Guard の設定

この章では、Cisco Guard（Guard）のサービスの設定方法について説明します。

この章には、次の主要な項があります。

- Guard のサービスのアクティブ化
- アクセス コントロールの設定：認証、認可、アカウンティングの使用
- Cisco Traffic Anomaly Detector との通信のイネーブル化
- 日付と時刻の設定
- SSH 鍵の管理
- SFTP 接続のための鍵の設定
- ホスト名の変更
- SNMP トラップのイネーブル化
- SNMP コミュニティ ストリングの設定

Guard のサービスのアクティブ化

Guard でアクティブにするサービスを定義することができます。正しい機能をイネーブルにするためには、サービスをイネーブルにして、そのサービスへのアクセスを許可する必要があります。Guard のサービスのアクティベーションを制御し、特定の IP アドレスに対してアクセス権を付与または拒否することにより、Guard にアクセスし、制御する IP アドレスを制限することができます。

表 3-1 で、Guard のサービスについて説明します。

表 3-1　Guard サービス

サービス	説明
internode-comm	ノード間通信サービス。Guard は、Cisco Traffic Anomaly Detector との通信チャネルを確立するときにこのサービスを使用します。
ntp	Network Time Protocol（NTP）サービス。Guard は、時刻同期サービスを提供します。この機能により、Guard を時刻同期サーバに同期させることができます。 時刻の同期を可能にするには、NTP サーバを設定する必要があります。詳細については、P.3-30 の「Guard のクロックと NTP サーバの同期」の表 3-9 を参照してください。
snmp-server	Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）サーバ サービス。SNMP を使用して Guard にアクセスすることにより、Riverhead 管理情報ベース（Riverhead の専用 MIB、MIB2、および UCDavis の MIB）で定義された情報を取得することができます。 MIB 定義の詳細については、このバージョンに付属の MIB ファイルを参照してください。 （注）　Riverhead MIB には、64 ビットのカウンタが含まれています。MIB を読み取るには、SNMP バージョン 2 をサポートするブラウザを使用する必要があります。

表 3-1　Guard サービス（続き）

サービス	説明
snmp-trap	SNMP トラップ サービス。snmp-trap サービスをアクティブにすると、Guard は SNMP トラップを生成します。詳細については、P.3-37 の「SNMP トラップのイネーブル化」を参照してください。
ssh	Secured Shell サービス（詳細については、P.3-33 の「SSH 鍵の管理」を参照）。
wbm	Web-Based Management（WBM）サービス。Web ブラウザを使用して、Web から Guard を制御できます。

Guard のサービスをアクティブにするには、次の手順を実行します。

ステップ 1　Guard のサービスをイネーブルにします。次のコマンドを入力します。

```
service {internode-comm | ntp | snmp-server | snmp-trap | wbm}
```

Guard のサービスについては、表 3-1 を参照してください。デフォルトでは、SSH 以外、Guard のすべてのサービスはディセーブルになっています。

ステップ 2　Guard のサービスに対するアクセス権を付与し、接続を可能にします。次のコマンドを入力します。

```
permit service ip-address-general [ip-mask]
```

表 3-2 に、**permit** コマンドの引数を示します。

表 3-2　permit コマンドの引数

パラメータ	説明
service	アクセスと操作の対象となるサービス。Guard のサービスについては、表 3-1 を参照してください。
ip-address-general	アクセスを許可する IP アドレス。IP アドレスをドット区切り 10 進表記で入力します（たとえば 192.168.10.2）。すべての IP アドレスからのアクセスを許可するには、アスタリスク（*）を使用します。
ip-mask	（オプション）IP サブネット マスク。サブネット マスクをドット区切り 10 進表記で入力します（たとえば 255.255.255.0）。デフォルトのサブネット マスクは、255.255.255.255 です。

注意　セキュリティ上の理由から、すべての IP アドレスからのサービスへのアクセスを許可する（* と入力する）ことは推奨しません。

次の例を参考にしてください。

```
user@GUARD-conf# service wbm
user@GUARD-conf# permit wbm 192.168.10.35
```

アクセス コントロールの設定：認証、認可、アカウンティングの使用

アクセス コントロールとは、Guard にアクセスできるユーザ、およびアクセス権を持ったユーザが使用できるサービスを制御することです。認証、認可、アカウンティング（AAA）のセキュリティ サービスは、アクセスを設定するための基本的なフレームワークとなります。

- 認証：ユーザにシステムおよびシステム　サービスへのアクセスを許可する前に、そのユーザを識別する方法。
- 認可：システムへのアクセスを取得した後で、ユーザが実行することのできる内容を決定するプロセス。通常は、ユーザが認証され、システムの操作を開始した後で実行されます。
- アカウンティング：ユーザが実行中または実行済みの内容を記録する処理。アカウンティングにより、ユーザがアクセスしているサービスを追跡することができます。

Guard には、次のシステム ユーザ アカウントが事前設定されています。

- admin：admin ユーザ アカウントには、管理者アクセス権が設定されています。このアカウントを使用することで、Guard の CLI およびすべての機能にアクセスできます。Guard CLI に初めて接続すると、このアカウントに対するパスワードを設定するように要求されます。新しいユーザ アカウントを設定するには admin ユーザ アカウントを使用します。
- riverhead：riverhead ユーザ アカウントには、ダイナミック（dynamic）のアクセス権が設定されています。Guard は、このユーザ アカウントを使用して Cisco Traffic Anomaly Detector と通信します。Guard CLI に初めて接続すると、このアカウントに対するパスワードを設定するように要求されます。

  Cisco Traffic Anomaly Detector は、リモートでの Guard のアクティベーションに riverhead ユーザ名を使用します。

システム ユーザ アカウントは削除できません。

ユーザ定義を使用すると、Guard のユーザ コミュニティをドメインに分割し、安全な管理アクセスのために必要に応じてパスワードを割り当てることができます。初期設定が完了した後は、ユーザのアクションを監視できるように新しいアカウントを作成し、システム ユーザ アカウントは使用しないことをお勧めします。

次の各項では、アクセス コントロールの設定方法について説明します。

認証の設定

ユーザが Guard にログインしようとするとき、または（**enable** コマンドを使用して）上位の特権レベルを要求するときに、Guard で使用する認証方式を設定することができます。Guard は、次の認証オプションを提供します。

