧めします**。Video Mesh ノードで証明書とキーペアを作成してアップロードするには、**[サーバー証明書（Server Certificates）]** に移動し、次の手順を実行します。

a) 認定プロバイダから発行された証明書が必要な場合は、**[証明書署名要求の作成（Create a Certificate Signing Request）]** をクリックします。必要な情報（共通名を含む必要がある FQDN である**サブジェクト代替名**を含む）を入力します。その後、CSR を生成してダウンロードし、要求をプロバイダに送信します。複数の CSR を作成できます。プロバイダは、認証局（CA）の署名付き証明書を返します。（CSR の作成手順で、すでに秘密キーが生成されています。）

（注） 共通名は URL ではありません。プロトコル（http:// や https:// など）、ポート番号、またはパス名は含まれません。X.509 証明書仕様の `commonName` フィールドは、技術的には共通名を表します。`https://www.example.com` の場合、正しい値は `example.com` です。

b) 証明書とキーを有している場合、**[サーバー証明書のアップロード（.crt または .pem ファイル）（Upload a Server Certificate（.crt or .pem file））]** をクリックし、証明書ファイルを選択して、**[秘密キーのアップロード（.key ファイル）（Upload a Private Key（.key file））]** をクリックし、パスフレーズがある場合はパスフレーズを入力します。

秘密キーは、CSR が生成されたときにすでに配置されています。CSR の作成手順を使用しない場合、必要なのは秘密キーをアップロードすることだけです。

c) 証明書を取得したら、クラスタ内の最初の Video Mesh ノードに移動し、**[サーバー証明書のインストール（Install Server Certificate）]** をクリックし、プロンプトを読み、**[インストール（Install）]** をクリックして **[OK]** をクリックします。

クラウドに登録された Video Mesh ノードは、コールが終了するまで最長で 2 時間待機し、一時的に非アクティブ状態（休止）となります。既存のコールが終了した時点と 2 時間が経過した時点のいずれか早い時点において、このノードは証明書のインストールを完了します。サーバー証明書のインストール完了時にプロンプトが表示され、ページを再ロードして新しい証明書とキーエントリを表示できます。

d) 証明書とキーファイルの横にある **[ダウンロード（Download）]** をクリックして、ローカルコピーを保存します。

ファイルを覚えやすい場所に保存し、ブラウザタブでインスタンスを開いたままにしておきます。

e) クラスタ内の 2 番目の Video Mesh ノードに移動し、パスフレーズを入力して、秘密キーファイルをアップロードします。その後、**[サーバー証明書のアップロード（Upload a Server Certificate）]** をクリックし、**[サーバー証明書のインストール（Install Server Certificate）]** を選択し、プロンプトを読み、**[インストール（Install）]** をクリックして **[OK]** をクリックします。

f) 同じクラスタ内の他のすべての Video Mesh ノードで、この手順を繰り返します。

ステップ 3 外部サーバーの CA 証明書の署名方法に応じて、オプションを選択します。

- サーバーの CA 証明書が、一般的に認知されている組織（DigiCert、GeoTrust、GlobalSign など）によって署名されている場合、Video Mesh ノードは、定期的に更新される、Video Mesh ノードのホスト OS からのルート証明書のリストに基づいて信頼します。手順ステップ 6 （156 ページ） に進みます。

- サーバーの CA 証明書が内部の企業 CA ルート証明書で署名されている場合、その権限のルート証明書を Video Mesh ノードに追加する必要があります。次の手順に進んでください。

ステップ 4 外部サーバーが使用する証明書または証明書信頼リスト（CTL）を取得します。

Video Mesh ノード証明書と同様に、覚えやすい場所に外部サーバーファイルを保存します。

ステップ 5 Webex Video Mesh ノードのインターフェイスのタブに戻り、**[信頼ストアおよびプロキシ（Trust Store & Proxy）]** をクリックし、次のオプションを選択します。

- 単一の CA 証明書をインストールするには、**[ルート証明書またはエンドエンティティ証明書のアップロード（.crt または .pem ファイル）（Upload a Root Certificate or End Entity Certificate（.crt or .pem file））]** をクリックし、コンピュータから証明書ファイルを選択し、**[すべての証明書を信頼ストアにインストール （Install All Certificates into the Trust Store）]** をクリックし、プロンプトを読んで **[インストール（Install）]** をクリックし、ノードを再起動します。
- 証明書チェーンをインストールするには、ルート CA 証明書と中間 CA 証明書をアップロードし、**[すべての証明書を信頼ストアにインストール（Install All Certificates into the Trust Store）]** をクリックし、プロンプトを読んで **[インストール（Install）]** をクリックします。

クラウドに登録された Video Mesh ノードは、コールが終了するまで最長で 2 時間待機し、一時的に非アクティブ状態（休止）となります。証明書をインストールするには、ノードが再起動する必要があり、この再起動は自動的に実行されます。オンラインに戻ると、証明書が Video Mesh ノードにインストールされている場合にはプロンプトが表示され、ページを再ロードして新しい証明書を表示できます。

ステップ 6 同じクラスタ内の他のすべての Video Mesh ノードで、証明書または証明書チェーンのアップロードを繰り返します。

サポート用の Video Mesh ログの生成

ログをシスコに直接送信するよう指示される場合があります。また、ケースに添付するためにログをダウンロードすることもできます。ログを生成してシスコに送信するか、任意の Video Mesh ノードからログをダウンロードするには、ウェブインターフェイスから次の手順を実行します。生成されるログパッケージには、メディアログ、システムログ、およびコンテナログが含まれます。このバンドルは、シスコが Video Mesh ノードの展開をトラブルシュートできるようにするため、Webex への接続、プラットフォームの問題、およびコールのセットアップまたはメディアについての有益な情報を提供します。

手順

ステップ 1 Webex Video Mesh ノードインターフェイスを開きます。

ステップ 2 **[トラブルシューティング（Troubleshooting）]** に移動し、**[ログの送信（Send Logs）]** の横にあるオプションを選択します。

- **[シスコにログを送信（Send Logs to Cisco）]** をクリックしてノードからログバンドルを生成し、1 つの手順を実行してそのバンドルをシスコに直接送信します。ログが圧縮、zip、およびアップロードされるのに伴って変化するステータスインジケータが表示されます。
- **[ダウンロード（Download）]** をクリックしてノードからログバンドルを生成します。このログバンドルは、ローカルに保存したり、後でケースに添付したりできます。

生成されたログは、ノードに履歴として保存され、再起動後もノードに残ります。アップロード識別子がページに表示されます。サポートはこの値を使用して、アップロードされたログを識別します。

ステップ 3 ケースを開始したり、Cisco TAC で操作したりする場合は、サポートエンジニアがログにアクセスできるよう、アップロード識別子の値を含める必要があります。

ログをシスコに直接送信した場合は、ログバンドルを TAC ケースにアップロードする必要はありません。

次のタスク

ログがシスコにアップロードされている間、またはダウンロードされている間、同じ画面からパケットキャプチャを実行できます。

サポート用の Video Mesh パケット キャプチャの生成

詳細な分析のために、パケットキャプチャ（PCAP）を実行し、シスコに送信できます。パケットキャプチャでは、ノードのネットワークインターフェイスを通過するデータパケットのスナップショットを取得します。パケットをキャプチャして送信すると、シスコでは送信されたキャプチャを分析し、Video Mesh ノードの展開のトラブルシューティングをサポートできます。

始める前に

⚠

注意 パケットキャプチャ機能は、デバッグのみを目的としています。アクティブコールをホストしているライブの Video Mesh ノードでパケットキャプチャを実行すると、パケットキャプチャがノードのパフォーマンスに影響を及ぼし、生成されたファイルが上書きされる可能性があります。これは、キャプチャされたデータが失われる原因となります。パケットキャプチャは、オフピーク時、またはノードのコール数が 3 未満の場合にのみ実行することをお勧めします。

手順

ステップ 1 Webex Video Mesh ノードインターフェイスを開きます。

ステップ 2 **[トラブルシューティング（Troubleshooting）]** に移動します。

パケットキャプチャの開始と、ログのアップロードを同時に実行できます。

ステップ 3 （任意）**[パケットキャプチャ（Packet Capture）]** セクションでは、特定のインターフェイスのパケットにキャプチャを制限したり、特定のホストとの間のパケットによってフィルタ処理したり、1 つまたは複数のポートのパケットによってフィルタ処理したりできます。

