Cisco Nexus 1000V インタークラウド セキュリティ コンフィギュレーション ガイド リリース 5.2(1)IC1(1.1)

初版：2013 年 07 月 02 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

Text Part Number: OL-29150-01-J

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。 このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。 このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。 添付されていない場合には、代理店にご連絡ください。

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。 シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。 マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。 説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2013 Cisco Systems, Inc. All rights reserved.

目 次

はじめに ix

対象読者 ix

表記法 ix

Cisco Nexus 1000V InterCloud の関連資料 xi

マニュアルに関するフィードバック xii

マニュアルの入手方法およびテクニカル サポート xii

概要 1

ユーザ アカウント 1

認証、許可、アカウンティング 1

RADIUS セキュリティ プロトコル 2

TACACS+ セキュリティ プロトコル 2

SSH 2

Telnet 3

アクセス コントロール リスト 3

ユーザ アカウントの管理 5

ユーザ アカウントについて 5

ロール 5

ユーザ名 6

パスワード 6

パスワード強度のチェック 7

有効期限 8

ユーザ アカウント作成の注意事項と制限事項 8

ユーザ アカウント作成の注意事項 8

ユーザ アクセスのデフォルト設定 9

ユーザ アクセスの設定 9

パスワード強度チェックのイネーブル化 9

パスワード強度チェックのディセーブル化 10
ユーザ アカウントの作成 11
ロールの作成 12
機能グループの作成 14
インターフェイス アクセスの設定 15
VLAN アクセスの設定 16
ユーザ アクセス設定の確認 17
設定例 18
機能グループ作成の設定例 18
ロール作成の設定例 18
MIB 18
ユーザ アカウント機能の履歴 19
AAA の設定 21
AAA について 21
AAA セキュリティ サービス 21
認証 22
許可 24
アカウンティング 24
AAA サーバ グループ 24
AAA の前提条件 24
注意事項と制約事項 25
AAA のデフォルト設定 25
AAA の設定 25
ログイン認証方式の設定 25
ログイン認証失敗メッセージのイネーブル化 26
AAA 設定の確認 27
AAA の設定例 28
AAA 機能の履歴 28
RADIUS の設定 29
RADIUS について 29
RADIUS ネットワーク環境 29
RADIUS の動作 30

RADIUS サーバ モニタリング 31
ベンダー固有属性 32
RADIUS の前提条件 33
注意事項と制約事項 33
デフォルト設定 33
RADIUS サーバの設定 34
RADIUS サーバ ホストの設定 34
RADIUS グローバル キーの設定 35
RADIUS サーバ キーの設定 36
RADIUS サーバ グループの設定 36
RADIUS サーバの誘導要求のイネーブル化 38
すべての RADIUS サーバのグローバル タイムアウトの設定 39
すべての RADIUS サーバのグローバル リトライ回数の設定 40
単一 RADIUS サーバのタイムアウト間隔の設定 41
単一 RADIUS サーバのリトライ回数の設定 42
RADIUS アカウンティング サーバの設定 43
RADIUS 認証サーバの設定 44
RADIUS サーバの定期的モニタリングの設定 45
グローバル デッド タイム間隔の設定 46
RADIUS サーバまたはサーバ グループの手動モニタリング 47
RADIUS 設定の確認 48
RADIUS サーバ統計情報の表示 48
RADIUS の設定例 48
RADIUS の機能の履歴 48
TACACS+ の設定 51
TACACS+ について 51
ユーザ ログインにおける TACACS+ の動作 52
デフォルトの TACACS+ サーバ暗号化タイプと事前共有キー 52
TACACS+ サーバのモニタリング 53
ベンダー固有属性 53
シスコの VSA 形式 54
TACACS+ の前提条件 54

TACACS+ の注意事項と制約事項 54
TACACS+ のデフォルト設定 55
「Configuring TACACS+」 55
TACACS+ のイネーブル化またはディセーブル化 58
共有キーの設定 59
TACACS+ サーバ ホストの設定 61
TACACS+ サーバ グループの設定 62
TACACS+ サーバの誘導要求のイネーブル化 64
TACACS+ のグローバル タイムアウト間隔の設定 65
個別 TACACS+ ホストのタイムアウト間隔の設定 66
TACACS+ ホストの TCP ポートの設定 67
TACACS+ ホストのモニタリングの設定 68
TACACS+ グローバル デッド タイム間隔の設定 70
TACACS+ ホストの統計情報の表示 71
TACACS+ の設定例 71
TACACS+ 機能の履歴 71
SSH の設定 73
SSH に関する情報 73
SSH サーバ 73
SSH クライアント 73
SSH サーバ キー 74
SSH の前提条件 74
SSH の注意事項および制約事項 75
デフォルト設定 75
SSH の設定 75
SSH サーバ キーの生成 75
公開キーを持つユーザ アカウントの設定 77
OpenSSH キーの設定 77
IETF または PEM キーの設定 78
SSH セッションの開始 79
SSH ホストのクリア 80
SSH サーバのディセーブル化 80

SSH サーバ キーの削除 81
SSH セッションのクリア 83
SSH の設定の確認 83
SSH の設定例 84
SSH 機能の履歴 84
Telnet の設定 87
Telnet サーバの概要 87
Telnet の前提条件 87
Telnet の注意事項と制限事項 87
Telnet のデフォルト設定 88
Telnet の設定 88
Telnet サーバのディセーブル化 88
リモート装置との IP Telnet セッションの開始 89
Telnet セッションのクリア 89
Telnet の設定の確認 90
Telnet 機能の履歴 91
IP ACL の設定 93
ACL について 93
ACL のタイプと適用 94
ACL の適用順序 94
ルール 94
送信元と宛先 95
プロトコル 95
暗黙のルール 95
その他のフィルタリング オプション 95
シーケンス番号 96
IP ACL の前提条件 96
IP ACL の注意事項と制約事項 96
IP ACL のデフォルト設定 97
IP ACL の設定 97
IP ACL の作成 97
IP ACL の変更 98

IP ACL の削除 99
IP ACL 内のシーケンス番号の変更 100
IP ACL のポート プロファイルへの追加 101
管理インターフェイスへの IP ACL の適用 102
IP ACL の設定の確認 103
IP ACL のモニタリング 104
IP ACL の機能の履歴 104

はじめに

ここでは、次の項について説明します。

- 対象読者，ix ページ
- 表記法，ix ページ
- Cisco Nexus 1000V InterCloud の関連資料，xi ページ
- マニュアルに関するフィードバック ，xii ページ
- マニュアルの入手方法およびテクニカル サポート，xii ページ

対象読者

このマニュアルは、Cisco Nexus デバイスのコンフィギュレーションおよびメンテナンスを担当するネットワーク管理者を対象としています。

このマニュアルは、次のような経験と知識を持つネットワーク管理者とサーバ管理者を対象としています。

- 仮想化の知識
- VMM ソフトウェアを使用した仮想マシンの作成と VMware vSwitch の設定
- Amazon Web Service（AWS）などのプロバイダー クラウドのアカウントを作成できること。
- VMware vNetwork Distributed Switch の知識は必要ありません。

表記法

コマンドの説明には、次のような表記法が使用されます。

表記法	説明
bold	太字の文字は、表示どおりにユーザが入力するコマンドおよびキーワードです。
italic	イタリック体の文字は、ユーザが値を入力する引数です。
[x]	省略可能な要素（キーワードまたは引数）は、角カッコで囲んで示しています。
[x | y]	いずれか 1 つを選択できる省略可能なキーワードや引数は、角カッコで囲み、縦棒で区切って示しています。
{x | y}	必ずいずれか1つを選択しなければならない必須キーワードや引数は、波カッコで囲み、縦棒で区切って示しています。
[x {y | z}]	角カッコまたは波カッコが入れ子になっている箇所は、任意または必須の要素内の任意または必須の選択肢であることを表します。 角カッコ内の波カッコと縦棒は、省略可能な要素内で選択すべき必須の要素を示しています。
`variable`	ユーザが値を入力する変数であることを表します。イタリック体が使用できない場合に使用されます。
string	引用符を付けない一組の文字。 stringの前後には引用符を使用しません。引用符を使用すると、その引用符も含めてstringとみなされます。

例では、次の表記法を使用しています。

表記法	説明
`screen フォント`	スイッチが表示する端末セッションおよび情報は、screenフォントで示しています。
`太字の screen フォント`	ユーザが入力しなければならない情報は、太字の screen フォントで示しています。
イタリック体の *screen* フォント	ユーザが値を指定する引数は、イタリック体の screen フォントで示しています。
<>	パスワードのように出力されない文字は、山カッコ（<>）で囲んで示しています。
[ ]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。

表記法	説明
!、#	コードの先頭に感嘆符（!）またはポンド記号（#）がある場合には、コメント行であることを示します。

このマニュアルでは、次の表記法を使用しています。

（注） 「注釈」です。 役立つ情報やこのマニュアルに記載されていない参照資料を紹介しています。

注意 「要注意」の意味です。 機器の損傷またはデータ損失を予防するための注意事項が記述されています。

Cisco Nexus 1000V InterCloud の関連資料

この項では、Cisco Nexus 1000V InterCloud とともに使用されるマニュアルの一覧を示します。これらのマニュアルは、Cisco.com の次に示す URL で入手できます。

http://www.cisco.com/en/US/partner/products/ps12904/tsd_products_support_series_home.html

一般情報

『*Cisco Nexus 1000V InterCloud Release Notes*』

インストール & アップグレード

『*Cisco Nexus 1000V InterCloud Installation Guide*』

コンフィギュレーション ガイド

『*Cisco Nexus 1000V InterCloud License Configuration Guide*』

『*Cisco Nexus 1000V InterCloud High Availability and Redundancy Configuration Guide*』

『*Cisco Nexus 1000V InterCloud Interface Configuration Guide*』

『*Cisco Nexus 1000V InterCloud Layer 2 Configuration Guide*』

『*Cisco Nexus 1000V InterCloud Port Profile Configuration Guide*』

『*Cisco Nexus 1000V インタークラウド セキュリティ コンフィギュレーション ガイド*』

『*Cisco Nexus 1000V InterCloud System Management Configuration Guide*』

リファレンス

『*Cisco Nexus 1000V InterCloud Command Reference*』

『*Cisco Nexus 1000V InterCloud Verified Scalability Reference*』

『*Cisco Nexus 1000V MIB Quick Reference*』

トラブルシューティング & アラート

『*Cisco Nexus 1000V Password Recovery Procedure*』

Cisco Nexus 1000V のマニュアル

Cisco Nexus 1000V for VMware のマニュアル

http://www.cisco.com/en/US/products/ps9902/tsd_products_support_series_home.html

Cisco Prime Network Services Controller のマニュアル

http://www.cisco.com/en/US/products/ps13213/tsd_products_support_series_home.html

マニュアルに関するフィードバック

このマニュアルに関する技術的なフィードバック、または誤りや記載もれなどお気づきの点がございましたら、HTML ドキュメント内のフィードバック フォームよりご連絡ください。ご協力をよろしくお願いいたします。

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

『*What's New in Cisco Product Documentation*』は RSS フィードとして購読できます。また、リーダー アプリケーションを使用してコンテンツがデスクトップに直接配信されるように設定することもできます。 RSS フィードは無料のサービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。

第 1 章

概要

この章の内容は、次のとおりです。

- ユーザ アカウント，1 ページ
- 認証、許可、アカウンティング，1 ページ
- RADIUS セキュリティ プロトコル，2 ページ
- TACACS+ セキュリティ プロトコル，2 ページ
- SSH，2 ページ
- Telnet，3 ページ
- アクセス コントロール リスト，3 ページ

ユーザ アカウント

Cisco Nexus 1000V へのアクセスは、各ユーザに許可される特定のアクションを定義するユーザ アカウントを設定することで実現されます。 ユーザ アカウントは最大 256 個作成できます。 管理者は、各ユーザ アカウントに対して、ロール、ユーザ名、パスワード、および有効期限を定義します。

認証、許可、アカウンティング

認証、許可、アカウンティング（AAA）は、3 つの独立した、一貫性のあるモジュラ型のセキュリティ機能を設定するためのアーキテクチャ フレームワークです。

- 認証：ログイン/パスワード ダイアログ、チャレンジ/レスポンス、メッセージング サポート、および暗号化（選択したセキュリティ プロトコルに基づく）などによるユーザの識別方法を提供します。 認証は、ユーザに対してネットワークとネットワーク サービスへのアクセスを許可する前に、ユーザの識別を行う方法です。 AAA 認証を設定するには、まず認証方式の名前付きリストを定義し、そのリストを各種インターフェイスに適用します。

- 認可：ワンタイム許可またはサービスごとの許可、ユーザ単位のアカウント リストとプロファイル、ユーザ グループ サポート、および IP、IPX、ARA、Telnet のサポートなど、リモート アクセスの制御方法を提供します。 RADIUS や TACACS+ などのリモート セキュリティ サーバは、適切なユーザで該当する権利を定義した属性値（AV）のペアをアソシエートすることによって、ユーザに特定の権限を付与します。 AAA 許可は、ユーザが何を実行する権限を与えられるかを表す一連の属性を組み立てることで機能します。 これらの属性とデータベースに格納されているユーザの情報とが比較され、その結果が AAA に返されてユーザの実際の権限と制限事項が決定されます。
- アカウンティング：ユーザ ID、開始時刻と終了時刻、実行コマンド（PPP など）、パケット数、バイト数といった、課金、監査、およびレポートに使用するセキュリティ サーバ情報の収集と送信を行う手段を提供します。 アカウンティングを使用することで、ユーザがアクセスしているサービスや、ユーザが消費しているネットワーク リソース量を追跡できます。

（注） 認証は AAA と別個に設定することができます。 ただし RADIUS または TACACS+ を使用する場合や、バックアップの認証方式を設定する場合は、AAA を設定する必要があります。

RADIUS セキュリティ プロトコル

AAA は、ネットワーク アクセス サーバと RADIUS セキュリティ サーバ間の通信を確立します。 RADIUS は、不正アクセスからネットワークを保護する分散型クライアント/サーバ システムで、AAA を使用して実装されます。 シスコの実装では RADIUS クライアントは Cisco ルータ上で稼働します。認証要求は、すべてのユーザ認証情報とネットワーク サービス アクセス情報が格納されている中央の RADIUS サーバに送信されます。

TACACS+ セキュリティ プロトコル

AAA は、ネットワーク アクセス サーバと TACACS+ セキュリティ サーバ間の通信を確立します。

TACACS+ は、ルータまたはネットワーク アクセス サーバにアクセスしようとするユーザの検証を集中的に行うセキュリティ アプリケーションで、AAA を使用して実装されます。 TACACS+ サービスは、通常 UNIX または Windows NT ワークステーション上で稼働する TACACS+ デーモンのデータベースで管理されます。 TACACS+ は独立したモジュラ型の認証、許可、アカウンティング機能を提供します。

SSH

Secure Shell（SSH; セキュア シェル）サーバを使用すると、SSH クライアントはデバイスとの間でセキュアな暗号化された接続を確立できます。 SSH は強化暗号化を使用して認証を行います。 SSH サーバは、市販の一般的な SSH クライアントとの相互運用が可能です。

SSH クライアントは、市販の一般的な SSH サーバと連動します。

Telnet

Telnet プロトコルは、ホストとの TCP/IP 接続を確立するのに使用できます。 Telnet を使用すると、あるサイトのユーザが別のサイトのログインサーバと TCP 接続を確立し、デバイス間でキーストロークをやり取りできます。 Telnet は、リモート デバイス アドレスとして IP アドレスまたはドメイン名のいずれかを受け入れます。

アクセス コントロール リスト

IP ACL

IP ACL は、トラフィックをパケットのレイヤ 3 ヘッダーの IPv4 情報に基づいてフィルタリングするために使用できるルールの順序セットです。 各ルールには、パケットがルールに一致するために満たさなければならない条件のセットが規定されています。 Cisco NX-OS ソフトウェアがパケットに IP ACL を適用することを判定するときは、すべてのルールの条件に照らしてパケットを調べます。 最初の一致によってパケットを許可するか拒否するか判定します。一致するものがない場合は、Cisco NX-OS ソフトウェアは適切なデフォルト ルールを適用します。 Cisco NX-OS ソフトウェアは、許可されたパケットの処理を継続し、拒否されたパケットをドロップします。

第 2 章

ユーザ アカウントの管理

この章は、次の項で構成されています。

- ユーザ アカウントについて，5 ページ
- ユーザ アカウント作成の注意事項と制限事項，8 ページ
- ユーザ アカウント作成の注意事項，8 ページ
- ユーザ アクセスのデフォルト設定，9 ページ
- ユーザ アクセス設定の確認，17 ページ
- MIB，18 ページ
- ユーザ アカウント機能の履歴，19 ページ

ユーザ アカウントについて

Cisco Nexus 1000V へのアクセスは、各ユーザに許可される特定のアクションを定義するユーザ アカウントを設定することで実現されます。ユーザアカウントは最大256個作成できます。各ユーザ アカウントには、次の情報が含まれています。

- ロール
- ユーザ名
- パスワード
- 有効期限

ロール

ロールとは、同じグループのユーザによって共有可能なアクションを具体的に定義する規則の集合です。たとえば、次のような幅広い権限を持つロールをユーザアカウントに割り当てることが

できます。 これらのロールは Cisco Nexus 1000V 内であらかじめ定義されたものであり、変更はできません。

```
role: network-admin
  description: Predefined network admin role has access to all commands
  on the switch
  ------------------------------------------------------------------
  Rule    Perm    Type        Scope               Entity
  ------------------------------------------------------------------
  1       permit  read-write

role: network-operator
  description: Predefined network operator role has access to all read
  commands on the switch
  ------------------------------------------------------------------
  Rule    Perm    Type        Scope               Entity
  ------------------------------------------------------------------
  1       permit  read
```

管理者は、ユーザのアクセス権を定義するロールをこの他に 64 個作成できます。

各ユーザ アカウントには少なくとも 1 つのロールを割り当てる必要があり、最大 64 個を割り当てることができます。

管理者が作成できるロールでは、アクセスを許可できるコマンドがデフォルトでは次のものに限られています。 機能の設定をユーザに許可するには、規則を追加する必要があります。

- **show**
- **exit**
- **end**
- **configure terminal**

ユーザ名

ユーザ名とは、個々のユーザを特定するための一意の文字列です（たとえば「daveGreen」）。ユーザ名は、最大 28 文字で、英数字を使用でき、大文字と小文字が区別されます。 数字だけで構成されたユーザ名は許可されません。 すべてが数字のユーザ名が AAA サーバに存在し、ログインの際に入力されても、そのユーザはログインできません。

パスワード

パスワードは、大文字と小文字が区別される文字列です。パスワードによって特定のユーザによるアクセスが可能になり、不正なアクセスの防止に役立ちます。 パスワードを指定せずにユーザを追加することもできますが、そのユーザはデバイスにアクセスできなくなる可能性があります。パスワードは、強力なものでなければなりません。容易に推測できるパスワードは、不正アクセスの原因となります。

次の文字は、クリア テキスト パスワードには使用できません。

- ドル記号（$）
- スペース

- 等号（=）

次の特殊文字は、パスワードの先頭には使用できません。

- 引用符（" および '）
- 縦線（|）
- 右山カッコ（>）

次の表に、強力なパスワードの特性を示します。

表 *1*：強力なパスワードの特性

強力なパスワードに含まれるもの	強力なパスワードに含まれないもの
最低 8 文字	連続する文字（例：abcd）
大文字の英字	文字の繰り返し（例：aaabbb）
小文字の英字	辞書に載っている単語
数字	固有名詞
特殊文字	

