



## 第 21 章 システム メンテナンス

MARS アプライアンスのシステム メンテナンス情報の多くは、『*Install and Setup Guide for Cisco Security Monitoring, Analysis, and Response System*』にのみ記載されています。

MARS アプライアンスはメンテナンスがほとんど不要です。メンテナンス タスクを実行するには、必要に応じて CLI (コマンドライン インターフェイス) または HTML インターフェイスを使用できます。ハードウェア メンテナンス タスクには、MARS アプライアンスへの物理アクセスが必要な場合があります。

この章の具体的な内容は次のとおりです。

- ・ 実行時ロギング レベルの設定
- ・ アプライアンスのログ ファイルの表示
- ・ 監査証跡の表示
- ・ 未処理メッセージの取得
- ・ ハードドライブ
- ・ リチウム セル CMOS バッテリの交換
- ・ 管理者アカウントのデフォルト パスワードの変更

MARS アプライアンスのデータのアップグレード、バックアップ、および復元方法については、『*Install and Setup Guide for Cisco Security Monitoring, Analysis, and Response System*』の次の項を参照してください。

- ・ [Performing Command Line Administration Tasks \(p.6-1\)](#)
- ・ [Checklist for Upgrading the Appliance Software \(p.6-7\)](#)
- ・ [Configuring and Performing Appliance Data Backups \(p.6-18\)](#)
- ・ [Recovery Management \(p.6-26\)](#)

### 実行時ロギング レベルの設定

アプライアンスの実行時ロギング レベルを設定するには、**Admin > System Maintenance > Set Runtime Logging Levels** の順にナビゲートします。通常は、このページ設定をデフォルトのままにしておくことを推奨します。

ロギング レベルを選択したら、**Change Logging Levels** ボタンをクリックします。

使用できるログ レベルは、次のとおりです。

- ・ **Fatal**: 重大ロギング メッセージをイネーブルにします。重大メッセージには、アプリケーションの中断をもたらす可能性のある非常に重大なエラー イベントが記録されています。
- ・ **Error**: エラーおよび重大ロギング メッセージをイネーブルにします。エラー メッセージには、アプリケーションが動作を継続できるエラー イベントが記録されています。
- ・ **Warn**: 警告、エラー、および重大ロギング メッセージをイネーブルにします。警告メッセージには、潜在的に危険な状況が記録されます。
- ・ **Info**: 情報、警告、エラー、および重大ロギング メッセージをイネーブルにします。情報メッセージは主に、アプリケーションの大きな進捗状況を示します。

- ・ **Debug**: デバッグ、情報、警告、エラー、および重大ロギングメッセージをイネーブルにします。デバッグメッセージには、アプリケーションのデバッグに最も役立つ詳細な情報イベントが記録されています。
- ・ **Trace**: トレース、デバッグ、情報、警告、エラー、および重大ロギングメッセージをイネーブルにします。トレースメッセージには、デバッグメッセージよりも詳細な情報イベントが記録されています。

## アプライアンスのログ ファイルの表示

アプライアンスのログ ファイルを表示したり、レベルやソースを変更したりするには、**Admin > System Maintenance > View Log Files** の順にナビゲートします。

図 21-1 バックエンド ログの表示オプション

View Backend Log

Last:  Days  Hrs  Mins
 Select Level: 
Select Source:

Start:     Hrs  Mins
 143387

End:     Hrs  Mins

アプライアンスのバックエンド ログを表示するには、日数、時間、分を選択するか、開始日と開始時刻および終了日と終了時刻を選択します。

必要なログ レベルを選択できます。選択できるタイプは、All、Fatal、Error、Warn、Info、および Debug です。

表示するファイルのソースを選択できます。選択肢は Backend または GUI です。

## バックエンド ログの表示

**ステップ 1** 該当するオプション ボタンをクリックします。

- ・ **Last**: 現在時刻から、入力した日数、時間、分だけさかのぼった時刻
- ・ **Start/End**: 日付から分までの単位で定義された、絶対的なリテラル時間範囲

**ステップ 2** ユーザ、グループなどを選択します。

**ステップ 3** ソースを選択します。

**ステップ 4** **Submit** をクリックします。

## 監査証跡の表示

アプライアンスのユーザ アクティビティを追跡するには、アプライアンスのログ ファイルを分析します。アプライアンスの監査証跡ログを設定するには、**Admin > System Maintenance > View Audit Trail** の順にナビゲートします。通常は、このページ設定をデフォルトのままにしておくことを推奨します。

