Cisco ASA での 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 2 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 デバイスに管理アクセスするための、一元化されたセキュリティ制御を提供します。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 Adaptive Security Appliance（ASA）を使用する TACACS+ の構成例を示します。

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 ASA 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 ASA 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
- Cisco 適応型セキュリティ仮想アプライアンス（ASAv）、Cisco ASA ソフトウェアのバージョン 9.5(2) と Adaptive Security Device Manager（ASDM）バージョン 7.5(2)
- Oracle Java™ SE ランタイム環境、ビルド 1.7.0_40-b43

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。

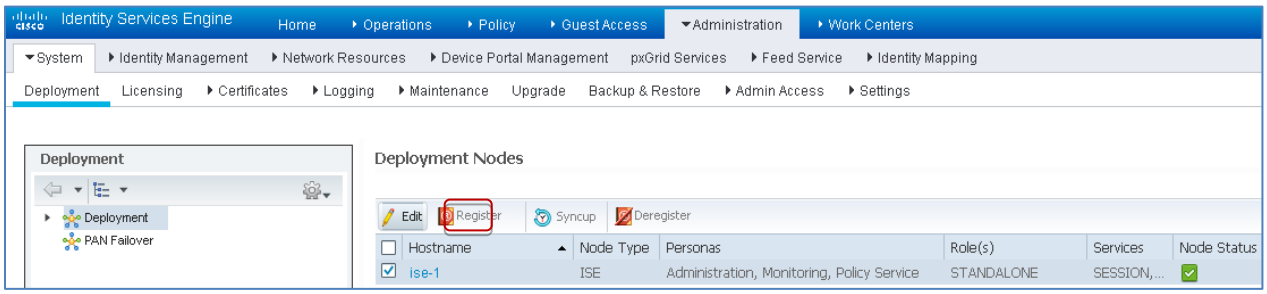