次に、強力なパスワードの例を示します。

- If2CoM18
- 2004AsdfLkj30
- Cb1955S21

パスワード強度のチェック

デバイスによるパスワード強度のチェックは、デフォルトでは自動的に行われます。 管理者がユーザ名とパスワードを追加するときに、パスワードの強度が評価されます。 これが脆弱なパスワードの場合、次のエラー メッセージが表示されて、通知されます。

```
switch# config terminal
switch (config)# username daveGreen password davey
password is weak
Password should contain characters from at least three of the classes:
 lower case letters, upper case letters, digits, and special characters
```

パスワード強度チェックはディセーブルにすることができます。

有効期限

デフォルトでは、ユーザ アカウントは無期限に有効です。 ただし、管理者はアカウントがディセーブルになる有効期限を明示的に設定することができます。

ユーザ アカウント作成の注意事項と制限事項

- あらかじめ定義された 2 つのユーザ ロールに加えて、最大 64 個のロールを作成できます。
- 1 つのユーザ ロールに最大 256 個の規則を作成できます。
- 最大 64 個の機能グループを作成できます。
- 最大 256 人のユーザを追加できます。
- 1 つのユーザ アカウントに最大 64 個のユーザ ロールを割り当てられます。
- ローカル ユーザ アカウントと同じ名前のリモート ユーザ アカウントが AAA サーバ上に存在する場合は、そのリモート ユーザには AAA サーバ上で設定されているユーザ ロールでなく、ローカル ユーザ アカウントのユーザ ロールが適用されます。

ユーザ アカウント作成の注意事項

- ユーザ アカウントは最大 256 個追加できます。
- ユーザ アカウントに対する変更が有効になるのは、そのユーザがログインして新しいセッションを作成したときです。
- 次に示す語をユーザ アカウントで使用しないでください。 これらは、他の目的のために予約されています。

adm	gdm	mtuser	rpcuser
bin	gopher	neews	shutdown
daemon	haltlp	nobody	sync
FTP	mail	nscd	sys
ftpuser	mailnull	operator	uucp
games	man	rpc	xfs

- 追加するユーザ パスワードは、クリア テキストと暗号化テキストのどちらでも指定できます。

- クリアテキストのパスワードは、実行コンフィギュレーションに保存される前に暗号化されます。
- 暗号化されたパスワードは、それ以上の暗号化を行わずに実行コンフィギュレーションに保存されます。

- 1 つのユーザ アカウントが最大 64 個のロールを持つことができますが、少なくとも 1 つのロールを持つ必要があります。 ロールの詳細については、ユーザ アカウント作成の注意事項, （8 ページ）を参照してください。
- パスワードを指定しない場合、そのユーザがログインできなくなる可能性があります。
- パスワードでなく SSH 公開キーを使用する手順については、OpenSSH キーの設定, （77 ページ）を参照してください。

ユーザ アクセスのデフォルト設定

パラメータ	デフォルト
ユーザ アカウント パスワード	未定義
ユーザ アカウントの有効期限	なし
ユーザ アカウント ロール	network-operator
インターフェイス ポリシー	すべてのインターフェイスにアクセス可能
VLAN ポリシー	すべての VLAN にアクセス可能

ユーザ アクセスの設定

パスワード強度チェックのイネーブル化

Cisco Nexus 1000V でパスワード強度のチェックをイネーブルにして、ユーザ アカウントに対して弱いパスワードを設定できないようにするには、この手順を使用します。

パスワード強度のチェックは、デフォルトではイネーブルになっています。 ディセーブルにされていても、ここで説明する手順を実行すれば再度イネーブルにすることができます。

はじめる前に

この手順を開始する前に、EXEC モードで CLI にログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **password strength-check**	パスワードの強度確認をイネーブルにします。デフォルトではイネーブルになっています。 パスワード強度のチェックをディセーブルにするには、このコマンドの no 形式を使用します。
ステップ 3	switch(config)# **show password strength-check**	（任意） パスワードの強度の確認の設定を表示します。
ステップ 4	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を永続的に保存します。

```
switch# configure terminal
switch(config)# password strength-check
switch(config)# show password strength-check
Password strength check enabled
switch(config)# copy running-config startup-config
```

パスワード強度チェックのディセーブル化

はじめる前に

この手順を開始する前に、EXEC モードで CLI にログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **no password strength-check**	パスワード強度のチェックをディセーブルにします。 デフォルトではイネーブルになっています。
ステップ 3	switch(config)# **show password strength-check**	（任意） パスワードの強度の確認の設定を表示します。

	コマンドまたはアクション	目的
ステップ 4	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を永続的に保存します。

```
switch# configure terminal
switch(config)# no password strength-check
switch(config)# show password strength-check
switch(config)# copy running-config startup-config
```

ユーザ アカウントの作成

はじめる前に

この手順を開始する前に、EXEC モードで CLI にログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **show role**	（任意） ユーザに割り当てることのできるロールを表示します。
ステップ 3	switch(config)# **username** *name* [**password** [**0** | **5**] *password*] [**expire date**] [**role** *role-name*]	ユーザ アカウントを作成します。 引数およびキーワードは次のとおりです。 • name：最大 28 文字の英数字ストリングです。大文字と小文字が区別されます。 • password：デフォルトのパスワードは定義されていません。 ◦ 0 =（デフォルト）入力するパスワードがクリア テキストであることを指定します。 Cisco Nexus 1000V は、実行コンフィギュレーションに保存する前にクリア テキストのパスワードを暗号化します。 例では、実行コンフィギュレーションのパスワード 4Ty18Rnt は password 5 形式で暗号化されています。

	コマンドまたはアクション	目的
		◦ 5 = 入力したパスワードがすでに暗号化形式であることを指定します。 Cisco Nexus 1000V は、実行コンフィギュレーションに保存する前にパスワードを暗号化しません。 ユーザのパスワードは、設定ファイルでは表示されません。 • expire date：YYYY-MM-DD。 デフォルトは無期限です。 • role：少なくとも 1 つのロールを割り当てる必要があります。 最大 64 個のロールを割り当てることができます。 デフォルトのロールは、**network-operator** です。
ステップ 4	switch(config)# **show user-account** *username*	新しいユーザ アカウントの設定を表示します。
ステップ 5	switch(config)# **copy running-config startup-config**	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を永続的に保存します。

```
switch# configure terminal
switch(config)# show role
switch(config)# username NewUser password 4Ty18Rnt
switch(config)# show user-account NewUser
user: NewUser
     this user account has no expiry date
     roles:network-operator network-admin
switch# copy running-config startup-config
```

ロールの作成

はじめる前に

- この手順を開始する前に、EXEC モードで CLI にログインする必要があります。
- 最大 64 個のユーザ ロールを設定できます。
- 1 つのロールに最大 256 個の規則を設定できます。
- 1 つのロールを複数のユーザに割り当てることができます。

- 規則番号は、その規則が適用される順序を表します。規則は番号の降順で適用されます。 たとえば、あるロールに 3 つの規則がある場合は、最初に規則 3 が適用され、次に規則 2、最後に規則 1 が適用されます。
- デフォルトでは、管理者が作成するユーザ ロールでアクセスを許可できるコマンドは、show、exit、end、および configure terminal コマンドだけです。 機能の設定をユーザに許可するには、規則を追加する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **role name** *role-name*	ユーザ ロールに名前をつけて、そのロールのロール コンフィギュレーション モードに切り替えます。 *role-name*は大文字と小文字が区別される 16 文字以下の英数字文字列です。
ステップ 3	switch(config-role)# **description** *description-string*	（任意） ロールの説明を設定します。説明にはスペースを含めることができます。
ステップ 4	switch(config-role)# **rule** *number* {**deny**| **permit**} **command** *command-string* • switch(config-role)# **rule** *number* {**deny** | **permit**} {**read** | **read-write**} すべての操作を許可または拒否する 1 個の規則を作成します。 • switch(config-role)# **rule** *number* {**deny** | **permit**} {**read** | **read-write**} **feature** *feature-name* 機能アクセスの規則を作成します。 **show role feature** コマンドを実行すると、使用可能な機能の一覧が表示されます。 • switch(config-role)# **rule** *number* {**deny** | **permit**} {**read** | **read-write**} **feature-group** *group-name* 機能グループ アクセスの規則を作成します。	特定のコマンドを許可または拒否する規則を作成します。 指定するコマンドには、スペースや正規表現を含めることができます。

	コマンドまたはアクション	目的
	show role feature-group コマンドを使用すれば、機能グループのリストが表示されます。 例： この例では、**clear users** コマンドへのアクセスを拒否する規則を設定します。	
ステップ 5	指定したロールに必要なすべての規則を作成するには、ステップ 4 を繰り返します。	
ステップ 6	switch(config-role)# **show role**	（任意） ユーザ ロールの設定を表示します。
ステップ 7	switch(config-role)# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

```
switch# configure terminal
switch(config)# role name UserA
switch(config-role)# description Prohibits use of clear commands
switch(config-role)# rule 1 deny command clear users
switch(config-role)# rule 2 deny read-write

switch# configure terminal
switch(config)# role name UserA
switch(config-role)# rule 3 permit read feature snmp
switch(config-role)# rule 2 permit read feature dot1x
switch(config-role)# rule 1 deny command clear *
```

機能グループの作成

ここでは、機能グループを作成して設定する手順を説明します。 最大 64 個のカスタム機能グループを作成できます。

はじめる前に

- この手順を開始する前に、EXEC モードで CLI にログインする必要があります。
- 最大 64 個のカスタム機能グループを作成できます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **role feature-group name** *group-name*	グループ名を指定して、そのグループのロール機能グループ コンフィギュレーション モードを開始します。 group-name：最大 32 文字の英数字ストリングです。大文字と小文字が区別されます。
ステップ 3	switch(config-role-featuregrp)# **show role feature**	機能グループを定義するときに使用できる機能の一覧を表示します。
ステップ 4	switch(config-role-featuregrp)# **feature** *feature-name*	機能を機能グループに追加します。 機能グループに追加するすべての機能に対してこの手順を繰り返します。
ステップ 5	switch(config-role-featuregrp)# **show role feature-group**	（任意） 機能グループの設定を表示します。
ステップ 6	switch(config-role-featuregrp)# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

インターフェイス アクセスの設定

デフォルトでは、ロールによってすべてのインターフェイスへのアクセスが許可されます。 すべてのインターフェイスへのアクセスを拒否し、選択したインターフェイスへのアクセスを許可して、すでに作成されているロールを変更します。

はじめる前に

この手順を開始する前に、次のことを確認してください。

- CLI に EXEC モードでログインしていること。
- 1 つまたは複数のユーザ ロールを作成していること。 この手順では、作成済みのロールに変更を加えます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config) # **role name** *role-name*	ユーザ ロールを指定して、そのロールのロール コンフィギュレーション モードを開始します。
ステップ 3	switch(config-role)# **interface policy deny**	インターフェイス コンフィギュレーション モードを開始し、このロールによるすべてのインターフェイス アクセスを拒否します。 これで、**permit interface** コマンドを使用して明示的に定義しない限り、このロールはインターフェイスに一切アクセスできなくなりました。
ステップ 4	switch(config-role-interface)# **permit interface***interface-list*	このロールに割り当てられたユーザにアクセスを許可するインターフェイスを指定します。 このロールに割り当てられたユーザにアクセスを許可するインターフェイスがすべて指定されるまで、このコマンドを繰り返します。
ステップ 5	switch(config-role-interface)# **show role** *role-name*	（任意） ロール設定を表示します。
ステップ 6	switch(config-role-featuregrp)# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

VLAN アクセスの設定

デフォルトでは、すべての VLAN へのアクセスが許可されます。 この手順では、すべての VLAN へのアクセスを拒否してから、選択した VLAN へのアクセスを許可して、作成済みのロールを変更します。

はじめる前に

この手順を開始する前に、次のことを実行する必要があります。

- EXEC モードで CLI にログインしてください。
- 1 つまたは複数のユーザ ロールを作成しておいてください。 この手順では、作成済みのロールに変更を加えます。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config) # **role name** *role-name*	ユーザ ロールを指定し、ロール コンフィギュレーション モードを開始します。
ステップ 3	switch(config-role)# **vlan policy deny**	VLAN コンフィギュレーション モードを開始し、このロールによるすべての VLAN アクセスを拒否します。 これで、permit vlan コマンドを使用して明示的に定義しない限り、このロールは VLAN に一切アクセスできなくなりました。
ステップ 4	switch(config-role-vlan)# **permit vlan** *vlan-range*	このロールに割り当てられたユーザにアクセスを許可する VLAN を指定します。 ダッシュを使用して VLAN の範囲を指定します（1-9 または 20-30 など）。 このロールに割り当てられたユーザにアクセスを許可する VLAN がすべて指定されるまで、このコマンドを繰り返します。
ステップ 5	switch(config-role)# **show role** *role-name*	（任意） ロール設定を表示します。 role-name は、作成したロールに割り当てた名前です。
ステップ 6	switch(config-role)# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

ユーザ アクセス設定の確認

次のいずれかのコマンドを使用して、設定を確認します。

コマンド	目的
show role	使用可能なユーザ ロールとその規則を表示します。
show role feature	使用可能な機能のリストを表示します。

コマンド	目的
show role feature-group	使用可能な機能グループのリストを表示します。
show startup-config security	スタートアップコンフィギュレーションのユーザ アカウント設定を表示します。
show running-config security [**all**]	実行コンフィギュレーションのユーザアカウント設定を表示します。 **all** キーワードを指定すると、ユーザアカウントのデフォルト値が表示されます。
show user-account	ユーザ アカウント情報を表示します。

設定例

機能グループ作成の設定例

```
switch# config terminal
switch(config-role)# role feature-group name security-features
switch(config-role)# feature radius
switch(config-role)# feature tacacs
switch(config-role)# feature dot1x
switch(config-role)# feature aaa
switch(config-role)# feature snmp
switch(config-role)# feature acl
switch(config-role)# feature access-list
```

ロール作成の設定例

```
switch# config terminal
switch(config)# role name UserA
switch(config-role)# rule 3 permit read feature snmp
switch(config-role)# rule 2 permit read feature dot1x
switch(config-role)# rule 1 deny command clear *
```

MIB

MIB	MIB のリンク
CISCO-COMMON-MGMT-MIB	MIB を検索およびダウンロードするには、次の URL にアクセスしてください。 http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

ユーザ アカウント機能の履歴

この表には、機能の追加や変更によるリリースの更新内容のみが記載されています。

機能名	リリース	機能情報
ユーザ アカウント	Release 5.2(1)IC1(1.1)	この機能が導入されました。

第 3 章

AAA の設定

この章は、次の項で構成されています。

- AAA について，21 ページ
- AAA の前提条件，24 ページ
- 注意事項と制約事項，25 ページ
- AAA のデフォルト設定，25 ページ
- AAA の設定，25 ページ
- AAA 設定の確認，27 ページ
- AAA の設定例，28 ページ
- AAA 機能の履歴，28 ページ

AAA について

AAA セキュリティ サービス

AAA は、ユーザ ID とパスワードの組み合わせに基づいて、ユーザを認証および許可するために使用されます。 キーは、AAA サーバとの通信を保護します。

多くの場合、AAA は RADIUS または TACACS+ などのプロトコルを使用してセキュリティ機能を管理します。 ルータまたはアクセス サーバがネットワーク アクセス サーバとして動作している場合は、ネットワーク アクセス サーバと RADIUS または TACACS+ セキュリティ サーバとの間の通信を確立する手段に、AAA が使用されます。

AAA は主要な（推奨される）アクセス コントロール方式ですが、さらに、ローカル ユーザ名認証、回線パスワード認証、イネーブル パスワード認証など、AAA の範囲外で簡単なアクセス コントロールを行う機能も用意されています。 ただし、これらの機能では、AAA を使用した場合と同レベルのアクセス コントロールは実現できません。

次のサービスごとに別個の AAA 設定が作成されます。

- User Telnet または Secure Shell（SSH）ログイン認証
- コンソール ログイン認証
- ユーザ管理セッション アカウンティング

AAAサービスコンフィギュレーションオプション	関連コマンド
Telnet または SSH ログイン	aaa authentication login default
コンソール ログイン	aaa authentication login console

認証

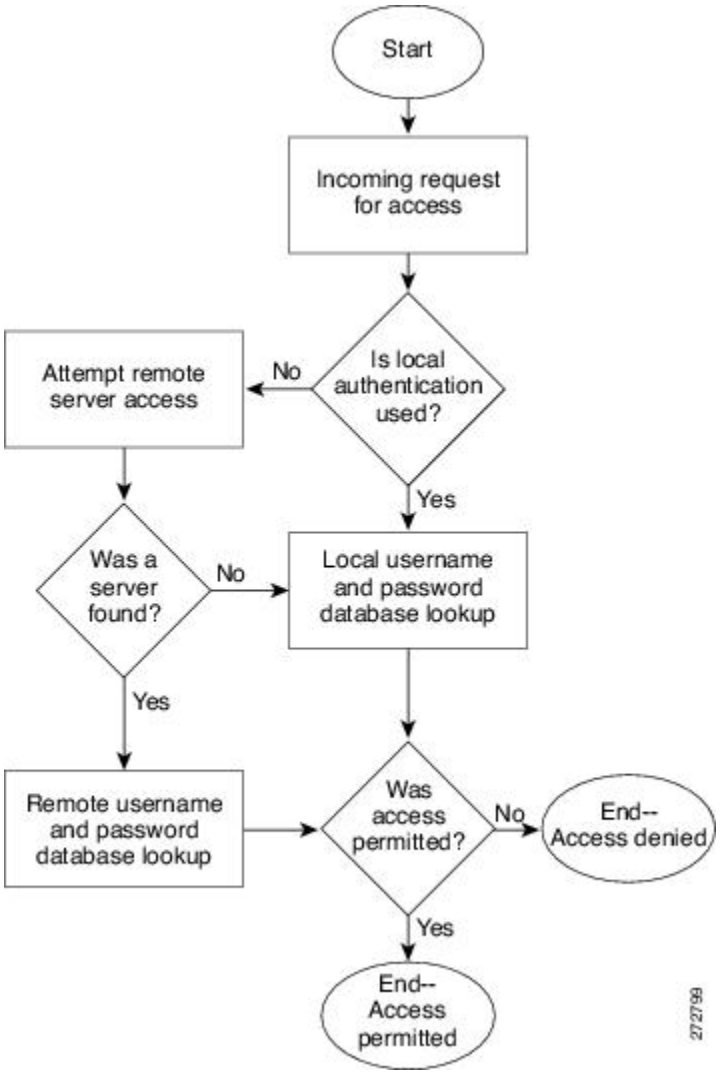
認証は、ログイン/パスワード ダイアログ、チャレンジ/レスポンス、メッセージング サポート、および選択したセキュリティ プロトコルによっては暗号化など、ユーザを識別する手段を提供します。 認証は、ユーザに対してネットワークとネットワーク サービスへのアクセスを許可する前に、ユーザの識別を行う方法です。 AAA認証を設定するには、まず認証方式の名前付きリストを定義し、そのリストを各種インターフェイスに適用します。

認証は次のように実行されます。

認証方式	説明
ローカル データベース	ユーザ名またはパスワードのローカル ルックアップデータベースによって次の認証を行います。 • コンソール ログイン認証 • ユーザ ログイン認証 • ユーザ管理セッション アカウンティング
リモート RADIUS または TACACS+ サーバ	ユーザ名またはパスワードのローカル ルックアップデータベースによって次の認証を行います。 • コンソール ログイン認証 • ユーザ ログイン認証 • ユーザ管理セッション アカウンティング

