CHAPTER 5

ネットワーク ヘルスのメンテナンス

ここでは、次の内容について説明します。

アラームとイベントの設定

[Alarm Clean Up and Display Options] の指定

[Administration] > [System Settings] > [Alarms and Events] ページでは、アラームを削除するときや、アラームの表示と電子メール オプションを設定する方法を指定できます。

ステップ 1 [Administration] > [System Settings] の順に選択します。

ステップ 2 左側のサイドバーのメニューから、[Alarms and Events] を選択します。[Administration] > [System Settings] > [Alarms and Events] ページが表示されます。

ステップ 3 [Alarm and Event Cleanup Options] を変更します。

- [Delete active and cleared alarms after]：アクティブなアラームまたはクリアされたアラームが削除されるまでの日数を入力します。チェックボックスをオフにすることで、このオプションを無効にできます。
- [Delete cleared security alarms after]：セキュリティ アラーム、不正 AP アラーム、およびアドホック不正アラームが削除されるまでの日数を入力します。
- [Delete cleared non-security alarms after]：セキュリティ アラーム以外のアラームが削除されるまでの日数を入力します。セキュリティ アラーム以外のアラームには、[Security]、[Rogue AP]、または [Adhoc Rogue] カテゴリに属するアラーム以外のすべてのアラームが含まれます。

- [Delete all events after]：すべてのイベントが削除されるまでの日数を入力します。この削除タスクが最初に行われるようにするには、他のすべての [Alarm and Event Cleanup Options] より小さい値に設定する必要があります。

（注） Prime Infrastructure は、通常のデータ クリーンアップ タスクの一部として毎夜古いアラームを削除し、1 時間に 1 回アラームのテーブル サイズを確認します。アラーム テーブルのサイズが 300K を超えると、Prime Infrastructure は 300K 以内に収まるまで、クリアされたアラームのうち一番古いアラームを削除します。クリアされたアラームを 7 日より多く保持する場合は、アラーム テーブルのサイズが 300K に達するまでに、[Delete cleared non-security alarms after] テキスト ボックスに 7 日より大きい値を指定します。

ステップ 4　[Syslog Cleanup Options] の下の [***Delete all syslogs after***] フィールドで、すべての syslog が削除される日数を入力します。

ステップ 5　[Alarm Display Options] を変更します。

- [Hide acknowledged alarms]：チェックボックスをオンにすると、承認済みのアラームは [Alarm Summary] ページに表示されません。このオプションは、デフォルトで有効です。シビリティの変化に関係なく、承認済みのアラームに対して、電子メールは生成されません。
- [Hide assigned alarms]：チェックボックスをオンにすると、割り当て済みのアラームは [Alarm Summary] ページに表示されません。
- [Hide assigned alarms]：チェックボックスをオンにすると、クリアされたアラームは [Alarm Summary] ページに表示されません。このオプションは、デフォルトで有効です。
- [Add controller name to alarm messages]：チェックボックスをオンにすると、アラーム メッセージにコントローラ名が追加されます。
- [Add Prime Infrastructure address to e-mail notifications]：チェックボックスをオンにすると、電子メール通知に Prime Infrastructure アドレスが追加されます。

（注） これらのオプションの変更は、[Alarm Summary] ページにだけ影響します。エンティティに対するアラームの簡易検索は、アラーム ステートに関係なく、そのエンティティのすべてのアラームを表示します。

ステップ 6　[Alarm Email Options] を変更します。

- [Include alarm severity in the email subject line]：チェックボックスをオンにすると、電子メールの件名にアラームのシビリティが含まれるようになります。このオプションは、デフォルトで有効です。
- [Include alarm Category in the email subject line]：このチェックボックスをオンにすると、電子メールの件名にアラームのカテゴリが含まれるようになります。このオプションは、デフォルトで有効です。
- [Include prior alarm severity in the e-mail subject line]：チェックボックスをオンにすると、電子メールの件名に重要度の高いアラームのシビリティが含まれるようになります。
- [Include custom text in the e-mail subject line]：チェックボックスをオンにすると、電子メールの件名にカスタム テキストが追加されます。[Replace the e-mail subject line with custom text] チェックボックスをオンにして、電子メールの件名をカスタム テキストに置き換えることもできます。
- [Include custom text in body of email]：チェックボックスをオンにすると、電子メールの本文にカスタム テキストが追加されます。
- [Include alarm condition in body of e-mail]：チェックボックスをオンにすると、電子メールの本文にアラーム状態が含まれるようになります。

