ネットワークの管理

この 章 では、Cisco Prime ネットワーク解析モジュール ソフトウェアで実行する必要があるユーザおよびシステム管理タスク、およびテクニカル サポートの要求時に診断情報を生成する方法について説明します。

この章は、次の項で構成されています。

システム データの管理

管理者のロールの 1 つは、次の目的のために、Prime NAM のネットワーク データの収集および保持を管理することです。

- システムのユーザの実際のニーズに合わせて拡張する。
- 監視対象デバイス、アプリケーション、およびネットワーク帯域幅の負荷を最小限に抑える。
- ハードウェア障害に対処する。

次の各項では、これらの目標を達成する方法、およびその他のデータ管理タスクを実行する方法について説明します。

バックアップの処理

必要に応じて設定およびデータを復元できるように、システムをバックアップすることが重要です。十分なデータのバックアップがスケジュールされていることを確認します。

ストレージ要件の縮小

ネットワーク管理者は、ネットワークのストレージの要件を縮小し、バックアップおよびリカバリなどのタスクでの帯域幅効率を向上させる方法を一貫して探しています。

サポートされるプラットフォーム上で Prime NAM のパケットの重複排除を設定することで、検査したセグメントが特定の時間ウィンドウ内の別のパケットと一致するパケットは重複としてマークされ、転送されません。

設定時の注意事項および手順については、「ハードウェア内の重複排除の設定」（P.3-39）を参照してください。

システム管理の実行

次のシステム管理タスクを実行できます。

Prime NAM のヘルスおよびトラフィック統計情報のモニタリング

Cisco NAM が過負荷にならずに効率的かつ効果的にトラフィックを処理することを確認することが重要なタスクです。

Cisco NAM で受信されたネットワーク トラフィックに加え、そのヘルスに関するデータ（サーバ ネットワークの詳細、および CPU、メモリ、データ使用状況など）を表示するには、[Administration] > [System] > [Overview] を使用します。

スケーラビリティの問題を特定し、トラブルシューティングを支援するには、[Inputs] および [Resources] タブで提供されるデータを使用します。

表 6-1 に、[System Overview] ウィンドウの情報の種類を示します。

表 6-1　システムの概要

フィールド	説明
[Inputs] タブ	
Cumulative Input Statistics	NAM が受信するすべてのトラフィックのヘルスおよび使用状況の情報。受信パケット数（Rx Packets）、消失またはドロップされたパケット数（Rx Packets Lost）、受信バイト数（Rx Bytes）を表示します。[Cumulative] カラムは NAM が起動してからの累積カウント、[Rate] カラムは直前の 10 秒間の同じカウンタを示します。
Input Traffic	選択した入力に基づくバイトおよびパケット単位の使用状況情報。図表形式または表形式を切り替えることができます。データは、30 秒ごとに更新され、過去 1 時間のデータが含まれます。テーブルの時間間隔は変更できません。入力テーブル レートは 10 秒ごとに計算されます。凡例は、ある期間にわたって収集されたデータに関してソフトウェアによって提供される標準統計情報のデータを提供します。 **（注）** このページで PA トラフィックを表示するには、ポート 3100 を使用して PA トラフィックを NAM に送信するようにデバイスを設定する必要があります。
[Resources] タブ	
Date	現在の日付と時刻（スイッチ、ルータ、または NTP サーバと同期している）
Host Name	NAM のホスト名
IP Address	選択（IPv4 または IPv6）に基づく NAM IP アドレス情報。
System Uptime	ホストが中断なしで稼働する時間の長さ
Disk Usage	config、root、および data パーティションと、それぞれの総容量および空き容量。パフォーマンス データベース ファイル（DB）およびディスクに対するパケット キャプチャ（キャプチャ ファイル）で使用されるディスク容量も表示します。 十分なディスク容量があることを確認し、必要に応じて必要なメンテナンスを実行するためにこの情報を使用します。
Utilization	NAM によって消費されるメモリ リソースの比率、および使用可能な合計メモリ。
CPU Usage	NAM によって消費される CPU リソースの比率。マルチ CPU プラットフォームの CPU はそれぞれ個別に示されます。

ネットワーク パラメータの設定

サイトのネーム サーバなどのネットワーク パラメータを表示および設定するには、次の手順を実行します。

ステップ 1　[Administration] > [System] > [Network Parameters] を選択します。

[Network Parameters] ウィンドウが表示されます。

ステップ 2　情報を入力または変更します。

ステップ 3　次のどちらかを実行します。

- 変更を保存するには、[Submit] をクリックします。
- 変更を取り消すには、[Reset] をクリックします。

SNMP エージェントの設定

SNMP エージェントは、管理対象デバイス内のネットワーク管理ソフトウェア モジュールです。管理情報に関するローカルな知識があり、その情報を SNMP と互換性のある形式に変換します。

SNMPv2 および SNMPv1 に加えて、SNMPv3 でデバイスを管理できます。NAM は管理対象デバイスをポーリングして、その基本的な状態およびインターフェイスの統計情報を取得します。NAM ブレードの場合、管理対象デバイスは NAM が挿入されているスイッチで、NAM ソフトウェアは、ポーリングを行うために、SNMP およびコミュニティ ストリングの使用をスイッチとネゴシエーションします。このコミュニティ ストリングは NAM と使用する場合のみ有効です。セキュリティを考慮して、スイッチではコミュニティ ストリングが NAM の IP アドレスのみに関連付けられ、他の SNMP アプリケーションではこのスイッチとの通信にこのコミュニティ ストリングを使用することはできません。コミュニティ ストリングの詳細については、「NAM コミュニティ ストリングの使用」（P.6-5）を参照してください。

