Esempio di configurazione degli attributi TACACS+ e RADIUS per diversi dispositivi Cisco e non Cisco

Sommario

Introduzione

Questo documento offre una compilazione di attributi che diversi prodotti Cisco e non Cisco si aspettano di ricevere da un server di autenticazione, autorizzazione e accounting (AAA); in questo caso, il server AAA è un Access Control Server (ACS). L'ACS può restituire questi attributi insieme a un Access-Accept come parte di un profilo shell (TACACS+) o di un profilo di autorizzazione (RADIUS).

In questo documento vengono fornite istruzioni dettagliate su come aggiungere attributi personalizzati ai profili shell e ai profili di autorizzazione. Questo documento contiene anche un elenco di dispositivi e gli attributi TACACS+ e RADIUS che i dispositivi si aspettano vengano restituiti dal server AAA. Tutti gli argomenti includono esempi.

L'elenco degli attributi fornito in questo documento non è esaustivo né autorevole e può essere modificato in qualsiasi momento senza un aggiornamento del documento.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il riferimento delle informazioni contenute in questo documento è la versione 5.2/5.3 di ACS.

Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

Creazione di un profilo di shell (TACACS+)

Un profilo shell è un contenitore di autorizzazioni di base per l'accesso basato su TACACS+. È possibile specificare gli attributi e i valori degli attributi TACACS+ da restituire con Access-Accept, oltre al livello di privilegio Cisco® IOS, al timeout della sessione e ad altri parametri.

Completare questi passaggi per aggiungere attributi personalizzati a un nuovo profilo shell:

1. Accedere all'interfaccia ACS.
2. Passare a **Elementi dei criteri > Autorizzazioni e autorizzazioni > Amministrazione dispositivi > Profili shell**.
3. Fare clic sul pulsante **Crea**.
4. Assegnare un nome al profilo della shell.
5. Fare clic sulla scheda **Attributi personalizzati**.
6. Immettere il nome dell'attributo nel campo **Attributo**.
7. Scegliere se il requisito è **obbligatorio** o **facoltativo** dall'elenco a discesa Requisito.
8. Lasciare l'elenco a discesa per il valore dell'attributo impostato su **Static**. Se il valore è statico, è possibile immetterlo nel campo successivo. Se il valore è dinamico, non è possibile immettere l'attributo manualmente; viene invece mappato a un attributo in uno degli archivi identità.
9. Immettere il valore dell'attributo nell'ultimo campo.
10. Per aggiungere la voce alla tabella, fare clic sul pulsante **Add** (Aggiungi).
11. Ripetere l'operazione per configurare tutti gli attributi necessari.
12. Fare clic sul pulsante **Invia** nella parte inferiore della schermata.

