Video Meshの管理とトラブルシューティング

Video Mesh 分析

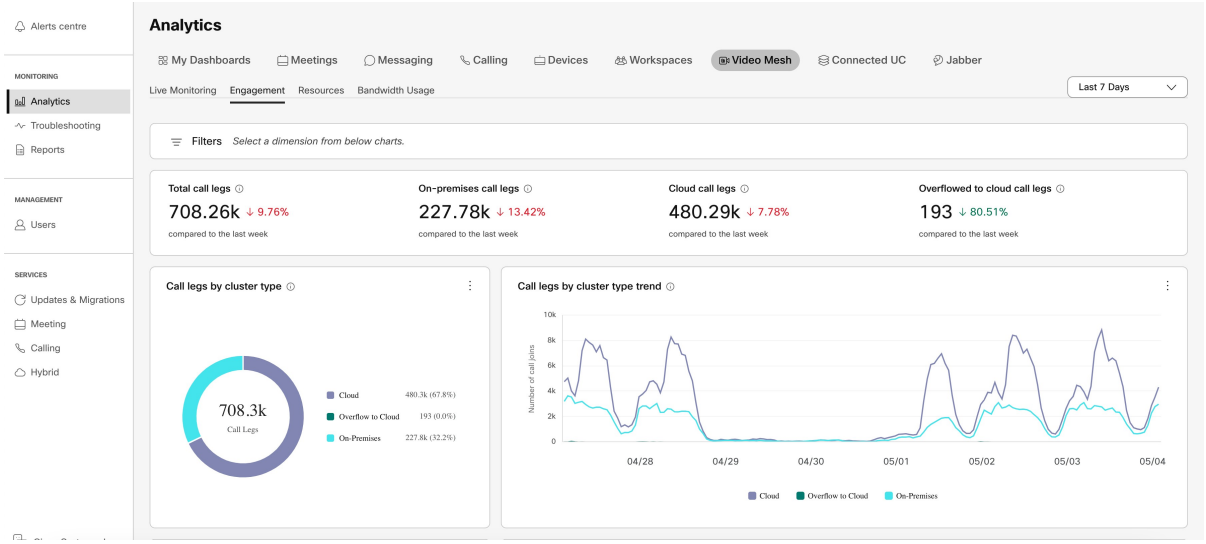
分析は、Webex 組織内でのオンプレミス Video Mesh ノードおよびクラスタの使用方法に関する情報を提供します。メトリックビューの履歴データを使用すると、オンプレミスリソースのキャパシティ、使用率、および可用性をモニタリングすることによって、Video Mesh リソースをより効果的に管理できます。この情報を使用して、クラスタへの Video Mesh ノードの追加や新しいクラスタの作成などの判断を行うことができます。Video Mesh 分析は、Control Hub の **[分析（Analytics）]** > **[Video Mesh]** で確認できます。