- [Add link to Alarm detail page in body of e-mail] : チェックボックスをオンにすると、電子メールの本文に [Alarm detail] ページへのリンクが追加されます。
- [Enable Secure Message Mode] : チェックボックスをオンにすると、セキュア メッセージ モードが有効になります。[Mask IP Address and Mask Controller Name] チェックボックスをオンにした場合、アラーム電子メールはセキュア モードで送信され、すべての IP アドレスとコントローラ名はマスクされます。

ステップ 7　[Alarm Other Settings] を変更します。

- [Controller license count threshold] : 維持する使用可能なコントローラ ライセンスの最小数を入力します。アラーム数は、使用可能なアクセス ポイントがこのしきい値を下回る場合にトリガーされます。
- [Controller access point count threshold] : 維持する使用可能なコントローラ アクセス ポイントの最大数を入力します。アラーム数は、使用可能なアクセス ポイントがこのしきい値を超えた場合にトリガーされます。

ステップ 8　[Save] をクリックします。

アラームの重大度の変更

新しく生成されるアラームの重大度を変更できます。

（注）　既存のアラームは変更されません。

新しく生成されるアラームの重大度を設定するには、次の手順を実行します。

ステップ 1　[Administration] > [System Settings] の順に選択します。

ステップ 2　左側のサイドバーのメニューから、[Severity Configuration] を選択します。

ステップ 3　重大度を変更するアラーム状態のチェックボックスをオンにします。

ステップ 4　[Configure Severity Level] ドロップダウン リストから、新しい重大度（[Critical]、[Major]、[Minor]、[Warning]、[Informational]、または [Reset to Default]）を選択します。

ステップ 5　[Go] をクリックし、[OK] をクリックします。

監査の設定

監査設定のセットアップ

[Administration] > [SystemSettings] > [Audit] ページでは、監査の種類と監査を実行するパラメータを決定できます。

- 監査の種類の選択：基本監査およびテンプレート ベースの監査のいずれかを選択します。
- 監査するパラメータの選択：すべてのパラメータの監査を実行するか、選択したパラメータでグローバル監査を実行するかを選択します。

監査の種類の選択

[Audit Mode] グループ ボックスでは、基本監査およびテンプレート ベースの監査のいずれかを選択できます。デフォルトでは、基本監査が選択されています。

- [Basic Audit] : Prime Infrastructure データベースの設定オブジェクトを現在の WLC デバイスの値に対して監査します。Prime Infrastructure の 5.1.0.0 よりも前のバージョンでは、この監査モードのみが使用可能でした。

（注）　設定オブジェクトは、Prime Infrastructure データベースに保存されているデバイス構成を参照します。

- [Template-based Audit] : 適用されたテンプレート、設定グループのテンプレート（バックグラウンド監査に選択）、および設定の監査（該当するテンプレートが存在しない場合）を現在のコントローラ デバイスの値に対して監査します。

ステップ 1　[Administration] > [System Settings] の順に選択します。

ステップ 2　左側のサイドバーのメニューから、[Audit] を選択します。[Audit] ページが表示されます。

ステップ 3　[Basic Audit] または [Template Based Audit] を選択します。

- 基本監査では、Prime Infrastructure データベースのデバイス構成を現在のコントローラの設定に対して監査します。
- テンプレートベースの監査では、適用されたテンプレート、設定グループのテンプレート、および設定オブジェクト（該当するテンプレートが存在しない場合）を現在のコントローラの設定に対して監査します。

ステップ 4　すべてのパラメータの監査を実行するか、選択したパラメータの監査のみを実行するかを選択します。[Selected Parameters] オプション ボタンを選択した場合は、[Configure Audit Parameters] 設定ページにアクセスできます。（「監査通知の変更の有効化」（P.5-6）を参照してください）。

選択した監査パラメータは、ネットワーク監査およびコントローラ監査で使用されます。

ステップ 5　[Save] をクリックします。

これらの設定は、コントローラの監査またはネットワークの監査が実行される場合に有効です。

監査するパラメータの選択

[Audit On] グループ ボックスでは、すべてのパラメータを監査するか、監査する特定のパラメータを選択できます。[Selected Parameters] オプション ボタンを選択すると、[Select Audit Parameters] 設定ページにアクセスできます。選択した監査パラメータは、ネットワーク監査およびコントローラ監査で使用されます。

グローバルな監査の監査パラメータを設定するには、次の手順を実行します。

ステップ 1　[Administration] > [System Settings] の順に選択します。

ステップ 2　左側のサイドバーのメニューから、[Audit] を選択します。

ステップ 3　[Selected Parameters] オプション ボタンを選択して、[Select Audit Parameters] リンクを表示してから、[Save] をクリックします。

