CHAPTER 2

モニタリング用にネットワークを設定する方法

Prime Collaboration でネットワークの音声およびビデオ エンドポイントをモニタリングする前に、複数のタスクを完了する必要があります。

表 2-1 に、音声およびビデオ エンドポイントのモニタリングの前提条件についての情報を提供します。

表 2-1　音声およびビデオ エンドポイントのモニタリングの前提条件

モニタ対象	前提条件
音声およびビデオ エンドポイント	「デバイスの検出」（P.2-1）
ビデオ エンドポイント	「CTS-Manager および Cisco TMS からのセッションのインポート」（P.2-2）
音声エンドポイント	• 「CDR トランク使用率設定の設定」（P.2-3） • 「データ ソース クレデンシャルの管理」（P.2-3） • 「Cisco 1040 センサーの設定」（P.2-4） • 「コールの分類」（P.2-5） • 「SFTP の設定」（P.2-6） • 「SRST ポーリング設定のインポート」（P.2-7）

デバイスの設定の詳細については、『Setting up Devices for Prime Collaboration wiki』を参照してください。

デバイスの検出

Prime Collaboration のデータベースに新しいデバイスを追加するたびにデバイスを検出する必要があります。

デバイスを検出するには、次の手順を実行します。

1. [Manage Credentials] ページ（[Operate] > [Device Work Center] > [Manage Credentials]）を使用して、デバイスのクレデンシャルを入力します。

   Prime Collaboration を使用してモニタするすべてのデバイスのクレデンシャルを入力する必要があります。

2. [Inventory] ページ（[Operate] > [Device Work Center] > [Discover Devices]）を使用して、デバイスを検出します。

Cisco TelePresence Manager（CTS-Manager）、Cisco TelePresence Management Suite（TMS）、Cisco Unified CM、VCS などの管理デバイスや、コールおよびセッション制御デバイスをネットワークに導入してある場合は、これらのデバイスを最初に検出する必要があります。アプリケーション マネージャまたはコール プロセッサの検出を実行すると、登録されているすべてのコラボレーション デバイスが検出されます。

（注）　Cisco Unified CM に登録されているエンドポイントの場合は、JTAPI がイネーブルであることを確認します。Cisco Unified CM がすでに検出されている場合、エンドポイントを再度検出する必要があります。

デバイス ディスカバリの詳細については、『*Cisco Prime Collaboration 9.0 Device Management Guide*』の「Discovering Devices」の章を参照してください。

CTS-Manager および Cisco TMS からのセッションのインポート

CTS-Manager および Cisco TMS には、スケジュール済みセッションに関する詳細が含まれます。Prime Collaboration では、定期的にこれらのデバイスをポーリングして、セッションの詳細を取得します。定期的なポーリングの頻度は、ビジネスのニーズに合わせて設定できます。

セッションの継続的なモニタリングをイネーブルにするには、[Manage Clusters] オプション（[Operate] > [Device Work Center] > [Manage Clusters]）を使用して CTS-Manager または Cisco TMS クラスタを管理できます。

Cisco TMS の場合、スケジュール済みのセッションが進行中の場合にスケジュール設定されていないエンドポイントが追加されると、Prime Collaboration にはそのエンドポイントのセッションの詳細が示されます。

定期的なポーリングに加えて、セッションの詳細をすぐにインポートする場合は、[Import Sessions] リンク（[Operate] > [Diagnose] > [Session Diagnostics] > [Import Sessions]）をクリックできます。

（注）　[Import Sessions] タスクは、Prime Collaboration のシステム パフォーマンスに影響を与えます。[Import Sessions] リンクは、必要な場合に限り使用してください。

Prime Collaboration は 5 日分のスケジュール済みセッションのデータをインポートします（前日、当日および今後 3 日）。

セッションを Cisco TMS からインポートする場合は、次の点に注意してください。

- Cisco TMS の Booking Confirm 電子メールの場合、Prime Collaboration では、デフォルトの電子メール テンプレートのみをサポートします。デフォルト電子メール テンプレートを使用していない場合、セッションは、Cisco TMS からインポートされません。
- 「Reservation Only」会議の詳細は、Cisco TMS からインポートされません。このタイプの会議の場合はスケジュール中にリソースが割り当てられないため、Prime Collaboration では、このタイプの会議はサポートされません。

CTS-Manager で、スケジュール設定時刻前にセッションを開始するよう設定している場合、Prime Collaboration で同じ時刻を設定する必要があります。つまり、スケジュール設定時刻の 5 分前にセッションを開始するよう設定している場合、同じ時刻を [Device Monitoring Configuration] ページで設定する必要があります。そうしないと、Prime Collaboration に、スケジュール設定時刻前に開始したスケジュール済み会議の 2 つのセッションがリストされます。

[Import Session] タスクに対し、2 つのジョブが作成されます。これらのジョブは、[Administration] > [Job Management] ページでモニタします。[Job Management] ページでは、ジョブ タイプが Synch_CtsMAN-MEETING_UniqueJobID および Synch_TMS-MEETING_UniqueJobID として表示されます。