ステップ 4 プロセスを開始するには、**[パケットキャプチャの開始（Start Packet Capture）]** 設定をオンに切り替えます。

ステップ 5 完了したら、**[パケットキャプチャの開始（Start Packet Capture）]** 設定をオフに切り替えます。

ステップ 6 次のいずれかを選択します。

- **[PCAP をシスコに送信（Send PCAP to Cisco）]** をクリックして、ノードからシスコに直接パケットキャプチャを送信します。パケットキャプチャがアップロードされるのに伴って変化するステータスインジケータが表示されます。
- **[ダウンロード（Download）]** をクリックして、ノードからのパケットキャプチャのローカルコピーを保存します。後でケースに添付できます。

パッケージキャプチャをアップロードすると、アップロード識別子がページに表示されます。サポートはこの値を使用して、アップロードされたパケットキャプチャを識別します。パケットキャプチャの最大サイズは 2 GB です。

ステップ 7 ケースを開始したり、Cisco TAC で操作したりする場合は、サポートエンジニアがパケットキャプチャにアクセスできるよう、アップロード識別子の値を含める必要があります。

Video Mesh ノード ウェブ インターフェイスからの Ping の実行

Video Mesh ノードのウェブインターフェイスから ping を実行できます。この手順では、入力した接続先をテストし、Video Mesh ノードが到達可能かどうかを確認します。

手順

ステップ 1 Webex Video Mesh ノードインターフェイスを開きます。

ステップ 2 **[トラブルシューティング（Troubleshooting）]** に移動し、**[Ping]** までスクロールして、**[ping を使用した接続のテスト（Test Connectivity Using Ping）]** の **[FQDN または IP アドレス（FQDN or IP Address）]** フィールドにテストする接続先アドレスを入力します。

ステップ 3 [Ping] をクリックします。

テストを実行すると、Ping の成功または失敗のメッセージが表示されます。テストにはタイムアウト制限はありません。失敗のメッセージが表示された場合、またはテストが無限に実行される場合は、入力した接続先の値とネットワーク設定を確認します。

Video Mesh ウェブ インターフェイスからのトレースルートの実行

Video Mesh ノード ウェブ インターフェイスからトレースルートを実行できます。この手順は、入力した接続先に向かってパケットがノードから取ったルートを示します。トレースルート情報を表示すると、特定の接続が不安定となり得る原因を特定し、問題を特定するのに役立ちます。

手順

ステップ 1 Webex Video Mesh ノードインターフェイスを開きます。

ステップ 2 **[トラブルシューティング（Troubleshooting）]** に移動し、**[トレースルート（Traceroute）]** までスクロールして、**[ホストへのトレースルート（Trace Route to Host）]** の **[FQDN または IP アドレス（FQDN or IP Address）]** フィールドにテストする接続先アドレスを入力します。

テストを実行すると、トレースルートの成功または失敗のメッセージが表示されます。テストは 16 秒後にタイムアウトします。失敗のメッセージが表示された場合、またはテストがタイムアウトする場合は、入力した接続先の値とネットワーク設定を確認します。

Video Mesh ノード ウェブ インターフェイスからの NTP サーバーの確認

Network Time Protocol（NTP）サーバーの FQDN または IP アドレスを入力して、Video Mesh ノードがサーバーにアクセス可能か確認できます。このテストは、時刻同期の問題に気付いて、NTP サーバーの到達可能性を除外する場合に役立ちます。

手順

ステップ 1 Webex Video Mesh ノードインターフェイスを開きます。

ステップ 2 **[トラブルシューティング（Troubleshooting）]** に移動し、**[NTP サーバーの確認（Check NTP Server）]** までスクロールして、**[SNTP クエリの応答の表示（View SNTP Query Response）]** の **[FQDN または IP アドレス（FQDN or IP Address）]** フィールドにテストする接続先アドレスを入力します。

テストを実行すると、クエリの成功または失敗のメッセージが表示されます。テストにはタイムアウト制限はありません。失敗のメッセージが表示された場合、またはテストが無限に実行される場合は、入力した接続先の値とネットワーク設定を確認します。

ウェブインターフェイスのリフレクタツールを使用したポートの問題の特定

必要な TCP/UDP ポートが Video Mesh ノードから開かれているかどうかを確認するため、リフレクタツール（Video Mesh ノードとクライアント上の Python スクリプトを使用したサーバーの組み合わせ）が使用されます。

始める前に

- https://github.com/CiscoDevNet/webex-video-mesh-reflector-client から Reflector ツールクライアント（Python スクリプト）のコピーをダウンロードします。
- スクリプトを正常に動作させるには、使用している環境で Python 2.7.10 またはそれ以降を実行していることを確認してください。
- 現在、このツールでは、Video Mesh ノードおよびクラスタ内検証に SIP エンドポイントをサポートしています。

手順

ステップ 1 https://admin.webex.com のカスタマービューで、値リストコレクション作成者のメンテナンスノードを有効にするには、次の手順に従います。

ステップ 2 ノードが Control Hub で [メンテナンス可能（Ready for maintenance）] ステータスを表示するまで待機します。

ステップ 3 Webex Video Mesh ノードインターフェイスを開きます。

この説明については、「ウェブインターフェイスからの Video Mesh ノードの管理 （144 ページ）」を参照してください。

ステップ 4 **[リフレクタツール（Reflector Tool）]** までスクロールし、使用するプロトコルに応じて **[TCP リフレクタサーバー（TCP Reflector Server）]** または **[UDP リフレクタサーバー（UDP Reflector Server）]** のいずれかを起動します。

ステップ 5 **[リフレクタサーバーの起動（Start Reflector Server）]** をクリックし、サーバーが正常に起動するまで待機します。

サーバーの起動時に通知が表示されます。

ステップ 6 Video Mesh ノードの到達先とするネットワーク上のシステム（PC など）から、次のコマンドでスクリプトを実行します。

```
$ python <local_path_to_client_script>/reflectorClient.py --ip <ip address of the server>
 --protocol <tcp or udp>
```

実行の終了時に、必要なすべてのポートが開かれている場合、クライアントは成功メッセージを表示します。

```
$ python reflectorClient.py --ip 10.22.162.102 --protocol tcp
Please wait while verifying tcp for ports: ['5004', '5060-5061'] ...
 [----------------------------->] 100.00%  Success/Failed/Total: 3/0/3

############################
No ports are blocked for tcp in ['5004', '5060-5061']
############################
Exiting Reflector Client tool...
$
```

必要なポートが開いていない場合、クライアントは、失敗した旨を通知するメッセージを示します。

```
$ python reflectorClient.py --ip 10.22.162.102 --protocol tcp --start-port 5060 --end-port 5062
Please wait while verifying tcp for port range: 5060 - 5062 ...
 [----------------------------->] 100.00%  Success/Failed/Total: 2/1/3

Failed ports in the first try:  ['5062']
Retrying(4 times) the above failed ports:
Retry number 1:
   Verifying port -> 5062
Retry number 2:
   Verifying port -> 5062
Retry number 3:
   Verifying port -> 5062
Retry number 4:
   Verifying port -> 5062
#########################
Ports which are not open for tcp are: ['5062']
#########################
Exiting Reflector Client tool...
```

ステップ 7 ファイアウォール上のポートの問題を解決してから、上記の手順を再実行します。

ステップ 8 詳細については、**--help** を使用してクライアントを実行してください。

```
$ python reflectorClient.py --help
Usage:
      --ip and --protocol are mandatory.
      If start-port is specified, end-port is considered mandatory. If no starting port is specified, default ports are verified for connectivity.
      By default, tool checks for QoS ports unless --non-qos option is specified.
      Default QoS ports include: TCP - 5004, 5060, 5061 and UDP - 5004, 52500-59499 and 63000-64667.
      Default non QoS ports include: TCP - 5004, 5060, 5061 and UDP - 5004, 34000-34999.
      To verify single port, both start and end port should be the required port to verify.
      Examples:
      Below run is to verify non-qos ports using an input port range:
        python reflectorClient.py --ip <hmn-ip-address> --protocol <udp/tcp> --start-port 52000 --end-port 52501 --non-qos
      Below run in to verify default qos ports:
        python reflectorClient.py --ip <> --protocol <udp/tcp>
$
```

Video Mesh ノード ウェブ インターフェイスからのデバッグユーザーアカウントの有効化

シスコ TAC が Webex Video Mesh ノードへのアクセスを要求する場合は、デバッグ用のユーザーアカウントを一時的に有効にすると、サポートによるさらなるトラブルシューティングの実行が可能になります。

手順

ステップ 1 Webex Video Mesh ノードインターフェイスを開きます。

ステップ 2 **[トラブルシューティング（Troubleshooting）]** に移動し、**[デバッグユーザーの有効化（Enable Debug User）]** 設定をオンに切り替えます。

