トラブルシューティング

この章は、次の項で構成されています。

- システム情報の収集 （1 ページ）
- ハードウェア問題のトラブルシューティング （1 ページ）
- 機能の設定に関する問題のトラブルシューティング （2 ページ）
- 一般的なトラブルシューティング リソース （2 ページ）
- 管理対象アプライアンスのパフォーマンスに関する問題のトラブルシューティング （2 ページ）
- 特定の機能で発生する問題のトラブルシューティング （2 ページ）
- テクニカル サポートの使用 （4 ページ）
- パケット キャプチャの実行 （7 ページ）
- アプライアンスの電源のリモート リセット （8 ページ）

システム情報の収集

シリアル番号を含む、アプライアンスとそのステータスについての情報を取得できます。参照 システム ステータスのモニタリング

ハードウェア問題のトラブルシューティング

ハードウェア アプライアンスの前面/背面パネルのライトは、アプライアンスの状態およびステータスを示します。これらのインジケータの説明については、『*Cisco x90 Series Content Security Appliances Installation and Maintenance Guide*』などのハードウェア ガイドを参照してください（に記載されている場所から入手できます）。

温度範囲など、アプライアンスの仕様についてもこれらのマニュアルで確認できます。

（注） x80 または x90 アプライアンスの電源を再投入する場合は、アプライアンスが起動するまで（すべての LED が緑色になるまで）少なくとも 20 分間待ってから、電源ボタンを押してください。

機能の設定に関する問題のトラブルシューティング

機能を設定できない問題が発生した場合は、各機能で実行する必要があるタスクの概要を参照してください。概要には、それぞれの具体的な情報へのリンクが記載されています。

- 中央集中型 Web レポーティングおよびトラッキングの設定
- 中央集中型の電子メール レポーティングの設定
- 中央集中型メッセージ トラッキングの設定
- 中央集中型スパム隔離の設定
- 集約されたポリシー、ウイルス、およびアウトブレイク隔離
- 中央集中型で Web Security Appliances を管理する Configuration Master の設定

一般的なトラブルシューティング リソース

一般的なトラブルシューティング リソースは次のとおりです。

- 最新アラート。最新アラートの表示を参照してください。
- ログ ファイル。参照先ログ
- 「マニュアルの更新」セクションを含むリリース ノート。資料を参照してください。
- Cisco Bug Search Tool（アクセスの手順はリリース ノートを参照してください）
- ナレッジ ベースの記事（TechNotes）
- シスコ サポート コミュニティ

管理対象アプライアンスのパフォーマンスに関する問題のトラブルシューティング

パフォーマンスに関する問題が発生した場合にシステムが最もリソースを使用している部分を特定するため、すべての管理対象アプライアンス（電子メールまたはWebセキュリティ）と、各管理対象アプライアンスのシステム キャパシティ レポートを参照できます。Eメールセキュリティ アプライアンスの場合、[システム容量（System Capacity）] ページを参照してください。Web セキュリティ アプライアンスの場合、#unique_220を参照してください。

特定の機能で発生する問題のトラブルシューティング

機能の設定に関する問題のトラブルシューティング （2 ページ）も参照してください。

Web セキュリティ関連の問題

- すべてのレポートのトラブルシューティング
- Web レポーティングおよびトラッキングのトラブルシューティング

- コンフィギュレーション管理上の問題のトラブルシューティング
- 機能に関連する問題は、Web セキュリティ アプライアンスの設定が原因の場合もあります。資料に記載されている場所で、ご使用のリリースのリリース ノートおよびオンライン ヘルプかユーザ ガイドを参照してください。

電子メール セキュリティ関連の問題

- すべてのレポートのトラブルシューティング
- メール レポートのトラブルシューティング
- メッセージ トラッキングのトラブルシューティング
- スパム隔離機能のトラブルシューティング
- 集約されたポリシー隔離のトラブルシューティング
- 機能に関連する問題は、E メール セキュリティ アプライアンスの設定が原因の場合もあります。資料に記載されている場所で、ご使用のリリースのリリース ノートおよびオンライン ヘルプかユーザ ガイドを参照してください。