また、さらにセキュリティ上の問題を軽減するために、SNMP は NAM ブレードの間で交換を行い、スイッチは内部バックプレーン バスで行われます。これらの SNMP パケットは、スイッチの外にあるどのネットワークまたはインターフェイスでも見えません。スイッチ内部では、完全にセキュアなアウトオブバンド チャネルです。

Cisco NAM アプライアンスなど他のプラットフォームの場合は、任意の IP アドレスを入力し、それを管理対象デバイスとして使用できます。管理対象デバイスの設定では、仮想 NAM プラットフォーム管理対象デバイスは NAM アプライアンスと同様に機能します。すべてのプラットフォームで、NAM は一度に 1 台の管理対象デバイスのみデータをモニタし、表示できます。

この場合、管理対象デバイスは、よりセキュアであるという理由で SNMPv3 のみ使用する場合があります。

（注）　NAM ブレードは、SNMPv2 を使用して、管理対象デバイスをローカルに管理します。

NAM SNMP エージェントを表示および設定するには、次の手順を実行します。

ステップ 1　[Administration] > [System] > [SNMP Agent] を選択します。

ステップ 2　[NAM SNMP] ウィンドウの情報を入力または変更します。フィールドは、表 6-2 で詳しく説明されています。

表 6-2　[System SNMP] ダイアログボックス

フィールド	説明
Contact	NAM の担当者の名前
Name	NAM の名前
Location	（任意）NAM を搭載するスイッチまたはルータの物理的な場所

ステップ 3　次のどちらかを実行します。

- 変更を保存するには、[Submit] をクリックします。
- 変更を取り消すには、[Reset] をクリックします。

NAM コミュニティ ストリングの使用

コミュニティ ストリングを使用することにより、他のアプリケーションが、SNMP get および SNMP set 要求の NAM への送信、収集の設定、データのポーリングなどを実行できるようになります。

NAM コミュニティ ストリングの作成

NAM コミュニティ ストリングを作成するには、次の手順を実行します。

ステップ 1　[Administration] > [System] > [SNMP Agent] を選択します。

ウィンドウの下部に、[NAM Community Strings] ダイアログボックスが表示されます。

ステップ 2　[作成（**Create**）] をクリックします。

[SNMP Agent] ダイアログボックスが表示されます。

ステップ 3　コミュニティ ストリングを入力します（意味のある名前を使用）。

ステップ 4　[Verify Community] フィールドに、コミュニティ ストリングを再入力します。

ステップ 5　次の基準を使用して、読み取り専用権限、または読み取り / 書き込み権限を割り当てます。

- 読み取り専用は、SNMP MIB 変数への読み取りアクセスだけが可能です（get）。
- 読み取り / 書き込みは、SNMP MIB 変数への完全な読み取りおよび書き込みアクセスが可能です（get と set）。

ステップ 6　次のどちらかを実行します。

- 変更するには、[Submit] をクリックします。
- リセットするには、[Reset] をクリックします。
- キャンセルし、前のウィンドウに戻るには [Cancel] をクリックします。

NAM コミュニティ ストリングの削除

NAM コミュニティ ストリングを削除するには、次の手順を実行します。

ステップ 1　[Administration] > [System] > [SNMP Agent] を選択します。

ウィンドウの下部に、[NAM Community Strings] ダイアログボックスが表示されます。

ステップ 2　エントリを選択して、[Delete] をクリックします。

注意　NAM コミュニティ ストリングを削除すると、SNMP エージェントの外部から NAM への SNMP 要求がブロックされます。

コミュニティ ストリングが削除されます。

ルータ コミュニティ ストリングのテスト

ルータが SNMP を使用して NAM に情報を送信する前に、NAM で設定されているルータ コミュニティ ストリングは実際のルータで設定されているコミュニティ ストリングと一致する必要があります。[Router Parameters] ダイアログボックスに、ルータ名、ハードウェア、スーパーバイザ エンジン ソフトウェアのバージョン、システム稼働時間、ロケーション、連絡先情報が表示されます。

ローカル ルータ IP アドレスおよび SNMP コミュニティ ストリングは、NAM がローカル ルータと通信できるように設定する必要があります。

コミュニティ ストリングをルータに設定するには、ルータ CLI を使用します。CLI の使用方法については、デバイスに付属しているマニュアルを参照してください。

注意　入力するルータ コミュニティ ストリングは、ルータの読み取り / 書き込みコミュニティ ストリングと一致する必要があります。一致しない場合、ルータと通信できません。

ルータ コミュニティ ストリングをテストするには、次の手順を実行します。

ステップ 1　[Setup] > [Managed Device] > [Device Information] を選択します。

[Device Information] ダイアログボックスが表示されます。

ステップ 2　デバイスのコミュニティ ストリングを入力します。

ステップ 3　[Test Connectivity] をクリックします。

ステップ 4　NAM がデバイスと通信できるようになるまでしばらく待ちます。OK と表示されたら、[Submit] をクリックします。

システム時刻の同期

Prime NAM ソフトウェア アプリケーションの Linux システム時刻がパケットのタイムスタンプ、および NAM プラットフォームの外側の標準時刻源と同期していることを確認します。パケット タイミング分析は、アプリケーション応答時間の測定、音声とビデオの品質メトリック、パケットのデコード データ、レポート、およびその他の多くのネットワーク統計をサポートするために使用します。

NAM は、NAM プラットフォームのタイプに応じて複数のソースから UTC（GMT）を取得します。すべての NAM は、外部 NTP サーバから時刻を取得するように設定できます。他の NAM プラットフォームは、高い確度と精度のために IEEE 1588 高精度時間プロトコル（PTP）ベースのマスターも使用できます。

注意　クライアント コンピュータおよび NAM サーバ両方で、それぞれ該当のタイム ゾーンの時間が正確に設定されている必要があります。クライアントまたはサーバ時間に誤りがあれば、GUI に表示されるデータに誤りが生じます。

