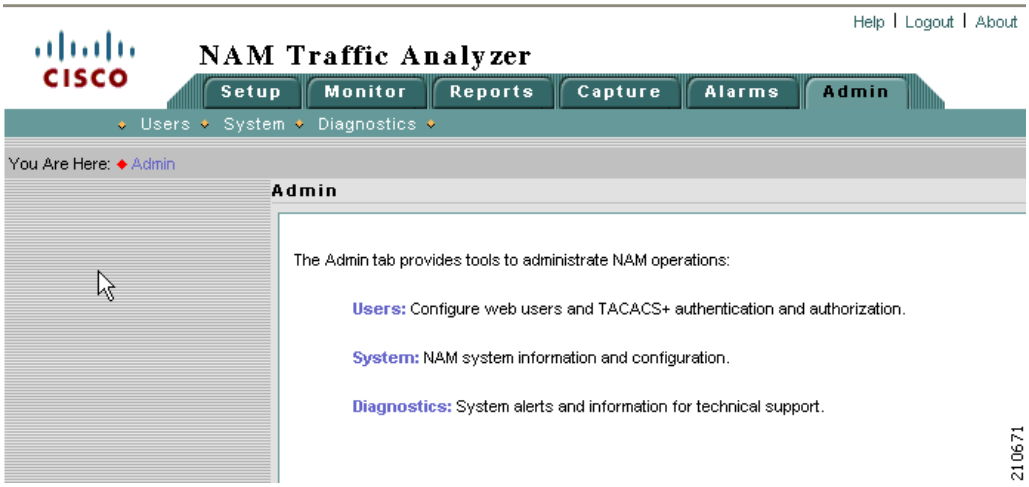
CHAPTER 2

ユーザおよびシステム管理

この章では、ユーザおよびシステム管理タスクの実行と、技術サポートを得るために必要な診断情報の生成について説明します。トップ レベルの [Admin] ウィンドウは、Cisco NAM VB GUI の [Admin] タブをクリックすると表示されます。図 2-1 は、トップレベルの [Admin] ウィンドウを示しています。

図 2-1　　トップレベルの [Admin] ウィンドウ



この章には次の項があります。

- 「ユーザ管理」（P.2-2）では、ユーザ認証および認可のために、ローカル データベースを設定する方法、または、TACACS+ データベースの情報を提供する方法を説明します。この項では、現在のユーザ セッションのウィンドウについても説明します。
- 「システム管理」（P.2-9）では、システム管理タスクおよび NAM の管理を行うメニュー オプションを説明します。
- 「診断」（P.2-18）では、問題の診断およびトラブルシューティングに役立つメニュー オプションを説明します。
- 「WAAS の NAM デフォルト パスワードのリセット」（P.2-23）では、NAM VB ルート パスワードをデフォルト値にリセットする方法を説明します。

ユーザ管理

NAM Traffic Analyzer をインストールするとき、NAM Command-Line Interface（CLI; コマンドライン インターフェイス）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。これは、RMON 収集の設定、システム パラメータの設定、RMON データの表示など、各ユーザが実行できるタスクに対応する特権を割り当てることで行います。

表 2-1 に、「ユーザの特権」と各特権の説明を示します。

表 2-1　ユーザの特権

特権	アクセス レベル
Account Mgmt	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。
System Config	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。
Alarm Config	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。
Collection Config	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
Collection View	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。

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.2-3）および「ユーザの編集」（P.2-4）を参照してください。

パスワードの回復

NAM Traffic Analyzer 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] タブをクリックし、[Users] をクリックして、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 Traffic Analyzer ユーザ作成を要求します。

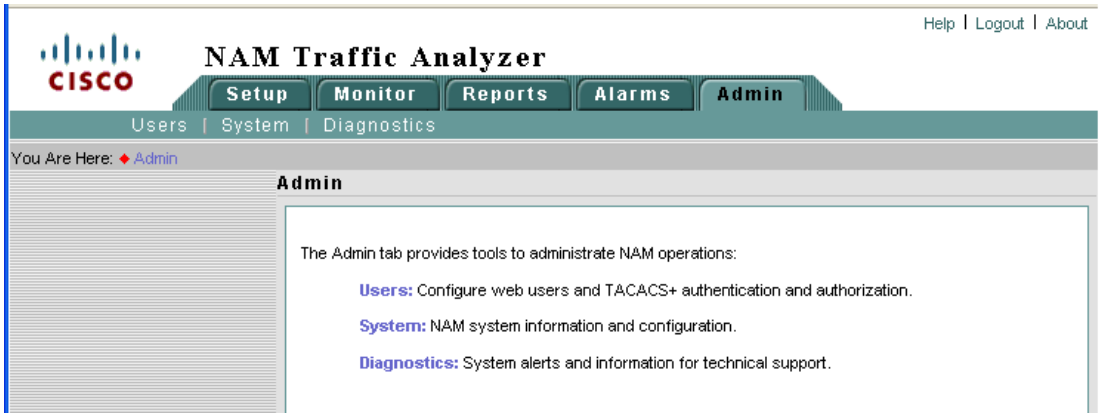
スイッチまたはルータに定義されている NAM ユーザ アカウントの変更

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 Traffic Analyzer 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 Traffic Analyzer に追加することもできません。

