Konfigurationsbeispiel für TACACS+- und RADIUS-Attribute für verschiedene Geräte von Cisco und anderen Anbietern

Inhalt

Einführung

Dieses Dokument enthält eine Zusammenstellung von Attributen, die verschiedene Produkte von Cisco und anderen Anbietern von einem AAA-Server (Authentication, Authorization, Accounting) erwarten. In diesem Fall ist der AAA-Server ein Zugriffssteuerungsserver (Access Control Server, ACS). Der ACS kann diese Attribute zusammen mit einem Access-Accept als Teil eines Shell-Profils (TACACS+) oder Autorisierungsprofils (RADIUS) zurückgeben.

Dieses Dokument enthält schrittweise Anweisungen zum Hinzufügen benutzerdefinierter Attribute zu Shell-Profilen und Autorisierungsprofilen. Dieses Dokument enthält außerdem eine Liste der Geräte sowie die TACACS+- und RADIUS-Attribute, die Geräte voraussichtlich vom AAA-Server zurückgeben. Alle Themen enthalten Beispiele.

Die Liste der in diesem Dokument enthaltenen Attribute ist weder vollständig noch autoritär und kann jederzeit ohne Aktualisierung dieses Dokuments geändert werden.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf der ACS-Version 5.2/5.3.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Erstellen eines Shell-Profils (TACACS+)

Ein Shell-Profil ist ein einfacher Berechtigungscontainer für TACACS+-basierten Zugriff. Sie können festlegen, welche TACACS+-Attribute und Attributwerte mit Access-Accept zusätzlich zu der Cisco® IOS-Berechtigungsebene, dem Sitzungs-Timeout und anderen Parametern zurückgegeben werden sollen.

Gehen Sie wie folgt vor, um einem neuen Shell-Profil benutzerdefinierte Attribute hinzuzufügen:

1. Melden Sie sich bei der ACS-Schnittstelle an.
2. Navigieren Sie zu **Richtlinienelemente > Autorisierung und Berechtigungen > Geräteverwaltung > Shell-Profile**.
3. Klicken Sie auf die Schaltfläche **Erstellen**.
4. Nennen Sie das Shell-Profil.
5. Klicken Sie auf die Registerkarte **Benutzerdefinierte Attribute**.
6. Geben Sie den Attributnamen im Feld **Attribut ein**.
7. Wählen Sie aus der Dropdown-Liste **Anforderung** aus, ob die Anforderung **obligatorisch** oder **optional** ist.
8. Lassen Sie das Dropdown-Menü für den Attributwert auf **Statisch**. Wenn der Wert statisch ist, können Sie den Wert im nächsten Feld eingeben. Wenn der Wert dynamisch ist, können Sie das Attribut nicht manuell eingeben. Stattdessen wird das attributierte Attribut einem Attribut in einem der Identitätsdatenspeicher zugeordnet.
9. Geben Sie den Wert des Attributs im letzten Feld ein.
10. Klicken Sie auf die Schaltfläche **Hinzufügen**, um den Eintrag der Tabelle hinzuzufügen.
11. Wiederholen, um alle erforderlichen Attribute zu konfigurieren.
12. Klicken Sie unten im Bildschirm auf die Schaltfläche **Submit** (Senden).