シスコ TAC に提供できる暗号化されたパスフレーズが表示されます。

ステップ 3 パスフレーズをコピーし、サポートチケットに貼り付けるか、サポートエンジニアに直接貼り付け、保存したら **[OK]** をクリックします。

デバッグユーザーアカウントは 3 日後に失効します。

次のタスク

[トラブルシューティング（Troubleshooting）] ページに戻り、**[デバッグユーザーの有効化（Enable Debug User）]** 設定をオフに切り替えると、失効する前にアカウントを無効にできます。

ウェブインターフェイスからの Video Mesh ノードの工場出荷時状態へのリセット

登録解除のクリーンアップの一環として、ウェブインターフェイスから Video Mesh ノードを工場出荷時状態にリセットできます。この手順では、ノードがアクティブだったときに設定した内容が削除されますが、仮想マシンのエントリは削除されません。後で、最初から構築した別のクラスタの一部として、このノードを再登録できます。

始める前に

Control Hub を使用して、Control Hub に登録されているクラスタから Video Mesh ノードノードを登録解除する必要があります。

手順

ステップ 1 Webex Video Mesh ノードインターフェイスを開きます。

ステップ 2 **[トラブルシューティング（Troubleshooting）]** に移動し、**[初期設定へのリセット（Factory Reset）]** までスクロールして、**[ノードのリセット（Reset Node）]** をクリックします。

ステップ 3 警告プロンプトに表示される情報を理解したら、**[リセットおよび再起動（Reset and Reboot）]** をクリックします。

初期設定へのリセット後、ノードは自動的に再起動します。

ウェブインターフェイスからのローカル管理者アカウントの無効化または再有効化

Webex Video Mesh ノードをインストールする場合は、最初に「admin」というユーザー名の組み込みローカルアカウントを使用してサインインします。ノードを Webex クラウドに登録すると、Webex 組織の管理ログイン情報を使用して Control Hub から Video Mesh ノードを管理できるようになります。この方法により、Control Hub に適用される管理者アカウントポリシーと管理プロセスは、Video Mesh ノードにも適用されます。さらなる制御が必要な場合は、組み込みの「admin」アカウントを無効にして、Control Hub がすべての管理者の認証と管理を処理するようにすることができます。

ノードをクラウドに登録した後で、管理者ユーザーアカウントを無効化（または後で再有効化）するには、次の手順を使用します。管理者アカウントを無効にした場合は、Control Hub を使用してノードのウェブインターフェイスにアクセスする必要があります。

重要 この機能を使用できるのは、Webex 組織のフルアクセス権を持つ管理者のみです。他の管理者（パートナーや外部のフルアクセス権を持つ管理者を含む）は、Video Mesh リソース用に **[ノードに移動（Go To Node）]** オプションを持っている必要はありません。

手順

ステップ 1 https://admin.webex.com のカスタマービューから、**[サービス（Services）]** > **[ハイブリッド（Hybrid）]** に移動します。

ステップ 2 Video Mesh カードの **[リソース（Resources）]** で **[すべて表示（View all）]** をクリックします。

ステップ 3 クラスタをクリックし、アクセスするノードをクリックします。[ノードに進む（Go to Node）] をクリックします

ステップ 4 **[管理（Administration）]** に移動します。

ステップ 5 **[管理者ユーザーの有効化（Enable Admin User）]** スイッチをオフに切り替えてアカウントを無効にするか、またはオンに切り替えて再有効にします。

（注） ノードをクラウドに登録するまで、管理者アカウントを無効にすることはできません。

ステップ 6 確認画面で、**[無効（Disable）]** または **[有効（Enable）]** をクリックして変更を完了します。

管理者ユーザーを無効にすると、WebUI または SSH から起動した CLI から Video Mesh ノードにサインインできなくなります。ただし、VMware ESXi コンソールから起動した CLI を通じて、管理者ユーザーのログイン情報を使用してサインインすることはできます。

ウェブインターフェイスからの管理パスフレーズの変更

ウェブインターフェイスを使用して、Webex Video Mesh ノード用の管理者のパスフレーズ（パスワード）を変更するには、次の手順を使用します。

手順

ステップ 1 Webex Video Mesh ノードインターフェイスを開きます。

ステップ 2 **[管理（Administration）]** に移動し、**[パスフレーズの変更（Change Passphrase）]** の横にある **[変更（Change）]** をクリックします。

ステップ 3 **[現在のパスフレーズ（Current Passphrase）]**を入力し、**[新しいパスフレーズ（New Passphrase）]** と **[新しいパスフレーズの確認（Confirm New Passphrase）]** の両方に新しいパスフレーズの値を入力します。

ステップ 4 **[パスフレーズの保存（Save Passphrase）]** をクリックします。

「パスワードが変更されました（password changed）」というメッセージが表示され、[サインイン（Sign In）] 画面に戻ります。

ステップ 5 新しい管理者ログイン名とパスフレーズ（パスワード）を使用してサインインします。

ウェブインターフェイスからのパスフレーズの有効期間の変更

ウェブインターフェイスを使用して、デフォルトパスフレーズの有効期限の間隔を 90 日に変更するには、次の手順を使用します。間隔を広げると、Video Mesh ノードにサインインするときに新しいパスフレーズの入力を求められます。

手順

ステップ 1 Webex Video Mesh ノードインターフェイスを開きます。

ステップ 2 **[管理（Administration）]** に移動し、**[パスフレーズの有効期間の変更（Change Passphrase Expiry）]** の横で **[有効期限の間隔（日数）（Expiry Interval（Days））]** に新しい値を入力して、**[パスフレーズの有効期間の保存（Save Passphrase Expiry Interval）]** をクリックします。

成功した旨が画面に表示されたら、**[OK]** をクリックして終了します。

[管理（Administration）] ページには、最後にパスフレーズを変更した日と次回のパスワードの失効日も表示されます。

Syslog サーバーへの外部ロギングの設定

syslog サーバーがある場合、Webex Video Mesh ノードを設定して、外部サーバーの監査証跡情報にログを記録できます。以下は一例です。

- 管理者のサインインの詳細
- 設定の変更（メンテナンスモードのオン/オフを含む）
- ソフトウェアのアップデート

ノードは、ログがある場合は集約し、10 分ごとにサーバーに送信します。

手順

ステップ 1 Webex Video Mesh ノードインターフェイスを開きます。

ステップ 2 **[管理（Administration）]** に移動します。

ステップ 3 **[外部ロギング（External Logging）]** の横にある **[外部ロギングの有効化（Enable External Logging）]** をオンにします。

ステップ 4 **[Syslog サーバーの詳細（Syslog Server Details）]** で、ホスト IP アドレスまたは完全修飾ドメイン名と syslog ポートを入力します。

サーバーがノードから DNS 解決できない場合は、**[ホスト（Host）]** フィールドで IP アドレスを使用します。

ステップ 5 **[プロトコル（Protocol）]**（UDP または TCP）を選択します。

TLS 暗号化を使用するには、**[TCP]** を選択し、**[TLS の有効化（Enable TLS）]** をオンに切り替えます。ノードと syslog サーバー間の TLS 通信に必要なセキュリティ証明書もアップロードしてインストールしてください。証明書がインストールされていない場合、ノードはデフォルトで自己署名証明書を使用します。ヘルプについては、「セキュリティ証明書のアップロード （154 ページ）」を参照してください。

ステップ 6 **[外部ロギング設定の保存（Save External Logging Configuration）]** をクリックします。

ログメッセージのプロパティの形式は、優先順位 タイムスタンプ ホスト名 タグ メッセージです。

プロパティ	説明
Priority	式（優先順位 =（ファシリティ コード * 8）+ 重大度）に基づいて、値は常に 131 です。 「local0」の場合、ファシリティ コードは 16 です。「通知」の場合、重大度は 3 です。
タイムスタンプ	タイムスタンプの形式は「Mmm dd hh:mm:ss」です。

プロパティ	説明
ホストネーム	Video Mesh ノードのホスト名。
タグ	値は常に syslogAuditMsg です。
メッセージ	メッセージは、1 KB 以上の 1 つの JSON 文字列です。サイズは、10 分間の間隔で集約されたイベントの数によって異なります。