ユーザ監査証跡を表示するには、日数、時間、分を選択します。特定のインターバルを表示するには、開始日と開始時刻および終了日と終了時刻を選択します。

## 監査証跡の表示手順

**ステップ 1** 該当するオプション ボタンをクリックします。

- ・ Last: DD-HH-MM
- ・ Start/End: YY-MM-DD-HH-MM

**ステップ 2** リストからユーザまたはユーザ グループを選択します。

**ステップ 3** Submit をクリックします。

## 未処理メッセージの取得

この機能を使用すると、アーカイブ サーバ([Configuring and Performing Appliance Data Backups](#) [p.6-18] を参照)または Local Controller で稼働中のデータベースから未処理メッセージを取得できます。これらの 2 つの方法にはさまざまな利点があります。

- ・ **アーカイブ サーバ** - アーカイブ サーバから未処理メッセージまたはイベント データを取得する方法は、データベースから取得する方法よりもはるかに高速です。したがって、この方法を使用でき、かつ調査期間がカバーされている場合は、この方法を推奨します。ただし、このオプションを使用できるのは、データ アーカイブがイネーブルで、初期アーカイブ動作が発生するまで必要な時間を待機した場合のみです。動作は、午前 2:00 ごろに実行するようにスケジュールされています。初期アーカイブが実行されると、イベント データが 1 時間ごとにアーカイブ サーバに書き込まれます。このデータはリアルタイムでアーカイブされないため、このオプションには、調査できるのが過去の期間であるという別の制限事項があります。1 時間前のデータよりも新しいデータを表示する必要がある場合は、Database オプションを選択して、正しいデータが取得されるようにする必要があります。その他のすべての期間には、アーカイブ サーバ オプションを推奨します。アーカイブをイネーブルにするには、[Configuring and Performing Appliance Data Backups](#) (p.6-18) を参照してください。
- ・ **データベース** - データベースからイベント データを取得する方法は、アーカイブ サーバ方式よりも低速です。ただし、受信した最新データにアクセスできます。このオプションを選択した場合は、受信したレコードを書き込む場所 (デフォルトのローカル ディレクトリ、またはリモート サーバが使用できる場合はリモート サーバ) を指定できます。

ここで説明する内容は、次のとおりです。

- ・ アーカイブ サーバからの未処理メッセージの取得
- ・ Local Controller のデータベースからの未処理メッセージの取得

## アーカイブ サーバからの未処理メッセージの取得

アーカイブがイネーブルな場合は、この方法を使用します。

アーカイブ サーバからイベント データを取得する手順は、次のとおりです。

**ステップ 1** Admin > System Maintenance > Retrieve Raw Messages の順にクリックします。

Retrieve Raw Messages:

Specify Time Range:

Start: 2005 October 7 7 Hrs 12 Mins 15 Secs  
 End: 2005 October 7 7 Hrs 22 Mins 15 Secs

Retrieve Data From Archived Files

Retrieve Data From DB

Save To Local  Save To Remote

Force Generate Files    Maximum No. of Files: 10

Select Reporting Device:

All Devices

143783

**ステップ 2** Start および End フィールドに値を指定して、時間範囲を指定します。

**ステップ 3** Retrieve Data From Archived Files が選択されていることを確認します。

Admin > System Maintenance > Data Archiving で識別されたサーバからデータが取得されます。

**ステップ 4** Submit をクリックします。



**注** MARS がファイルを生成している間、システムでほかのタスクを実行することができます。

**結果:** Retrieving Progress 0% 画面が表示されます。この処理が完了したら、Raw Message Files 画面が表示され、指定した時間範囲に基づくファイル名を持つ新しい Gzip アーカイブ ファイルが識別されます。

Get More Files

Raw Message Files

Download

2005-10-07-06-14-28\_2005-10-08-06-24-28.gz Click Here to Download

143797

**ステップ 5** 生成された未処理メッセージ ファイルをダウンロードして表示するには、ファイル名の横にある Click Here to Download をクリックします。

ファイル名の構文は、次のとおりです。YYYY-MM-DD-HH-MM-SS\_YYYY-MM-DD-HH-MM-SS.gz

**ステップ 6** Gzip アーカイブ ファイルの内容を抽出するには、WinZip または別のアーカイブ展開プログラムを使用します。

**ステップ 7** GNU Zip アーカイブ フォーマットから抽出されるテキストファイルの内容は、次のようになります。

```
33750&»Wed Jul 27 16:16:06 PDT 2005&»BR-FW-1&»10.4.1.1 Mon Jan 6 11:05:34 2003 <134>Jan 06
2003 11:03:53: %PIX-6-302001:Built inbound TCP connection 21000 for faddr 10.1.2.4/9000
gaddr 10.1.5.20/80 laddr 10.1.5.20/80
```