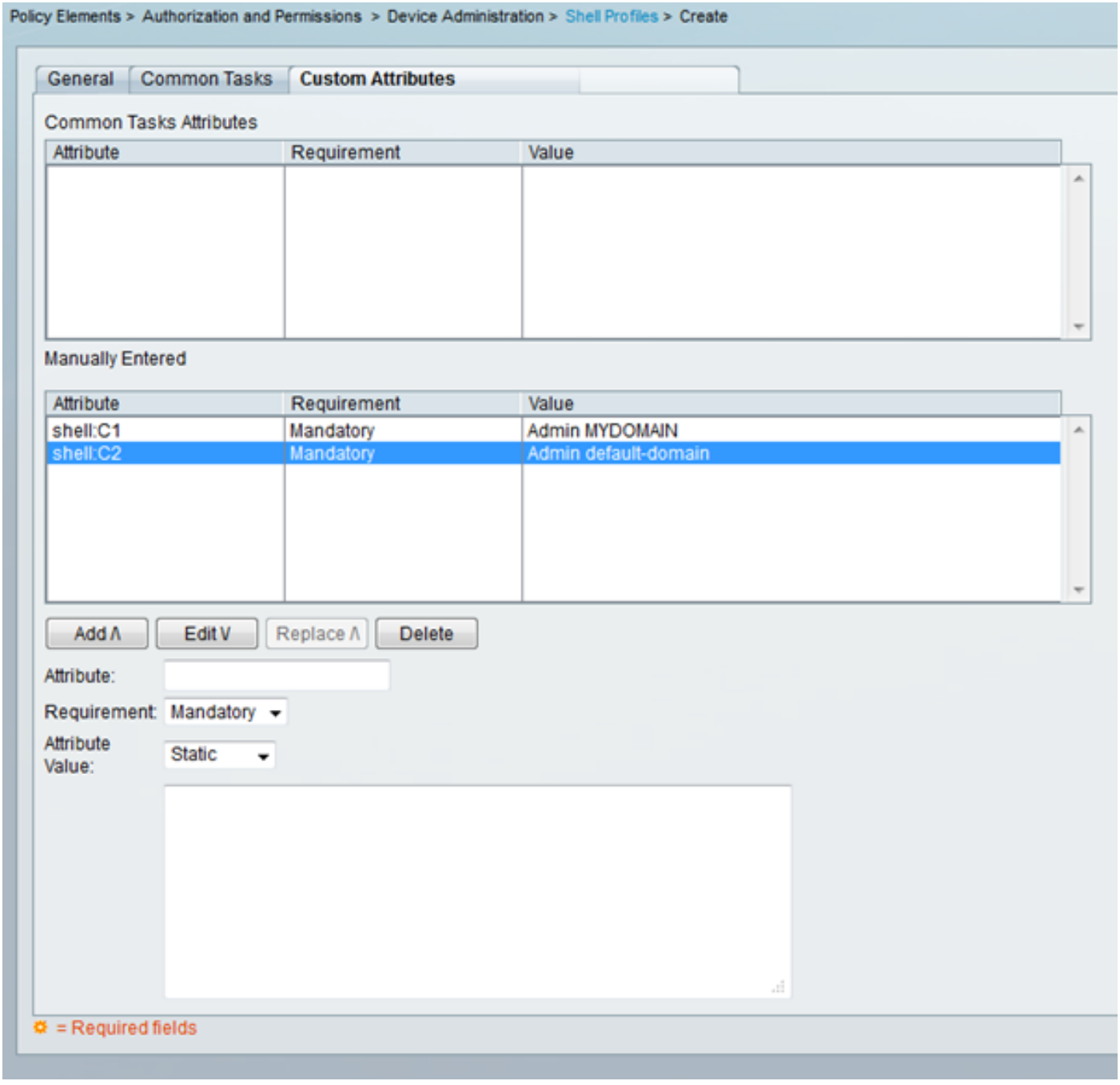
Konfigurationsbeispiel

Gerät: Application Control Engine (ACE)

Attribut(e): `shell:<context-name>`

Wert(e): `<Name der Rolle> <Domänenname1>`

Verwendung: Rolle und Domäne werden durch ein Leerzeichen getrennt. Sie können einen Benutzer (z. B. USER1) so konfigurieren, dass ihm eine Rolle (z. B. ADMIN) und eine Domäne (z. B. MYDOMAIN) zugewiesen wird, wenn sich der Benutzer bei einem Kontext anmeldet (z. B. C1).



Erstellen eines Autorisierungsprofils (RADIUS)

Ein Autorisierungsprofil ist ein Standardberechtigungscontainer für RADIUS-basierten Zugriff. Sie können festlegen, welche RADIUS-Attribute und Attributwerte mit Access-Accept zusätzlich zu den VLANs, Zugriffskontrolllisten (ACLs) und anderen Parametern zurückgegeben werden sollen.