次にメッセージの例を示します。

```
{
  "events": [
    {
      "event": "{\hostname\": \"test-machine\", \"event_type\": \"login_success\",
       \"event_category\": \"node_events\", \"source\": \"mgmt\", \"session_data\":
       {\"session_id\": \"j02wH5uFTKB22SqdYCrzPrqDWkXIAKCz\", \"referer\":
       \"https://IP address/signIn.html?%2Fsetup\", \"url\":
       \"https://IP address/api/v1/auth/signIn\", \"user_name\": \"admin\",
       \"remote_address\": \"IP address\", \"user_agent\": \"Mozilla/5.0
       (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko)
       Chrome/87.0.4280.67 Safari/537.36\"}, \"event_data\": {\"type\": \"Conf_UI\"},
       \"boot_id\": \"6738705b-3ae3-4978-8502-13b74983e999\", \"timestamp\":
       \"2020-12-07 22:40:27 (UTC)\", \"uptime\": 358416.23, \"description\":
       \"Log in to Console or Web UI successful\"}"
    },
    {
      "event": "{\hostname\": \"test-machine\", \"event_type\":
       \"software_update_completed\", \"event_category\": \"node_events\", \"source\":
       \"mgmt\", \"event_data\": {\"release_tag\": \"2020.12.04.2332m\"}, \"boot_id\":
       \"37a8d17a-69d8-4b8c-809d-3265aec56b53\", \"timestamp\":
       \"2020-12-07 22:17:59 (UTC)\", \"uptime\": 137.61, \"description\":
       \"Completed software update\"}"
    }
  ]
}
```

Video Mesh アラートのウェブフック

Video Mesh は、組織管理者が特定のイベントに関するアラートを受信できるようにするウェブフックアラートをサポートしています。管理者は、コールオーバーフローやコールリダイレクトなどのイベントの通知を受け取ることを選択できるため、展開をモニタリングするために Control Hub にログインする必要が最小限に抑えられます。これは、アラートが送信されるターゲット URL が管理者によって提供されるウェブフック サブスクリプションを作成することによって実現されます。アラートにウェブフックを使用すると、関連するデベロッパー API を使用せずにパラメータをモニタリングすることもできます。

次のイベントタイプは、ウェブフックを介してモニターできます。

- クラスタコールリダイレクト（Cluster Call Redirects）：特定のクラスタからリダイレクトされたコール。
- 組織コールオーバーフロー（Org Call Overflows）：組織のクラウドへの合計コールオーバーフロー。

ウェブフックのサブスクリプションを作成する

手順

ステップ 1 管理者クレデンシャルを使用して Cisco Webex デベロッパー ポータルにログインします。

ステップ 2 デベロッパーポータルで、**[ドキュメント（ Documentation）]** をクリックします。

ステップ 3 左側のスクロールバーから下にスクロールし、**[全 API リファレンス（Full API Reference）]** をクリックします。

ステップ 4 下に展開するオプションから、下にスクロールして、**[ウェブフック（Webhooks）]** > **[ウェブフックの作成（Create a Webhook）]** の順にクリックします。

ステップ 5 次のパラメータを入力して、サブスクリプションを作成します。

例

- **name**：例 - Video Mesh ウェブフックアラート
- **targetUrl**：例 - https://10.1.1.1/webhooks
- **resource**：videoMeshAlerts
- **event**：triggered
- **ownedBy**：org

（注） targetUrl パラメータに入力された URL はインターネットにアクセス可能であり、Webex Webhook によって送信された POST リクエストを受け入れるように設定されたサーバーが必要です。

開発者 API を使用したしきい値構成を設定する

Video Mesh デベロッパー API を使用して、イベント（組織コールオーバーフローとクラスタコールリダイレクト）のしきい値を設定できます。しきい値のパーセンテージ値を設定できます。この値を超えると、ウェブフックアラートがトリガーされます。たとえば、組織コールオーバーフローのしきい値が 20 に設定されている場合、20% を超えるコールがクラウドにオーバーフローするとアラートが送信されます。

Cisco Webex デベロッパーポータルでしきい値を設定および更新するには、次の 4 つの API のセットを使用できます。

- イベントしきい値の設定のリスト

- イベントしきい値の設定の取得
- イベントしきい値の設定の更新
- イベントしきい値の設定のリセット

API は https://developer.webex.com/docs/api/v1/video-mesh で入手できます。

シナリオ 1：オーバーフローした組織コールのしきい値を設定する

手順

ステップ 1 **[イベントしきい値の設定のリスト（List Event Threshold Configuration）]** API をクリックします。

ステップ 2 イベントスコープ を **ORG** に設定し、**[実行（Run）]** をクリックします。

ステップ 3 次のようなレスポンスが表示されます。

例：

```
{
"eventName": "orgCallsOverflowed",
"eventThresholdId":
"Y2lzY29zcGFyazovL3VzL0VWRU5ULzQyN2U5ZTk2LTczYTctNDYwYS04MGZhLTcyNWU4MWE2MDg3ZjowM2ZkYjkzZC1jNTllLT
QzMjQtODIwNS1lNDIyYzA3NGQ5Mzg",
"eventScope": "ORG",
"entityId":
"Y2lzY29zcGFyazovL3VzL09SR0FOSVpBVElPTi8yYzNjOWY5NS03M2Q5LTQ0NjAtYTY2OC0wNDcxNjJmZjFiYWQ",
"thresholdConfig": {
"minThreshold": 10,
"defaultMinThreshold": 10
}
```

ステップ 4 「eventThresholdId」フィールドの値をコピーします。これは、しきい値を更新および取得するために使用されるイベントしきい値 ID です。

ステップ 5 次に示す JSON 構造の「eventThresholdId」フィールドに値を貼り付け、JSON 構造全体をコピーします。

例：

```
[
{
"eventThresholdId":
"Y2lzY29zcGFyazovL3VzL0VWRU5UL2E3YmM3ODE2LWU3YTAtNDk0Zi1iZDZhLTRhMGIyNWY2OGFhNjoyNWE3ODY1Yi0yYjQ3
LTM4M2YtYWI3YS00MzYxY2ExN2FiOTI",
"thresholdConfig": {
"minThreshold": 5
}
}
```

ステップ 6 **[イベントしきい値の設定の更新（Update Event Threshold Configuration）]** API をクリックします。

ステップ 7 **[イベントしきい値の設定の更新（Update Event Threshold Configuration）]** API の本文に JSON 構造を貼り付けます。

ステップ 8 「minThreshold」値を、設定する新しいしきい値に設定します。

ステップ 9 （注） JSON構造にカンマ区切り値として入力することで、複数のイベントしきい値IDに対してこの操作を実行できます。

[実行（Run）] をクリックすると、**[組織コールオーバーフロー（Org Call Overflows）]** のしきい値が新しい値に設定されます。

次のタスク

特定のイベントしきい値 ID に設定されているしきい値を表示するには、

- **[イベントしきい値の設定の取得（Get Event Threshold Configuration）]** API をクリックします。
- イベントしきい値 ID を API のヘッダーに貼り付け、**[実行（Run）]** をクリックします。
- デフォルトの最小しきい値と設定されたしきい値がレスポンスに表示されます。

シナリオ 2：リダイレクトされたクラスタコールのしきい値を設定する

手順

ステップ 1 **[イベントしきい値設定のリスト（List Event Threshold Configuration）]** API をクリックします。

ステップ 2 イベントスコープ を **[クラスタ（CLUSTER）]** に設定し、**[実行（Run）]** をクリックします。

ステップ 3 レスポンスには、組織内のすべてのクラスタの設定がリストされます。

ステップ 4 （注） 特定のクラスタの設定を受信するには、clusterID パラメータを入力します。

値を更新するクラスタの「eventThresholdId」フィールドの値をコピーします。これは、しきい値を更新および取得するために使用されるイベントしきい値 ID です。

ステップ 5 次に示す JSON 構造の「eventThresholdId」フィールドに値を貼り付け、JSON 構造全体をコピーします。

例：

```
[
{
"eventThresholdId":
"Y2lzY29zcGFyazovL3VzL0VWRU5UL2E3YmM3ODE2LWU3YTAtNDk0Zi1iZDZhLTRhMGIyNWY2OGFhNjoyNWE3ODY1Yi0yYjQ3
LTM4M2YtYWI3YS00MzYxY2ExN2FiOTI",
"thresholdConfig": {
"minThreshold": 5
}
}
]
```

ステップ 6 **[イベントしきい値の設定の更新（Update Event Threshold Configuration）]** API をクリックします。

ステップ 7 **[イベントしきい値の設定の更新（Update Event Threshold Configuration）]** API の本文に JSON 構造を貼り付けます。