User Administration GUI

User Administration GUI を使用してユーザを管理できます。図 2-2 は、トップレベルの [User Admin GUI] ウィンドウを示しています。

図 2-2　User Admin GUI



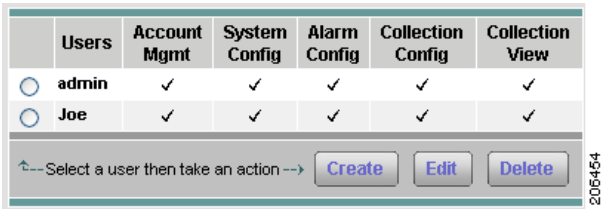
新しいユーザの作成

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　[Admin] > [Users] を選択します。

図 2-3 に示すとおり、GUI にローカル データベース内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。

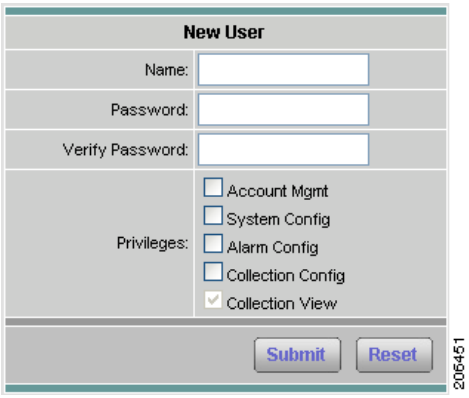
図 2-3　Users テーブル



ステップ 2　[Create] をクリックします。

GUI に、[New User] ダイアログボックス（図 2-4）が表示されます。

図 2-4　[New User] ダイアログボックス



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 2-1 を参照してください。表 2-2 に、「[New User] ダイアログボックス」のフィールドを示します。

表 2-2　[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。

ユーザ名およびパスワードは、32 文字以下の英数字で、次を除く特殊文字を含めることができます。

- 大なり記号（<）
- 小なり記号（>）
- カンマ（,）
- ピリオド（.）
- 二重引用符（"）
- 一重引用符（'）

ステップ 4　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。

ユーザの編集

ユーザの設定を編集するには、次の手順を実行します。

ステップ 1　[Admin] > [Users] を選択します。

Users テーブルが表示されます。

ステップ 2　ユーザ名を選択します。

ステップ 3　[Edit] をクリックします。

ステップ 4　[Modify Users] ダイアログボックスで、必要な情報を変更します。各フィールドの説明については、[New User] ダイアログボックス（図 2-4）を参照してください。

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し、以前の設定に戻すには、[Reset] をクリックします。

ユーザの削除

ユーザを削除するには、次の手順を実行します。

ステップ 1　[Admin] > [Users] を選択します。

Users テーブルが表示されます。

ステップ 2　ユーザ名を選択します。

ステップ 3　[Delete] をクリックします。

（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。

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、認可およびイベント 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システムズの拡張です。

ユーザが NAM Traffic Analyzer 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を判別し、付与されているアクセス権限を判別します。

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　[Admin] > [Users] を選択します。

ステップ 2　コンテンツ メニューで [TACACS+] をクリックします。

[TACACS+ Authentication and Authorization] ダイアログボックス（図 2-5）が表示されます。

図 2-5　[TACACS+ Authentication and Authorization] ダイアログボックス

ステップ 3　「[TACACS+ Authentication and Authorization] ダイアログボックス」（表 2-3）に示されている適切な情報を入力または選択します。

表 2-3　[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（オプション）。 **（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+ パスワードを入力します。
[Verify Secret Key]	TACACS+ パスワードを再入力します。

ステップ 4　次のいずれかを実行します。

- 変更内容を保存するには、[Apply] 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+ の設定された NAM Traffic Analyzer 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。詳細については、「ユーザ名およびパスワードの問題」（P.A-2）を参照してください。

NAM 認証と認可をサポートする TACACS+ サーバの設定

[Admin] タブから TACACS+ オプションをイネーブルにするだけでなく、NAM Traffic Analyzer ユーザの認証および認可ができるように TACACS+ サーバを設定する必要があります。

（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。

Cisco ACS TACACS+ サーバの設定

Windows NT および 2000 システムの場合

Cisco ACS 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　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] または [Restart] をクリックします。

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] または [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　[User Setup] を選択します。

ステップ 6　ユーザのパスワードを入力します。

ステップ 7　必要に応じて、ユーザ グループを割り当てます。

ステップ 8　[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 9　[Unlisted Arguments] で [Deny] を選択します。

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; パスワード認証プロトコル）	`pap`

Current User Sessions テーブルの表示

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　[Admin] > [Users] を選択します。

ステップ 2　コンテンツで [Current Users] をクリックします。

「Current User Sessions テーブル」（表 2-4）が表示されます。

表 2-4　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

システム管理

[Admin] タブの [System] オプションでは、次の機能にアクセスできます。

- 「システム リソース」（P.2-10）
- 「ネットワーク パラメータの設定と表示」（P.2-10）
- 「NAM SNMP システム グループの設定と表示」（P.2-11）
- 「NAM のシステム時刻」（P.2-14）
- 「E メールの設定」（P.2-15）
- 「FTP の設定」（P.2-16）
- 「Web パブリケーション」（P.2-16）
- 「応答時間のエクスポート」（P.2-18）