一般的な問題

- コンフィギュレーション ファイルをロードできない場合は、[管理アプライアンス（Management Appliance）]>[システム管理（System Administration）]>[ディスク管理（Disk Management）] ページのテーブルでディスク領域量が各機能の現在のサイズよりも大きいことを確認します。
- アップグレードを最近実行し、オンライン ヘルプの表示が古い場合や、新しい機能に関する情報が見つからない場合は、ブラウザのキャッシュをクリアしてからブラウザ ウィンドウを再度開きます。
- 複数のブラウザ ウィンドウまたはタブを同時に使用している場合、Web インターフェイスを使用して設定を行うと、予期しない動作が発生することがあります。
- アラートへの応答 （3 ページ）を参照してください。
- 管理ユーザ アクセスのトラブルシューティングを参照してください。

アラートへの応答

アラート：380または680ハードウェアでバッテリ再学習タイムアウト（RAIDイベント）（Battery Relearn Timed Out (RAID Event) on 380 or 680 Hardware）

問題：380 または 680 ハードウェアに関して、件名 [バッテリ再学習タイムアウト（Battery Relearn Timed Out）] のアラートを受信します。

解決策：このアラートは、問題を示している場合と示していない場合があります。バッテリ再学習タイムアウト自体は、RAID コントローラに問題があることを示すものではありません。コントローラは、後続の再学習で回復します。以降 48 時間他の RAID アラートに関する電子メールを監視して、この問題が他の問題の副作用ではないことを確認してください。システムから他の RAID 関連のアラートが表示されない場合は、この警告を無視してかまいません。

追加のアラートの説明

追加のアラートについては、次を参照してください。

- ハードウェア アラートの説明
- システム アラートの説明

次の作業

- アラートの管理

テクニカル サポートの使用

アプライアンスからのサポート ケースのオープンおよび更新

この方法を使用して Cisco TAC または独自のサポート サービスに連絡することができます。

始める前に

Cisco TAC に連絡する場合：

- 緊急の問題の場合、この方法は使用しないでください。代わりに、カスタマーサポートに示されるその他の方法の 1 つを使用してサポートください。
- ヘルプに関しては別の選択肢を検討してみてください。
- この手順を使用してサポート事例を開くと、アプライアンスの設定ファイルがシスコ カスタマー サポートに送信されます。アプライアンスの設定を送信したくない場合、別の方法を使用してカスタマー サポートにお問い合わせください。
- アプライアンスがインターネットに接続され電子メールを送信できる必要があります。
- 既存の事例に関する情報を送信する場合は、ケース番号を確認してください。

ステップ 1 アプライアンスへのログイン

ステップ 2 [ヘルプとサポート（Help and Support）]>[テクニカルサポートに問い合わせる（Contact Technical Support）]を選択します。

ステップ 3 サポート リクエストの受信者を設定します。

要求を Cisco TAC に送信する	[Ciscoテクニカルサポート（Cisco Technical Support）] チェックボックスをオンにします。
内部サポート デスクにだけ要求を送信する	• [Ciscoテクニカルサポート（Cisco Technical Support）] チェックボックスをオフにします。 • サポート デスクの電子メール アドレスを入力します。
（任意）他の受信者を追加する	電子メール アドレスを入力します。

ステップ 4 フォームに入力します。

ステップ 5 [送信（Send）] をクリックします。

仮想アプライアンスのサポートの取得

Cisco Content Security 仮想アプライアンスのサポート ケースを報告する場合は、仮想ライセンス番号（VLN）、契約番号、および製品 ID コード（PID）を提供する必要があります。

発注書を参照するか以下の表を使用すると、仮想アプライアンスで動作中のソフトウェア ライセンスに基づく PID を特定できます。

機能	PID	説明
すべての中央集中型 Web セキュリティ機能	SMA-WMGT-LIC=	—
すべての中央集中型電子メール セキュリティ機能	SMA-EMGT-LIC=	

