さまざまなシスコおよびシスコ以外のデバイスの TACACS+ および RADIUS 属性の設定例

目次

概要

このドキュメントでは、さまざまなシスコおよびシスコ以外の製品が認証、認可、アカウンティング（AAA）サーバから受信する属性をまとめています。 この場合、AAA サーバは、Access Control Server（ACS）です。 ACS は、これらの属性をシェル プロファイル（TACACS+）または許可プロファイル（RADIUS）の一部として Access-Accept とともに送信できます。

このドキュメントでは、カスタム属性をシェル プロファイルおよび許可プロファイルに追加する方法の詳細な手順について説明します。 また、デバイスおよびデバイスに AAA サーバから返される TACACS+ および RADIUS 属性のリストを提供します。 これらにはすべて例が示されます。

このドキュメントで提供される属性のリストは、完全または正式なものではなく、このドキュメントを更新せずに変更される可能性があります。

前提条件

要件

このドキュメントに関する固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情報は、ACS バージョン 5.2/5.3 に基づくものです。

表記法

ドキュメント表記の詳細は、『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。

シェル プロファイルの作成（TACACS+）

シェル プロファイルは、TACACS+ ベース アクセスの基本許可コンテナです。 TACACS+ が帰因させる属性値は Cisco ® IOS 特権レベル、セッション タイムアウトおよび他のパラメータに加えて Access-Accept と、戻す必要があります規定でき。

カスタム属性を新しいシェル プロファイルに追加するには、次のコマンドを入力します。

1. ACS インターフェイスにログインします。
2. [Policy Elements] > [Authorization and Permissions] > [Device Administration] > [Shell Profiles] に移動します。
3. [Create] ボタンをクリックします。
4. シェル プロファイルに名前を付けます。
5. [Custom Attributes] タブをクリックします。
6. 属性名を [Attribute] フィールドに入力します。
7. [Requirement] ドロップダウン リストから [Mandatory] または [Optional] を選択します。
8. 属性値のドロップダウンを [Static] の設定のままにします。 値がスタティックの場合、次のフィールドに値を入力できます。 値がダイナミックの場合、手動では属性を入力できません。 その代わり、属性はいずれかのアイデンティティ ストアの属性にマップされます。
9. 最後のフィールドに属性の値を入力します。
10. [Add] ボタンをクリックして、テーブルにエントリを追加します。
11. 必要なすべての属性について設定を繰り返します。
12. 画面下部の [Submit] ボタンをクリックします。

設定例

デバイス： Application Control Engine（ACE）

[Attribute]： `<context-name>`

Value `<Role-name> <domain-name1>`

使用方法： ロールとドメインは空白文字で区切られます。 ユーザ（例：USER1）がコンテキスト（例：C1）にログインしたときに、ロール（例：ADMIN）とドメイン（例：MYDOMAIN）が

ユーザに割り当てられるように設定できます。

許可プロファイルの作成（RADIUS）

許可プロファイルは、RADIUS ベース アクセスの基本許可コンテナです。 VLAN、Access Control List（ACL）およびその他のパラメータのほか、Access-Accept と返される RADIUS 属性および属性値を指定できます。

カスタム属性を新しい許可プロファイルに追加するには、次のコマンドを入力します。

1. ACS インターフェイスにログインします。
2. [Policy Elements] > [Authorization and Permissions] > [Network Access] > [Authorization Profiles] に移動します。
3. [Create] ボタンをクリックします。
4. 許可プロファイルに名前を付けます。
5. [RADIUS Attributes] タブをクリックします。
6. [Dictionary Type] ドロップダウン メニューからディクショナリを選択します。
7. [RADIUS Attribute] フィールドで属性を選択するには、[Select] ボタンをクリックします。 新しいウィンドウが表示されます。
8. 使用可能な属性を確認し、選択して、[OK] をクリックします。 [Attribute Type] の値は、デフォルトで、選択した属性に基づいて、設定されます。
9. 属性値のドロップダウンを [Static] の設定のままにします。 値がスタティックの場合、次のフィールドに値を入力できます。 値がダイナミックの場合、手動では属性を入力できません。 その代わり、属性はいずれかのアイデンティティ ストアの属性にマップされます。
10. 最後のフィールドに属性の値を入力します。
11. [Add] ボタンをクリックして、テーブルにエントリを追加します。
12. 必要なすべての属性について設定を繰り返します。
13. 画面下部の [Submit] ボタンをクリックします。

設定例

デバイス： ACE

[Attribute]： `cisco-av-pair`

Value `<context-name>=<Role-name> <domain-name1> <domain-name2>`

使用方法： 等号記号の後の値はそれぞれ空白文字で区切られます。 ユーザ（例：USER1）がコンテキスト（例：C1）にログインしたときに、ロール（例：ADMIN）とドメイン（例：MYDOMAIN）がユーザに割り当てられるように設定できます。