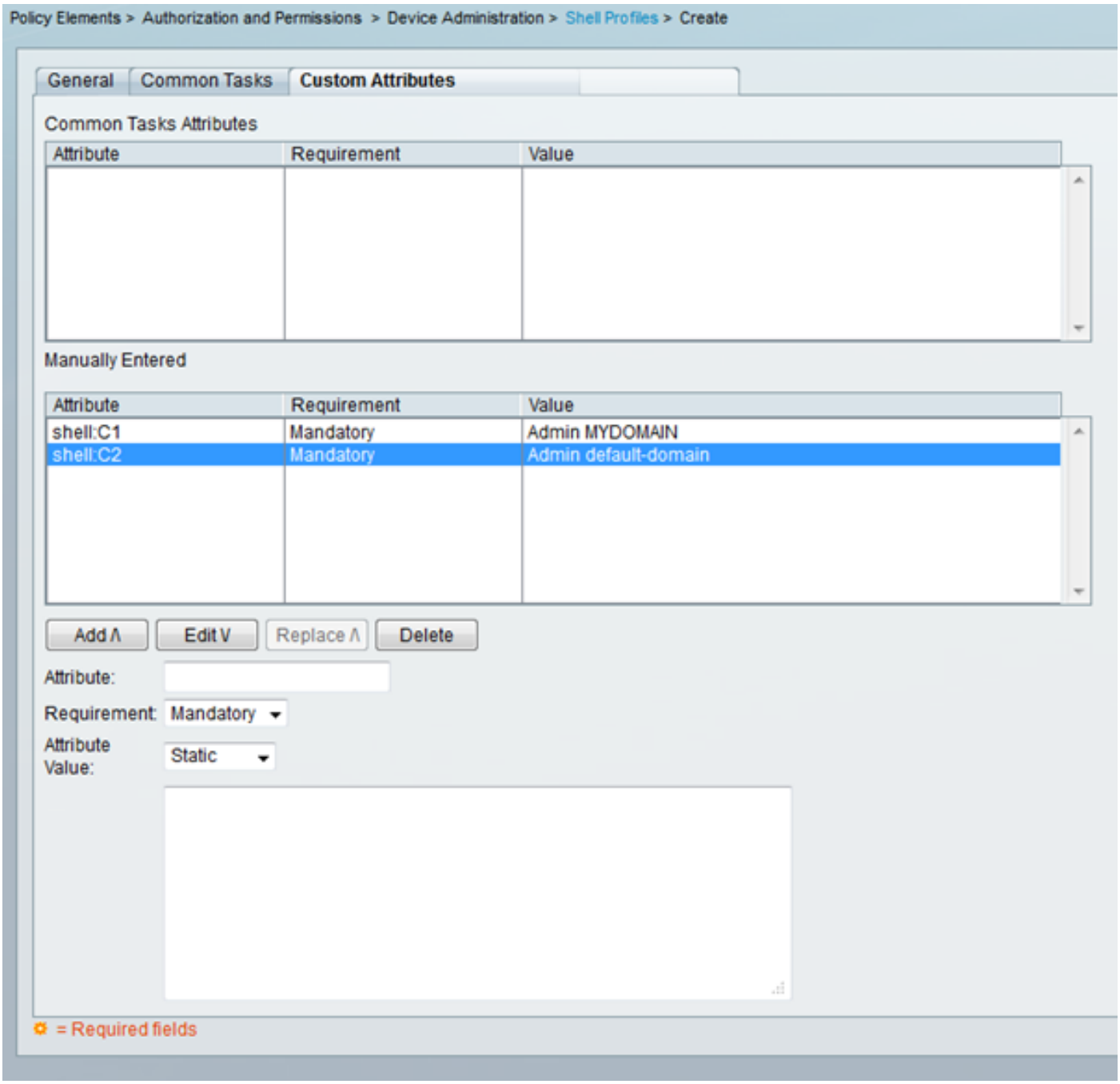
Esempio di configurazione

Sul dispositivo bootflash o slot0:: Application Control Engine (ACE)

Attributo/i: `shell:<nome-contesto>`

Valore/i: `<Nome-ruolo> <Nome-dominio1>`

Utilizzo: Il ruolo e il dominio sono separati da uno spazio. È possibile configurare un utente (ad esempio, USER1) in modo che gli vengano assegnati un ruolo (ad esempio, ADMIN) e un dominio (ad esempio, MYDOMAIN) quando l'utente accede a un contesto (ad esempio, C1).



Creazione di un profilo di autorizzazione (RADIUS)

Un profilo di autorizzazione è un contenitore di autorizzazioni di base per l'accesso basato su RADIUS. È possibile specificare gli attributi RADIUS e i valori degli attributi da restituire con Access-Accept, oltre alle VLAN, agli Access Control Lists (ACL) e ad altri parametri.

Per aggiungere attributi personalizzati a un nuovo profilo di autorizzazione, completare la procedura seguente:

1. Accedere all'interfaccia ACS.
2. Passare a **Elementi criteri > Autorizzazioni e autorizzazioni > Accesso alla rete > Profili di autorizzazione**.
3. Fare clic sul pulsante **Crea**.
4. Assegnare un nome al profilo di autorizzazione.
5. Fare clic sulla scheda **Attributi RADIUS**.
6. Selezionare un dizionario dal menu a discesa **Tipo di dizionario**.
7. Per impostare l'attributo di selezione per il campo Attributo RADIUS, fare clic sul pulsante **Seleziona**. Viene visualizzata una nuova finestra.
8. Esaminare gli attributi disponibili, effettuare la selezione e fare clic su **OK**. Il valore **Tipo attributo** viene impostato per impostazione predefinita in base alla selezione dell'attributo appena effettuata.
9. Lasciare l'elenco a discesa per il valore dell'attributo impostato su **Static**. Se il valore è statico, è possibile immetterlo nel campo successivo. Se il valore è dinamico, non è possibile immettere l'attributo manualmente; viene invece mappato a un attributo in uno degli archivi identità.
10. Immettere il valore dell'attributo nell'ultimo campo.
11. Per aggiungere la voce alla tabella, fare clic sul pulsante **Add** (Aggiungi).
12. Ripetere l'operazione per configurare tutti gli attributi necessari.
13. Fare clic sul pulsante **Invia** nella parte inferiore della schermata.