Gehen Sie wie folgt vor, um einem neuen Autorisierungsprofil benutzerdefinierte Attribute hinzuzufügen:

1. Melden Sie sich bei der ACS-Schnittstelle an.
2. Navigieren Sie zu **Richtlinienelemente > Autorisierung und Berechtigungen > Netzwerkzugriff > Autorisierungsprofile**.
3. Klicken Sie auf die Schaltfläche **Erstellen**.
4. Nennen Sie das Autorisierungsprofil.
5. Klicken Sie auf die Registerkarte **RADIUS-Attribute**.
6. Wählen Sie aus dem Dropdown-Menü **Dictionary Type** ein Wörterbuch aus.
7. Um das Attribut für das RADIUS-Attribut festzulegen, klicken Sie auf die Schaltfläche **Auswählen**. Ein neues Fenster wird angezeigt.
8. Überprüfen Sie die verfügbaren Attribute, treffen Sie eine Auswahl, und klicken Sie auf **OK**. Der **Attributtyp-**Wert wird standardmäßig auf der Grundlage der gerade vorgenommenen Attributauswahl festgelegt.
9. Lassen Sie das Dropdown-Menü für den Attributwert auf **Statisch**. Wenn der Wert statisch ist, können Sie den Wert im nächsten Feld eingeben. Wenn der Wert dynamisch ist, können Sie das Attribut nicht manuell eingeben. Stattdessen wird das attributierte Attribut einem Attribut in einem der Identitätsdatenspeicher zugeordnet.
10. Geben Sie den Wert des Attributs im letzten Feld ein.
11. Klicken Sie auf die Schaltfläche **Hinzufügen**, um den Eintrag der Tabelle hinzuzufügen.
12. Wiederholen, um alle erforderlichen Attribute zu konfigurieren.
13. Klicken Sie unten im Bildschirm auf die Schaltfläche **Submit** (Senden).