CTS-Manager 1.7 以上をご使用の場合、セッションのインポート タスクの間隔を最低 5 分以上確保する必要があります。5 分以内にセッションをインポートすると、ジョブは失敗します。

CDR トランク使用率設定の設定

すべてのクラスタのトランク使用率設定データをインポートするには、トランクおよびゲートウェイの最大容量を設定する必要があります。

トランクまたはゲートウェイの最大容量を設定するには、次の手順を実行します。

ステップ 1　[Administration] > [System Setup] > [Assurance Setup] > [CDR Trunk Utilization Settings] を選択します。

ステップ 2　ドロップダウン リストから、設定する Cisco Unified CM クラスタを選択します。

ステップ 3　ゲートウェイまたはトランクのタイプを選択します。

ステップ 4　[Configure Maximum Capacity] をクリックし、適切な入力を行います。

ステップ 5　[Apply] をクリックし、さらに [Close] をクリックします。

すべてのクラスタに関するトランク使用率データのインポート

トランク使用率の設定の実施後に、トランク使用率データをインポートする必要があります。

すべての Cisco Unified CM クラスタのトランク使用率データをインポートするには、次の手順を実行します。

ステップ 1　[Administration] > [System Setup] > [Assurance Setup] > [CDR Trunk Utilization Settings] を選択します。

ステップ 2　[Bulk Export] をクリックします。

ステップ 3　[Export Trunk Configuration] ウィンドウで、[Export] をクリックして、デフォルト名のエクスポート CSV ファイルを受け入れます。

ステップ 4　CSV ファイルを開き、必要に応じてデータを編集します。

すべてのゲートウェイおよびトランクがファイルにリストされます。ファイルだけに値を入力する必要があります。

ステップ 5　[Bulk Import] をクリックします。

ステップ 6　CSV ファイルの場所を参照して選択し、[Import] をクリックします。

データ ソース クレデンシャルの管理

Prime Collaboration では、Cisco Unified CM クラスタ、Cisco 1040 センサー、および NAM から Mean Opinion Score（MOS）データを収集できます。

これらのセッション アプリケーションからのデータ収集を可能にするために Cisco 1040 センサーにクレデンシャルを提供する必要はありません。ただし、NAM と Cisco Unified CM パブリッシャ サーバについては、次の作業を行う必要があります。

- Prime Collaboration にクレデンシャルを設定する。
- クレデンシャルを最新の状態に保つ。(NAM または Cisco Unified CM パブリッシャ サーバでクレデンシャルを更新する場合、Prime Collaboration で対応するクレデンシャルも更新する必要があります)。

クレデンシャルを更新するには、[Administration] > [System Setup] > [Assurance Setup] > [Call Quality Data Source Management] を選択します。

Cisco 1040 センサーの設定

Prime Collaboration では、Cisco 1040 センサーから受信したデータを使用して、ネットワークでの音声送信品質を判断します。

Cisco 1040 センサーを設定するには、次の手順を実行します。

1. Prime Collaboration および Cisco 1040 センサー用の TFTP サーバを 1 台または複数追加します。
2. ステップ 1 で追加した各 TFTP サーバのルート位置に、Prime Collaboration サーバからバイナリ イメージ ファイルをコピーします。
3. デフォルトのコンフィギュレーション ファイルを作成します。

設定した各 TFTP サーバに、Prime Collaboration によって Cisco 1040 センサーのコンフィギュレーション ファイルがコピーされます。Cisco 1040 センサーをネットワークに接続すると、コンフィギュレーション ファイルが TFTP サーバからダウンロードされ、その後で Prime Collaboration に登録されます。

TFTP サーバとして Cisco Unified CM を使用している場合は、Prime Collaboration サーバ上のイメージ ファイル ディレクトリから Cisco Unified CM サーバのルート位置に手動でデフォルト コンフィギュレーション ファイルをコピーする必要があります。

TFTP サーバの設定

Prime Collaboration に登録する Cisco 1040 センサーをイネーブルにするには、1 台以上の TFTP サーバを定義する必要があります（[Administration] > [System Setup] > [Cisco 1040] > [TFTP Servers]）。Prime Collaboration では、Cisco 1040 センサー コンフィギュレーション ファイルおよびバイナリ イメージ ファイルをこれらの TFTP サーバ提供します。

TFTP サーバを追加する場合は、次の点に注意してください。

- Prime Collaboration を TFTP サーバとして使用することはサポートされません。また、Prime Collaboration サーバ上の CiscoWorks Common Services（CWCS）TFTP サービスを無効にすることを推奨します。
- Cisco Unified CM バージョン 4.2 以降を TFTP サーバとして使用する場合は、次の点を考慮してください。
  - コンフィギュレーション ファイルとイメージ ファイルを手動で、Prime Collaboration から Cisco Unified CM サーバのルート位置にコピーする必要があります。
  - ファイルを更新して、TFTP サーバにコピーしたら、Prime Collaboration サーバの Cisco TFTP サービスを再起動する必要があります。

Cisco 1040 センサーを追加または編集すると、Prime Collaboration では、コンフィギュレーション ファイルをローカルに（サーバ上で）更新し、その後で既知のすべての TFTP サーバにコピーします。