ステップ 4　[Select Audit Parameters] **をクリックして、**[Administration] > [System Settings] > [Audit] > [Select Audit Parameters] ページの監査に必要なパラメータを選択します。

ステップ 5　必要な情報を入力し、[Submit] をクリックします。選択した監査パラメータが、[Selected Attributes] タブに表示されます。

[Configure] > [Controllers] ページから現在の [Controller Audit Report] にアクセスするには、[Audit Status] カラムのオブジェクトを選択します。

コントローラを監査するには、[Configure] > [Controllers] ページの [Select a command] ドロップダウン リストから [Audit Now] を選択するか、[Controller Audit Report] から直接 [Audit Now] をクリックします。

監査レコードからの syslog の削除

古いレコードがサーバの容量を占有しないように、監査レコードを定期的に削除（消去）する必要があります。[Administration] > [System Settings] > [Audit Log Purge Settings] ページでは、syslog を消去し、ゴミ箱またはリモート ディレクトリに消去したログを送信できます。

syslog の消去設定を設定するには、次の手順を実行します。

ステップ 1　[Administration] > [System Settings] の順に選択します。

ステップ 2　左側のサイドバーのメニューから、[Audit Log Purge Settings] を選択します。

ステップ 3　[Keep logs younger than days] テキスト ボックスで、ログの消去設定を定義するための日数を入力します。指定した日数を経過したログは、消去されます。

ステップ 4　消去されたログをクリアするために次のオプションのいずれかを選択し、[Save] をクリックします。

- [Send To Trash]：消去されたログはごみ箱に送信されます。
- **[Remote Directory]**：消去されたログは、[Remote Directory] テキスト ボックスに指定されたパスに送信されます。

監査通知の変更の有効化

Prime Infrastructure は、定義した監査の一部である、インベントリまたは設定パラメータに変更を加えるたびに Java Message Service（JMS）に通知を送信できます。

デフォルトでは、監査変更の JMS 通知は無効になっています。この機能を Prime Infrastructure で有効にするには、[Enable Change Audit JMS Notification] チェックボックスをオンにする必要があります。Prime Infrastructure は、XML 形式のすべての監査通知の変更をトピック **ChangeAudit.All** に送信します。通知を受信するように、**ChangeAudit.All** に加入している必要があります。

ステップ 1　[Administration] > [System Settings] の順に選択します。

ステップ 2　左側のサイド バーのメニューから [Change Audit Notification] を選択します。[Change Audit Notification Settings] ページが表示されます。

ステップ 3　[Enable Change Audit JMS Notification] チェックボックスをオンにして通知を有効にしてから、[Save] をクリックします。

エラー ログのダウンロードおよび電子メールでの送信

Prime Infrastructure は、Prime Infrastructure で管理されるすべてのデバイスが生成するすべてのエラー、情報、およびトレース メッセージをログに記録します。Prime Infrastructure は、受信したすべての SNMP メッセージと Syslog もログに記録します。

Prime Infrastructure のトラブルシューティングに使用するために、ログをダウンロードして電子メールで送信するには、次の手順を実行します。

ステップ 1　[Administration] > [Logging] の順に選択します。[General Logging Options] 画面が表示されます。

ステップ 2　メッセージ レベルを選択します。

ステップ 3　さまざまな管理モジュールを有効にするには、[Enable Log Module] オプション内のチェックボックスをオンにします。すべてのモジュールを選択するには、[Log Modules] をクリックします。

ステップ 4　[Log File Settings] セクションに、必要な設定を入力します。これらの設定は、Prime Infrastructure の再起動後に有効になります。

デフォルトでは、[File Prefix] フィールドは **ncs-%g-%u.log** です。ここで、*%g* は、ログ ファイルの一意の連番で、*%u* は、ローカル ディスク ファイル システムによって割り当てられた一意の番号です。たとえば、最初に作成されたログ ファイルは ncs-1-0.log です。

ステップ 5　ローカル マシンにログ ファイルをダウンロードするには、[Download] をクリックします。

（注）　logs.zip のファイル名には、プレフィックスとしてホスト名と日時が付いているため、保管されたログ ファイルを簡単に識別できます。ログ ファイルについて記述した HTML ファイルが ZIP ファイルに含まれます。

ステップ 6　ログ ファイルを送信するには、電子メール ID を（複数の場合はカンマで区切って）入力し、[Send] をクリックします。

（注）　ログ ファイルを電子メールで送信するには、電子メール サーバを設定しておく必要があります。

SNMP トレーシングの有効化

SNMP によって送受信されたパケットに関する詳細情報にアクセスするために、SNMP トレーシングを有効にできます。指定する SNMP トレーシングの設定は、Prime Infrastructure SNMP サーバに保存され、使用されます。SNMP トレーシングを有効にする手順は、次のとおりです。