図 1. ISE 展開ページ

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。

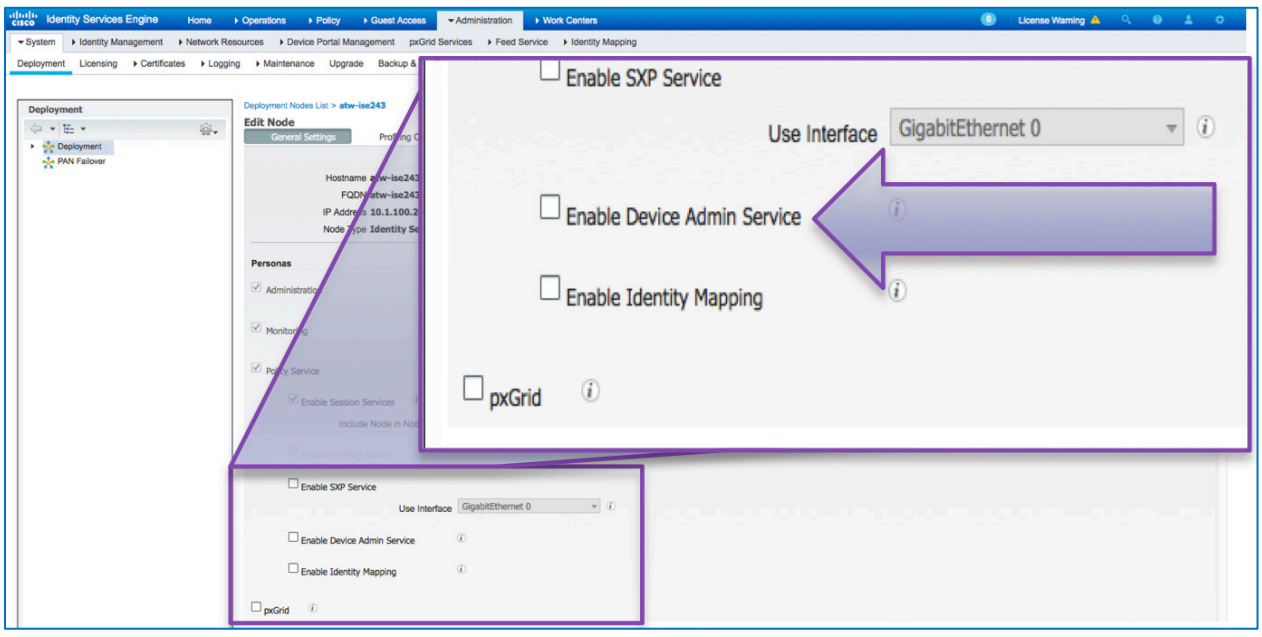

図 2. ISE 展開の全般設定

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。

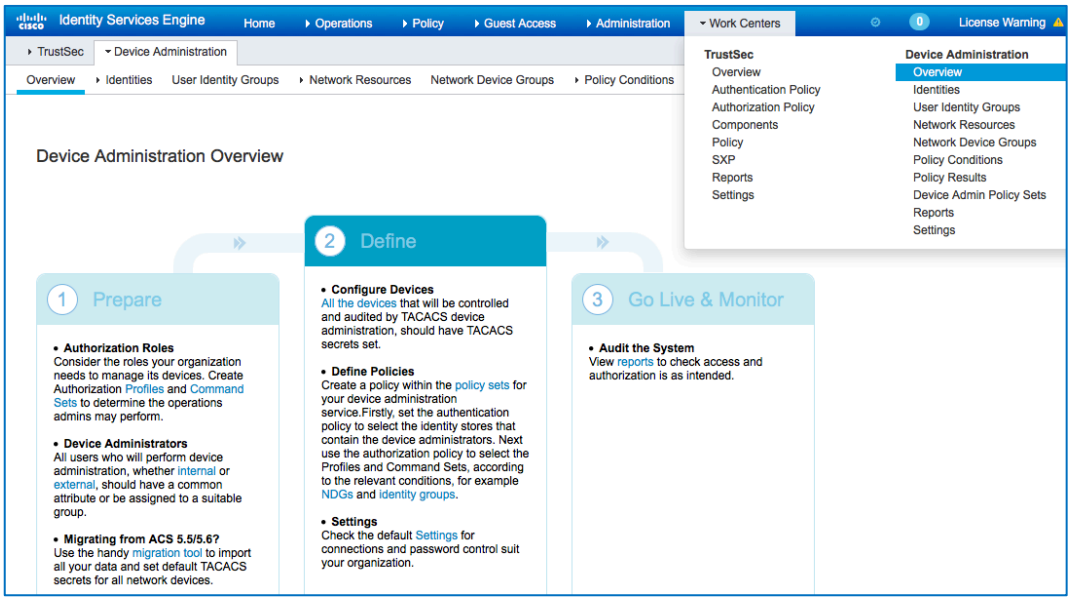

図 3.　デバイス管理の概要

[デバイス管理の概要(Device Administration Overview)] では、デバイス管理の使用例に必要な手順の概要を提供します。

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。

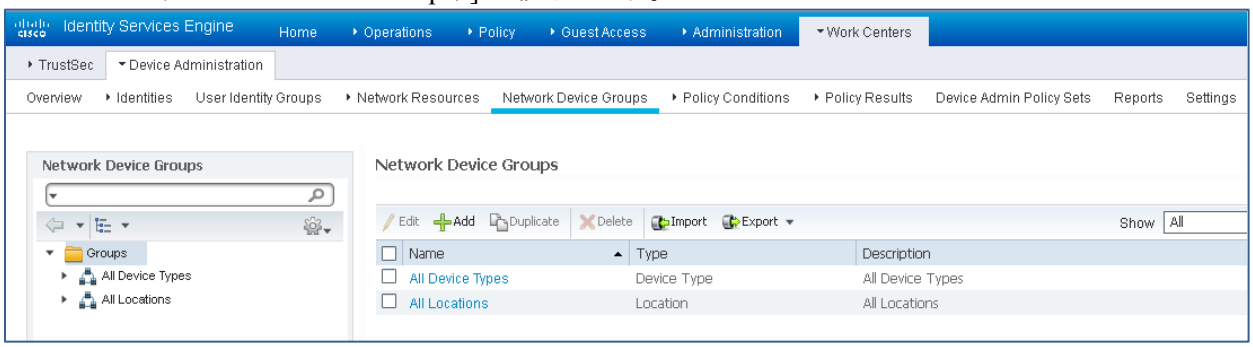

図 4.　ネットワーク デバイス グループ

[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。

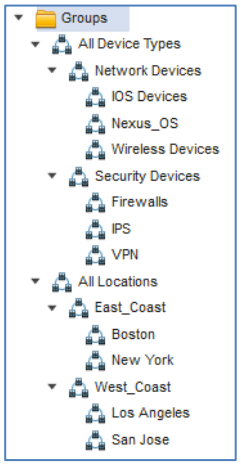

図 5. ネットワーク デバイス グループのツリー ビュー

手順 3 ここでは、ネットワーク デバイスとして ASAv 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_ASAv** を追加します。