- ローカル認証：ローカル認証では、ローカルに設定されたログイン名およびイネーブル パスワードが認証に使用されます。これはデフォルトの認証方式です。詳細については、P.3-8 の「ローカル認証の設定」を参照してください。
- TACACS+ 認証 ：TACACS+ 認証では、1 つの TACACS+ サーバまたは複数の TACACS+ サーバのリストを使用してユーザが認証されます。

  ユーザを 1 つの TACACS+ サーバにしか設定しない場合、その TACACS+ サーバで当該ユーザに対して認可も設定する必要があります。設定しないと、そのユーザは show コマンドにしかアクセスできません。

シーケンシャルな認証リストを設定することができます。認証リストでは、ユーザの認証に使用する認証方式を定義します。この定義により、認証に使用する 1 つ以上の方式を指定することができます。したがって、最初の方式が失敗した場合は、認証のバックアップ システムが提供されます。

Guard は、最初にリストされた方式を使用してユーザを認証します。その方式が応答しない場合、Guard は 2 番目の認証方式を選択します。両方の認証方式を試してもうまくいかない場合、認証は失敗します。

分散認証方式を設定することもできます。Guard は、最初の TACACS+ サーバを使用してユーザを認証します。認証で拒否が返された場合、Guard は TACACS+ サーバ リスト、および、存在する場合は代替の認証方式（ローカル）をスキャンします。リストをすべて試してもうまくいかない場合、認証は失敗します。このオプションは、*first-hit* オプションを設定していない場合にのみ有効です。

（注）　ユーザ データベースが、複数の TACACS+ サーバに分散している、または 1 つの TACACS+ サーバとローカル ユーザ データベースに分散している場合は、**no tacacs-server first-hit** コマンドを使用してください。

認証方式の設定

Guard で使用する認証方式を設定するには、次の手順を実行します。

ステップ 1　TACACS+ 認証が必要な場合は、TACACS+ サーバ接続を設定します。詳細については、P.3-18 の「TACACS+ サーバ アトリビュートの設定」を参照してください。

ステップ 2　認証方式を定義します。次のコマンドを入力します。

```
aaa authentication {enable | login} {local | tacacs+}
[tacacs+ | local]
```

表 3-3 に、**aaa authentication** コマンドの引数を示します。

表 3-3　aaa authentication コマンドのキーワード

パラメータ	説明
enable	Guard は、上位の特権レベルに入るときに認証を行います。
login	Guard へのログイン時に認証が行われます。
local	Guard は、ローカル データベースを使用してユーザを認証します。
tacacs+	TACACS+ サーバによってユーザが認証されます。
tacacs+ | local	（オプション）設定された方式が失敗した場合の代替認証方式を設定します。

Guard にコンソール セッションからアクセスする場合は、定義されている認証方式にかかわらず、ローカル ユーザ データベースが認証に使用されます。

認証方式を変更するには、このコマンドを再入力します。

次の例は、上位の特権レベルに入る際に認証を行うように設定する方法を示しています。最初の認証方式は TACACS+ に設定され、2 番目の認証方式はローカル ユーザ データベースに設定されています。

```
user@GUARD-conf# aaa authentication enable tacacs+ local
```

ローカル認証の設定

Guard には、管理者特権を持つユーザ名があらかじめ設定されています。このユーザ名を使用して新しいユーザを作成できます。ユーザ定義を使用すると、Guard のユーザ コミュニティをドメインに分割し、安全な管理アクセスのために必要に応じてパスワードを割り当てることができます。

TACACS+ サーバを使用した CLI ユーザの認証をイネーブルにするには、P.3-6 の「認証の設定」を参照してください。

ユーザの追加

Guard のローカル データベースにユーザを追加するには、次のコマンドを入力します。

username *username* {**admin** | **config** | **dynamic** | **show**} [*password*]

表 3-4 に、**username** コマンドの引数とキーワードを示します。

表 3-4　username コマンドの引数とキーワード

パラメータ	説明
username	ユーザ名。1 ～ 63 文字の英数字の文字列です。大文字と小文字が区別され、先頭は英字である必要があります。この文字列にはスペースを含めることはできませんが、アンダースコアを含めることはできます。
admin | **config** | **dynamic** | **show**	ユーザの特権レベル。詳細については、表 2-4 を参照してください。
password	（オプション）パスワード。6 ～ 24 文字の文字列を入力します。スペースは使用できず、大文字と小文字が区別されます。パスワードを入力しない場合、入力するよう要求されます。

次の例を参考にしてください。

```
user@GUARD-conf# username Robbin config 1234
```

ユーザはパスワードをクリア テキストで入力しますが、Guard の設定ファイルでは、パスワードが暗号化された形式で表示されます。次に示すのは、Guard の設定ファイル（running-config）の表示の例です。

```
username Richard config encrypted 840xdMk3
```

上の例の encrypted オプションは、パスワードが暗号化されていることを示しています。

Guard 上に設定されているユーザのリストを表示するには、**show running-config** コマンドまたは **show guard** コマンドを使用します。現在 CLI にログインしているユーザのリストを表示するには、**show users** コマンドを使用します。

Guard のユーザ リストからユーザを削除するには、**no username** *username* コマンドを使用します。

パスワードの変更

ユーザは、自分自身のパスワードを変更することができます。管理者は、自分自身のパスワードと、他のすべてのユーザのパスワードを変更できます。

自分自身のパスワードを変更するには、次の手順を実行します。

ステップ 1　次のコマンドを入力します。

password

ステップ 2　現在のパスワードを入力します。新しいパスワードの入力を求めるプロンプトが表示されます。

ステップ 3　新しいパスワードを入力します。パスワードは、スペースを含まない、6 ～ 24 文字の英数字の文字列である必要があります。パスワードでは大文字と小文字が区別されます。新しいパスワードをもう一度入力し、確認するように求めるプロンプトが表示されます。

次の例を参考にしてください。

```
user@GUARD# password
Old Password: <old-password>
New Password: <new-password>
Retype New Password: <new-password>
```