（注）　WCS Release 7.x から Prime Infrastructure Release 2.0 にアップグレードする場合、[Administration] > [Logging Options] > [SNMP Logging Options] の下位の設定は保持されません。

ステップ 1　[Administration] > [Logging] の順に選択します。[Logging Options] ページが表示されます。

ステップ 2　左側のサイドバーのメニューから、[SNMP Logging Options] を選択します。

ステップ 3　コントローラと Prime Infrastructure 間での SNMP メッセージ（トラップも含む）の送信を有効にするために、[Enable SNMP Trace] チェックボックスをオンにして、[Display Values] チェックボックスをオンにし、SNMP メッセージ値を参照します。

ステップ 4　SNMP トラップをトレースする 1 つ以上の IP アドレスを設定します。このテキスト ボックスには、最大 10 個の IP アドレスを追加できます。

ステップ 5　最大 SNMP ファイル サイズおよび SNMP ファイルの数を設定できます。

Syslog ロギング オプションの変更

ステップ 1　[Administration] > [Logging] を選択し、[Syslog Logging Options] をクリックします。

ステップ 2　[Enable Syslog] チェックボックスをオンにして、システム ログの収集および処理を有効にします。

ステップ 3　メッセージの送信元にするインターフェイスの Syslog ホスト IP アドレスを入力します。

ステップ 4　[Syslog Facility] を選択します。syslog メッセージの送信用に、8 個のローカル用途のファシリティから任意に選択できます。このローカル用途のファシリティは予約されておらず、一般的な用途で使用可能です。

ステップ 5　[Save] をクリックします。

ロギング オプションの変更によるトラブルシューティングの強化

問題をデバッグするのに Prime Infrastructure が収集するデータの量を変更できます。問題を簡単に再現できるよう、TAC への連絡に先立って次の手順を実行してください。

収集するトラブルシューティング データの量を収集する変更するには、次の手順を実行します。

ステップ 1　[Lifecycle view] の場合：[Administration] > [Logging] の順に選択します。

ステップ 2　[Message Level] ドロップダウン リストから [Trace] を選択します。

ステップ 3　各チェックボックスをクリックして、すべてのログ モジュールを有効にします。

ステップ 4　現在の問題を再現させます。

ステップ 5　[Logging Options] ページに戻り、[Download Log File] セクションから [Download] をクリックします。

logs.zip のファイル名には、プレフィックスとしてホスト名と日時が付いているため、保管されたログ ファイルを簡単に識別できます。ログ ファイルについて記述した HTML ファイルが ZIP ファイルに含まれます。

ステップ 6　ログを取得したら、[Message Level] ドロップダウン リストから [Information] を選択します。

注意　[Message Level] を [*Trace*] のままにすると、長期間のうちにパフォーマンスに悪影響を与えるおそれがあります。

Mobility Service Engine ロギング オプションの変更

Prime Infrastructure を使用して、ログに記録する Mobility Services Engine のロギング レベルとメッセージ タイプを指定できます。

ステップ 1　[Classic View] の場合：[Design] > [Mobility Services] > [Mobility Services Engine] を選択してから、設定するモビリティ サービス エンジンの名前を選択します。

ステップ 2　[System] > [Log] を選択して、[Logging Level] ドロップダウン リストから適切なオプションを選択します。

ロギング オプションは、[Off]、[Error]、[Information]、および [Trace] の 4 つです。ログ レベルを [Error] またはこれよりも前のレベルに設定した場合、ログ レコードはすべて、新しいエラー ログ ファイル locserver-error-%u-%g.log に記録されます。これは、ロケーション サーバの locserver-%u-%g.log ログ ファイルとともに維持される追加のログ ファイルです。このエラー ログ ファイルには、[Error] レベルのログとそのコンテキスト情報が記録されます。コンテキスト情報には、当該エラーよりも前の 25 ログ レコードが含まれています。最大 10 のエラー ログ ファイルを維持できます。各ログ ファイルの最大許容サイズは 10 MB です。

注意　[Error] と [Trace] は、Cisco TAC の指示がある場合にだけ使用してください。

ステップ 3　イベントのロギングを開始する各要素の横の [Enable] チェックボックスをオンにします。

ステップ 4　[Advanced Parameters] ダイアログボックスの [Enable] チェックボックスをオンにし、詳細デバッグを有効にします。デフォルトでは、このオプションは無効になっています。