システム リソース

[Admin] > [System] を選択し、[System Overview] ウィンドウ（図 2-6）を表示します。

図 2-6　[System Overview] ウィンドウ

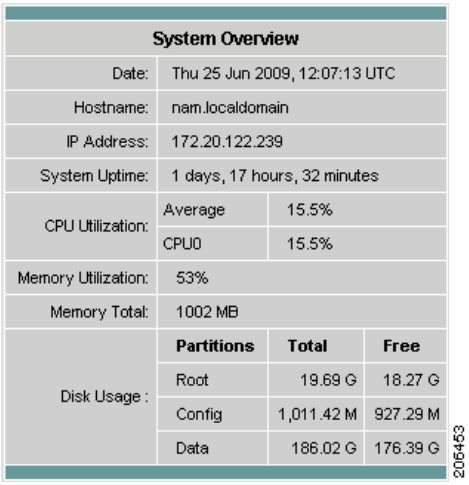


表 2-5 に、[System Overview] ウィンドウのフィールドを示します。

表 2-5　System Overview

フィールド	説明
[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）
[Hostname]	NAM のホスト名
[IP Address]	NAM の IP アドレス
[System Uptime]	ホストが中断なしで稼動する時間の長さ
[CPU Utilization]	NAM によって消費される CPU リソースの比率
[Memory Utilization]	NAM によって消費されるメモリ リソースの比率
[Disk Usage]	ディスク パーティションと、それぞれの総容量および空き容量を表示

ネットワーク パラメータの設定と表示

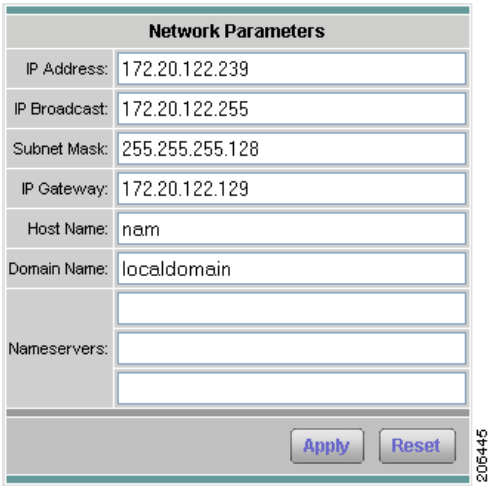
ネットワーク パラメータを表示および設定するには、次の手順を実行します。

ステップ 1　[Admin] > [System] を選択します。

ステップ 2　コンテンツで、[Network Parameters] をクリックします。

[Network Parameters] ダイアログボックス（図 2-7）が表示されます。

図 2-7　[Network Parameters] ダイアログボックス



ステップ 3　「[Network Parameters] ダイアログボックス」（表 2-6）で、情報を入力または変更します。

（注）　NAM 4.2 は、ネットワーク パラメータの IP アドレスでの IPv6 の使用をサポートしません。

表 2-6　[Network Parameters] ダイアログボックス

フィールド	説明
[IP Address]	NAM の IP アドレス
[IP Broadcast]	NAM のブロードキャスト アドレス
[Subnet Mask]	NAM のサブネット マスク
[IP Gateway]	NAM IP ゲートウェイ アドレス
[Host Name]	NAM のホスト名
[Domain name]	NAM のドメイン名
[Nameservers]	NAM のネームサーバ アドレス（複数可）

ステップ 4　次のいずれかを実行します。

- 変更内容を保存するには、[Apply] 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 SNMP システム グループの設定と表示

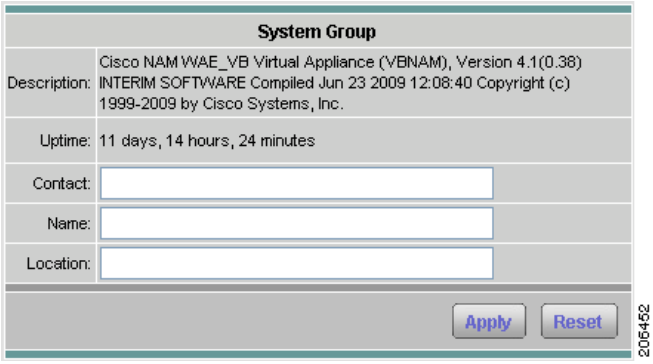
NAM SNMP システム グループを表示および設定するには、次の手順を実行します。

ステップ 1　[Admin] > [System] を選択します。

ステップ 2　コンテンツで、[NAM SNMP] をクリックします。

ウィンドウの上部に、[SNMP System Group] ダイアログボックス（図 2-8）および [NAM Community Strings] ダイアログボックス（図 2-9）が表示されます。