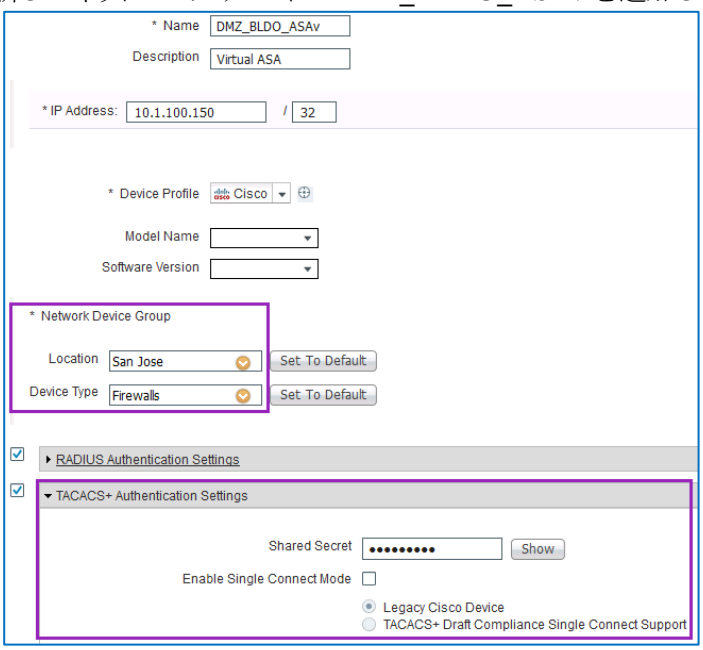

図 6. ネットワーク デバイスの追加

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。

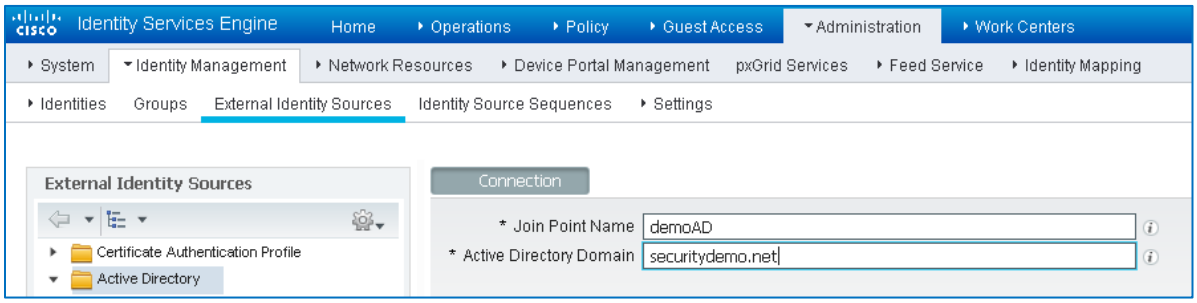

図 3. AD 参加ポイントの追加

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。

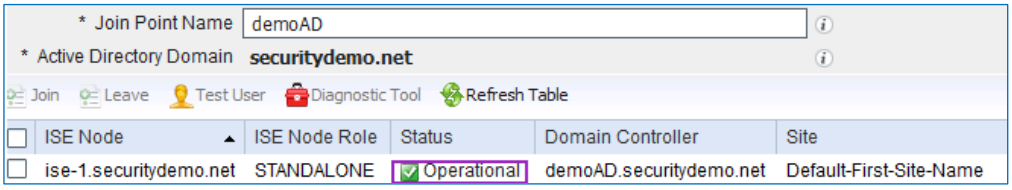

図 4. ISE の AD への参加

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。

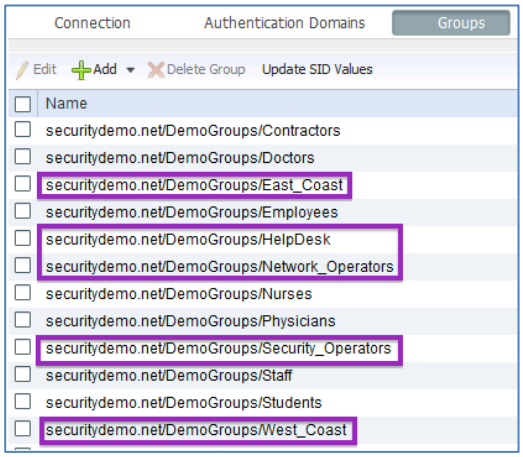

図 5. AD グループ

TACACS プロファイル

Cisco ASA は、コマンド認証に 16 のレベルのアクセス権限を提供します。次の 3 つはデフォルトで定義されています。

権限レベル 0：*show checksum*、*show curpriv*、*show history*、*show version,*、*enable*、*help*、*login*、*logout*、*pager*、*show pager*、*clear pager*、および *quit* コマンドを許可します。ログイン後、1 が最低限のアクセス可能レベルなので、このレベル 0 のすべてのコマンドはすべてのユーザが実行できます。

権限レベル 1：非特権またはユーザ EXEC モードは、ログインしたユーザのデフォルトの権限レベルです。シェル プロンプトは、「ciscoasa>」など、デバイス名に山カッコが続きます。

権限レベル 15：特権 EXEC モードは、enable コマンド後のレベルです。シェル プロンプトは、「ciscoasa#」など、デバイスのホスト名にシャープ記号が続きます。

デフォルトでは、ASA のコマンドの特権レベルはすべて、0、1、または 15 です。ASDM のロールベースの制御では、レベル 15（管理者）、レベル 5（読み取り専用）、レベル 3（モニタのみ）の 3 つの ASDM ユーザ ロールを事前定義します。これらは、ISE ポリシーで使用し、後で、「ASDM 定義ユーザ ロール」で設定します。

EXEC 認証では、ユーザにシェル（EXEC）セッションの開始が許可されているかどうかを確認するために、ASA デバイスは認証直後に AAA サーバに TACACS+ 認証要求を送信します。ISE は、次の 2 つの属性を適用して、これをユーザ単位にカスタマイズできます。

デフォルトの権限（Default Privilege）：シェル セッションに対する初期（デフォルト）の権限レベルを指定します。承認済みユーザはレベル 1 ではなく、このレベルに初期化されます。

最大権限（Maximum Privilege）：シェル セッションで許可される最大レベルを指定します。承認済みユーザは、より低いデフォルト レベルにログインし、enable コマンドを使用して、この属性で割り当てられた値に達するまで、より高いレベルに移行できます。外部 AAA サーバを使用する場合は、ASA は 15 までの有効化のみを許可します。

ASA Monitor Only

これは、ASDM の [ホーム（Home）] ペインと [モニタリング（Monitoring）] ペインにユーザを制限することです。

手順 1 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て、**ASA Monitor Only** という名前を付けます。

手順 2 [共通タスク（Common Tasks）] セクションまでスクロールします。ドロップダウン セレクタから値が 3 のデフォルトの権限、ドロップダウンから値が 4 の最大権限を有効にします。

