

Motorola WiNGS 5.X (AP) と ACS バージョン 5.4 の統合の設定例

目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[ACS の設定](#)

[デバイス タイプ](#)

[ネットワーク デバイスおよび AAA クライアント](#)

[ID グループ](#)

[シェル プロファイル](#)

[デバイス認可プロファイル](#)

[Motorola ソリューション WiNG 5.2 設定](#)

[AAA TACACS ポリシー](#)

[AAA TACACS ポリシーの例](#)

[管理ポリシー](#)

[管理ポリシーの例](#)

[確認](#)

[ロール割り当て](#)

[トラブルシューティング](#)

概要

このドキュメントでは、Cisco Secure Access Control Server (ACS) バージョン 5.4 を使用して、Motorola ワイヤレス コントローラおよびアクセス ポイント上で TACACS+ 認証、認可、およびアカウントिंग (AAA) をサポートするのに必要な設定例を紹介します。このドキュメントでは、各ユーザのロールとアクセス権限を決定するために、Motorola のベンダー固有属性と値が ACS のグループに割り当てられています。属性と値は、各グループでイネーブルにされているユーザ定義サービスとプロトコルを使用してグループに割り当てられます。

前提条件

要件

ACS バージョン 5.x が Motorola WiNGS 5.x に接続されている必要があります。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- ACS バージョン 5.4
- WiNGS 5.2

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たものです。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

設定

ACS 設定

デバイス タイプ

次の例に、WiNG 5 デバイスを Cisco Secure ACS バージョン 5.x 上のデバイス タイプとして定義する方法を示します。デバイス タイプを使用すると、デバイスを Cisco Secure ACS バージョン 5.x 内でグループ化でき、デバイス認可ポリシーを定義する際に使用できます。

ACS GUI で、[Network Resources] > [Network Device Groups] > [Device Type] の順に移動し、[Create] をクリックします。

[Name] と [Description] に入力し、[Parent] を選択します。[Submit] をクリックします。

これで、Motorola ソリューション デバイス用の [Network Device Group] が作成されます。

ネットワーク デバイスおよび AAA クライアント

次の例に、WiNG 5 デバイスを Cisco Secure ACS バージョン 5.x 上の AAA クライアントとして追加する方法を示します。

Cisco Secure ACS で、[Network Resources] > [Network Devices and AAA Clients] の順に移動し、[Create] をクリックします。

このワイヤレスコントローラの [Name] を入力し、[Location] を選択します。前のセクションで作成した [Device Type] を割り当て、[TACACS+] チェックボックスをオンにします。[Shared Secret] に入力し、適切な IP アドレス オプションの横にあるオプション ボタンをクリックします。この例では、[IP Range(s) By Mask] が選択され、ワイヤレスコントローラの接続先 IPv4 サブネット (192.168.20.0/24) が定義されています。すべての情報を入力したら、[Submit] をクリックします。

これで、このワイヤレスコントローラが [Network Devices and AAA Clients] として定義されます。

ID グループ

この例では、MotorolaRO および MotorolaRW という名前の 2 つのグループを定義します。MotorolaRO グループに割り当てられたユーザにはモニタ ロールが割り当てられ、Web アクセス権限が付与されます。一方、MotorolaRW グループに割り当てられたユーザにはスーパーユーザ ロールが割り当てられ、すべてのアクセス権限が付与されます。

[Users and Identity Stores] > [Identity Groups] > [Create] の順に移動します。

読み取り専用アクセスグループの [Name] と [Description] を入力し、[Submit] をクリックします。

2 番目のグループを作成します。読み書きアクセスグループの [Name] と [Description] を入力し、[Submit] をクリックします。

これで、2 つの [Identity Groups] が作成されました。

Shell Profiles

次の例に、シェルプロファイルを Cisco Secure ACS バージョン 5.x 上で定義する方法を示します。この例では、MOTO RO および MOTO RW という 2 つのシェルプロファイルを、各管理ユーザが割り当てられるロールとアクセス権限を決定する属性によって定義します。各シェルプロファイルの名前は、TACACS+ AAA ポリシーで定義された TACACS+ 認証サービスの名前と一致する必要があります。

[Policy Elements] > [Authorization and Permissions] > [Device Administration] > [Shell Profiles] に移動します。[Create] をクリックします。