図 2-8　[SNMP System Group] ダイアログボックス



ステップ 3　「[System SNMP] ダイアログボックス」（表 2-7）で、情報を入力または変更します。

表 2-7　[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]	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 4　次のいずれかを実行します。

- 変更内容を保存するには、[Apply] 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

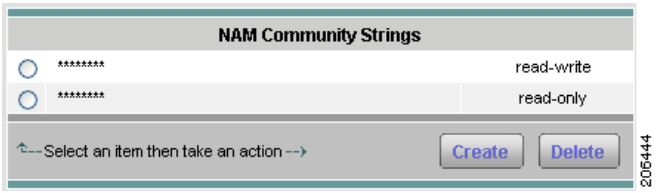
NAM コミュニティ ストリングを作成するには、次の手順を実行します。

ステップ 1　[Admin] > [System] を選択します。

ステップ 2　コンテンツで、[NAM SNMP] をクリックします。

ウィンドウの下部に、[NAM Community Strings] ダイアログボックス（図 2-9）が表示されます。

図 2-9　[NAM Community Strings] ダイアログボックス



ステップ 3　[Create] をクリックします。

[Create Community String] ダイアログボックス（図 2-10）が表示されます。

図 2-10　[Create Community String] ダイアログボックス

ステップ 4　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 5　[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 6　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 7　次のいずれかを実行します。

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

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　[Admin] > [System] を選択します。

ステップ 2　コンテンツで、[NAM SNMP] をクリックします。

ウィンドウの下部に、[NAM Community Strings] ダイアログボックス（図 2-9）が表示されます。

ステップ 3　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。

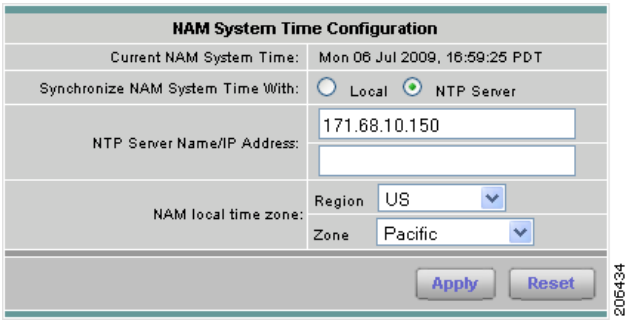
コミュニティ ストリングが削除されます。

NAM のシステム時刻

NAM VB CLI **clock set** コマンドを使用、または 1 つ以上の外部 NTP サーバを使用して、NAM システム時刻をローカルに設定できます。1 つの NTP サーバを使用する場合、割り当てられた IP アドレスまたは FQDN 名を入力します。

NAM VB は、NTP サーバから UTC (GMT) を取得します。NAM システム時刻の設定後に、[NAM System Time Configuration] 画面を使用してローカル時間帯を設定できます。図 2-11 に、「[NAM System Time Configuration] 画面」を示します。

図 2-11　[NAM System Time Configuration] 画面



NAM システム時刻のローカルな同期

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

ステップ 1　NAM VB 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　NAM GUI で、[Admin] > [System] をクリックします。

ステップ 4　[Content] メニューで、[NAM System Time] をクリックします。

ステップ 5　[Local] オプション ボタンをクリックします。

ステップ 6　リストから地域とローカル時間帯を選択します。

ステップ 7　次のいずれかを実行します。

- 変更内容を保存するには、[Apply] 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。

NTP サーバによる NAM のシステム時刻の同期

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　[NTP Server] オプション ボタンを選択します。

ステップ 2　2 つまでの 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 3　リストから地域とローカル時間帯を選択します。

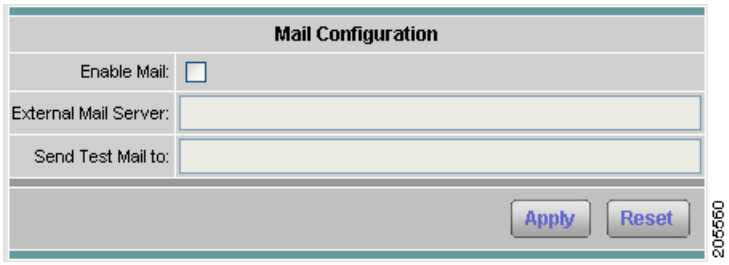
ステップ 4　次のいずれかを実行します。

- 変更内容を保存するには、[Apply] 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。

E メールの設定

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 NAM を設定できます。図 2-12 に、「[Mail Configuration] ウィンドウ」を示します。レポートの E メール送信を設定する方法の詳細については、「エクスポートのスケジュール設定」（P.5-22）の項の表 5-14、「[Scheduled Exports] ウィンドウのオプション」を参照してください。

図 2-12　[Mail Configuration] ウィンドウ



通知を E メールで送信するように NAM を設定する手順は、次のとおりです。

ステップ 1　[Admin] > [System] を選択します。

ステップ 2　[E-Mail Configuration] をクリックします。

[Mail Configuration] ウィンドウ（図 2-12）が表示されます。表 2-8 に「Mail Configuration オプション」を示します。

表 2-8　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]	最大 3 つまで、E メール受信者の E メール アドレスを一覧表示します。

