Cisco NX-OS 基本ネットワークデバイスの ISE TACACS+ 構成ガイド

セキュア アクセスを実現するハウツー ユーザ シリーズ

作成者：シスコ、セキュリティ ビジネス グループ、ポリシーとアクセス、テクニカル マーケティング

日付：2016 年 1 月

目次

このマニュアルについて

概要

クライアント/サーバ プロトコルである Terminal Access Controller Access Control System Plus（TACACS+）は、ルータなどの多くのタイプのネットワーク アクセス デバイスへの管理アクセスを提供するため、ユーザに一元化されたセキュリティ制御を実装します。TACACS+ では、次の AAA サービスを提供します。

- Authentication（認証）：ユーザは誰か
- Authorization（許可）：ユーザは何を実行できるか
- Accounting（アカウンティング）：誰が何を、いつ実行したか

このドキュメントでは、TACACS+ サーバとして Cisco Identity Services Engine（ISE）、TACACS+ クライアントとして Cisco NX-OS ネットワーク デバイスを使用する TACACS+ の設定例を示します。

このガイドの使用方法

このガイドでは、次の 2 部構成で、Cisco NX-OS 基本ネットワーク デバイスへの管理アクセスを ISE で管理できるようにします。

- パート 1：ISE のデバイス管理の設定
- パート 2：Cisco NX-OS の TACACS+ の設定

使用するコンポーネント

このドキュメントの情報は、以下のソフトウェア バージョンおよびハードウェア バージョンに基づいています。

- ISE VMware 仮想アプライアンス リリース 2.0
- VMware vSphere 用 Cisco Nexus1000V（N1Kv）、Cisco NX-OS 5.2(1)SV3(1.10)

ほとんどの Cisco NX-OS デバイスで動作します。

このドキュメントの資料はラボ環境のデバイスから作成されています。すべてのデバイスはクリア済み（デフォルト）の設定で開始しています。

ISE のデバイス管理の設定

ISE でのデバイス管理のライセンス

デバイス管理（TACACS+）は展開ごとにライセンスされ、有効な ISE BASE ライセンスまたはモビリティ ライセンスが必要です。

ISE でのデバイス管理の有効化

デバイス管理サービス（TACACS+）は ISE ノードでデフォルトで有効になっていません。最初の手順は、有効にすることです。

手順 1 サポートされているブラウザの 1 つを使用して ISE 管理 Web ポータルにログインします。

手順 2 [管理（Administration）] > [システム（System）] > [展開（Deployment）] に移動します。ISE ノードの隣にあるチェックボックスをオンにして、[編集（Edit）] をクリックします。

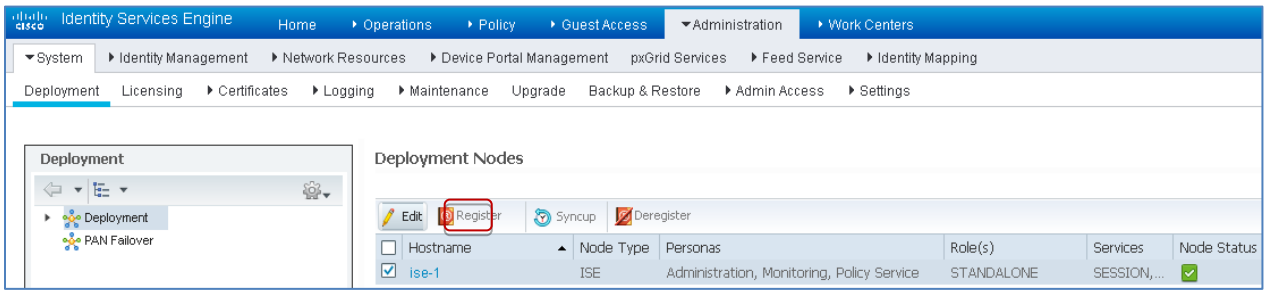

図 1. ISE 展開ページ

手順 3 [全般設定（General Settings）] で下にスクロールし、[デバイス管理サービスを有効にする（Enable Device Admin Service）] の隣にあるチェックボックスをオンにします。