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。

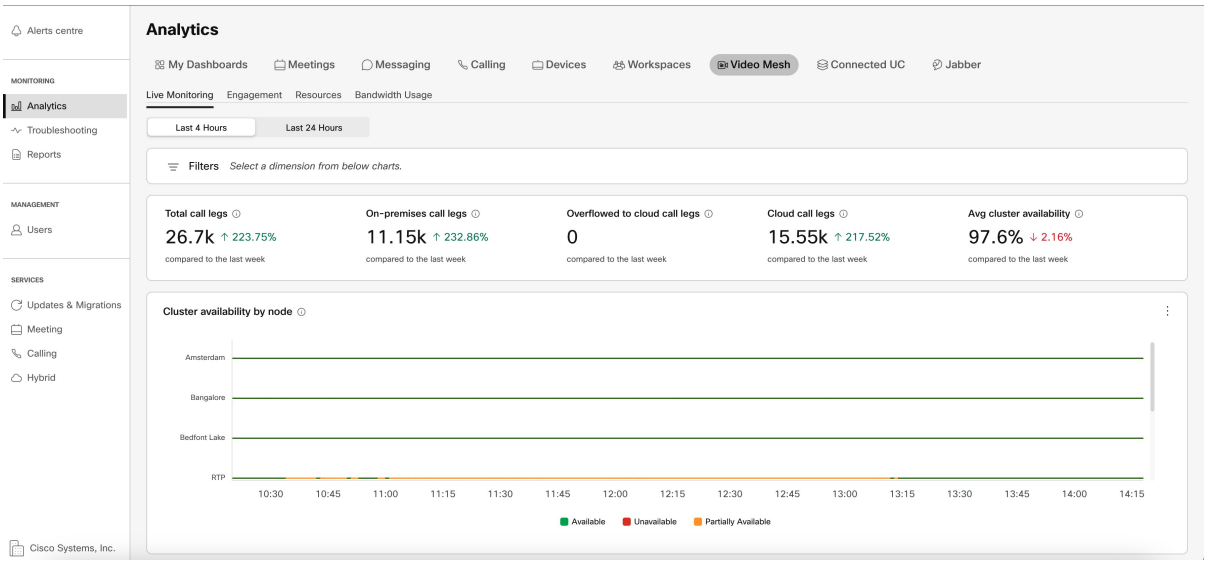
分析

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。

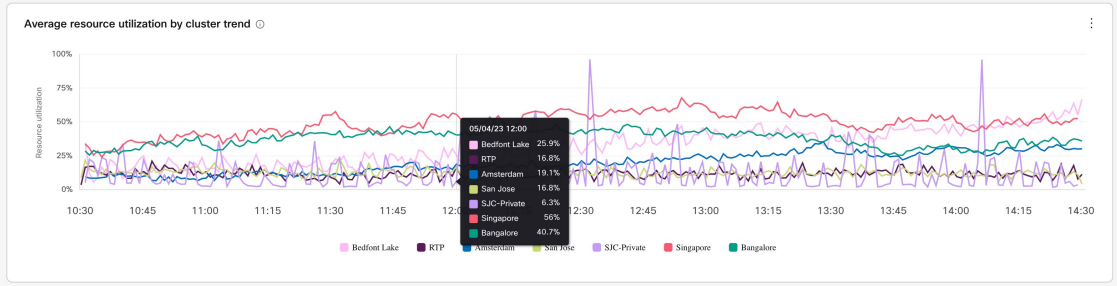
ヒント 情報 ⓘ をホバーすると、チャートの簡単な説明が表示されます。

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。

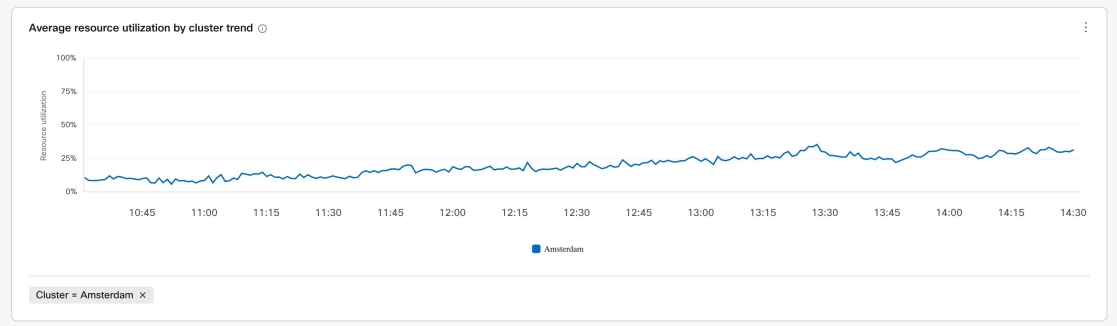
ステップ 3 必要に応じて、次のオプションを使用してチャートを操作します。

- 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。

