CHAPTER 6

Cisco Emergency Responder 8.6 Serviceability の設定

Cisco Emergency Responder（Emergency Responder）8.6 には、Emergency Responder 8.6 Serviceability 機能にアクセスできる Serviceability インターフェイスが含まれています。これらの機能は、[Tools]、[SNMP]、[System Monitor]、[Emergency Responder Logs] という、Serviceability Web インターフェイス上の 4 つのメイン メニューの下にグループ化されています。すべての Serviceability Web ページの詳細については、付録 B「Cisco Emergency Responder のサービスアビリティ Web インターフェイス」を参照してください。

次のトピックでは、Emergency Responder 8.6 Serviceability 機能を設定および使用する方法について説明します。

- 「Serviceability ツールの使用」（P.6-1）
- 「SNMP の設定」（P.6-3）
- 「System Monitor ツールの使用」（P.6-7）
- 「Cisco Emergency Responder ログの使用」（P.6-9）

Serviceability ツールの使用

次のトピックでは、Emergency Responder 8.6 Serviceability ツールについて説明します。

- 「Control Center の使用」（P.6-1）
- 「Event Viewer の使用」（P.6-2）

Control Center の使用

Control Center を使用すると、選択された Emergency Responder 8.6 システム上で実行されているサービスに対するアクションを実行できます。

選択された Emergency Responder 8.6 システム上で実行されているサービスに対するアクションを実行するには、次の手順を実行します。

手順

ステップ 1 Emergency Responder Serviceability Web インターフェイスから、[Tools]>[Control Center] の順に選択します。

[Control Center] ページが表示されます。

ステップ 2　サービスのステータスを変更するには、[Service Name] の左側にあるオプション ボタンをクリックし、必要なアクションに対応するボタンをクリックします。選択可能なアクションは次のとおりです。

- Start
- Stop
- Restart

（注）　Cisco Tomcat および Cisco IDS サービスは、Emergency Responder Serviceability Web サイトから開始、停止、または再開することはできません。これらのサービスは、CLI を使用してのみ開始、停止、または再開できます。詳細については、付録 F「コマンド ライン インターフェイス」を参照してください。

ステップ 3　ページを更新するには、[Refresh] をクリックします。

関連項目

- 「Control Center」（P.B-1）

Event Viewer の使用

Event Viewer を使用すると、過去 6 か月間のイベントを表示できます。

過去 6 か月間のイベントを表示するには、次の手順を実行します。

手順

ステップ 1　Emergency Responder Serviceability Web インターフェイスから、[Tools]>[Event Viewer] の順に選択します。

[Event Viewer] ページが表示されます。

ステップ 2　過去 6 か月間に発生したすべてのイベントを検索するには、検索条件を入力せずに [Find] をクリックします。

特定の条件に一致するイベントを検索するには、検索条件を入力します。

- 特定の月を選択すると、その月のイベントだけが表示されます。
- [Type] を選択した場合は、検索に使用するタイプを右側のプルダウン メニューから選択できます。

  [Module] を選択した場合は、検索に使用するモジュールを右側のプルダウン メニューから選択できます。

（注）　使用可能なタイプとモジュールのリストについては、「Event Viewer」（P.B-2）を参照してください。

検索条件を入力したら、[Find] をクリックします。

ステップ 3　結果を昇順または降順でソートできます。ソートを実行するには、[Time]、[Type]、または [Module] 列見出しの横にある上矢印または下矢印をクリックします。

関連項目

- 「Event Viewer」（P.B-2）

SNMP の設定

Emergency Responder 8.6 は、SNMP V1/V2C および V3 をサポートしています。Serviceability Web インターフェイスを使用すると、SNMP V1/V2C（コミュニティ ストリングと通知先）および SNMP V3（ユーザと通知先）を設定できます。

各 SNMP バージョンには、セキュリティ モデルとセキュリティ レベルがあります。ユーザは、セキュリティ モデルと指定されたセキュリティ レベルで定義されたグループに割り当てられます。各グループには、MIB オブジェクトのセットに対する読み取りおよび書き込みについて定義されたセキュリティ アクセス レベルもあります。これらはビューと呼ばれます。スイッチには、デフォルト ビュー（すべての MIB オブジェクト）と、SNMP V1 および V2C セキュリティ モデル用に定義されたデフォルト グループがあります。SNMP V3 は、メッセージの整合性、認証、および暗号化をカバーする追加のセキュリティ機能を提供します。さらに、SNMP V3 では、MIB ツリーの特定の領域へのユーザ アクセスも制御されます。