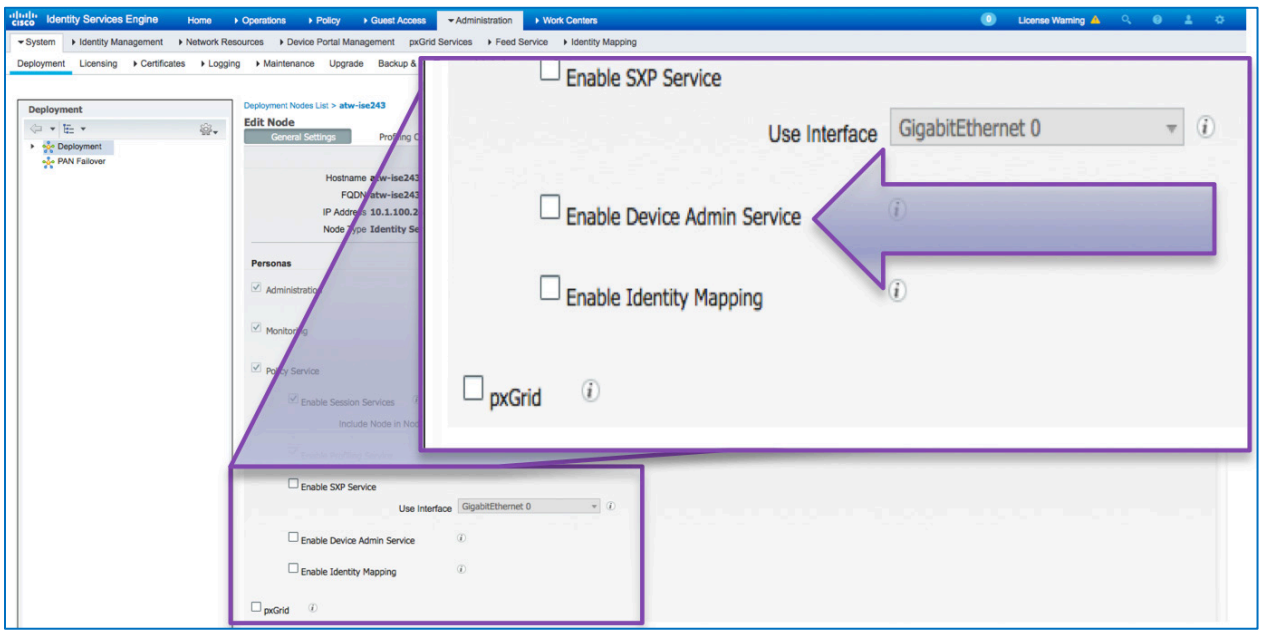

図 2. ISE 展開の全般設定

手順 4 [保存(Save)] で設定を保存します。これでデバイス管理サービスが ISE で有効になります。

デバイス管理ワーク センター

ISE 2.0 はワーク センターを導入しています。ワーク センターは、それぞれが特定のフィーチャのすべての要素を包含しています。

手順 1 [ワーク センター(Work Centers)] > [デバイス管理(Device Administration)] > [概要(Overview)] に移動します。

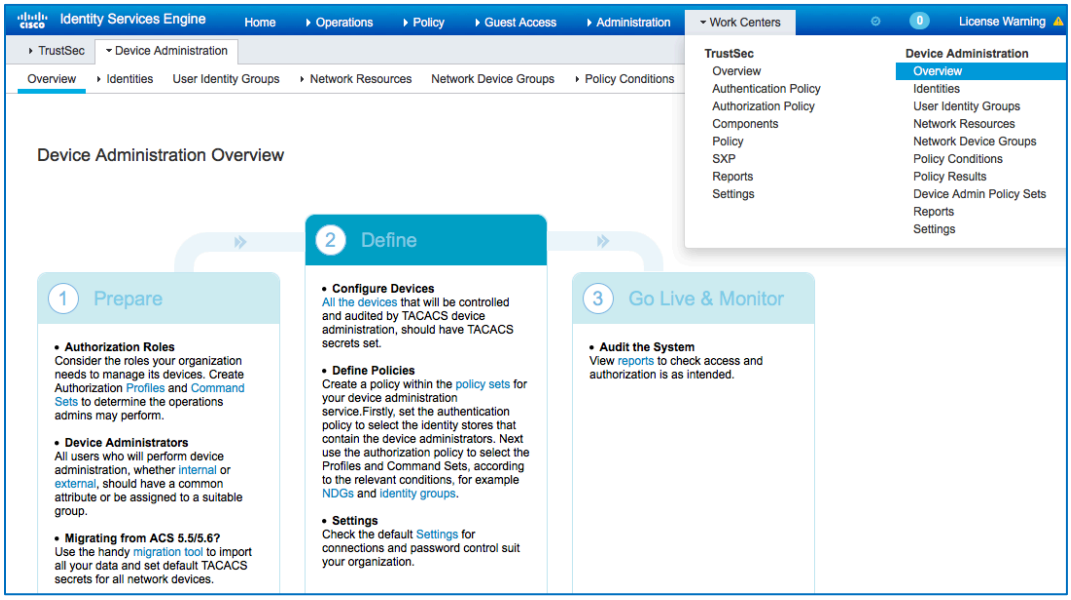

図 3. デバイス管理の概要

[デバイス管理の概要(Device Administration Overview)] では、使用例の大まかな手順を提供します。

ネットワーク デバイスとネットワーク デバイス グループ

ISE では、複数のデバイス グループ階層を使用する強力なデバイス グループ化機能を提供しています。各階層はネットワーク デバイスの別個の独立した分類を表します。