管理者は、他のユーザのパスワードを変更できます。

特定のユーザのパスワードを変更するには、次の手順を実行します。

ステップ 1　グローバル モードで次のコマンドを入力します。

password *username-password*

username-password 引数は、変更対象のパスワードを持つユーザです。

ステップ 2　新しいパスワードを入力します。パスワードは、スペースを含まない、6 ～ 24 文字の英数字の文字列である必要があります。パスワードでは大文字と小文字が区別されます。新しいパスワードをもう一度入力し、確認するように求めるプロンプトが表示されます。

次の例では、管理者はユーザ *John* のパスワードを変更しています。

```
user@GUARD# password Jose
New Password: <new-password>
Retype New Password: <new-password>
```

認可の設定

ユーザが使用できるサービスを制限することができます。認可をイネーブルにすると、Guard はユーザのプロファイルでそのユーザのアクセス権を確認します。プロファイルは、ローカル ユーザ データベースまたは TACACS+ セキュリティ サーバにあります。ユーザは、そのユーザのプロファイル内の情報で許可されている場合にのみ、要求したサービスへのアクセス権を付与されます。

ユーザがコマンドを実行しようとするときに Guard で使用する認可方式を設定することができます。Guard では、次の認可オプションが提供されています。

- TACACS+ 認可：TACACS+ 認可では、TACACS+ サーバを使用してユーザが認可されます。後続のサーバが定義されている場合は、1 つのサーバとの通信が失敗した場合にのみ、そのサーバへのアクセスが開始されます。

  TACACS+ 認可では、2 種類がサポートされています。実行認可では、ユーザの Guard へのログインの認証時にユーザの特権レベルが決定されます。コマンド認可では、ユーザがコマンドを入力すると、コマンドごとの認可を取得するために TACACS+ サーバに対して確認が行われます。

  TACACS+ 認可では、コマンドごとにアクセス権を指定することができます。

注意　**copy running-config** コマンドへの認可の付与には注意を払うことをお勧めします。

copy running-config コマンドの実行を認可すると、設定ファイル内ですべてのコマンドにそれぞれ認可を設定しているかどうかに関係なく、すべての設定コマンドに対して認可が与えられます。

- ローカル認可：ローカル認可では、コマンド グループのアクセス コントロールにローカルで設定されたユーザ プロファイルが使用されます。認可は、指定された特権レベルのすべてのコマンドに対して定義されます。これはデフォルトの認可方式です。

シーケンシャルな認可リストを設定することができます。認可リストでは、ユーザの認可に使用する認可方式を定義します。この定義により、認可に使用する 1 つ以上の方式を指定することができます。したがって、最初の方式に対する通信が失敗した場合は、認可のバックアップ システムが提供されます。

Guard は、最初にリストされた方式を使用してユーザを認可します。その方式が応答しない場合、Guard は 2 番目の認可方式を選択します。両方の認可方式が成功しなかった場合、認可は失敗します。

Guard のローカル認可は、TACACS+ サーバへの通信に失敗した場合に実行することができます。

ローカル認可の設定

Guard のサービスにアクセスできるかどうかは、ユーザの特権レベルによって決まります。システム管理者は、ユーザが使用できるサービスを制限することができます。Guard は、ユーザのプロファイルをチェックして、ユーザのアクセス権を確認します。認可されると、ユーザは、そのユーザのプロファイル内の情報で許可されている場合にのみ、要求したサービスへのアクセス権を付与されます。ユーザの特権レベルについては、表 2-4 を参照してください。

パスワードを使用した特権レベルの割り当て

管理者は、ユーザの特権レベルへのアクセスを制限するパスワードを設定できます。

ローカル パスワードを設定して特権レベルへのアクセスを制御するには、次のコマンドを入力します。

enable password [**level** *level*] [*password*]

表 3-5 で、**enable password** コマンドの引数について説明します。

表 3-5　enable password コマンドの引数

パラメータ	説明
level	（オプション）目的の特権レベル。このレベルには、admin、config、dynamic、show のいずれかを指定できます。詳細については、表 2-4 を参照してください。デフォルトのレベルは admin です。
password	（オプション）特権レベルのパスワード。パスワードは、スペースを含まない、6 ～ 24 文字の英数字の文字列である必要があります。パスワードでは大文字と小文字が区別されます。パスワードを入力しない場合、入力するよう要求されます。

次の例を参考にしてください。

```
user@GUARD-conf# enable password level admin <password>
```

ユーザ特権レベル間の移動

認可されたユーザは、ユーザ特権レベル間を移動することができます。

ユーザ特権レベル間を移動するには、次の手順を実行します。

ステップ 1　次のコマンドを入力します。

```
enable [level]
```

level 引数には、目的の特権レベルを指定します。このレベルには、admin、config、dynamic のいずれかを指定できます。デフォルトのレベルは **admin** です。詳細については、表 2-4 を参照してください。

ステップ 2　特権レベルのパスワードを入力します。

次の例を参考にしてください。

```
user@GUARD> enable admin
Enter enable admin Password: <password>
```

下位の特権レベル（show）に戻る場合は、**disable** コマンドを使用します。

認可方式の設定

認可方式を設定するには、次の手順を実行します。

ステップ 1　TACACS+ 認可が必要な場合は、TACACS+ サーバ接続を設定します。詳細については、P.3-18 の「TACACS+ サーバ アトリビュートの設定」を参照してください。

ステップ 2　認可方式を定義します。次のいずれかのコマンドを入力します。

- **aaa authorization exec tacacs+**
- **aaa authorization commands** *level* {**local** | **tacacs+**} [**local**]

認可方式のシーケンシャルなリストを設定できます。各方式について、**aaa authorization** コマンドを入力します。認証方式を削除するには、このコマンドの no 形を使用します。

表 3-6 に、**aaa authorization** コマンドの引数とキーワードを示します。

表 3-6　aaa authorization コマンドの引数とキーワード

パラメータ	説明
exec	ユーザが EXEC シェルの実行を許可されているかどうかを判別するために認可が実行されます。Guard は、TACACS+ サーバに確認して、認証されたユーザの特権レベルを判別します。 **注意**　認可を設定する前に、TACACS+ サーバにそのユーザを設定しておく必要があります。設定していない場合は、Guard にアクセスできないことがあります。
commands	指定された特権レベルのすべてのコマンドに対して認可が実行されます。複数の特権レベルの認可を設定するには、認可が必要な特権レベルごとにこのコマンドを発行します。
level	指定された特権レベルの認可を定義します。有効なエントリは、show、dynamic、config、および admin です。ユーザの特権レベルについては、表 2-4 を参照してください。
local	Guard のローカル データベースでユーザのアクセス権を確認します。
tacacs+	TACACS+ サーバでユーザのアクセス権を確認します。
local	（オプション）設定された認可方式が失敗した場合の代替の認可方式を設定します。