デバイス リスト

アグリゲーション サービス ルータ（ASR）

RADIUS（許可プロファイル）

[Attribute]： `cisco-av-pair`

Value `tasks= " #<role-name><permission>: <process>`

使用方法： <role-name> の値を、ルータでローカルに定義されているロールの名前に設定します。 ロール階層は、ツリーです。ルール #root はツリーのトップにあり、ロール #leaf はコマンドを追加します。 これらの 2 つのロールは、 `tasks= " #root#leaf`。

個々のプロセスに基づいて許可を返すことができるので、特定のプロセスの読み取り、書き込み、実行権限をユーザに付与できます。 たとえば、bgp プロセスの読み取りおよび書き込み権限をユーザに付与するには、値を `tasks= " #rootrw: bgp`。 属性の順序は任意です。 結果は値がに設定 されるかどうか同じです: `tasks= " #rootrw: bgp`または ro : `tasks= " rw: bgp#root`。

例：許可プロファイルへの属性の追加

Dictionary Type	RADIUS Attribute	Attribute Type	Attribute Value
RADIUS-Cisco	`cisco-av-pair`	String	`shell:tasks="#root,#leaf,rwx:bgp,r:ospf"`

Application Control Engine (ACE)

TACACS+ (シェル プロファイル)

[Attribute]： `<context-name>`

Value `<Role-name> <domain-name1>`

使用方法： ロールとドメインは空白文字で区切られます。 ユーザ (例：USER1) がコンテキスト (例：C1) にログインしたときに、ロール (例：ADMIN) とドメイン (例：MYDOMAIN) がユーザに割り当てられるように設定できます。

例：属性のシェル プロファイルへの追加

Attribute	Requirement	Attribute Value
`shell:C1`	Mandatory	`Admin MYDOMAIN`

USER1 が C1 コンテキストを介してログインすると、このユーザには ADMIN ロールおよび MYDOMAIN ドメインが自動的に割り当てられます (USER1 がログインすると、この許可プロファイルが割り当てられるように許可ルールが設定されている場合)。

ACS が送り返す属性の値で返されない別のコンテキストから USER1 がログインした場合、そのユーザには自動的にデフォルトのロール (Network-Monitor) とデフォルトのドメイン (default-domain) が割り当てられます。

RADIUS (許可プロファイル)

[Attribute]： `cisco-av-pair`

Value `<context-name>=<Role-name> <domain-name1> <domain-name2>`

使用方法： 等号記号の後の値はそれぞれ空白文字で区切られます。 ユーザ (例：USER1) がコンテキスト (例：C1) にログインしたときに、ロール (例：ADMIN) とドメイン (例：MYDOMAIN) がユーザに割り当てられるように設定できます。

例：許可プロファイルへの属性の追加

Dictionary Type	RADIUS Attribute	Attribute Type	Attribute Value
RADIUS-Cisco	`cisco-av-pair`	String	`shell:C1=ADMIN MYDOMAIN`

USER1 が C1 コンテキストを介してログインすると、このユーザには ADMIN ロールおよび MYDOMAIN ドメインが自動的に割り当てられます（USER1 がログインすると、この許可プロファイルが割り当てられるように許可ルールが設定されている場合）。

ACS が送り返す属性の値で返されない別のコンテキストから USER1 がログインした場合、そのユーザには自動的にデフォルトのロール（Network-Monitor）とデフォルトのドメイン（default-domain）が割り当てられます。

BlueCoat パケット シェーパ

RADIUS（許可プロファイル）

[Attribute]： `Packeteer-AVPair`

Value `access=<level>`

使用方法： <level> は、付与するアクセスのレベルです。 touch アクセスは読み取りおよび書き込みと同じで、look アクセスは読み取り専用と同じです。

BlueCoat VSA は、デフォルトでは、ACS ディクショナリにはありません。 許可プロファイルの BlueCoat 属性を使用するには、BlueCoat ディクショナリを作成して、BlueCoat 属性をそのディクショナリに追加する必要があります。

ディクショナリを作成します。

1. **システム 管理 > 設定 > 辞書 > プロトコル > RADIUS > RADIUS VSA** へのナビゲート。
2. [Create] をクリックします。
3. ディクショナリの詳細を入力します。[Name]： BlueCoat[Vendor ID]： 2334[Attribute Prefix]： Packeteer-
4. [Submit] をクリックします。

新しいディクショナリ内の属性を作成します。

1. **システム 管理 > 設定 > 辞書 > プロトコル > RADIU** へのナビゲート S > **RADIUS VSA > BlueCoat**。
2. [Create] をクリックします。
3. 属性の詳細を入力します。[Attribute]： `Packeteer-AVPair`[Description]： Used in order to specify access level[Vendor Attribute ID]： 1[Direction]： OUTBOUND[Multiple Allowed]： False[Include attribute in log]： オン[Attribute Type]： String
4. [Submit] をクリックします。