ステップ 8 「minThreshold」 値を、設定する新しいしきい値に設定します。

ステップ 9 （注） JSON構造にカンマ区切り値として入力することで、複数のイベントしきい値IDに対してこの操作を実行できます。

[実行（Run）] をクリックすると、**[リダイレクトされたクラスタコール（Cluster Calls Redirected）]** のしきい値が新しい値に設定されます。

次のタスク

特定のイベントしきい値 ID に設定されているしきい値を表示するには、

- **[イベントしきい値の設定の取得（Get Event Threshold Configuration）]** API をクリックします。
- イベントしきい値 ID を API のヘッダーに貼り付け、**[実行（Run）]** をクリックします。
- デフォルトの最小しきい値と設定されたしきい値がレスポンスに表示されます。

シナリオ 3：しきい値をリセットする

手順

ステップ 1 **[イベントしきい値の設定のリセット（Reset Event Threshold Configuration ）]** をクリックします。

ステップ 2 クラスタまたは組織のイベントしきい値 ID をコピーし、以下の JSON 構造の「eventThresholdId」 フィールドに貼り付けます。

例：

```
{
"eventThresholdIds": [
"Y2lzY29zcGFyazovL3VzL0VWRU5ULzQyN2U5ZTk2LTczYTctNDYwYS04MGZhLTcyNWU4MWE2MDg3Zjo2YzJhZGRmMS0wYjAz
LTRiZWEtYjIxYy0xYzFjYzdiY2UwOWQ"
]
}
```

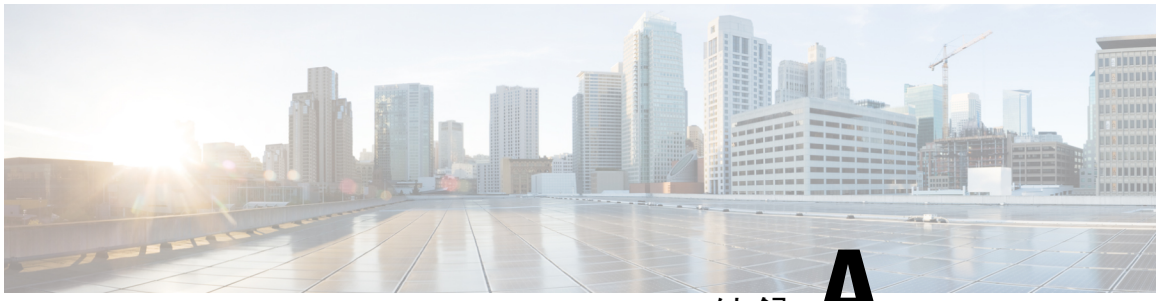
ステップ 3 JSON 構造を本文に貼り付け、**[実行（Run）]** をクリックします。

ステップ 4 （注） JSON構造にカンマ区切り値として入力することで、複数のイベントしきい値IDのしきい値をリセットできます。

しきい値はデフォルトの最小値に設定されます。

Video Mesh デベロッパー API

Video Mesh デベロッパー API は、Webex デベロッパーポータルを介して Video Mesh 展開の分析およびモニタリングデータを取得する方法です。API は https://developer.webex.com/docs/api/v1/video-mesh で入手できます。サンプルクライアントは https://github.com/CiscoDevNet/video-mesh-api-client にあります。



付録 A

付録

Video Mesh ノード デモ用ソフトウェア

Video Mesh ノードデモソフトウェアは基本的なデモのためだけに使用してください。デモノードを既存の本稼働クラスタに追加しないでください。デモ用クラスタは、本稼働のクラスタよりも受け入れるコールが少なく、クラウドに登録してから 90 日で期限が切れます。

（注）
- Video Mesh ノード デモ用ソフトウェアは、Cisco TAC ではサポートされていません。
- Video Mesh ノード デモソフトウェアを完全な実稼働ソフトウェアバージョンにアップグレードすることはできません。

このリンクからデモソフトウェアイメージをダウンロードしてください。

仕様

Video Mesh ノード ソフトウェアのスペックベースの構成については、「Video Mesh ノード ソフトウェアのシステム要件とプラットフォーム要件 （12 ページ）」を参照してください。

デモソフトウェアは、単一のネットワークインターフェイスまたはデュアルネットワークインターフェイスのいずれかをサポートします。

容量

キャパシティに対するデモイメージは、テストしません。これは、ミーティングの基本的なシナリオをテストするためだけに使用してください。ガイダンスとして、次のユースケースを参照してください。

Video Mesh ノード デモソフトウェアのユースケース

メディアがオンプレミスに固定されている

- デモ用ソフトウェアを使用して、ノードを展開し、構成する。
- 次の参加者を含むミーティングを実行する。Webex アプリ の参加者、Webex エンドポイントの参加者、および Cisco Webex Board。
- ミーティングが終了したら、https://admin.webex.com のカスタマービューで **[分析（Analytics）]** に移動して Video Mesh レポートにアクセスします。このレポートで、メディアがオンプレミスのままだったことがわかります。

クラウドとオンプレミスの参加者によるミーティング

- オンプレミスで Webex の参加者が数人とクラウドから 1 人参加している別のミーティングを実行します。
- すべての参加者がミーティングにシームレスに接続して参加できることを確認します。

コンソールからの Video Mesh ノードの管理

クラウドに登録されている Video Mesh ノードのネットワークを変更する前に、Control Hub を使用してノードをメンテナンスモードにする必要があります。詳細および従うべき手順については、「ノードのメンテナンスモードへの移行」を参照してください。

注意 メンテナンスモードは、特定のネットワーキング設定の変更（DNS、IP、FQDN）を行ったり、RAM やハードドライブの置き換えなどのハードウェア メンテナンスの準備を行ったりできるよう、ノードのシャットダウンまたは再起動を準備することのみを意図しています。

ノードがメンテナンスモードになっている場合、アップグレードは行われません。

ノードをメンテナンスモードにすると、コールサービスのグレースフルシャットダウンを実行します（新しいコールの受け入れを停止し、既存のコールが完了するまで最大 2 時間待機します）。コールサービスのグレースフルシャットダウンの目的は、コールのドロップを引き起こすことなく、ノードの再起動またはシャットダウンを可能にすることです。

コンソールでの Video Mesh ノードネットワーク設定の変更

ネットワークトポロジが変更された場合は、各 Video Mesh ノードのためにコンソールインターフェイスを開いて、そこでネットワーク設定を変更する必要があります。ネットワーク構成の変更については注意が表示されますが、Video Mesh ノードの設定を変更した後にネットワークに変更を加える場合は、変更を保存することができます。

手順

ステップ 1 VMware vSphere クライアントを通じてノードコンソールのインターフェイスを開き、管理者のログイン情報を使用してサインインします。

初めてネットワーク設定をセットアップした後、Video Meshが到達可能である場合は、セキュアシェル（SSH）を通じてノードインターフェイスにアクセスできます。

ステップ 2 Video Mesh ノード コンソールのメインメニュー で、**[2 構成の編集（2 Edit Configuration）]** のオプションを選択し、**[選択（Select）]** をクリックします。

ステップ 3 Video Mesh ノード でのコールの終了を求めるプロンプトを読み、**[はい（Yes）]** をクリックします。

ステップ 4 **[静的（Static）]** をクリックして、内部インターフェイスの **[IP アドレス（IP address）]**、ネットワークの、**[マスク（Mask）]**、**[ゲートウェイ（Gateway）]**、**[DNS]** の各値を入力します。

- Video Mesh ノード は、内部 IP アドレスと解決可能な DNS 名を持っている必要があります。ノード IP アドレスは、Video Mesh ノード 内部使用のために予約されている IP アドレスの範囲に属していてはなりません。デフォルトの予約済みIPアドレスの範囲は172.17.42.0 ～ 172.17.42.63 で、**[診断（Diagnostic）]** メニューで設定できます。この IP アドレスの範囲は、Video Mesh ノード 内、およびノードのさまざまなコンポーネント（SIP インターフェイスやメディアトランスコーディングなど）を保持するソフトウェアコンテナ間における通信のためのものです。
- すべてのノードを同じサブネットまたは VLAN に展開します。これにより、クラスタ内のすべてのノードは、ネットワーク内のクライアントのどこからでも到達可能になります。
- デュアル NIC DMZ を導入する場合は、内部ネットワーク構成を保存してノードをリブートした後、次の手順で外部 IP アドレスを設定することができます。

ステップ 5 組織の NTP サーバーまたは組織で使用可能な別の外部 NTP サーバーを入力します。

NTP サーバーを設定し、ネットワーク設定を保存した後は、「コンソールからの Video Mesh ノードの正常性チェック （179 ページ）」の手順に従って、指定されたNTPサーバーを介して時刻が正しく同期されていることを確認できます。