パフォーマンスへの影響を考慮し、show 特権レベルのコマンドには認可を設定しないことをお勧めします。

（注）　コンソール セッションから入力されたコマンドには、TACACS+ 認可は実行されません。

次の例は、*config* 特権レベルを必要とするコマンドの認可を設定する方法を示しています。最初の認可方式は TACACS+ に設定され、2 番目の認可方式はローカル ユーザ データベースに設定されています。

```
user@GUARD-conf# aaa authorization commands config tacacs+ local
```

注意　設定コマンド モードにアクセスできるようにするには、dynamic ユーザ特権レベルに対するアクセス権を付与するか、**configure** コマンドへのアクセス権を指定する必要があります。

TACACS+ サーバの設定例

TACACS+ サーバのデータベースで、各コマンドの認可を指定することができます。

次の例を参考にしてください。

```
user=Zoe {
    cmd = protect {
        permit .*
    }
    cmd = "no protect" {
        permit .*
    }
    cmd = learning {
        deny policy*
    }
    cmd = "no learning" {
        deny .*
    }
    cmd = dynamic-filter {
        permit .*
    }
    cmd = "no dynamic-filter" {
        permit .*
    }
    cmd = flex-filter {
        deny .*
    }
    cmd = "no flex-filter" {
        deny .*
    }
}
```

アカウンティングの設定

アカウンティング管理により、ユーザがアクセスしているサービスを追跡し、TACACS+ サーバにアカウンティング情報を保存することができます。課金、レポート、またはセキュリティの目的のため、要求されたサービスのアカウンティングをイネーブルにします。デフォルトでは、Guard はアカウンティング管理がディセーブルに設定されています。

アカウンティングを設定するには、次の手順を実行します。

ステップ 1　TACACS+ サーバ接続を設定します。詳細については、P.3-18 の「TACACS+ サーバ アトリビュートの設定」を参照してください。

ステップ 2　複数の特権レベルのアカウンティングを設定するには、アカウンティングが必要な特権レベルごとにこのコマンドを発行します。次のコマンドを入力します。

```
aaa accounting commands {show | dynamic | config | admin} stop-only
{local | tacacs+}
```

表 3-7 に、**aaa accounting** コマンドのキーワードを示します。

表 3-7　aaa accounting コマンドのキーワード

パラメータ	説明
show | dynamic | config | admin	指定された特権レベルのアカウンティングを定義します（ユーザの特権レベルについては、表 2-4 を参照してください）。
stop-only	コマンドの実行が終了したときにアクションを記録します。
tacacs+	アカウンティング情報の記録に TACACS+ サーバのデータベースを使用します。
local	アカウンティング情報を保存しません。

パフォーマンスへの影響を考慮し、アカウンティング管理は config ユーザ特権レベルに対してのみイネーブルにすることをお勧めします。

アカウンティング管理を削除するには、このコマンドの no 形を使用します。

次の例は、TACACS+ サーバ上で *config* 特権レベルを必要とするコマンドのアカウンティングを設定する方法を示しています。

```
user@GUARD-conf# aaa accounting commands config stop-only tacacs+
```

TACACS+ サーバ アトリビュートの設定

TACACS+ サーバのアトリビュートを設定するには、次の手順を実行します。

注意　TACACS+ 認証方式を適用する前に、TACACS+ サーバのアトリビュートを設定しておく必要があります。設定していない場合は、Guard にアクセスできないことがあります。

ステップ 1　TACACS+ サーバの IP アドレスを設定します。詳細については、P.3-19 の「TACACS+ サーバの IP アドレスの設定」を参照してください。

ステップ 2　Guard が TACACS+ サーバへのアクセスに使用する暗号鍵を設定します。詳細については、P.3-20 の「TACACS+ サーバの暗号鍵の設定」を参照してください。

ステップ 3　（オプション）Guard が認証に使用する検索方式を設定します。詳細については、P.3-20 の「TACACS+ の検索の設定」を参照してください。

ステップ 4　（オプション）TACACS+ サーバの接続タイムアウトを設定します。詳細については、P.3-21 の「TACACS+ サーバの接続タイムアウトの設定」を参照してください。

ステップ 5　TACACS+ サーバ接続の統計情報を表示します。詳細については、P.3-22 の「TACACS+ サーバの統計情報の表示」を参照してください。

Guard のユーザ特権レベルは、TACACS+ の特権番号に次のように対応しています。

- admin = 15
- config = 10
- dynamic = 5
- show = 0

TACACS+ サーバの IP アドレスの設定

認証、認可、およびアカウンティング用の TACACS+ サーバのシーケンシャルなリストを Guard が使用するように設定できます。Guard は、リストされた TACACS+ サーバを使用してユーザを認証、認可、またはアカウンティング イベントを送信します。そのサーバが応答しない場合、Guard は 2 番目のサーバを選択します。リストされたすべてのサーバを試してもうまくいかない場合、認証または認可は失敗します。

または、Guard がリストの最初の TACACS+ サーバだけを使用してユーザを認証するように設定することもできます（詳細については、P.3-20 の「TACACS+ の検索の設定」を参照）。

リストには、各 TACACS+ サーバの IP アドレスを定義する必要があります。最大 9 つの TACACS+ サーバを定義できます。

リストに TACACS+ サーバを追加し、IP アドレスを割り当てるには、設定モードで次のコマンドを入力します。

tacacs-server host *ip-address*

ip-address 引数には、TACACS+ サーバの IP アドレスを指定します。

TACACS+ サーバは、入力した順序でリストに追加されます。リストには、最大 9 つのサーバを追加できます。

次の例を参考にしてください。

```
user@GUARD-conf# tacacs-server host 192.168.33.45
```

TACACS+ サーバの暗号鍵の設定

TACACS+ サーバにアクセスするには、暗号鍵を設定する必要があります。コマンドの一部として入力される鍵は、TACACS+ サーバ上の鍵と一致している必要があります。鍵にスペースを含めることはできません。