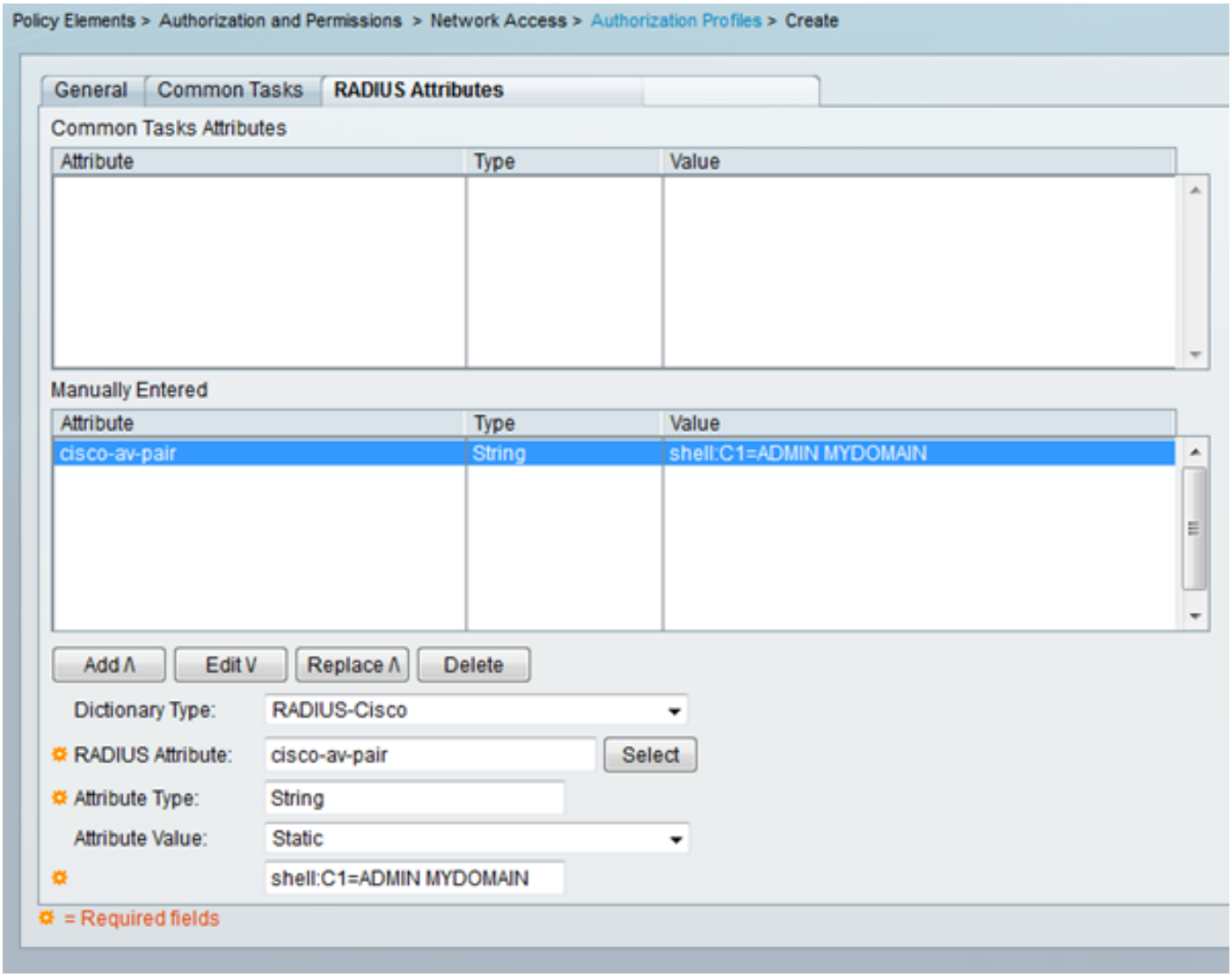
Konfigurationsbeispiel

Gerät: ACE

Attribut(e): `cisco-av-pair`

Wert(e): `shell:<context-name>=<Role-name> <domain-name1> <domain-name2>`

Verwendung: Jeder Wert nach dem Gleichheitszeichen wird durch ein Leerzeichen getrennt. Sie können einen Benutzer (z. B. USER1) so konfigurieren, dass ihm eine Rolle (z. B. ADMIN) und eine Domäne (z. B. MYDOMAIN) zugewiesen wird, wenn sich der Benutzer bei einem Kontext anmeldet (z. B. C1).



Geräteliste

Aggregation Services Router (ASR)

RADIUS (Authorization Profile)

Attribut(e): `cisco-av-pair`

Wert(e): `shell:tasks="#<role-name>,<permit>:<prozess>"`

Verwendung: Legen Sie die Werte von `<Rollenname>` auf den Namen einer lokal auf dem Router definierten Rolle fest. Die Rollenhierarchie lässt sich anhand einer Struktur beschreiben, in der die Rolle `#root` oben in der Struktur und die Rolle `#leaf` zusätzliche Befehle hinzufügt. Diese beiden Rollen können kombiniert und zurückgegeben werden, wenn: `shell:tasks="#root,#leaf"`.

Berechtigungen können auch auf Basis einzelner Prozesse zurückgegeben werden, sodass einem Benutzer Lese-, Schreib- und Ausführungsrechte für bestimmte Prozesse gewährt werden können. Um einem Benutzer beispielsweise Lese- und Schreibrechte für den BGP-Prozess zu gewähren, legen Sie den Wert auf: `shell:tasks="#root,rw:bgp"`. Die Reihenfolge der Attribute spielt keine Rolle. Das Ergebnis ist dasselbe, ob der Wert auf `shell:tasks="#root,rw:bgp"` oder ro `shell:tasks="rw:bgp,#root"` festgelegt ist.

Beispiel: *Hinzufügen des Attributs zu einem Autorisierungsprofil*

Wörterbuchtyp	RADIUS-Attribut	Attributtyp	Attributwert
RADIUS-Cisco	`cisco-av-pair`	Zeichenfolge	`shell:tasks="#root,#leaf, rwx:bgp,r:ospf"`

Application Control Engine (ACE)

TACACS+ (Shell-Profil)

Attribut(e): `shell:<context-name>`

Wert(e): `<Name der Rolle> <Domänenname1>`

Verwendung: Rolle und Domäne werden durch ein Leerzeichen getrennt. Sie können einen Benutzer (z. B. USER1) so konfigurieren, dass ihm eine Rolle (z. B. ADMIN) und eine Domäne (z. B. MYDOMAIN) zugewiesen wird, wenn sich der Benutzer bei einem Kontext anmeldet (z. B. C1).