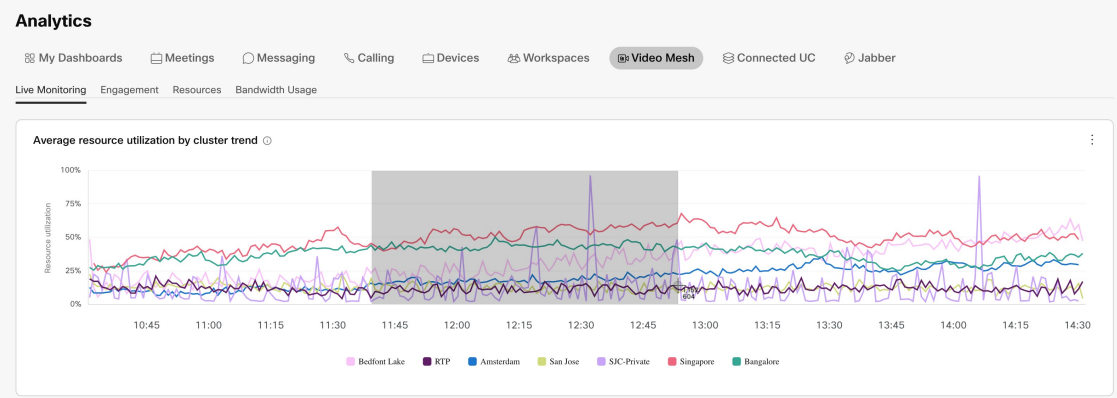


- グラフ上の凡例項目または概要をクリックし、**[適用（Apply）]** をクリックすると、その他の凡例項目のビューが更新されます。たとえば、アムステルダムの凡例項目を選択すると、折れ線グラフが更新され、その他の凡例項目を除外し、選択した項目のデータだけが含まれます。

（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**

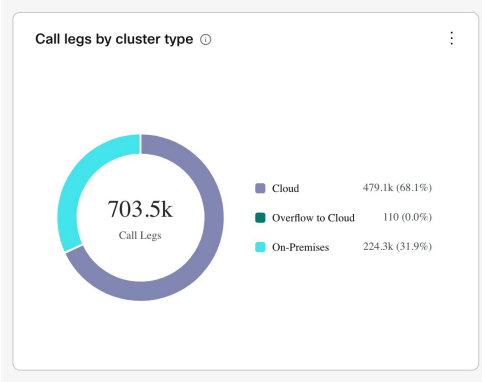
ヒント　情報 ⓘ をホバーすると、ドーナツグラフまたはチャートの簡単な説明が表示されます。

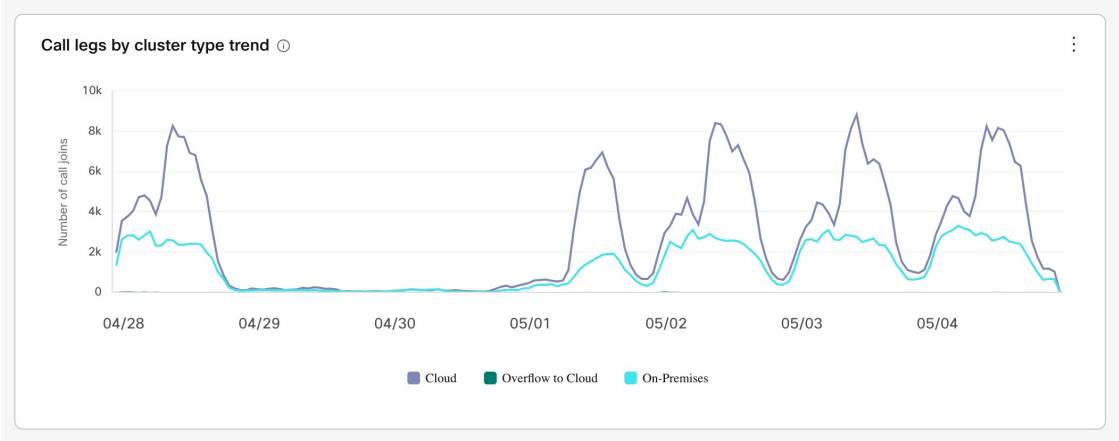
ステップ 3 右側のドロップダウンリストから、データを表示する過去の期間をフィルタ処理するオプションを選択します。