サーバの暗号アクセス鍵を設定するには、設定モードで次のコマンドを入力します。

tacacs-server key *tacacs-key*

引数 *tacacs-key* は、英数字の文字列です。

（注）　定義できる暗号鍵は 1 つだけです。複数の TACACS+ サーバを使用している場合、Guard は同じ鍵を使用してすべての TACACS+ サーバとの通信を暗号化します。

次の例は、TACACS+ サーバの暗号鍵を *TacacsKey* に設定する方法を示しています。

```
user@GUARD-conf# tacacs-server key <TacacsKey>
```

TACACS+ の検索の設定

Guard が、1 つの認証拒否を最終的なものと見なし、他の TACACS+ サーバやローカル認証方式を使用したそれ以上の検索を中止するように設定することができます。この場合、**tacacs-server first-hit** コマンドを使用します。Guard は、サーバ リストで最初に応答する TACACS+ サーバだけを使用してユーザ認証を実行します。最初の TACACS+ サーバが応答しない場合、Guard はリストにある次のサーバを選択します。Guard は、ユーザ認証に対して最初に受け取る承認または拒否を最終的なものと見なし、他の TACACS+ サーバまたはローカル ユーザ データベースを使用したそのユーザ認証の試行を停止します。

TACACS+ の検索方式を first-hit に設定しない場合、Guard はデフォルトでリスト内のすべての TACACS+ サーバでユーザを認証しようとします。ユーザ認証として first-hit 検索方式をイネーブルにする（**no tacacs-server first-hit** コマンドを使

用する）場合、Guard は、リストの最初にある TACACS+ サーバを使用してユーザを認証します。最初のサーバが応答しなかった、またはユーザの認証に失敗した場合は、Guard はリストにある次のサーバを選択します。リストにあるすべての TACACS+ サーバが応答しなかった、またはユーザ認証に失敗した場合、ローカルの認証方式が設定されていないと、そのユーザ認証は失敗します。

（注）　TACACS+ の検索方式は、認証にのみ適用されます。

Guard がリストの最初の TACACS+ サーバだけを使用してユーザを認証するように設定するには、設定モードで次のコマンドを入力します。

tacacs-server first-hit

次の例を参考にしてください。

```
user@GUARD-conf# tacacs-server first-hit
```

TACACS+ サーバの接続タイムアウトの設定

Guard が TACACS+ サーバからの応答を待つ時間を設定できます。タイムアウトが終了すると、Guard は次の TACACS+ サーバ（そのようなサーバが設定されている場合）との接続を確立しようとするか、ローカルの AAA にフォールバックします（そのようなフォールバックが設定されている場合）。フォールバックの方式が設定されていない場合、認証と認可は失敗します。

（注）　すべての TACACS+ サーバとの通信に同じサーバ タイムアウトが使用されます。

TACACS+ サーバの接続タイムアウトを設定するには、設定モードで次のコマンドを入力します。

tacacs-server timeout *timeout*

timeout 引数には、Guard が TACACS+ サーバの応答を待つ時間を秒単位で指定します。デフォルトのタイムアウトは 0 です。

次の例を参考にしてください。

```
user@GUARD-conf# tacacs-server timeout 600
```

ヒント　ネットワークに問題がある場合や、小さいタイムアウト値を使用していて、TACACS+ サーバの応答が遅いためにタイムアウトが継続的に発生する場合には、タイムアウトの値を大きくすることができます。

TACACS+ サーバの統計情報の表示

TACACS+ サーバに関連する統計情報を表示することができます。統計データは、各サーバに対して提供されます。

TACACS+ 関連の統計情報を表示するには、**show tacacs statistics** コマンドを使用します。

TACACS+ の統計情報をクリアするには、**clear tacacs statistics** コマンドを使用します。

表 3-8 で、**show tacacs statistics** コマンド出力のフィールドについて説明します。

表 3-8　show tacacs statistics コマンド出力のフィールドの説明

フィールド	説明
PASS	サービスが TACACS+ サーバに正常にアクセスし、アクセス権を付与された回数。
FAIL	サービスが TACACS+ サーバに正常にアクセスし、アクセス権を拒否された回数。
ERROR	サービスが TACACS+ サーバにアクセスできなかった回数。

Cisco Traffic Anomaly Detector との通信のイネーブル化

Guard と Cisco Traffic Anomaly Detector（Detector）の間に安全な通信チャネルを確立すると、次のタスクを実行できます。

- Remote activation of zone protection：Detector はゾーン トラフィックの異常を検出すると、通信チャネルを使用して、Guard によるゾーン保護をアクティブにします。
- Synchronization of zone configuration information：Detector と Guard は、通信チャネルを介してゾーン設定情報を交換します。

Guard は、次の 2 つのタイプの通信チャネルをサポートしています。

- Secure Sockets Layer（SSL）：Remote activation of zone protection および Synchronization of zone configuration information をイネーブルにします。
- セキュア シェル 2（SSH2）：Remote activation of zone protection のみをイネーブルにします。

Detector は、ゾーン保護をアクティブにする対象、およびゾーン情報を同期させる対象となる Guard のリストを保持します。このリストは、リモート Guard リストと呼ばれます。Detector は、リモート Guard リストに設定されている各 Guard に対して通信チャネルを確立します。

Detector は、SSL 通信チャネルを確立する前に各 Guard に対して SSH 通信チャネルを確立します。したがって、両方のタイプのリストを設定済みである場合、SSH 通信チャネルの設定を行う必要はありません。SSH 通信チャネルは SSL 通信チャネルによって設定されるためです。

この項では、次のトピックについて取り上げます。

SSL 通信チャネルの設定

Guard と Detector は、通信チャネル用に Secure Sockets Layer（SSL）接続を使用します。SSL は、プライバシー、認証、およびデータ整合性を組み合せることにより、接続のセキュリティを確保します。SSL の高度なセキュリティは、デジタル証明書、秘密と公開の鍵交換ペア、および Diffie-Hellman 鍵合意パラメータによって実現されます。

SSL では、デバイス認証とデータ暗号化により、安全なネットワーク通信チャネルが提供されます。Guard と Detector はそれぞれ、通信チャネルを介して通信を試みるデバイスを認証します。デバイス認証は、デジタル証明書とデバイス固有の情報（IP アドレスなど）を使用して実行されます。SSL により、Guard と Detector が交換するデータは暗号化されます。データを解読できるのは、指定された受信者だけです。