Beispiel: *Hinzufügen des Attributs zu einem Shell-Profil*

Attribut	Anforderung	Attributwert
`shell:C1`	Obligatorisch	`Admin MYDOMAIN`

Wenn sich USER1 über den C1-Kontext anmeldet, wird diesem Benutzer automatisch die ADMIN-Rolle und die MYDOMAIN-Domäne zugewiesen (vorausgesetzt, dass eine Autorisierungsregel konfiguriert wurde, in der nach der Anmeldung von USER1 dieses Autorisierungsprofil zugewiesen wird).

Wenn sich USER1 über einen anderen Kontext anmeldet, der nicht im Wert des Attributs zurückgegeben wird, das der ACS zurücksendet, wird diesem Benutzer automatisch die Standardrolle (Network-Monitor) und die Standarddomäne (Standarddomäne) zugewiesen.

RADIUS (Authorization Profile)

Attribut(e): `cisco-av-pair`

Wert(e): `shell:<context-name>=<Role-name> <domain-name1> <domain-name2>`

Verwendung: Jeder Wert nach dem Gleichheitszeichen wird durch ein Leerzeichen getrennt. Sie können einen Benutzer (z. B. USER1) so konfigurieren, dass ihm eine Rolle (z. B. ADMIN) und eine Domäne (z. B. MYDOMAIN) zugewiesen wird, wenn sich der Benutzer bei einem Kontext anmeldet (z. B. C1).

Beispiel: *Hinzufügen des Attributs zu einem Autorisierungsprofil*

Wörterbuchtyp	RADIUS-Attribut	Attributtyp	Attributwert
RADIUS-Cisco	`cisco-av-pair`	Zeichenfolge	`shell:C1=ADMIN MYDOMAIN`

Wenn sich USER1 über den C1-Kontext anmeldet, wird diesem Benutzer automatisch die ADMIN-Rolle und die MYDOMAIN-Domäne zugewiesen (vorausgesetzt, dass eine Autorisierungsregel konfiguriert wurde, in der nach der Anmeldung von USER1 dieses Autorisierungsprofil zugewiesen wird).

Wenn sich USER1 über einen anderen Kontext anmeldet, der nicht im Wert des Attributs zurückgegeben wird, das der ACS zurücksendet, wird diesem Benutzer automatisch die Standardrolle (Network-Monitor) und die Standarddomäne (Standarddomäne) zugewiesen.

BlueCoat Packet Shaper

RADIUS (Authorization Profile)

Attribut(e): `Packeteer-AVPair`

Wert(e): `access=<Ebene>`

Verwendung: `<Ebene>` ist die Zugriffsebene für die Gewährung. Der Touchzugriff entspricht dem Schreibzugriff, während der Zugriff auf den Textausschnitt dem Schreibzugriff entspricht.

Der BlueCoat VSA ist in den ACS-Wörterbüchern standardmäßig nicht vorhanden. Um das BlueCoat-Attribut in einem Autorisierungsprofil zu verwenden, müssen Sie ein BlueCoat-Wörterbuch erstellen und diesem Wörterbuch die BlueCoat-Attribute hinzufügen.

Erstellen Sie ein Wörterbuch:

1. Navigieren Sie zu **Systemverwaltung > Konfiguration > Wörterbücher > Protokolle > RADIUS > RADIUS VSA.**
2. Klicken Sie auf **Erstellen**.
3. Geben Sie die Details des Wörterbuchs ein:Name: BlueCoatAnbieter-ID: 2334Attributpräfix: Paket-
4. Klicken Sie auf **Senden**.

