

DAY ONE : JUNOSの基本設定

Junosを初めて導入する（Day One）場合に何をすればよいか。

Junosを設定し、作業に取りかけられるように解説しています。

このDay Oneブックレットを使用すれば、数時間でルーター、スイッチ、およびセキュリティデバイスの基本システムの設定が可能です。

Junos[®] 基本シリーズ

Day One : Junos の基本設定

著者：イアン・ジャレット、ショーン・クラーク

第1章：チェックリストの作成5

第2章：システムの基本設定 11

第3章：ユーザーの設定27

第4章：SNMP の設定 35

第5章：モニタリングおよびログ収集の使用... 45

第6章：設定テンプレートおよび
その他のショートカットを使用した作業61

本書の PDF 版を www.juniper.net/dayone から入手できます。

付録：Day One ワークシート、設定、
およびその他77

© 2009 by Juniper Networks, Inc. All rights reserved. Juniper Networks、Juniper Networks の ロゴ、Junos、NetScreen、ScreenOS は、Juniper Networks, Inc. (以下、ジュニパーネットワークス) の米国およびその他の国における登録商標です。Junose は、ジュニパーネットワークスの商標です。その他の商標、サービスマーク、登録商標、登録サービスマークは、それぞれの所有者に帰属します。

ジュニパーネットワークスは、本書に誤りが含まれることがあっても責任を負いません。ジュニパーネットワークスは予告なく本書を変更、修正、転載、別の形態に改訂する権利を留保します。ジュニパーネットワークスが製造、販売する製品、あるいはその部品は、ジュニパーネットワークスが保有する、あるいはライセンスを受けた以下の米国特許のうち1件または複数により保護されている場合があります。米国特許第 5,473,599 号、第 5,905,725 号、第 5,909,440 号、第 6,192,051 号、第 6,333,650 号、第 6,359,479 号、第 6,406,312 号、第 6,429,706 号、第 6,459,579 号、第 6,493,347 号、第 6,538,518 号、第 6,538,899 号、第 6,552,918 号、第 6,567,902 号、第 6,578,186 号、第 6,590,785。

Day One シリーズ編集者：キャシー・ガデッキ
著者：イアン・ジャレット、ショーン・クラーク
編集：ナンシー・ケルベル
出版管理：Ames & Eames, Inc.
印刷：Vervante Corporation (米国)

改訂：第3版、2009年11月
45678910

著者の紹介

イアン・ジャレットは、ジュニパーネットワークスの製品シニアマネージャで、Junos の責任者です。Junos の担当者として11年以上の経験があり、その幅広い知識を多くの方と共有できることを望んでいます。

ショーン・クラークは、ジュニパーネットワークスのシニア・システム・エンジニアで、Junos については9年以上のエンジニアリング経験があります。

著者の謝辞

本書の制作にご協力いただいた多くの方々に感謝を申し上げます。このプロジェクトの

出版管理マネージャであるパトリック・エイムズ氏には全体的なガイド役として、ナンシー・ケルベル氏には原稿の編集者としてお世話になりました。Day One シリーズの編集者キャシー・ガデッキには、何度も助けられ、多くの期間にわたりご尽力をいただきました。マイケル・スクラッグス氏とマリリン・カー氏には、読み手に分かりやすい文章となるよう修正を加えていただきました。デビッド・グエン氏、ジェリッシュ・パラプラス氏、ジェニファー・パルシファー氏、ブラッド・ウッドバーグ氏には、我々の質問にご回答いただき、各セクションの技術レビューをお願いしました。イアン・ジャレットは、本書の出版の実現にご尽力いただいたジュニパーネットワークスの関係者すべてにお礼を申し上げます。ショーン・クラークは、専門用語を避けて分かりやすい表現で本書を記述した制作チームにお礼を申し上げるとともに、マリアンへの支援にも感謝します。

本書の PDF 版は、無料で www.juniper.net/dayone から入手できます。

Day One へようこそ

Day One ブックレットは、新しいテーマにすぐに取りかかれるように、作業の初日に必要となる情報だけをまとめたものです。Day One シリーズでは、分かりやすく、ステップごとに手順を説明し、そのまま使えるような詳しい例を数多く掲載しています。また、さらに詳しい解説が記載された資料についても提示しています。

Day One ブックレットの目的

本書は、ジュニパー製の機器を短時間で、効果的に使いこなせるようにするものです。さまざまな技術資料のすべてに目を通している時間的な余裕はありません。どこから着手すれば良いのかも分からないことがあります。知りたいのは、初日に何をすべきかということでしょう。

Day One ブックレットでは、ジュニパーの専門家によって、デバイスの操作方法だけでなく、ショートカットの場所、問題の回避方法、さらにベストプラクティスなどが示されています。

本書で得られる情報

本書は、お使いのデバイスの基本的な設定方法や設定モードに関する詳細を理解することを支援するためのものです。これらの基本設定は、ルーター、スイッチ、セキュリティ・プラットフォームのどの Junos デバイスでも、セットアップの第一歩となります。

本書を読むことで、以下の事柄が行えるようになります。

- ✓ システムの基本設定の便利なチェックリストを作成する
- ✓ システムの基本設定を行う
- ✓ ログインアカウントおよびパーミッションを作成する
- ✓ 既存のシステムで使用できるように SNMP を設定する
- ✓ リモートからデバイスを監視し、システムログを設定する
- ✓ Web ベース管理機能をインストールする
- ✓ 設定ショートカットを使用して素早く変更を行う
- ✓ 設定グループやテンプレートを使用してデバイスのセットアップを合理化する
- ✓ 設定結果をブックレットの設定例と比較する

実際にデバイスで試す前に

本書を読むときには、実際にJunosデバイスにアクセスして、記載例の手順を実行したりコマンドを入力したりすることで、内容をより理解できるようにします。本書の電子版の付録には、参考設定が掲載されています。自身のデバイスで、左マージンの矢印 ▶ で示された設定コマンドすべて(ただし、それらのコマンドのみ)を入力すると、付録に記載された参考設定と同じ結果が得られます。例:

```
▶ root@juniper1# set class super-user
```

Junosオペレーティング・システムにアクセスするには、まずデバイス自体にアクセスできなければなりません。これは、コンソールポートまたは管理ポートから行います。各ネットワークは異なるため、配備済みの機器にログインする手順を逐一説明することは、本書が目的とする範囲を超えます。そのため、Junosコマンドライン・インタフェースにログインする前に、ネットワーク上の対象デバイスへのアクセス方法を把握しておくか、または物理的にアクセスできる手段を確保しておいてください。

さらに詳しくは デバイスの配備に関する情報については、該当する製品の『*Quick Start*』ガイドを参照してください(www.juniper.net/techpubs/から入手可能)。

デバイスへの入力

Day Oneブックレットは、実際の操作に焦点を当て、多数の例を掲載しています。掲載されている例は 等幅 フォントで画面に出力され、入力するコマンドは 太字 で示されています。コマンドに、ユーザーが名前を付けた項目の入力(ファイル名、グループ名、またはポリシー名)が含まれる場合、それらは例では 太字イタリック で示されています。本書では、入力の種類を区別するために、例や説明文でこれらの表記を使用します。ただし、CLI(Command-Line Interface)にコマンドを入力するときには、プレーンテキスト形式で入力します。

本書を読む前に知っておくべきこと

本書を読む前に、基本的なネットワーク概念や、『Junos基本シリーズ』の最初のブックレットに記載されたトピックスについて理解しておく必要があります。『*Day One: Junos CLIの探究*』では、Junosデバイスを設定および操作するための基本的なコマンドを紹介しています。これらは、付録(電子版)の表にまとめてあります。

第1章

チェックリストの作成

| | |
|-------------------------------|----|
| ホスト名..... | 6 |
| ループバック・インタフェース..... | 6 |
| 管理インタフェース..... | 7 |
| バックアップルーター..... | 7 |
| DNS (Domain Name System)..... | 7 |
| 時刻サーバー..... | 8 |
| ユーザー名およびパスワード..... | 8 |
| リモート認証サーバー..... | 9 |
| ネットワーク・インタフェース..... | 9 |
| ネットワーク管理システム..... | 10 |
| 必要な情報の収集..... | 10 |

Junos OS は、ジュニパーネットワークスが提供するプラットフォームの多くで稼働するネットワーク・オペレーティング・システムです。本書には、新しいルーター、スイッチ、セキュリティ・プラットフォームなどのデバイスを初めてセットアップする際に必要となる、Junos の基本設定の手順が記載されています。これらの手順は、経験のあるネットワーク管理者には良く知られた一般的なプラクティスに従ったもので、分かりやすく説明されています。

他のメーカーによるネットワークデバイスと同様、これらを運用可能な状態にするためには、いくつかの基本的な設定を行う必要があります。例えば、ユーザーは、デバイスに割り当てられた IP アドレスを設定したり、基本的な管理機能を設定したりしなければなりません。

第1章では、デバイスの基本設定を行うために必要な情報のリストとそれぞれの内容を示します。この重要な情報は、本書の余白を利用してメモをとったり、付録のワークシートに書き込んでおくことをお勧めします。ラック間を移動する際は、手書きで紙に情報を書きとめ、それを参照する方が作業しやすいことがあります。第1章に記載されたすべての情報をまとめておけば、第2～5章で説明するデバイスの基本設定も簡単になります。

ホスト名

ネットワーク・インフラストラクチャに配備されているルーター、スイッチ、サーバー、またはファイアウォールをはじめとする大半のデバイスは、デバイスの IP アドレスではなく、固有の名前によって識別されています。これは、何桁もの数字が並ぶ IP アドレスよりも、単純な名前の方が簡単に区別したり、覚えたりすることができるためです。こうしたデバイス名は、ホスト名とも呼ばれています。

管理者は、多くのケースで、ネットワークにおける対象デバイスの役割が分かるような名前をホスト名として付けています。例えば、uk-london-R1 と付けます。ホスト名は、デバイスに固有のもので、通常は、DNS サーバーに追加され、管理者は覚えやすいホスト名を使用してデバイスに接続できるようにします。

ループバック・インタフェース

お使いのデバイスで設定するアドレスの大半は、物理的なインタフェースです。これに対して、ループバック・インタフェースは、どのハードウェアやネットワークとも関連付けられていない仮想のインタフェースです。物理インタフェースは、ネットワークから切り離したりアドレスを変更したりできますが、ループバックアドレスは不変です。ループバックアドレスは、ネットワークの運用や管理でさまざまな用途があります。

管理インターフェース

管理インターフェースを使用することで、認証されたユーザーや管理システムがネットワークを介してデバイスに接続できるようになります。デバイスによっては、フロントパネルに専用の管理ポートが搭載されていることがあります。Jシリーズや、SRX100、SRX210、SRX240、および SRX650 サービス・ゲートウェイなど他のタイプのプラットフォームでは、ネットワーク・インターフェースの1つに管理インターフェースを設定して、これを管理専用とするか、他のトラフィックと共有させることができます。

ユーザーが管理インターフェースにアクセスできるようにするには、まず設定が必要です。管理インターフェースの設定に必要な情報には、IP アドレスとプレフィックスがあります。多くの Junos デバイス（または推奨設定）では、管理インターフェースと他のポートの間のトラフィックをルーティングできません。そのため、別の（論理）ネットワーク内の別のプレフィックス（ネットマスク）を持つ IP アドレスを選択する必要があります。

バックアップルーター

Junos がレイヤー 3 フォワーディングを実行するネットワークデバイスで稼働している場合（ルーターなど）には、バックアップルーターを指定できます。バックアップルーターは、まだルーティングプロトコルがコンバージェンス状態に至っていない、Junos の初回起動プロセス中に使用することができます。バックアップルーターの使用によってデバイスは素早くレイヤー 3 接続を確立できるようになり、利用できない時間を最小限まで短縮できます。一般には、お使いのデバイスに直接接続された管理ネットワークのデフォルトゲートウェイをバックアップルーターとして選択します。

DNS (Domain Name System)

一般的に、何桁もの数字を覚えるよりも、名前を覚える方が簡単です。特に、桁数の多い IPv4 アドレスでは、それが顕著になります。このような理由から、DNS (Domain Name System) サーバーを使用して、デバイスのホスト名と IP アドレスをマッピングします。

DNS では、デバイスが通信する可能性のあるファイルサーバーやログサーバーなど、主要な外部システムを名前指定できます。DNS サーバーでは、ネットワーク上のデバイスのホスト名を保存する一元化されたレポジトリを維持しながら、デバイスホスト名が重複しないようにしています。この一元化されたレポジトリを使用することで、ネットワーク IP アドレスとホスト名に対するクエリーを送信したり、変換を管理したりできます。IP アドレスを介して1つまたは複数の DNS サーバーにクエリーを送信するように、デバイスを設定できます。

時刻サーバー

NTP (Network Time Protocol) は、IETF によって定義された、ネットワーク上で相互接続されたコンピュータシステムのクロックを同期するためのプロトコルです。大規模なネットワークの多くは、デバイスの場所に制限されることなく全デバイスの時刻を同期させる NTP サーバーを配備しています。ネットワーク上で NTP サーバーが稼働している場合には、そのアドレスを確認しておいてください。

ユーザー名およびパスワード

パスワードは、漏洩しないように注意してください。ここにパスワードを記入した場合には、第三者の目に触れないよう、本書を安全な場所に保管してください。

Junos の root アカウントには、デバイスの設定や運用のすべてを制御できる完全な管理権限が与えられています。この root アカウントは、一般に、スーパーユーザーと呼ばれています。

新しいデバイスでは、root アカウントにはパスワードはまだ設定されていません。設定をコミットするには、あらかじめ root アカウントにパスワードを設定しておく必要があります。パスワードを強くするほど、推測されにくくなり、アカウントの悪用が回避できます。

Junos では、こうした強いパスワードが設定されます。例えば、有効なパスワードは、

- 6 文字以上で
- 大文字 / 小文字または文字クラスを混在させる必要があります。
- パスワードには、ほぼすべての文字クラス（大文字、小文字、数字、句読点、その他の特殊文字）を含めることができます。

ただし、パスワードに制御文字を使用することは推奨されていません。

ベストプラクティス

安全なパスワードを設定するには、パスワードの文字数を増やし、大文字 / 小文字、数字、句読点をできるだけ混在させます。良いパスワード例は、t3aMX*u7rS です。

root ユーザーの他に、1 つ以上のローカルユーザーを作成しておくことを強く推奨します。このユーザーは、デバイスで管理作業やメンテナンス作業を実施する必要があるときにログインします。

ユーザー名には、空白文字、制御文字、コロン、カンマを含めることはできません。ユーザー名は、最大 64 文字に制限されます。また、ユーザーパスワードは、大文字 / 小文字、数字、その他の特殊記号が混在している必要があります。

リモート認証サーバー

多くのネットワークでは、すでにリモート認証サーバーを配備しています。こうしたサーバーを使用することで、ネットワーク内のすべてのデバイスに対して一元化されたユーザー・アカウント・セットを作成できるようになるため、ベストプラクティスとして推奨されています。

一元化されたサーバーを使用することには、各デバイスでローカルユーザーを作成するよりも、作業時間を短縮でき、エラーの発生を抑えられるなど数多くのメリットがあります。一元化された認証システムを構築することで、SecureIDなどのワンタイム・パスワード・システムを簡単に使用できるようになるため、取得したパスワードを使ってシステム管理者になりすますパスワードのスニффイングやリプレイアタックなどの攻撃から保護されます。

現在、多くの組織で採用しているリモート認証には、RADIUS (Remote Authentication Dial In User Service) および TACACS+ (extended Terminal Access Control Access Control System) の2種類があります。Junos では、両タイプの複数のリモート認証サーバーにクエリーを送信するように設定できます。

さらに詳しくは RADIUS または TACACS+ テクノロジーに関する情報については、Junos 技術資料の『*System Basics Configuration Guide*』を参照してください。ジュニパーの技術資料はすべて、www.juniper.net/techpubs/ から入手できます。

ネットワーク・インタフェース

お使いのデバイスでレイヤー3 フォワーディング (IP ルーティングなど) を実行している場合には、インタフェースに1つ以上のIPアドレスを割り当てる必要があります。複数のネットワーク・インタフェースがある場合には、それぞれに1つ以上のIPアドレスを割り当てます。本書には、お使いのデバイスをネットワーク上で運用できるように、ギガビットイーサネット・インタフェースを設定するための情報が掲載されています。