安全な接続を確保するために、Detector は秘密および公開鍵ペアを生成し、公開鍵をリモート Guard リスト内の Guard に配布します。

Guard 上で通信チャネル サービスをイネーブルにしたら、Detector から通信チャネルを確立します。Detector は、最初に、Guard 上のユーザ *riverhead* に対して SSH2 接続を確立します。次に、Detector は、安全な SSH2 接続を使用して SSL 接続鍵を交換します。

この項では、次のトピックについて取り上げます。

- SSL 通信チャネルの確立
- SSL 証明書の再生成

SSL 通信チャネルの確立

Guard と Detector の間に SSL 通信チャネルを確立するには、次のタスクを実行する必要があります。

1. Guard と Detector の両方で通信チャネル サービスをイネーブルにします。
2. Guard と Detector の両方で通信チャネル サービスへのアクセスを許可します。
3. Detector から通信チャネルを確立します。

Detector は、最初に、Guard 上のユーザ *riverhead* に対して SSH2 接続を確立します。次に、Detector は、安全な SSH2 接続を使用して SSL 接続鍵を交換します。

注意　Guard で TACACS+ 認証を使用してユーザを認証している場合、Detector で SSH2 接続を確立できるようにするには、TACACS+ サーバにユーザ *riverhead* を定義する必要があります。

Guard 上で通信チャネルをイネーブルにするには、Guard 上で次の手順を実行します。

（注）　Detector 上で通信チャネルをイネーブルにするには、Detector 上で同じコマンドを使用します。

ステップ 1　Guard 上で **permit ssh** *ip-address-general* [*ip-mask*] を設定モードで入力して、Detector の IP アドレスから SSH サービスへのアクセスを許可します。

引数 *ip-address-general* および *ip-mask* には、Guard へのアクセス権を付与する Detector の IP アドレスを定義します。

（注）　SSH サービスはすでにイネーブルになっているので、ここでイネーブルにする必要はありません。

ステップ 2　**service internode-comm** コマンドを設定モードで入力して、通信チャネル サービスをイネーブルにします。

ステップ 3　**permit internode-comm** *ip-address-general* [*ip-mask*] コマンドを設定モードで入力して、Detector の IP アドレスから通信チャネル サービスへのアクセスを許可します。

引数 *ip-address-general* および *ip-mask* には、Guard へのアクセス権を付与する Detector の IP アドレスを定義します。

（注）　SSL 証明書にある Guard と Detector の ID は、IP アドレスに関連付けられます。通信チャネルの一方の側で Guard または Detector の IP アドレスを変更する場合は、SSL 証明書を再生成する必要があります。P.3-26 の「SSL 証明書の再生成」を参照してください。

SSL 証明書の再生成

SSL 証明書で Guard と Detector を識別する鍵は、IP アドレスに関連付けられます。

次の変更のどちらかを行う場合は、通信チャネルの両側で Guard と Detector の新しい SSL 証明書を生成する必要があります。

- いずれか一方のデバイスの IP アドレスを変更する。
- いずれか一方のデバイスを交換（スワップアウト）する。

新しい SSL 証明書を生成するには、まず、現在使用している証明書を両方のデバイスで削除する必要があります。

現在使用している SSL 証明書を消去するには、次の手順を実行します。

ステップ 1　Detector から、Guard の SSL 証明書を削除します。

ステップ 2　Guard から、Detector の SSL 証明書を削除します。

設定モードで次のコマンドを入力します。

```
cert remove cert-host-ip
```

cert-host-ip 引数には、Detector の IP アドレスを指定します。Guard との通信チャネルを確立しているすべての Detector の SSL 証明書を削除するには、アスタリスク（*）を入力します。

ステップ 3　Guard デバイスを物理的に交換した場合は、Guard SSH ホスト鍵を Detector から削除する必要があります。

ステップ 4　Guard と Detector の間に新しい SSL 通信チャネルを確立します。詳細については、P.3-24 の「SSL 通信チャネルの確立」を参照してください。

次の例は、SSL 証明書を削除する方法を示しています。

```
user@GUARD-conf# cert remove 10.56.36.4
```

SSH 通信チャネルの設定

トラフィックの異常を検出すると、Detector はそのイベントをログに記録するか、SSH 接続を使用して Guard によるゾーン保護をアクティブにします。SSH 通信チャネルを使用する場合、Detector では次のタスクを実行できません。

- ゾーン設定を同期化する。
- Guard　を監視して、ゾーンに対する攻撃が終了したことを確認する。したがって、Detector を検出およびラーニングの動作状態でアクティブにした場合、Detector ではゾーンに対する攻撃が終了したことを確認できないため、リモート Guard をアクティブにした後はゾーン トラフィックのラーニングを継続しません。

安全な SSH2 接続を確保するために、Detector は秘密および公開 SSH 鍵ペアを生成し、公開 SSH 鍵を Detector のリモート Guard リストにある Guard に配布します。

この項では、次のトピックについて取り上げます。

- SSH 通信チャネルの確立
- SSH 通信チャネル鍵の再生成

SSH 通信チャネルの確立

Guard と Detector の間に通信チャネルを確立するには、次のタスクを実行する必要があります。

1. Guard 上で **permit ssh** コマンドを入力して、Detector の IP アドレスから SSH サービスへのアクセスを許可します。
2. Detector から SSH 通信チャネルを確立します。

注意　Guard で TACACS+ 認証を使用してユーザを認証している場合、Detector で SSH2 接続を確立できるようにするには、TACACS+ サーバにユーザ *riverhead* を定義する必要があります。

Guard デバイスを交換（スワップアウト）する場合は、SSH 通信チャネルを再生成する必要があります。P.3-28 の「SSH 通信チャネル鍵の再生成」を参照してください。