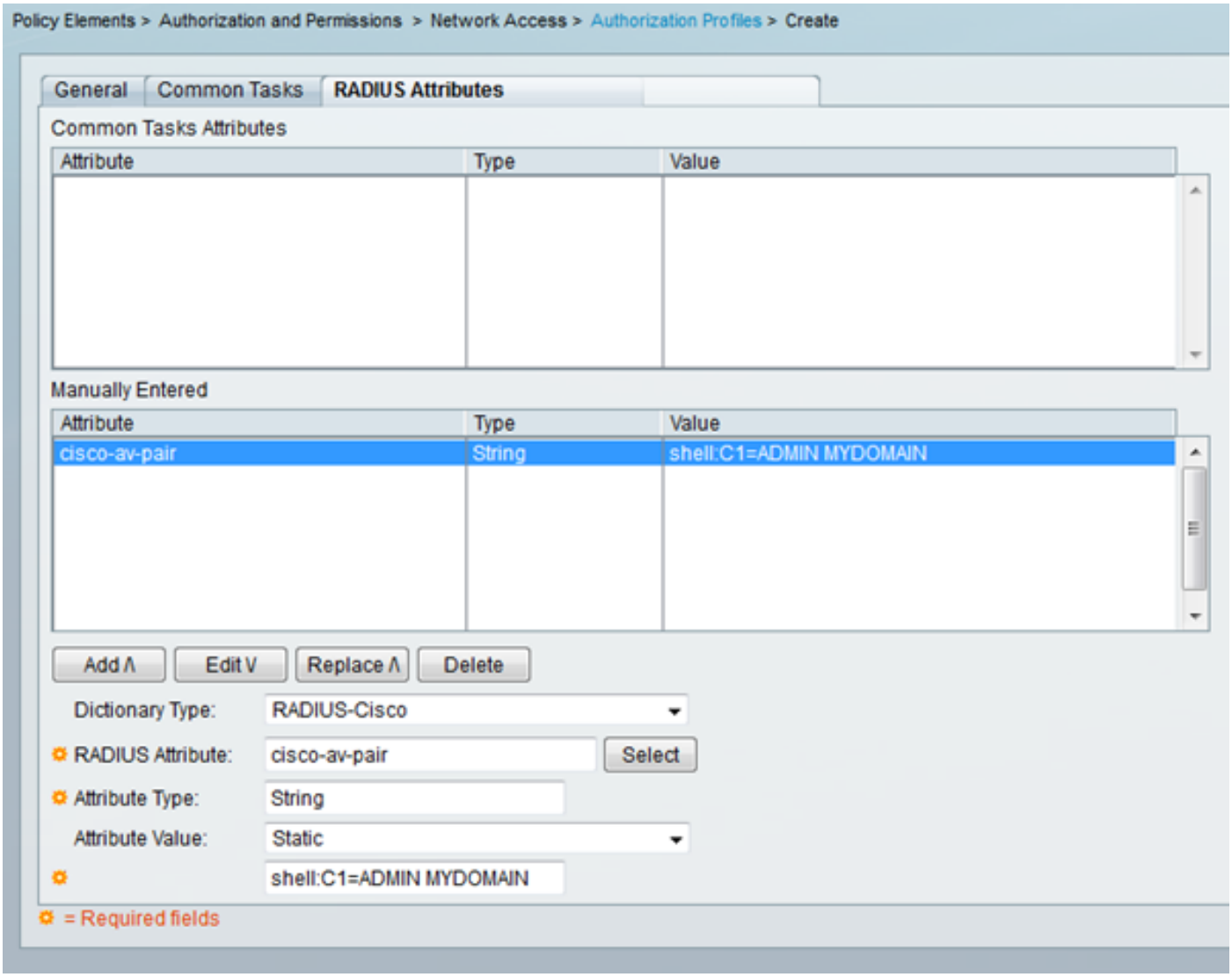
Esempio di configurazione

Sul dispositivo bootflash o slot0:: ASSO

Attributo/i: `cisco-av-pair`

Valore/i: `shell:<nome-contesto>=<nome-ruolo> <nome-dominio1> <nome-dominio2>`

Utilizzo: Ogni valore dopo il segno di uguale è separato da uno spazio. È possibile configurare un utente (ad esempio, USER1) in modo che gli vengano assegnati un ruolo (ad esempio, ADMIN) e un dominio (ad esempio, MYDOMAIN) quando l'utente accede a un contesto (ad esempio, C1).



