システム パラメータの設定

このセクションでは、次の点について説明します。

- システム パラメータの設定 （1 ページ）

システム パラメータの設定

Cisco Prime Collaboration Assurance のシステム設定パラメータは、次のとおりです。

- SMTP サーバ:このパラメータを次の下で設定します。 **[アシュアランス管理（Assurance Administration）] > [アラームとイベントの電子メール設定（E-mail Setup for Alarms & Events）]**SMTP サーバの設定を参照してください。

  Cisco Prime Collaboration リリース 11.5 以降の場合

  SMTPサーバ:このパラメータを次の下で設定します。**[アラームおよびレポート管理（Alarm & Report Administration）] > [アラームとイベントの電子メール設定（E-mail Setup for Alarms & Events）]**SMTP サーバの設定を参照してください。

- コール品質データソースの管理：Cisco Prime Collaboration Assurance は、VoIP ネットワークで音声品質の測定値を監視します。このリアルタイムによるサービス品質情報は、Unified CM、、またはPrime vNAMから収集されます。このパラメータを次の下で設定するには、次の手順に従います。 **[アシュアランス管理（Assurance Administration）] > [CDS ソース設定（CDR Source Settings）] > [通話品質データソース管理（Manage Call Quality Data Sources）]**[データ ソース クレデンシャルの更新（Update Data Source Credentials）]を参照してください。

  Cisco Prime Collaboration リリース 11.5 以降の場合

  コール品質データソースの管理：Cisco Prime Collaboration Assurance は、VoIP ネットワークで音声品質の測定値を監視します。このリアルタイムによるサービス品質情報は、Unified CM、、またはPrime vNAMから収集されます。このパラメータを次の下で設定するには、次の手順に従います。 **[アラームおよびレポート管理（Alarm & Report Administration）] > [CDS ソース設定（CDR Source Settings）] > [通話品質データソース管理（Manage Call Quality Data Sources）]**[データ ソース クレデンシャルの更新（Update Data Source Credentials）]を参照してください。

- [LDAP 設定（LDAP Settings）]：このパラメータを次の設定で設定します。**[システム管理（System Administration）]** > **[LDAP 設定（LDAP Settings）]**[LDAP サーバの設定（Configure an LDAP Server）]を参照してください。
- [ログの管理（Log Management）]：このパラメータを次の設定で設定します。**[システム管理（System Administration）]** > **[ログの管理（Log Management）]**[ログ レベル（Log Levels）]を参照してください。
- SFTP 設定：Unified CM からのコールを監視するには、SFTP を設定する必要があります。このパラメータを次の下で設定するには、次の手順に従います。**[アシュアランス管理（Assurance Administration）]** > **[CDS ソース設定（CDR Source Settings）]** > **[CUCM SFTPクレデンシャル（CUCM SFTP Credentials）]**[SFTP 設定の構成（Configure SFTP Settings）] を参照してください。

  Cisco Prime Collaboration リリース 11.5 以降の場合

  SFTP 設定：Unified CM からのコールを監視するには、SFTP を設定する必要があります。このパラメータを次の下で設定するには、次の手順に従います。**[アラームおよびレポート管理（Alarm & Report Administration）]**> **[CDR ソース設定（CDR Source Settings）]**> **[CUCM SFTP クレデンシャル（CUCM SFTP Credentials）]**[SFTP 設定の構成（Configure SFTP Settings）] を参照してください。

  Cisco Prime Collaboration リリース 12.1 SP3 以降の場合

  SFTP 設定：Unified CM からのコールを監視するには、SFTP を設定する必要があります。このパラメータを次の下で設定するには、次の手順に従います。**[インベントリ（Inventory）]** > **[インベントリ管理（Inventory Management）]**。**[CUCM SFTP クレデンシャル（CUCM SFTP Credentials）]** タブをクリックし、「SFTP 設定の構成」 を参照してください。
- クラスタ デバイスの検出設定：Cisco Prime Collaboration Assurance が、Unified CM から収集したインベントリとデバイス登録情報を統合できるようにします。このパラメータを次の下で設定するには、次の手順に従います。**[インベントリ（Inventory）]** > **[クラスタ デバイス検出スケジュール（Cluster Device Discovery Schedule）]**クラスタ デバイスの検出をスケジュールを参照してください。

グローバル システム パラメータ

これらのページで行った変更は、すべてのまたはドメイン（Enterprise モード）に適用されます。

表 *1:* システム パラメータ

タスク	ナビゲーション
シングル サインオンを設定します。	**[システム管理（System Administration）]** > **[シングル サインオン（Single Sign-On）]**