ステップ 3　[Enable EMail] をオンにします。

ステップ 4　[External Mail Server] に外部メール サーバの識別名を入力します。

ステップ 5　変更を保存するには、[Apply] 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。

FTP の設定

アラーム通知やレポートを FTP で送信するように NAM を設定できます。図 2-13 に、「[FTP Configuration] ウィンドウ」を示します。FTP を使用したレポートの転送を設定する方法の詳細については、「エクスポートのスケジュール設定」（P.5-22）の項の表 5-14、「[Scheduled Exports] ウィンドウのオプション」を参照してください。

図 2-13　[FTP Configuration] ウィンドウ

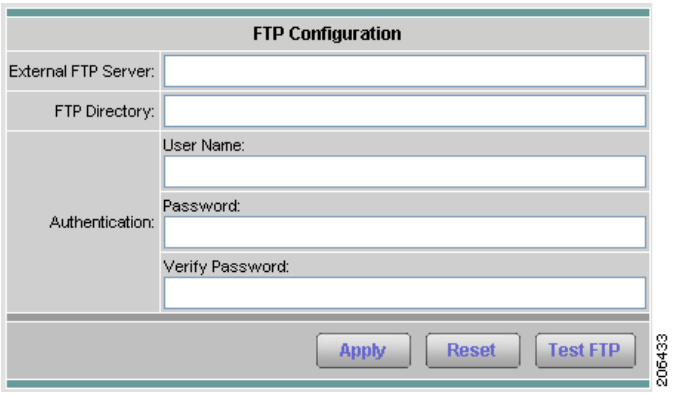


表 2-9 に、FTP の設定に使用するフィールドを示します。

表 2-9　FTP Configuration オプション

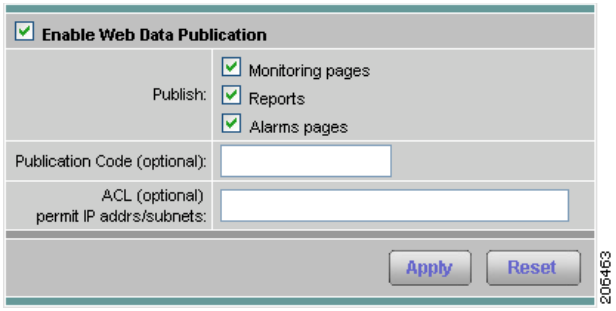
フィールド	説明
[External FTP Server]	FTP サーバのホスト名または IP アドレス
[FTP Directory]	FTP ファイルが格納されるディレクトリのフル パス名
[Authentication]	外部 FTP サーバの認証に使用されるユーザ名フィールドとパスワード フィールド

Web パブリケーション

Web 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 パブリケーションは、オープンにすることもできれば、Access Control List（ACL; アクセス コントロール リスト）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。図 2-14 に、「[Web Data Publication] ウィンドウ」を示します。

図 2-14　[Web Data Publication] ウィンドウ



Web 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　[Admin] > [System] を選択します。

ステップ 2　[System] メニューで、[Web Publishing] をクリックします。

ステップ 3　Web パブリッシングで使用可能にする各項目をオンにします。

表 2-10、「Web Data Publication プロパティ」に、[Enable Web Publishing] ウィンドウのフィールドを示します。

表 2-10　Web Data Publication プロパティ

フィールド	説明
[Monitoring pages except Voice]	オンにすると、[Voice Monitor] 画面を除くすべての Monitor 画面を公開します。
[Reports]	オンにするとすべてのレポートを公開します。
[Alarms pages]	オンにすると、[NAM and Switch Alarms] ページを公開します。
[Publication Code]	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 URL にある公開された [Monitor] > [PortStat] ウィンドウにアクセスできます。 http://<nam-hostname>/monitor/sup/ether/supetherstats.php?sortCol=utilization&publicationcode=abc123
[ACL permit IP addrs/subnets]	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。 IP アドレスまたはサブネットを入力すると、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。

ステップ 4　Web パブリッシングをイネーブルにするには、[Apply] 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。

応答時間のエクスポート

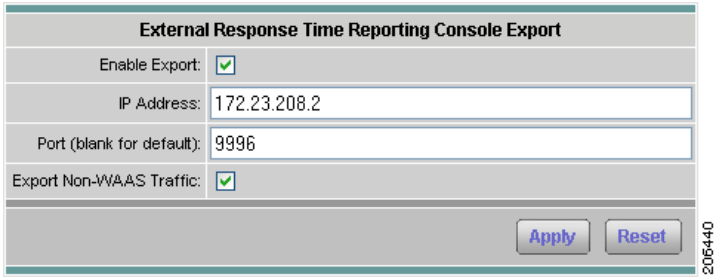
NetQoS SuperAgent などの外部レポート コンソールへの応答時間データのエクスポートをイネーブルにできます。このウィンドウは、[Setup] > [Data Sources] > [WAAS--Devices] > [Add/Config] ウィンドウと連携して動作します。[Response Time Export] をイネーブルにすると、[Export Passthru to External Console] オプションが、[Add/Config WAAS Device] ウィンドウに表示されます。