クロック ID は、以下の例に示すように、MAC アドレスの最初の 3 オクテット、「ff fe」、MAC アドレスの最後の 3 オクテットで構成されています。

```
root@nam.localdomain# sho time ptp parent
PTP PARENT PROPERTIES
  Parent Clock:
  Parent Clock Identity: 0xec:44:76:ff:fe:5d:12:0
  Parent Port Number: 6
```

NAM が時間を取得したら、[NAM System Time] 設定ウィンドウを使用してローカル タイム ゾーンを設定できます。

特定のハードウェア プラットフォームに対して NAM システム時刻を設定する方法の詳細については、「特定のプラットフォームに対する NAM システム時刻の同期」（P.6-7）を参照してください。

特定のプラットフォームに対する NAM システム時刻の同期

NAM システム時刻が正しく設定されていることを確認します。システム時刻に誤りがあれば、時間範囲のために NAM データ プレゼンテーションが不正確になるので、NAM データの解釈が正しくなくなる可能性があります。

一部のプラットフォームは自動的に同期されますが、データが正確になるためには、NAM およびルータまたはスイッチに加えてクライアント ブラウザが同期する必要があります。プラットフォームの時刻の同期を実行することを推奨します。

次のいずれかの方法を使用して NAM システム時刻を設定できます。

- 「NAM システム時刻とスイッチまたはルータとの同期」（P.6-8）

  このオプションは NAM-1X、NAM-2X、NAM-3、NME-NAM、SM-SRE、および NAM-NX1 にのみ有効です。

- 「NAM システム時刻のローカルな同期」（P.6-8）

  このオプションは Cisco NAM アプライアンス、Nexus 1000 VSB、vNAM にのみ有効です。

- 「NTP サーバによる NAM システム時刻の設定」（P.6-8）

  これはすべてのプラットフォームに有効で、推奨オプションです。

- 「高精度時間プロトコル（IEEE 1588）を使用した NAM システム時刻の設定」（P.6-9）

  このオプションは、NAM-NX1 および NAM-3 に有効です。

NAM システム時刻とスイッチまたはルータとの同期

（注）　この項は、NAM-1X、NAM-2X、NAM-3、NME-NAM、SM-SRE、および NAM-NX1 にのみ有効です。追加のプラットフォーム オプションについては、「特定のプラットフォームに対する NAM システム時刻の同期」（P.6-7）を参照してください。

スイッチまたはルータから NAM システム時刻を設定するには、次の手順を実行します。

ステップ 1　[Administration] > [System] > [System Time] を選択します。

ステップ 2　[Switch] または [NTP Server] オプション ボタンを選択します。

ステップ 3　地域とローカル タイム ゾーンをリストから選択します。

ステップ 4　次のどちらかを実行します。

- 変更を保存するには、[Submit] をクリックします。
- 設定を変更しない場合は、[Reset] をクリックします。

NAM システム時刻のローカルな同期

（注）　この項は、Cisco NAM アプライアンス、Nexus 1000V、vNAM に有効です。追加のプラットフォーム オプションについては、「特定のプラットフォームに対する NAM システム時刻の同期」（P.6-7）を参照してください。

NAM システム時刻をローカルに設定するには、NAM コマンドラインを使用します。

ステップ 1　NAM のコマンドライン インターフェイスにログインします。

ステップ 2　CLI **clock set** コマンドを使用してクロックを設定します。

clock set ***<hh:mm:ss:>*** ***<mm/dd/yyyy>***

ステップ 3　Prime NAM GUI で、[Administration] > [System] > [System Time] を選択します。

ステップ 4　[Local] オプション ボタンをクリックします。

ステップ 5　地域とローカル タイム ゾーンをリストから選択します。

ステップ 6　次のどちらかを実行します。

- 変更を保存するには、[Submit] をクリックします。
- 設定を変更しない場合は、[Reset] を選択します。

NTP サーバによる NAM システム時刻の設定

NTP サーバを使用して NAM のシステム時刻を設定するには、次の手順を実行します。

ステップ 1　NAM アプライアンス GUI で、[Administration] > [System] > [System Time] を選択します。

ステップ 2　[NTP Server] オプション ボタンを選択します。

ステップ 3　1 つまたは 2 つの NTP サーバ名または IP アドレスを、[NTP sever name] テキスト ボックスまたは [IP Address] テキスト ボックスに入力します。

ステップ 4　地域とローカル タイム ゾーンをリストから選択します。

ステップ 5　変更を保存するには、[Submit] をクリックします。

高精度時間プロトコル（IEEE 1588）を使用した NAM システム時刻の設定

高精度時間プロトコル（PTP）を使用するには、PTP 対応またはマルチキャスト対応のスイッチを NAM-3 の前面にある SYN ポートに接続するだけでなく、PTP マスターをスイッチに接続する必要があります。

（注）　この項は、NAM-3 および NAM-NX1 に適用できます。この機能に関連しているハードウェア設定の要件の詳細については、特定の NAM installation guide を参照してください。追加のプラットフォーム オプションについては、「特定のプラットフォームに対する NAM システム時刻の同期」（P.6-7）を参照してください。

PTP を使用して NAM システム時刻を設定するには、次の手順を実行します。

ステップ 1　NAM で、[Administration] > [System] > [System Time] を選択します。

ステップ 2　[PTP] オプション ボタンを選択します。

ステップ 3　[PTP Interface IP Address] フィールドに PTP インターフェイスの IP アドレスを入力します。

ステップ 4　[PTP Interface Subnet Mask] フィールドにサブネット マスクを入力します。

ステップ 5　NAM ローカル タイム ゾーンに対して、ドロップダウン リストから地域とゾーンを選択します。

ステップ 6　変更を保存するには、[Submit] をクリックして、引き続き次の項「高精度時間プロトコルのステータス表示」で PTP の詳細情報を表示します。

高精度時間プロトコルのステータス表示

ステップ 1　上記の手順「高精度時間プロトコル（IEEE 1588）を使用した NAM システム時刻の設定」を使用して PTP を設定します（これはステータスが正常に表示される前に行う必要があります）。