次のトピックでは、SNMP V1/V2C および V3 の設定方法について説明します。

- 「SNMP コミュニティ ストリングの設定」（P.6-3）
- 「SNMP V1/V2C 通知ストリングの設定」（P.6-4）
- 「SNMP ユーザの設定」（P.6-5）
- 「SNMP V3 通知先の設定」（P.6-5）
- 「MIB2 の設定」（P.6-6）

SNMP コミュニティ ストリングの設定

SNMP を設定することによって、Emergency Responder SNMP エージェントへの SNMP アクセスを制御できます。管理ステーションは、まず認証のための有効なコミュニティ ストリングを送信する必要があります。

コミュニティ ストリングを設定するには、コミュニティ ストリング名、そのコミュニティ ストリングを使用して認証できるホストの IP アドレス、および許可されるアクセス権限を入力します。使用可能なアクセス権限は次のとおりです。

- ReadOnly
- ReadWrite
- ReadWriteNotify
- NotifyOnly
- None

SNMP コミュニティ ストリングを設定するには、次の手順を実行します。

手順

ステップ 1　Emergency Responder Serviceability Web インターフェイスから、[SNMP]>[V1/V2C Configuration]>[Community String] の順に選択します。

[SNMP Community String Configuration] ページが表示されます。

ステップ 2　[Community String Name] テキスト ボックスに、コミュニティ ストリングの名前を入力します。

ステップ 3　SNMP パケットを受け入れる特定のホストを指定するには、[Accept SNMP Packets only from these hosts] オプション ボタンをクリックし、テキスト ボックスに IP アドレスを入力して [Insert] をクリックします。

任意のホストから SNMP パケットを受け入れるには、[Accept SNMP Packets from any host] オプション ボタンをクリックします。

ステップ 4　既存のホストを削除するには、ホストの IP アドレスを選択し、[Remove] をクリックします。

ステップ 5　[Access Privileges] プルダウン メニューから、ホストのアクセス権限を選択し、[Insert] をクリックします。

関連項目

- 「SNMP Community String Configuration」（P.B-4）

SNMP V1/V2C 通知ストリングの設定

SNMP V1/V2C 通知ストリングを使用すると、SNMP V1/V2C トラップ メッセージの送信先のホストとポートを選択できます。すべての通知ストリングを認証する必要があります。SNMP V1/V2C を使用する場合、認証はコミュニティ ストリングを使用して実行されます。

SNMP V1/V2C 通知ストリングを設定するには、次の手順を実行します。

手順

ステップ 1　Emergency Responder Serviceability Web インターフェイスから、[SNMP]>[V1/V2C Configuration]>[Notification Destination] の順に選択します。

[SNMP Notification Destination Configuration] ページが表示されます。

ステップ 2　新しい SNMP 通知先を追加するには、[Add New] をクリックします。

ステップ 3　[Host IP Addresses] プルダウン メニューから、[Add New] を選択します。追加のフィールドが表示されます。

ステップ 4　テキスト ボックスに、ホストの IP アドレスとポート番号を入力します。

ステップ 5　[V1] または [V2C] オプション ボタンのどちらかをクリックして、SNMP バージョンを選択します。

[V1] をクリックすると、[Community String] プルダウン メニューが表示されます。ステップ 7 に進みます。

[V2C] をクリックすると、[Notification Type] プルダウン メニューが表示されます。

ステップ 6　[Notification Type] プルダウン メニューから、[Inform] または [Trap] を選択します。[Community String] プルダウン メニューが表示されます。

ステップ 7　[Community String] プルダウン メニューから、使用するコミュニティ ストリングを選択します。

ステップ 8　[Insert] をクリックします。

変更を有効にするには SNMP マスター エージェントを再起動する必要があることを知らせるメッセージが表示されます。[OK] をクリックして SNMP マスター エージェントを再起動するか、または [Cancel] をクリックしてマスター エージェントを再起動せずに続行します。

[SNMP Notification Destination Configuration] ページにある宛先のリストに通知先が追加されます。

ステップ 9　通知先を追加するには、ステップ 2 ～ステップ 8 を繰り返します。

関連項目

- 「SNMP V1/V2c Notification Destination Configuration」（P.B-6）

SNMP ユーザの設定

SNMP V3 は、メッセージの整合性、認証、および暗号化をカバーする追加のセキュリティ機能を提供します。さらに、SNMP V3 では、MIB ツリーの特定の領域へのユーザ アクセスも制御されます。

SNMP ユーザを設定するには、次の手順を実行します。

手順

ステップ 1　Emergency Responder Serviceability Web インターフェイスから、[SNMP]>[V3 Configuration]>[User] の順に選択します。