手順 1 [ワーク センター(Work Centers)] > [デバイス管理(Device Administration)] > [ネットワーク デバイス グループ(Network Device Groups)] に移動します。

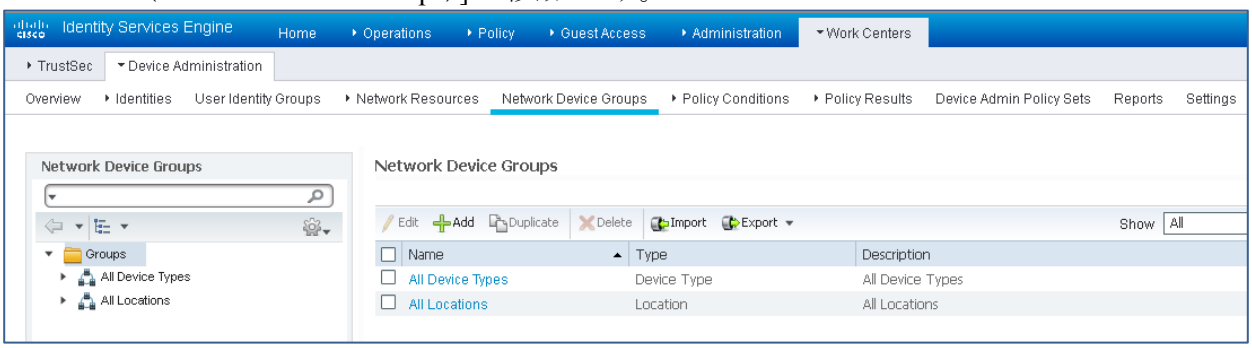

図 4. ネットワーク デバイス グループ

[すべてのデバイス タイプ（All Device Types）] と [すべてのロケーション（All Locations）] は、ISE により提供されるデフォルトの階層です。独自の階層を追加したり、後でポリシー条件に使用できるネットワーク デバイスを識別するためにさまざまなコンポーネントを定義したりできます。

手順 2 階層を定義すると、ネットワーク デバイス グループは、次のように表示されます。

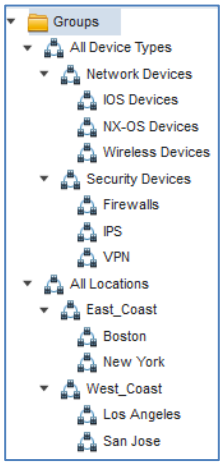

図 5. ネットワーク デバイス グループのツリー ビュー

手順 3 ここでは、ネットワーク デバイスとして N1Kv を追加します。[ワーク センター（Work Centers）] > [デバイス管理（Device Administration）] > [ネットワーク リソース（Network Resources）] に移動します。[追加（Add）] をクリックし、新しいネットワーク デバイス **DMZ_BLDO_N1Kv** を追加します。

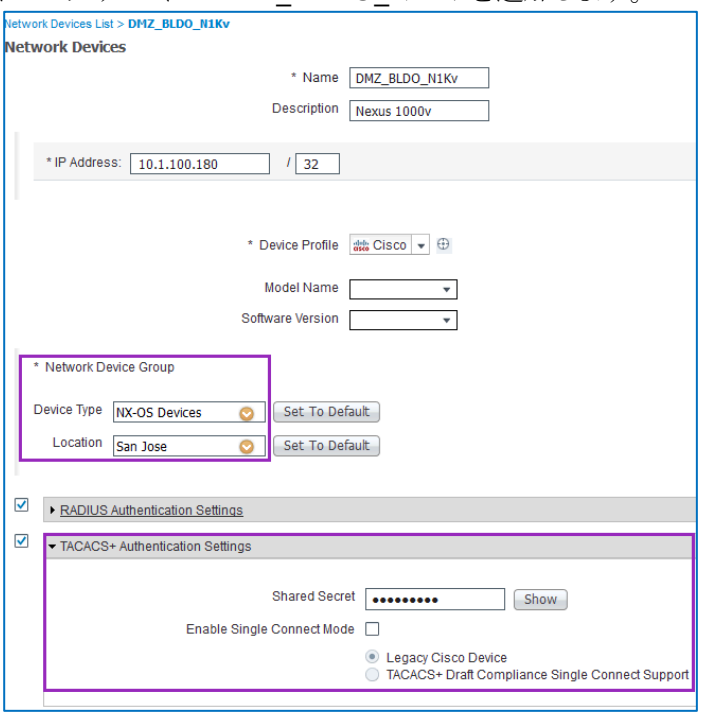

図 6. ネットワーク デバイスの追加

デバイスの IP アドレスを入力し、デバイスの [ロケーション（Location）] と [デバイス タイプ（Device Type）] がマッピングされることを確認します。最後に、[TACACS+ 認証設定（TACACS+ Authentication Settings）] を有効にし、[共有秘密（Shared Secret）] を指定します。