各値は次のとおりです。device ID>>date>>device name>>raw message



**注** 生成されたテキスト ファイルに漢字またはその他の見慣れない文字列が表示された場合は、Microsoft Internet Explorer を使用してファイルを表示し、Western European ISO または Western European Windows のエンコードが選択されていることを確認してください( [表示] > [エンコード] の順に選択)。互換性のあるエンコードが選択されている場合は、「&»」記号がセパレータとして正しく表示されます。

## Local Controller のデータベースからの未処理メッセージの取得

アーカイブがイネーブルでない場合、または過去 1 時間以内に受信したイベント データを表示する必要がある場合は、この方法を使用します。

データベースからイベント データを取得する手順は、次のとおりです。

**ステップ 1** Admin > System Maintenance > Retrieve Raw Messages の順にクリックします。

## Retrieve Raw Messages:

Specify Time Range:

Start: 2005 October 7 7 Hrs 12 Mins 15 Secs  
 End: 2005 October 7 7 Hrs 22 Mins 15 Secs

Retrieve Data From Archived Files

Retrieve Data From DB

Save To Local  Save To Remote

Force Generate Files Maximum No. of Files: 10

Select Reporting Device:

All Devices

143784

**ステップ 2** Start および End フィールドに値を指定して、時間範囲を指定します。

**ステップ 3** Retrieve from Database を選択します。

**ステップ 4** 次のいずれかのオプションを選択します。

- ・ **Save to Local** - データベースからデータを取得し、ローカル アプライアンスに格納します。
- ・ **Save to Remote** - データベースからデータを取得し、Admin > System Maintenance > Data Archiving で識別されたアーカイブサーバに格納します。

**ステップ 5** Cached Files 時間範囲情報を確認してから、次のいずれかを実行します。

- ・ この時間範囲のデータが必要な場合、Force Generate Files は不要です。
- ・ Cached Files 時間範囲外のデータが必要な場合は、**Force Generate Files** チェックボックスをオンにします。
- ・ キャッシュされているファイル情報がない場合は、**Force Generate Files** チェックボックスをオンにします。

キャッシュされているファイル データが表示されない場合は、それ以前のクエリーが実行および保存されていません。たとえば、時間範囲 A を使用し、データベースから 3 つの異なるクエリーを実行して、ローカル MARS アプライアンスにファイルを保存するとします。あとで同じ時間範囲 A を指定し、データを検索したとしても、Force Generate Files チェックボックスをオフにしなかった場合は、システムによってクエリーが実行され、ファイルが再生成されます。ただし、以前にデータの一部を取得して保存したことがある場合は、Force Generate Files チェックボックスをオフにして、保存されたファイルからデータを取得するように指定できます。

**ステップ 6** Maximum No. of Files フィールドに、保持する取得済みファイルの最大数を入力します。

この値は、このクエリーで生成されるイベントファイルの最大数を表します。



**注** 多数のファイルを要求する処理には、時間がかかることがあります。

**ステップ 7** Reporting Devices リストで、イベント データをプルするデバイスのリストを選択します。

名前を使用して特定のデバイスを選択するか、または All Devices を選択します。

**ステップ 8** Submit をクリックします。



**注** MARS がファイルを生成している間、システムでほかのタスクを実行することができます。

**結果:** Retrieving Progress 0% 画面が表示されます。この処理が完了したら、Raw Message Files 画面が表示され、指定した時間範囲に基づくファイル名を持つ新しい Gzip アrchive ファイルが識別されます。

Get More Files

Raw Message Files

Download

2005-10-07-06-14-28\_2005-10-08-06-24-28.gz Click Here to Download

143797

**ステップ 9** 生成された未処理メッセージ ファイルをダウンロードして表示するには、ファイル名の横にある Click Here to Download をクリックします。

ファイル名の構文は、次のとおりです。YYYY-MM-DD-HH-MM-SS\_YYYY-MM-DD-HH-MM-SS.gz

**ステップ 10** Gzip アーカイブ ファイルの内容を抽出するには、WinZip または別のアーカイブ展開プログラムを使用します。

**ステップ 11** GNU Zip アーカイブ フォーマットから抽出されるテキストファイルの内容は、次のようになります。

```
33750&#x2192;Wed Jul 27 16:16:06 PDT 2005&#x2192;BR-FW-1&#x2192;10.4.1.1 Mon Jan 6 11:05:34 2003 <134>Jan 06
2003 11:03:53: %PIX-6-302001:Built inbound TCP connection 21000 for faddr 10.1.2.4/9000
gaddr 10.1.5.20/80 laddr 10.1.5.20/80
```