Erstellen Sie ein Attribut im neuen Wörterbuch:

1. Navigieren Sie zu **Systemverwaltung > Konfiguration > Wörterbücher > Protokolle > RADIUS > RADIUS VSA > BlueCoat.**
2. Klicken Sie auf **Erstellen**.
3. Geben Sie die Details des Attributs ein:Attribut: `Packeteer-AVPair`Beschreibung: Wird verwendet, um die Zugriffsebene festzulegen.Attribut-ID des Anbieters: 1Richtung: AUSGEHENDMehrere zulässig: FalschAttribut in Protokoll einschließen: AktiviertAttributtyp: Zeichenfolge
4. Klicken Sie auf **Senden**.

Beispiel: ***Hinzufügen des Attributs zu einem Autorisierungsprofil (für schreibgeschützten Zugriff)***

Wörterbuchtyp	RADIUS-Attribut	Attributtyp	Attributwert
RADIUS-BlueCoat	`Packeteer-AVPair`	Zeichenfolge	`access=look`

Beispiel: ***Hinzufügen des Attributs zu einem Autorisierungsprofil (für Lese- und Schreibzugriff)***

Wörterbuchtyp	RADIUS-Attribut	Attributtyp	Attributwert
RADIUS-BlueCoat	`Packeteer-AVPair`	Zeichenfolge	`access=touch`

Brocade-Switches

RADIUS (Authorization Profile)

Attribut(e): `Tunnel-Private-Group-ID`

Wert(e): `U:<VLAN1>`; `T:<VLAN2>`

Verwendung: Legen Sie `<VLAN1>` den Wert des Daten-VLAN fest. Legen Sie `<VLAN2>` den Wert des Sprach-VLAN fest. In diesem Beispiel ist das Daten-VLAN VLAN VLAN 10 und das Sprach-VLAN VLAN VLAN 21.

Beispiel: *Hinzufügen des Attributs zu einem Autorisierungsprofil*

Wörterbuchtyp	RADIUS-Attribut	Attributtyp	Attributwert
RADIUS-IETF	`Tunnel-Private-Group-ID`	Tagged String	`U:10;T:21`

Cisco Unity Express (CUE)

RADIUS (Authorization Profile)

Attribut(e): `cisco-av-pair`

Wert(e): `fndn:groups=<Gruppenname>`

Verwendung: `<group-name>` der Name der Gruppe mit den Berechtigungen, die Sie dem Benutzer gewähren möchten. Diese Gruppe muss auf Cisco Unity Express (CUE) konfiguriert werden.

Beispiel: *Hinzufügen des Attributs zu einem Autorisierungsprofil*

Wörterbuchtyp	RADIUS-Attribut	Attributtyp	Attributwert
RADIUS-Cisco	`cisco-av-pair`	Zeichenfolge	`fndn:groups=Administrators`

Infoblox

RADIUS (Authorization Profile)

Attribut(e): `Infoblox-Gruppeninfo`

Wert(e): `<Gruppenname>`

Verwendung: `<group-name>` der Name der Gruppe mit den Berechtigungen, die Sie dem Benutzer gewähren möchten. Diese Gruppe muss auf dem Infoblox-Gerät konfiguriert werden. In diesem Konfigurationsbeispiel lautet der Gruppenname MyGroup.

Der Infoblox VSA ist in den ACS-Wörterbüchern standardmäßig nicht vorhanden. Um das Infoblox-Attribut in einem Autorisierungsprofil zu verwenden, müssen Sie ein Infoblox-Wörterbuch erstellen und diesem Wörterbuch die Infoblox-Attribute hinzufügen.

Erstellen Sie ein Wörterbuch:

1. Navigieren Sie zu **Systemverwaltung > Konfiguration > Wörterbücher > Protokolle > RADIUS > RADIUS VSA.**
2. Klicken Sie auf **Erstellen**.
3. Klicken Sie auf den kleinen Pfeil neben **Erweiterte Anbieteroptionen verwenden**.
4. Geben Sie die Details des Wörterbuchs ein:Name: InfobloxAnbieter-ID: 7779Feldgröße für Länge des Anbieters: 1Feldgröße des Anbietertyps: 1
5. Klicken Sie auf **Senden**.