ステップ 2　[Administration] > [System] > [System Time] を選択します。

ステップ 3　ドロップダウン メニューから選択し、[Show] ボタンをクリックします。表示されるポップアップ ウィンドウに、選択した内容の詳細情報が表示されます。

- clock
- foreign-master-record
- parent
- time-property

アラームの電子メール通知の設定

アラーム通知やレポートを電子メールで送信するように Prime NAM を設定できます。

電子メール通知を設定するには、次の手順を実行します。

ステップ 1　[Administration] > [System] > [E-Mail Setting] を選択します。

ステップ 2　[Enable Mail] チェックボックスをオンにし、必須情報またはオプション フィールド情報を入力します。

表 6-3 に 「Mail Configuration オプション」を示します。

ステップ 3　オプションの [Advanced Settings] チェックボックスをオンにし、表示されたフィールドに詳細を入力します。

ステップ 4　変更を保存するには、[Submit] をクリックします。または、ダイアログに入力した文字をクリアする、または以前の設定に戻すには、[Reset] をクリックします。

表 6-3　Mail Configuration オプション

フィールド	説明
Enable Mail	レポートおよびアラーム通知の E メール送信をイネーブルにします。
External Mail Server	外部メール サーバの識別名。
Send Test Mail to	オプション 最大 3 つまで、E メール受信者の電子メール アドレスを一覧表示します。
Mail Alarm to	この受信者はアラーム通知およびスケジュールされたエクスポートを受信します。
Advanced Settings	電子メール アクセス サーバ ポートを指定できるほか、暗号化プロトコルを選択できます。
Mail Server Port	オプション NAM の電子メール ポートを指定します。
Mail Server Encryption	オプション 電子メール メッセージに対して暗号化されたセキュア ソケット レイヤ（SSL）またはトランスポート層セキュリティ（TLS）を選択します。

Web データ パブリケーションの有効化による NAM データの共有

Web データ パブリケーションでは、一般の Web ユーザや Web サイトが、ログイン セッションを確立することなく、選択された NAM のモニタ画面やレポート画面にアクセス（またはリンク）できます。

Web データ パブリケーションは、オープンにすることもできれば、アクセス コントロール リスト（ACL）またはパブリケーション コード、もしくは両方を使用して制限することもできます。公開されたデータにアクセス可能にするために、必要な場合は、パブリケーション コードを URL アドレスまたはクッキーで提供する必要があります。

Web データ パブリッシングをイネーブルにするには、次の手順を実行します。

ステップ 1　[Administration] > [System] > [Web Data Publication] を選択します。

ステップ 2　[Enable Web Data Publication] チェックボックスをオンにします。

ステップ 3　パブリケーション コードを入力します（オプション）。これは、開されたページにアクセスするために、URL のクッキーに必要なパスコード。たとえば、*abc123* に設定されたパブリケーション コードでは、次の公開されたウィンドウにアクセスできます。

http://<nam-hostname>/application-analysis/index?publicationcode=abc123

ステップ 4　ACL Permit IP Address/Subnets を入力すると、それらの IP アドレスまたはサブネットだけに、Web パブリケーションへのアクセスを許可します。何も入力しないと、対象を問わずオープンなアクセスを提供します。

ステップ 5　Web パブリッシングをイネーブルにするには、[Submit] をクリックします。または、ダイアログに入力した文字をクリアするには、[Reset] をクリックします。

（注）　新しい iSCSI ストレージ エントリを有効にするには、NAM システムをリブートする必要があります。

Syslog メッセージを受信するリモート サーバの設定

NAM syslogs は、アラームしきい値イベント、音声しきい値イベント、またはシステム アラートについて作成されます。syslog メッセージは、NAM 上でローカルにロギングされるようにするか、リモート ホストでロギングされるようにするか、または両方でロギングされるようにするかを指定できます。NAM を使用して、ローカルの NAM syslog を表示できます。

リモート ホストでロギングする場合、ほとんどの Unix 対応システムでは、着信 syslog メッセージを処理する Syslog Collector は facility フィールドを使用して、メッセージに書き込むファイルを判断します。*local7* というファシリティが使用されます。*local7* が正しく処理されるよう、Syslog Collector の設定を確認します。

NAM syslog を設定するには、次の手順を実行します。

ステップ 1　[Administration] > [System] > [Syslog Setting] を選択します。

[NAM Syslog Setting] ウィンドウが表示されます。

ステップ 2　[Remote Server Names）] フィールドに、syslog メッセージのロギングを行う最大 5 つのリモート システムの IP アドレスまたは DNS 名を入力します。入力した各アドレスが、3 種類のアラームすべて（アラームしきい値、音声シグナリングのしきい値、およびシステム）を受け取ります。

ステップ 3　[Submit] をクリックして変更内容を保存するか、または [Reset] をクリックしてキャンセルします。

Prime NAM から SNMP トラップを受信するホストの設定

トラップは、イベントにまたがるしきい値によってトリガーされたアラームの保存に使用されます。アラームがトリガーされたら、イベントをトラップして、別のホストに送信することができます。トラップによる通知を使用すると、それほど重要ではない SNMP 要求を削減できるので、ネットワークとエージェントのリソースを大幅に節約できます。