タスク	ナビゲーション
ライセンス ファイルを追加します。	**[システム管理（System Administration）] > [ライセンス管理（License Management）]**
SMTP サーバを設定します。	**[アラームおよびレポート管理（Alarm & Report Administration）] > [アラームとイベント用に電子メールをセットアップ（E-mail Setup for Alarms & Events）]**
デバイス検出のため SSL 証明書認証を設定します。	**[システム管理（System Administration）] > [証明書管理（Certificate Management）]**
ユーザの詳細にアクセスするため LDAP サーバを設定します。	**[システム管理（System Administration）] > [LDAP 設定（LDAP Settings）]**
ログレベルを変更します。デフォルト値は「[エラー（Error）]」 です。	**[システム管理（System Administration）] > [ログの管理（Log Management）]**
Unified CM からのコールを監視するため SFTP パラメータを設定します。	**[インベントリ（Inventory）] > [インベントリ管理（Inventory Management）] > [CUCM/sFTP クレデンシャル（CUCM/sFTP Credentials）]** **Cisco Prime Collaboration リリース 12.1 SP3 以降の場合** **[インベントリ（Inventory）] > [インベントリ管理（Inventory Management）]**。[CUCM SFTP クレデンシャル（CUCM SFTP Credentials）] タブをクリックします。
Unified CM でパラメータを設定して、インベントリとデバイスの登録情報を統合させます。	**[インベントリ（Inventory）] > [クラスタ デバイス検出スケジュール（Cluster Device Discovery Schedule）]**
ダイヤル プランを追加します。	**[アラームおよびレポート管理（Alarm & Report Administration）] > [CDR 分析の設定（CDR Analysis Settings）] > [ダイヤル プランの設定（Dial Plan Configuration）]**
コール カテゴリを作成します。	**[アラームとレポート管理（Alarm & Report Administration）] > [CDR 分析の設定（CDR Analysis Settings）] > [コール カテゴリの設定（Set Call Category）]**
パラメータを設定してデバイスをポーリングします。	**[アラームとレポート管理（Alarm & Report Administration）] > [ポーリング設定（Polling Settings）]**

タスク	ナビゲーション
Syslog ルールをカスタマイズして不具合を監視します。	**[アラームおよびレポート管理（Alarm & Report Administration）] > [イベントのカスタマイズ（Event Customization）] > [Syslog ルール（Syslog Rules）]**
アラーム通知（電子メール、syslog、トラップ）を設定します。	**[アラームおよびレポート管理（Alarm & Report Administration）] > [通知のセットアップ（Notification Setup）] > [カスタム通知（Custom Notification）]**
音声コールグレード設定（Good、Acceptable、Poor）を構成します。	**[アラームとレポート管理（Alarm & Report Administration）] > [CDR 分析の設定（CDR Analysis Settings）] > [音声コールグレードの設定（Configure Voice Call Grade）]**
音声電話レポート（IP フォンの監査、移動、疑いのある IP フォン）、ファイル形式、エクスポート ファイルの場所、電子メール通知など、音声電話レポートのエクスポートパラメータを設定します。	**[レポート（Reports）] > [UCM/CME Phone Activity Reports] > [音声電話のエクスポート（Export Audio Phones）]**
定期的なバックアップをスケジュール設定します。	**[システム管理（System Administration）] > [バックアップ設定（Backup Settings）]**

SMTP サーバの設定

SMTP サーバ名と送信者 AAA 電子メールアドレスを、**[アラームとイベントの電子メール設定（E-mail Setup for Alarms & Events）]** ページ（**[アラームとイベントの電子メール設定（E-mail Setup for Alarms & Events）]**）で指定することで、アラームの電子メール通知を送受信するように SMTP サーバを設定することができます。[Sender AAA E-mail Address] フィールドの値は、多数のサーバがある場合に、電子メールを受信したサーバを特定するのに便利です。

Cisco Prime Collaboration Assurance サーバのタイム ゾーンの設定

Cisco Prime Collaboration Assurance サーバのタイム ゾーンを設定するには、次の手順を実行します。

ステップ 1 インストールで作成したアカウントを使用して Cisco Prime Collaboration Assurance サーバにログインします。デフォルト設定は、*admin* です。

ステップ 2 次のコマンドを入力して、サポートされているタイム ゾーンのリストを表示します。

例：

```
cm/admin# show timezones
```

ステップ 3 Cisco Prime Collaboration Assurance サーバのタイム ゾーンを設定するには、次のコマンドを入力します。

例：

```
cm/admin(config)# config t cm/admin(config)# clock timezone US/Pacific cm/admin(config)# exit
```

ステップ 4 実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーするには、次のコマンドを入力します。

例：

```
cm/admin# write memory
```

ステップ 5 Cisco Prime Collaboration Assurance サーバを再起動するには、次のコマンドを入力します。

例：

```
cm/admin# application stop cpcm cm/admin# show application status cpcm cm/admin# application start
 cpcm
```

ステップ 6 再起動プロセスが終了するまで 10 分間待機してから次のコマンドを入力し、タイム ゾーンが新しい値に設定されているかどうかを確認します。

例：

```
cm/admin# show timezone US/Pacific
```

（注） データの不一致を回避するために、postgres データベースで設定したタイム ゾーンの値をシステムのタイムゾーンの値と同じにすることをお勧めします。システムのタイムゾーンを手動で変更する場合は、cpcm データベースと qovr データベースの両方を含めて、`/opt/postgres/9.2/data`（Analytics データベース）および `/opt/postgres/9.2/cpcmdata`（Assurance データベース）の `postgres.conf` ファイルで log_timezone パラメータおよび timezone パラメータをシステムのタイム ゾーンと一致するように変更して、システムを再起動します。postgres データベースでタイム ゾーンの値を変更する場合は、root アクセス機能が必要です。そのため、root アクセス権を取得するために TAC ケースを送信する必要があります。