認証方式	説明
なし	ユーザ名だけで次の認証を行います。 • コンソール ログイン認証 • ユーザ ログイン認証 • ユーザ管理セッション アカウンティング

図 *1* : ユーザ ログインの認証



許可

許可では、ユーザが実行を許可される操作を制限します。 ワンタイム許可またはサービスごとの許可、ユーザ単位のアカウント リストとプロファイル、ユーザ グループ サポート、および IP、IPX、ARA、Telnet のサポートなど、リモート アクセスの制御方法を提供します。

RADIUS や TACACS+ などのリモート セキュリティ サーバは、適切なユーザで該当する権利を定義した属性値（AV）のペアをアソシエートすることによって、ユーザに特定の権限を付与します。 AAA 許可は、ユーザが何を実行する権限を与えられるかを表す一連の属性を組み立てることで機能します。 これらの属性とデータベースに格納されているユーザの情報とが比較され、その結果が AAA に返されてユーザの実際の権限と制限事項が決定されます。

アカウンティング

アカウンティングで、ユーザ識別、開始時刻と終了時刻、実行コマンド（PPP など）、パケット数、バイト数などといったセキュリティ サーバ情報の収集と送信を行い、課金、監査、およびレポートに使用する手段を提供します。 アカウンティングを使用することで、ユーザがアクセスしているサービスや、ユーザが消費しているネットワーク リソース量を追跡できます。

アカウンティングでは、すべての SVS 管理セッションを追跡し、ログに記録して管理します。 この情報を使用して、トラブルシューティングや監査のためのレポートを生成できます。 アカウンティング ログは、ローカルに保存することもできれば、リモート AAA サーバに送信することもできます。

AAA サーバ グループ

リモート AAA サーバ グループは、1 台のリモート AAA サーバが応答しない場合にフェールオーバーを提供できます。すなわち、グループの最初のサーバが応答しない場合に、サーバが応答するまでグループ内の次のサーバで試行します。 複数のサーバ グループがある場合、同じ方法で、相互にフェールオーバーを提供できます。

すべてのリモート サーバ グループが応答しない場合は、ローカル データベースが認証に使用されます。

AAA の前提条件

- 少なくとも 1 台の TACACS+ サーバまたは RADIUS サーバが IP で到達可能になっていること。
- VSM が AAA サーバのクライアントとして設定されていること。
- 共有秘密キーが VSM およびリモート AAA サーバに設定されていること。

注意事項と制約事項

Cisco Nexus 1000V では、すべてが数字のユーザ名はサポートされず、すべてが数字のローカルユーザ名は作成されません。 すべてが数字のユーザ名が AAA サーバにすでに存在し、ログインの際に入力された場合、Cisco Nexus 1000V はそのユーザを認証します。

AAA のデフォルト設定

パラメータ	デフォルト
コンソール認証方式	local
デフォルト認証方式	local
ログイン認証失敗メッセージ	無効

AAA の設定

ログイン認証方式の設定

TACACS+ サーバ グループを使用して認証が行われる場合は、グループが追加済みです。

はじめる前に

この手順を開始する前に、EXEC モードで CLI にログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **aaa authentication login** {**console** | **default**} {**group** *group-list* [**none**] | **local** | **none**}	コンソールまたはデフォルトログイン認証方式を設定します。 次のキーワードと引数があります。 • group：サーバ グループによって認証が行われます。 • group-list：スペースで区切ったサーバ グループ名のリストです。認証なしの場合は none です。 • group-list none：認証なし。

	コマンドまたはアクション	目的
		• local：ローカル データベースが認証に使用されます。 （注） デフォルトはlocalで、方式が設定されていない場合、または設定されたすべての認証方式で応答が得られなかった場合に使用されます。 • none：ユーザ名によって認証が行われます
ステップ 3	switch(config)# **exit**	グローバルコンフィギュレーションモードを終了し、EXEC モードに戻ります。
ステップ 4	switch# **show aaa authentication**	（任意） 設定されたログイン認証方式を表示します。
ステップ 5	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

```
switch# configure terminal
switch(config)# aaa authentication login console group tacgroup
switch(config)# exit
switch# show aaa authentication
         default: group tacgroup
         console: group tacgroup
switch# copy running-config startup-config
switch#
switch# configure terminal
switch(config)# aaa authentication login default group tacacs
switch(config)# aaa authentication login console group tacacs
```

ログイン認証失敗メッセージのイネーブル化

リモートAAAサーバが応答しない場合のログイン認証失敗メッセージの表示をイネーブルにするには、次の手順を実行します。

次に、ログイン認証エラー メッセージを示します。

```
Remote AAA servers unreachable; local authentication done.
Remote AAA servers unreachable; local authentication failed.
```

はじめる前に

この手順を開始する前に、EXEC モードで CLI にログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **aaa authentication login error-enable**	ログイン認証失敗メッセージをイネーブルにします。 デフォルトではディセーブルになっています。
ステップ 3	switch(config)# **exit**	グローバル コンフィギュレーション モードを終了して、EXEC モードに戻ります。
ステップ 4	switch# **show aaa authentication login error-enable**	（任意） ログイン失敗メッセージの設定を表示します。
ステップ 5	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

```
switch# configure terminal
switch(config)# aaa authentication login error-enable
switch(config)# exit
switch# show aaa authentication login error-enable
enabled
```

AAA 設定の確認

次のいずれかのコマンドを使用して、設定を確認します。

コマンド	目的
show aaa authentication [**login** {**error-enable** | **mschap**}]	AAA 認証情報を表示します。
show aaa groups	AAA サーバ グループの設定を表示します。
show running-config aaa [**all**]	実行コンフィギュレーションの AAA 設定を表示します。
show startup-config aaa	スタートアップコンフィギュレーションのAAA設定を表示します。

例：show aaa authentication

```
switch# show aaa authentication login error-enable
disabled
switch#
```

例：show running config aaa

```
switch# show running-config aaa all
version 4.0(1)
aaa authentication login default local
aaa accounting default local
no aaa authentication login error-enable
no aaa authentication login mschap enable
no radius-server directed-request
no snmp-server enable traps aaa server-state-change
no tacacs-server directed-request
switch#
```

例：show startup-config aaa

```
switch# show startup-config aaa
version 4.0(1)
```

AAA の設定例

次に、AAA の設定例を示します。

```
aaa authentication login default group tacacs
aaa authentication login console group tacacs
```

AAA 機能の履歴

この表には、機能の追加や変更によるリリースの更新内容のみが記載されています。

機能名	リリース	機能情報
AAA	Release 5.2(1)IC1(1.1)	この機能が導入されました。

第 4 章

RADIUS の設定

この章では、Cisco NX-OS デバイスで Remote Access Dial-In User Service（RADIUS）プロトコルを設定する手順について説明します。

- RADIUS について，29 ページ
- RADIUS の前提条件，33 ページ
- 注意事項と制約事項，33 ページ
- デフォルト設定，33 ページ
- RADIUS 設定の確認，48 ページ
- RADIUS サーバ統計情報の表示，48 ページ
- RADIUS の設定例，48 ページ
- RADIUS の機能の履歴，48 ページ

RADIUS について

RADIUS 分散クライアント/ サーバ システムを使用すると、不正アクセスからネットワークを保護できます。 シスコの実装では、RADIUS クライアントは Cisco NX-OS デバイス上で稼働します。認証要求とアカウンティング要求は、すべてのユーザ認証情報とネットワーク サービスアクセス情報が格納されている中央の RADIUS サーバに送信されます。

RADIUS ネットワーク環境

RADIUS は、高度なセキュリティを必要とし、同時にリモートユーザのネットワーク アクセスを維持する必要があるさまざまなネットワーク環境に実装できます。

RADIUS は、アクセス セキュリティを必要とする次のネットワーク環境で使用します。

- RADIUS をサポートしている複数ベンダーのネットワーク デバイスを使用したネットワーク たとえば、複数ベンダーのネットワーク デバイスで、単一の RADIUS サーバ ベースのセキュリティ データベースを使用できます。
- すでに RADIUS を使用中のネットワーク。 RADIUS 機能を持つ Cisco NX-OS デバイスをネットワークに追加できます。 この作業は、AAA サーバに移行するときの最初の手順になります。
- リソース アカウンティングが必要なネットワーク。 RADIUS アカウンティングは、RADIUS 認証または RADIUS 許可とは個別に使用できます。 RADIUS アカウンティング機能を使用すると、サービスの開始および終了時に、セッション中に使用したリソース（時間、パケット、バイトなど）の量を示すデータを送信できます。 インターネット サービス プロバイダー（ISP）は、RADIUS アクセス コントロールおよびアカウンティング用ソフトウェアのフリーウェア版を使用して、特殊なセキュリティおよび課金ニーズに対応しています。
- 認証プロファイルをサポートするネットワーク ネットワークで RADIUS サーバを使用すると、AAA 認証を設定し、ユーザごとのプロファイルをセットアップできます。 ユーザ単位のプロファイルにより、既存の RADIUS ソリューションを使用するポートの管理性が向上し、共有リソースを効率的に管理して、各種のサービスレベル契約を提供できるようになります。

RADIUS の動作

RADIUS を使用する Cisco NX-OS デバイスに、ユーザがログインおよび認証を試みると、次のように処理されます。

1. ユーザが、ユーザ名とパスワードの入力を求められ、入力します。
2. ユーザ名および暗号化されたパスワードが、ネットワーク経由で RADIUS サーバに送信されます。
3. ユーザは、RADIUS サーバから次のいずれかの応答を受信します。
   - ACCEPT：ユーザが認証されたことを表します。
   - REJECT：ユーザは認証されず、ユーザ名とパスワードの再入力を求められるか、アクセスを拒否されます。
   - CHALLENGE：RADIUS サーバによってチャレンジが発行されます。 チャレンジは、ユーザから追加データを収集します。
   - CHANGE PASSWORD：RADIUS サーバからユーザに対して新しいパスワードの選択を求める要求が発行されます。

ACCEPT または REJECT 応答には、EXEC またはネットワーク許可に使用される追加データが含まれています。 RADIUS 許可を使用するには、まず RADIUS 認証を完了する必要があります。 ACCEPT または REJECT パケットに含まれる追加データの内容は次のとおりです。

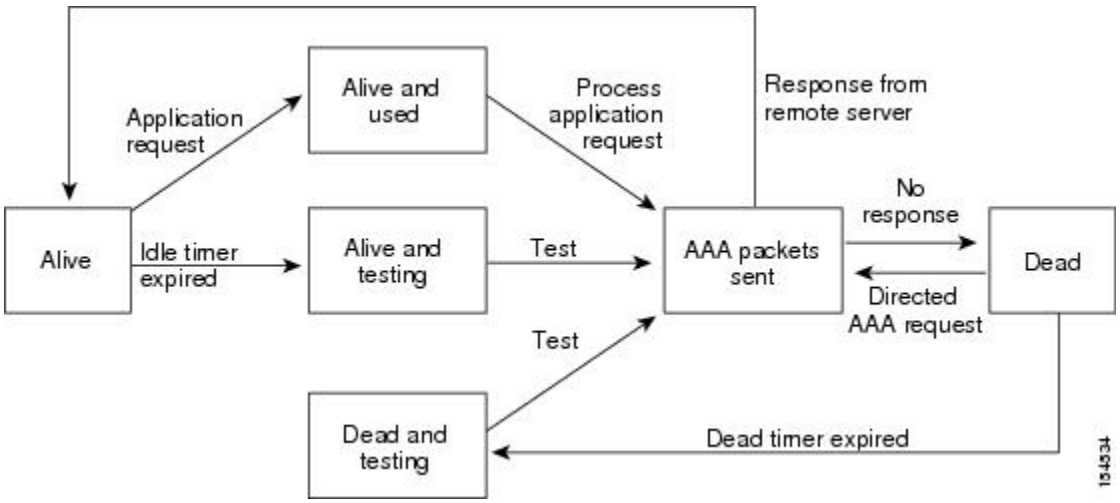
- ユーザがアクセス可能なサービス（Telnet、rlogin、または local-area transport（LAT; ローカル エリア トランスポート）接続、PPP（ポイントツーポイントプロトコル）、シリアルライン インターネット プロトコル（SLIP）、EXEC サービスなど）
- ホストまたはクライアントの IPv4 アドレス、アクセス リスト、ユーザ タイムアウトなどの接続パラメータ

RADIUS サーバ モニタリング

応答しない RADIUS サーバがあると、AAA 要求の処理が遅れることがあります。 AAA 要求の処理時間を短縮するために、RADIUS サーバを定期的にモニタして RADIUS サーバが応答している（アライブ）かどうかを調べることができます。 応答しない RADIUS サーバはデッド（dead）としてマークされ、AAA 要求は送信されません。 デッド RADIUS サーバは定期的にモニタされ、応答があればアライブ状態に戻されます。 このモニタリング プロセスでは、実際の AAA 要求が送信される前に、RADIUS サーバが稼働状態であることを確認します。 RADIUS サーバがデッドまたはアライブの状態に変わると簡易ネットワーク管理プロトコル（SNMP）トラップが生成され、障害が発生していることを示すエラー メッセージが表示されます。

（注） アライブ サーバとデッド サーバのモニタリング間隔は異なります。これらはユーザが設定できます。 RADIUS サーバ モニタリングを実行するには、テスト認証要求を RADIUS サーバに送信します。

図 *2* : ***RADIUS*** サーバの状態



ベンダー固有属性

インターネット技術特別調査委員会（IETF）が、ネットワーク アクセス サーバと RADIUS サーバの間でのベンダー固有属性（VSA）の通信のための方式を規定する標準を作成しています。IETF は、属性 26 を使用します。 VSA を使用するとベンダーは、一般的な用途には適合しない独自の拡張属性をサポートできます。 シスコの RADIUS 実装は、この仕様で推奨される形式を使用して、1 つのベンダー固有オプションをサポートしています。 シスコのベンダー ID は 9、サポートされるオプションのベンダー タイプは 1（名前付き cisco-av-pair）です。 値は、次の形式のストリングです。

```
protocol : attribute separator value *
```

protocol は、特定の認証タイプを表すシスコの属性です。 区切り文字は、必須属性の場合 =（等号）、任意の属性の場合は *（アスタリスク）です。

認証に RADIUS サーバを使用した場合、RADIUS プロトコルでは RADIUS サーバに対して、認証結果とともに権限付与情報などのユーザ属性を返すように指示します。 この許可情報は、VSA で指定されます。

次の VSA プロトコル オプションがサポートされています。

- shell：ユーザ プロファイル情報を提供する access-accept パケットで使用されるプロトコル。
- Accounting：accounting-request パケットで使用されるプロトコル。 値にスペースが含まれている場合は、二重引用符で囲む必要があります。

次の属性がサポートされます。

- roles：ユーザが属するすべてのロールの一覧です。 値フィールドは、スペースで区切られたロール名を一覧表示したストリングです。 たとえば、ユーザが属しているロールが network-operator と vdc-admin ならば、値フィールドは「network-operator vdc-admin」となります。この属性は、RADIUS サーバから送信される Access-Accept フレームの VSA 部分に格納されます。この属性はシェル プロトコル値とだけ併用できます。 次に、Cisco Access Control System（ACS）でサポートされるロール属性の例を示します。

  ```
  shell:roles="network-operator vdc-admin"
  ```

  ```
  shell:roles*"network-operator vdc-admin"
  ```

  次に、FreeRADIUS でサポートされるロール属性の例を示します。

  ```
  Cisco-AVPair = "shell:roles=\"network-operator vdc-admin\""
  ```

  ```
  Cisco-AVPair = "shell:roles*\"network-operator vdc-admin\""
  ```

  Cisco ACS を使用していて、Cisco Nexus 1000V 認証と Cisco UCS 認証の両方に同じ ACS グループを使用する場合は、次のロール属性を使用します。

  ```
  cisco-av-pair*shell:roles="network-admin admin"
  ```

（注） VSA を shell:roles*"network-operator vdc-admin" または "shell:roles*\"network-operator vdc-admin\"" として指定した場合、この VSA はオプション属性としてフラグ設定され、他のシスコ デバイスはこの属性を無視します。

- accountinginfo：標準の RADIUS アカウンティング プロトコルで処理される属性に加えて、アカウンティング情報が格納されます。 この属性は、スイッチ上の RADIUS クライアントからの Account-Request フレームの VSA 部分だけに送信されます。 この属性と共に使用できるのは、アカウンティングの Protocol Data Unit（PDU; プロトコル データ ユニット）だけです。

RADIUS の前提条件

- RADIUS サーバの IP アドレスまたはホスト名がわかっていること。
- ネットワーク内での RADIUS 通信を保護するために使用されるキーがわかっていること。
- デバイスが AAA サーバの RADIUS クライアントとして設定されていること。

注意事項と制約事項

最大 64 の RADIUS サーバを設定できます。

デフォルト設定

表 *2*：デフォルトの *RADIUS* パラメータ

パラメータ	デフォルト
サーバの役割	認証とアカウンティング
デッド タイマー間隔	0 分
再送信回数	1
再送信タイマー間隔	5 秒
アイドル タイマー間隔	0 分
サーバの定期的モニタリングのユーザ名	test

パラメータ	デフォルト
サーバの定期的モニタリングのパスワード	test

RADIUS サーバの設定

RADIUS サーバ ホストの設定

認証に使用される各 RADIUS サーバの IP アドレスまたはホスト名を設定するには、次の手順を実行します。 次の情報を知っている必要があります。

- 最大 64 の RADIUS サーバを設定できます。
- すべての RADIUS サーバ ホストは自動的にデフォルトの RADIUS サーバ グループに追加されます。

はじめる前に

この手順を開始する前に、EXEC モードで CLI にログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **radius-server host** {*ipv4-address* | *host-name*}	RADIUS サーバの IP アドレスまたはホスト名、または RADIUS サーバのドメイン ネーム サーバ（DNS）名を定義します。 ホスト名は英数字（大文字と小文字を区別）で、最大文字数は 256 です。
ステップ 3	switch(config)# **exit**	EXEC モードに戻ります。
ステップ 4	switch# **show radius-server**	（任意） RADIUS サーバの設定を表示します。
ステップ 5	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

```
switch# configure terminal
switch(config)# radius-server host 10.10.1.1
switch(config)# exit
```

```
switch# show radius-server
switch# copy running-config startup-config
```

RADIUS グローバル キーの設定

この手順を使用して、すべての RADIUS サーバが Cisco Nexus 1000V での認証に使用するキーを設定します。

RADIUS サーバ認証に使用されるグローバル キーを知っている必要があります。

はじめる前に

この手順を開始する前に、EXEC モードで CLI にログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **radius-server key** [**0** | **7**]*key-value*	すべての RADIUS サーバで使用する事前共有キーを指定します。 クリアテキスト形式（0）または暗号化形式（7）の事前共有キーを指定できます。 デフォルトの形式はクリア テキストです。 最大で 63 文字です。 デフォルトでは、事前共有キーは設定されません。
ステップ 3	switch(config)# **exit**	EXEC モードに戻ります。
ステップ 4	switch# **show radius-server**	（任意） RADIUS サーバの設定を表示します。 （注） 事前共有キーは、実行コンフィギュレーション内に暗号化形式で保存されます。 暗号化された事前共有キーを表示するには、show running-config コマンドを使用します。
ステップ 5	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

```
switch# configure terminal
switch(config)# radius-server key 0 QsEfThUkO
switch(config)# exit
switch# show radius-server
switch# copy running-config startup-config
```

