SDM を使用した Cisco IOS ロールベース アクセス コントロール：運用グループごとの個別の構成アクセス権の設定

内容

概要
前提条件
要件
使用するコンポーネント
表記法
背景説明
設定
ユーザとビューの関連付け
パーサービューの設定
SDM CLIビューのサポート
確認
トラブルシュート
関連情報

概要

ルーティングおよびセキュリティ機能は、従来、独立したデバイスでサポートされています。これによって、ネットワーキング インフラストラクチャとセキュリティ サービスの間での管理責任の分離が明確になります。Cisco サービス統合型ルータのセキュリティ機能とルーティング機能のコンバージェンスでは、このようなマルチデバイスにおける明快な分離が提供されません。一部の組織では、機能の境界に沿って顧客またはサービス管理グループを制限するために、設定機能を分離する必要があります。Cisco IOS®ソフトウェア機能のCLIビューは、ロールベースのCLIアクセスを使用してこのニーズに対応することを目指しています。このドキュメントでは、Cisco IOSロールベースアクセスコントロール(RBAC)のSDMサポートによって定義された設定について説明し、Cisco IOSコマンドラインインターフェイス(CLI)からのCLIビューの機能の背景説明を示します。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

ドキュメント表記の詳細については、『シスコ テクニカル ティップスの表記法』を参照してください。

背景説明

多くの組織は、ルーティングとインフラストラクチャのネットワーク運用グループへの接続のメンテナンスと、ファイアウォール、VPN、および侵入防御機能のメンテナンスの責任をセキュリティ運用グループに委任しています。CLIビューを使用すると、セキュリティ機能の設定とモニタリング機能をセキュリティグループに制限し、逆にネットワーク接続、ルーティング、その他のインフラストラクチャ作業をネットグループに制限できます。

一部のサービスプロバイダーは、お客様に限定的な設定やモニタリング機能を提供したいと考えていますが、お客様が他のデバイス設定を設定したり表示したりすることはできません。ここでも、CLIビューはCLI機能を詳細に制御し、ユーザまたはユーザグループが許可されたコマンドのみを実行することを制限します。

Cisco IOSソフトウェアは、ユーザ名またはユーザグループメンバーシップに基づいてCLIコマンドを実行する権限を許可または拒否する権限をTACACS+サーバで制限する機能を提供しています。CLIビューにも同様の機能がありますが、ポリシー制御は、AAAサーバからユーザの指定ビューを受信した後にローカルデバイスによって適用されます。AAAコマンド許可を使用する場合、すべてのコマンドがAAAサーバによって個別に許可される必要があります。これにより、デバイスとAAAサーバ間で頻繁にダイアログが発生します。CLIビューではデバイスごとのCLIポリシー制御が可能ですが、AAAコマンド許可では、ユーザがアクセスするすべてのデバイスに同じコマンド許可ポリシーが適用されます。

設定

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供しています。

注：このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登

録ユーザ専用）を参照してください。一部ツールについては、ゲスト登録のお客様にはアクセスできない場合がありますことをご了承ください。

ユーザとビューの関連付け

ユーザは、AAAからの戻り属性またはローカル認証設定によって、ローカルCLIビューに関連付けることができます。ローカル構成では、ユーザー名に追加の表示オプションが設定され、**設定さ**れたパーサービュー名と一致する**ビューが設**定されます。次のユーザ例は、デフォルトのSDMビュー用に設定されています。

```
username fw-user privilege [privilege-level] view SDM_Firewall
username monitor-user privilege [privilege-level] view SDM_Monitor
username vpn-user privilege [privilege-level] view SDM_EasyVPN_Remote
username sdm-root privilege [privilege-level] view root
```

特定のビューに割り当てられているユーザは、入力するビューのパスワードを持っている場合、一時的に別のビューに切り替えることができます。ビューを変更するには、次のexecコマンドを発行します。

```
enable view view-name
```