さらに詳しくは 『*Day One: Configuring Junos Interfaces and Routing*』では、他のタイプのインタフェースの設定方法について説明します。該当する製品がある場合には、www.juniper.net/dayone からダウンロードできます。

ネットワーク管理システム

一元化されたネットワーク管理システム（NMS）は使用していますか。多くのネットワーク管理システムでは、トラップと呼ばれる未承諾メッセージを送信する Junos デバイスのステータスを監視できる、SNMP のいずれかのバージョンを使用しています。Junos でトラップの送信先アドレスを設定するために、ネットワーク管理システムの IP アドレスを指定できます。

SNMP では、コミュニティ文字列と呼ばれる基本的な認証方法を使用して、マネージャとリモートエージェント間のアクセスを制御します。コミュニティ文字列は、デバイス（およびそれらで稼働するエージェント）のグループを共通の管理ドメインにまとめるための管理用の名前です。マネージャとエージェントが同じコミュニティを共有している場合には、相互通信が可能です。

SNMP コミュニティ文字列は、その機能が似ているパスワードおよびキーのような概念と捉えられています。そのため、SNMP コミュニティは従来から文字列と呼ばれています。コミュニティ文字列は、Junos の SNMP エージェントによって実装される管理認証の第一段階です。

デバイスでは、リモートログ収集も設定できます。Junos では、多くの Unix デバイスと同様の Syslog メカニズムを使用して、指定したログ・ホスト・アドレスにログメッセージを転送します。これにより、各デバイスから中央のホストにメッセージを転送できるようになり、ネットワーク全体を監視することが容易になります。Syslog は、きわめて高い柔軟性と機能性を備えたメッセージのログ収集方法で、SNMP トラップで提供される情報を補助するために多くのデバイスベンダーで採用されています。

必要な情報の収集

以上で、初日の設定で必要となる情報が揃いました。付録の「設定情報ワークシート」（本書の電子版に付属）をプリントアウトし、収集した情報を記入しておいてください。あるいは、本書の余白にデバイスの詳細をメモしておきます。これは、以降の章で説明するコマンドや手順を実行する際に参照できるようにしておいてください。

第2章

システムの基本設定

| | |
|-------------------|----|
| システムの基本設定 | 12 |
| DNSサーバーへの到達 | 18 |
| 日付と時刻の設定 | 19 |
| インタフェースの概要 | 21 |
| 作業のレビュー | 24 |

第1章では、以降の章で使用する重要な設定情報を収集しました。本章では、ベースシステム、ユーザーアカウント、リモートアクセス、およびインタフェースなど、デバイスの基本的な設定を実際に行います。

お使いのデバイスで、左マージンの矢印▶で示された設定コマンドをすべてを入力すると、付録に記載された参考設定と同じ結果が得られます。

実際の環境に合わせて、第1章で収集した情報を使用してコマンドエントリをカスタマイズできます。設定結果と付録に記載された参考設定を比較した場合、カスタマイズ可能なフィールドのみが異なり、デバイスの基本設定が完了して実際のネットワークで運用できる準備が整います。

システムの基本設定

本セクションでは、root（管理者）のパスワード、ホスト名、管理インタフェース、ループバック・インタフェース、バックアップルーターのベースシステムの設定をはじめ、デバイス設定の第一歩を順に説明します。第1章で収集した情報を参照しながら本セクションを読み、root（管理者）のベースシステムの設定を含め、実際に運用するネットワークに合わせてデバイス設定をカスタマイズしてください。

注 本書では、設定モードでのコマンド例を示す際に、コマンドプロンプトを必ずしも表示しません。

ヒント 初めて Junos を使用する場合、または最後にデバイスの設定を行ってからしばらく時間が経過している場合には、設定できる基本項目を [edit system] 階層で確認することができます。

```
[edit system]
root@juniper1# set system ?
Possible completions:

+ authentication-order Order in which authentication methods are invoked
> backup-router        IPV4 router to use while booting
  domain-name          Domain name for this router
  host-name             Hostname for this router
> location              Location of the system, in various forms
> login                 Names, login classes, and passwords for users
> name-server           DNS name servers
> ntp                   Network Time Protocol services
> radius-options        RADIUS options
> radius-server         RADIUS server configuration
```

```
> root-authentication Authentication information for the root login
> syslog               System logging facility
   time-zone           Time zone name
<snip>
```

root 認証パスワード

root アカウントは、Junos で事前定義されたユーザー名です。root ユーザーは、デフォルトでは管理者またはスーパーユーザーに設定されており、デバイスにソフトウェアをインストールして設定する完全なパーミッションが与えられています。

Junos では、設定をコミットする前に、root のパスワードを設定しておく必要があります。新しいデバイスでは、root のパスワードが初めてコミットする設定に含まれている必要があります。以下のコマンドを使用して、root ユーザーのプレーンテキスト形式によるパスワードを設定します。

```
▶ set system root-authentication plain-text-password
▶ New password: #####
▶ Retype new password: #####
```

パスワードをプレーンテキスト形式で入力すると、Junos ではそれを直ちに暗号化します。他のシステムのように、Junos に対してパスワードを暗号化するよう指示する必要はありません。そのため、プレーンテキスト形式によるパスワードは表示されず、Junos 設定リスティンクでは「## SECRET-DATA」と示されます（付録の例を参照）。

ベストプラクティス

セキュリティを強化するために、root アクセスはコンソールポートからのみ許可します。

```
set system services ssh root-login deny
```

ホスト名

デバイスのホスト名は、さまざまな用途で ID の役割を果たします。Junos では、設定したホスト名をコマンドプロンプトで使用してログファイルや関連するアカウント情報情報の先頭に付加したり、デバイス識別が役立つ状況で使用したりします。本書では、ホスト名として *juniper1* を使用しますが、実際の環境に適した名前を付けることができます。

```
▶ set system host-name juniper1
```

ループバック・インタフェース

ループバック・インタフェースは、各種のネットワーク機能や運用機能をサポートする、常に起動状態のインタフェースです。ループバック・インタフェースは、例えば一部の物理インタフェースが停止している、切り離されている、またはその IP アドレスが変更されていても、デバイスに到達できるようにします。大半のケースで、必ずループバック・インタフェースを定義します。

Junos では、`lo0` をループバック・インタフェースの識別名として使用する IP 規則に従います。ループバック・インタフェース用に選択した IP アドレスについては、第 1 章を確認してください。

```
► set interfaces lo0 unit 0 family inet address 192.26.0.110/32
```

注 `set interfaces` コマンド形式の詳細については、本章の「インタフェースの概要」セクションを参照してください。

警告! Junos では、ループバック・インタフェースを /32 ネットワークマスクで設定する必要があります（不必要なアドレススペースの割り当てを避けるため）。

必要な数のアドレスを `lo0` インタフェースで設定できるため、そのうちの 1 つを優先アドレスとすることをお奨めします。

```
► set interfaces lo0 unit 0 family inet address 192.26.0.110/32 preferred
```

マスター・ループバック・インタフェースとして設定できるのは `unit 0`（ユニットは Junos インタフェースにおける論理チャンネル）のみです。さらに他の IP アドレスを追加するには、優先オプションを使用せずに、通常の方法で `unit 0` に設定します。

```
set interfaces lo0 unit 0 family inet address 192.168.1.1/32
set interfaces lo0 unit 0 family inet address 192.168.2.1/32
```

ベストプラクティス `lo0.0` インタフェース（.0 は論理チャンネル）では、IP アドレス `127.0.0.1` を設定しておくことが役立ちます。これは、NTP および MPLS ping などいくつかのプロセスで、このデフォルト・ホスト・アドレスを使用するためです。

```
► set interfaces lo0 unit 0 family inet address 127.0.0.1/32
```

`127.0.0.1/32` アドレスは、Martian IP アドレス（ルーティングには無効なアドレス）であるため、ジュニパー製デバイスでの使用はお奨めしません。

注 ネットワークの設定に応じて、IS-IS ルーティングプロトコル用に ISO アドレスの設定が必要な場合もあります。

```
set interfaces lo0 unit 0 family iso address 49.0026.0000.0000.0110.00
```

管理インタフェース

管理インタフェースは、認証されたユーザーおよび管理システムのデバイスへのアクセスをサポートします。ユーザーは、SSH および Telnet などの標準ユーティリティを使用して（設定方法については第3章を参照）、ネットワークを介して管理インタフェースに接続できます。

多くの Junos プラットフォームでは、フロントパネルに専用の管理ポートを搭載しています。他のデバイスについては、イーサネットポートの1つを管理インタフェースとして設定できます。

管理用にネットワーク・イーサネット・インタフェースを使用するプラットフォームには、SRX100、SRX210、SRX240、および SRX650 サービス・ゲートウェイ、さらには J シリーズ サービスルーターなどがあります。ネットワーク・インタフェースは、帯域外管理専用として、または管理トラフィックとネットワーク・トラフィックで共有するように設定できます。

さらに詳しくは お使いのデバイスが専用管理ポートを備えている場合でも、管理トラフィックを伝送するようにネットワーク・インタフェースを設定することもできます。例えば、別個の管理インフラストラクチャを構築するコストが妥当でないと考えられる場合、組織としてこのアプローチをとることもできます。帯域内管理での EX シリーズ イーサネットスイッチの設定方法については、Whitepaper『*Deploying EX-series Switches in Branch Offices*』を参照してください。これは、www.juniper.net/us/en/products-services/switching/ex-series/ からダウンロードできます。

専用管理ポート

専用管理ポートは、デバイス内のネットワーク・トラフィックから物理的に完全分離した帯域外管理アクセスをサポートします。このアプローチでは、デバイスへのアクセスが制限されるため、問題が生じることもあります。また、管理トラフィックのみを伝送するため、デバイスが攻撃にさらされた場合には、管理ポートを問題の分析と対応専用を使用することができます。

専用管理ポートを設定するには

専用管理ポートを設定するには、管理インターフェースとして使用する IP アドレスを割り当てるだけです。Junos コマンドで使用するインターフェース名は、設定対象のデバイスタイプに応じて異なります。

以下の例では、EX シリーズ スイッチで専用管理ポートを設定するためのコマンド形式を示します。EX シリーズ イーサネットスイッチは、インターフェース名 `me0` を管理ポート名として使用します。

```
▶ set interfaces me0 unit 0 family inet address 172.26.27.44/24
```

他の Junos デバイスでは、専用管理ポートの名前として `fxp0` を使用します。表 2.1 に、ジュニパーの各種プラットフォームで、専用管理ポートとして割り当てられた名前を示します。これ以外のプラットフォームを使用している場合は、上記のコマンド・ステートメントでインターフェース名 `me0` の代わりに `fxp0` を使用してください。

表 2.1 専用管理ポート名

| プラットフォーム | 専用管理ポート |
|---------------------------------|-----------------------|
| EX シリーズ イーサネットスイッチ | me0 (次のページの上部の「注」を参照) |
| M、MX、および T シリーズ ルーター | fxp0 |
| SRX5xxx および SRX3xxx サービス・ゲートウェイ | fxp0 |

さらに詳しくは J シリーズの管理インターフェースの詳細については、www.juniper.net/techpubs の該当資料を参照してください。

注 EX シリーズでは、さらに `vme` と呼ばれる、仮想シャーシ内でデバイス群をグループ化して管理する仮想管理インターフェースを使用します。詳細については、『*Day One: Configuring EX Series Ethernet Switches*』を参照してください。これは www.juniper.net/dayone から入手できます。

ネットワーク・インタフェースを介した管理

お使いのデバイスタイプで管理トラフィックの伝送用にネットワーク・インタフェースを使用している場合は、同様に、管理インタフェースとして使用する IP アドレスを設定します。以下の例では、帯域外管理専用のネットワーク・インタフェースに設定した管理インタフェース例を示します。

次のセクションでは、拠点 / 支店向け SRX シリーズまたは J シリーズのデバイス上で管理インタフェースをフローベースモードで設定する方法について説明します。

ゾーンを用いて専用ネットワーク・インタフェースに管理インタフェースを設定するには

1. インタフェースに、管理用に使用する IP アドレスを設定します。

```
set interfaces ge-0/0/0 unit 0 family inet address
172.26.27.44/24
```

2. インタフェースがトラフィックを伝送できるようにするには、まず、設定した管理インタフェースをゾーンに割り当てる必要があります。このゾーンによってトラフィックを仮想的に分離でき、ポリシー・エンフォースメント・ポイントとして機能します。機能ゾーン management は、これらのプラットフォームの帯域外管理用に事前定義された特別なゾーンです。以下のコマンドを使用して、このゾーンに論理インタフェースを加えます。

```
set security zones functional-zone management interfaces ge-
0/0/0.0
```

3. 機能ゾーンを設定したら、以下の例のように、インタフェースが応答するプロトコルを指定する必要があります。

```
set security zones functional-zone management host-inbound-
traffic system-services ssh
```

さらに詳しくは 機能ゾーンおよびセキュリティゾーンの詳細については、『*Security Configuration Guide*』を参照してください。これは、www.juniper.net/techpubs から入手できます。

バックアップルーター

Junosでは、レイヤー3デバイスで初回の起動プロセス中にバックアップルーターを使用するように設定できます。ルートの確立（およびその他の機能）を担うJunosプロセスは、RPD（Routing Protocol Daemon）と呼ばれています。Junosの起動中はまだRPDが起動していないため、デバイスではルートが確立されていません。バックアップルーターを設定することで、デバイスは起動時にレイヤー3接続を確立できるため、デバイスが利用できない時間を最小限まで短縮できます。

```
► set system backup-router 172.26.31.1 destination 172.16.0.0/12
```

この例では、管理システムのデフォルトゲートウェイを選択すると、管理ネットワーク（IPレンジ172.16/12のすべて）は、まだルーティングプロトコルがコンバージェンス状態に至っていない起動プロセスの早い時期に、ネクストホップ172.26.31.1を介して到達可能になります。

注 Junosでは、起動シーケンス中にのみバックアップルーターを使用します。バックアップルーターを起動後に使用できるように設定するには、『*Day One: Configuring Junos Interfaces and Routing*』で説明するようにデフォルトルートを設定できます。これは、www.juniper.net/dayone から入手できます。

DNS サーバーへの到達

JunosでDNSサーバーの場所を把握している場合には、ホスト名をIPアドレスに対して解決できます。これは、WebブラウザがWebサイトのネットワークアドレスを解決するのと似たアプローチです。

また、Junosでは、（ドメイン名が省略されているなど）完全修飾でないホスト名を解決するために使用するために、1つまたは複数のドメイン名を設定できます。これは、完全なドメイン名を参照することなく、Junosの設定および運用で単にホスト名だけを使用することができる便利な方法です。

ショートカット Junosの設定にDNSサーバー（複数可）およびドメイン名（複数可）を追加すると、設定およびコマンドで、IPアドレスの代わりにDNSで解決できるホスト名を使用できるようになります。

DNS サーバーを設定するには

1. まず、DNSサーバー（複数可）のIPアドレス（複数可）を `name-server` ステートメント（複数可）で指定します。

```
► set system name-server 172.26.27.2
```

```
▶ set system name-server 172.26.27.3
```

2. デバイス自体が属するドメイン名を設定することを推奨します。Junos では、設定したこのドメイン名をデフォルトのドメイン名として、完全修飾でないホスト名に付加します。

```
▶ set system domain-name enterprise.com
```

3. デバイスから複数のドメインに到達できる場合には、これらを検索するドメインリストとして設定できます。Junos では、このリストを使用して、ホストの IP アドレスの検索時にドメイン名を付加する順序が設定されます。

```
▶ set system domain-search [enterprise.com department.enterprise.com]
```

このコマンド例では、Junos で完全修飾ではないホストを解決するときに、まず `enterprise.com`、次に `department.enterprise.com` という順序で、ドメイン名を検索するように設定しています。

確認 Junos デバイスのホスト名および IP アドレスを DNS サーバーで設定し、設定をコミットしたら、以下のコマンドを発行して DNS が正しく動作しており、到達可能であることを確認します。

最初のコマンドでは、デバイスの IP アドレスを使用して、設定したホスト名が解決できることを確認します。

```
root@juniper1> show host 172.26.27.44
44.27.26.172.in-addr.arpa domain name pointer juniper1.enterprise.com.
```