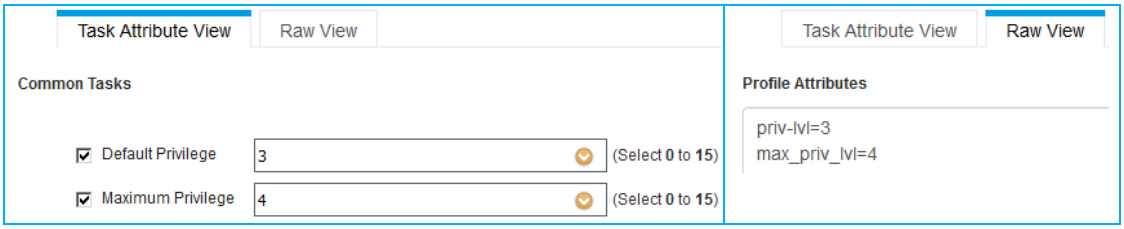

図 6. ASA Monitor Only の TACACS プロファイル

最大権限の 4 は説明のためだけに示されていて、今回は使用しません。外部 AAA サーバを使用しているときは ASA 有効化は 15 しか許可しないからです。

手順 3 [送信(Submit)] をクリックしてプロファイルを保存します。

ASA Read Only

これは、ユーザに ASDM の読み取り専用アクセスを提供することです。

手順 4 新しい TACACS プロファイルを追加し、**ASA Read Only** という名前を付けます。

手順 5 [共通タスク(Common Tasks)] セクションまでスクロールします。ドロップダウン セレクタから値が 5 のデフォルトの権限、ドロップダウンから値が 7 の最大権限を有効にします。

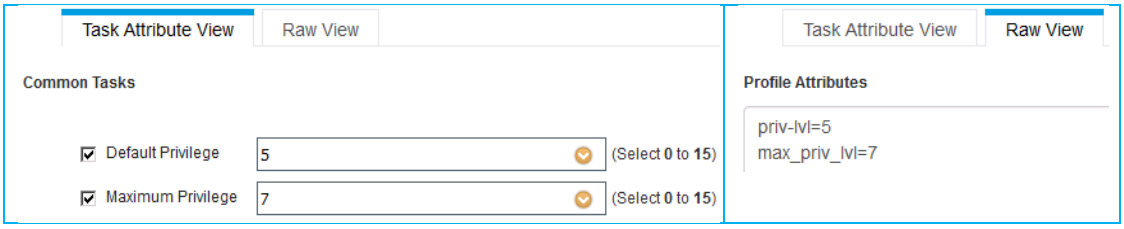

図 7. ASA Read Only の TACACS プロファイル

最大権限の 7 は説明のためだけに示されていて、今回は使用しません。外部 AAA サーバを使用しているときは ASA 有効化は 15 しか許可しないからです。

手順 6 [送信(Submit)] をクリックしてプロファイルを保存します。

ASA Admin

これは、ASDM の無制限のアクセス権を付与します。

手順 7 別のプロファイルを追加し、**ASA Admin** という名前を付けます。

手順 8 [共通タスク(Common Tasks)] セクションまでスクロールします。ドロップダウン セレクタから値が 15 のデフォルトの権限、ドロップダウンから値が 15 の最大権限を有効にします。

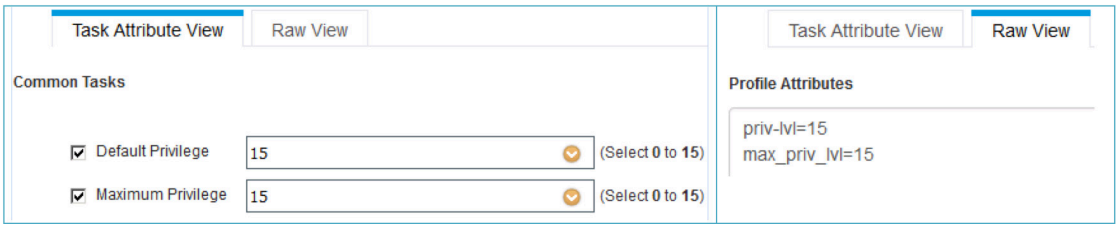

図 8. ASA Admin の TACACS プロファイル

最大権限の 15 は、ユーザが ユーザ EXEC モードで「enable」を発行したときに、ASA CLI で使用されます。

手順 9 [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

ASA コマンド認証は、デバイスの管理者が権限レベルにかかわらず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。

4 つのコマンドセット、HelpDesk_Commands、Permit_All_Commands、ASA Basic、ASA_ReadOnly_Extra 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 1 ISE GUI 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 2 [✚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
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 3 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 4 [送信（Submit）] 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 5 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 6 [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 7 [送信（Submit）] をクリックして、コマンド セットを保存します。

ASA Basic

手順 8 新しいセットを追加し、**ASA Basic** という名前を付けます。

手順 9 [✚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
許可	show	checksum|curpriv|history|pager|version
許可	enable	
許可	help	
許可	login	
許可	logout	
許可	pager	
許可	clear	pager
許可	quit	
許可	exit	

最初のエントリは、**show** コマンドに続けることができる引数の一覧を示します。これは、`show checksum`、`show curpriv`、`show history`、`show pager`、および `show version` のいずれかに相当します。

手順 10 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 11 [送信(Submit)] をクリックして、コマンド セットを保存します。

ASA ReadOnly Extra

手順 12 新しいセットを追加し、**ASA ReadOnly Extra** という名前を付けます。

手順 13 [✚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
許可	more	
許可	dir	
許可	export	

手順 14 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 15 [送信(Submit)] 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 ASA デバイスでは権限レベルとコマンド セットを使用し、WLC デバイスではカスタム属性を使用します。

ASDM はメニューや他のグラフィカル ユーザ インターフェイス要素によって駆動されるため、ASDM アクセスには ASA CLI より多くのコマンドを許可する必要があります。

2 つのポリシー セット、ASDM アクセスを認証するポリシーと、他の ASA 管理アクセスを認証するポリシーを定義します。

ASDM Authz

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 **ASDM Authz** を追加します。

S	名前	説明	条件
√	ASDM Authz		DEVICE:Device Type EQUALS Device Type#All Device Types#Network Devices#Firewalls AND TACACS:Type EQUALS Authorization AND TACACS:Port EQUALS 443