バイナリ イメージ ファイルの TFTP サーバへのコピー

バイナリ イメージ ファイル SvcMonAB*n_nnn*.img を、Prime Collaboration サーバ上の ImageDir から TFTP サーバのルート位置にコピーする必要があります。

（注）　root としてログインする必要があります。

コールの分類

Prime Collaboration では、コール分類をコール詳細レコード（CDR）レポートにコールを分類するために使用します。

Prime Collaboration は、次のデータを分析して、システム定義のコール カテゴリに入るかコールかどうかを判別します。

- コール詳細レコード（CDR）
- ソース エンドポイントとターゲット エンドポイントのデバイス タイプ。
- コールの方向（着信または発信）
- プロトコル（H.323、MGCP、または SIP）

Prime Collaboration では、次の場合、ユーザ定義コール カテゴリにコールを分類します。

- コールがすでに [Internal]、[VG/Trunk-Outgoing]、[OnNet Trunk] のいずれかに分類されている。
- ユーザ定義ダイヤル プランがコールが発生したクラスタに割り当てられている。

ダイヤル パターンをダイヤル プランに追加するときに、コール カテゴリ名を作成することができます。コール カテゴリを追加するには、[Administration] > [Configuration] > [Call Classification] > [Call Category] を選択します。

ダイヤル プランを追加するには、[Administration] > [Configuration] > [Call Classification] > [Dial Plan Configuration] を選択します。ダイヤル プランの追加時に、デフォルト ダイヤル プランのコピーが表示され、更新できるようになります。

同じダイヤル プランをすべてのクラスタに割り当てることができます。また、Prime Collaboration に追加された各クラスタにそれぞれ異なるダイヤル プランを割り当てることもできます。

ゲートウェイ コードの設定

Prime Collaboration では、設定したゲートウェイ コードを使用して、外部コールのコール分類を決定します。

（注）　ゲートウェイ コードがすでに設定されているゲートウェイを表示するには、クラスタを選択して [View] をクリックします。

ゲートウェイ コードを設定するには、次の手順を実行します。

ステップ 1　[Administration] > [Configuration] > [Call Classification] > [Gateway Code] を選択します。
ステップ 2　[Gateway Code Summary] ページでクラスタを選択して、[Manage Gateway Code] をクリックします。
ステップ 3　ゲートウェイ コードを入力し、[Apply] をクリックします。

SFTP の設定

Cisco Unified CM を使用してコールをモニタしている場合は、SFTP 設定を実行する必要があります。SFTP を設定するには、次の手順を実行します。

ステップ 1　[Administration] > [System Setup] > [Assurance Setup] > [SFTP Settings] を選択します。
ステップ 2　必要な情報を入力します。フィールドの説明については、表 2-2 を参照してください。
ステップ 3　[Apply] をクリックします。

表 2-2 に、[SFTP Settings] ページのフィールドの説明を示します。

表 2-2　[SFTP Settings] ページ - フィールドの説明

フィールド	説明 / 処理
Low-Volume Schedule Hours	
<day> <timerange>	timerange は、各曜日について、Prime Collaboration で処理するレコードの少ない時間を示します。少量スケジュールの期間中、Prime Collaboration はデータベースのメンテナンスを実行します。
Miscellaneous	
Wait for Diagnostic Report (min)	データが大量である場合、Prime Collaboration による検索時にここで指定した分単位の時間が経過すると、その時点までに検出された一致レコードが診断レポート用に表示されます。
Report Data Retention Period (days)	データが Prime Collaboration データベースに保持される日数。この日数が経過すると、データは消去されます。
SFTP	
Username	ユーザ名は smuser から変更できません。 同じユーザ名（smuser）が Cisco Unified CM に設定されている必要があります。
[Change password] チェックボックス	パスワードを変更するには、このチェックボックスをオンにします。 **（注）**　デフォルトのパスワードは smuser です。ここでパスワードを変更した場合は、Cisco Unified CM の smuser のパスワードも変更する必要があります。

SRST ポーリング設定のインポート

Prime Collaboration で SRST モードの電話機を表示して、関連イベントを生成するには、SRST ポーリング設定をインポートする必要があります。

SRST 情報をインポートするには、次の手順を実行します。

ステップ 1　[Administration] > [System Setup] > [SRST] > [SRST Import] を選択します。

ステップ 2　[Filename] フィールドにシード ファイルの名前を入力し、[OK] をクリックします。

Prime Collaboration によって、ルータに到達できることが確認されてから、ルータ上に IP SLA ジッタ テストが作成されます。これには少し時間がかかることがあります。

ステップ 3　srst_test_creation_results.log ファイルを調べて、すべての IP SLA ジッター テストが正常に作成されたことを確認します。

IP SLA ジッタ テストが正常に作成されなかった場合は、次の手順に従います。

a.　ログ ファイルを使用して、問題を特定します。

b.　インポート ファイルを修正して、ステップ 1 に戻り、SRST 情報を再びインポートします。

SRST ポール設定のステータスを表示するには、[Administration] > [System Setup] > [SRST] > [SRST Operations] を選択します。