2 つ目のコマンドでは、設定したホスト名を使用して、IP アドレスが解決できることを確認します。

```
root@juniper1> show host juniper1
juniper1.enterprise.com has address 172.26.27.44
```

注 DNS サーバーでは、デバイスに到達できるアドレスである限り、任意の IP アドレスを Junos デバイスに割り当てることができます。ここでは、管理インターフェースを使用していますが、DNS サーバーではループバック・インターフェース、ネットワーク・インターフェース、または複数アドレスを設定することができます。

日付と時刻の設定

初めてデバイスを設定するときには、イベントの発生を正確に記録できるように時刻を設定しておきます。Junos デバイスの時刻を設定するには、手動で設定するか、NTP サーバーからシステム時刻を取得するように設定できます。

ローカルで時刻を設定するには

NTP にアクセスできない場合は、オンボードクロックを使用して独自のローカル時刻を維持するよう Junos を設定できます。Junos の運用モードで、日付と時刻を手動で設定できます。

```
root@juniper1> set date 200901011200.00
```

日付の形式は、YYYYMMDDhhmm.ss です。

リモート時刻サーバーを使用するには

大規模なネットワークでは、すべてのネットワークデバイスにわたって時刻を合わせるために、NTP サーバーを設定することが役立ちます。基準時刻を設定することで、トラブルシューティングのためにログファイルやトレースファイルのタイムスタンプを相互に関連付けることができます。

以下の手順に従って、デバイスで1つまたは複数の NTP サーバーを使用するよう設定します。

1. 最も簡単に NTP で時刻を設定できるのは、Junos の起動時に時刻を取得する方法です。以下のコマンドを使用して、NTP サーバーの IP アドレスを指定します。

```
▶ set system ntp boot-server 172.26.27.4
```

2. 定期更新でデバイスを同期させるには、参照先 NTP サーバーを設定します（複数設定可能）。Junos デバイスは長期間にわたって動作し続けることで、クロックがずれる可能性があるため、この方法が推奨されます。

```
▶ set system ntp server 172.26.27.4
```

3. 次に、デバイスの場所をローカル・タイム・ゾーンに合わせます（デフォルトは UTC）。これにより、Junos では、年間で数回変更することのある UTC からのオフセットなどが考慮された、ロケーションに適した正しい形式で時刻を示すようになります。

```
▶ set system time-zone Europe/Amsterdam
```

ヒント 管理者の多くは、すべてのデバイスで UTC タイムゾーンを設定しています。このアプローチは、異なるタイムゾーンに配備されたデバイス群にわたってログやその他のイベントのタイムスタンプが簡単に比較できるようになるというメリットがあります。

4. Junos を起動したばかりで、リモートの時刻ソースと時刻を同期させる必要がある場合には、運用モードで行えます。

```
root@juniper1> set date ntp 172.26.27.4
```

```
7 Apr 10:32:27 ntpdate[4544]:step time server 172.26.27.4 offset -0.000565 sec
```

設定時刻を確認するには

時刻を設定したら、以下の方法で設定内容をチェックします。

確認 任意のタイミングでシステム時刻を確認します。

```
root@juniper1> show system uptime
Current time:2009-04-06 15:36:10 CEST
System booted:2009-03-27 12:56:33 CET (1w3d 01:39 ago)
Protocols started:2009-03-27 12:58:04 CET (1w3d 01:38 ago)
Last configured:2009-04-06 15:27:02 CEST (00:09:08 ago) by username
3:36PM up 10 days, 1:40, 1 user, load averages: 0.00, 0.00, 0.00
```

このリスティングには、現在の時刻の他、デバイスを最後に起動した日時、プロトコルを開始した日時、最後にデバイスを設定した日時なども示されます。

また、以下の2つのコマンドを使用して、NTP サーバーのステータスおよびデバイスで使用したクロックソースの対応を確認できます。

```
root@juniper1> show ntp associations
      remote          refid      st t when poll reach  delay  offset jitter
=====
*172.26.27.4      203.26.24.6      3 u  16  64  377  0.256  -0.164  0.022

root@juniper1> show ntp status
status=0644 leap_none, sync_ntp, 4 events, event_peer/strat_chg,
version="ntpd 4.2.0-a Wed Mar 25 07:21:19 UTC 2009 (1)",
processor="i386", system="Junos9.4R2.9", leap=00, stratum=4,
precision=-19, rootdelay=502.545, rootdispersion=74.632, peer=59484,
refid=172.26.27.4,
reftime=cd847dfc9.ccb54775 Mon, Apr 6 2009 15:11:05.799, poll=6,
clock=cd847dfc.4a08cfa9 Mon, Apr 6 2009 15:11:24.289, state=4,
offset=-0.164, frequency=52.814, jitter=0.030, stability=0.005
```

インタフェースの概要

Junos デバイスが備えるインタフェースには、デバイスでトラフィックを伝送する物理インタフェースと、管理インタフェースやループバック・インタフェースなどの特殊インタフェースがあります（前述の「管理インタフェース」および「ループバック・インタフェース」の各セクションを参照）。

このセクションでは、デバイスの基本設定のうち、インタフェース名の付け方、論理インタフェースの概要、およびギガビット・イーサネット・インタフェースの設定方法について説明します。

さらに詳しくは『*Day One: Configuring Junos Interfaces and Routing*』では、他のタイプのインタフェースの設定方法について説明します。該当する製品がある場合には、www.juniper.net/dayone からダウンロードできます。

物理インタフェースの名前付け

お使いのプラットフォームでは、トラフィック伝送用のイーサネット・インタフェースや、各種の Junos デバイスで提供される1つまたは複数の WAN インタフェースを備えていることがあります。どのようなタイプのインタフェースであっても、Junos では、その名前は共通の形式に従います。インタフェース名は、インタフェースタイプおよびインタフェース・ナンバリングの2つの部分で構成されます。

Junos では、インタフェースの各タイプをテキスト識別子で表します。例えば、ギガビットインタフェースの識別子は文字列 `ge` です。

ジュニパーのエンジニアは、(各ハードウェア・プラットフォーム内の)各インタフェース・ロケーションに対応するインタフェース番号を割り当てます。一般に、以下の規則に基づいて、デバイスインタフェースに対して0から順に番号を割り当てていきます。

- **スロット**: 最初の番号は、スロットの場所を示します。小さなプラットフォームでは、固定インタフェースは、通常、スロット0に割り当てられます。ハイ・エンド・プラットフォームでは、物理スロットにFPC (Flexible PIC Concentrator) を挿入できます。FPCは、多数のインタフェースカードを搭載できる大きな基板です。
- **PIC**: 2つ目の番号は、スロット内のPIC (物理インタフェースカード) の位置を示します。
- **ポート**: 3つ目の番号は、PICのポート番号を示します。

これらをつなげたインタフェース名は、例えば、`ge-0/0/1` となります。この例では、インタフェースタイプはギガビットイーサネット、スロット番号は0、PIC番号は0、そしてポート番号は1です。

ヒント 複数のFPCやPICを扱う場合でも区別できるように、PIC自体にもポート番号が記載されています。

試してみよう: ハードウェア設定の参照

以下の運用モードコマンドをデバイスに入力して、物理的な設定を確認します。

```
root@juniper1> show chassis hardware
```

論理ユニット

ネットワークの設定時には、物理インタフェースを複数の論理インタフェースに分割した方が良い場合があります。- 例えば、イーサネット・インタフェースを複数の VLAN (仮想 LAN) に分割することができます。Junos では、こうした論理インタフェースを **ユニット** と呼びます。Junos では、一般に、各物理インタフェースで1つ (または複数) の論理ユニットの設定が必要です。

Junos では、論理インタフェースの名前を付ける際、単に物理ポートに論理ユニットを付加します。論理ユニット (またはチャンネルとも呼ばれる) **0** を上記の例に追加した場合、インタフェースの完全な名前は以下ようになります。

```
ge-0/0/1.0
```

注 他のベンダーでは、プラットフォームの論理インタフェースを **サブインタフェース**と呼んでいます。

ギガビットイーサネット

Junos でのインタフェース設定方法を習得するには、例を使うのが最良の方法です。ここでは、ギガビット・イーサネット・インタフェース `ge-0/0/1` を設定するものとします。 `set interfaces` コマンドを使用して、IPv4 アドレス `192.168.100.1/30` を指定します。

```
set interfaces ge-0/0/1 unit 0 family inet address 192.168.100.1/30
```

コマンドの各レベルについて説明します。

- **ge-0/0/1** は、物理的なギガビットイーサネット・インタフェースの名前です。
- **unit 0** は、物理インタフェース内で設定した論理ユニットです。トラフィックを伝送できるようにするには、あらかじめ各物理インタフェースに1つ以上の論理インタフェースを設定する必要があります。論理インタフェースは、(1ではなく) 0 から順に番号が付けられます。

- **family inet** は、論理インタフェースで使用するプロトコルを示します。各論理インタフェースに、1つ以上のファミリーを必ず設定します。本書では、どの設定例でも、Junos が IPv4 を参照する **inet** を使用します。
- **address 192.168.100.1/30** は、論理インタフェースのアドレスです。各論理インタフェースで、複数のアドレスをサポートできます。そのため、追加アドレスを設定しても、既存のアドレスは上書きされません。

確認 ギガビット・イーサネット・インタフェースの設定内容を表示させます。

```
root@juniper1# show interfaces
ge-0/0/1 {
  unit 0 {
    family inet {
      address 192.168.100.1/30;
    }
  }
}
```

作業のレビュー

デバイスで重要な基本設定を行った後、これまでの作業内容をレビューします。まず、設定をコミットします。次に、リスティング内容と、矢印 ▶ で示されるコマンドによって定義された設定を比較します。参考設定は、本書の PDF 版の付録に掲載されています。

運用モードで `show configuration` コマンドを使用して、コミット完了後にアクティブな設定の内容を表示させます。デバイスでも同じように設定していた場合には、`ge-0/0/1` インタフェースについて、以下のステートメントが記述されているはずで

```
root@juniper1> show configuration interfaces ge-0/0/1
unit 0 {
  family inet {
    address 192.168.100.1/30;
  }
}
```

アクティブな設定を一連の `set` コマンドとして表示させるには

表示されたリスティングは、元の `set` コマンドに簡単に変換できます。これは、出力を `| display set` 修飾子にパイプして挿入することで行います。この方法では、どのコマンドによって設定が作成されたかを簡単に確認することができます。

```
root@juniper1> show configuration interfaces ge-0/0/1 | display
set
set interfaces ge-0/0/1 unit 0 family inet address
192.168.100.1/30
```

注 Junos では、`show configuration | display set` リスティングを設定モードの上位から表示します。すなわち、`set` コマンドは、設定の `[edit]` 階層にて使用する形式で記述されています。

ヒント 運用モードの `show` コマンドを使用して出力を確認する際、`detail` または `extensive` キーワードを使用して、より詳細な情報を表示することもできます。

第3章

ユーザーアカウントの設定

| | |
|--------------------|----|
| ログインバナーの作成 | 28 |
| ログインアカウントの設定 | 29 |
| リモート認証の設定 | 31 |
| リモートアクセスの有効化 | 33 |
| 変更のコミット | 34 |

Junos では、ユーザーアカウント、認証、およびパーミッションを設定して管理するための柔軟性の高い機能を豊富に備えています。本章では、初日の作業で必要なこと、さらには Junos オペレーティング・システムのより高度な機能を活用する際に役立つ、いくつかの参考情報を示します。

ログインバナーの作成

デバイスにアクセスするユーザーのために、ログインの前または後に表示されるログインバナーを作成できます。初回ログインメッセージを作成してから、ユーザーアカウントを作成することをお奨めします。

ログインメッセージ

ログインメッセージには、ユーザーがデバイスにアクセスしてログインする前に、バナーが表示されます。このメッセージは、`\n` (改行。キャリッジリターンやラインフィードに相当) を区切り文字として、複数行に分割することができます。

▶ **set system login message "Welcome \n to \n Junos Training\n "**

上記のメッセージを設定すると、デバイスにアクセスするどのユーザーの画面にも、このメッセージが表示されます。例えば、リモートクライアントで SSH を使用している場合には、以下が表示されます。

```
$ ssh juniper1
Welcome
to
Junos Training
root@juniper1's password:
```

ヒント ログインメッセージを使用して、認証されていないデバイスへのアクセスが禁止されていることを通知できます (組織に適した具体的なメッセージ文については、それぞれの法務部にお問い合わせください)。

```
set system login message "WARNING:Unauthorized access is an offense"
```

ログイン通知

認証されたユーザーのみに対して、ログインした後に、通知を表示することもできます。例えば、近いうちに実施されるメンテナンス作業をお知らせすることができます。認証されたユーザーに限定して通知を表示させるには、`set system login announcement` コマンドを使用します。

▶ **set system login announcement "Maintenance scheduled 11PM to 2AM tonight"**

ログインアカウントの設定

Junos では、ユーザーがデバイスにログインする前に、あらかじめそれぞれのアカウントが定義されている必要があります。さらに、ユーザーごとにデバイスのどの箇所にアクセスが許可されるのかを、ログインアカウントで設定することができます。アカウントは、ローカルユーザーとパスワード、あるいはローカルユーザーと RADIUS または TACACS+ プロトコル（後述）を使用して認証を行うリモートサーバーによって異なるユーザーテンプレートで設定できます。

ローカルユーザーとパスワード

以下の手順に従って、ローカルユーザーの名前とパスワードを設定します。次のセクションでは、それぞれのユーザークラスを追加します。

1. まず、設定の [edit system login] セクションに移動します。

```
[edit]
▶ root@juniper1# edit system login
[edit system login]
root@juniper1#
```

2. 割り当てたアカウントログイン名を使用して、新しいユーザーを追加します。この例では、ユーザー名が jadmin である新しいユーザーが作成されます。

```
[edit system login]
▶ root@juniper1# edit user jadmin
```

3. アカウントに対して詳細な名前（フルネーム）を設定することもできます。フルネームに空白文字が含まれる場合は、名前全体を二重引用符で囲みます。

```
[edit system login user jadmin]
▶ root@juniper1# set full-name "Juniper Network Administrator"
```

4. アカウントの UID を設定します。UID は、Unix システムと同様、ユーザーのパーミッションとファイルアクセスを設定するものです。UID を指定しなかった場合には、Junos で自動的に割り当てます。UID は、100 ~ 64000 の範囲の数字です。UID を設定するには、以下のよう
に記述します。

```
[edit system login user jadmin]
▶ root@juniper1# set uid 1250
```

5. ユーザーのパスワードを設定します。第 2 章で説明したように、set コマンドを使用してパスワードをプレーンテキスト形式で作成すると、Junos でそれを内部的に暗号化します。

```
[edit system login user jadmin]
root@juniper1# set authentication plain-text-password
New password: ####
Retype new password: ####
```

Junos では、デフォルトで、設定内にあるローカルアカウントを使用してソフトウェアへのログインを試行するすべてのユーザーに対して、ローカルで認証を行います。

さらに詳しくは ユーザー（および root）パスワードは、暗号化されたパスワードとしてローカルで設定することもできます。これらの設定方法については、『*Systems Basics Guide*』の「Configuring User Accounts」セクションを参照してください。この資料は www.juniper.net/techpubs から入手できます。

ログインクラス

すべてのユーザーアカウントには、ユーザー名とパスワードの他に、ログインクラスの設定が必要です。ログインクラスは、実行可能なコマンドのパーミッションを定義するものです。ユーザーが、コマンドラインにコマンドを入力すると、Junos では各コマンドのログインクラスのパーミッションレベルをチェックしてからそれを許可します。Junos では、あらかじめ 4 つのログインクラスが定義されています。

- **super-user** : すべてのパーミッション
- **operator** : パーミッションのクリア、ネットワーク、リセット、トレース、および参照
- **read-only** : パーミッションの参照
- **unauthorized** : パーミッションなし

上記の例で作成した新しいユーザーに対して、ログインクラス **super-user** を設定します。デバイスでは、常に 1 つ以上の **super-user** をローカルで設定しておく必要があります。

```
[edit system login user jadmin]
root@juniper1# set class super-user
```