（注） 複数の NTP サーバーを設定する場合、フェールオーバーのポーリング間隔は 40 秒です。

ステップ 6 （オプション）必要に応じて、ホスト名またはドメインを変更します。

（注）
- クラウドに問題なく登録できるように、Video Mesh ノードに設定するホスト名は小文字のみを使用します。現時点では、大文字と小文字はサポートされていません。
- FQDN またはホスト名を使用または設定する場合は、有効で解決可能なドメインを入力する必要があります。FQDN の長さは、64 文字以下にする必要があります。

ステップ 7 **[保存（Save）]** をクリックし、**[変更を保存して再起動（Save Changes & Reboot）]** の順に選択します。

ドメインを指定した場合は、保存中に DNS の検証が行われます。指定された DNS サーバーアドレスを使用して FQDN（ホスト名とドメイン）を解決できない場合、警告が表示されます。警告を無視して保存を選択できますが、ノードに設定されている DNS で FQDN を解決できるまで、コールは機能しません。Video Mesh ノード リブート後、ネットワーク構成の変更が有効になります。

Video Mesh ノード管理者のパスフレーズの変更

ノードのコンソールで Video Mesh ノード用の管理者のパスフレーズ（パスワード）を変更するには、次の手順を使用します。

手順

ステップ 1 VMware vSphere クライアントまたは到達可能な IP アドレスへとつながる SSH を通じてノードコンソールのインターフェイスを開き、管理者のログイン情報を使用してサインインします。

ステップ 2 Video Mesh ノードの VM の VMware ESXi コンソールを開いてログインします。

ステップ 3 メイン メニューで、**[3 管理者パスフレーズの管理（3 Manage Administrator Passphrase）]** オプションを選択し、次に **[1 管理者パスフレーズの変更（1 Change Administrator Passphrase）]** を選択して **Enter** キーを押します。

ステップ 4 [パスワードの有効期限が切れています] ページの情報を読み、**Enter** キーを押し、パスワードの有効期限のメッセージの後にもう一度押します。

ステップ 5 Enter を押します。

ステップ 6 コンソールからサインアウトすると [サインイン（Sign In）] 画面に戻るため、管理者のログイン名と期限切れのパスフレーズ（パスワード）を使用してサインインします。
パスワードの変更を求めるプロンプトが表示されます。

ステップ 7 [現在のパスワード（Old password）] に、現在のパスフレーズを入力してから **Enter** キーを押します。

ステップ 8 [新しいパスワード（New password）] に新しいパスフレーズを入力し、**Enter** キーを押します。

ステップ 9 [新しいパスワードの再入力（Re-enter new password）] に新しいパスフレーズを再入力し、**Enter** キーを押します。

「パスワードが変更されました（password changed）」というメッセージが表示され、[サインイン（Sign In）] 画面に戻ります。

ステップ 10 新しい管理者ログイン名とパスフレーズ（パスワード）を使用してサインインします。

Video Mesh ノードコンソールからの Ping の実行

Video Mesh ノードのコンソールインターフェイスから ping を実行できます。この手順では、入力した宛先をテストし、Video Mesh ノードが到達可能かどうかを確認します。

手順

ステップ 1 VMware vSphere クライアントまたは到達可能な IP アドレスへとつながる SSH を通じてノードコンソールのインターフェイスを開き、管理者のログイン情報を使用してサインインします。

ステップ 2 Video Mesh ノードコンソールから、**[4 診断（4 Diagnostics）]** に移動し、**[Ping]** を選択します。

ステップ 3 **[Ping]** フィールドに、IP アドレスやホスト名など、テストする宛先アドレスを入力し、**[OK]** をクリックします。

テストを実行すると、Ping の成功または失敗のメッセージが表示されます。失敗メッセージが表示される場合は、入力した宛先の値とネットワーク設定を確認します。

コンソールを通じたデバッグユーザーアカウントの有効化

サポートが Video Mesh ノードへのアクセスを要求した場合、コンソールインターフェイスを使用してデバッグユーザーアカウントを一時的に有効にし、サポートがノードで詳細なトラブルシューティングを実行できるようすることができます。

手順

ステップ 1 VMware vSphere クライアントまたは到達可能な IP アドレスへとつながる SSH を通じてノードコンソールのインターフェイスを開き、管理者のログイン情報を使用してサインインします。

ステップ 2 Video Mesh ノードコンソールから、**[4 診断（4 Diagnostics）]** に移動し、**[2 デバッグユーザーアカウントの有効化（2 Enable Debug User Account）]** を選択して、プロンプトが表示されたら、**[はい（Yes）]** をクリックします。

ステップ 3 デバッグユーザーアカウントが正常に作成されたことを示すメッセージが表示されたら、**[OK]** をクリックして、暗号化されたパスフレーズを表示します。

暗号化されたパスフレーズをサポートに送信します。トラブルシューティングのために、この一時的なアカウントを使用し、パスフレーズを解読して Video Mesh ノードに安全にアクセスします。このアカウントは、3 日後に有効期限が切れるか、サポートが終了した時点で無効にできます。

ステップ 4 暗号化されたデータの開始と終了を選択してコピーし、サポートに送信するサポートチケットまたは電子メールに貼り付けます。

ステップ 5 この情報をサポートに送信した後、Video Mesh ノードコンソールに戻り、任意のキーを押してメインメニューに戻ります。

次のタスク

アカウントの有効期間は3日間ですが、ノードのトラブルシューティングが終了した旨の通知がサポートからあった場合は、Video Mesh ノードコンソールに戻り、**[4 診断（4 Diagnostics）]** に移動し、**[3 デバッグユーザーアカウントを無効にする（3 Disable Debug User Account）]** を選択して、失効前にアカウントを無効化できます。

Video Mesh ノードコンソールからのログの送信

Cisco または Secure Copy（SCP）に、ログを直接送信するよう指示される場合があります。クラウドに登録した Video Mesh ノードからログを直接送信するには、次の手順を実行し ます。

手順

ステップ 1 VMware vSphere クライアントまたは到達可能な IP アドレスへとつながる SSH を通じてノードコンソールのインターフェイスを開き、管理者のログイン情報を使用してサインインします。

ステップ 2 メイン メニューで、**[4 診断（4 Diagnostics）]** オプションをクリックし、**Enter** キーを押します。

ステップ 3 **[4 ログファイルのエクスポート（4 Export Log Files）]** をクリックし、必要に応じてフィードバックを提供し、**[次へ（Next）]** をクリックします。

ステップ 4 次のオプションを選択します。

- **SCP を使用してログを送信し**、ログのエクスポートを確認して、SCP の詳細（**ホスト**、**ユーザー名**、**Dest_Folder**）を入力し、 **[OK]** をクリックします。
- **[Cisco にログを送信（Send Logs to Cisco）]** を選択し、ログをエクスポートすることを確認します。

ステップ 5 Video Mesh ノードのメインメニューに戻るには、**[OK]** を選択します。

ステップ 6 （任意） ログを Cisco に送信した場合は、**[Cisco に送信したログファイルのステータスを確認（Check Status of Log Files Sent to Cisco）]** を選択します。

次のタスク

ヒント ログを送信した後、Webex アプリ からフィードバックを直接送信することを推奨します。これにより、サポート連絡先にすべての情報を提供することができます。

関連トピック

サポートに問い合わせる

コンソールからの Video Mesh ノードの正常性チェック

ノードの正常性は、Video Mesh ノードから直接表示できます。結果は情報提供に過ぎませんが、トラブルシューティング手順で役立つ場合があります。たとえば、NTP の同期が動作していなければ、ネットワーク構成の NTP サーバーの値を確認できます。

手順

ステップ 1 VMware vSphere クライアントまたは到達可能な IP アドレスへとつながる SSH を通じてノードコンソールのインターフェイスを開き、管理者のログイン情報を使用してサインインします。

ステップ 2 Video Mesh ノードコンソールから **[4 診断（4 Diagnostics）]** に移動し、**[6 ノードの正常性を確認（6 Check Node Health）]** を選択してノードに関する次の情報を表示します。

- **管理サービスコンテナ**
- **ETCD**（クラスタ全体でデータを確実に保存するキー バリュー型ストア）
- **同期済み NTP**
- **ディスク容量（空き/使用済み %）**
- **メモリ（空き/使用済み %）**