図 9. ASDM Authz のポリシー設定条件

ASDM 認証要求は、デフォルトの HTTPS ポートを使用しているときは、TACACS ポートの値 443 を使用して送信されます。ASDM が代替ポートを使用する場合は、この条件の値をカスタマイズしたポートに更新します。

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 を使用して、認証要求のユーザ名を特定するために使用します。

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

図 10. ASDM Authz の認証ポリシー

手順 3 承認ポリシーを定義します。ASDM アクセスには 3 つの事前定義された権限レベルが適用されます。したがって、簡単にするために、すべての認証された管理者に Permit_All_Commands を付与します。

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	Permit_All_Commands	ASA Monitor Only
√	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	Permit_All_Commands	ASA Monitor Only
√	Security West	DEVICE:Location CONTAINS All Locations#West_Coast AND demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/West_Coast AND	Permit_All_Commands	ASA Admin

S	ルール名	条件	コマンド セット	シェル プロファイル
		demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/Security_Operators		
√	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	Permit_All_Commands	ASA 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	ASA Read Only
√	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	ASA Read Only
√	Default	なにも一致しない場合	DenyAllCommands	

図 11. ASDM Authz の承認ポリシー

ASA Regular

手順 4 [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。既存のポリシー セット ***ASDM Authz*** を選択し、[以下を複製(Duplicate Below)] を選択します。新しいポリシー セットは以前のセットの下にランク付けされるので、その条件は非限定的になることがあります。複製したコピーを更新し、次のようにデバイス タイプのみを調整します。

S	名前	説明	条件
√	ASA Regular		DEVICE:Device Type EQUALS Device Type#All Device Types#Network Devices#Firewalls

図 12. ASA Regular のポリシー設定条件

手順 5 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 Admin and use: demoAD

図 13. ASA Regular の認証ポリシー

手順 6 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。シェル プロファイルは主に、ASDM アクセスと、ASA でローカル コマンド認証を使用する ASA CLI のためのものです。

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	ASA_Basic AND HelpDesk_Commands	ASA Monitor Only
√	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	ASA_Basic AND HelpDesk_Commands	ASA Monitor Only
√	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	Permit_All_Commands	ASA 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	Permit_All_Commands	ASA 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	ASA_Basic AND HelpDesk_Commands AND ASA_ReadOnly_Commands	ASA Read Only

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	ASA_Basic AND HelpDesk_Commands AND ASA_ReadOnly_Commands	ASA Read Only
√	Default	なにも一致しない場合	DenyAllCommands	

図 14. ASA Regular の承認ポリシー

これで、ASA のデバイス管理の ISE 設定が完了しました。

ASA の TACACS+ の設定

TACACS+ を設定する前に、IP アドレッシングと、適切なリモート接続プロトコルを最初に設定する必要があります。次に、ASA CLI アクセス用の SSH および ASDM アクセス用の HTTP を有効にする方法を示しています。

```
hostname ASAv
domain-name securitydemo.net

crypto key generate rsa modulus 2048 noconfirm

console timeout 0

interface Management0/0
 management-only
 nameif management
 security-level 100
 ip address 10.1.100.150 255.255.255.0
 no shutdown

route management 0.0.0.0 0.0.0.0 10.1.100.1 1

ssh 10.1.100.0 255.255.255.0 management
ssh timeout 30
ssh version 2

http server enable
http 10.1.100.0 255.255.255.0 management

username sec-admin password ISEisC00L privilege 15

aaa authentication ssh console LOCAL
aaa authentication enable console LOCAL
aaa authorization exec LOCAL auto-enable
```

この段階でサンプル ネットワーク デバイスに有効な IP アドレスがあるため、コンソール ログインは認証されていなくても、10.1.100.0/24 のクライアントから 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。

バージョン 9.5(1) から、ASA には管理専用インターフェイスとしてルーティング テーブルがあります。接続されているどのサブネット上にも存在しないファイル サーバに接続する、デフォルト ルートを追加します。

ASA バージョン 9.2(1) では、十分な権限を持つデバイス管理者がパスワードを 2 回入力しなくてもいいように、Cisco IOS と ASA の動作を近づけるために、EXEC 認証の *auto-enable* オプションが追加されました。

ASDM を使用するには、ASDM バイナリを disk0 にアップロードする必要があります。たとえば、ASA で以下のコマンドを実行します。

```
copy http://a.web.file.server/path/to/asdm-752.bin disk0:/
```

Cisco ASDM-IDM Launcher がまだインストールされていない場合は、Web ブラウザを使用して https://10.1.100.150/admin にアクセスし、[ASDM Launcher のインストール（Install ASDM Launcher）] または [ASDM の実行（Run ASDM）] のいずれかをクリックします。グローバル イネーブル パスワードがない場合は、ASDM-IDM Launcher で 10.1.100.150 を指し、空のユーザ名とパスワードでログインするか、ローカル管理者のクレデンシャルを使用できます。

Cisco ASA 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。

```
aaa-server demoTG protocol tacacs+
aaa-server demoTG (management) host 10.1.100.21
 key ISEisC00L

clear configure aaa

aaa authentication ssh console demoTG LOCAL
aaa authentication enable console demoTG LOCAL
aaa authentication http console demoTG LOCAL
aaa authentication secure-http-client
```