Prime NAM がトラップを送信するホストの宛先を設定、編集、または削除するには、次の手順を実行します。

ステップ 1　[Administration] > [System] > [SNMP Trap Setting] を選択します。

[SNMP Trap Setting] ウィンドウが表示されます。

ステップ 2　[Create] ボタンをクリックします。

ステップ 3　[Community] フィールドに、[NAM Thresholds] に設定されたコミュニティ ストリングを入力します。

ステップ 4　[IP Address] フィールドに、アラームとトラップのコミュニティ ストリングが一致した場合のトラップの送信先とする IP アドレスを入力します。

ステップ 5　[UDP Port] フィールドに、UDP ポート番号を入力します。

ステップ 6　[Submit] をクリックして変更内容を保存するか、または [Reset] をクリックしてキャンセルし、設定を変更せずそのままにします。

システム設定のリセット

Prime NAM 表示やロギングの特性を変更するには、[Administration] > [System] > [Preferences] を選択します。表 6-4 に、[Preferences] ウィンドウのフィールドを示します。

表 6-4　System ビューとロギング プリファレンス

フィールド	説明
Refresh Interval (60-3600 sec)	ダッシュボードの情報をリフレッシュする時間の間隔。
Top N Entries (1-10)	Top N グラフの色分けバーの数。
Perform IP Host Name Resolution	IP アドレスの代わりにホスト名を表示します。このオプションは、DNS ルックアップを使用して変換を実行します。
Data Displayed In	ビットまたはバイト単位で表示されるデータ。
International Notation	番号付けの表示オプション。
Audit Trail	記録された最近のイベントのリストを表示します。これには、CLI および GUI 設定イベントが含まれます。
Capture File Download Format	キャプチャされたファイルをローカル マシンにダウンロードする方法を変更するには、ENC（**.enc**）または PCAP（**.pcap**）形式を選択します。

診断ツールを使用したトラブルシューティング

[Administration] メニューの [Diagnostics] オプションには、トラブルシューティングを支援するツールがあります。Cisco Technical Assistance Center（TAC）からのサポートが必要な問題が発生したときに、これらのツールを使用できます。次のオプションがあります。オプションは次のとおりです。

- 「システム アラート」（P.6-13）
- 「監査証跡」（P.6-13）
- 「テクニカル サポート」（P.6-14）

NAM のトラブルシューティングの詳細については、ネットワークおよび NAM の問題のトラブルシューティングを参照してください。

システム アラート

通常の運用中に NAM が検出した障害または問題を表示できます。[System Alerts] を表示するには、**[Admin] > [Diagnostics] > [System Alerts]** を選択します。

各アラートに、日付、アラートが発生した時刻、アラートを説明するメッセージが示されます。NAM は最大で 1,000 個の最新アラートを表示します。1,000 個を超えるアラートが発生している場合、すべてのアラートを表示するには、NAM CLI コマンド **show tech support** を使用する必要があります。

アラートの発生状況に気付き、アラートの原因となっている状況をトラブルシューティングし解決しようとする場合は、[Clear] をクリックしてアラートのリストを削除し、追加のアラートが発生するかどうかを確認します。

監査証跡

Audit Trail オプションは、内部の **syslog** ログ ファイルに記録された最近の重要なアクティビティのリストを表示します。また、syslog メッセージを外部のログに送信することもできます。

監査証跡には、次のユーザ アクティビティが記録されます。

- すべての CLI コマンド
- ユーザ ログイン（失敗した試行を含む）
- 不正アクセスの試行
- SPAN の変更
- NetFlow データ ソースの変更
- データ収集のイネーブル化およびディセーブル化
- キャプチャの開始および停止
- ユーザの追加および削除

各ログ エントリには、次の情報が含まれます。

- ユーザ ID
- Time stamp
- IP アドレス（リモート Web アクセスの場合）
- アクティビティの説明

[Audit Trail] ウィンドウにアクセスするには、次の手順を実行します。

ステップ 1　[Administration] > [Diagnostics] > [Audit Trail] を選択します。

[Audit Trail] ウィンドウが表示されます。

[Audit Trail] ウィンドウでは、ユーザ アクセス ログを表示し、時刻、ユーザ、実行元（IP アドレス）、またはアクティビティに基づいてエントリをフィルタできます。内部ログ ファイルは、一定のサイズ制限に達すると、順次、別の新たなログ ファイルが作成され記録されます。

テクニカル サポート

NAM の syslog は NAM システム アラートを記録します。アラートには、イベントの内容、日付およびタイムスタンプが含まれ、予期しない、または潜在的に重大な状態が示されます。この機能によって、潜在的で広範囲にわたるさまざまな内蔵システムのトラブルシューティング コマンドおよびシステム ログの結果が表示される可能性があります。監査証跡ウィンドウに記録されるユーザ アクティビティのリストについては、「監査証跡」（P.6-13）を参照してください。

この情報は、普通のユーザにはあまり重要ではありません。これは、Cisco TAC がデバッグを目的として使用するためのものです。この情報を理解する必要はありませんが、情報を保存し、Cisco TAC への電子メール メッセージに添付する必要があります。

[Tech-Support] ページを表示する前に、[Administration] > [Users] > [Local Database] ページで System Config ユーザ特権をイネーブルにする必要があります。ユーザ特権の編集については、「TACACS+ 認証および認可の確立」（P.6-17）を参照してください。

（注）　この情報は、NAM CLI で表示することもできます。NAM CLI の使用方法については、『*Cisco Network Analysis Module Command Reference*』を参照してください。

テクニカル サポートを表示するには、次の手順を実行します。

ステップ 1　[Administration] > [Diagnostics] > [Tech Support] を選択します。

数分後、大量の診断情報が生成され、[Diagnostics Tech Support] ウィンドウに表示されます。

ステップ 2　情報を保存するには、ブラウザ メニューで [File] > [Save As...] を選択するか、下部までスクロールし [NAM-logs.tar.bz2] をクリックして、ローカル PC に保存します。