Erstellen Sie ein Attribut im neuen Wörterbuch:

1. Navigieren Sie zu **Systemverwaltung > Konfiguration > Wörterbücher > Protokolle > RADIUS > RADIUS VSA > Infoblox.**
2. Klicken Sie auf **Erstellen**.
3. Geben Sie die Details des Attributs ein:Attribut: `Infoblox-Gruppeninfo`Attribut-ID des Anbieters: 009Richtung: AUSGEHENDMehrere zulässig: FalschAttribut in Protokoll einschließen: AktiviertAttributtyp: Zeichenfolge
4. Klicken Sie auf **Senden**.

Beispiel: ***Hinzufügen des Attributs zu einem Autorisierungsprofil***

Wörterbuchtyp	RADIUS-Attribut	Attributtyp	Attributwert
RADIUS-Infoblox	`Infoblox-Group-Info`	Zeichenfolge	`MyGroup`

Intrusion Prevention System (IPS)

RADIUS (Authorization Profile)

Attribut(e): `IPS-Rolle`

Wert(e): `<Rollenname>`

Verwendung: Der Wert `<role name>` kann eine der vier Benutzerrollen des Intrusion Prevention System (IPS) sein: Viewer, Operator, Administrator oder Service. Weitere Informationen zu den Berechtigungen für die einzelnen Benutzerrollen finden Sie im Konfigurationsleitfaden für Ihre Version von IPS.

- Cisco Intrusion Prevention System Geräte-Manager Konfigurationsleitfaden für IPS 7.0
- Cisco Intrusion Prevention System Device Manager Configuration Guide IPS 7.1

Beispiel: *Hinzufügen des Attributs zu einem Autorisierungsprofil*

Wörterbuchtyp	RADIUS-Attribut	Attributtyp	Attributwert
RADIUS-Cisco	`cisco-av-pair`	Zeichenfolge	`ips-role:administrator`

Juniper

TACACS+ (Shell-Profil)

Attribut(e): `allow-Commands`; `allow-configuration`; `local-user-name`; `deny-Commands`; `deny-configuration`; `Benutzerberechtigungen`

Wert(e): `<allow-commands-regex>`; `<allow-configuration-regex>` ; `<lokaler Benutzername>`; `<deny-commands-regex>`; `<Konfiguration verweigern-regex>`

Verwendung: Legen Sie den Wert von `<local-username>` (d. h. den Wert des Attributs für den lokalen Benutzernamen) auf einen Benutzernamen fest, der lokal auf dem Juniper-Gerät vorhanden ist. Sie können beispielsweise einen Benutzer (z. B. USER1) so konfigurieren, dass ihm dieselbe Benutzervorlage wie einem Benutzer (z. B. JUSER) zugewiesen wird, die lokal auf dem Juniper-Gerät vorhanden ist, wenn Sie den Wert des Attributs für den lokalen Benutzernamen auf JUSER festlegen. Die Werte der Attribute allow-Commands, allow-configuration, deny-Commands und deny-configuration können im regex-Format eingegeben werden. Die Werte, auf die diese Attribute festgelegt werden, werden zusätzlich zu den Befehlen im Betriebs-/Konfigurationsmodus festgelegt, die durch die Berechtigungsbits der Benutzeranmeldeklasse autorisiert wurden.

Beispiel: *Hinzufügen von Attributen zu einem Shell-Profil 1*

Attribut	Anforderung	Attributwert
`allow-commands`	Optional	`"(request system) | (show rip neighbor)"`
`allow-configuration`	Optional	
`local-user-name`	Optional	`sales`
`deny-commands`	Optional	`"<^clear"`
`deny-configuration`	Optional	

Beispiel: *Hinzufügen von Attributen zu einem Shell-Profil 2*

Attribut	Anforderung	Attributwert
`allow-commands`	Optional	`"monitor | help | show | ping | traceroute"`
	Optional	

allow-configuration		
local-user-name	Optional	engineering
deny-commands	Optional	"configure"
deny-configuration	Optional	

Nexus-Switches

RADIUS (Authorization Profile)

Attribut(e): cisco-av-pair

Wert(e): shell:roles="<role1> <role2>"

Verwendung: Legen Sie die Werte von <role1> und <role2> auf die lokal auf dem Switch definierten Rollennamen fest. Wenn Sie mehrere Rollen hinzufügen, trennen Sie diese durch ein Leerzeichen. Wenn mehrere Rollen vom AAA-Server an den Nexus-Switch zurückgegeben werden, hat der Benutzer Zugriff auf Befehle, die in der Union aller drei Rollen definiert sind.