Video Mesh ノード上のコンテナネットワークの設定

Video Meshノードは、ノード内での内部使用のためのサブネット範囲を予約します。デフォルトの範囲は、172.17.42.0 ～ 172.17.42.63 です。ノードは、この範囲から発信される外部からVideo Mesh ノードへのトラフィックには応答しません。ネットワーク内の他のデバイスと競合しないように、コンテナのブリッジ IP アドレスを変更するためにノードコンソールを使用することもできます。

手順

ステップ 1 VMware vSphere クライアントまたは到達可能な IP アドレスへとつながる SSH を通じてノードコンソールのインターフェイスを開き、管理者のログイン情報を使用してサインインします。

ステップ 2 Video Mesh ノードコンソールのメインメニューから、**[4 診断（4 Diagnostics）]** に移動し、**[7 コンテナネットワークの構成（7 Configure Container Network）]** を 選択します。このノードでアクティブなコールが終了することを示す注意が表示されたら、**[はい（Yes）]** をクリックします。

ステップ 3 必要に応じて **[コンテナ ブリッジ IP（Container Bridge IP）]** と **[ネットワークマスク（Network Mask）]** の値を変更し、**[保存（Save）]** をクリックします。

Video Mesh ノード上の内部操作用として予約されている IP アドレスの範囲を含む、コンテナネットワーク情報を表示する画面が表示されます。

ステップ 4 **[OK]** をクリックします。

コンソールでのリフレクタツールを使用したポートの問題の特定

必要な TCP/UDP ポートが Video Mesh ノードから開かれているかどうかを確認するため、リフレクタツール（Video Mesh ノードとクライアント上の Python スクリプトを使用したサーバーの組み合わせ）が使用されます。

始める前に

- リフレクタツールクライアント（Python スクリプト）のコピーをダウンロードし、簡単に見つけられる場所にそのファイルを解凍します。Zip ファイルには、スクリプトと Readme ファイルが含まれています。
- スクリプトを正常に動作させるには、使用している環境で Python 2.7.10 またはそれ以降を実行していることを確認してください。
- 現在、このツールでは、Video Mesh ノードおよびクラスタ内検証に SIP エンドポイントをサポートしています。

手順

ステップ 1 https://admin.webex.com のカスタマービューで、値リストコレクション作成者のメンテナンスノードを有効にするには、次の手順に従います。

ステップ 2 ノードが Control Hub で [メンテナンス可能（Ready for maintenance）] ステータスを表示するまで待機します。

ステップ 3 VMware vSphere クライアントまたは到達可能な IP アドレスへとつながる SSH を通じてノードコンソールのインターフェイスを開き、管理者のログイン情報を使用してサインインします。

ステップ 4 値リストコレクション作成者インターフェイスから、**[診断（Diagnostics）] > [リフレクタサーバー（Reflector Server）] > [TCP または（UDP）向けのリフレクタサーバ（Reflector Server for TCP or (UDP)）]** の順に選択します。TCP または UDP のいずれかのサーバーを起動します。

ステップ 5 **[リフレクタツール（Reflector Tool）]** までスクロールし、使用するプロトコルに応じて **[TCP リフレクタサーバー（TCP Reflector Server）]** または **[UDP リフレクタサーバー（UDP Reflector Server）]** のいずれかを起動します。

ステップ 6 **[リフレクタサーバーの起動（Start Reflector Server）]** をクリックし、サーバーが正常に起動するまで待機します。

サーバーの起動時に通知が表示されます。

ステップ 7 Video Mesh ノードの到達先とするネットワーク上のシステム（PC など）から、次のコマンドでスクリプトを実行します。

```
$ python <local_path_to_client_script>/reflectorClient.py --ip <ip address of the server>
 --protocol <tcp or udp>
```

実行の終了時に、必要なすべてのポートが開かれている場合、クライアントは成功メッセージを表示します。

```
$ python reflectorClient.py --ip 10.22.162.102 --protocol tcp
Please wait while verifying tcp for ports: ['5004', '5060-5061'] ...
 [------------------------------>] 100.00%  Success/Failed/Total: 3/0/3

############################
No ports are blocked for tcp in ['5004', '5060-5061']
############################
Exiting Reflector Client tool...
$
```

必要なポートが開いていない場合、クライアントは、失敗した旨を通知するメッセージを示します。

```
$ python reflectorClient.py --ip 10.22.162.102 --protocol tcp --start-port 5060 --end-port 5062
Please wait while verifying tcp for port range: 5060 - 5062 ...
 [------------------------------>] 100.00%  Success/Failed/Total: 2/1/3

Failed ports in the first try:  ['5062']
Retrying(4 times) the above failed ports:
Retry number 1:
   Verifying port -> 5062
Retry number 2:
   Verifying port -> 5062
Retry number 3:
   Verifying port -> 5062
Retry number 4:
   Verifying port -> 5062
#########################
Ports which are not open for tcp are: ['5062']
#########################
Exiting Reflector Client tool...
```

ステップ 8 ファイアウォール上のポートの問題を解決してから、上記の手順を再実行します。

ステップ 9 詳細については、**--help** を使用してクライアントを実行してください。

```
$ python reflectorClient.py --help
Usage:
      --ip and --protocol are mandatory.
      If start-port is specified, end-port is considered mandatory. If no starting port is specified, default ports are verified for connectivity.
      By default, tool checks for QoS ports unless --non-qos option is specified.
      Default QoS ports include: TCP - 5004, 5060, 5061 and UDP - 5004, 52500-59499 and 63000-64667.
      Default non QoS ports include: TCP - 5004, 5060, 5061 and UDP - 5004, 34000-34999.
      To verify single port, both start and end port should be the required port to verify.
      Examples:
      Below run is to verify non-qos ports using an input port range:
        python reflectorClient.py --ip <hmn-ip-address> --protocol <udp/tcp> --start-port 52000 --end-port 52501 --non-qos
      Below run in to verify default qos ports:
        python reflectorClient.py --ip <> --protocol <udp/tcp>
$
```

コンソールからの Video Mesh ノードの工場出荷時状態へのリセット

登録解除のクリーンアップの一部として、Video Mesh ノードを初期設定へのリセットすることができます。この手順では、ノードがアクティブだったときに設定した内容が削除されますが、仮想マシンのエントリは削除されません。後で、最初から構築した別のクラスタの一部として、このノードを再登録できます。

始める前に

Control Hub を使用して、Control Hub に登録されているクラスタから Video Mesh ノードを登録解除する必要があります。

手順

ステップ 1 VMware vSphere クライアントまたは到達可能な IP アドレスへとつながる SSH を通じてノードコンソールのインターフェイスを開き、管理者のログイン情報を使用してサインインします。

ステップ 2 Video Mesh ノードコンソールで、**[4 診断（4 Diagnostics）]** に移動して、**[8 初期設定へのリセット（8 Factory Reset）]** を選択し ます。

ステップ 3 注意事項に表示される情報を理解したら、**[リセット（Reset）]** をクリックします。

初期設定へのリセット後、ノードは自動的に再起動します。

既存のハードウェアプラットフォームからの Video Mesh ノードへの移行

サポートされている既存のプラットフォーム（Cisco Meeting Server を実行する CMS1000 など）を Video Mesh に移行できます。次の手順を使用して、移行プロセスを実行します。

（注） この手順は、ハードウェアプラットフォーム上の ESXi のバンドルバージョンに応じて異なります。

始める前に

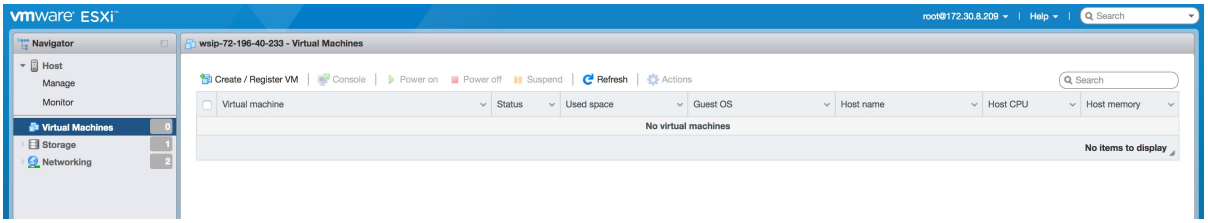
最新の Video Mesh ノードソフトウェアのイメージ（OVA）の新しいコピーをダウンロードします。前にダウンロードした OVA を使用して新しい Video Mesh ノードを展開しないでください。

手順

ステップ 1 仮想マシンインターフェイスにサインインし、プラットフォーム上で実行されているソフトウェアをシャットダウンします。

ステップ 2 プラットフォーム上で実行されていたソフトウェアアプリケーションを削除します。

プラットフォーム上にソフトウェアイメージが残っていないようにする必要があります。また、同じプラットフォーム上の他のソフトウェアと一緒に Video Mesh ノードソフトウェアを実行することはできません。