Elenco dispositivi

Aggregation Services Router (ASR)

RADIUS (profilo di autorizzazione)

Attributo/i: `cisco-av-pair`

Valore/i: `shell:tasks="#<nome-ruolo>,<autorizzazione>:<processo>"`

Utilizzo: Impostare i valori di `<nome-ruolo>` sul nome di un ruolo definito localmente sul router. La gerarchia dei ruoli può essere descritta in termini di struttura ad albero, dove il ruolo `#root` si trova nella parte superiore della struttura ad albero e il ruolo `#leaf` aggiunge comandi aggiuntivi. Questi due ruoli possono essere combinati e restituiti se: `shell:tasks="#root,#leaf"`.

Èinoltre possibile passare le autorizzazioni a un singolo processo, in modo da concedere a un utente i privilegi di lettura, scrittura ed esecuzione per determinati processi. Ad esempio, per concedere a un utente i privilegi di lettura e scrittura per il processo bgp, impostare il valore su: `shell:tasks="#root,rw:bgp"`. L'ordine degli attributi è irrilevante; il risultato è lo stesso indipendentemente dal fatto che il valore sia impostato su `shell:tasks="#root,rw:bgp"` o su ro `shell:tasks="rw:bgp,#root"`.

Esempio - *Aggiungere l'attributo a un profilo di autorizzazione*

Tipo di dizionario	Attributo RADIUS	Tipo di attributo	Valore attributo
RADIUS-Cisco	`cisco-av-pair`	Stringa	`shell:tasks="#root,#leaf,rwx:bgp,r:ospf"`

Application Control Engine (ACE)

TACACS+ (profilo shell)

Attributo/i: `shell:<nome-contesto>`

Valore/i: `<Nome-ruolo> <Nome-dominio1>`

Utilizzo: Il ruolo e il dominio sono separati da uno spazio. È possibile configurare un utente (ad esempio, USER1) in modo che gli vengano assegnati un ruolo (ad esempio, ADMIN) e un dominio (ad esempio, MYDOMAIN) quando l'utente accede a un contesto (ad esempio, C1).

Esempio - *Aggiungere l'attributo a un profilo di shell*

Attributo	Requisito	Valore attributo
`shell:C1`	Obbligatorio	`Admin MYDOMAIN`

Se USER1 esegue l'accesso tramite il contesto C1, a tale utente vengono automaticamente assegnati il ruolo ADMIN e il dominio MYDOMAIN, a condizione che sia stata configurata una regola di autorizzazione alla quale, dopo l'accesso USER1, viene assegnato questo profilo di autorizzazione.

Se l'utente USER1 esegue l'accesso in un contesto diverso, che non viene restituito nel valore dell'attributo restituito da ACS, a tale utente viene assegnato automaticamente il ruolo predefinito (Network-Monitor) e il dominio predefinito (default-domain).

RADIUS (profilo di autorizzazione)

Attributo/i: `cisco-av-pair`

Valore/i: `shell:<nome-contesto>=<nome-ruolo> <nome-dominio1> <nome-dominio2>`

Utilizzo: Ogni valore dopo il segno di uguale è separato da uno spazio. È possibile configurare un utente (ad esempio, USER1) in modo che gli venga assegnato un ruolo (ad esempio, ADMIN) e un dominio (ad esempio, MYDOMAIN) quando l'utente accede a un contesto (ad esempio, C1).