[SNMP User Configuration] ページが表示されます。

ステップ 2　新しい SNMP ユーザを追加するには、[Add New] をクリックします。

ステップ 3　[User Name] テキスト ボックスに、新しいユーザの名前を入力します。

ステップ 4　認証を要求するには、[Authentication Required] チェックボックスをオンにして、[Password] テキスト ボックスにパスワードを入力し、[Reenter Password] テキスト ボックスにパスワードを再入力してから、[MD5] または [SHA] オプション ボタンのどちらかをクリックして使用するプロトコルを選択します。[Insert] をクリックして、ユーザを追加します。

ステップ 5　情報のプライバシーを要求するには、[Privacy Required] チェックボックスをオンにして、[Password] テキスト ボックスにパスワードを入力し、[Reenter Password] テキスト ボックスにパスワードを再入力してから、[DES] チェックボックスをクリックします。

（注）　変更を有効にするには SNMP マスター エージェントを再起動する必要があることを知らせるメッセージが表示されます。[OK] をクリックして SNMP マスター エージェントを再起動するか、または [Cancel] をクリックしてマスター エージェントを再起動せずに続行します。

[SNMP User Configuration] ページのユーザのリストに新しいユーザが追加されます。

ステップ 6　ユーザを追加するには、ステップ 2 ～ステップ 4 を繰り返します。

関連項目

- 「SNMP User Configuration」（P.B-7）

SNMP V3 通知先の設定

SNMP V3 の通知先ストリングでは、各通知ストリングがユーザと関連付けられるため強力なセキュリティを提供します。ユーザを設定する場合は、必要なレベルの認証とセキュリティを指定できます。

SNMP V3 通知ストリングを設定するには、次の手順を実行します。

手順

ステップ 1　Emergency Responder Serviceability Web インターフェイスから、[SNMP]>[V3 Configuration]>[Notification Destination] の順に選択します。

[SNMP Notification Destination Configuration] ページが表示されます。

ステップ 2　新しい SNMP 通知先を追加するには、[Add New] をクリックします。

ステップ 3　[Host IP Addresses] プルダウン メニューから、[Add New] を選択します。追加のフィールドが表示されます。

ステップ 4　テキスト ボックスに、ホストの IP アドレスとポート番号を入力します。

ステップ 5　[Notification Type] プルダウン メニューから、[Inform] または [Trap] を選択します。

[Trap] を選択すると、[Security Level] プルダウン メニューが表示されます。ステップ 7 に進みます。

[Inform] を選択すると、リモート エンジン ID の入力を求めるプロンプトが表示されます。

ステップ 6　リモート エンジン ID を入力します。

ステップ 7　[Security Level] プルダウン メニューから、必要なセキュリティ レベルを選択します。

ステップ 8　[User Name] の左側にあるオプション ボタンをクリックして、通知先に関連付けるユーザを選択します。

ステップ 9　通知先を追加するには、ステップ 2 ～ステップ 8 を繰り返します。

関連項目

- 「SNMP V3 Notification Destination Configuration」（P.B-9）

MIB2 の設定

SNMP MIB2 ツールでは、MIB2 管理ノードの連絡先担当者、および管理ノードの物理ロケーションを指定できます。

MIB2 を設定するには、次の手順を実行します。

手順

ステップ 1　Emergency Responder Serviceability Web インターフェイスから、[SNMP]>[System Group Configuration]>[MIB2 System Group Configuration] の順に選択します。

[SNMP MIB2 Configuration] ページが表示されます。

ステップ 2　[System Contact] テキストボックスに連絡先の名前を入力します。

ステップ 3　[Location] テキスト ボックスに、管理ノードのロケーションを入力します。

ステップ 4　ページの左上隅にある [Update] アイコンをクリックします。

ステップ 5　情報を変更するには、ページの左上隅にある [Clear] アイコンをクリックし、[System Contact] および [Location] テキスト ボックスに新しい情報を入力して、[Update] アイコンを再びクリックします。

関連項目

- 「MIB2 SystemGroup Configuration」（P.B-11）

System Monitor ツールの使用

次のトピックでは、System Monitor ツールの使用方法について説明します。

- 「CPU and Memory Usage ツールの使用」（P.6-7）
- 「Processes ツールの使用」（P.6-8）
- 「Disk Usage ツールの使用」（P.6-9）

CPU and Memory Usage ツールの使用

CPU and Memory Usage ツールを使用して、この情報を監視し、記録できます。デフォルトでは、情報は 30 秒ごとに更新されます。この情報の更新頻度は変更できます。または、自動更新機能を無効にすることもできます。