RADIUS サーバ キーの設定

単一の RADIUS サーバ ホストのキーを設定するには、次の手順を実行します。

リモート RADIUS ホストで使用されるキーを取得している必要があります。

はじめる前に

この手順を開始する前に、EXEC モードで CLI にログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **radius-server host** {*ipv4-address* | *host-name*} **key** [**0** | **7**] *key-value*	特定の RADIUS サーバの事前共有キーを指定します。 クリア テキスト形式（**0**）または暗号化形式（**7**）の事前共有キーを指定できます。 デフォルトの形式はクリア テキストです。 最大で 63 文字です。
ステップ 3	switch(config)# **exit**	EXEC モードに戻ります。
ステップ 4	switch# **show radius-server**	（任意） RADIUS サーバの設定を表示します。 （注） 事前共有キーは、実行コンフィギュレーション内に暗号化形式で保存されます。暗号化された事前共有キーを表示するには、show running-config コマンドを使用します。
ステップ 5	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

```
switch# configure terminal
switch(config)# radius-server host 10.10.1.1 key 0 PlIjUhYg
switch(config)# exit
switch# show radius-server
switch# copy running-config startup-config
```

RADIUS サーバ グループの設定

メンバー サーバが認証機能を共有する RADIUS サーバ グループを設定するには、次の手順を実行します。

グループ内のサーバへのアクセスは、サーバを設定した順番で行われます。

はじめる前に

- この手順を開始する前に、EXEC モードで CLI にログインする必要があります。
- RADIUS サーバ グループ内のすべてのサーバが、同じ RADIUS プロトコルに属しています。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **aaa group server radius** *group-name*	RADIUS サーバ グループを作成し、そのグループの RADIUS サーバ グループ コンフィギュレーション モードを開始します。 group-name 引数は、最大 127 文字の長さの英数字のストリングで、大文字小文字が区別されます。
ステップ 3	switch(config-radius)# **server** {*ipv4-address* | *server-name*}	RADIUS サーバを、RADIUS サーバ グループのメンバーとして設定します。 **ヒント** 指定した RADIUS サーバが見つからない場合は、radius-server host コマンドを使用してサーバを設定し、このコマンドをもう一度実行します。
ステップ 4	switch(config-radius)# **deadtime** *minutes*	（任意） モニタリング デッド タイムを設定します。 デフォルト値は 0 分です。 指定できる範囲は 1 ～ 1440 です。 **（注）** RADIUS サーバ グループのデッド タイム間隔が 0 より大きい場合は、この値がグローバルなデッド タイム値より優先されます。
ステップ 5	switch(config-radius)# **use-vrf** *vrf-name*	（任意） サーバ グループ内のサーバとの接続に使用する VRF を指定します。
ステップ 6	switch(config-radius)# **source-interface** {*interface-type*} {*interface-number*}	（任意） RADIUS サーバに到達するために使用される送信元インターフェイスを指定します。 インターフェイス タイプおよびインターフェイス番号は、次のように定義されています。 • loopback = 0 ～ 1023 の仮想インターフェイス番号 • mgmt = 管理インターフェイス 0

	コマンドまたはアクション	目的
		• null = ヌル インターフェイス 0 • port-channel = 1 ～ 4096 のポート チャネル番号
ステップ 7	switch(config-radius)# **show radius-server groups** [*group-name*]	（任意） RADIUS サーバ グループの設定を表示します。
ステップ 8	switch(config-radius)# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

```
switch# configure terminal
switch(config)# aaa group server radius RadServer
switch(config-radius)# server 10.10.1.1
switch(config-radius)# deadtime 30
switch(config-radius)# use-vrf vrf1
switch(config-radius)# source-interface mgmt0
switch(config-radius)# show radius-server group
total number of groups:2

following RADIUS server groups are configured:
        group Radserver:
                server: 10.10.1.1
                deadtime is 30
        group test:
                deadtime is 30
switch(config-radius)# copy running-config startup-config
```

RADIUS サーバの誘導要求のイネーブル化

ユーザが認証要求の送信先となる RADIUS サーバを指定できるようにすることができます。 これは、誘導要求と呼ばれます。

このオプションをイネーブルにした場合、ユーザは username@vrfname:hostname としてログインできます。ここで、*vrfname* は使用するルーティングおよび転送（VRF）、*hostname* は設定された RADIUS サーバの名前です。

デフォルトでは、誘導要求はディセーブルです。

（注） ユーザ指定のログインは Telnet セッションに限りサポートされます。

はじめる前に

この手順を開始する前に、EXEC モードで CLI にログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **radius-server directed-request**	誘導要求をイネーブルにします。 デフォルトではディセーブルになっています。
ステップ 3	switch(config)# **exit**	EXEC モードに戻ります。
ステップ 4	switch(config)# **show radius-server directed-request**	（任意） directed request の設定を表示します。
ステップ 5	switch(config)# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

```
switch# configure terminal
switch(config)# radius-server directed-request
switch(config)# exit
switch# show radius-server directed-request
switch# copy running-config startup-config
```

すべての RADIUS サーバのグローバル タイムアウトの設定

ここでは、RADIUS サーバからの応答を待つ時間を指定するグローバル タイムアウト間隔の設定手順を説明します。この時間が経過すると、タイムアウト障害となります。

「単一RADIUSサーバのタイムアウト間隔の設定」で指定したタイムアウトは、RADIUSのグローバル タイムアウトに優先します。

はじめる前に

この手順を開始する前に、EXEC モードで CLI にログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	switch(config)# **radius-server timeout** *seconds*	RADIUS サーバの送信タイムアウト間隔を指定します。デフォルトのタイムアウト間隔は 5 秒です。有効な範囲は 1 ～ 60 秒です。
ステップ 3	switch(config-radius)# **exit**	EXEC モードに戻ります。
ステップ 4	switch(config-radius)# **show radius-server**	（任意） RADIUS サーバの設定を表示します。
ステップ 5	switch(config-radius)# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

```
switch# configure terminal
switch(config)# n1000v(config)# radius-server timeout 101
switch(config-radius)# exit
switch(config-radius)# show radius-server
switch(config-radius)# copy running-config startup-config
```

すべての RADIUS サーバのグローバル リトライ回数の設定

ローカル認証に切り換える前に RADIUS サーバへの送信を再試行する最大回数を設定するには、次の手順を実行します。この設定はすべての RADIUS サーバに適用されます。

デフォルトでは、ローカル認証に切り換える前に、RADIUS サーバへの再送信を 1 回だけ試行します。

リトライ回数は最大 5 回まで増やすことができます。

「単一 RADIUS サーバのリトライ回数の設定」で単一の RADIUS サーバに指定したリトライ回数は、このグローバル設定よりも優先されます。

はじめる前に

この手順を開始する前に、EXEC モードで CLI にログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **radius-server retransmit***count*	ローカル認証に切り換える前に許可する再送信回数を定義します。 このグローバル設定はすべての RADIUS サーバに適用されます。 デフォル

	コマンドまたはアクション	目的
		トの再送信回数は 1 です。有効な範囲は 0 ～ 5 です。
ステップ 3	switch(config)# **exit**	EXEC モードに戻ります。
ステップ 4	switch# **show radius-server**	（任意） RADIUS サーバの設定を表示します。
ステップ 5	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

```
switch# configure terminal
switch(config)# radius-server retransmit 31
switch(config)# exit
switch# show radius-server
switch# copy running-config startup-config
```

単一 RADIUS サーバのタイムアウト間隔の設定

ここでは、RADIUS サーバからの応答を待つ時間を設定する手順を説明します。この時間が経過すると、タイムアウト障害となります。

単一の RADIUS サーバに指定したタイムアウトは、「すべての RADIUS サーバのグローバル タイムアウトの設定」の項で定義したタイムアウトに優先します。

はじめる前に

この手順を開始する前に、EXEC モードで CLI にログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **radius-server host** { *ipv4-address* | *host-name* } **timeout** *seconds*	特定のサーバのタイムアウト間隔を指定します。デフォルトのタイムアウト間隔は 5 秒です。有効な範囲は 1 ～ 60 秒です。 （注） 単一の RADIUS サーバに指定したタイムアウトは、RADIUS のグローバル タイムアウトに優先します。
ステップ 3	switch(config)# **exit**	EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 4	switch# **show radius-server**	（任意） RADIUS サーバの設定を表示します。
ステップ 5	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

```
switch# configure terminal
switch(config)# radius-server host server1 timeout 10
switch(config)# exit
switch# show radius-server
switch# copy running-config startup-config
```

単一 RADIUS サーバのリトライ回数の設定

ローカル認証に切り換える前に RADIUS サーバへの送信を再試行する最大回数を設定するには、次の手順を実行します。この設定は単一の RADIUS サーバに適用され、グローバル リトライ回数に優先します。

はじめる前に

この手順を開始する前に、EXEC モードで CLI にログインする必要があります。

次のことを知っている必要があります。

- デフォルトでは、ローカル認証に切り換える前に、RADIUS サーバへの再送信を 1 回だけ試行します。
- リトライ回数は最大 5 回まで増やすことができます。
- 単一の RADIUS サーバに指定したリトライ回数は、すべての RADIUS サーバ用に作成されるグローバル設定に優先します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **radius-server host** {*ipv4-address* |*host-name*} **retransmit** *count*	特定のサーバに対する再送信回数を指定します。 デフォルトはグローバル値です。 （注） この単一 RADIUS サーバの再送信回数は、すべての RADIUS サーバ用のグローバル設定に優先します。

	コマンドまたはアクション	目的
ステップ 3	switch(config)# **exit**	EXEC モードに戻ります。
ステップ 4	switch# **show radius-server**	（任意） RADIUS サーバの設定を表示します。
ステップ 5	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

```
switch# configure terminal
switch(config)# radius-server host server1 retransmit 3
switch(config)# exit
switch# show radius-server
switch# copy running-config startup-config
```

RADIUS アカウンティング サーバの設定

アカウンティング機能を実行するサーバを設定するには、次の手順を実行します。

デフォルトでは、RADIUS サーバはアカウンティングと認証の両方に使用されます。

はじめる前に

この手順を開始する前に

- EXEC モードで CLI にログインする必要があります。
- RADIUS アカウンティング メッセージの宛先 UDP ポート番号を知っている必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **radius-server host** {*ipv4-address* | *host-name*} **acct-port** *udp-port*	（任意） 特定のホストに RADIUS アカウンティング メッセージを受信する UDP ポートを関連付けます。デフォルトの UDP ポートは 1812 です。 範囲は、0 ～ 65535 です。

	コマンドまたはアクション	目的
ステップ 3	switch(config)# **radius-server host** {*ipv4-address* | *host-name*} **accounting**	（任意） 特定の RADIUS ホストをアカウンティング サーバとして指定します。デフォルトでは、アカウンティングと認証の両方に使用されます。
ステップ 4	switch(config)# **exit**	EXEC モードに戻ります。
ステップ 5	switch# **show radius-server**	（任意） RADIUS サーバの設定を表示します。
ステップ 6	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

```
switch# configure terminal
switch(config)# radius-server host 10.10.1.1 acct-port 2004
switch(config)# radius-server host 10.10.1.1 accounting
switch(config)# exit
switch# show radius-server
switch# copy running-config startup-config
```

RADIUS 認証サーバの設定

認証機能を実行するサーバを設定するには、次の手順を実行します。

デフォルトでは、RADIUS サーバはアカウンティングと認証の両方に使用されます。

はじめる前に

この手順を開始する前に

- EXEC モードで CLI にログインする必要があります。
- RADIUS 認証メッセージの宛先 UDP ポート番号を知っている必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **radius-server host** {*ipv4-address* | *hostname*} **auth-port** *udp-port*	（任意） 特定のホストに RADIUS 認証メッセージを受信する UDP ポートを関連付けます。 デフォルトの UDP ポートは 1812 です。 指定できる範囲は 0 ～ 65535 です。

	コマンドまたはアクション	目的
ステップ 3	switch(config)# **radius-server host** {*ipv4-address* | *host-name*} **authentication**	（任意） 特定の RADIUS ホストを認証サーバとして指定します。 デフォルトでは、アカウンティングと認証の両方に使用されます。
ステップ 4	switch(config)# **exit**	EXEC モードに戻ります。
ステップ 5	switch# **show radius-server**	（任意） RADIUS サーバの設定を表示します。
ステップ 6	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

```
switch# configure terminal
switch(config)# radius-server host 10.10.2.2 auth-port 2005
switch(config)# radius-server host 10.10.2.2 authentication
switch(config)# exit
switch# show radius-server
switch# copy running-config startup-config
```

RADIUS サーバの定期的モニタリングの設定

RADIUS サーバのモニタリングを設定するには、次の手順を実行します。

テスト アイドル タイマーには、応答しない RADIUS サーバにテスト パケットが送信されるまでの経過時間を指定します。

デフォルトのアイドル タイマー値は 0 分です。 アイドル時間の間隔が 0 分の場合、Cisco NX-OS デバイスは RADIUS サーバの定期モニタリングを実行しません。

（注） セキュリティ上の理由から、RADIUS データベースに存在するユーザ名をテスト ユーザ名として設定しないでください。

はじめる前に

この手順を開始する前に、EXEC モードで CLI にログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	switch(config)# **radius-server host** {*ipv4-address* | *host-name*} **test** {**idle-time** *minutes* | **password** *password* [**idle-time** *minutes*] | **username** *name* [**password** *password* [**idle-time***minutes*]]}	サーバ モニタリング用のパラメータを指定します。 デフォルトのユーザ名はtest、デフォルトのパスワードは test です。 デフォルトのアイドル タイマー値は 0 分です。 指定できる範囲は、0 ～ 1440 分です。 （注） RADIUS サーバの定期的なモニタリングを行うには、アイドル タイマーに 0 より大きな値を設定する必要があります。
ステップ 3	switch(config)# **radius-server dead-time** *minutes*	デッドと宣言された RADIUS サーバにテスト パケットを送信するまで待機する分数を指定します。 デフォルト値は 0 分です。 有効な範囲は 1 ～ 1440 分です。
ステップ 4	switch(config)# **exit**	EXEC モードに戻ります。
ステップ 5	switch# **show radius-server**	（任意） RADIUS サーバの設定を表示します。
ステップ 6	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

```
switch# configure terminal
switch(config)# radius-server host 10.10.1.1 test username user1 password Ur2Gd2BH idle-time
 3
switch(config)# radius-server dead-time 5
switch(config)# exit
switch# show radius-server
switch# copy running-config startup-config
```

グローバル デッド タイム間隔の設定

すべての RADIUS サーバのデッド タイム間隔を設定するには、次の手順を実行します。 デッド タイム間隔には、RADIUS サーバをデッドであると宣言したあと、そのサーバがアライブになったかどうかを確認するためにテストパケットを送信するまで待機する時間を指定します。デフォルト値は 0 分です。

（注） デッド タイム間隔が 0 分の場合、RADIUS サーバは、応答を返さない場合でも、デットとしてマークされません。 RADIUS サーバ グループに対するデッド タイム間隔を設定できます。

はじめる前に

この手順を開始する前に、EXEC モードで CLI にログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **radius-server deadtime** *minutes*	デッド タイム間隔を設定します。 デフォルト値は 0 分です。 有効な範囲は 1 ～ 1440 分です。
ステップ 3	switch(config)# **exit**	EXEC モードに戻ります。
ステップ 4	switch# **show radius-server**	（任意） RADIUS サーバの設定を表示します。
ステップ 5	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

```
switch# configure terminal
switch(config)# radius-server deadtime 5
switch(config)# exit
switch# show radius-server
switch# copy running-config startup-config
```

RADIUS サーバまたはサーバ グループの手動モニタリング

RADIUS サーバまたはサーバ グループにテスト メッセージを手動で送信するには、次の手順を実行します。

はじめる前に

この手順を開始する前に、EXEC モードで CLI にログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **test aaa server radius** {*ipv4-address* | *server-name*} [**vrf** *vrf-name*] *username password*	RADIUS サーバにテスト メッセージを送信して可用性を確認します。

	コマンドまたはアクション	目的
ステップ 2	switch(config)# **test aaa group** *group-name username password*	RADIUS サーバ グループにテスト メッセージを送信して可用性を確認します。

```
switch# test aaa server radius 10.10.1.1 user1 Ur2Gd2BH
switch# test aaa group RadGroup user2 As3He3CI
```

RADIUS 設定の確認

次のいずれかのコマンドを使用して、設定を確認します。

コマンド	目的
show running-config radius [**all**]	実行コンフィギュレーションの RADIUS 設定を表示します。
show startup-config radius	スタートアップ コンフィギュレーションの RADIUS 設定を表示します。
show radius-server [*server-name* | *ipv4-address*] [**directed-request** | **groups** | **sorted** | **statistics**]	設定済みのすべての RADIUS サーバのパラメータを表示します。

RADIUS サーバ統計情報の表示

RADIUS サーバのアクティビティに関する統計情報を表示するには、次のコマンドを使用します。

show radius-server statistics { *hostname* | *ipv4-address* }

RADIUS の設定例

次に、グローバル RADIUS キーと RADIUS サーバ ホスト キーを設定する例を示します。

```
switch# configure terminal
switch(config)# radius-server key 7 "ToIkLhPpG"
switch(config)# radius-server host 10.10.1.1 key 7 "ShMoMhTl" authentication accounting
switch(config)# aaa group server radius RadServer
    server 10.10.1.1
```

RADIUS の機能の履歴

この表には、機能の追加によるリリースの更新内容のみが記載されています。

機能名	リリース	機能情報
RADIUS	Release 5.2(1)IC1(1.1)	この機能が導入されました。

第 5 章

TACACS+ の設定

この章の内容は、次のとおりです。

- TACACS+ について，51 ページ
- TACACS+ の前提条件，54 ページ
- TACACS+ の注意事項と制約事項，54 ページ
- TACACS+ のデフォルト設定，55 ページ
- 「Configuring TACACS+」，55 ページ
- TACACS+ ホストの統計情報の表示，71 ページ
- TACACS+ の設定例，71 ページ
- TACACS+ 機能の履歴，71 ページ

TACACS+ について

TACACS+ は、デバイスにアクセスしようとするユーザの検証を集中的に行うセキュリティ プロトコルです。 TACACS+ サービスは、通常 UNIX または Windows NT ワークステーション上で動作する TACACS+ デーモンのデータベースで管理されます。 デバイスに設定した TACACS+ 機能を使用可能にするには、TACACS+ サーバにアクセスして TACACS+ サーバを設定しておく必要があります。

TACACS+ は、独立した認証、許可、アカウンティング サービスを提供します。 TACACS+ デーモンは各サービスを個別に提供します。 各サービスを固有のデータベースに結合し、デーモンの機能に応じてそのサーバまたはネットワークで使用できる他のサービスを使用できます。

TACACS+ クライアント/サーバ プロトコルでは、トランスポート要件を満たすため TCP（TCP ポート 49）を使用します。 TACACS+ プロトコルを使用して集中型の認証が提供されます。

ユーザ ログインにおける TACACS+ の動作

パスワード認証プロトコル（PAP）を使用して TACACS+ サーバへのログインを試みると、次の一連のイベントが発生します。

1 接続が確立すると、ユーザ名とパスワードを取得するために TACACS+ デーモンが接続されます。

（注） TACACS+ では、デーモンがユーザを認証するために十分な情報を得られるまで、デーモンとユーザとの自由な対話を許可します。 通常、デーモンはユーザ名とパスワードを入力するよう求めますが、ユーザの母親の旧姓などの追加情報を求めることもできます。

2 TACACS+ デーモンは、次のいずれかの応答を提供します。

   a ACCEPT：ユーザの認証に成功したので、サービスを開始します。 ユーザ許可が必要な場合は、許可が始まります。

   b REJECT：ユーザの認証に失敗しました。 TACACS+ デーモンは、ユーザに対してそれ以上のアクセスを拒否するか、ログイン シーケンスを再試行するよう要求します。

   c ERROR：デーモンによる認証の途中でエラーが発生したか、またはネットワーク接続でエラーが発生しました。 ERROR 応答を受信した場合、デバイスは別の方法でユーザの認証を試行します。