[General] タブで、追加する必要がある TACACS+ サービスとプロトコルを定義します。現在のサービスとプロトコルを使用するか、または独自に作成することもできます。この例では、WiNG 5 デバイスに読み取り専用アクセスを提供するため、MOTO RO という名前でサービスとプロトコルを定義します。

[Common Tasks] タブで、[Maximum Privilege] を [Static] に設定し、値として [1] を選択します。

[Custom Attributes] タブの、[Attribute] フィールドおよび [Attribute Value] フィールドで、ユーザに割り当てられる属性を定義します。この例では、読み取り専用ユーザがモニタ ロールに指定され、Web アクセス権限が付与されます。[Submit] をクリックします。

新しい [Shell Profile] を作成します。[General] タブで、追加する必要がある TACACS+ サービスとプロトコルを定義します。現在のサービスとプロトコルを使用するか、または独自に作成することもできます。この例では、WiNG 5 デバイスに読み書きアクセス権を提供する、MOTO RW という名前のサービスとプロトコルを定義します。

[Common Tasks] タブで、[Maximum Privilege] を [Static] に設定し、値として [1] を選択します。

[Custom Attributes] タブの、[Attribute] フィールドおよび [Attribute Value] フィールドで、ユーザに割り当てられる属性を定義します。この例では、読み書きユーザがスーパーユーザ ロールに指定され、すべてのアクセス権限が付与されます。[Submit] をクリックします。

これで、MOTO RO と MOTO RW という名前のシェル プロファイルが作成されました。

デバイス認可プロファイル

次の例に、Cisco Secure ACS バージョン 5.x 上でデバイス認可ポリシーを定義する方法を示します。デバイス認可ポリシーは、各管理ユーザが割り当てられるシェル プロファイルを、認証、場所、および ID グループ メンバーシップを要求するデバイス タイプに基づいて決定します。この例では、MotorolaRO および MotorolaRW という名前の 2 つのデバイス認可ポリシーを定義します。

Cisco Secure ACS で、[Access Policies] > [Default Device Admin] > [Authorization] > [Customize] の順に移動します。

[Identity Group]、[NDG: Location]、[NDG: Device Type]、および [Protocol] という名前の [Customize Conditions] を追加します。[Customize Results] の下に [Shell Profile] を追加し、[OK] をクリックします。

[Create] をクリックします。[Name] フィールドに、「MotorolaRO」と入力し、[Identity Group]、[NDG: Location]、および [NDG: Device Type] を選択します。[Protocol] を [Tacacs] に設定し、[MOTO RO] という名前の [Shell Profile] を選択します。[OK] をクリックします。

[Create] をクリックします。[Name] フィールドに、「MotorolaRW」と入力し、[Identity Group]、[NDG: Location]、および [NDG: Device Type] を選択します。[Protocol] を [Tacacs] に設定し、[MOTO RW] という名前の [Shell Profile] を選択します。[OK] をクリックします。

これで、MotorolaRO および MotorolaRW という名前のデバイス認可ポリシーが作成されました。

Motorola ソリューション WiNG 5.2 設定

AAA TACACS ポリシー

AAA TACACS ポリシーは、WiNG 5 デバイス上に TACACS+ クライアント設定を定義します。それぞれの AAA TACACS ポリシーには、Cisco Secure ACS で定義された TACACS+ 認証サービスおよびプロトコルの名前に加えて、2 つまでの TACACS+ AAA サーバ エントリを登録できます。TACACS+ AAA ポリシーは、アカウントिंग サーバに転送される情報も決定します。

この AAA TACACS ポリシー例では、TACACS+ AAA 用に Cisco Secure ACS を定義し、MOTO RO および MOTO RW という名前の TACACS+ サービスおよびプロトコルを定義して、CLI コマンドとセッション アカウントिंगを有効にします。

AAA TACACS ポリシーの例

```
aaa-tacacs-policy CISCO-ACS-SERVER

authentication server 1 host 192.168.10.21 secret 0 hellomoto

authorization server 1 host 192.168.10.21 secret 0 hellomoto
```

```
accounting server 1 host 192.168.10.21 secret 0 hellomoto
authentication service MOTO protocol RO
authentication service MOTO protocol RW
accounting commands
accounting session
!
```