カスタム・ログイン・クラスを設定するには

4 つのデフォルトのクラスで提供されるパーミッションよりも、さらに詳細なものが必要な場合には、独自のカスタム・ログイン・クラスを作成できます。カスタム・ログイン・クラスごとに、含めるまたは除外するコマンドを細かく指定することができます。こうして、特定のユーザーグループごとのニーズに合わせたユーザークラスを作成できます。

1. 例えば、ネットワーク運用スタッフ用に *netops* という名前のカスタム・ログイン・クラスを作成できます。

```
set system login class netops
```

2. 各ログインクラスについて、許可または拒否するパーミッションを指定できます。この例では、設定をシンプルにするために、*netops* クラスに対してすべてのアクセスを許可します。

```
set system login class netops permissions all
```

さらに詳しくは 独自のユーザークラスの設定方法など、ユーザークラスの詳細については、『*System Basics Configuration Guide*』の「Configuring User Accounts」を参照してください。この資料は www.juniper.net/techpubs から入手できます。

リモート認証の設定

一般に、ユーザーに関する情報は、リモート認証サーバーを使用して一元化して保存します（第1章を参照）。Junos では、RADIUS および TACACS+ サーバーをはじめ、1つまたは複数のリモート認証サーバーを使用するよう設定できます。

Junos デバイスでリモート認証を設定するには、サーバーへのアクセス、認証の順序、およびローカル・ユーザー・アカウントを設定する必要があります。リモートサーバーによって認証されたユーザーと、デバイスでローカルに定義されたユーザーアカウントをマッピングするために、いくつかのオプションが提供されています。

以下の例では、remote テンプレート・アカウントを使用した方法を示します。ユーザー名 *remote* は、Junos での特殊なケースです。これは、リモートの RADIUS または TACACS+ サーバーによって認証されたが、デバイスでローカルに設定されたユーザーアカウントがないユーザー用のテンプレートとして機能します。この場合、Junos は *remote* テンプレートのパーミッションを、ローカルに定義されたアカウントがない認証ユーザーに適用します。remote テンプレートにマッピングされたすべてのユーザーは、同じログインクラスとなります。

注 リモートで認証されたユーザーをマッピングする方法としては、同一ユーザークラスのすべてのユーザー用に共有アカウントを設定する方法もあります。この方法は、リモートユーザーに対して複数のタイプのテンプレートが必要なときに使用します。詳細については、Junos 資料『*Administration Guide*』の「Creating a Local Template Account」を参照してください。この資料は www.juniper.net/techpubs から入手できます。

RADIUS サーバーによる認証の設定を開始するには

以下の手順に従って、RADIUS サーバーによるユーザー認証の設定を開始します。そして手順 3 および 4 に進み、設定を完了します。

1. RADIUS 設定ステートメントを入力します。

```
set system radius-server 172.26.27.5
```

2. コマンド・ステートメントには、共有のパスワードや、必要に応じてポート番号を含めることができます。

- ▶

```
set system radius-server 172.26.27.5 port 1845
```
- ▶

```
set system radius-server 172.26.27.5 secret Jun1p3r
```

TACACS+ サーバーによる認証の設定を開始するには

以下の手順に従って、TACACS+ サーバーによるユーザー認証の設定を開始します。そして手順 3 および 4 に進み、設定を完了します。

1. TACACS+ 設定ステートメントを入力します。

```
set system tacplus-server 172.26.27.6
```

2. コマンド・ステートメントには、共有のパスワードや、必要に応じてポート番号を含めることができます。

- ▶

```
set system tacplus-server 172.26.27.6 port 49
```
- ▶

```
set system tacplus-server 172.26.27.6 secret Jun1p3r
```

ログイン方法を指定するには

3. Junos で認証を試行する順序を指定します。

- ▶

```
set system authentication-order [ radius tacplus password ]
```

上記の例では、RADIUS と TACACS+ の両サーバーがネットワークに配備されていることを想定しています。いずれにしても、RADIUS および / または TACACS+ を設定する手順で、このコマンドを記述する必要があります。この例では、ユーザーがログインを試行するたびに、Junos では認証のために RADIUS サーバーにクエリーを送信します。失敗すると、次に TACACS+ サーバーで認証を試して、最後にローカルで設定したユーザーアカウントを確認します。

警告! パスワードオプションを設定していない（および認証サーバーが使用できる）場合、Junos ではローカルパスワードを使用した認証を試行しません。

リモートサーバーによる認証の設定を完了するには

4. 各ユーザーには、ローカルでユーザー名を定義するか、デフォルトの `remote` ユーザーを設定できます。ローカルユーザー `adminjlk` および `remote` テンプレートを設定するには、以下を記述します。

```
▶ set system login user adminjlk class super-user
▶ set system login user remote class super-user
```

リモート認証サーバーによる設定を確認するには

1. サーバーでの設定がすべて正しければ、Syslog メッセージファイルに以下のメッセージが表示されます。この確認方法を行うには、第5章で説明するシステムログ収集をあらかじめ設定しておく必要があります。

```
root@juniper1> show log messages
Apr 22 13:38:58 juniper1 sshd[17859]:Accepted password for adminjlk from 172.30.48.10
port 61729 ssh2
```

RADIUS サーバーにログインしたユーザー名がない場合は、メッセージログに以下のエラーメッセージが表示されます。

```
Apr 22 13:40:57 juniper1 sshd[17873]:Failed password for username from 172.30.48.10 port
64844 ssh2
```

2. SSH セッション接続内容も表示することができます。

```
root@juniper1> show system connections
Active Internet connections (including servers)
Proto Recv-Q Send-Q Local Address          Foreign Address        (state)
tcp4      0    48 172.30.53.101.22      172.30.48.10.61729    ESTABLISHED
```

リモートアクセスの有効化

SSH、Telnet、および FTP は、ネットワークデバイスへのリモートログインやシステム間のファイル交換で広く使用されている規格です。認証されたユーザーがデバイスにアクセスできるようにする、またはお使いのデバイスと他のシステムの間でデータを交換できるようにするには、あらかじめこれらのサービスを設定しておく必要があります。Junos では、これらのサービスはデフォルトでは無効化されています。

SSH は、Telnet の後継としてリモートアクセス通信に推奨されるプロトコルです。SSH は、パスワードを含むすべてのトラフィックを暗号化して、盗聴、接続ハイジャック、およびその他の攻撃を効果的に排除します。SSH ユーティリティには、SSH を使用するファイル転送プログラムである SCP (Secure Copy) が含まれており、セキュアなファイル交換法として推奨されています。

以下のコマンドを使用して、デバイスで必要なサービスを設定します。

```
set system services ftp
set system services telnet
▶ set system services ssh
```

ベストプラクティス

Telnet および FTP はどちらも、純粋なテキスト形式パスワードを使用する従来型のアプリケーションであるため（セキュリティの脆弱性を生む）、SSH（および SCP）の使用を推奨します。Telnet および FTP を使用する予定がない場合には、デバイスでそれらを設定する必要はありません。ただし、一部のユーザーは、FTP を使用して設定テンプレートの保存、ソフトウェアの取得、あるいは他の管理タスクを実行することがあります。

変更のコミット

次の章に進む前に、設定をコミットして、アクティブな設定となるように適用させます。

第 4 章

SNMP の設定

| | |
|--|----|
| <i>SNMP コミュニティーの設定</i> | 36 |
| <i>SNMP トラップの設定</i> | 39 |
| <i>設定グループの適用</i> | 40 |
| <i>SNMP システム詳細の設定</i> | 41 |
| <i>View Based Access Control の設定</i> | 42 |
| <i>変更のコミット</i> | 44 |

この時点で、ベースシステムとユーザーの設定が完了しています。本章および次章では、お使いのデバイスの管理機能の基本設定について説明します。本章（第4章）ではSNMPの設定方法を、第5章ではその他の管理ツールについて説明します。初日の作業の目標は、新しく導入したJunosデバイスをできる限り素早く簡単に既存のネットワーク管理インフラストラクチャに統合することです。

現在、多くのネットワーク管理システムはSNMPベースであるため、どのネットワークデバイスを稼働させる場合にも、SNMPプロトコルのサポートは不可欠な機能です。

Junosは、各種の詳細情報へのアクセスを実現するリモート管理アプリケーションを提供するために、オンボードのSNMPエージェントを備えています。JunosのSNMPエージェントは、SNMPv1、SNMPv2c、およびSNMPv3プロトコルをサポートするため、現在市販されている大半の管理アプリケーションとの相互運用が可能です。業界標準および組織固有のMIB（Management Information Base）が提供されています。

警告！ Junosでは、デフォルトで、SNMPエージェントが無効化されています。本章の手順に従って、デバイスでSNMPを設定してください。

SNMP コミュニティーの設定

JunosでのSNMPエージェントの設定は、ネットワーク内の他の管理デバイスと似たような設定項目によるもので、作業も複雑ではありません。

例えば、Junosでは、SNMPコミュニティー文字列およびトラップ送信先の設定が必要です。コミュニティー文字列は、デバイス（およびそれらで稼働するエージェント）のグループを共通の管理ドメインにまとめるための管理用の名前です（第1章を参照）。基本的に、マネージャとエージェントが同じコミュニティーを共有している場合には、相互通信が可能です。

SNMPコミュニティーによって、利用可能なMIBオブジェクト、それらのオブジェクトに対して有効な操作（読み込み専用、または読み込み/書き込み）、許可されているSNMPクライアントなど、ソースIPアドレスに基づいてメンバーに与えられる許可レベルが定義されます。

試してみよう: オンラインヘルプ機能

作業を開始する前に、運用モードでSNMPに関するオンラインヘルプ項目について確認します。お使いのソフトウェアバージョンでJunosがサポートする設定オプションを確認します。

```
jadmin@juniper1> help reference snmp community
```

トピックまたは設定ステートメントに対する、より詳細な使用ガイドラインを取得します。

```
jadmin@juniper1> help topic snmp community
```

最後に、SNMPステートメントが記述されるすべてのJunosコマンドのリストを取得します。

```
jadmin@juniper1> help apropos snmp
```

設定グループ

共通のSNMP設定をJunos設定グループに含めることで、作業がしやすくなります(第6章を参照)。設定グループを使用することで、カスタマイズした設定ステートメントすべてを一箇所にまとめることができ、さらに、後でデバイス間でテンプレートをコピーできるようになります。

新しい設定グループ *common* を作成するには、設定モードで以下を入力します。

```
▶ edit groups common
```

ここでSNMP設定ステートメントを *common* グループに追加して、後で設定内の目的の箇所に適用させることができます。

注 第4～6章で示す例では、*jadmin* をユーザーアカウントとして使用します。

読み込み専用のSNMPコミュニティを作成するには

1. 第1章で、ネットワークで使用するSNMPコミュニティのコミュニティ文字列として書き取っておいた情報を参照します。この例では、事実上の標準名 *public* を使用して、読み込み専用の限定的なアクセスを与えるコミュニティを作成します。

```
[edit groups common]
```

```
▶ jadmin@juniper1# set snmp community public
```

2. この設定階層の新しい分岐に、設定ステートメントをまとめて記述します。

▶ **edit snmp community public**

3. コミュニティーの許可レベルを定義します。

```
[edit groups common snmp community public]
```

▶ **set authorization read-only**

上記のコマンドによって、*public* コミュニティーは読み込み専用アクセスに制限されます。これにより、*public* コミュニティーに属するSNMP クライアント（SNMP 管理システムなど）は、デバイスのMIB 変数を読み込むことはできますが、設定（変更）することはできません。

4. Junos デバイスのSNMP エージェントとの通信が許可される *public* コミュニティーに属するクライアントのリストを定義します。クライアントは、IP アドレスとプレフィックスで指定します。一般に、このリストには、ネットワーク内のSNMP ネットワーク管理システムまたは管理ネットワークのアドレスが含まれます。以下のステートメントによって、ネットワーク192.168.1.0（および含まれるホスト）が許可されます。

▶ **set clients 192.168.1.0/24**

5. *public* コミュニティー内で許可されていないクライアントを定義します。これらは、IP アドレスと、続く *restrict* ステートメントで指定します。

▶ **set clients 0.0.0.0/0 restrict**

読み込み / 書き込み SNMP コミュニティーを作成するには

Junos デバイスに対して、読み込み / 書き込み アクセスが許可されるメンバーで構成されたコミュニティも定義できます。

1. 前の例に従って、実際にデバイスに設定を入力した場合は、設定階層の1つ上の層で新しいコミュニティを作成します。また、この新しいコミュニティは、*common* という Junos 設定グループ内に設定します。以下のように、編集バナーにより設定のこの分岐に移動していることを確認します。

▶ **jadmin@juniper1# up**

```
[edit groups common snmp]
jadmin@juniper1#
```

2. この例では、事実上の標準コミュニティ文字列 *private* を使用して、デバイス上で動作する SNMP エージェントへの読み込み / 書き込みアクセスが許可されたコミュニティを示します。

▶ **edit community private**

3. 以下のコマンドを使用して、許可レベルおよびクライアントを設定し、アクセスが許可される IP アドレスを指定します。

▶ **set authorization read-write**

▶ **set clients 192.168.1.15/24**

▶ **set clients 0.0.0.0/0 restrict**

注 後述のセクションでは、MIB ビューを定義し、それを SNMP コミュニティに割り当てることで、SNMP MIB ツリーの特定の分岐に対するアクセスを制御する方法について説明します。

SNMP トラップの設定

トラップは、SNMP エージェントからリモートのネットワーク管理システムやトラップレシーバーに送信される未承諾メッセージです。多くの組織では、SNMP トラップとシステムログ収集（第 5 章を参照）を組み合わせたフォルト・モニタリング・ソリューションを採用しています。Junos では、デフォルトで SNMP トラップは転送されないため、SNMP トラップを使用する場合にはトラップグループを設定する必要があります。

トラップグループを設定するには

1. デバイスから送信されるトラップに対して Junos で適用する、固定ソースアドレスを 1 つ作成します。大半の Junos デバイスは多数のアウトバウンド・インタフェースを備えていますが、単一のソースアドレスを使用することで、リモートのネットワーク管理システムではトラップのソースを個別デバイスに関連付けることができるというメリットが得られます。

▶ **admin@juniper1# edit groups common snmp**

[edit groups common snmp]

▶ **admin@juniper1# set trap-options source-address 100**

上記のコマンドで、ステートメントは定義された *common* 設定グループ内に記述されます。そのデバイスから送信されるすべての SNMP トラップのソースアドレスとして、ループバック・インタフェース *100*（第 2 章を参照）の IP アドレスを使用します。

2. 転送されるトラップのタイプと受信するリモート管理システムのターゲット（アドレスなど）をリストで指定するトラップグループを作成します。

▶ **set trap-group managers version v2 targets 192.168.1.15**

上記のコマンドによって、アドレス192.168.1.15のホストにSNMPバージョン2形式による通知を送信する *managers* という名前のトラップグループが作成されます。このステートメントにより、あらゆるカテゴリーのトラップが転送されます。

3. 転送するトラップカテゴリーの特定のサブセットを定義するには、*categories* ステートメントを使用します。

▶ **set trap-group managers version v2 targets 192.168.1.15
categories authentication**

表 4.1 に、Junos で使用される各種トラップカテゴリーを示します。

表 4.1 Junos の SNMP トラップカテゴリー

| 設定オプション | MIB | 説明 |
|----------------|-----------|---------------------------|
| authentication | 標準 MIB-II | エージェント（デバイス）での認証失敗 |
| chassis | ジュニパー社独自 | シャーシおよびルーター環境通知 |
| configuration | ジュニパー社独自 | 設定モード通知 |
| link | ジュニパー社独自 | インタフェース移行（上から下への移行など） |
| rmon-alarm | ジュニパー社独自 | SNMP リモート・モニタリング・イベント |
| routing | ジュニパー社独自 | ルーティングプロトコル通知 |
| startup | 標準 MIB-II | ルーター再起動（ソフト/ウォームおよびフル再起動） |

設定グループの適用

本章では、これまでに、すべての SNMP 設定ステートメントを *common* という名前の *Junos* 設定グループ内に記述してきました。また、後で作業しやすいように、設定グループを使用してきました。この *common* ステートメントは、後で設定内の別の箇所で再利用したり、別のデバイスにコピーすることもできます。