ここでは、SSH および ASDM のアクセスを認証するために TACACS+ に切り替えました。TACACS+ を使用した SSH への正常なログインの権限レベルはすべて 1、ASDM の場合の権限レベルはすべて 15 です。

「enable」認証行は、すべての接続タイプ向けなので、VTY および CONSOLE の両方が TACACS+ を使用して「イネーブル」アクセスを認証します。最大権限レベルが 15 の管理者のみが、「enable」を正常に発行できます。AAA の「イネーブル」認証は引数なしで実行され、デフォルトで 15 に設定されるためです。

設定された TACACS+ サーバが利用できなくなるイベントでは、ログイン認証とイネーブル認証はどちらも「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。フォールバック アクセスが許可されるユーザは、透過的にアクセスするために、ローカル パスワードを外部 AAA サーバと同じにする必要があります。

コマンド認証

EXEC 認証

EXEC 認証は、コマンド認証の特別な形式です。ユーザのログイン直後に行われ、以下を追加することで有効化できます。

```
aaa authorization exec authentication-server auto-enable
```

前に説明したように、`auto-enable` は、ASA 9.2(1) で追加されるため、古いコードの ASA を実行している場合は、このオプションは省略します。この時点で、*デフォルト*の権限属性を持つシェル プロファイルは、新しい SSH セッションに適用されます。

バージョン 9.4(1) から、ASA は ASDM の EXEC 認証とその他の接続タイプを分離するため、以下も追加します。

```
aaa authorization http console demoTG
```

ローカル コマンド認証

ローカル コマンド認証を使用すると、管理者は、自分の権限レベル以下に割り当てられたコマンドを使用することができます。以下のように設定します。

```
aaa authorization command LOCAL
```

ASDM 定義ユーザ ロール

ASDM 定義ユーザ ロールは、ASDM アクセスの 3 つの権限レベル（3、5、15）を表します。これらを設定するには、ASDM では、この 3 つの権限レベルにコマンドを再度割り当てます。これらは、ローカル コマンド認証で直接使用するか、TACACS+ コマンド認証のフォールバックとして使用します。

フル アクセス権を持つ ASA 管理者として ASDM にログインし、[設定（Configuration）] > [デバイス管理（Device Management）] > [ユーザ/AAA（Users/AAA）] > [AAA アクセス（AAA Access）] > [認証（Authorization）] の順に移動し、[ASDM 定義ユーザ ロールの設定...（Set ASDM Defined User Roles...）] ボタンをクリックします。[ASDM 定義ユーザ ロール設定（ASDM Defined User Role Setup）] ポップアップ ウィンドウで [はい（Yes）] をクリックします。