外部コンソールへの NAM による応答時間データのエクスポート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　NAM GUI で、[Admin] > [System] > [Response Time Export] をクリックします。

[Export] ウィンドウ（図 2-15）が表示されます。

図 2-15　外部応答時間のレポート コンソールへのエクスポート



ステップ 2　[IP Address] フィールドに外部レポートコンソールの IP アドレスを入力します。

ステップ 3　外部コンソールの UDP ポート番号を入力します。

NetQoS SA の以前のバージョンはポート 9995 をサポートします。最新バージョンはポート 9996 をサポートします。どのポートを使用すべきかは、SA のマニュアルを参照してください。

ステップ 4　[Export] をクリックして、NAM によるデータのエクスポートをイネーブルにします。

ステップ 5　オプションで、[Export Non-WAAS Traffic] をクリックします。

これによって、WAAS トラフィックのエクスポートがイネーブルになります。

ステップ 6　[Apply] をクリックして、トラフィックのエクスポートをイネーブルにします。

診断

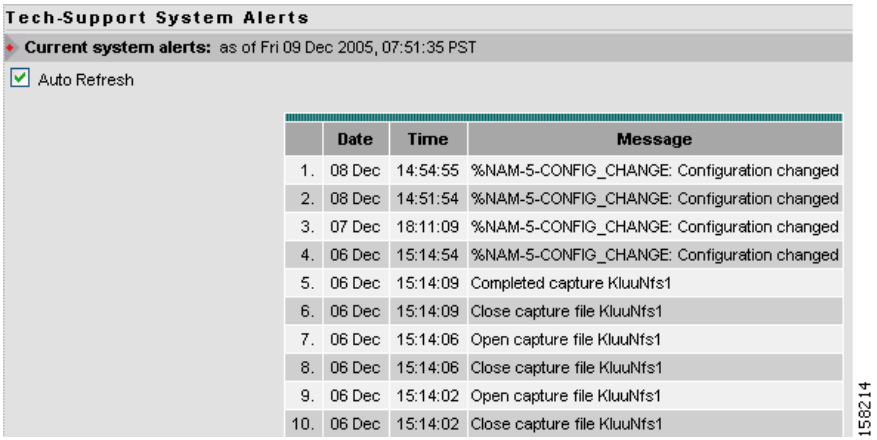
[Admin] タブの [Diagnostics] オプションには、トラブルシューティングを支援するツールがあります。Cisco Technical Assistance Center（TAC）からのサポートが必要な問題が発生したときに、これらのツールを使用できます。次のオプションがあります。オプションは次のとおりです。

- 「システム アラートの表示」（P.2-19）
- 「監査証跡の表示」（P.2-19）
- 「設定情報のモニタリング」（P.2-20）
- 「テクニカル サポートの表示」（P.2-21）

システム アラートの表示

通常の運用中に NAM Traffic Analyzer 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] を選択します。[System Alerts] はデフォルト ウィンドウです。図 2-16 に、「[System Alerts] ウィンドウ」を示します。

図 2-16　[System Alerts] ウィンドウ



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。

監査証跡の表示

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
- NDE 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
- レポートの作成および削除
- 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
- タイムスタンプ
- 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。