シスコのテクニカル サポート担当者のリモート アクセスの有効化

シスコのカスタマーアシスタンスのみ、次の方法を使用してアプライアンスにアクセスできます。

インターネット接続されたアプライアンスへのリモート アクセスの有効化

サポートは、この手順でアプライアンスと upgrades.ironport.com のサーバ間で作成される SSH トンネル経由でアプライアンスにアクセスします。

始める前に

インターネットから到達可能なポートを識別します。デフォルトでは、ポート25で、このポートは大部分の環境で機能します。このポート経由の接続は、ほとんどのファイアウォール設定で許可されます。

ステップ 1 アプライアンスにログインします。

ステップ 2 GUI ウィンドウの右上にある、[ヘルプとサポート（Help and Support）] > [リモートアクセス（Remote Access）] を選択します。

ステップ 3 [有効化（Enable）] をクリックします。

ステップ 4 情報を入力します。

ステップ 5 [送信（Submit）] をクリックします。

次のタスク

サポート担当者のリモート アクセスが必要なくなったときは、テクニカル サポートのトンネルの無効化 （6 ページ）を参照してください。

インターネットに直接接続されていないアプライアンスへのリモートアクセスの有効化

インターネットに直接接続されていないアプライアンスの場合、インターネットに接続されている第 2 のアプライアンスを介してアクセスされます。

始める前に

- アプライアンスは、インターネットに接続されている第 2 のアプライアンスにポート 22 で接続する必要があります。
- インターネットに接続されているアプライアンスで該当アプライアンスへのサポート トンネルを作成するには、インターネット接続されたアプライアンスへのリモートアクセスの有効化 （5 ページ）の手順を実行します。

ステップ 1 サポートが必要なアプライアンスのコマンドライン インターフェイスから、`techsupport` コマンドを入力します。

ステップ 2 `sshaccess` と入力します。

ステップ 3 プロンプトに従います。

次のタスク

サポート担当者のリモートアクセスが必要なくなったときは、次のトピックを参照してください。

- リモート アクセスの無効化 （7 ページ）
- テクニカル サポートのトンネルの無効化 （6 ページ）

テクニカル サポートのトンネルの無効化

有効にした techsupport トンネルは、upgrades.ironport.com に 7 日間接続されたままになります。その後、確立された接続は切断されませんが、いったん切断されるとトンネルに再接続できません。

ステップ 1 アプライアンスにログインします。

ステップ 2 GUI ウィンドウの右上にある、[ヘルプとサポート（Help and Support）] > [リモートアクセス（Remote Access）] を選択します。

ステップ 3 [無効（Disable）] をクリックします。

リモート アクセスの無効化

techsupport コマンドを使用して作成したリモート アクセス アカウントは、非アクティブ化されるまでアクティブのままです。

ステップ 1 コマンドライン インターフェイスから、`techsupport` コマンドを入力します。
ステップ 2 `sshaccess` と入力します。
ステップ 3 `disable` と入力します。

サポートの接続状態の確認

ステップ 1 コマンドライン インターフェイスから、`techsupport` コマンドを入力します。
ステップ 2 status と入力します。

パケット キャプチャの実行

パケット キャプチャは、サポート担当者が TCP/IP データおよびその他にアプライアンスから出入りするパケットを表示できるようにします。これはネットワーク設定をデバッグしたり、どのようなネットワーク トラフィックがアプライアンスに到達または送出されているかを検出することができます。

ステップ 1 [ヘルプとサポート（Help and Support）] > [パケットキャプチャ（Packet Capture）] を選択します。
ステップ 2 パケット キャプチャ設定の指定：

a) [パケットキャプチャ設定（Packet Capture Settings）] セクションで、[設定を編集（Edit Settings）] をクリックします。
b) （任意）パケット キャプチャの期間、制限およびフィルタを入力します。

サポート担当者が、これらの設定の方法を説明する場合があります。

時間の単位を指定しないでキャプチャ期間を入力すると、AsyncOS はデフォルトで秒を使用します。

[フィルタ（Filters）] セクションで次を実行します。

- カスタム フィルタでは UNIX の `tcpdump` コマンドでサポートされる host 10.10.10.10 && port 80 のような構文を使用できます。
- クライアント IP は、E メール セキュリティ アプライアンスを介してメッセージを送信するメール クライアントなどのアプライアンスに接続しているマシンの IP アドレスです。
- サーバ IP は、アプライアンスがメッセージを配信する Exchange サーバなどのアプライアンスが接続しているマシンの IP アドレスです。