Die integrierten Rollen werden unter Konfigurieren von Benutzerkonten und RBAC definiert.

Beispiel: *Hinzufügen des Attributs zu einem Autorisierungsprofil*

Wörterbuchtyp	RADIUS-Attribut	Attributtyp	Attributwert
RADIUS-Cisco	cisco-av-pair	Zeichenfolge	shell:roles="network-admin vdc-admin vdc-operator"

Riverbed

TACACS+ (Shell-Profil)

Attribut(e): Service; Lokaler Benutzername

Wert(e): rbt-exec; <Benutzername>

Verwendung: Um dem Benutzer schreibgeschützten Zugriff zu gewähren, muss der <Benutzername> Wert auf Monitor eingestellt werden. Um dem Benutzer Lese- und Schreibzugriff zu gewähren, muss der <Benutzername> auf admin gesetzt werden. Wenn Sie neben Admin und Monitor ein anderes Konto definiert haben, konfigurieren Sie diesen Namen für die Rückgabe.

Beispiel: *Hinzufügen von Attributen zu einem Shell-Profil (für schreibgeschützten Zugriff)*

Attribut	Anforderung	Attributwert
service	Obligatorisch	rbt-exec
local-user-name	Obligatorisch	monitor

Beispiel: *Hinzufügen von Attributen zu einem Shell-Profil (für Lese- und Schreibzugriff)*

Attribut	Anforderung	Attributwert
`service`	Obligatorisch	`rbt-exec`
`local-user-name`	Obligatorisch	`admin`

Wireless LAN Controller (WLC)

RADIUS (Authorization Profile)

Attribut(e): `Servicetyp`

Wert(e): `Verwaltung (6)` / `NAS-Aufforderung (7)`

Verwendung: Um dem Benutzer Lese-/Schreibzugriff auf den Wireless LAN Controller (WLC) zu gewähren, muss der Wert "Verwaltung" lauten. für schreibgeschützten Zugriff muss der Wert NAS-Prompt sein.

Ausführliche Informationen finden Sie unter Konfigurationsbeispiel für die RADIUS-Serverauthentifizierung von Verwaltungsbenutzern bei Wireless LAN Controller (WLC).

Beispiel: *Hinzufügen des Attributs zu einem Autorisierungsprofil (für schreibgeschützten Zugriff)*

Wörterbuchtyp	RADIUS-Attribut	Attributtyp	Attributwert
RADIUS-IETF	`Service-Type`	Enumeration	`NAS-Prompt`

Beispiel: *Hinzufügen des Attributs zu einem Autorisierungsprofil (für Lese- und Schreibzugriff)*

Wörterbuchtyp	RADIUS-Attribut	Attributtyp	Attributwert
RADIUS-IETF	`Service-Type`	Enumeration	`Administrative`

Data Center Network Manager (DCNM)

DCNM muss nach dem Ändern der Authentifizierungsmethode neu gestartet werden. Andernfalls kann der Netzwerkbetreiber Berechtigungen anstelle des Netzwerkadministrators zuweisen.

DCNM-Rolle	RADIUS Cisco-AV-Paar	Taktiken Cisco-AV-Paar
Benutzer	`shell:roles = "network-operator"`	`cisco-av-pair=shell:roles="network-operator"`
Administrator	`shell:roles = "network-admin"`	`cisco-av-pair=shell:roles="network-admin"`

Zugehörige Informationen

- Technischer Support und Dokumentation - Cisco Systems
- Terminal Access Controller Access Control System (TACACS+)
- RADIUS (Remote Authentication Dial-In User Service)
- Anforderungen für Kommentare (RFCs)