ID ストア

このセクションでは、デバイス管理者の ID ストアを定義します。ID ストアは ISE 内部ユーザおよびサポートされる外部 ID ソースにすることができます。ここでは、Active Directory（AD）、外部 ID ソースを使用します。

手順 1 [管理（Administration）] > [ID の管理（Identity Management）] > [外部 ID ソース（External Identity Sources）] > [Active Directory] に移動します。[追加（Add）] をクリックし、新しい AD の参加ポイントを定義します。参加ポイント名と AD ドメイン名を指定し、[送信（Submit）] をクリックします。

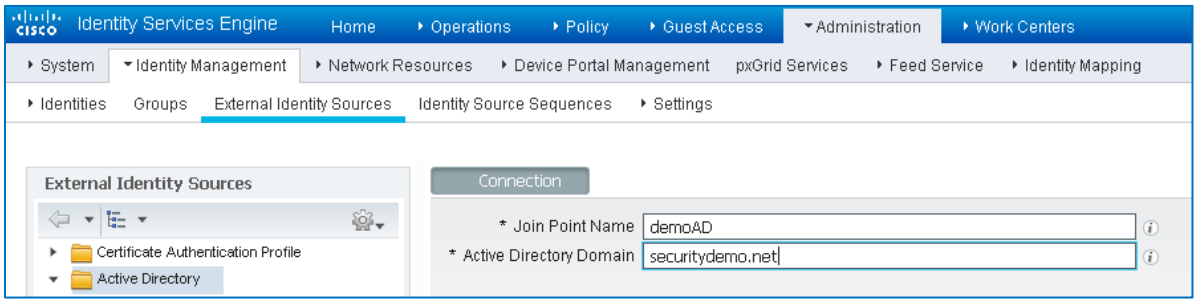

図 3. AD 参加ポイントの追加

手順 2 「この Active Directory ドメインにすべての ISE ノードを参加させますか?（Would you like to Join all ISE Nodes to this Active Directory Domain?）」というプロンプトが表示されたら、[はい（Yes）] をクリックします。AD への参加特権があるクレデンシャルを入力し、[参加（Join）] で ISE を AD に参加させます。[ステータス（Status）] をチェックし、稼働中であることを確認します。

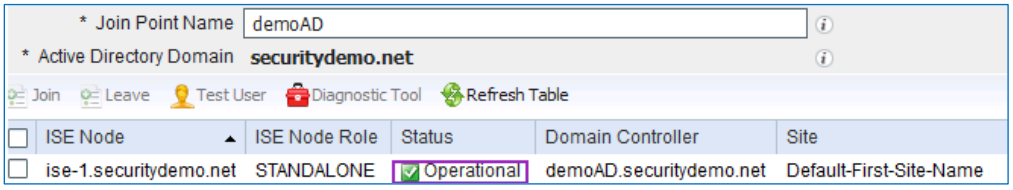

図 4. ISE の AD への参加

手順 3 [グループ（Groups）] タブに移動し、[追加（Add）] をクリックして、デバイス アクセスが許可されるユーザに基づいて必要なグループをすべて取得します。このガイドの承認ポリシーに使用するグループを以下の例に示します。

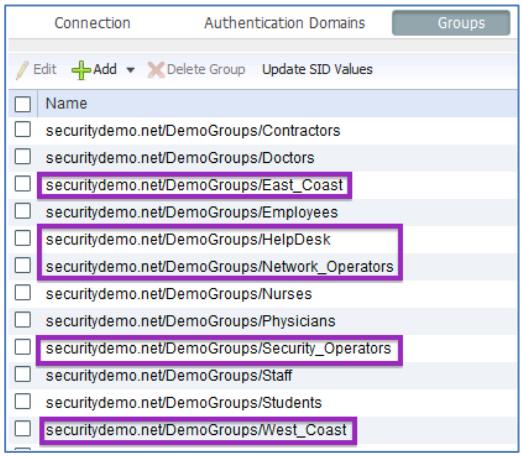

図 5. AD グループ

TACACS プロファイル

Cisco TACACS+ は、Internet Engineering Task Force（IEFT）仕様の cisco-av-pair ベンダー固有属性（VSA）オプションを実装しています。フォーマットは、`protocol : attribute separator value *` です。

Cisco NX-OS デバイスが認証に TACACS+ を使用すると、TACACS+ サーバは Cisco VSA の認証結果とともにユーザの属性を返します。TACACS+ 認証については、Cisco NX-OS ソフトウェアが以下のようにサポートします。

シェル：access-accept パケットのプロトコルとして、ユーザ プロファイル情報を提供します。
ロール：access-accept パケットの属性として、ユーザが属するすべてのロールをリストします。ロール名は空白で区切られます。