クライアントとサーバの IP アドレスを使用して、中間に E メール セキュリティ アプライアンスがある特定のクライアントと特定のサーバ間のトラフィックを追跡できます。

c) [送信（Submit）] をクリックします。

ステップ 3 [キャプチャを開始（Start Capture）] をクリックします。

- キャプチャは一度に 1 つだけ実行できます。
- パケット キャプチャが実行されている場合、[パケットキャプチャ（Packet Capture）] ページには、実行中のキャプチャのステータス（ファイル サイズや経過時間などの現在の統計情報）が表示されます。
- GUI に表示されるのは GUI で開始されたパケット キャプチャだけで、CLI で開始されたパケット キャプチャは表示されません。同様に、CLI には CLI で開始された現在のパケット キャプチャのステータスだけが表示されます。
- パケット キャプチャ ファイルは 10 個の部分に分割されます。パケット キャプチャが終了する前にパケット キャプチャ ファイルが最大サイズ制限に到達した場合は、そのファイルの最も古い部分が削除され（データが破棄されます）、現在のパケット キャプチャ データで新しい部分が開始されます。パケット キャプチャ ファイルは一度に 1/10 だけ破棄されます。
- GUI で開始されたキャプチャはセッション間で維持されます。（CLI で実行したキャプチャは、セッションが終了したときに停止します）。

ステップ 4 キャプチャを指定した期間実行するようにします。またはキャプチャを無期限に実行する場合、[キャプチャを停止（Stop Capture）] をクリックして停止します。

ステップ 5 パケット キャプチャ ファイルへアクセスします。

- [パケットキャプチャファイルの管理（Manage Packet Capture Files）] リストでファイルをクリックして、[ファイルのダウンロード（Download File）] をクリックします。
- アプライアンスの captures サブ ディレクトリ内のファイルにアクセスするには、FTP または SCP を使用します。

次のタスク

サポートでファイルを使用できるようにします。

- アプライアンスへのリモート アクセスを許可した場合、Technician が FTP または SCP を使用してパケット キャプチャ ファイルにアクセスできます。シスコのテクニカル サポート担当者のリモート アクセスの有効化 （5 ページ）を参照してください。
- 電子メールでファイルをサポートに送信します。

アプライアンスの電源のリモート リセット

アプライアンスのハード リセットが必要な場合は、サードパーティの Platform Management（IPMI）ツールを使用してアプライアンス シャーシをリモートからリブートできます。

制約事項

- リモート電源管理は、特定のハードウェアでのみ使用できます。

  詳細については、リモート電源再投入の有効化を参照してください。

- この機能を使用可能にするには、事前に有効にする必要があります。

  詳細については、リモート電源再投入の有効化を参照してください。

- 次の IPMI コマンドのみがサポートされています。

  `status、on、off、cycle、reset、diag、soft`

  サポートされていないコマンドを発行すると、「権限不足」エラーが発生します。

始める前に

- IPMI バージョン 2.0 を使用してデバイスを管理できるユーティリティを取得し、設定します。
- サポートされている IPMI コマンドの使用方法を理解します。IPMI ツールのマニュアルを参照してください。

ステップ 1 IPMI を使用して、必要なクレデンシャルと共に、先に設定したリモート電源管理ポートに割り当てられた IP アドレスに、サポートされている電源の再投入コマンドを発行します。

たとえば、IPMI をサポートする UNIX タイプのマシンからは、次のようなコマンドを発行します。

```
ipmitool -I lan -H 192.0.2.1 -U remoteresetuser -P password chassis power reset
```

ここで `192.0.2.1` は、リモート電源管理ポートに割り当てられた IP アドレスであり、remoteresetuser およびパスワードは、この機能を有効にしたときに入力したクレデンシャルです。

ステップ 2 アプライアンスが再起動されるまで、少なくとも 11 分間待ちます。