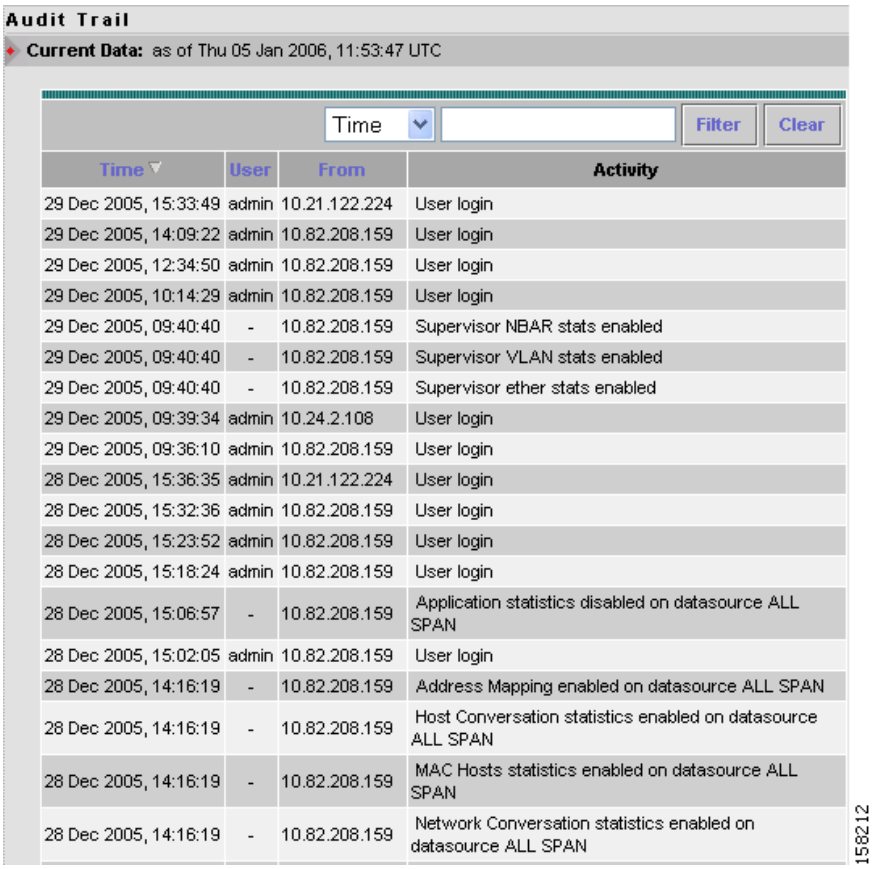
ステップ 1　[Admin] > [Diagnostics] を選択します。

ステップ 2　[Audit Trail] をクリックします。

[Audit Trail] ウィンドウ（図 2-17）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。

図 2-17　[Audit Trail] ウィンドウ



設定情報のモニタリング

[Monitor Configuration] ウィンドウには、NAM Traffic Analyzer およびその他の管理アプリケーションによって設定された NAM データ収集に関する情報が含まれています。[Monitoring Configuration Information] ウィンドウを表示するには、次の手順を実行します。

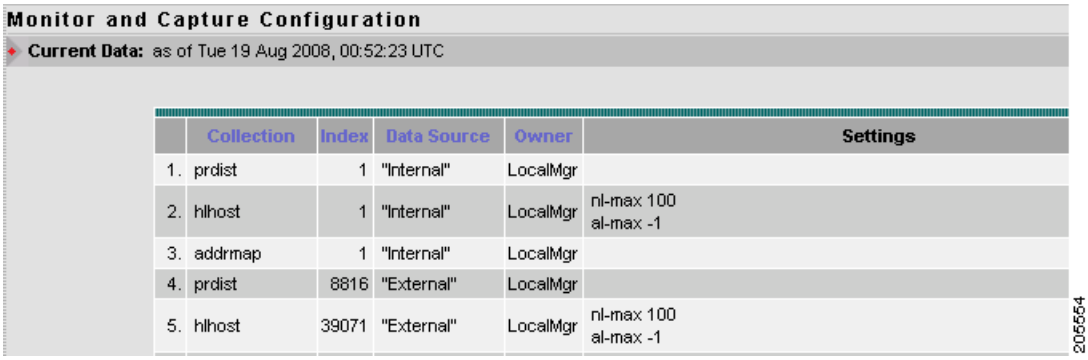
ステップ 1　[Admin] > [Diagnostics] を選択します。

ステップ 2　コンテンツ メニューで [Monitor Configuration] をクリックします。

NAM によって、[Monitor and Capture Configuration] ウィンドウ（図 2-18）が表示されます。ウィンドウの各行は、NAM 収集、キャプチャ、フィルタ、データ ソース、およびアラームに関する内部設定文を示しています。ご利用の設定には、次のような数十の文があります。

（注）　通常、この情報はユーザにはあまり意味がありませんが、Cisco TAC に相談する場合や、テクニカル サポートが必要な場合に役立ちます。

図 2-18　[Monitor and Capture Configuration] ウィンドウ



ステップ 3　情報を保存するには、ブラウザ メニューで [File] > [Save As...] を選択します。

ステップ 4　出力先、ファイル名、形式を選択して、[Save] をクリックします。

[Owner] カラムに名前 LocalMgr が表示される場合は、NAM Traffic Analyzer によって収集が設定されています。

テクニカル サポートの表示

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。

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、[Admin] > [Users] 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、「ユーザの編集」（P.2-4）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。
http://www.cisco.com/en/US/docs/net_mgmt/network_analysis_module_software/4.2/command/reference/guide/cmdref.html