パーサービューの設定

CLIビューは、ルータのCLIから、またはSDMから設定できます。「SDM CLIビューのサポート」セクションで説明されているように、SDMは4つのビューを静的にサポートします。コマンドラインインターフェイス(CLI)からCLIビューを設定するには、ユーザをルートビューユーザとして定義する必要があります。または、パーサービューの設定にアクセスできるビューに属している必要があ**り**ます。ビューに関連付けられていないユーザや、ビューを設定しようとするユーザには、次のメッセージが表示されます。

```
router(config#parser view test-view
No view Active! Switch to View Context
```

CLIビューを使用すると、実行モードと構成モードの両方、またはその一部に対して、完全なコマンド階層を含めたり除外したりできます。特定のビューでコマンドまたはコマンド階層を許可または禁止するには、次の3つのオプションを使用できます。

```
router(config-view)#commands configure ?
  exclude            Exclude the command from the view
  include            Add command to the view
  include-exclusive  Include in this view but exclude from others
```

CLIビューは、running-configを切り捨てて、Parser View設定が表示されないようにします。ただし、Parser Viewの設定はstartup-configに表示されます。

ビュー定義の詳細については、「ロールベースのCLIアクセス」を参照してください。

パーサービューの関連付けの確認

Parser Viewに割り当てられたユーザは、ルータにログインしたときに割り当てられるビューを決定できます。**show parser viewコマンドを使用してユ**ーザビューを表示できる場合は、**show parser viewコマンドを発行して表示**を確認できます。

```
router#sh parser view
Current view is 'SDM_Firewall'
```

SDM CLIビューのサポート

SDMには3つのデフォルトビューがあり、ファイアウォールとVPNコンポーネントの設定とモニタリング用に2つのデフォルトビューと、制限されたモニタリング専用ビューが1つあります。SDMでは、追加のデフォルトルートビューも使用できます。

SDMには、各デフォルトビューに含まれるコマンドや各デフォルトビューから除外されるコマンドを変更する機能はなく、追加のビューを定義する機能もありません。CLIから追加のビューが定義されている場合、SDMはUser Accounts/Views構成パネルで追加のビューを提供しません。

次のビューとそれぞれのコマンド権限は、SDM用に事前に定義されています。

SDM_Firewallビュー

```
parser view SDM_Firewall
 secret 5 $1$w/cD$T1ryjKM8aGCnIaKSm.Cx9/
 commands interface include all ip inspect
 commands interface include all ip verify
 commands interface include all ip access-group
 commands interface include ip
 commands interface include description
 commands interface include all no ip inspect
 commands interface include all no ip verify
 commands interface include all no ip access-group
 commands interface include no ip
 commands interface include no description
 commands interface include no
 commands configure include end
 commands configure include all access-list
 commands configure include all ip access-list
 commands configure include all interface
 commands configure include all zone-pair
 commands configure include all zone
 commands configure include all policy-map
 commands configure include all class-map
 commands configure include all parameter-map
 commands configure include all appfw
 commands configure include all ip urlfilter
 commands configure include all ip inspect
 commands configure include all ip port-map
 commands configure include ip cef
 commands configure include ip
 commands configure include all crypto
 commands configure include no end
 commands configure include all no access-list
 commands configure include all no ip access-list
 commands configure include all no interface
 commands configure include all no zone-pair
 commands configure include all no zone
 commands configure include all no policy-map
 commands configure include all no class-map
 commands configure include all no parameter-map
 commands configure include all no appfw
 commands configure include all no ip urlfilter
 commands configure include all no ip inspect
```

```
 commands configure include all no ip port-map
 commands configure include no ip cef
 commands configure include no ip
 commands configure include all no crypto
 commands configure include no
 commands exec include all vlan
 commands exec include dir all-filesystems
 commands exec include dir
 commands exec include crypto ipsec client ezvpn connect
 commands exec include crypto ipsec client ezvpn xauth
 commands exec include crypto ipsec client ezvpn
 commands exec include crypto ipsec client
 commands exec include crypto ipsec
 commands exec include crypto
 commands exec include write memory
 commands exec include write
 commands exec include all ping ip
 commands exec include ping
 commands exec include configure terminal
 commands exec include configure
 commands exec include all show
 commands exec include all debug appfw
 commands exec include all debug ip inspect
 commands exec include debug ip
 commands exec include debug
 commands exec include all clear
```