Junos で、*common* 設定グループ内のステートメントを識別できるようにするには、それらを適用することが必要です。

```
▶ jadmin@juniper1# top
```

```
[edit]
```

```
▶ jadmin@juniper1# set apply-groups common
```

この例では、Junos 設定グループ *common* を設定の最上位層で適用して、グループが設定全体に適用されるようにします。

警告! グループステートメントは指定した（およびそれ以下の）階層のみに継承されるため、設定内で設定グループを適用する場所が重要となります。さらに、Junos では適用された順序でステートメントが継承されるため、設定グループの順序も重要です。

確認 トラップ設定はコミットしましたか。コミットした場合には、クイックテストを実行して、SNMPトラップが正しく設定されたことを確認します。この例は、認証失敗トラップを作成するものですが（SNMP エージェントで未知のコミュニティからのリクエストを受信するなど）、他のトラップタイプのスプーフィングも設定できます。

```
jadmin@juniper1> request snmp spoof-trap authenticationFailure  
Spoof-trap request result:trap sent successfully
```

SNMP システム詳細の設定

SNMP を使用して、コンタクト名やデバイスの場所など、基本的な管理詳細情報を保存することもできます。問題のトラブルシューティングや監査を行う際には、リモートの管理システムからこれらの情報を取得できるようになります。SNMP では、これらは MIB-2 (RFC 1213 で定義) システムグループ内の *sysContact*、*sysDescription*、および *sysLocation* オブジェクトと呼ばれています。単純な Junos 設定プロセスを通じて、初期値を直接設定することができます。

システムコンタクト詳細を設定するには

1. システムコンタクト詳細を設定するには、*contact* ステートメントを設定の `[edit snmp]` 階層に記述するか、前述の適切な設定グループに含めます。

```
▶ set contact "For help, please email support@enterprise.com"
```

2. システム詳細を設定します。

▶ **set description "Juniper EX4200"**

3. システムのロケーションを設定します。

▶ **set location "London Corporate Office"**

確認 これらの変更とともに設定をコミットしたら、クイックテストを実行して、システム詳細が正しく入力されたことを確認します。以下の運用モードコマンドを入力します。

```

jadmin@juniper1> show snmp mib walk system
sysDescr.0 = Juniper EX4200
sysObjectID.0 = jnxProductNameEX4200
sysUpTime.0 = 85957438
sysContact.0 = For help, please email support@enterprise.com
sysName.0 = junos
sysLocation.0 = London Corporate Office
sysServices.0 = 4

```

show snmp mib walk system コマンドによって、システムテーブルの MIB ウォークスルーが実行されます (RFC 1213 で定義の MIB-2 より)。Junos の SNMP エージェントは、テーブルの各行および対応する値をプリントアウトすることで、これに応答します。このコマンドは、エージェントでサポートされる MIB ツリーのどの箇所の MIB ウォークスルーも実行できます。

View Based Access Control の設定

SNMPv3 は、MIB ビュー (ビュー・ベース・アクセス・コントロールと呼ばれる。RFC 3415 を参照) という概念を定義する規格です。これにより、エージェントでは、MIB ツリー内の特定の分岐やオブジェクトにアクセスできる対象を詳細に制御できるようになります。ビューとは、明示的に包含または除外される SNMP オブジェクト識別子の集合と名前によって構成されます。ビューは、定義されると、SNMPv3 グループまたは SNMPv1/v2c コミュニティー (複数可) に割り当てられ、そのグループまたはコミュニティーに属するメンバーがアクセスできる (またはできない) エージェントの MIB ツリー部分を自動的にマスキングします。

MIB ビューを作成するには

大半のネットワーク管理システムでは、SNMPv3 を採用しはじめていますが、Junos の SNMP エージェントは、SNMPv1 および SNMPv2c コミュニティーのどちらでも MIB ビューを使用できるという特長があります。以下の例でその方法を示します。

1. Junos CLI の設定モードに切り替え、`view` ステートメントを記述して `ping-mib-view` を作成します。

▶ **set snmp view ping-mib-view oid 1.3.6.1.2.1.80 include**

注 oid ステートメントでは、オブジェクト識別子の先頭のドットは不要です。

`snmp view` ステートメントには、オブジェクト識別子 `.1.3.6.1.2.1.80` の下の分岐が含まれるようになります（すなわち、DISMAN-PING-MIB サブツリー全体。RFC 2925 で定義）。これにより、その分岐の下にあるオブジェクトにはアクセスが許可されます。

▶ 2. 同じ MIB ビューに、2 つ目の分岐を追加します。

set snmp view ping-mib-view oid jnxPingMIB include

注 この例では、オブジェクト識別子は、ドット付きの oid 番号ではなく、オブジェクト識別名で指定されています。

追加の `snmp view` ステートメントによって、上記で作成した MIB ビューが拡張され、ジュニパーネットワークスの組織固有拡張子が `jnxPingMIB` 分岐内にある DISMAN-PING-MIB に含まれるようになります（`.1.3.6.1.4.1.2636.3.7` の下）。

MIB ビューをコミュニティに割り当てるには

MIB ビューを作成したら、アクセスを許可する適切なコミュニティに割り当てるだけです。この例では、DISMAN-PING-MIB 内にエントリーを作成できる読み込み / 書き込みアクセスが与えられる新しいコミュニティ `ping-mib` が作成されます。

1. コミュニティー全体に対して読み込み / 書き込みアクセスを与えます。

▶ **set snmp community ping-mib authorization read-write**

2. 前に作成した MIB ビューを新しいコミュニティに割り当てます。

▶ **set snmp community ping-mib view ping-mib-view**

設定をコミットすると、ping-mib コミュニティーに属するメンバーには、ping-mib-view の下で指定した分岐での読み込み / 書き込みアクセスが与えられます。

変更のコミット

変更をコミットしたら、本書の PDF 版の付録を参照して、記載の参考設定と比較してください。

第 5 章

モニタリングおよびログ収集の使用

| | |
|-------------------------------|----|
| <i>Junos</i> ヘルスモニターの発見 | 46 |
| リモートからのデバイス監視..... | 47 |
| システムログの設定 | 50 |
| Web ベース管理機能の使用 | 56 |
| 作業のレビュー | 59 |

Junos では、SNMP の他に、Junos ヘルスマニター、リモートモニタリング、システムログ収集、および Web ベース管理用の J-Web など、さまざまな管理ツールが提供されています。デバイスを監視および制御するためのこれらのツールを設定すれば、Junos の基本設定は完了します。

Junos ヘルスマニターの発見

組織のネットワークでは、数多くのネットワークデバイスを配備しているため、すべてのポーリングを実行するために一元化されたネットワーク管理システムを採用することが、もはや実用的ではないケースもあります。より拡張性のあるアプローチとしては、何らかの対処が必要などときには、ネットワークデバイス側からネットワーク管理システムに通知する機能を備える方法があります。Junos では、ヘルスマニターと呼ばれる便利なメカニズムを提供しているため、デバイス側で自身の主要な運用基準を監視して、通常の運用パラメータを超えたときにアラームをトリガーすることができます。

Junos ヘルスマニターは、基盤となる RMON (Remote Monitoring) メカニズムを採用し (次章で説明)、事前定義されたオブジェクト・インスタンス群を監視して、さらに基本的な RMON 機能を拡張してダイナミック・オブジェクト・インスタンスをサポートします。事前定義されるオブジェクト・インスタンスには、例えば、ファイルシステム使用率、CPU 使用率、およびメモリ使用率があります。ダイナミック・オブジェクト・インスタンスとしては、実行時にのみ確認されるソフトウェアプロセスやその他のエンティティーなどがあります。Junos ヘルスマニターでは、標準 RMON とは異なり、役に立つモニタリング・アプリケーションを作成するためにデバイス固有の深い知識や経験は必要ありません。一旦ヘルスマニターを設定すれば、イベントがトリガーされるまで特に操作はいりません。

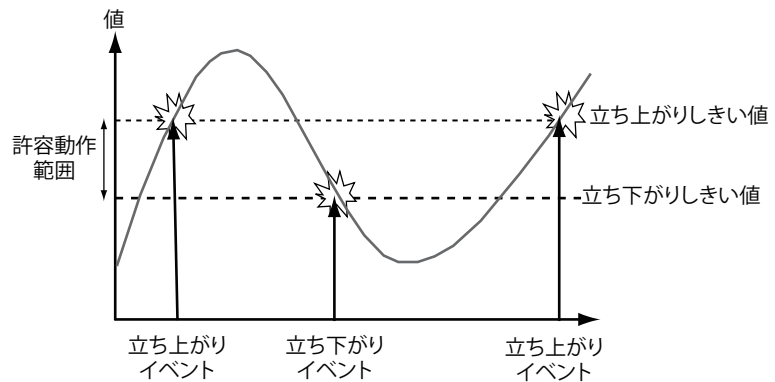
RMON と Junos ヘルスマニターは、どちらも立ち上がりおよび立ち下がりしきい値を使用して、次のページの図 5.1 で示すように、オブジェクトに対して許可される動作範囲を定義します。図 5.1 で示すように、監視対象オブジェクトがしきい値に到達するたびに、イベントがトリガーされます。立ち上がりイベントによってアラームが発生し、立ち下がりイベントによってアラームがクリア (リセット) されます。この方法で、リモートのネットワーク管理システムが処理する上で役立つ情報が得られます。

Junos ヘルスマニターを設定するには

1. `health-monitor` ステートメントを設定の SNMP 階層に記述します。

```
[edit snmp]
set health-monitor
```

図 5.1 RMON しきい値



この設定例では、ヘルスマニターのデフォルト値を使用しています。立ち上がりしきい値は 80%、立ち下がりしきい値は 70% に設定され、ポーリング間隔はデフォルトで 300 秒 (5 分) です。

2. しきい値は、デフォルト値から変更できます。ヘルスマニターで対象オブジェクトを監視するために使用する、立ち上がりおよび立ち下がりしきい値 (パーセンテージ) をより低い値に設定して、間隔 (秒) を調整します。

```
[edit snmp health-monitor]
set rising-threshold 70
set falling-threshold 60
set interval 900
```

注 SNMPトラップを有効にしている場合は、ヘルスマニターによって RMON立ち上がりおよび立ち下がりしきい値イベントが生成されます。Syslogを有効にしている場合、ヘルスマニターではHEALTHMONITOR Syslogタグを使用します。

リモートからのデバイス監視

多くの組織では、SNMP エージェントの RMON 機能を使用して、IP ネットワークの事象を監視しています。例えば、ネットワークでは *RMON* プローブと呼ばれる専用デバイスを使用して、スタティック・レポートングのためにトラフィックの分析をすることもあります。あるいは、IP ルーターやイーサネットスイッチなどのデバイスに組み込まれたエージェントを使用することもあります。Junos では、組み込み RMON エージェ

ント機能を提供しており、RFC 2819 で定義されているリモート・ネットワーク・モニタリング MIB からの RMON アラームやイベントグループをサポートします。

RMON アラームとイベントは、互いに補完し合う機能です。RMON エージェントが変数リストから定期的に統計サンプルを取り、それをしきい値と比較するように、アラームを設定します。監視対象の変数がしきい値に到達すると、Junos では対応するイベントを生成して、デバイスから通知を送信します (SNMP トラップまたは Syslog メッセージ)。

このセクションでは、Junos CLI を介して RMON アラームおよびイベントを設定する方法について説明します。MIB グループでは書き込みが許可されているため、書き込みアクセスを設定すれば、SNMP 管理システムでアラームとイベントの双方をリモートから設定できます (第 4 章の「ビュー・ベース・アクセス・コントロールの設定」を参照)。

例えば、不正なコミュニティを使用して、リモートホストが Junos の SNMP エージェントへクエリー送信を試行する回数を監視するとします。- この回数に応じて、悪意のある攻撃またはネットワーク管理システムの設定における問題が生じている可能性が把握できます。この値は、snmpInBadCommunityNames オブジェクトによって SNMP を介してレポートされます (RFC 1907 で定義の SNMPv2 MIB を参照)。これは整数値であるため、Junos の RMON エージェントによって簡単に監視できます。

RMON アラームを作成するには

RMON アラームを作成するときには、監視対象オブジェクト、モニタリング間隔、しきい値、関連イベントなどのアラームパラメータも定義できます。

1. RMON アラームを [edit snmp] 設定分岐の下に作成します。

```
[edit snmp]
set rmon alarm 100
```

2. RMON アラームのパラメータを調整します。

```
[edit snmp rmon alarm 100]
set variable snmpInBadCommunityNames.0
set sample-type delta-value
set rising-threshold 100
set falling-threshold 90
```

```
set interval 900
set falling-event-index 100
set rising-event-index 100
```

この例では、`snmpInBadCommunityNames` は、Junos デバイスで未知のコミュニティからの、または未知のコミュニティに対する SNMP 要求を受信するたびに増加するカウンターオブジェクトです。デバイスで、最近の 900 秒間 (15 分間) でこうしたリクエストを 100 回以上受信した場合には、アラームによってイベント番号 100 がトリガーされます。

3. アラームに対応するイベントを作成します。

```
[edit snmp]
set rmon event 100

[edit snmp rmon event 100]
set community managers
set description "snmpInBadCommunityName threshold event"
set type log-and-trap
```

このイベントがトリガーされると、SNMP トラップが生成され、トラップグループ *managers* に送信します。また、RMON ログテーブルに新しいエントリーを作成します (詳細については RFC 2819 を参照)。これらのエントリーは、ネットワーク管理システムで独自に、ある一定時間内にデバイスで生成された RMON イベント数に関する統計を収集する場合に役立ちます。

確認 これらの変更をコミットした後で、クイックテストを実行して、RMON アラームとイベントエントリーが正しく入力されたことを確認します。運用モードで以下のコマンドを入力します。

```
jadmin@juniper1> show snmp mib walk rmon
```

`show snmp mib walk rmon` コマンドによって、`rmon` テーブルの MIB ウォークスルーが実行され (RFC 2819 で定義)、各行および対応する値がプリントアウトされます。このコマンドは、Junos エージェントでサポートする MIB ツリーのどの箇所の MIB ウォークスルーも実行できます。

ヒント RMON オペレーションのトラブルシューティングを行うには、ジュニパーネットワークスのエンタープライズ RMON MIB である `jnxRmon` のコンテンツをクエリーします。ジュニパーの MIB によって、例えば

アラームで指定された OID が存在しない場合に発生する可能性がある、トリガーに失敗するアラームエントリーに関する重要な情報が提供されます。

さらに詳しくは Junos では、イベントがトリガーされると、SNMPトラップを生成するだけではありません。例えば、重複を取り除くための複数の一致イベントの相互関連付け、Syslog メッセージの送信（下記を参照）、さらには設定の変更も行えます。イベントがトリガーされたときに Junos でさらに多くのアクションを実行するには、『*Day One: Applying Junos Event Automation*』を参照してください。これは www.juniper.net/dayone から入手できます。

システムログの設定

システムログ（通常、*Syslog* と呼ばれる）は、イベントメッセージをきわめて柔軟に生成および処理する手段で、Unix のようなイベント配信レポート・メカニズムです。Syslog は、従来 Unix 環境で採用されていたもので、分散されたホストによってログホストと呼ばれる中央の Syslog サーバーにメッセージが転送されます。

Syslog メッセージは、イベントのソースを示すファシリティと、その重要度を示すレベルによって分類されます。Junos は、メッセージでレポートされるファシリティとレベルの組み合わせに基づくさまざまなアクションをもって、各イベントに応答できます。こうしたアクションには、イベントメッセージをローカルで表示、メッセージをローカルで保存、サードパーティ製モニタリング・アプリケーションによるリアルタイム分析またはオフライン分析のためにメッセージを標準的なリモート Syslog サーバーに転送することが含まれます。管理者は、フォルトの重複除外や分析を行うために、すべてまたは選択した一部の Junos Syslog イベントメッセージを中央サーバーに転送できます。

ヒント お使いのデバイスで稼働している Junos バージョンでサポートされる Syslog 設定オプションを確認するには、以下の運用コマンドを入力します。

```
admin@juniper1> help reference system syslog
```