コア ファイルのダウンロード

[Tech-Support] ページからコア ファイルをダウンロードするには、[Core Files] セクションまで下にスクロールして、ファイル名をクリックし、指示に従います。

ユーザ アクセスの制御

[Administration] オプションを使用して、ユーザのアクセスを制御できます。

- 「ローカル データベース」（P.6-15）
- 「TACACS+ 認証および認可の確立」（P.6-17）
- 「NAM 認証と認可をサポートする TACACS+ サーバの設定」（P.6-18）

- 「Current User Sessions」（P.6-22）

ローカル データベース

NAM をインストールするとき、NAM コマンドライン インターフェイス（CLI）を使用して HTTP サーバをイネーブルにし、NAM に最初にアクセスするユーザ名とパスワードを確立します。

最初のユーザ アカウントの設定後は、追加のアカウントを作成し、さまざまなアクセス レベルをユーザごとに個別にイネーブルまたはディセーブルにできます。

表 6-6 に、「ユーザの権限」と各特権の説明を示します。

ユーザの作成と編集の詳細については、「新しいユーザの作成」（P.6-15）および「TACACS+ 認証および認可の確立」（P.6-17）を参照してください。

リセット : パスワード

NAM パスワードをリセットする最も簡単な方法は、CLI **clear system-passwords** コマンドを使用することです。このコマンドは、ルートとゲスト ユーザ パスワードの両方を工場出荷時のデフォルト状態にリセットします。パスワードをリセットするには、適切な権限が必要です。

スイッチまたはルータで CLI コマンドを使用して、パスワードを回復することもできます。NAM パスワードのリセットの詳細については、Cisco.com のプラットフォームのインストレーション ガイドを参照してください。

NAM 管理者パスワードを忘れた場合、次のいずれかの方法でパスワードを回復できます。

- 別のユーザがアカウント管理権限を持っている場合は、パスワードを忘れたユーザを削除してから、[Admin] > [Users] > [Local Database] を選択して、別のユーザとしてログインし、新しいユーザを作成します。
- パスワードを忘れたユーザ以外に他のローカル ユーザが設定されていない場合は、NAM の **rmwebusers** CLI コマンドを使用します。次に、http または https をイネーブルにして、NAM ユーザ作成を要求します。

スイッチまたはルータに定義されている NAM ユーザ アカウントの変更

事前定義された root および guest NAM ユーザ アカウント（スイッチまたはルータの **session** コマンドまたは NAM CLI への Telnet ログインでアクセス可能）は、静的で NAM から独立しています。これらの静的アカウントは変更できません。また、他の CLI ベースのユーザを NAM に追加することもできません。

新しいユーザの作成

新しいユーザを作成するには、次の手順を実行します。

ステップ 1　[Administration] > [Users] > [Local Database] を選択します。

GUI にローカル データベースのユーザが表示されます。チェックマークは、一覧で示された機能に対して各ユーザが特権を持っていることを示しています。

ステップ 2　[**作成（Create）**] をクリックします。

GUI に、[New User] ダイアログボックスが表示されます。

ステップ 3　新しいユーザの作成に必要な情報を入力し、ユーザに付与する特権を選択します。ユーザの特権の説明については、表 6-6 を参照してください。表 6-5 に、「[New User] ダイアログボックス」のフィールドを示します。

表 6-5　[New User] ダイアログボックス

フィールド	説明	使用方法
Name	アカウント名	ユーザのアカウント名を入力します。
Password **Verify Password**	アカウント パスワード	ユーザのサイト セキュリティ ポリシーに準拠するパスワードを入力します。
Privileges	このアカウントに関連付ける特権	ユーザに付与する特権をすべて選択します。

（注）　ユーザのログイン中にユーザ アカウントを削除した場合、そのユーザはログインしたままで、その特権も保持されます。セッションは、そのユーザがログアウトするまで有効です。セッション中にアカウントを削除、または権限を変更した場合、影響があるのはその後のセッションだけです。ログインしているユーザを強制的にログアウトするには、NAM を再起動します。

ステップ 4　1 つまたは複数のチェックボックスをオンにして、ユーザの権限を設定します。表 6-6 では、各特権について説明します。

表 6-6　ユーザの権限

特権	アクセス レベル
AccountMgmt	ユーザによるユーザ アカウントの作成、削除、編集が可能です。
SystemConfig	ユーザによる、IP アドレス、ゲートウェイ、HTTP ポートなどの基本的な NAM システム パラメータの編集が可能です。
Capture	ユーザはパケット キャプチャを実行し、キャプチャ セッションを管理できるようになります NAM プロトコル デコードを使用します。
AlarmConfig	ユーザによる、スイッチまたはルータおよび NAM のアラームの作成、削除、編集が可能です。
MonitorConfig	ユーザによる次の作成、削除、編集が可能です。 • 収集とレポート • プロトコル ディレクトリ エントリ • プロトコル グループ • URL-Based アプリケーション
MonitorView	ユーザによる、モニタリング データとレポートの表示（すべてのユーザに権限あり）が可能です。

ステップ 5　ユーザを作成するには、[Submit] をクリックします。または、ダイアログに入力した文字をクリアするには、[Reset] をクリックします。

無効なユーザ名およびパスワード文字

ユーザ名に、次を使用しないでください。

- 感嘆符 !
- アットマーク @
- ポンド記号 #
- ドル記号 $
- 比率（%）
- キャロット ^
- アンパサンド &
- アスタリスク *
- 左または右のカッコ ( )
- より大きい <
- より小さい >
- カンマ ,
- ピリオド .
- 二重引用符 "
- 一重引用符 '