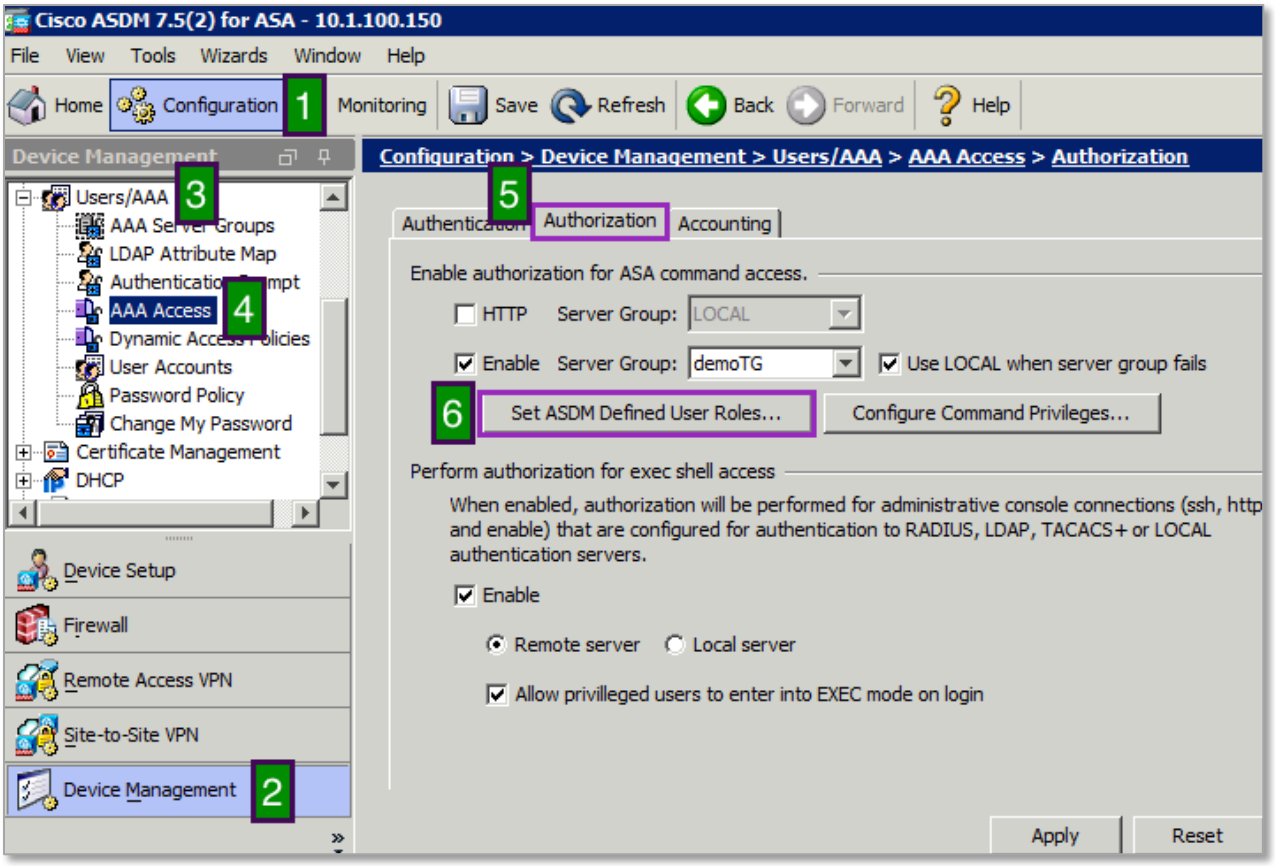

図 15. ASDM 定義ユーザ ロールの設定

このために設定されている特権コマンドの一覧を表示するには、図 16 に示すように、ASDM の設定でオプション [☑ デバイスに送信する前にプレビューする（Preview commands before sending them to the device）] をオンにします。[適用（Apply）] をクリックして ASA に設定を送信し、プレビュー オプションを有効にしている場合は、[CLI コマンドのプレビュー（Preview CLI Commands）] ポップアップ ウィンドウで [送信（Send）] をクリックします。

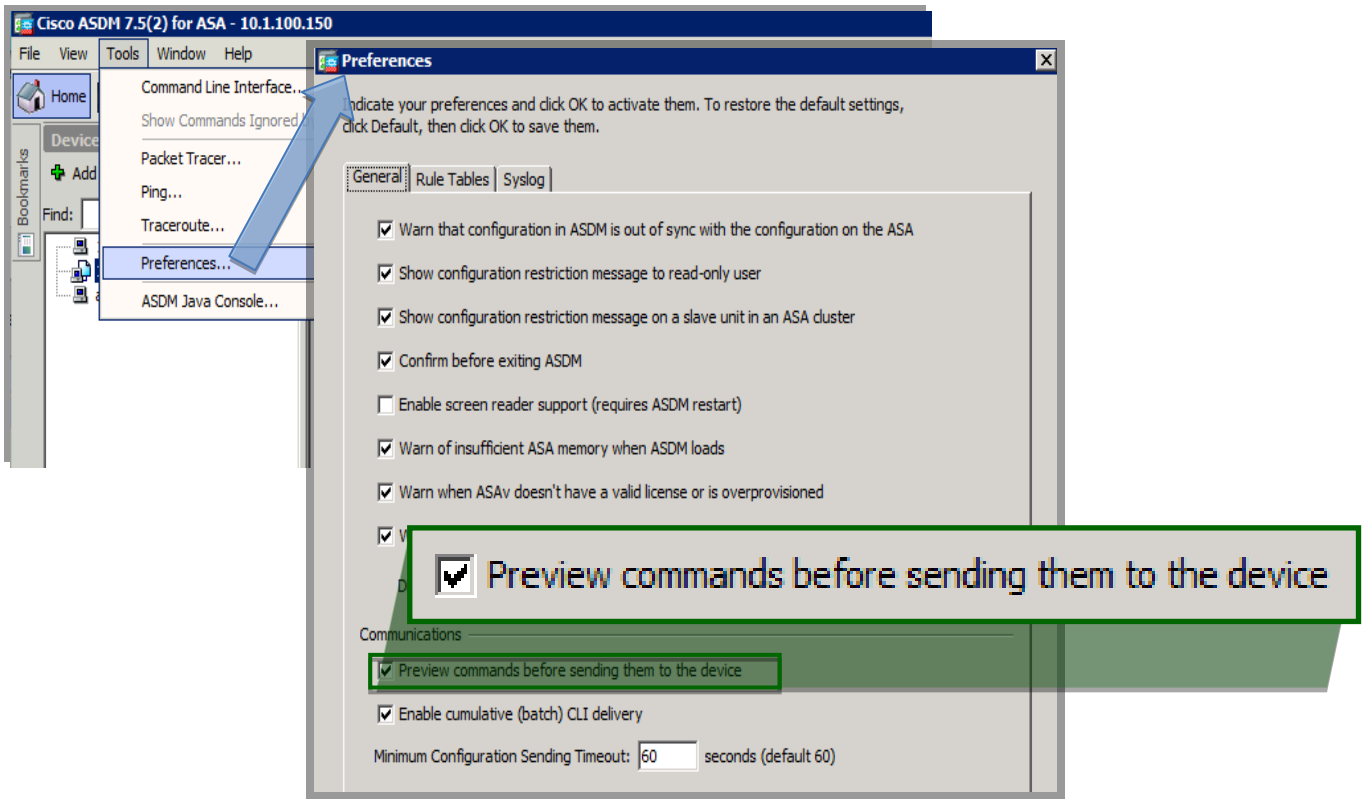

図 16. ASA 送信前にコマンドをプレビューする ASDM 設定

TACACS+ コマンド認証

TACACS+ コマンド認証を使用するには、次を設定します。

```
aaa authorization command demoTG LOCAL
```

これで、権限レベルごとに利用可能な一覧が上書きされ、TACACS+ サーバのコマンド一覧に管理者の現在の権限レベルよりも高い権限レベルのコマンドが含まれることがあります。

TACACS+ アカウンティング

ASA は、以下により、TACACS+ サーバ グループに管理ユーザのアクションの記録を有効にすることができます。

```
aaa accounting ssh console demoTG
aaa accounting serial console demoTG
aaa accounting enable console demoTG
```