- **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。

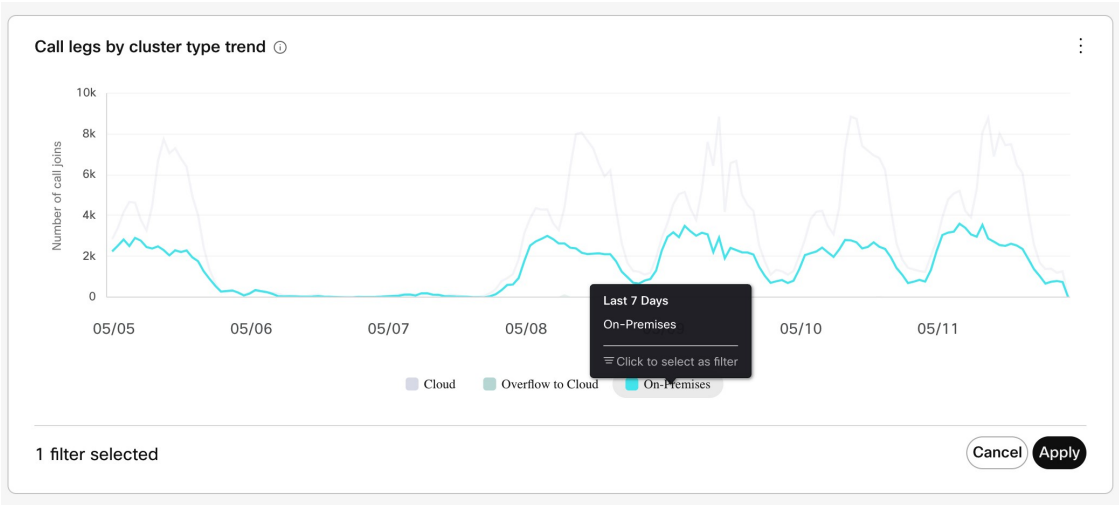
- ドーナツグラフまたはチャートビューで 1 つ以上のセグメントをクリックし、**[適用（Apply）]** をクリックして、そのドーナツビューと対応するチャートビューを更新します。