Esempio - *Aggiungere l'attributo a un profilo di autorizzazione*

Tipo di dizionario	Attributo RADIUS	Tipo di attributo	Valore attributo
RADIUS-Cisco	`cisco-av-pair`	Stringa	`shell:C1=ADMIN MYDOMAIN`

Se USER1 esegue l'accesso tramite il contesto C1, a tale utente vengono automaticamente assegnati il ruolo ADMIN e il dominio MYDOMAIN, a condizione che sia stata configurata una regola di autorizzazione alla quale, dopo l'accesso USER1, viene assegnato questo profilo di autorizzazione.

Se l'utente USER1 esegue l'accesso in un contesto diverso, che non viene restituito nel valore dell'attributo restituito da ACS, a tale utente viene assegnato automaticamente il ruolo predefinito (Network-Monitor) e il dominio predefinito (default-domain).

BlueCoat Packet Shaper

RADIUS (profilo di autorizzazione)

Attributo/i: `Packet-AVPair`

Valore/i: `access=<livello>`

Utilizzo: `<livello>` è il livello di accesso da concedere. L'accesso tramite tocco equivale alla lettura/scrittura, mentre l'accesso tramite look equivale alla sola lettura.

Per impostazione predefinita, la VSA BlueCoat non esiste nei dizionari ACS. Per utilizzare l'attributo BlueCoat in un profilo di autorizzazione, è necessario creare un dizionario BlueCoat e aggiungervi gli attributi BlueCoat.

Creare il dizionario:

1. Selezionare Amministrazione sistema > Configurazione > Dizionari > **Protocolli** > **RADIUS** > **RADIUS VSA**.
2. Fare clic su **Crea**.
3. Immettere i dettagli del dizionario:Nome: BlueCoatID fornitore: 2334Prefisso attributo: Packeteer
4. Fare clic su **Invia**.

Creare un attributo nel nuovo dizionario:

1. Selezionare Amministrazione sistema > Configurazione > Dizionari > Protocolli > RADIUS > **RADIUS VSA** > **BlueCoat**.
2. Fare clic su **Crea**.
3. Immettere i dettagli dell'attributo:Attributo: `Packet-AVPair`Descrizione: Utilizzato per specificare il livello di accessoID attributo fornitore: 1Direzione: IN USCITAMultiplo consentito: FalsoIncludi attributo nel registro: ControllatoTipo attributo: Stringa
4. Fare clic su **Invia**.

Esempio - ***Aggiungere l'attributo a un profilo di autorizzazione (per l'accesso in sola lettura)***

Tipo di dizionario	Attributo RADIUS	Tipo di attributo	Valore attributo
RADIUS-BlueCoat	`Packeteer-AVPair`	Stringa	`access=look`

Esempio - ***Aggiungere l'attributo a un profilo di autorizzazione (per l'accesso in lettura/scrittura)***

Tipo di dizionario	Attributo RADIUS	Tipo di attributo	Valore attributo
RADIUS-BlueCoat	`Packeteer-AVPair`	Stringa	`access=touch`

Switch Brocade

RADIUS (profilo di autorizzazione)

Attributo/i: `Tunnel-Private-Group-ID`

Valore/i: `U:<VLAN1>`; `T:<VLAN2>`

Utilizzo: Impostare `<VLAN1>` sul valore della VLAN dati. Impostare `<VLAN2>` sul valore della VLAN vocale. Nell'esempio, la VLAN dati è la VLAN 10 e la VLAN voce è la VLAN 21.

Esempio - ***Aggiungere l'attributo a un profilo di autorizzazione***

Tipo di dizionario	Attributo RADIUS	Tipo di attributo	Valore attributo
RADIUS-IETF	`Tunnel-Private-Group-ID`	Stringa con tag	`U:10;T:21`

Cisco Unity Express (CUE)

RADIUS (profilo di autorizzazione)

Attributo/i: `cisco-av-pair`

Valore/i: `fndn:groups=<nome-gruppo>`

Utilizzo: `<nome-gruppo>` è il nome del gruppo con i privilegi che si desidera concedere all'utente. Questo gruppo deve essere configurato su Cisco Unity Express (CUE).

Esempio - ***Aggiungere l'attributo a un profilo di autorizzazione***

Tipo di dizionario	Attributo RADIUS	Tipo di attributo	Valore attributo
RADIUS-Cisco	`cisco-av-pair`	Stringa	`fndn:groups=Administrators`

Infoblox

RADIUS (profilo di autorizzazione)

Attributo/i: `Infoblox-Group-Info`

Valore/i: `<nome-gruppo>`

Utilizzo: `<nome-gruppo>` è il nome del gruppo con i privilegi che si desidera concedere all'utente. Questo gruppo deve essere configurato nel dispositivo Infoblox. In questo esempio di configurazione il nome del gruppo è MyGroup.