各ユーザ ロールには、ロールに割り当てられたユーザに許可される操作を定義する 1 つ以上のルールが含まれています。各ユーザは、ロールによって許可されたすべてのコマンドの組み合わせを実行できるように、複数のロールを持つことができます。

NX-OS デバイスの定義済みロールは、NX-OS プラットフォームによって異なります。次の 2 つは共通です。

network-admin：事前定義のネットワーク管理ロールには、スイッチのすべてのコマンドの完全な読み取り/書き込みアクセス権があります。デバイス（Nexus 7000 など）に複数の VDC がある場合に限り、デフォルトの仮想デバイス コンテキスト（VDC）で利用できます。このロールで利用可能なすべてのコマンドのリストを表示するには、NX-OS CLI コマンド「`show cli syntax roles network-admin`」を使用します。
network-operator：事前定義のネットワーク管理ロールには、スイッチのすべてのコマンドの完全な読み取りアクセス権があります。デバイス（Nexus 7000 など）に複数の VDC がある場合に限り、デフォルトの VDC で利用できます。このロールで利用可能なすべてのコマンドのリストを表示するには、NX-OS CLI コマンド「`show cli syntax roles network-operator`」を使用します。

最近の NX-OS リリースでは VDC あたり最大 64 のユーザ ロールを作成することができます。ユーザ定義のユーザ ロールは、デフォルトでは、*show*、*exit*、*end*、および *configure terminal* コマンドのみのアクセスが許可されています。他のアクセスを付与するには、ルールとロール機能を追加する必要があります。

各ロール機能で許可されるコマンドのリストを表示するには、NX-OS CLI コマンド「`show role feature name <feature-name>`」を発行します。すべてのロールの機能のリストを表示するには、NX-OS CLI コマンド「`show role feature detail`」を発行します。**Interface** 機能で利用可能なことを表示する例を示します。

```
N1Kv# show role feature name interface
interface       (Interface configuration commands)
  show interface *
  config t ; interface *
```

TACACS+ ユーザのユーザ名が Cisco NX-OS デバイスでローカルに定義されているユーザ名と同じ場合は、Cisco NX-OS ソフトウェアは、TACACS+ サーバで設定されたユーザ ロールではなく、ローカル ユーザ アカウントのユーザ ロールを適用します。

3 つの TACACS プロファイル、NX-OS Operator、NX-OS Admin、および NX-OS Security を定義します。

NX-OS Operator

手順 4 ISE 管理 Web ポータルで、[ワーク センター(Work Centers)] > [デバイス管理(Device Administration)] > [ポリシー結果(Policy Results)] > [TACACS プロファイル(TACACS Profiles)] の順に移動します。新しい TACACS プロファイルを追加し、**NX-OS Operator** という名前を付けます。

手順 5 [カスタム属性(Custom Attributes)] セクションまで下にスクロールして、次のように属性を追加します。

タイプ	名前	値
必須	shell:roles	network-operator

手順 6 行を保持するには、エントリの末尾にある ✓ チェックマークをクリックします。

手順 7 [未処理(Raw)] ビューのタブをクリックします。以下が表示されます。

プロファイル属性

```
shell:roles=network-operator
```

手順 8 [送信(Submit)] をクリックしてプロファイルを保存します。

NX-OS Admin

手順 9 別のプロファイルを追加して、**NX-OS Admin** という名前を付けます。

手順 10 [カスタム属性(Custom Attributes)] セクションまで下にスクロールして、次のように属性を追加します。

タイプ	名前	値
必須	shell:roles	network-admin

手順 11 行を保持するには、エントリの末尾にある ✓ チェックマークをクリックします。

手順 12 [未処理(Raw)] ビューのタブをクリックします。以下が表示されます。

プロファイル属性

```
shell:roles=network-admin
```

手順 13 [送信(Submit)] をクリックしてプロファイルを保存します。

NX-OS Security

手順 14 ISE 管理 Web ポータルで、[ワーク センター(Work Centers)] > [デバイス管理(Device Administration)] > [ポリシー結果(Policy Results)] > [TACACS プロファイル(TACACS Profiles)] の順に移動します。新しい TACACS プロファイルを追加し、**NX-OS Operator** という名前を付けます。

手順 15 [カスタム属性(Custom Attributes)] セクションまで下にスクロールして、次のように属性を追加します。

タイプ	名前	値
必須	shell:roles	”network-operator demo-security”

値を二重引用符で囲むのは、空白文字で分離されている 2 つのロール名を含めるためです。demo-security ロールは、ユーザ定義ロールで、後で NX-OS デバイスで設定します。