例：許可プロファイルへの属性の追加（読み取り専用アクセス）

Dictionary Type	RADIUS Attribute	Attribute Type	Attribute Value
RADIUS-	`Packeteer-AVPair`	String	`access=look`

BlueCoat			

例：*許可プロファイルへの属性の追加（読み取りおよび書き込みアクセス）*

Dictionary Type	RADIUS Attribute	Attribute Type	Attribute Value
RADIUS-BlueCoat	`Packeteer-AVPair`	String	`access=touch`

Brocade スイッチ

RADIUS（許可プロファイル）

[Attribute]： `Tunnel-Private-Group-ID`

Value U:<VLAN1>; `T:<VLAN2>`

使用方法： <VLAN1> をデータ VLAN の値に設定します。 <VLAN2> を音声 VLAN の値に設定します。 この例では、データ VLAN は VLAN 10 で、音声 VLAN は VLAN 21 です。

例：*許可プロファイルへの属性の追加*

Dictionary Type	RADIUS Attribute	Attribute Type	Attribute Value
RADIUS-IETF	`Tunnel-Private-Group-ID`	Tagged String	`U:10;T:21`

Cisco Unity Express（CUE）

RADIUS（許可プロファイル）

[Attribute]： `cisco-av-pair`

Value `fndn: groups=<group >`

使用方法： <group-name> は、ユーザに認可する権限を含むグループの名前です。 このグループは、Cisco Unity Express（CUE）で設定する必要があります。

例：*許可プロファイルへの属性の追加*

Dictionary Type	RADIUS Attribute	Attribute Type	Attribute Value
RADIUS-Cisco	`cisco-av-pair`	String	`fndn:groups=Administrators`

Infoblox

RADIUS（許可プロファイル）

[Attribute]： `Infoblox-Group-Info`

Value `<group >`

使用方法： <group-name> は、ユーザに認可する権限を含むグループの名前です。 このグループは、Infoblox デバイスで設定する必要があります。 この設定例では、グループ名は MyGroup です。

Infoblox VSA は、デフォルトでは、ACS ディクショナリにはありません。 許可プロファイルの Infoblox 属性を使用するには、Infoblox ディクショナリを作成して、Infoblox 属性をそのディクショナリに追加する必要があります。

ディクショナリを作成します。

1. **システム 管理 > 設定 > 辞書 > プロトコル > RADIUS > RADIUS VSA** へのナビゲート。
2. [Create] をクリックします。
3. [Use Advanced Vendor Options] の横にある小さい矢印をクリックします。
4. ディクショナリの詳細を入力します。[Name]： Infoblox[Vendor ID]： 7779[Vendor Length Field Size]： 1[Vendor Type Field Size]： 1
5. [Submit] をクリックします。

新しいディクショナリ内の属性を作成します。

1. **システム 管理 > 設定 > 辞書 > プロトコル > RADIUS > RADIUS** へのナビゲート **VSA > Infoblox**。
2. [Create] をクリックします。
3. 属性の詳細を入力します。[Attribute]： `Infoblox-Group-Info`[Vendor Attribute ID]： 009[Direction]： OUTBOUND[Multiple Allowed]： False[Include attribute in log]： オン [Attribute Type]： String
4. [Submit] をクリックします。

例：許可プロファイルへの属性の追加

Dictionary Type	RADIUS Attribute	Attribute Type	Attribute Value
RADIUS-Infoblox	`Infoblox-Group-Info`	String	`MyGroup`

侵入防御システム（IPS）

RADIUS（許可プロファイル）

[Attribute]： `ips-role`

Value `<role name>`

使用方法： 値 <role name> は、4 つの Intrusion Prevention System（IPS）ユーザ ロール、viewer、operator、administrator、service のいずれかです。 各ユーザ ロール タイプに付与される権限の詳細については、使用しているバージョンの IPS の設定ガイドを参照してください。

- Cisco Intrusion Prevention System Device Manager コンフィギュレーション ガイド（IPS 7.0）
- IPS 7.1 のための Cisco 侵入防御システム デバイスマネージャ コンフィギュレーション ガイド

例：許可プロファイルへの属性の追加

Dictionary	RADIUS	Attribut	Attribute Value

Type	Attribute	e Type	
RADIUS-Cisco	cisco-av-pair	String	ips-role:administrator

Juniper

TACACS+ (シェル プロファイル)

[Attribute]： allow-commands ; allow-configuration ; local-user-name ; deny-commands ; deny-configuration; user-permissions

Value <allow-commands-regex> ; <allow-configuration-regex> ; <local-username> ; <deny-commands-regex> ; <deny-configuration-regex>