ステップ 5　サーバからログ ファイルをダウンロードするには、[Download Logs] をクリックします。詳細については、「Mobility Services Engine ログ ファイルのダウンロード」（P.5-9）を参照してください。

ステップ 6　[Log File Parameters] グループ ボックスに、以下の情報を入力します。

- Mobility Services Engine で維持するログ ファイルの数。Mobility Services Engine で維持できるログ ファイルの数は 5 ～ 20 です。
- 最大ログ ファイル サイズ（MB 単位）。ログ ファイルのサイズは 10 ～ 50 MB です。

ステップ 7　[MAC Address Based Logging Parameters] グループ ボックスで、次の手順に従います。

- [Enable] チェックボックスをオンにし、MAC アドレス ロギングを有効にします。デフォルトでは、このオプションは無効になっています。
- ロギングを有効にする 1 つ以上の MAC アドレスを追加します。また、以前に追加した MAC アドレスを削除できます。削除するには、リストから MAC アドレスを選択して [Remove] をクリックします。MAC アドレスに基づくロギングの詳細については、「MAC アドレスに基づくロギング」（P.5-9）を参照してください。

ステップ 8　[Save] をクリックして変更を適用します。

MAC アドレスに基づくロギング

この機能では、指定されている MAC アドレスのエンティティ固有のログ ファイルを作成できます。ログ ファイルは次に示すパスの locserver ディレクトリ内に作成されます。

```
/opt/mse/logs/locserver
```

一度に最大で 5 つの MAC アドレスをログに記録できます。MAC アドレス aa:bb:cc:dd:ee:ff のログ ファイルの形式は次のとおりです。

```
macaddress-debug-aa-bb-cc-dd-ee-ff.log
```

1 つの MAC アドレスに対して最大 2 つのログ ファイルを作成できます。2 つのログ ファイルのうち、1 つがメインのログファイルであり、もう 1 つがバックアップまたはロールオーバー ログ ファイルです。

MAC ログ ファイルの最小サイズは 10 MB です。最大許容サイズは、MAC アドレスあたり 20 MB です。MAC ログ ファイルの未更新時間が 24 を超えると、この MAC ログ ファイルはプルーニングされます。

Mobility Services Engine ログ ファイルのダウンロード

Mobility Services Engine ログ ファイルを解析する必要がある場合は、Prime Infrastructure を使用してログ ファイルをご使用のシステムにダウンロードします。Prime Infrastructure はログ ファイルが含まれている zip ファイルをダウンロードします。

ログ ファイルが含まれている zip ファイルをダウンロードするには、次の手順を実行します。

ステップ 1　[Classic view] の場合：[Design] > [Mobility Services] > [Mobility Services Engine] を選択します。

ステップ 2　ステータスを表示する Mobility Services Engine の名前を選択します。

ステップ 3　左側のサイドバーのメニューから、[System] > [Logs] の順に選択します。

ステップ 4　[Download Logs] ダイアログボックスで、[Download Logs] をクリックします。

ステップ 5　[File Download] ダイアログボックスの指示に従い、ファイルを開くかまたは zip ファイルをシステムに保存します。

テクニカル サポート リクエストの設定

シスコ テクニカルサポートでサポート ケースを作成するために、設定をカスタマイズできます。サポート ケースの作成については、『*Cisco Prime Infrastructure 2.0 User Guide*』の「Opening a Support Case」を参照してください。

ステップ 1　[Administration] > [System Settings] > [Support Request Settings] を選択します。

ステップ 2　Cisco Support Enabling が Prime Infrastructure サーバから直接対話する対話のタイプを選択します。

- [Enable interactions directly from the server]：Prime Infrastructure サーバから直接サポート ケースを作成するには、このオプションを指定します。サポート プロバイダーへの電子メールは、Prime Infrastructure サーバまたは指定した電子メール アドレスに関連付けられている電子メールから送信されます。
- [Interactions via client system only]：クライアント マシンにサポート ケースに必要な情報をダウンロードするには、このオプションを指定します。次にダウンロードされたサポート ケース詳細および情報をサポート プロバイダーに電子メールで送信する必要があります。

ステップ 3　テクニカル サポート プロバイダーを選択します。

- [Cisco] をクリックして Cisco Technical Support でサポート ケースを開いて、Cisco.com クレデンシャルを入力します。[Test Connectivity] をクリックして、次のサーバへの接続性を確認します。
  - Prime Infrastructure メール サーバ
  - Cisco サポート サーバ
  - フォーラム サーバ
- [Third-party Support Provider] をクリックして、サード パーティのサポート プロバイダーでサービス要求を作成します。プロバイダーの電子メール アドレス、件名、および Web サイト URL を入力する必要があります。