SSH 通信チャネル鍵の再生成

Guard デバイスを物理的に交換した場合は、次の手順に従って新しい SSH 通信チャネルを確立します。

ステップ 1　Detector から SSH2 ホスト鍵を削除します。Detector 上で、**no host-keys** *ip-address-general* コマンドを設定モードで入力します。

ip-address 引数には、リモート デバイスの IP アドレスを指定します。

Guard にリストされているホスト鍵を表示するには、**show host-keys** コマンドを使用します。

ステップ 2　次のいずれかのアクションを実行します。

- Detector から新しい SSH 通信チャネルを確立します（P.3-28 の「SSH 通信チャネルの確立」を参照）。

  または、次の操作を行います。

- Detector の公開鍵をリモート Guard に手動で追加します。

  Detector 上で **show public-key** コマンドを使用して、Detector の公開 SSH 鍵を表示します。

  Guard 上で **key add** コマンドを使用して、Detector の公開 SSH 鍵を設定します。

日付と時刻の設定

時刻と日付を設定するには、設定モードで次のコマンドを入力します。

date *MMDDhhmm*[[*CC*]*YY*][*.ss*]

表 3-9 に、**date** コマンドの引数とキーワードを示します。

表 3-9　date コマンドの引数

パラメータ	説明
MM	数字で表した月。
DD	月の日付。
hh	24 時間表記の時間。
mm	分。
CC	（オプション）年の最初の 2 桁（たとえば **20**05）。
YY	（オプション）年の最後の 2 桁（たとえば 20**05**）。
.ss	（オプション）秒（小数点が必要）。

次の例は、日付を 2003 年 10 月 8 日に、時刻を 5 時 10 分（17 時 10 分）17 秒に設定する方法を示しています。

```
user@GUARD-conf# date 1008171003.17
Wed Oct  8 17:10:17 EDT 2003
```

Guard のクロックと NTP サーバの同期

Guard のシステム クロックと Network Time Protocol（NTP）サーバが同期するように設定することもできます。Guard のクロックが NTP サーバと同期するように設定するには、設定モードで次の手順を実行します。

ステップ 1　日付と時刻をローカルに設定します。次のコマンドを入力します。

date *MMDDhhmm*[[*CC*]*YY*][*.ss*]

詳細については、P.3-30 の「日付と時刻の設定」を参照してください。

ステップ 2　Guard のシステムの時間帯を設定します。次のコマンドを入力します。

```
timezone timezone-name
```

timezone-name 引数には、関連する時間帯の名前を指定します。名前は、*陸地 / 都市*で構成されます。

陸地には、次のオプションがあります。

- Africa、America、Antarctica、Arctic、Asia、Atlantic、Australia、Europe、Indian、Pacific
- Etc：目的の時間帯のワイルド カード

ヒント　時間帯の名前では、大文字と小文字が区別されます。目的の陸地名を入力し、Tab キーを 2 回押すと、関連する都市のリストが表示されます。

ステップ 3　NTP サービスをイネーブルにします。次のコマンドを入力します。

```
service ntp
```

ステップ 4　ネットワーク アドレスから NTP サービスへのアクセス権を付与します。次のコマンドを入力します。

```
permit ntp ip-address
```

ステップ 5　目的の NTP サーバの IP アドレスを設定します。次のコマンドを入力します。

```
ntp server ip-address
```

ip-address 引数には、NTP サーバの IP アドレスを指定します。

Guard の設定をリロードする必要があります。

次の例を参考にしてください。

```
user@GUARD-conf# date 1008171003.17
user@GUARD-conf# timezone Africa/Timbuktu
user@GUARD-conf# service ntp
user@GUARD-conf# permit ntp 192.165.200.224
user@GUARD-conf# ntp server 192.165.200.224
```

SSH 鍵の管理

Guard は、安全なリモート ログインのために SSH をサポートしています。SSH 鍵のリストを追加すると、ログインとパスワードを入力しなくても、リモート デバイスから Guard への安全な通信をイネーブルにできます。

次の各項では、Guard の SSH 鍵リストの操作方法について説明します。

- SSH 鍵の追加
- SSH 鍵の削除

SSH 鍵の追加

ログイン名とパスワードを入力せずに SSH 接続をイネーブルにするには、Guard の SSH 鍵リストにリモート接続の SSH 公開鍵を追加します。

設定モードで次のコマンドを入力します。

key add [user-*name*] {**ssh-dsa** | **ssh-rsa**} *key-string comment*

表 3-10 に、**key add** コマンドの引数とキーワードを示します。

表 3-10　key add コマンドの引数とキーワード

パラメータ	説明
user-name	（オプション）指定されたユーザの SSH 鍵を追加します。他のユーザの SSH 鍵を追加できるのは管理者だけです。 デフォルトは、現行ユーザの SSH 鍵の追加です。
ssh-dsa	SSH2-DSA 鍵のタイプ。
ssh-rsa	SSH2-RSA 鍵のタイプ。
key-string	Detector またはリモート端末で作成された公開 SSH 鍵。鍵ストリングは、8,192 ビットまでに制限されています。 鍵タイプの識別（ssh-rsa または ssh-dsa）を除いた完全な鍵をコピーする必要があります。

表 3-10　key add コマンドの引数とキーワード（続き）

パラメータ	説明
comment	デバイスの説明。コメントの形式は、通常、鍵の生成に使用されるユーザとマシンを表す user@hostname になります。たとえば、Detector で生成される SSH 公開鍵に使用されるデフォルトのコメントは、**root@DETECTOR** です。

次の例を参考にしてください。

```
user@GUARD-conf# key add ssh-rsa 14513797528175730. . .user@Guard.com
```

SSH 鍵の削除

リストから SSH 鍵を削除できます。SSH 鍵を削除すると、次に Guard と SSH セッションを確立するときには認証を受ける必要があります。

Guard から SSH 鍵を削除するには、設定モードで次のコマンドを入力します。

key remove [*user-name*] *key-string*

表 3-11 で、**key remove** コマンドの引数について説明します。

表 3-11　key remove コマンドの引数

パラメータ	説明
user-name	（オプション）指定のユーザの SSH 鍵を削除します。 他のユーザの SSH 鍵を削除できるのは管理者だけです。デフォルトは、現行ユーザの SSH 鍵の削除です。
key-string	削除する公開 SSH 鍵。 プロンプトに SSH 公開鍵をペーストします。識別フィールド（ssh-rsa または ssh-dsa）は除き、鍵だけをペーストしてください。