手順 16 行を保持するには、エントリの末尾にある ✓ チェックマークをクリックします。

手順 17 [未処理(Raw)] ビューのタブをクリックします。以下が表示されます。

プロファイル属性

```
shell:roles=”network-operator demo-security”
```

手順 18 [送信(Submit)] をクリックしてプロファイルを保存します。

TACACS コマンド セット

NX-OS コマンド認証は、デバイスの管理者がコマンドの発行を承認されているかどうか確認するために、設定された TACACS+ サーバを照会します。NX-OS は、通常、ユーザ ロールで承認されます。使用可能なコマンドを最適化するために、ISE がユーザに許可するコマンドのリストを提供します。

3 つのコマンドセット HelpDesk_Commands、Permit_All_Commands、および NX-OS_Security_Commands を定義します。

HelpDesk コマンド

これは、IOS デバイスのガイドのものと同じです。すでに定義してある場合は、このセクションを省略してください。

手順 19 ISE 管理者 Web ポータルで、[ワーク センター（Work Centers）] > [デバイス管理（Device Administration）] > [ポリシー結果（Policy Results）] > [TACACS コマンド セット（TACACS Command Sets）] の順に移動します。新しいセットを追加し、**HelpDesk_Commands** という名前を付けます。

手順 20 [+追加（+Add）] をクリックして、セットにエントリを設定します。

付与	コマンド（Command）	引数
許可	debug	
許可	undebug	
許可	traceroute	
拒否	ping	^([0-9]{1,3})\.([0-9]{1,3})\.([0-9]{1,3})\.255$
許可	ping	
許可	show	

ヘルプデスクのアナリストに、debug、undebug、traceroute、および show の実行を許可します。ping については、引数列の正規表現に示すように、ネットワーク サブネットはブロードキャスト アドレスを 255 までと想定しているため、ブロードキャスト ping は制限されています。

手順 21 行を保持するには、各エントリの末尾にある ✓ チェックマークをクリックします。

手順 22 [保存（Save）] をクリックして、コマンド セットを保存します。

Permit All コマンド

これは、IOS デバイスのガイドのものと同じです。すでに定義してある場合は、このセクションを省略してください。

手順 23 新しいセットを追加し、**Permit_All_Commands** という名前を付けます。

手順 24 [下にリストされていないコマンドを許可（Permit any command that is not listed below）☑] の隣にあるチェックボックスをオンにして、コマンド リストを空のままにします。

付与	コマンド	引数

手順 25 [保存（Save）] をクリックして、コマンド セットを保存します。

NX-OS Security コマンド

手順 26 ISE 管理者 Web ポータルで、[ワーク センター（Work Centers）] > [デバイス管理（Device Administration）] > [ポリシー結果（Policy Results）] > [TACACS コマンド セット（TACACS Command Sets）] の順に移動します。新しいセットを追加し、**NX-OS_Security_Commands** という名前を付けます。

手順 27 [下にリストされていないコマンドを許可（Permit any command that is not listed below）☑] の隣のチェックボックスをオンにします。

手順 28 [+追加（+Add）] をクリックして、セットにエントリを設定します。

付与	コマンド	引数
拒否	interface	mgmt0
拒否	interface	control0

mgmt0 インターフェイスと control0 インターフェイスの設定以外のすべてのコマンドの実行をセキュリティ アナリストに許可します。

手順 29 行を保持するには、各エントリの末尾にある ✓ チェックマークをクリックします。

手順 30 [保存（Save）] をクリックして、コマンド セットを保存します。

デバイス管理ポリシー セット

ポリシー セットはデバイス管理でデフォルトで有効になっています。ポリシー セットはデバイス タイプに基づいてポリシーを分割できるため、TACACS プロファイルの適用が容易になります。たとえば、Cisco IOS デバイスでは権限レベルとコマンド セットを使用し、Cisco NX-OS デバイスではカスタム属性を使用します。

手順 1 [ワーク センター（Work Centers）] > [デバイス管理（Device Administration）] > [デバイス管理ポリシー セット（Device Admin Policy Sets）] に移動します。次の新しいポリシーセット **NX-OS Devices** を追加します。

S	名前	説明	条件
✓	NX-OS Devices		DEVICE:Device Type EQUALS Device Type#All Device Types#Network Devices#NX-OS Devices

図 6. ポリシー セットの条件

手順 2 承認ポリシーを作成します。認証では、ID ストアとして AD を使用します。

認証ポリシー	
✓	Default Rule（なにも一致しない場合）: Allow Protocols : Default Device Administration and use: demoAD

図 7. 認証ポリシー

手順 3 承認ポリシーを定義します。ここでは、AD のユーザ グループとデバイスのロケーションに基づいて承認ポリシーを定義します。たとえば、AD グループ West Coast のユーザは、West Coast のデバイスのみにアクセスできます。