使用方法： <local-username> の値 (つまり、local-user-name 属性の値) を Juniper デバイスのローカルにあるユーザ名に設定します。 たとえば、local-user-name 属性の値を JUSER に設定する場合、Juniper デバイスのローカルに存在するユーザ (例：JUSER) と同じユーザ テンプレートを割り当てるユーザ (例：USER1) を設定できます。 allow-commands、allow-configuration、deny-commands および deny-configuration 属性の値は、正規表現形式で入力できます。 ユーザのログイン クラス権限ビットで許可されるオペレーショナル/コンフィギュレーション モード コマンドのほか、次の属性の値が設定されます。

例：シェル プロファイル 1 への属性の追加

Attribute	Requirement	Attribute Value
allow-commands	Optional	"(request system) | (show rip neighbor)"
allow-configuration	Optional	
local-user-name	Optional	sales
deny-commands	Optional	"<^clear"
deny-configuration	Optional	

例–シェル プロファイル 2 に属性を追加して下さい

Attribute	Requirement	Attribute Value
allow-commands	Optional	"monitor | help | show | ping | traceroute"
allow-configuration	Optional	
local-user-name	Optional	engineering
deny-commands	Optional	"configure"
deny-configuration	Optional	

Nexus スイッチ

RADIUS (許可プロファイル)

[Attribute]： `cisco-av-pair`

Value `shell:roles="<role1> <role2>" "`

使用方法： role<1> および <role2> の値を、スイッチでローカルに定義されているロールの名前に設定します。 複数のロールを追加する場合、空白で区切ります。 複数のロールが AAA サーバから Nexus スイッチに返されると、ユーザは、3 つのロールすべてで定義されるコマンドにアクセスできます。

組み込みロールは、「ユーザ アカウントと RBAC の設定」で定義されます。

例：許可プロファイルへの属性の追加

Dictionary Type	RADIUS Attribute	Attribute Type	Attribute Value
RADIUS-Cisco	`cisco-av-pair`	String	`shell:roles="network-admin vdc-admin vdc-operator"`

Riverbed

TACACS+ (シェル プロファイル)

[Attribute]： service ; `local-user-name`

Value rbt-exec ; **`<username>`**

使用方法： ユーザに読み取り専用アクセスを付与する場合、<username> 値を monitor に設定する必要があります。 <ユーザに読み取りおよび書き込みアクセスを付与する場合、>username 値を admin に設定する必要があります。 admin および monitor の他に別のアカウントを定義する場合、返される名前を設定します。

例：シェル プロファイルへの属性の追加 (読み取り専用アクセス)

Attribute	Requirement	Attribute Value
`service`	Mandatory	`rbt-exec`
`local-user-name`	Mandatory	`monitor`

例：シェル プロファイルへの属性の追加 (読み取りおよび書き込みアクセス)

Attribute	Requirement	Attribute Value
`service`	Mandatory	`rbt-exec`
`local-user-name`	Mandatory	`admin`

ワイヤレス LAN コントローラ (WLC)

RADIUS (許可プロファイル)

[Attribute]： `Service-Type`

Value Administrative (6)/ NAS-Prompt (7))

使用方法： ワイヤレス LAN コントローラ（WLC）への読み取り/書き込みアクセスをユーザに付与するには、値を Administrative に設定する必要があります。 読み取り専用アクセスの場合、値を NAS-Prompt に設定する必要があります。

詳細については、「ワイヤレス LAN コントローラ（WLC）での管理ユーザの RADIUS サーバ認証の設定例」を参照してください。

例：許可プロファイルへの属性の追加（読み取り専用アクセス）

Dictionary Type	RADIUS Attribute	Attribute Type	Attribute Value
RADIUS-IETF	`Service-Type`	Enumeration	`NAS-Prompt`

例：許可プロファイルへの属性の追加（読み取りおよび書き込みアクセス）

Dictionary Type	RADIUS Attribute	Attribute Type	Attribute Value
RADIUS-IETF	`Service-Type`	Enumeration	`Administrative`

Data Center Network Manager（DCNM）

認証方式を変更した場合、DCNM を再起動する必要があります。 再起動しない場合、network-admin 権限ではなく、network-operator 権限が割り当てられることがあります。

DCNM Role	RADIUS Cisco-AV-Pair	Tacacs Cisco-AV-Pair
User	`shell:roles = "network-operator"`	`cisco-av-pair=shell:roles="network-operator"`
Administrator	`shell:roles = "network-admin"`	`cisco-av-pair=shell:roles="network-admin"`

関連情報

- テクニカルサポートとドキュメント - Cisco Systems
- Terminal Access Controller Access Control System（TACACS+）
- Remote Authentication Dial-In User Service（RADIUS）
- Requests for Comments（RFC）