管理ポリシー

AAA TACACS+ ポリシーを定義したら、TACACS+ を使用する前に、それを1つ以上の管理ポリシーに割り当てる必要があります。マネジメントポリシーは、各 WiNG 5 デバイスでイネーブルにされる管理インターフェイス、ローカル管理ユーザ、ロール、アクセス権限、および管理ユーザの認証に使用される外部 RADIUS または TACACS+ サーバを決定します。

デフォルトで、各 WiNG 5 デバイスは、「default」という名前の管理ポリシーに割り当てられます。これはプロファイルを使用して割り当てられます。TACACS+ は、デフォルトの管理ポリシーでも、ユーザ定義の管理ポリシーでも有効にできます。

最も一般的な導入では、ワイヤレスコントローラとアクセスポイント用にそれぞれ別個の管理ポリシーが設定されます。デバイスごとに管理上の要件やインターフェイスが異なるため、別個の管理ポリシーを設定するようにお勧めします。この例では、TACACS+ をワイヤレスコントローラとアクセスポイントの両方で有効にするため、TACACS+ をそれぞれの管理ポリシーで有効にする必要があります。

次のセクションの管理ポリシー例では、ワイヤレスコントローラとアクセスポイントに割り当てられたユーザ定義の管理ポリシー上で TACACS+ AAA を有効にします。認証用に定義された TACACS+ サーバに WiNG 5 デバイスがアクセスできない場合、ローカル認証に対する TACACS+ フォールバックも有効になります。

管理ポリシーの例

```
!
management-policy CONTROLLER-MANAGEMENT
no http server
https server
ssh
user admin password 0 hellomoto role superuser access all
snmp-server user snmptrap v3 encrypted des auth md5 0 hellomoto
snmp-server user snmpoperator v3 encrypted des auth md5 0 hellomoto
snmp-server user snmpmanager v3 encrypted des auth md5 0 hellomoto
aaa-login tacacs fallback
```

```
aaa-login tacacs authorization
aaa-login tacacs accounting
aaa-login tacacs policy CISCO-ACS-SERVER
!
!
management-policy AP-MANAGEMENT
ssh
user admin password 0 hellomoto role superuser access all
aaa-login tacacs fallback
aaa-login tacacs authorization
aaa-login tacacs accounting
aaa-login tacacs policy CISCO-ACS-SERVER
!
```

確認

このセクションでは、TACACS+ AAA を検証するために必要な手順を説明します。この例では、各 Cisco Secure ACS 上で 2 つのユーザ アカウントが定義され、適切なグループに割り当てられます。ユーザのグループ メンバーシップは、その管理ユーザに割り当てられるロールとアクセス権限を決定します。

Username	Role	Access Permissions
monitor	Monitor	Web
super	user	Superuser all

ロール割り当て

このセクションでは、認証およびロール割り当てを検証するために必要な検証手順を説明します。

Web UI で、「monitor」のユーザ名とパスワードを使用して、ワイヤレス コントローラにログインします。

ユーザの認証と承認、モニタ ロールへの割り当てが実行され、ワイヤレス コントローラに対する読み取り専用アクセスが提供されます。[Configuration] > [Devices] の順に選択し、デバイスの変更を試行します。

注: このユーザには読み取りアクセスのみが許可されているため、編集機能は使用できません。

デバイスに対するアクセス：（ [View] ボタンのみ使用可。 [Delete] ボタンはグレー表示 ）

Web UI で、「superuser」のユーザ名とパスワードを使用して、ワイヤレスコントローラにログインします。

ユーザの認証と承認、スーパーユーザロールへの割り当てが実行され、ワイヤレスコントローラに対するフルアクセスが提供されます。[Configuration] > [Devices] の順に選択し、デバイスの変更を試行します。

注: このユーザにはデバイスに対するフルアクセスが許可されているため、今回は [Edit] ボタンが使用できません。

トラブルシューティング

Cisco Secure ACS バージョン 5.X で、[Monitoring and Reports] > [Launch Monitoring & Report Viewer] > [Select Reports] > [Catalog] > [AAA Protocol] > [TACACS Authentication] > [Run] の順に移動します。

これで、ユーザ認証の成功と失敗の結果すべてが、失敗の原因を含めて表示されます。詳細を表示するには、虫めがね (詳細) ボタンをクリックします。