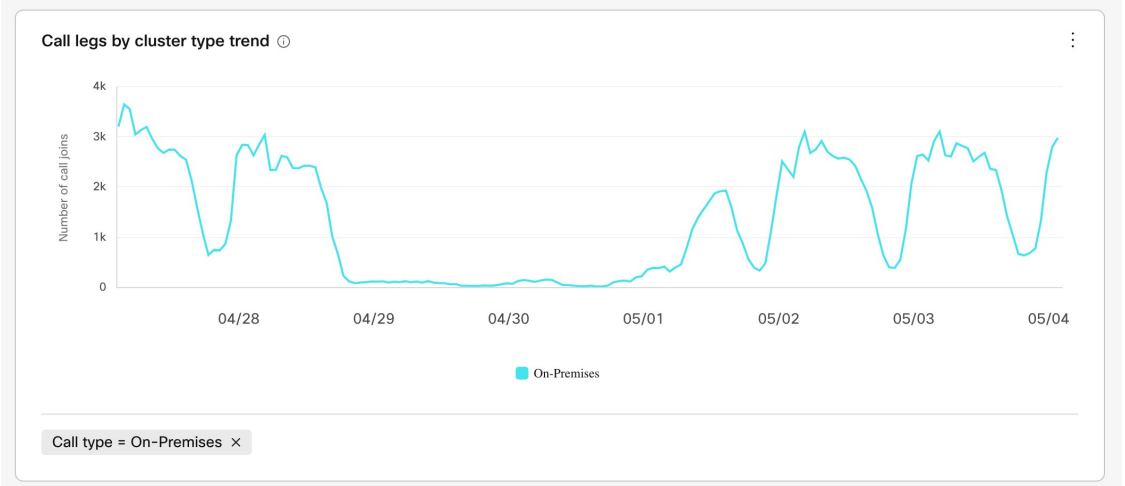




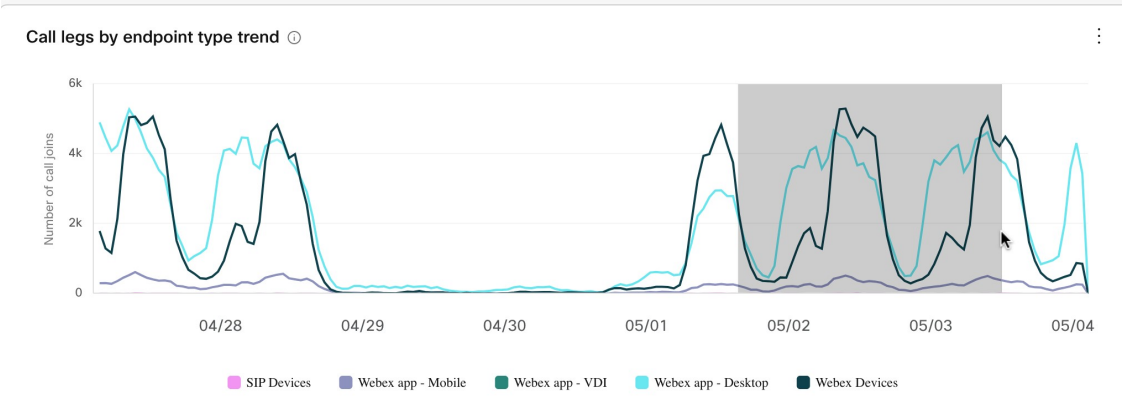
- グラフ上の凡例項目または概要を選択して、その特定の凡例項目のビューを更新し、**[適用（Apply）]**をクリックします。たとえば、[オンプレミス（On-Premises）]の凡例項目を選択すると、そのデータが強調表示された折れ線グラフが更新されます。