Per impostazione predefinita, la VSA di Infoblox non esiste nei dizionari ACS. Per utilizzare l'attributo Infoblox in un profilo di autorizzazione, è necessario creare un dizionario di Infoblox e aggiungere gli attributi a tale dizionario.

Creare il dizionario:

1. Selezionare Amministrazione sistema > Configurazione > Dizionari > **Protocolli** > **RADIUSS** > **RADIUS VSA**.
2. Fare clic su **Crea**.
3. Fare clic sulla piccola freccia accanto a **Usa opzioni avanzate fornitore**.
4. Immettere i dettagli del dizionario:Nome: InfobloxID fornitore: 7779Dimensione campo lunghezza fornitore: 1Dimensione campo tipo fornitore: 1
5. Fare clic su **Invia**.

Creare un attributo nel nuovo dizionario:

1. Selezionare Amministrazione sistema > Configurazione > Dizionari > Protocolli > RADIUS > **RADIUS VSA** > **Infoblox**.
2. Fare clic su **Crea**.
3. Immettere i dettagli dell'attributo:Attributo: `Infoblox-Group-Info`ID attributo fornitore: 009Direzione: IN USCITAMultiplo consentito: FalsoIncludi attributo nel registro: ControllatoTipo attributo: Stringa
4. Fare clic su **Invia**.

Esempio - ***Aggiungere l'attributo a un profilo di autorizzazione***

Tipo di dizionario	Attributo RADIUS	Tipo di attributo	Valore attributo
RADIUS-Infoblox	`Infoblox-Group-Info`	Stringa	`MyGroup`

IPS (Intrusion Prevention System)

RADIUS (profilo di autorizzazione)

Attributo/i: `ruolo ips`

Valore/i: `<nome ruolo>`

Utilizzo: Il valore `<nome ruolo>` può corrispondere a uno dei quattro ruoli utente IPS (Intrusion Prevention System) seguenti: visualizzatore, operatore, amministratore o servizio. Per i dettagli sulle autorizzazioni concesse a ciascun tipo di ruolo utente, consultare la guida alla configurazione della propria versione di IPS.

- Guida alla configurazione di Cisco Intrusion Prevention System Device Manager per IPS 7.0
- Guida alla configurazione di Cisco Intrusion Prevention System Device Manager per IPS 7.1

Esempio - *Aggiungere l'attributo a un profilo di autorizzazione*

Tipo di dizionario	Attributo RADIUS	Tipo di attributo	Valore attributo
RADIUS-Cisco	`cisco-av-pair`	Stringa	`ips-role:administrator`

Ginepro

TACACS+ (profilo shell)

Attributo/i: `allow-commands` ; `allow-configuration` ; `nome-utente-locale` ; `deny-commands` ; `negazione della configurazione`; `autorizzazioni utente`

Valore/i: `<allow-commands-regex>` ; `<allow-configuration-regex>` ; `<local-username>` ; `<deny-commands-regex>` ; `<deny-configuration-regex>`

Utilizzo: Impostare il valore di `<local-username>` (ovvero il valore dell'attributo local-user-name) su un nome utente che esiste localmente sul dispositivo Juniper. Ad esempio, è possibile configurare un utente (ad esempio, USER1) in modo che gli venga assegnato lo stesso modello utente di un utente (ad esempio, JUSER) che esiste localmente sul dispositivo Juniper quando si imposta il valore dell'attributo local-user-name su JUSER. I valori degli attributi allow-commands, allow-configuration, deny-commands e deny-configuration possono essere immessi in formato regex. I valori impostati per questi attributi sono in aggiunta ai comandi della modalità operativa/di configurazione autorizzati dai bit delle autorizzazioni della classe di accesso dell'utente.