   認証後、さらに許可が必要な場合は、続いてユーザの許可フェーズに入ります。 ユーザは TACACS+ 許可に進む前に、まず TACACS+ 認証を正常に完了する必要があります。

3 TACACS+ 許可が必要な場合は、TACACS+ デーモンに接続し、デーモンが ACCEPT または REJECT の許可応答を返します。 ACCEPT 応答には、ユーザに対する EXEC または NETWORK セッションの送信に使用される属性が含まれます。また ACCEPT 応答により、ユーザがアクセス可能なサービスが決まります。

   この場合のサービスは次のとおりです。

   - Telnet、rlogin、ポイントツーポイント プロトコル（PPP）、シリアル ライン インターネット プロトコル（SLIP）、EXEC サービス
   - 接続パラメータ（ホストまたはクライアントの IP アドレス、アクセス リスト、および ユーザ タイムアウトを含む）

デフォルトの TACACS+ サーバ暗号化タイプと事前共有キー

TACACS+ サーバに認証するには、TACACS+ 事前共有キーを設定する必要があります。 事前共有キーは、デバイスと TACACS+ サーバ ホストの間で共有される秘密テキスト ストリングです。キーの長さは 63 文字で、出力可能な任意の ASCII 文字を含めることができます（スペースは使用

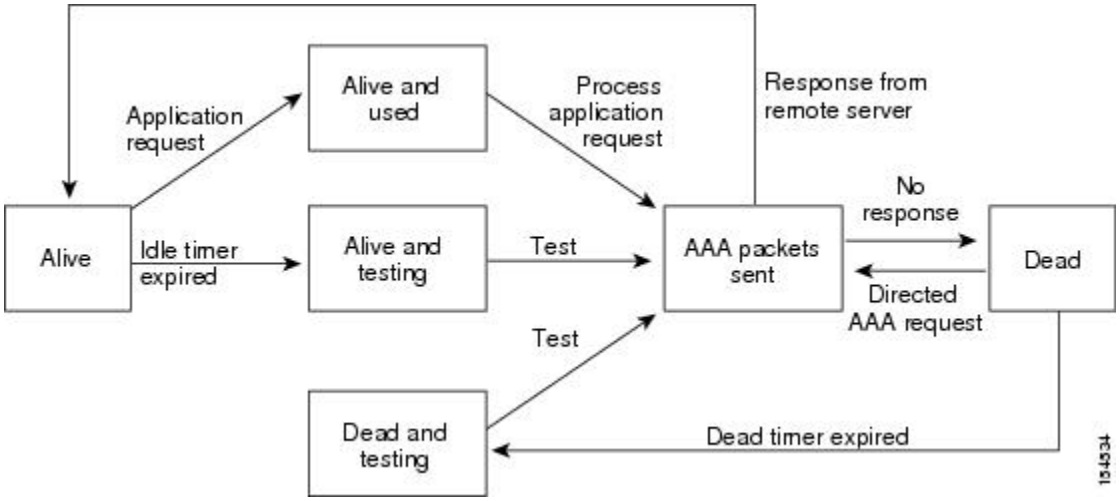
できません）。 すべての TACACS+ サーバ設定で使用されるグローバルな事前共有秘密キーを設定できます。

グローバルな事前共有キーの設定は、個々の TACACS+ サーバの設定時に明示的に key オプションを使用することによって無効にできます。

TACACS+ サーバのモニタリング

応答しない TACACS+ サーバはデッド（dead）としてマークされ、AAA 要求が送信されません。 デッド TACACS+ サーバは定期的にモニタされ、応答があればアライブに戻されます。 このプロセスにより、TACACS+ サーバが稼働状態であることを確認してから、実際の AAA 要求が送信されます。 次の図に、TACACS+ サーバの状態変化によって、どのように簡易ネットワーク管理プロトコル（SNMP）トラップが生成され、パフォーマンスに影響が出る前に障害を示すエラーメッセージが生成されるかを示します。

図 *3*：*TACACS+* サーバの状態



（注） アライブ サーバとデッド サーバのモニタリング間隔は異なります。 これらはユーザが設定できます。 TACACS+ サーバ モニタリングを実行するには、テスト認証要求を TACACS+ サーバに送信します。

ベンダー固有属性

インターネット技術特別調査委員会（IETF）ドラフト標準には、ネットワーク アクセス サーバと TACACS+ サーバの間でベンダー固有属性（VSA）を伝達する方法が規定されています。 IETF は、属性 26 を使用します。 VSA を使用するとベンダーは、一般的な用途には適合しない独自の拡張属性をサポートできます。

シスコの VSA 形式

シスコの TACACS+ 実装では、IETF 仕様で推奨される形式を使用したベンダー固有のオプションを 1 つサポートしています。 シスコのベンダー ID は 9、サポートされるオプションのベンダータイプは 1（名前付き cisco-av-pair）です。 値は、次の形式のストリングです。

```
protocol : attribute separator value *
```

protocol は、特定の認証タイプを表すシスコの属性です。 区切り文字は、必須属性の場合 =（等号）、任意の属性の場合は *（アスタリスク）です。

認証に TACACS+ サーバを使用した場合、TACACS+ プロトコルでは TACACS+ サーバに対して、認証結果とともに権限付与情報などのユーザ属性を返すように指示します。 この許可情報は、VSA で指定されます。

次の VSA プロトコル オプションがサポートされています。

- shell：ユーザ プロファイル情報を提供する access-accept パケットで使用されるプロトコル。
- Accounting：accounting-request パケットで使用されるプロトコル。 値にスペースが含まれている場合は、二重引用符で囲む必要があります。

次の属性もサポートされています。

- roles：ユーザが属するすべてのロールの一覧です。 値は、スペースで区切られたロール名を一覧表示した文字列です。 このサブ属性は Access-Accept フレームの VSA 部分に格納され、TACACS+ サーバから送信されます。この属性はシェル プロトコル値とだけ併用できます。
- accountinginfo：標準の TACACS+ アカウンティング プロトコルに含まれる属性とともにアカウンティング情報を格納します。 この属性は、スイッチ上の TACACS+ クライアントから、Account-Request フレームの VSA 部分にだけ格納されて送信されます。 この属性と共に使用できるのは、アカウンティングのプロトコル データ ユニット（PDU）だけです。

TACACS+ の前提条件

- TACACS+ サーバの IP アドレスまたはホスト名を取得すること。
- TACACS+ サーバから事前共有キーを取得していること。
- Cisco Nexus 1000V が AAA サーバの TACACS+ クライアントとして設定されていること。
- すでに、リモート TACACS+ 認証を含む AAA が設定されていること。

TACACS+ の注意事項と制約事項

- 最大 64 の TACACS+ サーバを設定できます。
- TACACS+ のログレベルは 5 に設定する必要があります。

TACACS+ のデフォルト設定

パラメータ	デフォルト
TACACS+	無効
デッド タイマー間隔	0 分
タイムアウト間隔	5 秒
アイドル タイマー間隔	0 分
サーバの定期的モニタリングのユーザ名	test
サーバの定期的モニタリングのパスワード	test

「Configuring TACACS+」

次のフロー チャートで、TACACS+ を設定する手順を示します。

（注） Cisco Nexus 1000V のコマンドは Cisco IOS のコマンドと異なる場合があることに注意してください。

図 *4*：***TACACS+*** 設定のフロー チャート

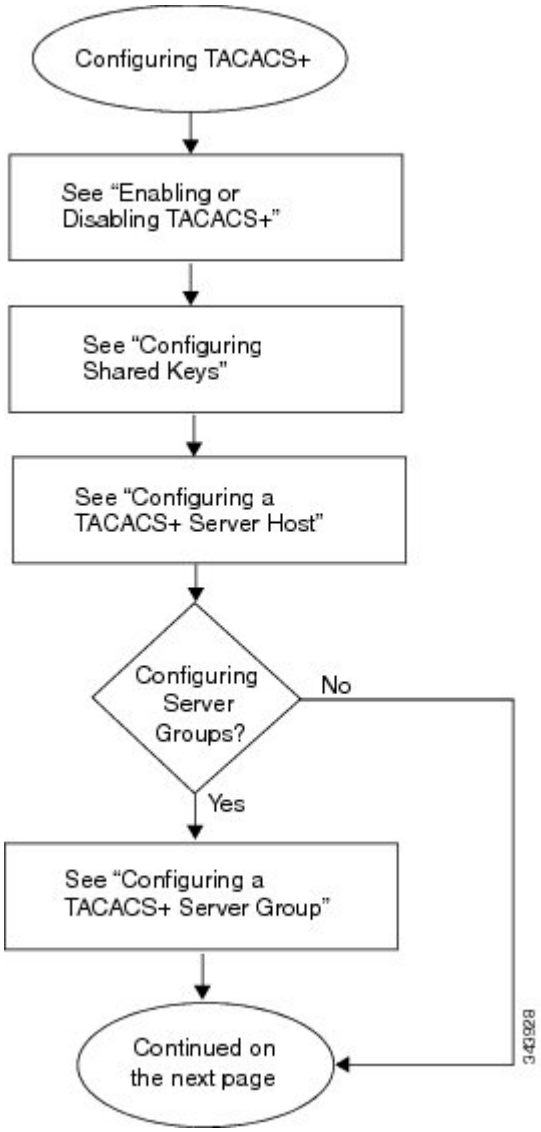


図 *5*：***TACACS+*** 設定のフロー チャート（続き）

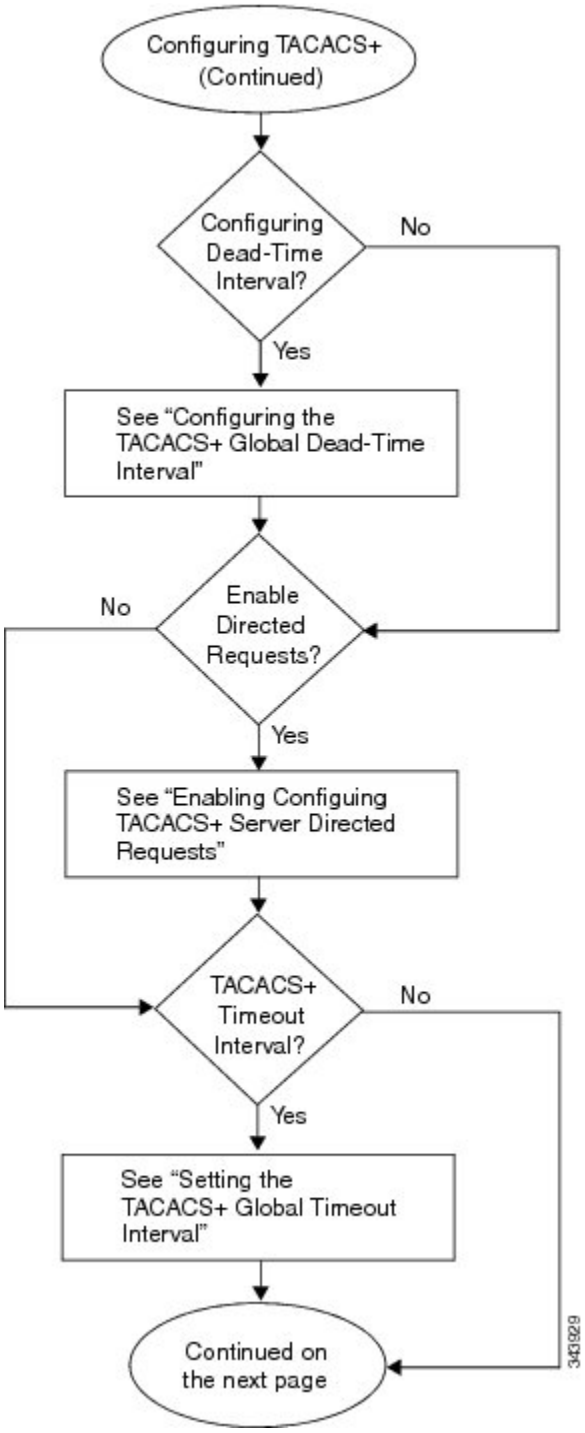
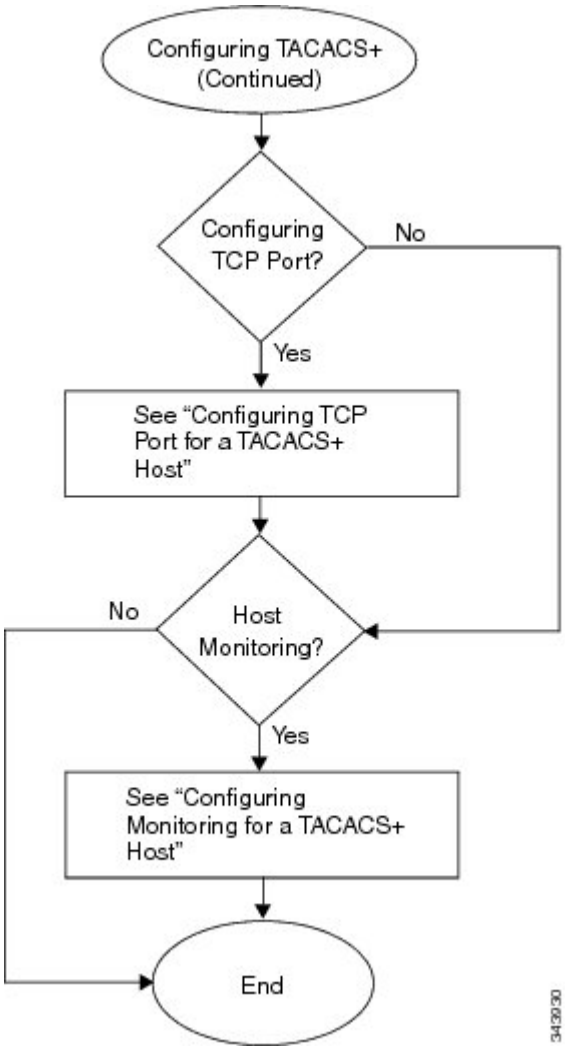


図 *6*：*TACACS+* 設定のフロー チャート（続き）



TACACS+ のイネーブル化またはディセーブル化

デフォルトでは、TACACS+ がディセーブルです。 TACACS+ 認証をサポートするコンフィギュレーション コマンドと検証コマンドを使用するには、TACACS+ 機能を明示的にイネーブルにする必要があります。

注意 TACACS+ をディセーブルにすると、関連するすべての設定が自動的に廃棄されます。

はじめる前に

この手順を開始する前に、EXEC モードで CLI にログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# [**no**] **tacacs+ enable**	TACACS+ をイネーブルまたはディセーブルにします。
ステップ 3	switch(config)# **exit**	グローバル コンフィギュレーション モードを終了し、EXEC モードに戻ります。
ステップ 4	switch(config)# **copy running-config startup-config**	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

```
switch# configure terminal
switch(config)# tacacs+ enable
switch(config)# exit
switch# copy running-config startup-config
```

共有キーの設定

デフォルトでは、グローバル キーは設定されません。

次のものを設定するには、次の手順を実行します。

- グローバル キー（Cisco Nexus 1000V とすべての TACACS+ サーバ ホストの間で共有される秘密テキスト ストリング）
- キー（Cisco Nexus 1000V と単一の TACACS+ サーバ ホストの間で共有される秘密テキスト ストリング）

はじめる前に

- CLI に EXEC モードでログインしていること。
- 認証用に TACACS+ をイネーブルにしたこと。
- TACACS+ サーバ ホストのキーがわかっていること。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。 次のどちらかを実行します。

	コマンドまたはアクション	目的
		• すべての TACACS+ サーバ ホストのグローバル キーを設定する場合は、次のステップに進みます。 • 単一の TACACS+ サーバ ホストのキーを設定する場合は、ステップ 3 に進みます。
ステップ 2	switch(config)# **tacacs-server key** [**0** | **7**] *global_key*	Cisco Nexus 1000V と TACACS+ サーバ ホストの間で共有されるグローバル キーを指定します。 • 0：使用するクリアテキストストリング（キー）を指定します。これがデフォルトです。 • 7：使用する暗号化された文字列（キー）を指定します。 • *global_key*：最大 63 文字のストリングです。 デフォルトでは、グローバルキーは設定されません。 ステップ 4 に進みます。
ステップ 3	switch(config)# **tacacs-server host** { *ipv4-address* | *host-name*} **key** [**0** | **7**] *shared_key*	Cisco Nexus 1000V とこの特定の TACACS+ サーバ ホストの間で共有されるキーを指定します。 0：使用するクリアテキストストリング（キー）を指定します。これがデフォルトです。 7：使用する暗号化された文字列（キー）を指定します。 *global key*：最大 63 文字の文字列です。 グローバル共有キーではなく、この共有キーが使用されます。
ステップ 4	switch(config)# **exit**	グローバル コンフィギュレーション モードを終了し、EXEC モードに戻ります。
ステップ 5	switch# **show tacacs-server**	（任意） TACACS+ サーバの設定を表示します。 （注） グローバル共有キーは実行コンフィギュレーションに暗号化形式で保存されます。 キーを表示するには、show running-config コマンドを使用します。
ステップ 6	switch(config)# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

```
switch# configure terminal
switch(config)# tacacs-server key 0 QsEFtkI#
switch(config)# exit
switch# show tacacs-server
Global TACACS+ shared secret:********
timeout value:5
deadtime value:0
total number of servers:1

following TACACS+ servers are configured:
        10.10.2.2:
                available on port:49
switch# copy running-config startup-config
```

TACACS+ サーバ ホストの設定

すべての TACACS+ サーバ ホストはデフォルトの TACACS+ サーバ グループに追加されます。

はじめる前に

この手順を開始する前に、次のことを確認してください。

- CLI に EXEC モードでログインしていること。
- 認証用に TACACS+ をイネーブルにしたこと。
- 共有キーが設定されていること。
- リモート TACACS+ サーバ ホストの IP アドレスまたはホスト名がわかっていること。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **tacacs-server host** {*ipv4-address* | *host-name*}	サーバの IP アドレスまたはホスト名を TACACS+ サーバ ホストとして設定します。
ステップ 3	switch(config)# **exit**	グローバル コンフィギュレーション モードを終了し、EXEC モードに戻ります。
ステップ 4	switch(config)# **show tacacs-server**	（任意） TACACS+ サーバの設定を表示します。
ステップ 5	switch(confgi)# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

```
switch# configure terminal
switch(config)# tacacs-server host 10.10.2.2
switch(config)# exit
switch# show tacacs-server
timeout value:5
deadtime value:0
total number of servers:1

following TACACS+ servers are configured:
        10.10.2.2:
                available on port:49
switch# copy running-config startup-config
```

TACACS+ サーバ グループの設定

メンバー サーバが認証機能を共有する TACACS+ サーバ グループを設定するには、次の手順を実行します。

TACACS+ サーバ グループが設定されると、メンバーのサーバへのアクセスは、サーバを設定した順番で行われます。

TACACS+ サーバ グループでは、1 台のサーバが応答できない場合に備えて、フェールオーバーを提供できます。 グループ内の最初のサーバが応答しない場合は、同じグループ内の次のサーバが試行され、サーバが応答するまでこの処理が行われます。 複数のサーバグループがある場合、同じ方法で、相互にフェールオーバーを提供できます。