CPU and Memory Usage ツールを使用するには、次の手順を実行します。

手順

ステップ 1　Emergency Responder Serviceability Web インターフェイスから、[System Monitor]>[CPU & Memory Usage] の順に選択します。

[CPU and Memory Usage] ページが表示されます。

このページは、[Processors] と [Memory] の 2 つのセクションに分かれています。表示される情報の詳細については、表 B-12（P.B-12）を参照してください。

ステップ 2　ページの更新間隔を変更するには、[Set the screen refresh value] テキストボックスに値（秒）を入力し、[Set] をクリックします。入力できる最小値は 5 秒です。

ステップ 3　自動更新機能を無効にするには、左上隅にある [Disable Auto-Refresh] チェックボックスをオンにします。

ステップ 4　CPU の使用状況のログ ファイルを作成するには、ページの [Processors] セクションの [Start Log] ボタンをクリックします。

同様に、メモリ使用状況のログ ファイルを作成するには、ページの [Memory] セクションにある [Start Log] ボタンをクリックします。

最大 25 のログ ファイルを作成できます。

デフォルトのロギング間隔は 10 秒です。ロギング間隔を変更するには、次の手順を実行します。

a.　CPU のロギング間隔を変更するには、[Set CPU Logging Interval] テキストボックスに 5 ～ 600 秒の値を入力し、[Set] をクリックします。

b.　メモリのロギング間隔を変更するには、[Set Memory Logging Interval] テキストボックスに 5 ～ 600 秒の値を入力し、[Set] をクリックします。

ステップ 5　ログ ファイルをダウンロードするには、[Download CPU Log File] または [Download Memory Log File] をクリックします。

現在のすべてのログ ファイルを示す [Log Files] ページが表示されます。その後、ログ ファイルはリサイクルされます。新しいログ ファイルが追加されると、最も古いログ ファイルが削除されます。

ステップ 6　個々のファイルをダウンロードするには、ダウンロードするログ ファイル名の左側にあるチェックボックスをオンにします。すべてのログ ファイルをダウンロードするには、[File Name] 列見出しの左側にあるチェックボックスをオンにします。ファイルを選択したら、[Download] をクリックします。

ダウンロード用に複数のファイルを選択すると、CPULogs（プロセッサのログ ファイルの場合）および MemoryLogs（メモリのログ ファイルの場合）という名前の圧縮ファイルが作成され、ダウンロードされます。

ステップ 7　ログ ファイルをダウンロードせずに、オンラインで表示することもできます。その場合は、ファイル名をクリックします。ログ ファイルの内容が表示されます。

関連項目

- 「CPU and Memory Usage」（P.B-12）

Processes ツールの使用

Processes ツールを使用して、プロセス情報を監視し、記録できます。デフォルトでは、情報は 30 秒ごとに更新されます。更新の最小値は 5 秒です。この情報の更新頻度は変更できます。または、自動更新機能を無効にすることもできます。

Processes ツールを使用するには、次の手順を使用します。

手順

ステップ 1　Emergency Responder Serviceability Web インターフェイスから、[System Monitor]>[Processes] の順に選択します。

[Processes] ページが表示されます。表示される情報の詳細については、表 B-13（P.B-13）を参照してください。

結果を昇順または降順でソートできます。ソートを実行するには、並べ替える列の見出しの横にある上向き矢印または下向き矢印をクリックします。たとえば、プロセスに基づいて降順のソートを実行するには、[Process] 列見出しの横にある下矢印をクリックします。同様に、プロセス ID に基づいて昇順のソートを実行するには、[PID] 列見出しの横にある上矢印をクリックします。

ステップ 2　ページの更新間隔を変更するには、左上隅にある [Set the screen refresh value] テキストボックスに値を入力し、[Set] をクリックします。入力できる最小値は 5 秒です。

ステップ 3　自動更新機能を無効にするには、左上隅にある [Disable Auto-Refresh] チェックボックスをオンにします。

ステップ 4　プロセスの詳細を表示するには、プロセス名の左側にあるチェックボックスをオンにして、[View Selected Processes] をクリックします。最大 10 のプロセスを選択できます。

[Selected Processes] に、プロセスの詳細が表示されます。このページで、更新頻度や自動更新機能の無効化の設定も行えます。プロセスのロギングを開始するには、[Start Log] をクリックします。ロギングを終了するには、[Stop Log] をクリックします。

プロセスのロギング間隔を変更するには、[Set Process Logging Interval] テキストボックスに 5 ～ 600 秒の値を入力し、[Set] をクリックします。