SDM_EasyVPN_Remoteビュー

```
parser view SDM_EasyVPN_Remote
 secret 5 $1$UnC3$ienYd0L7Q/9xfCNkBQ4Uu.
 commands interface include all crypto
 commands interface include all no crypto
 commands interface include no
 commands configure include end
 commands configure include all access-list
 commands configure include ip radius source-interface
 commands configure include ip radius
 commands configure include all ip nat
 commands configure include ip dns server
 commands configure include ip dns
 commands configure include all interface
 commands configure include all dot1x
 commands configure include all identity policy
 commands configure include identity profile
 commands configure include identity
 commands configure include all ip domain lookup
 commands configure include ip domain
 commands configure include ip
 commands configure include all crypto
 commands configure include all aaa
 commands configure include default end
 commands configure include all default access-list
 commands configure include default ip radius source-interface
 commands configure include default ip radius
 commands configure include all default ip nat
 commands configure include default ip dns server
 commands configure include default ip dns
 commands configure include all default interface
 commands configure include all default dot1x
 commands configure include all default identity policy
 commands configure include default identity profile
 commands configure include default identity
```

```
 commands configure include all default ip domain lookup
 commands configure include default ip domain
 commands configure include default ip
 commands configure include all default crypto
 commands configure include all default aaa
 commands configure include default
 commands configure include no end
 commands configure include all no access-list
 commands configure include no ip radius source-interface
 commands configure include no ip radius
 commands configure include all no ip nat
 commands configure include no ip dns server
 commands configure include no ip dns
 commands configure include all no interface
 commands configure include all no dot1x
 commands configure include all no identity policy
 commands configure include no identity profile
 commands configure include no identity
 commands configure include all no ip domain lookup
 commands configure include no ip domain
 commands configure include no ip
 commands configure include all no crypto
 commands configure include all no aaa
 commands configure include no
 commands exec include dir all-filesystems
 commands exec include dir
 commands exec include crypto ipsec client ezvpn connect
 commands exec include crypto ipsec client ezvpn xauth
 commands exec include crypto ipsec client ezvpn
 commands exec include crypto ipsec client
 commands exec include crypto ipsec
 commands exec include crypto
 commands exec include write memory
 commands exec include write
 commands exec include all ping ip
 commands exec include ping
 commands exec include configure terminal
 commands exec include configure
 commands exec include all show
 commands exec include no
 commands exec include all debug appfw
 commands exec include all debug ip inspect
 commands exec include debug ip
 commands exec include debug
 commands exec include all clear
```

SDM_Monitorビュー

```
parser view SDM_Monitor
 secret 5 $1$RDYW$OABbxSgtx1kOozLlkBeJ9/
 commands configure include end
 commands configure include all interface
 commands configure include no end
 commands configure include all no interface
 commands exec include dir all-filesystems
 commands exec include dir
 commands exec include all crypto ipsec client ezvpn
 commands exec include crypto ipsec client
 commands exec include crypto ipsec
 commands exec include crypto
 commands exec include all ping ip
 commands exec include ping
 commands exec include configure terminal
```

```
commands exec include configure
commands exec include all show
commands exec include all debug appfw
commands exec include all debug ip inspect
commands exec include debug ip
commands exec include debug
commands exec include all clear
```

確認

現在、この設定に使用できる確認手順はありません。

トラブルシュート

現在、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

- ロールベースのCLIアクセス
- テクニカル サポートとドキュメント – Cisco Systems