はじめる前に

この手順を開始する前に、次のことを確認してください。

- EXEC モードで CLI にログインしていること。
- TACACS+ サーバ グループに追加されたすべてのサーバが、TACACS+ プロトコルを使用していること。
- すでに事前共有キーが設定されていること。
- 認証用に TACACS+ がイネーブルになっていること。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminalt**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **aaa group server tacacs+** *group-name*	指定した名前で TACACS+ サーバ グループを作成し、そのグループの TACACS+ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	switch(config-tacacs+)# **server** { *ipv4-address* | *host-name*}	TACACS+ サーバのホスト名または IP アドレスを TACACS+ サーバ グループのメンバーとして設定します。 指定した TACACS+ サーバが見つからない場合は、tacacs-server host コマンドを使用してサーバを設定し、このコマンドをもう一度実行します。 （注） 指定した TACACS+ サーバが見つからない場合は、tacacs-server host コマンドを使用してサーバを設定し、このコマンドをもう一度実行します。
ステップ 4	switch(config-tacacs+)# **deadtime** *minutes*	（任意） この TACACS+ グループのモニタリングのデッド タイムを設定します。 デフォルト値は 0 分です。 指定できる範囲は 0 ～ 1440 です。 （注） TACACS+ サーバ グループのデッド タイム間隔が 0 より大きい場合は、その値がグローバルなデッド タイム値より優先されます。
ステップ 5	switch(config-tacacs+)# **use-vrf** *vrf-name*	（任意） このサーバ グループとの接続に使用する仮想ルーティングおよび転送（VRF）インスタンスを指定します。
ステップ 6	switch(config-tacacs+)# **source-interface** {*interface-type*} {*interface-number*}	（任意） TACACS+ サーバに到達するために使用される送信元インターフェイスを指定します。 • loopback = 0 ～ 1023 の仮想インターフェイス番号 • mgmt = 管理インターフェイス 0 • null = ヌル インターフェイス 0 • port-channel = 1 ～ 4096 のポート チャネル番号
ステップ 7	switch(config-tacacs+)# **show tacacs-server groups**	（任意） TACACS+ サーバ グループの設定を表示します。
ステップ 8	switch(config-tacacs+)# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

```
switch# config terminal
switch(config)# aaa group server tacacs+ TacServer
switch(config-tacacs+)# server 10.10.2.2
```

```
switch(config-tacacs+)# deadtime 30
switch(config-tacacs+)# use-vrf management
switch(config-tacacs+)# source-interface mgmt0
switch(config-tacacs+)# show tacacs-server groups
total number of groups:1

following TACACS+ server groups are configured:
        group TacServer:
                server 10.10.2.2 on port 49
                deadtime is 30
                vrf is management
switch# copy running-config startup-config
```

TACACS+ サーバの誘導要求のイネーブル化

この手順では、認証要求の送信先となる TACACS+ サーバを指定することができます。 これは directed-request（誘導要求）と呼ばれます。

誘導要求をイネーブルにした場合、ユーザは username@vrfname:hostname としてログインできます（*vrfname* は使用する VRF、hostname は設定された TACACS+ サーバの名前）。

（注） ユーザ指定のログインは Telnet セッションに限りサポートされます。

はじめる前に

この手順を開始する前に、次のことを確認してください。

- CLI に EXEC モードでログインしていること。
- 認証用に TACACS+ をイネーブルにしたこと。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバルコンフィギュレーションモードを開始します。
ステップ 2	switch(config)# **tacacs-server directed-request**	ログイン時に認証要求を送信する TACACS+ サーバを指定するために、誘導要求の使用をイネーブルにします。デフォルトではディセーブルになっています。
ステップ 3	switch(config)# **exit**	グローバルコンフィギュレーションモードを終了し、EXEC モードに戻ります。
ステップ 4	switch(config)# **show tacacs-server directed-request**	（任意） TACACS+ の directed request の設定を表示します。

	コマンドまたはアクション	目的
ステップ 5	switch(config)# **copy running-config startup-config**	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

```
switch# config terminal
switch(config)# tacacs-server directed-request
switch(config)# exit
switch# show tacacs-server directed-request
enabled
switch# copy running-config startup-config
```

TACACS+ のグローバル タイムアウト間隔の設定

Cisco Nexus 1000V が任意の TACACS+ サーバからの応答を待つ時間を秒単位で設定するには、次の手順を実行します。これを過ぎるとタイムアウトが宣言されます。

個別の TACACS+ サーバに指定したタイムアウトは、グローバル タイムアウト間隔に優先します。 個別サーバのタイムアウトの設定方法。

はじめる前に

この手順を開始する前に、次の作業を実行したことを確認してください。

- CLI に EXEC モードでログインしていること。
- 認証用に TACACS+ をイネーブルにしたこと。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **tacacs-server timeout** *seconds*	Cisco Nexus 1000V がサーバから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間隔は 5 秒です。 有効な範囲は 1 ～ 60 秒です。
ステップ 3	switch(confi)# **exit**	グローバル コンフィギュレーション モードを終了し、EXEC モードに戻ります。
ステップ 4	switch(config)# **show tacacs-server**	（任意） TACACS+ サーバの設定を表示します。

	コマンドまたはアクション	目的
ステップ 5	switch(confi)# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

```
switch# configure terminal
switch(config)# tacacs-server timeout 10
switch(config)# exit

switch# n1000v# show tacacs-server
Global TACACS+ shared secret:********
timeout value:10
deadtime value:0
total number of servers:1

following TACACS+ servers are configured:
        10.10.2.2:
                available on port:49
switch# copy running-config startup-config
```

個別 TACACS+ ホストのタイムアウト間隔の設定

Cisco Nexus 1000V が特定の TACACS+ サーバからの応答を待つ時間を秒単位で設定するには、次の手順を実行します。これを過ぎるとタイムアウトが宣言されます。 この設定は TACACS+ ホスト単位で設定します。

個別の TACACS+ サーバのタイムアウト設定は、グローバル タイムアウト間隔に優先します。

はじめる前に

この手順を開始する前に、次の作業を実行したことを確認してください。

- CLI に EXEC モードでログインしていること。
- 認証用に TACACS+ をイネーブルにしたこと。
- TACACS+ サーバを設定したこと。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **tacacs-server host** {*ipv4-address* | *host-name*} **timeout** *seconds*	特定のサーバのタイムアウト間隔を指定します。 デフォルトはグローバル タイムアウト間隔です。

	コマンドまたはアクション	目的
ステップ 3	switch(config)# **exit**	グローバル コンフィギュレーション モードを終了し、EXEC モードに戻ります。
ステップ 4	switch(config)# **show tacacs-server**	（任意） TACACS+ サーバの設定を表示します。
ステップ 5	switch(config)# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

```
switch# config terminal
switch(config)#  tacacs-server host 10.10.2.2 timeout 10
switch(config)# exit
switch# n1000v# show tacacs-server
Global TACACS+ shared secret:********
timeout value:10
deadtime value:0
total number of servers:1

following TACACS+ servers are configured:
        10.10.2.2:
                available on port:49
                timeout:10
switch# copy running-config startup-config
```

TACACS+ ホストの TCP ポートの設定

ポート 49（TACACS+ 要求のデフォルト）以外の TCP ポートを設定するには、次の手順を実行します。

はじめる前に

この手順を開始する前に、次の作業を実行したことを確認してください。

- CLI に EXEC モードでログインしていること。
- 認証用に TACACS+ をイネーブルにしたこと。
- TACACS+ サーバを設定したこと。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	switch(config)# **tacacs-server host** {*ipv4-address* | *host-name*} **port** *tcp-port*	使用する TCP ポートを指定します。 指定できるポート範囲：1 ～ 65535 デフォルトは 49 です。
ステップ 3	switch(config)# **exit**	グローバル コンフィギュレーション モードを終了し、EXEC モードに戻ります。
ステップ 4	switch(config)# **show tacacs-server**	（任意） TACACS+ サーバの設定を表示します。
ステップ 5	switch(config)# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

```
switch# configure terminal
switch(config)# tacacs-server host 10.10.2.2 port 2
switch(config)# exit
switch# show tacacs-server
Global TACACS+ shared secret:********
timeout value:10
deadtime value:0
total number of servers:1

following TACACS+ servers are configured:
        10.10.2.2:
                available on port:2
                timeout:10
switch# copy running-config startup-config
```

TACACS+ ホストのモニタリングの設定

次の情報を知っている必要があります。

- アイドル タイマーには、TACACS+ サーバがアイドル（要求を受信しない）状態を続ける時間を指定します。これを過ぎると TACACS+ サーバにテスト パケットが送信されます。
- デフォルトのアイドル タイマー値は 0 分です。アイドル時間の間隔が 0 分の場合、TACACS+ サーバの定期モニタリングは実行されません。

はじめる前に

この手順を開始する前に、次の作業を実行したことを確認してください。

- CLI に EXEC モードでログインしていること。
- 認証用に TACACS+ をイネーブルにしたこと。
- TACACS+ サーバを設定したこと。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **tacacs-server host** {*ipv4-address* | *host-name* } **test** { **idle-time** *minutes* | **password** *password* [**idle-time** *minutes*] | **username** *name* [**password** *password* [**idle-time** *minutes*]]}	サーバ モニタリングを設定します。 次のキーワードと引数があります。 • **username**：デフォルトは test です。 （注） ネットワークのセキュリティを保護するために、TACACS+ データベースに存在しないユーザ名を割り当てることを推奨します。 • **password**：デフォルトは test です。 • **idle-time**：デフォルトは 0 分です。 有効な範囲は 0 ～ 1440 分です。 （注） TACACS+ サーバの定期的なモニタリングを行うには、アイドル タイマーに 0 より大きな値を設定する必要があります。
ステップ 3	switch(config)# **tacacs-server dead-time** *minutes*	以前に応答しなかった TACACS+ サーバのチェックを始めるまでの時間を分単位で指定します。デフォルト値は 0 分です。有効な範囲は 0 ～ 1440 分です。
ステップ 4	switch(config)# **exit**	グローバル コンフィギュレーション モードを終了し、EXEC モードに戻ります。
ステップ 5	switch(config)# **show tacacs-server**	（任意） TACACS+ サーバの設定を表示します。
ステップ 6	switch(config)# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

```
switch# configure terminal
switch(config)# tacacs-server host 10.10.2.2 test username pvk2 password a3z9yjqz7 idle-time
 3
switch(config)# tacacs-server dead-time 5
switch(config)# exit
switch# show tacacs-server
Global TACACS+ shared secret:********
timeout value:10
deadtime value:5
total number of servers:1
```

```
following TACACS+ servers are configured:
        10.10.2.2:
                available on port:2
                timeout:10
switch# copy running-config startup-config
```

TACACS+ グローバル デッド タイム間隔の設定

以前に応答しなかったサーバにテスト パケットを送信するまで待機する時間を設定するには、次の手順を実行します。

デッド タイム間隔が 0 分の場合、TACACS+ サーバは、応答を返さない場合でも、デットとしてマークされません。 デッド タイムはグループ単位で設定できます。

はじめる前に

この手順を開始する前に、次の作業を実行したことを確認してください。

- CLI に EXEC モードでログインしていること。
- 認証用に TACACS+ をイネーブルにしたこと。
- TACACS+ サーバを設定したこと。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **tacacs-server deadtime** *minutes*	グローバルなデッドタイム間隔を設定します。デフォルト値は 0 分です。 有効な範囲は、1 ～ 1440 分です。
ステップ 3	switch(config)# **exit**	グローバル コンフィギュレーション モードを終了し、EXEC モードに戻ります。
ステップ 4	switch(config)# **show tacacs-server**	（任意） TACACS+ サーバの設定を表示します。
ステップ 5	switch(config)# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

```
switch# configure terminal
switch(config)#  tacacs-server deadtime 5
switch(config)# exit
switch# show tacacs-server
Global TACACS+ shared secret:********
timeout value:10
deadtime value:5
```

```
total number of servers:1

following TACACS+ servers are configured:
        10.10.2.2:
                available on port:2
                timeout:10
switch# copy running-config startup-config
```

TACACS+ ホストの統計情報の表示

TACACS+ ホストの統計情報を表示するには、次のコマンドを使用します。

コマンド	説明
show tacacs-server statistics {*hostname* | *ipv4-address*}	TACACS+ ホストの統計情報を表示します。

TACACS+ の設定例

次に、TACACS+ 設定の例を示します。

```
switch# configure terminal
switch(config)# feature tacacs+
switch(config-tacacs+)# tacacs-server key 7 "ToIkLhPpG"
switch# (config-tacacs+)# tacacs-server host 10.10.2.2 key 7 "ShMoMhTl"
switch# (config-tacacs+)# aaa group server tacacs+ TacServer
    server 10.10.2.2
```

TACACS+ 機能の履歴

この表には、機能の追加によるリリースの更新内容のみが記載されています。

機能名	リリース	機能情報
TACACS+	Release 5.2(1)IC1(1.1)	この機能が導入されました。

第 6 章

SSH の設定

この章は、次の項で構成されています。

- SSH に関する情報，73 ページ
- SSH の前提条件，74 ページ
- SSH の注意事項および制約事項，75 ページ
- デフォルト設定，75 ページ
- SSH の設定，75 ページ
- SSH の設定の確認，83 ページ
- SSH の設定例，84 ページ
- SSH 機能の履歴，84 ページ

SSH に関する情報

SSH サーバ

セキュア シェル（SSH）サーバを使用すると、SSH クライアントはセキュアな暗号化された接続を確立できます。 SSH は強化暗号化を使用して認証を行います。 SSH サーバは、市販の一般的な SSH クライアントとの相互運用が可能です。

SSH では、TACACS+ ユーザ認証およびローカルに保存されたユーザ名とパスワードがサポートされます。

SSH クライアント

SSH クライアントは、SSH プロトコルで稼働しデバイス認証および暗号化を提供するアプリケーションです。 SSH クライアントをインストールすると、SSH サーバを実行する任意のデバイスと

の間でセキュアな暗号化された接続を確立できるようになります。 この接続を通して、暗号化されたアウトバウンド接続が提供されます。 SSH クライアントは、認証および暗号化により、非セキュアなネットワーク上でセキュアな通信ができます。

SSH クライアントは、市販の一般的な SSH サーバと連動します。

SSH サーバ キー

SSH では、セキュアな通信を行うためにサーバ キーが必要です。 SSH サーバ キーは、次の SSH オプションに使用できます。

- Rivest, Shamir, and Adelman（RSA）公開キー暗号化を使用した SSH バージョン 2
- Digital System Algrorithm（DSA）を使用した SSH バージョン 2

SSH サービスをイネーブルにする前に、正しいバージョンの SSH サーバ キー ペアを取得しておいてください。 使用する SSH クライアントのバージョンに応じた SSH サーバ キー ペアを生成します。 SSH サービスは、SSH バージョン 2 で使用する次の 2 種類のキー ペアを受け入れます。

- dsa オプションを使用すると、SSH バージョン 2 プロトコルに対応する DSA キーペアが生成されます。
- rsa オプションを使用すると、SSH バージョン 2 プロトコルに対応する RSA キーペアが生成されます。

デフォルトでは、1024 ビットの RSA キーが生成されます。

SSH は、次の公開キー形式をサポートします。

- OpenSSH
- IETF SSH（SECSH）
- Privacy-Enhanced Mail（PEM）の公開キー証明書

注意 SSH キーをすべて削除すると、SSH サービスを開始できません。

SSH の前提条件

SSH を使用するには、次の前提条件を満たしている必要があります。

- レイヤ 3 インターフェイス上に IP、mgmt 0 インターフェイス上にアウトオブバンドを設定していること。
- SSH サーバをイネーブルにする前に、SSH キーを取得すること

SSH の注意事項および制約事項

SSH には、次の注意事項と制限事項があります。

- SSH バージョン 2（SSHv2）のみがサポートされます。
- SSH はデフォルトでイネーブルになります。
- Cisco NX-OS コマンドは Cisco IOS コマンドと異なる場合があります。

デフォルト設定

パラメータ	デフォルト
SSH サーバ	有効（Enabled）
SSH サーバ キー	2048 ビットで生成された RSA キー
RSA キー生成ビット数	1024

SSH の設定

SSH サーバ キーの生成

セキュリティ要件に応じた SSH サーバ キーを生成するには、次の手順を実行します。

デフォルトの SSH サーバ キーは、1024 ビットで生成される RSA キーです。

はじめる前に

この手順を開始する前に、EXEC モードで CLI にログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **no feature ssh**	SSH をディセーブルにします。
ステップ 3	switch(config)# **ssh key** {**dsa** [**force**] | **rsa** [*bits*[**force**]]}	SSH サーバ キーを生成します。

	コマンドまたはアクション	目的
		bits 引数には、キーの生成に使用するビット数を指定します。 有効な範囲は 768 ～ 2048 です。デフォルト値は 1024 です。 既存のキーを置き換える場合は、キーワード **force** を使用します。
ステップ 4	switch(config)# **feature ssh**	SSH をイネーブルにします。
ステップ 5	switch# **show ssh key**	（任意） SSH サーバ キーを表示します。
ステップ 6	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

```
switch# configure terminal
switch(config)# no feature ssh
XML interface to system may become unavailable since ssh is disabled
switch(config)# ssh key dsa force
generating dsa key(1024 bits).....
.
generated dsa key
n1000v(config)# feature ssh
n1000v(config)# show ssh key
*************************************
rsa Keys generated:Sun Jul 27 15:18:46 2008

ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAyKcb7Nv9Ki1OOId9/tdHHa/ngQujlvK5mXyL/n+DeOXK
fVhHbX2a+V0cm7CCLUkBh+BvZRmpmOVTmU/5awfVhVxMKXMiPOPBc+A6/n3FVroyRwupMki6mWoM6Uwa
GID5gsVPqFjFNSgMWtbhjo97XVKhgjFW+wOVt8QoAcrEtnwEfsnQk1EIr/0XIP1mqTsrqTsmjZ2vLk+f
FzTGYAxMvYZI+BrN47aoH2ywS7CpnODjCDXJuDYSPbc3PA8t0ghU/60m9R+s6AZPuljVQbGfxPrahEu4
GVc6sMJNU1JxmqDJkodhMArObB4Umzj7E3Rdby/ZWx/clTYiXQR1X1VfhQ==

bitcount:2048
fingerprint:
fd:ca:48:73:b9:ee:e7:86:9e:1e:40:46:f1:50:1d:44
*************************************
dsa Keys generated:Sun Jul 27 15:20:12 2008

ssh-dss AAAAB3NzaC1kc3MAAACBALpdxLjXNS/jcCNY+F1QZV9HegxBEb0DMUmq9bSq2N+KAcvHllEh
GnaiHhqarOlcEKqhLbIbuqtKTCvfa+Y1hBIAhWVjg1UR3/M22jqxnfhnxL5YRc1Q7fcesFax0myayAIU
nXrkO5iwv9XHTu+EInRc4kJ0XrG9SxtLmDe/fi2ZAAAAFQDbRabAjZa6GfDpwjXw5smRhrElJwAAAIEA
r50yi3hHawNnb5qgYLXhN+KA8XJF753eCWHtMw7NR8fz6fjQ1R2J97UjjGuQ8DvwpGeNQ5S+AuIo0rGq
svdg7TTecBcbgBOnR7Fs2+W5HiSVEGbvj1xaeK8fkNE6kaJumBB343b8Rgj0G97MP/os1GfkEqmX9glB
0IOM2mgHHyoAAACAfRir27hHy+fw8CxPlsK0R6cFhxYyd/qYYogXFKYIOPxpLoYrjqODeOFThU7TJuBz
aS97eXiruzbffHwzUGfXgmQT5o9IMZRTClWPA/5Ju4O9YABYHccUghf0W+QtgGOT6FOSvBh8uOV0kcHC
GMJAP8omphauZJlc+wgFxhnkyh4=

bitcount:1024
fingerprint:
44:91:32:1f:7a:d1:83:3c:f3:5e:db:53:0a:2d:ce:69
*************************************
```

公開キーを持つユーザ アカウントの設定

SSH 公開キーを設定すると、パスワードを要求されることなく、SSH クライアントを使用してログインできます。 SSH 公開キーは、次の 3 種類のいずれかの形式で指定できます。