ステップ 5　ログ ファイルをダウンロードするには、[Process Log Files] ページから [Download Process Logs] をクリックします。（ログ ファイルをダウンロードするには、[Processes] ページから [Download Log File] をクリックします）。

ステップ 6　個々のファイルをダウンロードするには、ダウンロードするログ ファイル名の左側にあるチェックボックスをオンにします。すべてのログ ファイルをダウンロードするには、[File Name] 列見出しの左側にあるチェックボックスをオンにします。ファイルを選択したら、[Download] をクリックします。ダウンロード用に複数のファイルを選択すると、ProcessLogs という名前の圧縮ファイルが作成され、ダウンロードされます。

ステップ 7　ログ ファイルをダウンロードせずに、オンラインで表示することもできます。その場合は、ファイル名をクリックします。別ウィンドウにログ ファイルの内容が表示されます。

関連項目

- 「Processes」（P.B-14）

Disk Usage ツールの使用

Disk Usage ツールは、システム内のさまざまなパーティションで使用されている使用可能なディスク領域の割合を表示します。

Disk Usage ツールを使用するには、次の手順を実行します。

手順

ステップ 1　Emergency Responder Serviceability Web インターフェイスから、[System Monitor]>[Disk Usage] の順に選択します。

[Disk Usage] ページが表示されます。[Disk Usage] ページの詳細については、表 B-17（P.B-16）を参照してください。

ステップ 2　昇順または降順のソートを実行するには、並べ替える基準にする列見出しの横にある上矢印または下矢印をクリックします。たとえば、パーティションに基づいて降順で並べ替えるには、[Partition] 列の見出しの横にある下向き矢印をクリックします。同様に、使用可能なディスク領域に基づいて昇順のソートを実行するには、[Available Space] 列見出しの横にある上矢印をクリックします。

関連項目

- 「Disk Usage」（P.B-15）

Cisco Emergency Responder ログの使用

Emergency Responder 8.6 には、システムやアプリケーションのログを収集するためのインターフェイスが用意されています。これらのログは同じユーザ インターフェイスを共有し、ログ ファイルは同じ方法で表示およびダウンロードできます。次の手順は、すべての Emergency Responder ログに適用されます。

Emergency Responder 8.6 ログは 3 つの種類に構成されます。これらの種類およびそれぞれに含まれるログは次のとおりです。

- Emergency Responder ログ
  - CER Admin
  - CER Server
  - CER Phone Tracking
  - JTAPI
  - Tomcat
  - Event Viewer

  - Audio Driver
- プラットフォーム ログ
  - CLI
  - CLM
  - Certificate Management/IPSec
  - DRS
  - Install/Upgrade
  - Remote Support
  - Syslog
  - Servm
- DB ログ
  - Cerdbmon
  - Install DB
- CLI 出力ファイル
  - Platform
  - DB

Emergency Responder ログを表示するには、次の手順を実行します。

手順

ステップ 1　Emergency Responder Serviceability Web インターフェイスから、[System Logs]>[Log Type]>[Log Name] の順に選択します。

選択された [Log Files] ページが表示されます。これらの各ページの詳細については、次の関連項目の項を参照してください。

結果を昇順または降順でソートできます。ソートを実行するには、並べ替える列の見出しの横にある上向き矢印または下向き矢印をクリックします。

ステップ 2　[Download] ボタンを使用して、ログ ファイルをローカル システムにダウンロードします。

個々のファイルを選択するには、ダウンロードするログ ファイル名の左側にあるチェックボックスをオンにします。すべてのログ ファイルを選択するには、[File Name] 列見出しの左側にあるチェックボックスをオンにします。ファイルを選択したら、[Download] をクリックします。ダウンロード用に複数のファイルを選択すると、CPULogs という名前の圧縮ファイルが作成され、ダウンロードされます。圧縮ファイルの名前は、次のように、含まれるログの種類に基づきます。

- CER Admin
- CERr Server
- CER Phone Tracking
- Syslog
- JTAPI
- Tomcat
- Install
- DRS

- CLILogs
- CMILogs
- ServmLogs
- RemoteSupportLogs
- InstallDBLogs
- CertificateManagement&IPSecLogs
- CerdbmonLogs
- CLIOutputPlatform
- CLIOutputDB

ステップ 3　ログ ファイルをダウンロードせずに、オンラインで表示することもできます。その場合は、ファイル名をクリックします。別ウィンドウにログ ファイルの内容が表示されます。表示しているログ ファイルを更新するには、[Reload Log File] をクリックします。表示しているログ ファイルをダウンロードするには、[Download Log] をクリックします。

関連項目

- 「[System Logs] メニュー」（P.B-16）