  （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。）

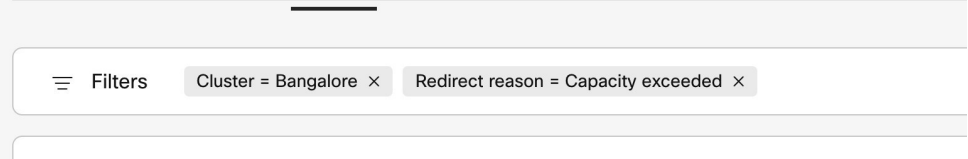


ヒント　ドーナツグラフ、グラフ上の折れ線、またはグラフ上のインサイトポイントのセクションをホバーすると、データの特定の時点に関する詳細が表示されます。

（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。

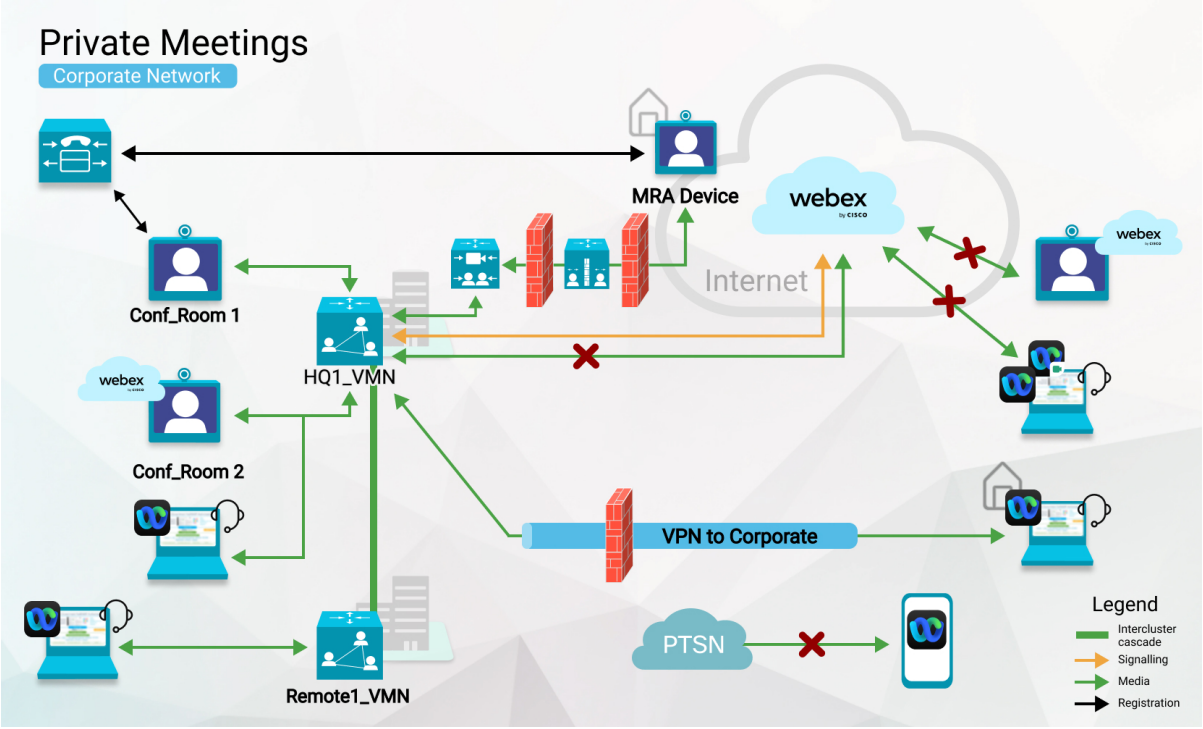
この設定がオフの場合、デフォルトは 720p です。

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」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」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。

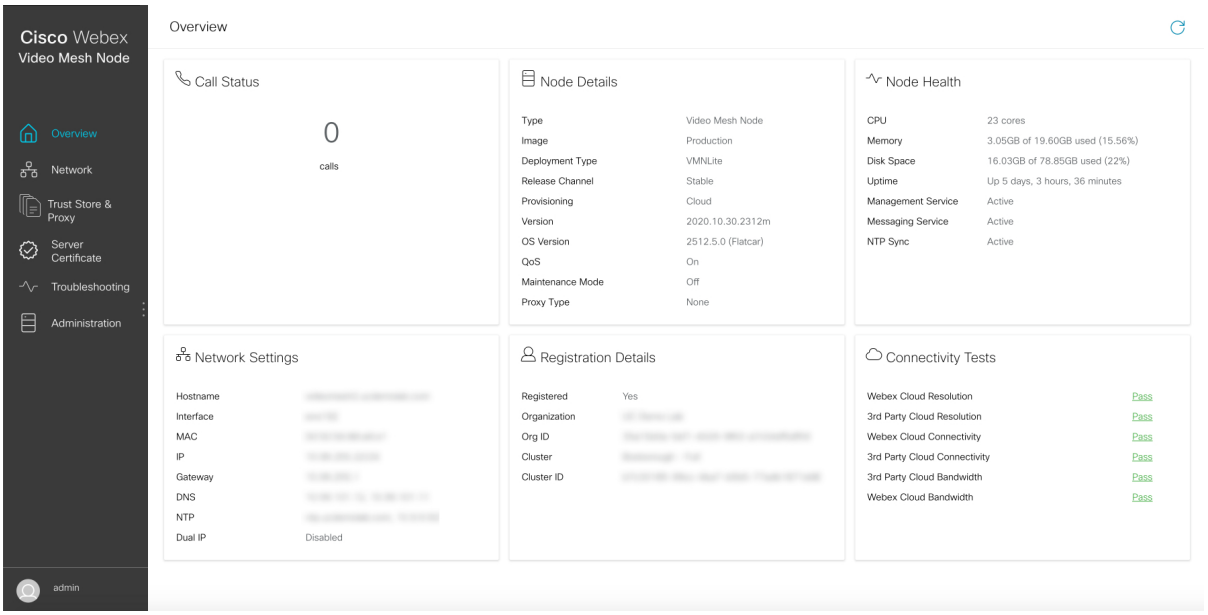
- **登録の詳細（Registration Details）**：登録ステータス、組織名、組織 ID、ノードが一部となっているクラスタ、およびクラスタ ID を提供します。
- **クラウド接続（Cloud Connectivity）**：ノードから、ノードが適切に実行するためにアクセスする必要がある Webex クラウドおよびサードパーティの接続先に対して、一連のテストを実行します。
  - DNS 解決、サーバー応答時間、および帯域幅の 3 種類のテストが実行されます。

（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 *1 : 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 （42 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 （40 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 （28 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 （38 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。

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。