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 command demoTG
```

これは、「show」コマンド以外のすべてのコマンドのアカウンティング メッセージを送信します。オプションの権限キーワードで最小限の権限レベルを指定できます。たとえば、「`aaa accounting command privilege 3 demoTG`」は、「show」を除く、レベル 3 以上の権限レベルのコマンド アカウンティングを送信します。

ASA の TACACS+ の設定が完了しました。

次のステップ

Cisco ASA 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 ASA 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 ユーザ接続を表示するには、以下を発行します。

```
show ssh sessions
show asdm sesssions
show curpriv
```

出力例は次のとおりです。

```
ASAv# show ssh sessions

SID Client IP       Version Mode Encryption Hmac     State            Username
2   10.1.100.6      2.0     IN   aes256-ctr sha1     SessionStarted   hellen
                            OUT  aes256-ctr sha1     SessionStarted   hellen
ASAv# show asdm sessions
0 10.1.100.6
AASAv# show curpriv
Username : hellen
Current privilege level : 3
Current Mode/s : P_PRIV
...
```

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 aaa common
debug tacacs
```

次にデバック出力例を示します。

```
mk_pkt - type: 0x1, session_id: 495
 user: neo
 Tacacs packet sent
Sending TACACS Start message.Session id: 495, seq no:1
Received TACACS packet.Session id:1117437566  seq no:2
tacp_procpkt_authen: GETPASS
mk_pkt - type: 0x1, session_id: 495
mkpkt_continue - response: ***
 Tacacs packet sent
Sending TACACS Continue message.Session id: 495, seq no:3
Received TACACS packet.Session id:1117437566  seq no:4
tacp_procpkt_authen: PASS
TACACS Session finished.Session id: 495, seq no: 3

mk_pkt - type: 0x2, session_id: 496
mkpkt - authorize user: neo
 Tacacs packet sent
Sending TACACS Authorization message.Session id: 496, seq no:1
Received TACACS packet.Session id:63315798  seq no:2
tacp_procpkt_author: PASS_ADD
tacp_procpkt_author: PASS_REPL
Attributes = priv-lvl
```

```
TACACS Session finished.Session id: 496, seq no: 1

mk_pkt - type: 0x2, session_id: 498
mkpkt - authorize user: neo
cmd=ping
cmd-arg=10.1.1.255  Tacacs packet sent
Sending TACACS Authorization message.Session id: 498, seq no:1
Received TACACS packet.Session id:244563180  seq no:2
tacp_procpkt_author: FAIL
TACACS Session finished.Session id: 498, seq no: 1
...
```

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	Device Port	Remote Address	Matched Command Set	Shell Profile
	All					
neo	Authorization	ASA Regular >> NetOps	22	10.1.100.6	HelpDesk Commands	
neo	Authorization	ASA Regular >> NetOps	0	10.1.100.6		ASA Read Only
neo	Authentication		87	10.1.100.6		
sean	Authorization	ASA Regular >> SecOps	22	10.1.100.6	Permit All Commands	
sean	Authorization	ASA Regular >> SecOps	22	10.1.100.6	Permit All Commands	
sean	Authorization	ASA Regular >> SecOps	0	10.1.100.6		ASA Admin
sean	Authentication		86	10.1.100.6		
hellen	Authorization	ASA Regular >> HelpDesk	22	10.1.100.6		
neo	Authorization	ASDM Authz >> NetOps	443	10.1.100.6	Permit All Commands	

図 17. 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。

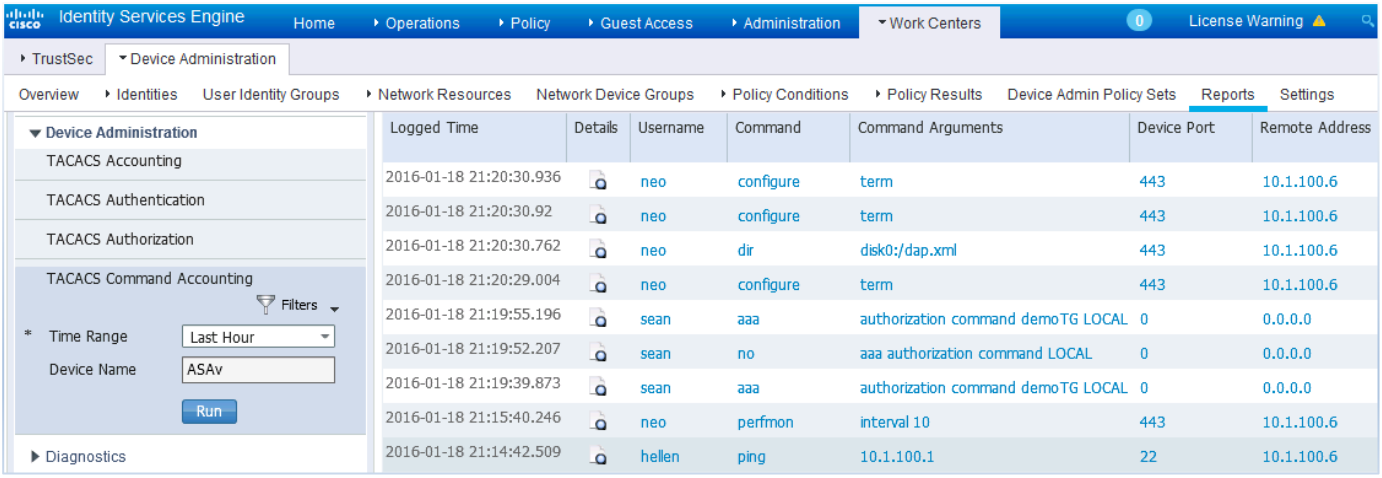

図 18. TACACS レポート