S	ルール名	条件	コマンド セット	シェル プロファイル
✓	HelpDesk West	DEVICE:Location CONTAINS All Locations#West_Coast AND demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/West_Coast AND demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/HelpDesk	HelpDesk_Commands	NX-OS Operator
✓	HelpDesk East	DEVICE:Location CONTAINS All Locations#East_Coast AND demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/East_Coast AND demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/HelpDesk	HelpDesk_Commands	NX-OS Operator
✓	Security West	DEVICE:Location CONTAINS All Locations#West_Coast AND demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/West_Coast AND demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/Security_Operators	NX-OS_Security_Commands	NX-OS Admin
✓	Security East	DEVICE:Location CONTAINS All Locations#East_Coast AND demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/East_Coast AND demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/Security_Operators	NX-OS_Security_Commands	NX-OS Admin
✓	Admin West	DEVICE:Location CONTAINS All Locations#West_Coast AND demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/West_Coast AND demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/Network_Operators	Permit_All_Commands	NX-OS Admin

S	ルール名	条件	コマンド セット	シェル プロファイル
✓	Admin East	DEVICE:Location CONTAINS All Locations#East_Coast AND demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/East_Coast AND demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/Network_Operators	Permit_All_Commands	NX-OS Admin
✓	Default	なにも一致しない場合	DenyAllCommands	

図 8.　許可ポリシー

これで、NX-OS のデバイス管理の ISE 設定が完了しました。

NX-OS の TACACS+ の設定

SSH は、Cisco NX-OS デバイスではデフォルトで有効にされているため、必要なのは、TACACS+ を設定する前に管理インターフェイスの適切な IP アドレッシングを確認することだけです。

```
ip domain-name securitydemo.net
switchname N1Kv

interface mgmt0
  ip address 10.1.100.180/24
  no shutdown

vrf context management
  ip route 0.0.0.0/0 10.1.100.1

!!! disable DNS lookup !!!
no ip domain-lookup

!!! VLANs !!!!
vlan 100
  name mgt

!!! Define VTY access !!!
ip access-list vtyAccess
  10 permit tcp 10.1.100.0/24 10.1.100.180/32 eq 22
  20 deny ip any any

line console
  exec-timeout 0
line vty
  access-class vtyAccess in
```

この段階で上述のサンプル ネットワーク デバイスに有効な IP アドレスがあるため、10.1.100.0/24 のクライアントからこの NX-OS デバイスに SSH 通信できます。AAA 設定時に発生する可能性のあるアクセス問題を避けるために、CONSOLE の EXEC タイムアウトは無効にされていることに注意してください。

Cisco NX-OS デバイスの TACACS+ AAA は次の順序で設定可能です。

1. TACACS+ 認証とフォールバックを有効化する
2. TACACS+ コマンド認証を有効化する
3. TACACS+ コマンド アカウンティングを有効化する

TACACS+ 認証とフォールバック

TACACS+ 認証は、次のような設定で有効化できます。

```
tacacs+ enable

role name demo-security
  description A user-defined role example for demo purposes
  rule 10 permit read-write feature interface
  interface policy deny
    permit interface Vethernet1

tacacs-server host 10.1.100.21 key ISEisC00L timeout 10
tacacs-server host 10.1.100.21 test username tp-test password tp-test idle-time 60

aaa group server tacacs+ demoTG
 server 10.1.100.21
 deadtime 10
 use-vrf management
 source-interface mgmt 0

aaa authentication login ascii-authentication
aaa authentication login default group demoTG
aaa authentication login console local
```

ここでは、VTY の行を認証するために TACACS+ に切り替えました。TACACS+ コマンドはまだ認証されていないので、TACACS+ ユーザは現在、ユーザ ロールに基づいて認証されます。

設定された TACACS+ サーバが利用できなくなるイベントでは、ログイン認証は「ローカル」のユーザ データベースにフォールバックします。

TACACS+ コマンド認証

これは、ユーザが各自のロールで認証できるので、オプションです。コンフィギュレーション モードおよび EXEC モード用の TACACS+ コマンド認証は次を追加することで有効化できます。

```
aaa authorization config-commands default group demoTG local
aaa authorization commands default group demoTG local
```

TACACS+ コマンド アカウンティング

コマンド アカウンティングによって、実行された各コマンドの情報（コマンド、日付、ユーザ名など）が送信されます。以下は、前述の設定例に、このアカウンティング機能の有効化を追加します。

```
aaa accounting default group demoTG
```

NX-OS の TACACS+ の設定が完了しました。

次のステップ

Cisco NX-OS のデバイス管理者の設定が完了しました。設定を確認する必要があります。

手順 1 SSH 通信で、さまざまなロールとして NX-OS デバイスにログインします。

手順 2 デバイスのコマンドライン インターフェイス(CLI)で、ユーザが適切なコマンドにアクセスできることを確認します。たとえば、ヘルプデスクのユーザは通常の IP アドレス(10.1.10.1 など)を ping できますが、ブロードキャスト アドレス(10.1.10.255 など)の ping は拒否されなければなりません。