次の例は、key remove コマンド用にカット アンド ペーストを行えるように、ユーザ鍵を表示する方法を示しています。

```
user@GUARD-conf# show keys Lilac
ssh-rsa 2352345234523456... user@Guard.com
user@GUARD-conf# key remove Lilac 2352345234523456...
```

SFTP 接続のための鍵の設定

Guard は、SSH2 の最上層で セキュア FTP（SFTP）をサポートしています。SFTP では、公開鍵による認証と強力なデータ暗号化を使用しています。これにより、ログイン、データ、およびセッションの情報が送信中に傍受されたり変更されたりすることを防止できます。

SFTP サーバ上に公開鍵を設定するには、Guard 上で次の操作を実行します。

ステップ 1　Guard の公開鍵を表示します。設定モードで **show public-key** コマンドを使用します。

鍵が存在している場合は、ステップ 2 を省略してステップ 3 に進みます。

鍵が存在しない場合は、ステップ 2 に進みます。

ステップ 2　秘密および公開鍵ペアを生成します。設定モードで次のコマンドを入力します。

```
key generate
```

SSH の鍵ペアがすでに存在している場合は、次のメッセージが表示されます。

```
/root/.ssh/id_rsa already exists.
Overwrite (y/n)?
```

目的のオプションを入力します。

Guard が秘密および公開鍵ペアを作成します。設定モードで **show public-key** コマンドを使用して、Guard の公開鍵を表示します。

ステップ 3　公開鍵をコピーし、SFTP サーバ上の鍵ファイル内にペーストします。

たとえば、Linux オペレーティング システム上にインストールされている SFTP サーバにルート ユーザで接続している場合は、Guard の公開鍵を /root/.ssh/authorized_keys2 ファイルに追加します。

鍵は 1 行に収まるようにコピーしてください。鍵が 2 行としてコピーされた場合は、1 行目の末尾にある改行文字を削除します。

ホスト名の変更

Guard のホスト名を変更できます。この変更はすぐに反映され、新しいホスト名は自動的に CLI プロンプト ストリングに組み込まれます。

Guard のホスト名を変更するには、設定モードで次のコマンドを入力します。

hostname *name*

name 引数には、新しいホスト名を指定します。

次の例を参考にしてください。

```
user@GUARD-conf# hostname CiscoGuard
admin@CiscoGuard-conf#
```

SNMP トラップのイネーブル化

Guard が SNMP トラップを送信し、Guard で発生する重大なイベントを管理者に通知するように設定することができます。Guard の SNMP トラップ ジェネレータを設定して、トラップ情報のスコープを定義することができます。

トラップのログは、Guard のイベント ログに記録され、トラップ条件が発生すると、SNMP エージェントがトラップを送信するかどうかに関係なく、イベント モニタに表示されます。

Guard が SNMP トラップを送信するように設定するには、次の手順を実行します。

ステップ 1　SNMP トラップ ジェネレータ サービスをイネーブルにします。設定モードで次のコマンドを入力します。

```
service snmp-trap
```

ステップ 2　SNMP トラップ ジェネレータのパラメータ（トラップの宛先 IP アドレスとトラップ情報のスコープ）を設定します。次のコマンドを入力します。

snmp trap-dest *ip-address* [*community-string* [*min-severity*]]

表 3-12 に、**snmp trap-dest** コマンドの引数を示します。

表 3-12　snmp trap-dest コマンドの引数

パラメータ	説明
ip-address	宛先ホストの IP アドレス。
community-string	（オプション）トラップとともに送信されるコミュニティ ストリング。このストリングは、宛先ホスト用に定義されたコミュニティ ストリングと一致する必要があります。デフォルトのコミュニティ ストリングは、*public* です。1 ～ 15 文字の英数字の文字列を入力します。この文字列にスペースを含めることはできません。
min-severity	（オプション）トラップ情報のスコープ。重大度レベルの範囲の下限を指定してスコープを定義します。この定義により、トラップは指定された重大度レベル以上のすべてのイベントを表示します。たとえば、重大度レベル *Warnings* を指定すると、トラップは *Warnings* から *Emergencies* までのすべての重大度レベルのイベントを表示します。重大度レベルのオプションを次に示します。 • **Emergencies**：システムは使用不能（重大度 = 0） • **Alerts**：即時のアクションが必要（重大度 = 1） • **Critical**：危険な状態（重大度 = 2） • **Errors**：エラー状態（重大度 = 3） • **Warnings**：警告状態（重大度 = 4） • **Notifications**：正常ではあるが、重要な状態（重大度 =5） • **Informational**：情報通知のためのメッセージ（重大度 = 6） • **Debugging**：デバッグ メッセージ（重大度 = 7） デフォルトでは、レポートにはすべての重大度レベルのイベントが表示されます。

SNMP トラップ ジェネレータ パラメータを削除するには、**no snmp trap-dest** コマンドを使用します。すべての SNMP トラップ宛先パラメータを削除するには * を使用します。

次に、*errors* 以上の重大度レベルのトラップが、SNMP コミュニティ ストリング *tempo* とともに宛先 IP アドレス *192.168.100.52* に送信される例を示します。

```
user@GUARD-conf# snmp trap-dest 192.168.100.52 tempo errors
```

SNMP コミュニティ ストリングの設定

Guard の SNMP サーバにアクセスすることにより、管理情報ベース 2（MIB2）および Riverhead 専用 MIB で定義された情報を取得することができます。コミュニティ ストリングは、パスワードのような役割を果たして、Guard SNMP エージェントからの読み取りアクセスを許可します。Guard の SNMP コミュニティ ストリングを設定して、異なる組織のクライアントがそれぞれ異なるコミュニティ ストリングを使用して SNMP エージェントにアクセスできるようにすることができます。

SNMP コミュニティ ストリングを追加するには、設定モードで次のコマンドを入力します。

snmp community *community-string*

community-string 引数には、目的の Guard のコミュニティ ストリングを指定します。1 ～ 15 文字の英数字の文字列を入力します。この文字列にスペースを含めることはできません。Guard のデフォルトのコミュニティ ストリングは *riverhead* です。コミュニティ名はいくつでも指定できます。コミュニティ ストリングを削除するには、**no community string** コマンドを使用します。すべての SNMP コミュニティ ストリングを削除するには * を使用します。

次の例を参考にしてください。

```
user@GUARD-conf# snmp community tempo
```