各値は次のとおりです。device ID>>date>>device name>>raw message



**注** 生成されたテキスト ファイルに漢字またはその他の見慣れない文字列が表示された場合は、Microsoft Internet Explorer を使用してファイルを表示し、Western European ISO または Western European Windows のエンコードが選択されていることを確認してください( [表示] > [エンコード] の順に選択)。互換性のあるエンコードが選択されている場合は、「&#x2192;」記号がセパレータとして正しく表示されます。

## ハードドライブ

### ステータス ライト

アプライアンスのモデルに応じて、各ハードドライブには、ドライブの下または横に 2 つのステータス ライトが装備されています。ステータス ライトによって、次の状態を判別できます。

- ・ グリーンに点灯している場合は、ドライブが正常に機能しています。
- ・ オレンジに点滅している場合は、ドライブが I/O 処理を実行しています。
- ・ 消灯している場合は、ディスクに電力が供給されていません。

### パーティション チェック

システムのリブート回数が 25 ~ 30 回に達した場合、またはアプライアンスが 180 日間リブートされていない場合は、ハードドライブの各パーティションが自動的にチェックされます。

### ハードドライブのホットスワップ

MARS 50、100、100e、200、GC、または GCm アプライアンス モデルで、ハードドライブに障害が発生した場合、MARS 管理者には電子メール通知が送信されます。この通知には、障害が発生したハードドライブのドライブ 番号が記載されています。

### ハードドライブの取り外し

**ステップ 1** CLI ツールを介してログインします。

**ステップ 2** hotswap コマンドを入力します。

**ステップ 3** ハードドライブを取り外します。

**ステップ 4** ハードドライブを交換します。

---

## ハードドライブの交換

---

**ステップ 1** シャーシ扉のキーで扉を開きます。

**ステップ 2** ドライブ ベイ キーを使用して、交換するドライブ ベイのロックを解除します。

**ステップ 3** ドライブを引き抜きます。

**ステップ 4** ドライバーを使用して、ハードドライブからドライブ ベイ ホルダーを取り外します。

**ステップ 5** ドライブ ベイ ホルダーに新しいハードドライブを差し込んで、ネジで固定します。

**ステップ 6** ドライブを元の位置にゆっくりと差し込みます。

**ステップ 7** ドライブ ベイをロックします。

**ステップ 8** ベイの扉を閉じて、ロックしなおします。



---

**注** 交換できるハードドライブは一度に 1 つずつです。新しいハードドライブの初期化が完了していることを確認してから、別のハードドライブと交換してください。

---

## リチウム セル CMOS バッテリーの交換



---

**注意** リチウム セル CMOS バッテリーを正しくないタイプのバッテリーで交換すると、爆発する可能性があります。リチウム セル CMOS バッテリーは絶対に交換しないでください。このバッテリーを交換する必要がある場合は、シスコの代理店にご相談ください。

---

## リチウム セル CMOS バッテリーの交換手順



---

**注** アプライアンスに物理的に触れる前に、ESD (静電気放電) 対策を十分に施してください。

---

CMOS バッテリーを交換する必要がある場合は、次の手順に従ってください。

---

**ステップ 1** アプライアンスの電源を切ります。

**ステップ 2** アプライアンスの電源コードを壁面コンセントから取り外します。

**ステップ 3** リチウム セル CMOS バッテリーの位置を確認します。

**ステップ 4** バッテリーを取り外します。

**ステップ 5** 新しいバッテリーを装着します。

**ステップ 6** アプライアンスの電源コードを壁面コンセントに取り付けます。

**ステップ 7** アプライアンスに電源を投入します。



---

**注** リチウム バッテリーは環境に有害な場合があります。バッテリーの安全な処分方法については、お近くのゴミ処理サービス会社にお問い合わせください。

---

## 管理者アカウントのデフォルト パスワードの変更

セキュリティを高めるには、デフォルト パスワードを変更する必要があります。MARS アプライアンスには強力なパスワードを使用することを推奨します。

ログイン名およびパスワードに関する注意事項:

- ・ 英数字を指定できる。
- ・ 大文字と小文字が区別される。
- ・ 特殊文字を使用できる(!, @, # など)。
- ・ 一重または二重引用符(` および ")は使用**できない**。

ログイン名の最大文字数は 20、パスワードの最大文字数は 64 である。

デフォルト パスワードを変更したり、管理者通知を設定する手順は、次のとおりです。

---

**ステップ 1** **Management > User Management** タブをクリックします。

**ステップ 2** Administrator の横にあるチェックボックスをオンにして、**Edit** をクリックします。

**ステップ 3** 新しい管理者パスワードおよび管理者の電子メール アドレスを入力します。

**ステップ 4** **Submit** をクリックします。

---