Web ユーザ パスワードの場合、次を使用しないでください。

- 二重引用符 "
- 一重引用符 '
- より大きい <
- より小さい >

ルートまたはゲスト ユーザ パスワードの場合、一重引用符のみ使用できません。

TACACS+ 認証および認可の確立

Terminal Access Controller Access Control System（TACACS）は、リモートアクセス認証、許可およびイベント ロギングなどの関連サービスを提供する認証プロトコルです。TACACS では、ユーザ パスワードおよび特権は個々のスイッチやルータではなく中央データベースで管理されるため、スケーラビリティが得られます。

TACACS+ は、認証および認可に追加サポートを提供するシスコの拡張です。

ユーザが NAM にログインすると、TACACS+ はユーザ名とパスワードが有効かどうかと、付与されているアクセス権限を確認します。

TACACS+ 認証および認可を確立するには、次の手順を実行します。

ステップ 1　[Administration] > [Users] > [TACACS+] を選択します。[TACACS+ Authentication and Authorization] ダイアログボックスが表示されます。

ステップ 2　「[TACACS+ Authentication and Authorization] ダイアログボックス」（表 6-7）に示されている適切な情報を入力または選択します。

表 6-7　[TACACS+ Authentication and Authorization] ダイアログボックス

フィールド	使用方法
Enable TACACS+ Authentication and Authorization	TACACS+ 認証および認可をイネーブルにするかどうかを決定します。 • イネーブルにするには、チェックボックスをオンにします。 • ディセーブルにするには、チェックボックスをオフにします。
Primary TACACS+ Server	プライマリ サーバの IP アドレスを入力します。
Backup TACACS+ Server	バックアップ サーバの IP アドレスを入力します（任意）。 **（注）** プライマリ サーバが 30 秒以内に応答しない場合は、バックアップ サーバに接続されます。
Secret Key	TACACS+ 秘密キーを入力します。
Verify Secret Key	TACACS+ 秘密キーを再入力します。

ステップ 3　次のどちらかを実行します。

- 変更を保存するには、[Submit] をクリックします。
- 取り消すには、[Reset] をクリックします。

ヒント　TACACS+ が設定された NAM にログインできない場合は、入力した TACACS+ サーバ名と秘密キーが正しいことを確認してください。

NAM 認証と認可をサポートする TACACS+ サーバの設定

[TACACS+] オプションをイネーブルにするだけでなく、NAM ユーザの認証および許可ができるように TACACS+ サーバを設定する必要があります。NAM は、ACS バージョン 5.2、5.1（パッチ 1 を含む）、および 4.2 をサポートします。

（注）　設定方法は、使用する TACACS+ サーバの種類によって異なります。

引き続き、次の特定のバージョン固有の項に進みます。

- Cisco ACS サーバ、バージョン 4.2 の設定
- Cisco ACS サーバ、バージョン 5.x の設定
- 汎用 TACACS+ サーバの設定

Cisco ACS サーバ、バージョン 4.2 の設定

バージョン 4.2 の Cisco ACS サーバを設定するには、2 つの作業を実行する必要があります。

- NAM のホスト名と IP アドレスを ACS サーバで設定します。「バージョン 4.2 向け Windows NT および 2000 システムの ACS への NAM の設定」（P.6-19）を参照してください。
- NAM ユーザまたはユーザ グループを追加するには、次の手順を実行します。「バージョン 4.2 向け NAM ユーザまたはユーザ グループの追加」（P.6-19）を参照してください。

バージョン 4.2 向け Windows NT および 2000 システムの ACS への NAM の設定

Cisco ACS TACACS+ サーバ（バージョン 4.2）を設定するには、次の手順を実行します。

ステップ 1　ACS サーバにログインします。

ステップ 2　[Network Configuration] をクリックします。

ステップ 3　[Add Entry] をクリックします。

ステップ 4　[Network Access Server] に、NAM ホスト名および IP アドレスを入力します。

ステップ 5　秘密キーを入力します。

（注）　秘密キーは、NAM で設定したものと同じにする必要があります。

ステップ 6　[Authenticate Using] フィールドで [TACACS+] を選択します。

ステップ 7　[Submit+Apply] をクリックします。

ステップ 8　引き続きバージョン 4.2 向け NAM ユーザまたはユーザ グループの追加に進み、次の設定作業を行います。

バージョン 4.2 向け NAM ユーザまたはユーザ グループの追加

NAM ユーザまたはユーザ グループを追加するには、次の手順を実行します。

ステップ 1　[User Setup] をクリックします。

ステップ 2　ユーザのログイン名を入力します。

ステップ 3　[Add/Edit] をクリックします。

ステップ 4　ユーザのデータを入力します。

ステップ 5　ユーザのパスワードを入力します。

ステップ 6　必要に応じて、ユーザ グループを割り当てます。

ステップ 7　[TACACS+ settings] で次を実行します。

a.　[Shell] を選択します。

b.　[IOS Command] を選択します。

c.　[Permit] を選択します。

d.　[Command] を選択します。

e.　**web** と入力します。

f.　[Arguments] フィールドに、次のように入力します。

```
permit capture
permit system
permit collection
```

```
permit account
permit alarm
permit view
```

ステップ 8　[Unlisted Arguments] で [Deny] を選択します。

ステップ 9　[Submit] をクリックします。`

Cisco ACS サーバ、バージョン 5.x の設定

バージョン 5.1（パッチ 1）または 5.2 Cisco ACS サーバを設定するには、次の作業を行う必要があります。ユーザまたはグループのポリシー ルールの設定をイネーブルにする追加の設定作業があります。