Syslog の転送先

Junos オペレーティング・システムでは、表 5.1 で示すように、Syslog メッセージをさまざまな転送先に送信できる柔軟性の高い機能が提供されています。

表 5.1 Syslog 転送先の詳細

| 転送先 | 説明 |
|---------|--|
| console | デバイスのコンソールにログメッセージを表示します。 |
| file | デバイスのハードディスクにローカルでログメッセージを表示します。一般に、ログファイルは /var/log ディレクトリに保存されます。 |
| host | さらに処理を行うために、ログメッセージを別の Syslog サーバー（一般に、別の Junos デバイスまたは Unix マシン）に転送します。 |
| user | ユーザーがログインしている pty (pseudo-teletype) ターミナルでログメッセージを表示します。 |

本書で例を示すように、これらのメッセージを 4 つの送信先すべてに転送することもできます。

メッセージのファシリティおよびレベル

システムのログ収集を設定する際には、収集対象のメッセージ、使用するファシリティ（ソース）、ネットワークにとって重要なレベル（重要度）も選択します。

Junos では、各メッセージを生成するソフトウェアプロセスを指定するために、各種 Syslog 機能が提供されます。監視対象のファシリティがはっきりと確定できない、またはどのファシリティが重要であるか不明な場合には、すべてを監視対象として、後で変更することもできます。

各ファシリティでは、レベル（重要度）が異なる各種メッセージを生成できます。例えば、即座にオペレータ対応が必要な重要なイベントが発生するファシリティに加えて、即座のアクションが必要ではない非重要イベントの発生を示す情報メッセージを生成できます。Junos でサポートされる全 Syslog レベルのリストを表 5.2 に示します。

表 5.2 Syslog レベル

| レベル数値 | レベル | 説明 |
|-------|-----------|--|
| - | なし | 対応するファシリティから転送先へのログの無効化 |
| 0 | emergency | ソフトウェア・コンポーネントの機能停止を招くシステムパニックまたはその他の状況 |
| 1 | alert | 破損したシステムデータベースなど、直ちに修復が必要な状況 |
| 2 | critical | 物理的なエラーなど重大な問題がある状況 |
| 3 | error | emergency、alert、critical レベルのイベントよりも、一般的に深刻度が低いエラー状況 |
| 4 | warning | モニタリングの必要性がある状況 |
| 5 | notice | エラーではないが、特別な処理が必要となる可能性がある状況 |
| 6 | info | 対象のイベントまたは非エラー状況 |
| 7 | any | ファシリティからの全レベルのメッセージ |

Syslog レベルを設定する際には、処理するログメッセージの最低レベルを指定するマスクを定義します。例えば、warning レベルのすべてのログメッセージを取得するよう指定した場合、Junos ではそのレベル以上のログメッセージを収集するため、error、critical、alert、および emergency レベルのメッセージが通知されます。

さらに詳しくは Syslog 設定の基本情報については、技術マニュアル『*System Basics Configuration Guide*』を参照してください。Junos でサポートされる全メッセージリストについては、『*System Log Messages Reference*』を参照してください。どちらも www.juniper.net/tech-pubs/ から入手できます。

ファイルへのメッセージの送信

Syslog の概要と Junos での Syslog の機能について説明しました。初日に実施する Syslog 設定の中で最も簡単かつ役立つものは、ローカルファイルへのメッセージの送信です。メッセージの監査証跡を保持する必要がある場合、または後で分析するためにメッセージを保存する場合には、ローカルでメッセージを保存することが役立ちます。

Syslog ファイルを設定するには

1. file ステートメントを Junos 設定の [edit system syslog] 階層に記述します。

```
▶ jadmin@juniper1# edit system syslog file all-messages
```

```
[edit system syslog file all-messages]
```

```
▶ jadmin@juniper1# set any warning
```

```
▶ jadmin@juniper1# set authorization notice
```

この例では、ファイル *all-messages* がローカルディレクトリ */var/log* に作成されます。ここには、すべてのファシリティからの warning レベル以上のメッセージが保存されます。また、notice レベル以上のユーザーログインなどの認証メッセージが保存されます。Junos では、ログファイルの量が増えるに従って、自動的にそれらを定期的にアーカイブ化します。

注 アーカイブ化動作をカスタマイズするには、Junos 設定の [system syslog archive] 設定を変更します。ただし、これは必ずしも初日に実行する必要はありません。

2. 設定をコミットしたら、運用モードで、ローカルファイルに保存されたログメッセージを参照できます。

```
jadmin@juniper1> show log all-messages | last 10
```

ここでは、last コマンド修飾子によって、ファイル *all-messages* 内の最後の 10 行（最近の 10 イベント）のみが画面上に表示されるよう指定されています。

ターミナルへのメッセージの転送

重要なメッセージを受信して、オペレータによる即座の処置が必要な状況では、オペレータの画面にメッセージを表示させて注意を引くことが最良の方法です。Junos では、ログインしているユーザーにメッセージを表示するとともに、デバイスのコンソールにもメッセージを表示させることができます。

メッセージを送信するには

1. ユーザーにメッセージを転送するには、以下の設定手順に従ってください。ユーザー名を [system syslog user] 階層に入力します。

```
▶ set system syslog user * any emergency
```

```
▶ set system syslog user jadmin any critical
```

1つ目の `set` コマンドによって、すべてのユーザーに emergency ログメッセージが転送されます。これは、Junos ワイルドカード文字 * によって示されています。2つ目の `set` コマンドによって、critical レベル以上のログメッセージが、ユーザー `jadmin` がログインしている画面に転送されます。これは、リモートにいる管理者に重要なメッセージを転送する効果的な方法です。

2. 別の方法としては、デバイスのコンソール画面にログメッセージを転送する方法があります。以下の例では、すべてのファシリティからの error レベル以上のログメッセージがデバイスのコンソールに転送されます。

▶ `set system syslog console any error`

リモートサーバーへのメッセージの転送

Junos では、1つまたは複数のリモートデバイスに Syslog メッセージを転送することもできます。多くの組織では、フォルト・モニタリング・ソフトウェアを使用して Syslog メッセージを受信および解釈するため、デバイスでローカルにログメッセージをレポートするだけでなく、リモートのフォルト・モニタリング・ソフトウェアにも各メッセージのコピーを転送するように設定することが理にかなっています。

ここでは、ネットワークに `loghost` という名前のデバイスがあり、サードパーティ製のフォルト・モニタリング・システムが稼働していると想定します。適切なファシリティおよびレベルを設定の `[edit system syslog host]` 階層で指定します。

▶ `set system syslog host loghost any notice`

この例では、すべてのファシリティからの notice レベル以上のログメッセージが `loghost` というリモートホストに転送されます。

ログメッセージ形式のカスタマイズ

多くの組織では、市販のフォルト・モニタリング・ソフトウェアを導入しています。これらのソフトウェアパッケージは、IP ネットワークに配備されたすべてのデバイスで生成される大量の Syslog メッセージを処理できるだけの拡張性があります。こうした製品の多くは、取るべきアクションを決定するために、ルールベースエンジンを介したフィルタリングによって受信メッセージをすべて解析します。このようなシステムは柔軟性が高い反面、設定は複雑になることがあります。

Junos は、サードパーティ製のフォルト・モニタリング・システムとの統合を容易にします。ログメッセージをカスタマイズできるため、受信側で必要となる設定作業と処理は少なくなります。

プレフィックス文字列

ここでは、ネットワークに 500 台以上の IP デバイスが配備されており、すべてのデバイスで Syslog メッセージが生成されるケースを想定します。Junos デバイス、Unix サーバー、他のベンダー製のネットワークデバイスが混在しています。大半の市販フォルト・モニタリング・アプリケーションでは、カスタムの規則を使用して Syslog メッセージを解析できますが、ベンダー固有の規則の構築は困難で時間がかかる作業です。このような状況では、Junos から送信されるすべての Syslog メッセージの先頭に特定の文字列を付加して、それらのメッセージをより簡単にリモートで照会および解析できるようにする方法もあります。

以下のコマンドを使用して、文字列 *Junos* を各 Syslog メッセージの先頭に付加してから、リモートデバイス *loghost* に転送します。

► **set system syslog host loghost log-prefix Junos**

これにより、固定プレフィックス *Junos* がデバイスから送信される各 Syslog メッセージに付加されます。このプレフィックスを使用することで、リモートのフォルト・モニタリング・アプリケーションでは、デバイスから送信されるすべてのログメッセージを簡単に特定できるようになります。

優先情報の追加

イベントのファシリティおよび重要度レベルを合わせたものを優先度と呼びます。優先度は、Syslog サーバーでは把握できますが、メッセージテキスト自体に表示されることはほとんどありません。そのため、特にメッセージがリモートホストに転送される場合、または他の優先度を持つメッセージとともにローカルでファイルに保存されている場合には、メッセージの優先度を識別することが困難ことがあります。

イベント優先度をメッセージテキストに挿入するには、`explicit-priority` ステートメントを `[system syslog host]` または `[system syslog file]` 階層に記述します。

► **set explicit-priority**

`explicit-priority` ステートメントによって、各メッセージの先頭に「ファシリティ - レベル」という形式で優先度が挿入されます。このケースでは、レベルは表 5.2 で示す数値で表されています。

ファシリティ・オーバーライド

一部のサードパーティ製 Syslog モニタリング・アプリケーションは、特定のファシリティを持つメッセージをリスンします。Junos では、リモートシステムからは特定できない多数のファシリティからのメッセージを生成できるため、元の値をオーバーライドすることで統一が容易になることがあります。

元の Syslog ファシリティをオーバーライドするには、Syslog ホストの設定時に `facility-override` ステートメントを使用します。

```
[edit system syslog host loghost]
▶ jadmin@juniper1# set facility-override local17
```

ベストプラクティス 一般に、「localX」ファシリティなど、リモートシステムで未使用の代替ファシリティを指定します。また、サードパーティ製 Syslog アプリケーションで、目的の方法でメッセージを処理するように設定する必要があります。

さらに詳しくは Syslog は、Junos でネットワークイベントのログ収集を行うために採用されたメカニズムの1つです。他には、トレースログ（トレースオプション）というツールもよく使用されます。トレースログでは、送受信されるルーティングパケットなど、特定のプロセスを追跡できます。トレースオプションは、他のシステムにおけるデバッグ出力と似ています。トレースログの詳細については、『*System Basics Configuration Guide*』を参照してください。これは www.juniper.net/techpubs から入手できます。

Web ベース管理機能の使用

ネットワークデバイスの監視、管理、およびトラブルシューティングを行うためのメインアプリケーションとして、多くの人は Web ブラウザーを選択します。Junos では、豊富な機能を備えた *J-Web* という Web ベースインターフェースが提供されています。

このセクションでは、初日に知っておくべき基本手順、すなわち *J-Web* のインストール状況の確認方法、インストール方法、および設定方法について説明します。

J-Web のインストール

J-Web は、EX シリーズ イーサネットスイッチ、J シリーズ ルーター、および SRX シリーズ サービス・ゲートウェイにあらかじめインストールされている市販製品です。M シリーズおよび MX シリーズ ルーターなど、他のプラットフォームでは、ソフトウェアパッケージを入手してインストールする必要があります。このセクションでは、J-Web の入手方法とインストール方法について説明します。

J-Web がインストールされているかを確認するには

以下の方法で、お使いのデバイスにあらかじめ J-Web がインストールされているか、およびインストールされているバージョンを確認します。

1. 以下の運用モードコマンドを実行します。

```
admin@juniper1> show version detail | match Web
```

ヒント match ステートメントは正規表現をサポートしているため、大量の出力を減らす柔軟性の高い方法です。

J-Web がインストールされている場合には、show version によって「Junos Web Management」とそのバージョン番号が表示されます。この場合、このセクションの残りを読まずに「*J-Web の設定*」に進んでください。

2. J-Web がインストールされていない場合は、入手してインストールする必要があります。稼働している Junos のバージョンを確認して、それと一致するバージョンの J-Web をインストールする必要があります。show version コマンドによって、必要な情報を取得できます。

```
admin@juniper1> show version
Hostname: junos
Model: m10
Junos software release [9.4R2.9]
```

J-Web パッケージをインストールするには

J-Web ソフトウェアパッケージを販売店から入手するか、ジュニパーネットワークスのサポート Web サイト www.juniper.net/customers/csc/software の Junos ソフトウェア・ダウンロード・セクションから入手してください。

Junos では、リモートサーバーからパッケージをプルすることもできます。この場合は、`request system software` コマンドを使用して、パッケージの場所を URL で指定します。以下の例では、Junos デバイスにパッケージをプルするためのプロトコルとして FTP を使用します。

```

jadmin@juniper1> request system software add ftp://ftp:secret@server/pub/junos/jweb-
9.4R2.9-signed.tgz
Installing package 'ftp://ftp:secret@server/pb/junos/jweb-9.4R2.9-signed.tgz' ...
Verified jweb-9.4R2.9.tgz signed by PackageProduction_9_4_0
Adding jweb...
Available space:671134 require: 8226
Mounted jweb package on /dev/md9...
Verified manifest signed by PackageProduction_9_4_0
Executing /packages/mnt/jweb-9.4R2.9/mount.post...
Reloading /config/juniper.conf.gz ...
Activating /config/juniper.conf.gz ...
mgd:commit complete
Restarting mgd ...
Saving package file in /var/sw/pkg/jweb-9.4R2.9-signed.tgz ...
Saving state for rollback ...

```

```

WARNING:cli has been replaced by an updated version:
CLI release 9.4R2.9 built by builder on 2009-03-25 07:29:27 UTC
Restart cli using the new version ?[yes,no] (yes)

```

```

Restarting cli ...
jadmin@juniper1>

```

J-Web の設定

Junos デバイスに J-Web パッケージをインストールしたら、設定作業に進みます。J-Web は、デフォルトでは設定および実行されないため、Junos CLI を介して初期設定を完了させる必要があります。これは、どの Junos デバイスでも必要です。

▶ **set system services web-management http**

設定の変更内容をコミットしたら、J-Web インタフェースを介して Junos OS にアクセスできます。Web ブラウザーに、Junos デバイスのホスト名または IP アドレスを URL として入力します。

J-Web インタフェースの詳細な操作方法については、『*J-Web Interface User Guide*』を参照してください。これは www.juniper.net/techpubs/ から入手できます。J-Web は、デバイスごとに若干の違いがあるため、お使いのプラットフォームに該当する資料を入手してください。

作業のレビュー

本章で、お使いのデバイスの基本設定は完了します。第 6 章では、デバイスでの設定の移動、追加、および変更を容易にする追加のコマンドやショートカットについて説明します。

お使いのデバイスで、矢印 ▶ で示されるコマンドを入力した場合には、本書の PDF 版の付録に掲載されている参考設定と一致するはずです。この PDF 版は、無料で www.juniper.net/dayone から入手できます。

第 6 章

設定テンプレートおよびその他のショートカットを使用した作業

| | |
|-------------------------|----|
| <i>set</i> コマンドの表示..... | 62 |
| 変更作業の短縮..... | 63 |
| グループの定義..... | 66 |
| 設定テンプレートの使用..... | 69 |
| 作業内容の保存..... | 70 |

本章では、コマンドライン・インタフェースで設定を作成および変更するとき、時間を大幅に節約できるような便利な手法について説明します。これらの手法を用いることで、設定の他の箇所を設定ステートメントを再利用するだけでなく、他のデバイスでも設定ステートメントを再利用することができます。例えば、設定グループを使用して同一設定内で再利用する共通要素を設定および適用したり、設定テンプレートを使用して別のデバイスの設定で使用した共通要素を読み込んだりすることができます。こうしたショートカットは、設定の編集にかかる時間を短縮するとともに、コマンドを繰り返し入力するときに生じる可能性があるミスを防ぐこともできます。

いくつかの例では、一般的に初日に実施する作業の範囲を超えているものもありますが、Junosの他の高度な機能を紹介する目的で示してあります。

ヒント 本書では、コマンドを簡単に参照できるように、コマンドをそのまま左マージンのセクションタイトルとして記載しています。

set コマンドの表示

最も頻繁に使用し、最も簡単な設定ショートカットは、機能すると分かっている既存のコマンドセットを表示し、それらを別の箇所でも再利用するものです。

```
admin@juniper1> show configuration interfaces ge-0/0/1 | display set
set interfaces ge-0/0/1 unit 0 family inet address
192.168.100.1/30
```

設定階層のどの位置に入力した set コマンドでも、show configuration | display set コマンドを使用して設定モードの最上位層から入力したようにリスト表示することができます。このコマンドを使用して、設定全体または上記の例のように設定の一部のみを表示できます。