手順 3 ユーザ接続とロールを表示するには、以下を発行します。

```
show users
show user-account [<user-name>]
```

出力例は次のとおりです。

```
N1Kv# show users
NAME     LINE         TIME         IDLE          PID COMMENT
admin    ttyS0        Jan 11 02:50   .21234
hellen   pts/0        Jan 11 02:52   .21697 (10.1.100.6) session=ssh *
N1Kv# show user-account hellen
user:hellen
        roles:network-operator
account created through REMOTE authentication
Credentials such as ssh server key will be cached temporarily only for this user account
Local login not possible...
```

手順 4 次のデバッグは、TACACS+ のトラブルシューティングに役に立ちます。

```
debug tacacs+ aaa-request
```

次にデバック出力例を示します。

```
2016 Jan 11 03:03:08.652514 tacacs[6288]:  process_aaa_tplus_request:Checking for state of mgmt0
port with servergroup demoTG
2016 Jan 11 03:03:08.652543 tacacs[6288]:  process_aaa_tplus_request: Group demoTG found.
corresponding vrf is management
2016 Jan 11 03:03:08.652552 tacacs[6288]:  process_aaa_tplus_request: checking for mgmt0
vrf:management against vrf:management of requested group
2016 Jan 11 03:03:08.652559 tacacs[6288]:  process_aaa_tplus_request:port_check will be done
2016 Jan 11 03:03:08.652568 tacacs[6288]:  state machine count 0
2016 Jan 11 03:03:08.652677 tacacs[6288]:  is_intf_up_with_valid_ip(1258):Proper IOD is found.
2016 Jan 11 03:03:08.652699 tacacs[6288]:  is_intf_up_with_valid_ip(1261):Port is up.
2016 Jan 11 03:03:08.653919 tacacs[6288]:  debug_av_list(797):Printing list
2016 Jan 11 03:03:08.653930 tacacs[6288]:  35 : 4 : ping
2016 Jan 11 03:03:08.653938 tacacs[6288]:  36 : 12 : 10.1.100.255
2016 Jan 11 03:03:08.653945 tacacs[6288]:  36 : 4 : <cr>
2016 Jan 11 03:03:08.653952 tacacs[6288]:  debug_av_list(807):Done printing list, exiting
function
2016 Jan 11 03:03:08.654004 tacacs[6288]:  tplus_encrypt(659):key is configured for this aaa
sessin.
2016 Jan 11 03:03:08.655054 tacacs[6288]:  num_inet_addrs: 1 first s_addr: -1268514550
180.100.1.10 s6_addr : 0a01:64b4::
2016 Jan 11 03:03:08.655065 tacacs[6288]:  non_blocking_connect(259):interface ip_type: IPV4
2016 Jan 11 03:03:08.656023 tacacs[6288]:  non_blocking_connect(369): Proceeding with bind
2016 Jan 11 03:03:08.656216 tacacs[6288]:  non_blocking_connect(388): setsockopt success error:22
2016 Jan 11 03:03:08.656694 tacacs[6288]:  non_blocking_connect(489): connect() is in-progress
for server 10.1.100.21
2016 Jan 11 03:03:08.679815 tacacs[6288]:  tplus_decode_authen_response: copying hostname into
context 10.1.100.21
```

手順 5 ISE GUI から、[運用（Operations）] > [TACACS ライブログ（TACACS Livelog）] の順に移動します。すべての TACACS 認証要求と許可要求がここでキャプチャされており、詳細ボタンにより、特定のトランザクションが成功または失敗した理由の詳細情報を確認できます。

Username	Type	Authorization Policy	Matched Comman...	Shell Profile	Failure Reason
	All				
hellen	Authorization	NX-OS Devices >> HelpDesk West			13025 Command failed to match a Permit rule
hellen	Authorization	NX-OS Devices >> HelpDesk West	HelpDesk Commands		
hellen	Authorization	NX-OS Devices >> HelpDesk West		NX-OS Operator	
hellen	Authentication				
sean	Authorization	NX-OS Devices >> Security West			13025 Command failed to match a Permit rule
sean	Authorization	NX-OS Devices >> Security West	NX-OS Security Co...		
sean	Authorization	NX-OS Devices >> Security West		NX-OS Security	
sean	Authentication				
neo	Authorization	NX-OS Devices >> Admin West	Permit All Commands		
neo	Authorization	NX-OS Devices >> Admin West		NX-OS Admin	
neo	Authentication				

図 9. TACACS Livelog

手順 6 履歴レポートを確認する場合は、[ワーク センター（Work Centers）] > [デバイス管理（Device Administration）] > [レポート（Reports）] > [デバイス管理（Device Administration）] の順に移動し、認証、許可、アカウンティングのレポートを取得します。