- NAM のホスト名と IP アドレスを ACS サーバで設定します。「バージョン 5.x 向け Windows NT および 2000 システムの ACS への NAM の設定」（P.6-20）を参照してください。
- NAM ユーザまたはユーザ グループを追加するには、次の手順を実行します。「バージョン 5.x 向け NAM ユーザまたはユーザ グループの追加」（P.6-20）を参照してください。
- ポリシー規則を設定します。「バージョン 5.x 向け ACS および NAM のアクセス ポリシーの設定」（P.6-21）を参照してください。

バージョン 5.x 向け Windows NT および 2000 システムの ACS への NAM の設定

Cisco ACS TACACS+ サーバ（バージョン 5.1(P1) または 5.2）を設定するには、次の手順を実行します。

ステップ 1　ACS サーバにログインします。

ステップ 2　NAM の任意のデバイス タイプを設定するには、[Network Resources] > [Network Device Groups] > [Device Type] をクリックし、デバイス タイプを作成します。たとえば、*NAM_Module* というデバイス タイムの名前を指定できます。

ステップ 3　[Network Resources] > [Network Devices and AAA Clients] をクリックし、NAM デバイスを追加します。

ステップ 4　[Network Access Server] に、NAM ホスト名および IP アドレスを入力します。

ステップ 5　[Authentication Options] フィールドで、[**TACACS+**] を選択します。

ステップ 6　秘密キーを入力します。

（注）　秘密キーは、NAM で設定したものと同じにする必要があります。

ステップ 7　[Submit] をクリックします。`

ステップ 8　引き続き「バージョン 5.x 向け NAM ユーザまたはユーザ グループの追加」（P.6-20）に進み、次の設定作業を行います。

バージョン 5.x 向け NAM ユーザまたはユーザ グループの追加

NAM ユーザまたはユーザ グループを追加するには、次の手順を実行します。

ステップ 1　[Users and Identity Stores] > [Internal Identity Stores] > [Users] をクリックします。

ステップ 2　[作成（Create）] をクリックします。

ステップ 3　ユーザのログイン名を入力します。

ステップ 4　ユーザのデータを入力します。

ステップ 5　必要に応じて、ユーザ グループを割り当てます。

ステップ 6　パスワード情報を入力します。

ステップ 7　[Submit] をクリックします。

バージョン 5.x 向け ACS および NAM のアクセス ポリシーの設定

バージョン 5.1（P1）、5.2、および 5.3 では、ACS および NAM の設定を行うにはアクセス ポリシーを設定する必要があります。

ステップ 1　ACS サーバで、[Policy Elements] > [Authorization and Permissions] > [Device Administration] > [Command Sets] をクリックし、[Create] をクリックして、Nam コマンド セットを作成します。

たとえば、NAM へフル アクセスする場合、*NAMfullAccess* というコマンド セットを作成し、チェックボックス [Permit any command that is not in the table below] をオンにします。

ステップ 2　NAM コマンド セットの入力を完了したら、[**Submit**] をクリックします。次のコマンドがすべて含まれていることを確認します。

```
permit capture
permit system
permit collection
permit account
permit alarm
permit view
```

ステップ 3　[Access Policies] > [Access Services] > [Create] をクリックして新しいサービス（たとえば、name = *namAdmin*; Service Type = Device Administration）を作成します。

ステップ 4　[Access Policies] > [Access Services] > [*namAdmin*] > [Authorization] > [Customize] に移動して、後の手順で必要なカスタマイズ条件を設定します。たとえば、次のように選択できます。NDG：デバイス タイプ、デバイスの IP アドレスなど）。*namAdmin* をこの手順で作成したサービスと置き換えます。

ステップ 5　[Access Policies] > [Access Services] > [*namAdmin*] > [Authorization] > [Customize] に移動して、すべてのログイン要求を許可する条件を設定します。NAM デバイスはこれらの条件を使用し、コマンド セット（ステップ 1 で作成）に従います。たとえば、条件は次のようになる場合があります。== NDG：Device Type は All Device Types：ステップ 2 で設定した NAM デバイス。

ステップ 6　[Access Policies] > [Service Selection] [Rules] をクリックして、サービスを選択します（たとえば、ステップ 3 で作成したサービス）。

ステップ 7　NAM にログインし、[NAM] > [Administration] > [Users] > [TACACS+] をクリックして ACS サーバの IP および秘密キーを設定します。

汎用 TACACS+ サーバの設定

汎用 TACACS+ サーバを設定するには、次の手順を実行します。

ステップ 1　リモート アクセス サーバとして NAM IP アドレスを指定します。

ステップ 2　NAM と通信する TACACS+ サーバの秘密キーを設定します。

（注）　秘密キーは、NAM で設定したものと同じにする必要があります。

ステップ 3　NAM へのアクセスを許可するユーザまたはグループごとに、次の TACACS+ パラメータを設定します。

パラメータ	入力
service	`shell`
cmd	`web`

cmd-arg	次のうちの 1 つまたは複数を入力します。
	`accountmgmt`
	`system`
	`capture`
	`alarm`
	`collection`
	`view`

password authentication method : Password Authentication Protocol（PAP）	`pap`

Current User Sessions

Current User Sessions テーブルは、アプリケーションにログインしているユーザのレコードです。ユーザ セッションは非アクティブになってから 30 分後にタイムアウトします。ユーザ セッションがタイムアウトすると、その行はテーブルから削除されます。

Current User Sessions テーブルを表示するには、次の手順を実行します。

ステップ 1　[Administration] > [Users] > [Current Users] を選択します。

「Current User Sessions テーブル」（表 6-8）が表示されます。

表 6-8　Current User Sessions テーブル

フィールド	説明
User ID	NAM へのログインに使用されたユーザ ID
From	ユーザがログインした接続元のマシン名
Login Time	ユーザがログインした時刻
Last Activity	最後のユーザ アクティビティのタイム スタンプ