Esempio - *Aggiunta di attributi a un profilo di guscio 1*

Attributo	Requisito	Valore attributo
`allow-commands`	Facoltativo	`"(request system) | (show rip neighbor)"`
`allow-configuration`	Facoltativo	
`local-user-name`	Facoltativo	`sales`
`deny-commands`	Facoltativo	`"<^clear"`
`deny-configuration`	Facoltativo	

Esempio - *Aggiunta di attributi a un profilo di guscio 2*

Attributo	Requisito	Valore attributo
`allow-commands`	Facoltativo	`"monitor | help | show | ping | traceroute"`
`allow-configuration`	Facoltativo	
	Facoltativo	

local-user-name		engineering
deny-commands	Facoltativo	"configure"
deny-configuration	Facoltativo	

Switch Nexus

RADIUS (profilo di autorizzazione)

Attributo/i: cisco-av-pair

Valore/i: shell:roles="<ruolo1> <ruolo2>"

Utilizzo: Impostare i valori di <ruolo1> e <ruolo2> sui nomi dei ruoli definiti localmente sullo switch. Quando si aggiungono più ruoli, separarli con uno spazio. Quando più ruoli vengono passati dal server AAA allo switch Nexus, il risultato è che l'utente ha accesso ai comandi definiti dall'unione di tutti e tre i ruoli.

I ruoli predefiniti sono definiti in Configurazione degli account utente e RBAC.

Esempio - ***Aggiungere l'attributo a un profilo di autorizzazione***

Tipo di dizionario	Attributo RADIUS	Tipo di attributo	Valore attributo
RADIUS-Cisco	cisco-av-pair	Stringa	shell:roles="network-admin vdc-admin vdc-operator"

Riverbed

TACACS+ (profilo shell)

Attributo/i: servizio ; nome-utente-locale

Valore/i: rbt-exec ; <nomeutente>

Utilizzo: Per concedere all'utente l'accesso in sola lettura, il valore <username> deve essere impostato su monitor. Per concedere all'utente l'accesso in lettura/scrittura, il valore <username> deve essere impostato su admin. Se oltre ad admin e monitor è stato definito un altro account, configurare il nome da restituire.

Esempio - ***Aggiungere attributi a un profilo di shell (per l'accesso in sola lettura)***

Attributo	Requisito	Valore attributo
service	Obbligatorio	rbt-exec
local-user-name	Obbligatorio	monitor

Esempio - ***Aggiungere attributi a un profilo di shell (per l'accesso in lettura/scrittura)***

Attributo	Requisito	Valore attributo
`service`	Obbligatorio	`rbt-exec`
`local-user-name`	Obbligatorio	`admin`

Controller LAN wireless (WLC)

RADIUS (profilo di autorizzazione)

Attributo/i: `Service-Type`

Valore/i: `Amministrativo (6)` / `Prompt NAS (7)`

Utilizzo: Per concedere all'utente l'accesso in lettura/scrittura al Wireless LAN Controller (WLC), il valore deve essere Administrative; per l'accesso in sola lettura, il valore deve essere NAS-Prompt.

Per i dettagli, vedere Esempio di configurazione dell'autenticazione server RADIUS degli utenti di gestione su controller WLC (Wireless LAN Controller)

Esempio - *Aggiungere l'attributo a un profilo di autorizzazione (per l'accesso in sola lettura)*

Tipo di dizionario	Attributo RADIUS	Tipo di attributo	Valore attributo
RADIUS-IETF	`Service-Type`	Enumerazione	`NAS-Prompt`

Esempio - *Aggiungere l'attributo a un profilo di autorizzazione (per l'accesso in lettura/scrittura)*

Tipo di dizionario	Attributo RADIUS	Tipo di attributo	Valore attributo
RADIUS-IETF	`Service-Type`	Enumerazione	`Administrative`

DCNM (Data Center Network Manager)

Dopo aver modificato il metodo di autenticazione, è necessario riavviare DCNM. In caso contrario, potrebbe assegnare il privilegio di operatore di rete anziché quello di amministratore di rete.

Ruolo DCNM	RADIUS Cisco-AV-Pair	Tacacs Cisco-AV-Pair
Utente	`shell:roles = "network-operator"`	`cisco-av-pair=shell:roles="network-operator"`
Amministratore	`shell:roles = "network-admin"`	`cisco-av-pair=shell:roles="network-admin"`

Informazioni correlate

- Documentazione e supporto tecnico – Cisco Systems
- TACACS+ (Terminal Access Controller Access Control System)
- RADIUS (Remote Authentication Dial-In User Service)
- RFC (Requests for Comments)