- OpenSSH 形式
- Internet Engineering Task Force（IETF）SECSH 形式
- Privacy Enhanced Mail（PEM）形式の公開キー証明書

OpenSSH キーの設定

ユーザ アカウントに OpenSSH 形式の SSH 公開キーを指定するには、次の手順を実行します。

SSH 公開キーを設定して、SSH クライアントでパスワードの入力を求められずにログインするには、次の手順を実行します。 SSH 公開キーは、次の 3 種類のいずれかの形式で指定できます。

- OpenSSH 形式
- Internet Engineering Task Force（IETF）SECSH 形式
- Privacy Enhanced Mail（PEM）形式の公開キー証明書

はじめる前に

この手順を開始する前に、次のことを確認してください。

- CLI に EXEC モードでログインしていること。
- OpenSSH 形式の SSH 公開キーを作成していること。
- 既存のユーザ アカウントがあること。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **username** *username* **sshkey** *ssh-key*	既存のユーザ アカウントで OpenSSH 形式の SSH 公開キーを設定します。 ユーザ アカウントを作成するには、**username** *name* **password** *pwd* コマンドを使用します。
ステップ 3	switch(config)# **exit**	グローバル コンフィギュレーション モードを終了して、EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 4	switch# **show user-account**	（任意） ユーザ アカウントの設定を表示します。
ステップ 5	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

```
switch# configure terminal
switch(config)# username user1 sshkey ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAyK
cb7Nv9Ki1OOId9/tdHHa/ngQujlvK5mXyL/n+DeOXKfVhHbX2a+V0cm7CCLUkBh+BvZRmpmOVTmU/5aw
fVhVxMKXMiPOPBc+A6/n3FVroyRwupMki6mWoM6UwaGID5gsVPqFjFNSgMWtbhjo97XVKhgjFW+wOVt8
QoAcrEtnwEfsnQk1EIr/0XIP1mqTsrqTsmjZ2vLk+fFzTGYAxMvYZI+BrN47aoH2ywS7CpnODjCDXJuD
YSPbc3PA8t0ghU/60m9R+s6AZPuljVQbGfxPrahEu4GVc6sMJNU1JxmqDJkodhMArObB4Umzj7E3Rdby
/ZWx/clTYiXQR1X1VfhQ==
switch(config)# exit
switch# show user-account
user:admin
        this user account has no expiry date
        roles:network-admin
user:user1
        this user account has no expiry date
        roles:network-operator
        ssh public key: ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAyKcb7Nv9Ki1OOId9/tdH
Ha/ngQujlvK5mXyL/n+DeOXKfVhHbX2a+V0cm7CCLUkBh+BvZRmpmOVTmU/5awfVhVxMKXMiPOPBc+A6
/n3FVroyRwupMki6mWoM6UwaGID5gsVPqFjFNSgMWtbhjo97XVKhgjFW+wOVt8QoAcrEtnwEfsnQk1EI
r/0XIP1mqTsrqTsmjZ2vLk+fFzTGYAxMvYZI+BrN47aoH2ywS7CpnODjCDXJuDYSPbc3PA8t0ghU/60m
9R+s6AZPuljVQbGfxPrahEu4GVc6sMJNU1JxmqDJkodhMArObB4Umzj7E3Rdby/ZWx/clTYiXQR1X1Vf
hQ==
switch# copy running-config startup-config
```

IETF または PEM キーの設定

ユーザ アカウントに IETF SECSH または PEM 形式の SSH 公開キーを指定するには、次の手順を実行します。

SSH 公開キーを設定して、SSH クライアントでパスワードの入力を求められずにログインするには、次の手順を実行します。 SSH 公開キーは、次の 3 種類のいずれかの形式で指定できます。

- OpenSSH 形式
- Internet Engineering Task Force（IETF）SECSH 形式
- Privacy Enhanced Mail（PEM）形式の公開キー証明書

はじめる前に

この手順を開始する前に、次のことを確認してください。

- CLI に EXEC モードでログインしていること。
- 次のいずれかの形式の SSH 公開キーを作成していること。
  - Internet Engineering Task Force（IETF）SECSH 形式

° Privacy Enhanced Mail（PEM）形式の公開キー証明書

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **copy** *server-file* **bootflash:** *filename*	サーバから SSH キーが入ったファイルをダウンロードします。 サーバは FTP、Secure Copy（SCP）、Secure FTP（SFTP）、または TFTP のいずれかを使用できます。
ステップ 2	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	switch(config)# **username** *username* **sshkey file bootflash:***filename*	SSH 公開キーを設定します。
ステップ 4	switch(config)# **exit**	グローバル コンフィギュレーション モードを終了して、EXEC モードに戻ります。
ステップ 5	switch# **show user-account**	（任意） ユーザ アカウントの設定を表示します。
ステップ 6	switch# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

```
switch# copy tftp://10.78.1.10/secsh_file.pub bootflash:secsh_file.pub vrf management
Trying to connect to tftp server......
Connection to server Established.
|
TFTP get operation was successful
switch# configure terminal
switch(config)# username User1 sshkey file bootflash:secsh_file.pub
switch(config)# exit
switch# show user-account
user:admin
        this user account has no expiry date
        roles:network-admin
user:user2
        this user account has no expiry date
        roles:network-operator
        ssh public key: ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAyKcb7Nv9Ki1OOId9/tdHHa/
ngQujlvK5mXyL/n+DeOXKfVhHbX2a+V0cm7CCLUkBh+BvZRmpmOVTmU/5awfVhVxMKXMiPOPBc+A6/n3FVroyRwupMki6
mWoM6UwaGID5gsVPqFjFNSgMWtbhjo97XVKhgjFW+wOVt8QoAcrEtnwEfsnQk1EIr/0XIP1mqTsrqTsmjZ2vLk+
fFzTGYAxMvYZI+BrN47aoH2ywS7CpnODjCDXJuDYSPbc3PA8t0ghU/60m9R+s6AZPuljVQbGfxPrahEu4GVc6sMJN
U1JxmqDJkodhMArObB4Umzj7E3Rdby/ZWx/clTYiXQR1X1VfhQ==
switch# copy running-config startup-config
```

SSH セッションの開始

IP を使用して SSH セッションを開始し、リモート装置と接続するには、次の手順を実行します。

はじめる前に

この手順を開始する前に、次のことを確認してください。

- CLI に EXEC モードでログインしていること。
- リモート デバイスのホスト名と、必要な場合はユーザ名も取得していること。
- リモート デバイスの SSH サーバがイネーブルであること。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **ssh** [**root@**] {*ip address* | *hostname* } [**vrf** *vrf-name*]	IP を使用してリモート装置との SSH IP セッションを作成します。 デフォルトの仮想ルーティングおよび転送（VRF）インスタンスはデフォルト VRF です。

```
switch# ssh root@172.28.30.77
root@172.28.30.77's password:
Last login: Sat Jul 26 11:07:23 2008 from 171.70.209.64
```

SSH ホストのクリア

SCP または SFTP を使用してサーバからファイルをダウンロードした際、またはリモート ホストへの SSH セッションを開始した際に追加された信頼できる SSH サーバのリストをアカウントからクリアするには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **clear ssh hosts**	SSH ホスト セッションをクリアします。

```
switch# clear ssh hosts
```

SSH サーバのディセーブル化

SSH サーバをディセーブルにしてスイッチへの SSH アクセスを禁止するには、この手順を使用します。 デフォルトでは、SSH サーバはイネーブルになっています。

SSH をディセーブルにした後で再度イネーブルにするには、初めに SSH サーバ キーを生成する必要があります。

はじめる前に

この手順を開始する前に、EXEC モードで CLI にログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **no feature ssh**	SSH サーバをディセーブルにします。 デフォルトではイネーブルになっています。
ステップ 3	switch(config)# **show ssh server**	（任意） SSH サーバの設定を表示します。
ステップ 4	switch(config)# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

```
switch# configure terminal
switch(config)# no feature ssh
XML interface to system may become unavailable since ssh is disabled
switch(config)#  show ssh server
ssh is not enabled
switch(config)# copy running-config startup-config
```

SSH サーバ キーの削除

SSH サーバをディセーブルにしたあと、SSH サーバ キーを削除するには、次の手順を実行します。

SSH をディセーブルにした後で再度イネーブルにするには、初めに SSH サーバ キーを生成する必要があります。

はじめる前に

この手順を開始する前に、EXEC モードで CLI にログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **no feature ssh**	SSH サーバをディセーブルにします。

	コマンドまたはアクション	目的
ステップ 3	switch(config)# **no ssh key** [**dsa** | **rsa**]	SSH サーバ キーを削除します。 デフォルトでは、すべての SSH キーが削除されます。
ステップ 4	switch(config)# **show ssh key**	（任意） SSH サーバ キーの設定を表示します。
ステップ 5	switch(config)# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

```
switch# configure terminal
switch(config)# no feature ssh
switch(config)# no ssh key rsa
switch(config)# show ssh key
**************************************
rsa Keys generated:Sun Jul 27 15:18:46 2008

ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAyKcb7Nv9Ki1OOId9/tdHHa/ngQujlvK5mXyL/n+DeOXK
fVhHbX2a+V0cm7CCLUkBh+BvZRmpmOVTmU/5awfVhVxMKXMiPOPBc+A6/n3FVroyRwupMki6mWoM6Uwa
GID5gsVPqFjFNSgMWtbhjo97XVKhgjFW+wOVt8QoAcrEtnwEfsnQk1EIr/0XIP1mqTsrqTsmjZ2vLk+f
FzTGYAxMvYZI+BrN47aoH2ywS7CpnODjCDXJuDYSPbc3PA8t0ghU/60m9R+s6AZPuljVQbGfxPrahEu4
GVc6sMJNU1JxmqDJkodhMArObB4Umzj7E3Rdby/ZWx/clTYiXQR1X1VfhQ==

bitcount:2048
fingerprint:
fd:ca:48:73:b9:ee:e7:86:9e:1e:40:46:f1:50:1d:44
**************************************
dsa Keys generated:Sun Jul 27 15:20:12 2008

ssh-dss AAAAB3NzaC1kc3MAAACBALpdxLjXNS/jcCNY+F1QZV9HegxBEb0DMUmq9bSq2N+KAcvHllEh
GnaiHhqarOlcEKqhLbIbuqtKTCvfa+Y1hBIAhWVjg1UR3/M22jqxnfhnxL5YRc1Q7fcesFax0myayAIU
nXrkO5iwv9XHTu+EInRc4kJ0XrG9SxtLmDe/fi2ZAAAAFQDbRabAjZa6GfDpwjXw5smRhrElJwAAAIEA
r50yi3hHawNnb5qgYLXhN+KA8XJF753eCWHtMw7NR8fz6fjQ1R2J97UjjGuQ8DvwpGeNQ5S+AuIo0rGq
svdg7TTecBcbgBOnR7Fs2+W5HiSVEGbvj1xaeK8fkNE6kaJumBB343b8Rgj0G97MP/os1GfkEqmX9glB
0IOM2mgHHyoAAACAfRir27hHy+fw8CxPlsK0R6cFhxYyd/qYYogXFKYIOPxpLoYrjqODeOFThU7TJuBz
aS97eXiruzbffHwzUGfXgmQT5o9IMZRTClWPA/5Ju4O9YABYHccUghf0W+QtgGOT6FOSvBh8uOV0kcHC
GMJAP8omphauZJlc+wgFxhnkyh4=

bitcount:1024
fingerprint:
44:91:32:1f:7a:d1:83:3c:f3:5e:db:53:0a:2d:ce:69
**************************************
mcs-srvr43(config)# no ssh key rsa
mcs-srvr43(config)# show ssh key
**************************************
could not retrieve rsa key information
**************************************
dsa Keys generated:Sun Jul 27 15:20:12 2008

ssh-dss AAAAB3NzaC1kc3MAAACBALpdxLjXNS/jcCNY+F1QZV9HegxBEb0DMUmq9bSq2N+KAcvHllEh
GnaiHhqarOlcEKqhLbIbuqtKTCvfa+Y1hBIAhWVjg1UR3/M22jqxnfhnxL5YRc1Q7fcesFax0myayAIU
nXrkO5iwv9XHTu+EInRc4kJ0XrG9SxtLmDe/fi2ZAAAAFQDbRabAjZa6GfDpwjXw5smRhrElJwAAAIEA
r50yi3hHawNnb5qgYLXhN+KA8XJF753eCWHtMw7NR8fz6fjQ1R2J97UjjGuQ8DvwpGeNQ5S+AuIo0rGq
svdg7TTecBcbgBOnR7Fs2+W5HiSVEGbvj1xaeK8fkNE6kaJumBB343b8Rgj0G97MP/os1GfkEqmX9glB
0IOM2mgHHyoAAACAfRir27hHy+fw8CxPlsK0R6cFhxYyd/qYYogXFKYIOPxpLoYrjqODeOFThU7TJuBz
aS97eXiruzbffHwzUGfXgmQT5o9IMZRTClWPA/5Ju4O9YABYHccUghf0W+QtgGOT6FOSvBh8uOV0kcHC
GMJAP8omphauZJlc+wgFxhnkyh4=
```

```
bitcount:1024
fingerprint:
44:91:32:1f:7a:d1:83:3c:f3:5e:db:53:0a:2d:ce:69
**************************************
mcs-srvr43(config)# no ssh key dsa
mcs-srvr43(config)# show ssh key
**************************************
could not retrieve rsa key information
**************************************
could not retrieve dsa key information
**************************************
no ssh keys present. you will have to generate them
**************************************
```

SSH セッションのクリア

デバイスから SSH セッションをクリアするには、次の手順を実行します。

はじめる前に

この手順を開始する前に、EXEC モードで CLI にログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **show users**	ユーザ セッション情報を表示します。
ステップ 2	switch# **clear line** *vty-line*	ユーザ SSH セッションをクリアします。
ステップ 3	switch# **show users**	（任意） ユーザ セッション情報を表示します。

```
switch# show users
NAME     LINE         TIME         IDLE          PID COMMENT
admin    tty1         Jul 25 19:13  old         2867
admin    pts/0        Jul 28 09:49 00:02       28556 (10.21.148.122)
admin    pts/1        Jul 28 09:46   .         28437 (::ffff:10.21.148.122)*
switch# clear line 0
switch# show users
NAME     LINE         TIME         IDLE          PID COMMENT
admin    tty1         Jul 25 19:13  old         2867
admin    pts/1        Jul 28 09:46   .         28437 (::ffff:10.21.148.122)*
mcs-srvr43(config)#
```

SSH の設定の確認

次のいずれかのコマンドを使用して、設定を確認します。

コマンド	目的
show ssh key [**dsa** | **rsa**]	SSH サーバ キー ペアの情報を表示します。

コマンド	目的
show running-config security [all]	実行コンフィギュレーション内の SSH とユーザ アカウントの設定を表示します。 キーワード all を指定すると、SSH およびユーザ アカウントのデフォルト値が表示されます。
show ssh server	SSH サーバの設定を表示します。

SSH の設定例

この例では、OpenSSH キーを使用して SSH を設定する手順を示します。

1. SSH サーバをディセーブルにします。

```
switch# configure terminal
switch(config)# no feature ssh
```

2. SSH サーバ キーを生成します。

```
switch(config)# ssh key rsa
generating rsa key(1024 bits).....
.generated rsa key
```

3. SSH サーバをイネーブルにします。

```
switch(config)# feature ssh
```

4. SSH サーバ キーを表示します。

```
switch(config)# show ssh key
rsa Keys generated:Sat Sep 29 00:10:39 2007

ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAvWhEBsF55oaPHNDBnpXOTw6+/OdHoLJZKr+MZm99n2U0
ChzZG4svRWmHuJY4PeDWl0e5yE3g3EO3pjDDmt923siNiv5aSga60K36lr39HmXL6VgpRVn1XQFiBwn4
na+H1d3Q0hDt+uWEA0tka2uOtXlDhliEmn4HVXOjGhFhoNE=

bitcount:1024
fingerprint:
51:6d:de:1c:c3:29:50:88:df:cc:95:f0:15:5d:9a:df
*************************************
could not retrieve dsa key information
*************************************
```

5. OpenSSH 形式の SSH 公開キーを指定します。

```
switch(config)# username User1 sshkey ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAy19oF6QaZl9G+3f1XswK3OiW4H7YyUyuA50rv7gsEPjhOBYmsi6PAVKui1nIf/
DQhum+lJNqJP/eLowb7ubO+lVKRXFY/G+lJNIQW3g9igG30c6k6+XVn+NjnI1B7ihvpVh7dLddMOXwOnXHYshXmSiH
3UD/vKyziEh5S4Tplx8=
```

6. 設定を保存します。

```
switch(config)# copy running-config startup-config
```

SSH 機能の履歴

この表には、機能の追加によるリリースの更新内容のみが記載されています。

機能名	リリース	機能情報
SSH	Release 5.2(1)IC1(1.1)	この機能が導入されました。

第 7 章

Telnet の設定

この章の内容は、次のとおりです。

- Telnet サーバの概要，87 ページ
- Telnet の前提条件，87 ページ
- Telnet の注意事項と制限事項，87 ページ
- Telnet のデフォルト設定，88 ページ
- Telnet の設定，88 ページ
- Telnet の設定の確認，90 ページ
- Telnet 機能の履歴，91 ページ

Telnet サーバの概要

Telnet プロトコルは、ホストとの TCP/IP 接続の確立を可能にします。 Telnet を使用すると、あるサイトのユーザが別のサイトのログインサーバと TCP 接続を確立し、キーストロークをデバイス間でやり取りできます。 Telnet は、リモート デバイス アドレスとして IP アドレスまたはドメイン名のいずれかを受け入れます。

Telnet の前提条件

レイヤ 3 インターフェイス上に IP、mgmt 0 インターフェイス上にアウトオブバンドを設定していること。

Telnet の注意事項と制限事項

- Telnet サーバはデフォルトでディセーブルになっています。

- Cisco NX-OS コマンドは Cisco IOS コマンドと異なる場合があります。

Telnet のデフォルト設定

パラメータ	デフォルト
Telnet サーバ	無効

Telnet の設定

Telnet サーバのディセーブル化

Telnet サーバはデフォルトでイネーブルになっていますが、必要な場合は、次の手順を実行して再度イネーブルにすることができます。

はじめる前に

この手順を開始する前に、EXEC モードで CLI にログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **feature telnet**	Telnet サーバをイネーブルにします。
ステップ 3	switch(config)# **show telnet server**	Telnet サーバをイネーブルにします。
ステップ 4	switch(config)# **show telnet server**	（任意） Telnet サーバの設定を表示します。
ステップ 5	switch(config)# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

```
switch# configure terminal
switch(config)# feature telnet
switch(config)# show telnet server
telnet service enabled
switch(config)# copy running-config startup-config
```

リモート装置との IP Telnet セッションの開始

はじめる前に

この手順を開始する前に、次のことを確認してください。

- CLI に EXEC モードでログインしていること。
- Telnet サーバがイネーブルで、リモート デバイスでもイネーブルであること。
- リモート デバイスのホスト名を取得し、必要な場合、リモート デバイスのユーザ名も取得していること。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **telnet** {*ip address* | *host-name*} [*port-number*] [**vrf** *vrf-name*]	指定した宛先との IP Telnet セッションを作成します。 次のキーワードと引数があります。 • *port-number*：このセッションで使用するポート番号（1 ～ 65535）。デフォルトのポート番号は 23 です。 • *vrf-name*：デフォルトの VRF はデフォルト VRF です。

```
switch# telnet 10.10.1.1
```