表示されたリスティングで、再利用する set コマンドを探し、キーボードの Ctrl+C などのコマンドを使用してコピーします。次に、コマンドの再利用先にカーソルを移動して、貼り付けます（キーボードの Ctrl+V コマンドを使用）。出力全体を切り取って、貼り付けることもできます（改行は各行末尾に埋め込まれる）。Enter を押す前であれば、IP アドレスの変更など、必要に応じてコマンドラインを変更することもできます。

ショートカット `top` コマンドを他のコマンドと組み合わせて、設定内で現在作業している場所にかかわらず、階層の最上位層から新しいステートメントを入力できます。以下に例を示します。

```
top set interfaces ge-0/0/1 unit 0 family inet address
192.168.100.1/30
```

変更作業の短縮

ネットワークは、新しいビジネスニーズに対応するために頻繁に変更が必要となる、複雑で動的なシステムです。Junos では、こうした既存の設定変更にかかる作業時間を短縮する、便利なコマンドを多数提供しています。

Rename

Junos 設定内のあるセクションの名前を変更するケースを考えます。例えば、新しいポリシーに合わせて従来の名前付け規則を変更するものとします。ここでは、`ge-0/0/0` を新しい名前規則に準じて `ge-1/0/0` に変更すると想定します。現在の設定（一部）は、以下のとおりです。

```
admin@juniper1# show interfaces ge-0/0/0
unit 0 {
    family inet {
        address 100.100.100.1/24;
    }
}
```

インタフェースの名前変更は、`rename` コマンドを使用して、1つの手順で完了できます。

```
admin@juniper1# rename interfaces ge-0/0/0 to ge-1/0/0
```

確認 `show` コマンドを使用すると、変更が適用されたことを確認できます。

```
admin@juniper1# show interfaces ge-1/0/0
unit 0 {
    family inet {
        address 100.100.100.1/24;
    }
}
```

注 この場合、Junos の `rename` コマンドは、Unix の `mv` (move) コマンドと同様に機能して、元のセクションのコピーを作成するのではなく、元のセクションの名前を変更します。

Copy

Junos では、`copy` コマンドを使用して設定の一部分のコピーを作成することもできます。ここでは、ローカルユーザー `logintemplate` に対するテンプレートを作成し、チームに最近参加した新しいユーザー `joe` に対してコピーを作成すると想定します。

```
admin@juniper1# show system login user
user logintemplate {
    full-name "Generate network operations user";
    class netops;
    authentication {
        encrypted-password "$1$Naeta3Iw$./sgTTPK0NoH0PJdsXvP6.";
    ## SECRET-DATA
    }
}
```

`copy` コマンドを使用して、新しいユーザー `joe` に対して、このテンプレートのコピーを作成します。

```
admin@juniper1# edit system login
admin@juniper1# copy user logintemplate to user joe
```

確認 Junos で新しいローカルユーザーが作成されたことを確認します。

```
admin@juniper1# show
user logintemplate {
    full-name "Generate network operations user";
    class netops;
    authentication {
        encrypted-password "$1$Naeta3Iw$./sgTTPK0NoH0PJdsXvP6.";
    ## SECRET-DATA
    }
}
user joe {
    full-name "network operations user";
    class netops;
    authentication {
        encrypted-password "$1$Naeta3Iw$./sgTTPK0NoH0PJdsXvP6.";
    ## SECRET-DATA
    }
}
```

後は、`joe` のパスワードを変更するだけで、設定が完了します。

Replace

他にも便利なコマンドとして、`replace` があります。これは、設定内の任意の文字列を別の文字列で置き換えます。ここでは、設定のプロトコル分岐に OSPF を設定しており、そこでインタフェース `ge-0/0/0` が参照されていると想定します。以下にその設定を示します。

```
admin@juniper1# show interfaces ge-0/0/0
unit 0 {
    family inet {
        address 100.100.100.1/24;
    }
}
admin@juniper1# show protocols ospf
area 0.0.0.0 {
    interface ge-0/0/0.0;
}
```

この例では、`replace` コマンドを使用して、設定全体にわたって、このインタフェースを新しい名前付け規則で置き換えることができます。

```
admin@juniper1# replace pattern ge-0/0/0 with ge-1/0/0
```

Insert

`insert` コマンドを使用することで、ある順序で並べられた項目の前または後ろに設定ステートメントを挿入できます。これは、ファイアウォールフィルタやルーティングポリシーを設定しており、それらの項目の順序を変更するケースで役立ちます。ここでは、以下のポリシーが設定されていると想定します。

```
[edit policy-options policy-statement multiterm]
admin@juniper1# show
term reject {
    then reject;
}
term accept {
    from protocol bgp;
    then accept;
}
```

これを BGP インポートまたはエクスポートポリシーに適用すると、`reject` 項目が `accept` 項目よりも上位にあり、上位の項目から順に処理されるため、すべてのルートが拒否されます。調整するには、`insert` コマンドを使用します。

```
[edit policy-options policy-statement multiterm]
jadmin@juniper1# insert term accept before term reject
```

ポリシーの順序に応じて、before または after を挿入できます。

さらに詳しくは ポリシーの設定方法については、『*Policy Framework Configuration Guide*』を参照してください。これは www.juniper.net/techpubs から入手できます。

グループの定義

インタフェース・パラメータなど、設定内の多くの箇所で繰り返されるものについては、設定グループを用いて作業を短縮することができます。設定グループとは、設定の複数の箇所に適用できるステートメントセットです。これらを使用して、より小さく、より論理的な構造の設定ファイルを作成できます。初回の設定作業も短縮できますが、変更する場合にも一箇所で行い、それを他の箇所に適用できます。

第 4 章で、すでに SNMP 管理用のグループの設定方法について説明しました。このセクションでは、インタフェースの設定でグループを使用する例を 2 つ示します。

グループステートメントは指定した（およびそれ以下の）階層のみに継承されるため、設定内で設定グループを適用する場所が重要になります。さらに、Junos では適用された順序でステートメントが継承されるため、設定グループの順序も重要です。

インタフェースグループの作成

ワイド・エリア・リンクの多くは、光ファイバー通信用の SONET/SDH 規格に基づいています。SONET インタフェースはすべて SDH フレーミングが必要となり、RFC 2615 で定義されたパラメータに準拠する必要があります。ここでは、以下のように多数の SONET/SDH インタフェースが設定されていると想定します。

```
jadmin@juniper1# show interfaces so-0/0/0
unit 0 {
  family inet {
    address 192.168.1.1/30;
  }
}
```

インタフェースグループを設定および適用するには

以下のコマンドによって、グループ `sdh` が設定され、設定全体にわたり適用されます。

1. グループを設定して、必要なパラメータを設定します。

```
set groups sdh interfaces <so-*> framing sdh
set groups sdh interfaces <so-*> sonet-options rfc-2615
```

ショートカット 上記の設定ステートメントでは、`<so-*>` は、すべてのSONET/SDHインタフェースのワイルドカードとして機能します。これを適用すると、その階層内のすべてのインタフェースがこれらの設定を継承します。

2. 次に、設定内の目的の箇所にグループを適用します。設定ツリーの最上位層から `set apply-groups` コマンドを適用すると、グループが設定全体にわたって適用されます。

```
set apply-groups sdh
```

警告! Junos 設定グループを使用する場合、デフォルトでは、`show` コマンドによって現在作業している分岐以下の設定のみが表示されます。リスティングには、設定の他の箇所に適用された設定グループから継承された設定は表示されません。例えば、以下の `show` コマンドを使用すると、適用しても `sdh` グループは表示されません。

```
admin@juniper1# show interfaces so-0/0/0
unit 0 {
  family inet {
    address 192.168.1.1/30;
  }
}
```

ヒント `show` の出力を `display inheritance` オプションを介してパイプし、適用された `sdh` グループとともに設定全体を表示します。

```
admin@juniper1# show interfaces so-0/0/0 | display inheritance
##
## 'framing' was inherited from group 'sdh'
##
framing {
  ##
  ## 'sdh' was inherited from group 'sdh'
  ##
  sdh;
}
##
```

```

## 'sonet-options' was inherited from group 'sdh'
##
sonet-options {
  ##
  ## 'rfc-2615' was inherited from group 'sdh'
  ##
  rfc-2615;
}
unit 0 {
  family inet {
    address 192.168.1.1/30;
  }
}

```

ショートカット 記述されているコメントを表示させると、設定が読みにくくなる場合があります。この場合、`except` コマンドを使用して、リスティングでコメントを非表示にします。

```

jadmin@juniper1# show interfaces so-0/0/0 | display inheritance
| except ##
framing {
  sdh;
}
sonet-options {
  rfc-2615;
}

unit 0 {
  family inet {
    address 192.168.1.1/30;
  }
}

```

適用したグループを除外するには

このセクションの例では、全体に適用したグループを設定の特定のセクションから除外する方法について説明します。

ここでは、ネットワークで ISO および MPLS プロトコルを使用するため、設定の最上位層にグループを適用したと想定します。そのため、これらのファミリーをインタフェースごとに設定する必要がないこととなります。ワイルドカードである `*` を使用することで、プロトコルが全体にわたり設定されるようになります。

```

groups {
  isis-mpls {
    interfaces {
      <*-*> {
        unit <*> {
          family iso;
          family mpls;
        }
      }
    }
  }
}

```



```
jadmin@juniper1# save common-template
Wrote 23 lines of configuration to 'common'
```

この例では、ファイル `common-template` が作成され、そこには [edit groups common] 階層以下に含まれるタイムスタンプやオープニング・グループ・ステートメントなどすべての情報が含まれます。ファイルは、デバイス内のユーザーのホームディレクトリ内にローカルで保存されます。 /var/home/jadmin.

ヒント テンプレートをFTPサーバーに保存すると、他のデバイスからアクセスしやすくなります。

テンプレートを読み込むには

設定テンプレートをファイルとしてローカルに保存した場合は、設定モードの最上位層から load コマンドを使用して、デバイスの設定に読み込むことができます。

```
[edit]
jadmin@juniper1# load merge common-template
load complete
```

この例では、load コマンドに merge 引数が与えられているため、Junos では現在の候補設定を読み込んだファイルの内容とマージします。Junos では、テンプレート・ステートメントを保存したとおりに、デバイス設定の [edit groups common] 階層に追加します。

ヒント 上記の例では、テンプレートはファイル `common-template` にローカルで保存されているものと想定しています。テンプレートがリモートのFTPサーバーに保存されている場合は、以下のように保存場所を URL で指定します。

```
jadmin@juniper1# load merge ftp://user:password@server/junos/
templates/common-template
```

ファイルを読み込んだ後で、新しい設定をコミットしてください。

作業内容の保存

このセクションでは、候補設定またはアクティブな設定を保存する方法を、さらにいくつかの例で示します。どちらの設定ファイルを保存しているかを混乱しないように、*候補* と *アクティブ* の両用語を 下線付き で示してあります。

このセクションで示すコマンド例では、設定全体または設定の一部をファイルとして作成し、それをローカルまたは他のデバイスに保存する方法を示します。さらに、Junos で アクティブ な設定ファイルを指定した間隔で、またはコミット時に自動的に保存するよう設定することもできます。

さらに詳しくは『*Day One: Junos CLI の探究*』では、サーバーへファイルをアップロードおよびサーバーからファイルをダウンロードするための運用モードでのファイルコマンドについて説明しています。

候補ファイルをローカルで保存するには

設定で定義されているすべての Junos ユーザーには、デバイス内に個々のホームディレクトリが以下の形式で与えられます。/var/home/username。ユーザーのホームディレクトリに 候補 設定を保存するには、運用モードで `save` でファイル名を指定して保存します。

```
admin@juniper1# save router-config
Wrote 206 lines of configuration to 'router-config'
```

確認 デバイスのホームディレクトリを確認するには、運用モードで `file list` コマンドを使用します。

```
admin@juniper1# run file list
router-config
```

`file show` コマンドを使用して、保存した設定ファイルの実際の内容を参照します。

```
admin@juniper1# run file show router-config
< 設定ファイルの内容がここに表示される >
```

候補設定の一部を保存するには

`save` コマンドを設定の深い階層で使用して、コマンドブロックとして 候補 設定の一部を保存し、これらのコマンドブロックをネットワーク内の別のデバイスで再利用します。例えば、ネットワーク内のすべてのスイッチについて、同じシステムログイン情報を使用します。

```
[edit system login]
admin@juniper1# save system-login
Wrote 29 lines of configuration to 'system-login'
```

設定ファイルをリモートで保存するには

以下の例では、候補 ファイル全体が、リモートサーバー `remot` に保存されます。ここでは、転送に SCP (Secure Copy) を使用します。

```
[edit]
admin@juniper1# save scp://admin@remot
The authenticity of host 'remot (172.26.25.4)' can't be established.
RSA key fingerprint is 13:ff:78:8a:fd:38:8f:d8:94:5e:39:9f:60:eb:9b:b5.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'remo,172.26.25.4' (RSA) to the list of known hosts.
admin@remot's password:
tempfile                               100% 4482    4.4KB/s   00:00
Wrote 270 lines of configuration to 'scp://admin@remot'
```

ヒント アクティブな設定を保存するには、運用モードの `file copy` コマンドを使用できます（『*Day One: Junos CLI の探究*』を参照）。あるいは、オプションとして、パイプを使用して、運用モードの `show` コマンドの出力を保存できます。以下のコマンドを使用することで、アクティブな設定のリスティングを作成してそれを保存し、`save` ステートメントにパイプして、`Tuesday-archive` という名前のローカルで保存したファイルを作成できます。

```

jadmin@juniper1# run show configuration | save Tuesday-archive
Wrote 115 lines of configuration to 'Tuesday-archive'

```

アクティブな設定を指定間隔で自動的に保存するには

毎週火曜日にログインして、Junos のアーカイブのコピーを作成するケースを想定します。火曜日だけでなく、これを毎日 Junos で自動的に実行できれば、非常に便利です。この場合、最新のアクティブな設定ファイルを自動的に保存して、リモートホストに転送するように Junos を設定することができます。

1. アーカイブホストまたはホストのセットを設定してある場合、以下のコマンドを使用して、Junos から設定を送信する各ホストの URL を指定します。

```

set system archival configuration archive-sites ftp://
jadmin:password@remot/archives

```

2. 次に、Junos でアクティブな設定を保存する間隔を秒で指定します。指定できる間隔は、15 分 (900 秒) から 48 分 (2880 秒) までです。

```

set system archival configuration transfer interval 1440

```

この例では、Junos でアクティブな設定のコピーを 1440 分ごと（24 時間、すなわち 1 日 1 回）に、`archives` の `ftp remot` サーバーに送信します。

アクティブな設定をコミット時に自動的に保存するには

別のオプションとして、コミットするたびに（すなわち、設定を変更するたびに）アクティブな設定をアーカイブするよう設定することもできます。

1. 保存したアクティブな設定のファイル送信先を設定します。

```

set system archival configuration archive-sites ftp://
jadmin:password@remot/archives

```

2. コミットするたびにアクティブな設定を転送するよう設定します。

```

set system archival configuration transfer-on-commit

```

あるユーザーがデバイスに対する変更をコミットすると、最新の アクティブ な設定のコピーがリモート・アーカイブ・ホストに転送されて保存されます。

設定の読み込み

load コマンドを使用して、保存した設定ファイルを候補に挿入することができます。ローカルファイル、リモートマシン上のファイル、またはターミナルエミュレータのキャプチャーウィンドウから設定全体または設定の一部を読み込むことができます。Junos で読み込んだファイルを候補に統合する方法を厳密に管理できる各種オプションが提供されています。

Load override

load override コマンドを使用して、現在の候補設定を以前保存したファイルで完全に置き換えることができます。設定モードの最上位層から load override コマンドを入力する必要があります。

この例では、前セクションで保存した `router-config` を、デバイスの `/var/tmp` ディレクトリに読み込み、既存の設定を完全に上書きします。

```

jadmin@juniper1# load override /var/tmp/router-config
load complete

[edit]
jadmin@juniper1# commit
commit complete