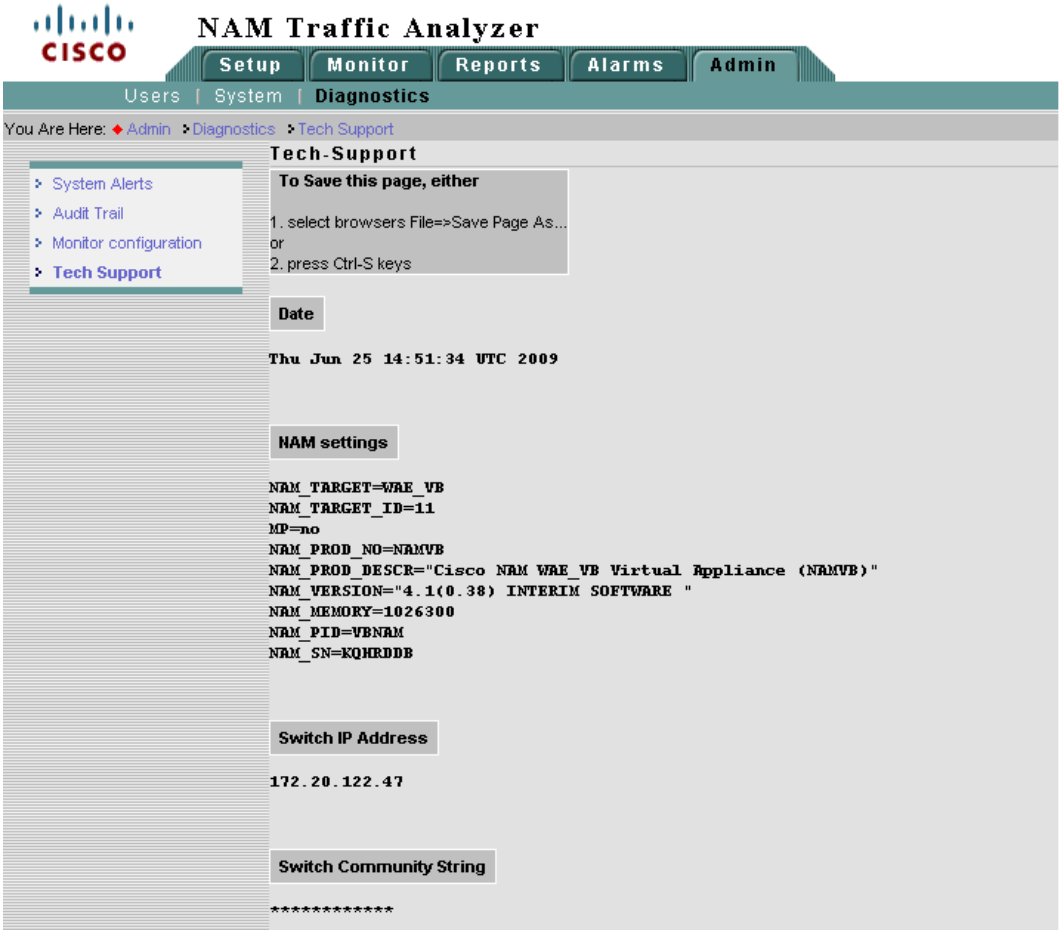
テクニカル サポートを表示するには、次の手順を実行します。

ステップ 1　[Admin] > [Diagnostics] を選択します。

ステップ 2　コンテンツ メニューで [Tech Support] をクリックします。

数分後、大量の診断情報が生成され、[Diagnostics Tech Support] ウィンドウ（図 2-19）に表示されます。

図 2-19　[Diagnostics Tech Support] ウィンドウ



ステップ 3　情報を保存するには、ブラウザ メニューで [File] > [Save As...] を選択します。

Internet Explorer を使用している場合は、ページ上部にある [Save This Page] ボタンをクリックすると、[Tech-Support] ページをテキスト ファイルとしてダウンロードできます。

ステップ 4　出力先、ファイル名、ファイル形式を選択して、[Save] をクリックします。

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ます。

WAAS の NAM デフォルト パスワードのリセット

ここでは、WAAS の NAM VB をデフォルト パスワードにリセットする方法を説明します。

ステップ 1　デバイス CLI で NAM VB をシャットダウンします。

virtual-blade 1 shutdown

ステップ 2　NAM VB ヘルパーにブートするように設定を変更します。

conf t
virtual-blade 1
boot from cd-rom
exit

ステップ 3　ヘルパーに NAM VB をブートします。

virtual-blade 1 start

ステップ 4　NAM VB へのセッションを確立し、NAM VB パスワードをリセットします。

virtual-blade 1 session

ステップ 5　**5** を入力して、アプリケーション イメージ CLI パスワードをデフォルト値にリセットします。

ステップ 6　**h** を入力して NAM VB をシャットダウンします。

これによって、ユーザ **root** の NAM CLI パスワードが *root* にリセットされます。

ステップ 7　NAM イメージにブートするように設定を変更します。

conf t
virtual-blade 1
boot from disk

ステップ 8　NAM イメージにブートします。

virtual-blade 1 start

root ID で NAM CLI にログインするには、パスワードとして root を使用します。

Nexus 1010 Virtual Services Appliance での NAM デフォルト パスワードのリセット

Nexus 1010 Virtual Services Appliance の NAM VB をデフォルトのパスワードにリセットする方法を説明します。

ステップ 1　NAM CLI で次のコマンドを実行します。

reboot -helper

ステップ 2　リブートをするかどうかの Y または N の確認を求められます。[Y] をクリックすると、NAM がヘルパー イメージにブートされ、メニューが表示されます。

```
=======================================================
Cisco Systems, Inc.
Network Analysis Module (NAM) helper utility
Version 4.2(1)

-----
Main menu
1 - Download application image and write to HDD
2 - Download application image and reformat HDD
3 - Install application image from CD
4 - Display software versions
5 - Reset application image CLI passwords to default
6 - Change file transfer method (currently ftp/http)
7 - Send Ping
n - Configure network
r - Exit and reset Services Engine
h - Exit and shutdown Services Engine Selection [1234567nh]:
```

ステップ 3　ヘルパー メニューで、5 の「Reset application image CLI passwords to default」を選択します。

ステップ 4　クリックして NAM をリセットします。

ステップ 5　NAM がもう一度ブートされた後、ルートとしてロブインする場合はデフォルト パスワードをリセットする必要があります。