Telnet セッションのクリア

はじめる前に

この手順を開始する前に、EXEC モードで CLI にログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **show users**	ユーザ セッション情報を表示します。
ステップ 2	switch# **clear line** *vty-line*	ユーザ Telnet セッションをクリアします。

	コマンドまたはアクション	目的
ステップ **3**	switch# **show users**	（任意） ユーザ セッション情報を表示します。

```
switch# show users
NAME     LINE         TIME         IDLE          PID COMMENT
admin    tty1         Jul 25 19:13  old         2867
admin    pts/1        Jul 28 14:04   .         31453 (::ffff:171.70.209.8)
admin    pts/2        Jul 28 14:04   .         31475 (171.70.209.8)*
switch# clear line 1
switch# show users
NAME     LINE         TIME         IDLE          PID COMMENT
admin    tty1         Jul 25 19:13  old         2867
admin    pts/2        Jul 28 14:04   .         31475 (171.70.209.8)*
switch#
```

Telnet の設定の確認

次のいずれかのコマンドを使用して、設定を確認します。

コマンド	目的
show running-config security [**all**]	実行コンフィギュレーションのユーザアカウント設定を表示します。 all キーワードを指定すると、ユーザアカウントのデフォルト値が表示されます。
show telnet server	Telnet サーバの設定を表示します。
show hosts	現在のホストの設定詳細を表示します。
show tcp connection	接続情報を表示します。

```
switch# show running-config security all
version 4.0(1)
username admin password 5 $1$xMw2Q/1S$ZEWRvyAxAJAFV0weuSPvg1  role network-admin
username user2 password 5 $1$byNNnnSP$xfXVKjE5UEScvriwX3Kyj0  role network-operator
username user2 sshkey ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAQEAyKcb7Nv9Ki1OOIc9/tcHHa/nqQrjlvK5mXyL/n+DeOXKfVHHbX2a+V0m7CCIUkEh+BvZRmpOVIrU/5awfVivMXMiROBc+A6/n3EVroyRwpMkiGmW
dMfiwGIDgsARpjNSjNthjc97XRgjBWwOvt8QAcmEnwEEsQkEIr/OXPmqlsrqIsmjZiUk+fZCYAMXZHBNTadH2xS7pnOjDXUDSBc3PA0ojU/6hRsGVRiJQG5PaHEiG3C6sMNU1
JxmqDJkodhMArObB4Umzj7E3Rdby/ZWx/clTYiXQR1X1VfhQ==
telnet server enable

banner motd # User Access Verification #

ssh key rsa 1024 force
no ssh key dsa force
ssh server enable
```

Telnet 機能の履歴

この表には、機能の追加によるリリースの更新内容のみが記載されています。

機能名		機能情報
Telnet	Release 5.2(1)IC1(1.1)	この機能が導入されました。

第 8 章

IP ACL の設定

この章では、Cisco NX-OS デバイスの IP アクセス コントロール リスト（ACL）を設定する方法について説明します。

特に指定がなければ、IP ACL は IPv4 および IPv6 の ACL を意味します。

- ACL について，93 ページ
- IP ACL の前提条件，96 ページ
- IP ACL の注意事項と制約事項，96 ページ
- IP ACL のデフォルト設定，97 ページ
- IP ACL の設定，97 ページ
- IP ACL の設定の確認，103 ページ
- IP ACL のモニタリング，104 ページ
- IP ACL の機能の履歴，104 ページ

ACL について

ACL とは、トラフィックのフィルタリングに使用する順序付きのルール セットのことです。 各ルールには、パケットがルールに一致するために満たさなければならない条件のセットが規定されています。 デバイスは、ある ACL がパケットに適用されると判断すると、そのすべてのルールの条件にパケットを照合し、テストします。 ルールは、そのパケットが許可されるか拒否されるかを決定します。 指定されたルールのいずれにも一致しなければ、デバイスは適用可能な暗黙のルールを適用します。 デバイスは、許可されたパケットの処理を続行し、拒否されたパケットはドロップします。

ACL を使用すると、ネットワークおよび特定のホストを、不要なトラフィックや望ましくないトラフィックから保護できます。 たとえば、ACL を使用して、厳重にセキュリティ保護されたネットワークからインターネットにハイパー テキスト トランスファ プロトコル（HTTP）トラフィックが流入するのを禁止できます。 また、ACL を使用して特定のサイトへの HTTP トラフィックを

許可することもできます。その場合は、サイトの IP アドレスが、IP ACL に指定されているかどうかによって判定します。

ACL のタイプと適用

Cisco Nexus 1000V インタークラウドでは、ACL はポート プロファイルにのみ適用できます。Cisco Nexus 1000V インタークラウドでは、vEthernet インターフェイスへの ACL 適用はサポートされていません。

Cisco Nexus 1000V インタークラウドでは、トラフィック フィルタリングに IP ACL がサポートされます。 IP ACL では、デバイスは IPv4 ACL を IP トラフィックだけに適用します。

（注） このリリースでは、Cisco Nexus 1000V インタークラウドは MAC ACL をサポートしません。

ACL の適用順序

デバイスは、パケットを処理する際に、そのパケットの転送パスを決定します。 デバイスは、次の順序で ACL を適用します。

1. 入力ポート ACL
2. 出力ポート ACL

ルール

ACL によるネットワーク トラフィックのフィルタリング方法を設定する際に、何を作成、変更、削除するかを決めるのがルールです。 ルールは実行コンフィギュレーション内に表示されます。 ACL をインターフェイスに適用するか、またはインターフェイスにすでに適用されている ACL 内のルールを変更すると、スーパーバイザ モジュールは実行コンフィギュレーション内のルールから ACL のエントリを作成し、それらの ACL エントリを適用可能なインタークラウド スイッチに送信します。

アクセス リスト コンフィギュレーション モードで **permit** または **deny** コマンドを使用すると、ACL にルールを作成できます。 これにより、デバイスは許可ルール内の基準と一致するトラフィックを許可し、拒否ルール内の基準と一致するトラフィックをブロックします。 ルールに一致するためにトラフィックが満たさなければならない基準を設定するためのオプションが多数用意されています。

送信元と宛先

各ルールには、ルールに一致するトラフィックの送信元と宛先を指定します。 指定する送信元および宛先には、特定のホスト、ホストのネットワークまたはグループ、あるいは任意のホストを使用できます。

プロトコル

ACLでは、プロトコルによってトラフィックを識別できます。 一部のプロトコルは名前で指定できます。 たとえば、IP ACL では、ICMP を名前で指定できます。

IP ACL では、インターネット プロトコル番号を表す整数でプロトコルを指定できます。 たとえば、レイヤ 2 トンネリング プロトコル（L2TP）を指定するには、115 を使用します。

暗黙のルール

IP ACL には暗黙のルールがあります。暗黙のルールとは、実行コンフィギュレーションには出現しないものの、ACL の他のルールが一致しないときにデバイスがトラフィックに適用するルールのことです。 ACLのルール単位の統計情報を維持するようにデバイスを設定した場合、暗黙ルールの統計情報はデバイスに維持されません。

すべての IP ACL には、不一致の IP トラフィックを拒否する次の暗黙ルールがあります。

```
deny ip any any
```

この暗黙ルールによって、トラフィックのレイヤ 2 ヘッダーに指定されているプロトコルに関係なく、不一致トラフィックが確実に拒否されます。

その他のフィルタリング オプション

追加のオプションを使用してトラフィックを識別できます。 これらのオプションは、ACLのタイプによって異なります。 次のリストには、ほとんどの追加フィルタリング オプションが含まれていますが、すべてを網羅しているわけではありません。

- IP ACL は、次の追加フィルタリング オプションをサポートしています。
  - レイヤ 4 プロトコル
  - TCP/UDP ポート
  - ICMP タイプおよびコード
  - IGMP タイプ Version1 のみ
  - 優先レベル
  - DiffServ コード ポイント（DSCP）値
  - ACK、FIN、PSH、RST、SYN、または URG ビットがセットされた TCP パケット

シーケンス番号

デバイスはルールのシーケンス番号をサポートしています。 入力するすべてのルールにシーケンス番号が割り当てられます（ユーザによる割り当てまたはデバイスによる自動割り当て）。 シーケンス番号によって、次の ACL 設定作業が容易になります。

- 既存のルールの間に新規のルールを追加する：シーケンス番号を指定することによって、ACL 内での新規ルールの挿入場所を指定します。 たとえば、ルール番号 100 と 110 の間に新しいルールを挿入する必要がある場合は、シーケンス番号 105 を新しいルールに割り当てます。
- ルールを削除する：シーケンス番号を使用しない場合は、ルールを削除するのに、次のようにルール全体を入力する必要があります。

  ```
  switch(config-acl)# no permit tcp 10.0.0.0/8 any
  ```

  このルールに 101 番のシーケンス番号が付いていれば、次のコマンドだけでルールを削除できます。

  ```
  switch(config-acl)# no 101
  ```

- ルールを移動する：シーケンス番号を使用すれば、同じ ACL 内の異なる場所にルールを移動する必要がある場合に、そのルールのコピーをシーケンス番号で正しい位置に挿入してから、元のルールを削除できます。 この方法により、トラフィックを中断せずにルールを移動できます。

シーケンス番号を使用せずにルールを入力すると、デバイスはそのルールを ACL の最後に追加し、そのルールの直前のルールのシーケンス番号よりも 10 大きい番号を割り当てます。 たとえば、ACL 内の最後のルールのシーケンス番号が 225 で、シーケンス番号を指定せずにルールを追加した場合、デバイスはその新しいルールにシーケンス番号 235 を割り当てます。

さらに、ACL内のルールにシーケンス番号を再割り当てすることも可能です。 シーケンス番号の再割り当ては、ACL内に、100、101のように連続するシーケンス番号のルールがある場合、それらのルールの間に 1 つ以上のルールを挿入する必要があるときに便利です。

IP ACL の前提条件

- IP ACL を設定するためには、IP アドレッシングおよびプロトコルに関する知識が必要です。
- ACL を設定するポート プロファイル インターフェイス タイプについての知識が必要です。

IP ACL の注意事項と制約事項

- ほとんどの場合、IP パケットの ACL 処理は、I/O モジュール上で実行されます。 管理インターフェイス トラフィックは、常にスーパーバイザ モジュールで処理されます。この場合、速度は遅くなります。
- IP ACL は、ポート プロファイルだけに適用され、インターフェイスには適用されません。

- システム VLAN を許容するポート プロファイルに IP ACL を適用しないでください。
- 存在しない ALC がポート プロファイルに適用されると、指定された名前の ACL が作成され、適用されたポートプロファイル内のすべてのトラフィックは暗黙拒否のためにブロックされます。

IP ACL のデフォルト設定

パラメータ	デフォルト
IP ACL	デフォルトの IP ACL は存在しません。
ACL ルール	すべての ACL に暗黙のルールが適用されます。

IP ACL の設定

IP ACL の作成

デバイスに IPv4 ACL を作成し、これにルールを追加できます。

はじめる前に

この手順を開始する前に、EXEC モードで CLI にログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# [**no**] **ip access-list** {*name* | **match-local-traffic**}	名前付き IP ACL（最大 64 文字）を作成し、IP ACL コンフィギュレーション モードを開始します。 match-local-traffic オプションは、ローカルに生成されたトラフィックのマッチングをイネーブルにします。 no オプションは指定されたアクセス リストを削除します。
ステップ 3	switch(config-acl)# [*sequence-number*] { **permit** | **deny**} *protocol source destination*	IP ACL 内にルールを作成します。 多数のルールを作成できます。 sequence-number 引数には、1 ～ 4294967295 の整数を指定できます。

	コマンドまたはアクション	目的
		permit キーワードと **deny** キーワードには、トラフィックを識別するための多くの方法が用意されています。
ステップ 4	switch(config-acl)# **show ip access-lists** *name*	（任意） IP ACL の設定を表示します。
ステップ 5	switch(config-acl)# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

```
switch# configure terminal
switch(config)# ip access-list acl-01
switch(config-acl)# permit ip 192.168.2.0/24 any
switch(config-acl)# show ip access-lists acl-01
switch(config-acl)# copy running-config startup-config
```

IP ACL の変更

既存の IPv4 ACL に対してルールの追加または削除を行うことができます。 既存のルールは変更できません。 ルールを変更するには、そのルールを削除してから、変更を加えたルールを再作成します。

既存のルールの間に新しいルールを挿入する必要がある場合で、現在のシーケンス番号の空き状況ではすべてを挿入できないときは、**resequence** コマンドを使用してシーケンス番号を再割り当てします。

はじめる前に

この手順を開始する前に、EXEC モードで CLI にログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバルコンフィギュレーションモードを開始します。
ステップ 2	switch(config)# **ip access-list** *name*	指定した ACL の IP ACL コンフィギュレーションモードを開始します。
ステップ 3	switch(config-acl)# [*sequence-number*] { **permit** | **deny**} *protocol source destination*	（任意） IP ACL 内にルールを作成します。 シーケンス番号を指定すると、ACL 内のルール挿入位置を指定できます。 シーケンス番号を指定しないと、ルールは ACL の末尾に追加されます。 sequence-number

	コマンドまたはアクション	目的
		引数には、1 ～ 4294967295 の整数を指定できます。 **permit** キーワードと **deny** キーワードには、トラフィックを識別するための多くの方法が用意されています。
ステップ 4	switch(config-acl)# **no** {*sequence-number* | {**permit** | **deny**} *protocol source destination}*	（任意） 指定したルールを IP ACL から削除します。 **permit** キーワードと **deny** キーワードには、トラフィックを識別するための多くの方法が用意されています。
ステップ 5	switch(config-acl)# **show ip access-lists** *name*	（任意） IP ACL の設定を表示します。
ステップ 6	switch(config-acl)# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

```
switch# configure terminal
switch(config)# show ip access-list acl-01
switch(config)# 80 permit ip 192.168.1.0/24 any
switch(config)# ip access-list acl-01
switch(config-acl)# 100 permit ip 192.168.2.0/24 any
switch(config-acl)# no 80
switch(config-acl)# show ip access-lists acl-01
switch(config-acl)# copy running-config startup-config
```

IP ACL の削除

ACLを削除しても、適用されているインターフェイスの設定には影響しません。代わりに、デバイスは削除されたACLが空であると見なし、暗黙拒否ルールによってすべてのトラフィックを拒否します。

はじめる前に

この手順を開始する前に、次のことを確認してください。

- CLI に EXEC モードでログインしていること。
- ACL がインターフェイスに適用されているかどうかがわかっていること。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **no ip access-list** *name*	名前で指定した IP ACL を実行コンフィギュレーションから削除します。
ステップ 3	switch(config)# **show ip access-list** *name* **summary**	（任意） IP ACL の設定を表示します。 ACL がインターフェイスに引き続き適用されている場合は、インターフェイスが表示されます。
ステップ 4	switch(config)# **copy running-config startup-config**	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

```
switch# configure terminal
switch(config)# no ip access-list acl-01
switch(config)# show ip access-lists acl-01 summary
switch(config)# copy running-config startup-config
```

IP ACL 内のシーケンス番号の変更

IP ACL 内のルールに付けられたすべてのシーケンス番号を変更できます。

はじめる前に

この手順を開始する前に、EXEC モードで CLI にログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **resequence ip access-list** *name starting-sequence-number increment*	ACL 内に記述されているルールにシーケンス番号を付けます。指定した開始シーケンス番号が最初のルールに付けられます。 後続の各ルールには、直前のルールよりも大きい番号が付けられます。 番号の間隔は、指定した増分によって決まります。 starting-sequence-number 引数と increment 引数は、1 ～ 4294967295 の整数で指定します。

	コマンドまたはアクション	目的
ステップ 3	switch(config)# **show ip access-lists** *name*	IP ACL の設定を表示します。
ステップ 4	switch(config)# **show ip access-lists** *name*	（任意） IP ACL の設定を表示します。
ステップ 5	switch(config)# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

```
switch# configure terminal
switch(config)# resequence access-list ip acl-01 100 10
switch(config)# show ip access-lists acl-01
switch(config)# copy running-config startup-config
```

IP ACL のポート プロファイルへの追加

IP ACL をポート プロファイルに追加するには、次の手順を実行します。

次の情報を知っている必要があります。

- 新しいポートプロファイルを作成する場合は、プロファイルに指定する名前を知っている必要があります。
- このポート プロファイルに対して設定する IP アクセス コントロール リストの名前。
- アクセス リストのパケット フローの方向。

はじめる前に

この手順を開始する前に、次のことを確認してください。

- CLI に EXEC モードでログインしていること。
- このポート プロファイルに追加する IP ACL が作成され、名前がわかっていること。
- 既存のポートプロファイルを使用する場合は、それが作成され、名前がわかっていること。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	switch(config)# **port-profile** [**type vethernet**] *name*	名前付きポート プロファイルのポート プロファイル コンフィギュレーション モードを開始します。
ステップ 3	switch(config-port-prof)# **ip port access-group** *name* { **in** | **out** }	着信トラフィックまたは発信トラフィックのポートプロファイルに名前付き ACL を追加します。
ステップ 4	switch(config-port-prof)# **show port-profile** [**brief** | **expand-interface** | **usage**] [**name** *profile-name*]	（任意） 確認のためにコンフィギュレーションを表示します。
ステップ 5	switch(config-port-prof)# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

```
switch# configure terminal
switch(config)# port-profile AccessProf
switch(config-port-prof)# ip port access-group allaccess4 out
switch(config-port-prof)# show port-profile name AccessProf
switch(config-port-prof)# copy running-config startup-config
```

管理インターフェイスへの IP ACL の適用

管理インターフェイス mgmt0 に IPv4 または ACL を適用するには、次の手順を実行します。

適用する ACL が存在し、目的に応じたトラフィック フィルタリングが設定されていることを確認します。

はじめる前に

この手順を開始する前に、EXEC モードで CLI にログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **interface mgmt0**	管理インターフェイスのインターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	switch(config-if)# [**no**] **ip access-group***access-list* [**in** | **out**]	指定したインバウンド IPv4 ACL またはアウトバウンド IPv4 ACL をインターフェイスに適用します。 no オプションは指定された設定を削除します。
ステップ 4	switch(config-if)# **show ip access-lists** *access-list*	（任意） ACL の設定を表示します。
ステップ 5	switch(config-if)# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

```
switch# configure terminal
switch(config)# interface mgmt0
switch(config-if)# ip access-group telnet in
switch(config-if)# show ip access-lists telnet summary
IP access list telnet
statistics per-entry
Total ACEs Configured:2

Configured on interfaces:
mgmt0 - ingress (Router ACL)

Active on interfaces:
mgmt0 - ingress (Router ACL)
switch(config-if)# copy running-config startup-config
```

IP ACL の設定の確認

次のいずれかのコマンドを使用して、設定を確認します。

コマンド	目的
show running-config aclmgr	IP ACL の設定および IP ACL が適用されているインターフェイスを含めて、ACL の設定を表示します。
show ip access-lists [*name*]	すべての IPv4 アクセス コントロール リスト（ACL）または特定の IPv4 ACL を表示します。
show ip access-list [*name*] **summary**	設定済みのすべての IPv4 ACL または名前付き IPv4 ACL の要約を表示します。
show running-config port profile	ACL を適用したポートプロファイルのコンフィギュレーションを表示します。

IP ACL のモニタリング

IP ACL のモニタリングには、次のいずれかのコマンドを使用します。

コマンド	目的
show ip access-lists	IPv4 ACL の設定を表示します。
show ip access-summary	アクセスリストが設定されているインターフェイスの詳細を表示します。

IP ACL の機能の履歴

この表には、機能の追加によるリリースの更新内容のみが記載されています。

機能の履歴	リリース	機能情報
IP ACL	Release 5.2(1)IC1(1.1)	この機能が導入されました。