```

警告! 新しく読み込んだ設定ファイルは、候補設定のみを置き換えます。実行中のアクティブなファイルにするには、commit コマンドを入力しなければなりません。

Load merge

設定を置き換える代わりに、デバイスに設定の一部を追加するケースを想定します。例えば、load merge コマンドを使用して、デバイスのローカルディレクトリに以前保存したシステムログイン設定ステートメントを追加することができます。

```

[edit]
jadmin@juniper1# load merge system-login
load complete

```

この例では、デバイスに `system-login` ファイルが読み込まれ、設定ツリーの最上位層から候補設定ファイルにマージされます。設定モードの最上位層から load merge コマンドを入力する必要があります。Junos では、これらのステートメントを保存したとおりに、設定の [edit system login] 階層に追加します。

- 注 `save` コマンドを使用すると、必ず設定の `root` から階層参照がキャプチャーされるため、`load merge` コマンドによって、ステートメントは保存した場所とまったく同じ場所に追加されます。保存したステートメントを、設定内の別の場所に追加する場合は、以下のセクションで説明する `relative` オプションを使用して、保存したファイルの設定ステートメントを Junos で読み込む場所を指定することができます。

Load merge terminal

ある Junos デバイス上ですでに設定した Syslog 設定をコピーして、別のデバイスの設定内に貼り付けるケースを想定します。

```
system {
  syslog {
    user * {
      any emergency;
    }
  }
  host 172.26.27.8 {
    any notice;
    authorization info;
    interactive-commands info;
  }
  file messages {
    any notice;
    authorization info;
  }
}
```

まず、`Ctrl+C` などのコピーコマンドを使用して、ソースから設定の一部をコピーします。次に、貼り付け先のルーターで `load merge terminal` コマンドを入力して、`Ctrl+V` などの貼り付けコマンドを使用してコピーしたものを貼り付けます。

```
[edit]
jadmin@juniper1# load merge terminal
[Type ^D at a new line to end input]

system {
  syslog {
    user * {
      any emergency;
    }
  }
  host 172.26.27.8 {
    any notice;
    authorization info;
    interactive-commands info;
  }
  file messages {
    any notice;
    authorization info;
```

```
}  
  }  
}  
^D  
load complete
```

警告! ターミナルコマンドを使用する場合は、Ctrl+D (^D) でターミナルを終了します。

新しい Syslog ステートメントを設定に適用できるようになります。

```
jadmin@juniper1# commit
```

Load merge terminal relative

ここでは、設定の一部を、Junos 設定ツリーの分岐の深い階層にマージするケースを想定します。この場合は、`relative` キーワードを `load merge` コマンドの末尾に追加します。

例えば、前の例の Syslog ホストのみをコピーするには、Ctrl+C などのコピーコマンドを使用してホストの詳細をコピーします。このとき、閉じ波括弧を記述し忘れないでください。

追加先のデバイスで、Junos 設定内の目的のセクションまで移動します。

```
jadmin@juniper1# edit system syslog  
[edit system syslog]  
jadmin@juniper1#
```

次に、前と同じように `load` コマンドを発行します。ただし、ここでは `relative` キーワードを末尾に加えます。

```
jadmin@juniper1# load merge terminal relative  
[Type ^D at a new line to end input]  
host 172.26.27.8 {  
    any notice;  
    authorization info;  
    interactive-commands info;  
}  
^D  
load complete  
[edit system syslog]
```

ヒント ファイルから設定の一部を読み込むときにも、`relative` オプションを使用できます。コマンドの形式は、上記の例とほぼ同じです。 `load merge filename relative`。(load コマンドの他の使用例については、『*CLI User Guide*』を参照。この資料は www.juniper.net/techpubs から入手可能)

次に参照すべき資料およびサイト

www.juniper.net/dayone

本書の印刷版をお読みの場合は、このサイトからPDF版をダウンロードできます。PDF版の付録には、補足情報が含まれています。さらに、このサイトでは、現在入手可能な他のDay Oneシリーズについても確認できます。

www.juniper.net/junos

Junosの導入と習得に必要な資料がすべて揃います。

<http://forums.juniper.net/jnet>

ジュニパーがスポンサーであるJ-Net Communitiesフォーラムは、ジュニパー製品、テクノロジー、およびソリューションに関する情報、ベストプラクティス、質問を共有するための場です。この無料のフォーラムに参加するには、登録が必要です。

www.juniper.net/techpubs

このサイトでは、ジュニパーで開発した製品のすべてのマニュアル類を入手できます。各製品シリーズごとに、Junosオペレーティング・システムについて知っておくべきことをご確認ください。

www.juniper.net/books

ジュニパーは、いくつかの出版社との提携により、ネットワーク管理に不可欠なトピックについて書かれた技術本を制作および出版しています。今後も増え続ける新刊リストをご確認ください。

www.juniper.net/training/fasttrack

オンライン、オンサイト、または世界中のパートナー・トレーニング・センターで受講できるコースをご用意しています。JNTCP (ジュニパーネットワークス技術認定資格プログラム) では、ジュニパー製品の設定およびトラブルシューティングに関する能力認定を行っています。短い期間でエンタープライズ向けルーティング、スイッチング、またはセキュリティでの認定を受けるには、提供されているオンラインコース、受講ガイド、およびラボガイドをご利用ください。

付録

| | |
|--------------------------|----|
| 設定情報ワークシート..... | 78 |
| <i>Junos</i> の基本設定 | 80 |
| コマンドリファレンス..... | 84 |

注：この付録は、
『*Day One: Junos* の基本設定』の PDF 版にのみ掲載されています。

設定情報ワークシート

ホスト名

管理ポートの IP アドレス

管理ポートのネットワーク・プレフィックス

ループバック・インタフェースの IP アドレス

バックアップルーターの IP アドレス

DNS の IP アドレス (複数可)

NTP サーバーの IP アドレス

パスワードは、漏洩しないように注意してください。ここにパスワードを記入した場合には、第三者の目に触れないよう、本書を安全な場所に保管してください。

初期 root パスワード

ローカルユーザー名

初期ローカルパスワード

使用するリモート認証方法

リモート認証サーバー（複数可）の IP アドレス（複数可）

サーバー認証パスワード

認証サーバーにアクセスするには、デバイスで暗号化用の秘密鍵が必要となることがあります。

インタフェース（複数可）の IP アドレス

ネットワーク管理システムの IP アドレス

SNMP コミュニティ

ログホストの IP アドレス

『Day One: Junos の基本設定』設定リスティング

このセクションでは、本書で説明するデバイスでのステートメント設定で得られる、すべての設定リスティングを示します。以降のページに示すリスティングは、本書において左マージンの矢印で示されたすべてのコマンドを入力した場合に得られる設定結果です。これらのコマンドについては、第2章～第5章で説明しています。

デバイスの設定結果リスティングには、以前に定義したデフォルト設定や事前設定に関連する他のステートメントが追加されていることもあります。ネットワークに固有のカスタム設定でデバイスを設定した場合には、そうした設定名やアドレスなどの固有情報が出力に含まれています。

```
## Last commit:2009-06-16 08:32:35 CEST by root
version "9.5I0 [builder]";
groups {
  common {
    snmp {
      community public {
        authorization read-only;
        clients {
          192.168.1.0/24;
          0.0.0.0/0 restrict;
        }
      }
      community private {
        authorization read-write;
        clients {
          192.168.1.15/24;
          0.0.0.0/0 restrict;
        }
      }
    }
    trap-options {
      source-address lo0;
    }
    trap-group managers {
      version v2;
      categories {
        authentication;
      }
      targets {
        192.168.1.15;
      }
    }
  }
}
```

```
}
apply-groups common;
system {
    host-name juniper1;
    domain-name enterprise.com;
    domain-search [ enterprise.com department.enterprise.com ];
    backup-router 172.26.31.1 destination [ 172.26.31.1/32
172.16.0.0/12 ];
    time-zone Europe/Amsterdam;
    authentication-order [ radius tacplus password ];
    name-server {
        172.26.27.2;
        172.26.27.3;
    }
    radius-server {
        172.26.27.5 {
            port 1845;
            secret "$9$8.wx-b4aU.PQZG39pulINdb";
        }
    }
    tacplus-server {
        172.26.27.6 {
            port 49;
            secret "$9$KyEwXNs2aikP4oT39Cu0LxN";
        }
    }
    login {
        announcement «Maintenance scheduled 11PM to 2AM tonight»;
        message "Welcome \n to \n Junos\n";
        user jadmin {
            full-name "Juniper Network Administrator";
            uid 1250;
            class super-user;
            authentication {
                encrypted-password "$1$jetUXT44$D9KVQKofqwKMEfcBjp
3zg0";
            }
        }
        user remote {
            uid 2001;
            class super-user;
        }
        user adminjlk {
            uid 2002;
            class super-user;
        }
    }
    services {
        ssh;
    }
}
```

```
        web-management {
            http;
        }
    }
    syslog {
        user * {
            any emergency;
        }
        user jadmin {
            any critical;
        }
        host loghost {
            any notice;
            facility-override local7;
            log-prefix Junos;
        }
        host set {
            explicit-priority;
        }
        file all_messages {
            any warning;
            authorization notice;
        }
        console {
            any error;
        }
        time-format;
    }
    ntp {
        boot-server 172.26.27.4;
        server 172.26.27.4;
    }
}
interfaces {
    ge-0/0/1 {
        unit 0 {
            family inet {
                address 192.168.100.1/30;
            }
        }
    }
}
me0 {
    unit 0 {
        family inet {
            address 172.26.27.44/24;
        }
    }
}
lo0 {
    unit 0 {
```

```
        family inet {
            address 192.26.0.110 {
                preferred;
            }
            address 127.0.0.1/32;
        }
    }
}
snmp {
    description "Juniper EX4200";
    location "London Corporate Office";
    contact "For help, please email support@enterprise.com";
    view ping-mib-view {
        oid 1.3.6.1.2.1.80 include;
        oid jnxPingMIB include;
    }
    community ping-mib {
        view ping-mib-view;
        authorization read-write;
    }
    community managers;
    rmon;
    health-monitor {
        interval 900;
        rising-threshold 70;
        falling-threshold 60;
    }
}
```

コマンドリファレンス

(『Day One : Junos CLI の探究』からのコマンドのサマリー)

設定モードのコマンド

activate 設定で非アクティブな箇所をアクティブにします。

annotate 設定に注釈を付けます。

commit 変更の候補セットをコミットします。

commit at 指定時間に候補をコミットします。

commit check 変更内容をアクティブにせずに、候補設定を確認します。

commit confirmed ユーザーがコマンドに対して確定しなかった場合には、ロールバックを自動実行します。

compare 2つの設定の相違点を表示します。

copy ステートメントをコピーします。

deactivate 設定の一部を非アクティブとして示します。

delete 設定ステートメント（複数可）または識別子を削除します。

edit 指定した階層に移動します。

exit この設定階層から出ます。最上位層の場合は、設定モードから出ます。

exit configuration-mode 設定モードから出ます。

help オンボードヘルプ機能を使用します。

pipe あるコマンドの出力を別のコマンドの入力として使用する、または出力をファイルに送ります。

rename 設定または識別子に新しい名前を付けます。

rollback 候補ファイルを以前にコミットした設定に戻します。

run 運用モードコマンドを実行します。

set ステートメント階層を作成して、識別子の値を設定します。

show 候補設定を表示します。

top 階層の第1層に移動します。

up 1階層分上に移動します。

運用モードのコマンド

clear システム情報を削除します。

configure 設定モードに切り替えます。

configure exclusive 他のユーザーが編集できないように、候補に排他的ロックを指定します。

configure private ユーザーに独自の候補設定を与えます。

exit 運用モードから出ます。

file copy ファイルを作成して、アーカイブ化します。

file list デバイスのファイルおよびディレクトリをリスト表示します。

file show ファイルの内容を参照します。

help オンボードヘルプ機能を使用します。

monitor リアルタイムのデバッグ情報を表示します。

ping 接続を確認するために、別のホストにメッセージを送信します。

pipe あるコマンドの出力を別のコマンドの入力として使用する、または出力をファイルに送ります。

request 新しいソフトウェアバージョンをインストールし、再起動して、シャットダウンします。

restart 個別のオペレーティング・システム・デーモンを再起動します。

set システムプロパティを設定します。

show システム情報を表示します。

ssh 別のホストでSSHを起動します。

start shell Cシェルインタフェースにログインします。

telnet ネットワーク上の別のデバイスまたはホストへのターミナル接続を確立します。

traceroute 1つの場所から別の場所への各IPパケットホップを記録して、表示します。

コマンドリファレンス

(本書からの新しいコマンドのサマリー)

設定モードのコマンド

commit synchronize 変更の候補セットを、単一デバイスの両ルーティングエンジンにコミットします。

commit comment コミットした設定を説明するコメントを追加します。

commit and-quit ソフトウェアの設定変更を保存し、設定をアクティブにして、設定モードから出ます。

insert 新しく順序が指定されたデータ要素を挿入します。

load merge 現在の設定と読み込んだ設定をまとめます。

load override 現在の設定を読み込んだ設定で置き換えます。

pipe あるコマンドの出力を別のコマンドの入力として使用する、または出力をファイルに送ります。

quit この設定階層から出ます。最上位層の場合は、設定モードから出ます。

replace 設定の文字列を置き換えます。

save 設定を ASCII ファイルに保存します。

set apply-groups 設定グループを、設定内の特定の階層に適用します。

set groups 設定グループを作成します。

set interfaces このデバイスのインタフェースです。

set snmp このデバイスの SNMP 設定です。

set system ステートメント階層を作成し、設定のシステム分岐で識別子の値を設定します。

set system authentication-order 認証方法を呼び出す順序です。

set system backup-router 起動中に使用する IPv4 ルーターです。

set system domain-name このデバイスのドメイン名です。

set system domain-search 検索対象のドメイン名です。

set system host-name このデバイスのホスト名です。

set system login ユーザーの名前、ログインクラス、およびパスワードです。

set system name-server DNS 名サーバーです。

set system ntp boot-server NTP 起動サーバーです。

set system ntp server NTP サーバーです。

set system radius-server RADIUS サーバー設定です。

set system root authentication root ログインの認証情報です。

set system services デバイスのサービスです。

set system syslog システムログ収集のファシリテーターです。

set system tacplus-server TACACS+ サーバー設定です。

set system time-zone タイムゾーン名です。

Day One : Junosの基本設定

Junos基本シリーズの第2のブックレットである本書は、お使いのデバイスの基本的な設定方法や設定モードに関する詳細を理解することを支援するためのものです。これらの基本設定は、ルーター、スイッチ、セキュリティ・プラットフォームのどのJunosデバイスでも、セットアップの第一歩となります。

最初のブックレットで基本知識を習得した後で、本書『Day One: Junosの基本設定』はJunosおよびジュニパー製品を初めてご利用になるユーザーにとって実務上のガイドとなるものですが、より経験のあるJunos管理者にも参考になる、あるいは知識のリフレッシュとなるように書かれています。

「ジュニパーネットワークス製デバイスを日々の業務で使用していく上で、Day Oneシリーズは非常に役立ちます。Junos設定プロセスがどのように機能するのか、またネットワーク内でのデバイスの設定方法に関する質問に対して、ジュニパーの専門家によって、数多くの実用的なヒントや例とともに答えが出されます。まさに、探し求めていたものです。」

Gadde Pradeep氏 (JNCIA-M、JNCIS-M、JNCIA-EX、JNCIA-ER、JNCIS-ER)

『Day One: Junosの基本設定』では以下の手順について説明します。

- ・ システムの基本設定の便利なチェックリストを作成する
- ・ システムの基本設定を行う
- ・ ログインアカウントおよびパーミッションを作成する
- ・ 既存のシステムで使用できるようにSNMPを設定する
- ・ リモートからデバイスを監視し、システムログを設定する
- ・ Webベース管理機能をインストールする
- ・ 設定ショートカットを使用して素早く変更を行う
- ・ 設定グループやテンプレートを使用してデバイスのセットアップを合理化する
- ・ 設定結果をブックレットの設定例と比較する

ジュニパーネットワークスのDay Oneブックレットでは、初めてご利用になる際に必要となる情報のみを提供しています。これらは、ネットワークの設定と実行を専門とする技術専門家とエンジニアによって書かれています。高性能のネットワークソリューションに関するその他のブックレットは、www.juniper.net/dayoneを参照してください。

本書は、PDF版、印刷版のどちらも入手可能です。



7100105