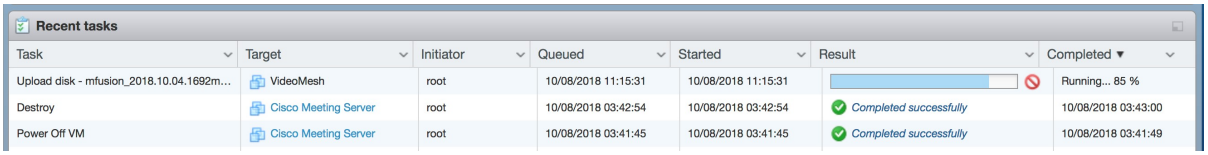


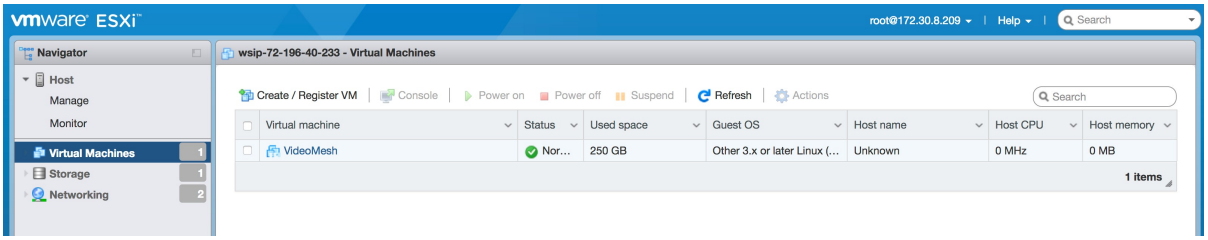
ステップ 3 新しい OVF または OVA ファイルから新しい仮想マシンを展開します。

ステップ 4 仮想マシンの名前を入力し、Video Mesh ノード の OVA ファイルを選択します。

ステップ 5 ディスクプロビジョニングを [Thick（シック）] に変更します。

ステップ 6 ダウンロードした **mfusion.ova** ソフトウェアイメージをアップロードします。





ステップ 7 仮想マシンが実行されている場合は、「Video Mesh ノード コンソールへのログイン （59 ページ）」に戻って、Video Mesh ノードの初期設定を続行します。

Collaboration Meeting Room Hybrid から Video Mesh への移行パスと機能比較

機能の比較

CMR ハイブリッドから Video Mesh に移行する際の利点を把握するために役立つよう、この表では、各オファーの主要機能を並べて比較しています。Video Mesh に関して下記に詳述されている新機能同様、Video Mesh と組み合わせた際は、既存の Webex 機能もこれまで通り作動します。ミーティングの機能拡張に加えて、Video Mesh は、クラウドベースの管理へのアジリティを利用し、既存の投資を継続的に保護することができます。

機能	Video Mesh および Cisco Webex Meeting Center ビデオ	CMRハイブリッド
会議の種類	スケジュール済み ワンクリック（インスタント） パーソナルミーティング（PMR） オンプレミスとクラウドベースのミーティングで一貫性のあるエクスペリエンス	スケジュール済みのみ
スケジューリング	Webex 生産性向上ツール（Windows および Mac） @webex を使用したハイブリッドカレンダーのスケジュール設定 Webex ポータル	Webex 対応 TelePresence の Windows および Mac 生産性向上ツール TMS のスケジュール設定
ミーティング参加オプション	ダイヤルインとダイヤルアウト PIN による保護（ホスト） ワンボタン機能（OBTP）	ダイヤルインのみ OBTP
ミーティング中のエクスペリエンス	統一名簿（Webex クライアント） 統一されたコントロール（Webex クライアント） ミーティングのロック/ロック解除 TelePresence 参加者のミュート/ミュート解除	統一名簿なし（Webex クライアントと Telepresence Server） ばらばらのコントロール（Webex クライアントと Telepresence Server）

機能	Video Mesh および Cisco Webex Meeting Center ビデオ	CMRハイブリッド
キャパシティと展開モデル	無制限のキャパシティ オンプレミスと自動オーバーフロー スイッチングとトランスコーディング	トランスコーディングキャパシティは TelePresence Server に限定

移行パスのチェックリスト

以下は、既存のサイトをビデオ プラットフォーム バージョン 2.0 に移行して、そのサイトを Video Mesh に統合するための準備方法に関するハイレベルの概要です。この手順は、既存の環境によって異なる場合があります。パートナーまたはカスタマー サクセス マネージャと協力して、スムーズな移行を行います。

1. Meeting Center Video の会議機能が Webex サイトにプロビジョニングされていることを確認します。
2. サイト管理者が、管理ポータルアカウントを受け取ります。次に、管理者は Webex 組織の Video Mesh ノードを展開します。
3. サイト管理者は、CMR Hybrid ユーザーのすべてまたは一部が Cisco Webex Meeting Center ビデオを利用できるように CMR の権限を割り当てます。
4. （オプション）このサブセットに対する CMR Hybrid セッション タイプを無効にして、ユーザープロファイルの Cisco Webex Meeting Center ビデオを有効にします。
5. サイト管理者が設定 Video Mesh を行い、**[ud Collaboration Meeting Room オプション（Cloud Collaboration Meeting Room Options）]** でメディアリソースの種類として、**[ハイブリッド（Hybrid）]** を選択します。
6. サイト管理者が、オンプレミスの TelePresence Management Suite（TMS）とワンボタン機能（OBTP）をセットアップし、Cisco Webex Meeting Center ビデオと連携させます。ガイダンスとして、『*Cisco Webex Meeting Center* ビデオ会議エンタープライズ導入ガイド』[英語] を参照してください。
7. ユーザーの CMR 権限を有効にすると、Webex 生産性向上ツールは、デフォルトの Cisco Webex Meeting Center ビデオ バージョンに設定されます。ユーザーがスケジュールを設定した新しいミーティングは、すべて Cisco Webex Meeting Center ビデオミーティングです。
8. 招待に会議室が含まれている場合、OBTP 情報が TMS を介して会議室にプッシュされます（CMR ハイブリッドミーティングの場合のみ）。
9. CMR ハイブリッドユーザーが Cisco Webex Meeting Center ビデオに切り替わる前に設定した既存のミーティングは、オンプレミスの MCU と TMS の設定が維持される限り、引き続き機能するはずです。

10. 既存の CMR ハイブリッド ミーティングを変更または更新して、Cisco Webex Meeting Center ビデオ ミーティング情報を反映させることはできません。ユーザーが新しい招待を使用する場合は、古いミーティングを削除し、新しいミーティングを作成する必要があります。
11. オンプレミスの MCU、TMS を廃止する場合、古い CMR ハイブリッドミーティングは機能しなくなります。Cisco Webex Meeting Center ビデオ情報を使用して、新しいミーティングを作成する必要があります。

TelePresence 相互運用性プロトコルとセグメント切り替え

Video Mesh 1 画面と 3 画面の両方の IX と TX エンドポイントに対して、TelePresence 相互運用性プロトコル（TIP）と多重化（MUX）のネゴシエーションをサポートしています。

3 画面のエンドポイントでは、会議の参加者数が十分な場合、3 つのすべての画面にビデオを表示します。会議内に別の 3 画面システムが存在する場合は、部屋の切り替えではなく、セグメントの切り替えが行われます。つまり、別の 3 画面システムで誰かが話している場合に、3 つの画面すべてが拡大表示されるのではなく、アクティブなペインだけが拡大表示されます。他の 2 つのペインには、他のシステムからのビデオが表示されます。縮小表示されている場合、3 つのペインは 1 つの枠でまとめられ、名前ラベルとともに表示されます（1 画面または 3 画面のすべてのデバイス）。

クラウドのホスティング リソースに応じて、3 画面 ルームの 3 つの画面すべてがフィルム ストリップ状に表示されるエンドポイントと、1 つのペインしか表示されないエンドポイントがあります。メディアがオンプレミスの場合でも、Webex アプリ アプリには 1 つのペインだけが表示されます。

ミーティングの規模が大きく、1 つ目のノードからオーバーフローして 2 つ目のノードにカスケードする場合、別のノードにホストされるエンドポイントでも、3 画面システムをホストするエンドポイントと同じ画面が表示されます（レイアウトによって1つのペインのみを表示）。プレゼンテーションの共有には、コールパスを通じて BFCP のネゴシエーションが必要になります。

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。