TACACS+ y atributos de RADIUS para diverso Cisco y el ejemplo de configuración de los dispositivos del no Cisco

Contenido

Introducción

Este documento proporciona una compilación de los atributos que diverso Cisco y los Productos del no Cisco esperan recibir de un servidor del Authentication, Authorization, and Accounting (AAA); en este caso, el servidor de AAA es un Access Control Server (ACS). El ACS puede volver estos atributos junto con un access-accept como parte de un perfil del shell (TACACS+) o el perfil de la autorización (RADIUS).

Este documento proporciona las instrucciones paso a paso en cómo agregar los atributos personalizados para descascar los perfiles y los perfiles de la autorización. Este documento también contiene una lista de dispositivos y el TACACS+ y los atributos de RADIUS que los dispositivos esperan considerar vuelto del servidor de AAA. Todos los temas incluyen los

ejemplos.

La lista de atributos proporcionados en este documento no es exhaustiva o autoritaria y puede cambiar en cualquier momento sin una actualización a este documento.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información en este documento se basa en el ACS versión 5.2/5.3.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Cree un perfil del shell (el TACACS+)

Un perfil del shell es un envase básico de los permisos para el acceso TACACS+-based. Usted puede especificar qué TACACS+ atribuye y los valores de atributo se deben volver con el access-accept, además del nivel de privilegio IOS del Cisco®, del tiempo de espera de la sesión, y de otros parámetros.

Complete estos pasos para agregar los atributos personalizados a un nuevo perfil del shell:

1. Inicie sesión a la interfaz ACS.
2. Navegue a los **elementos** > a la **autorización y a los permisos de la directiva** > **Device Administration (Administración del dispositivo)** > los **perfiles del shell**.
3. Haga clic el **botón Create**.
4. Nombre el perfil del shell.
5. Haga clic la lengueta de los **atributos personalizados**.
6. Ingrese el nombre del atributo en el campo del **atributo**.
7. Elija si el requisito es **obligatorio** u **opcional de la** lista desplegable del requisito.
8. Deje el descenso-abajo por el valor de atributo fijado a los **parásitos atmosféricos**. Si el valor es estático, usted puede ingresar el valor en el campo siguiente. Si el valor es dinámico, usted no puede ingresar el atributo manualmente; en lugar atribuido se asocia a un atributo en uno de los almacenes de la identidad.
9. Ingrese el valor del atributo en el campo más reciente.
10. Haga clic el **botón Add** para agregar la entrada a la tabla.
11. Relance para configurar todos los atributos que usted necesita.
12. Haga clic el **botón Submit Button** en la parte inferior de la pantalla.

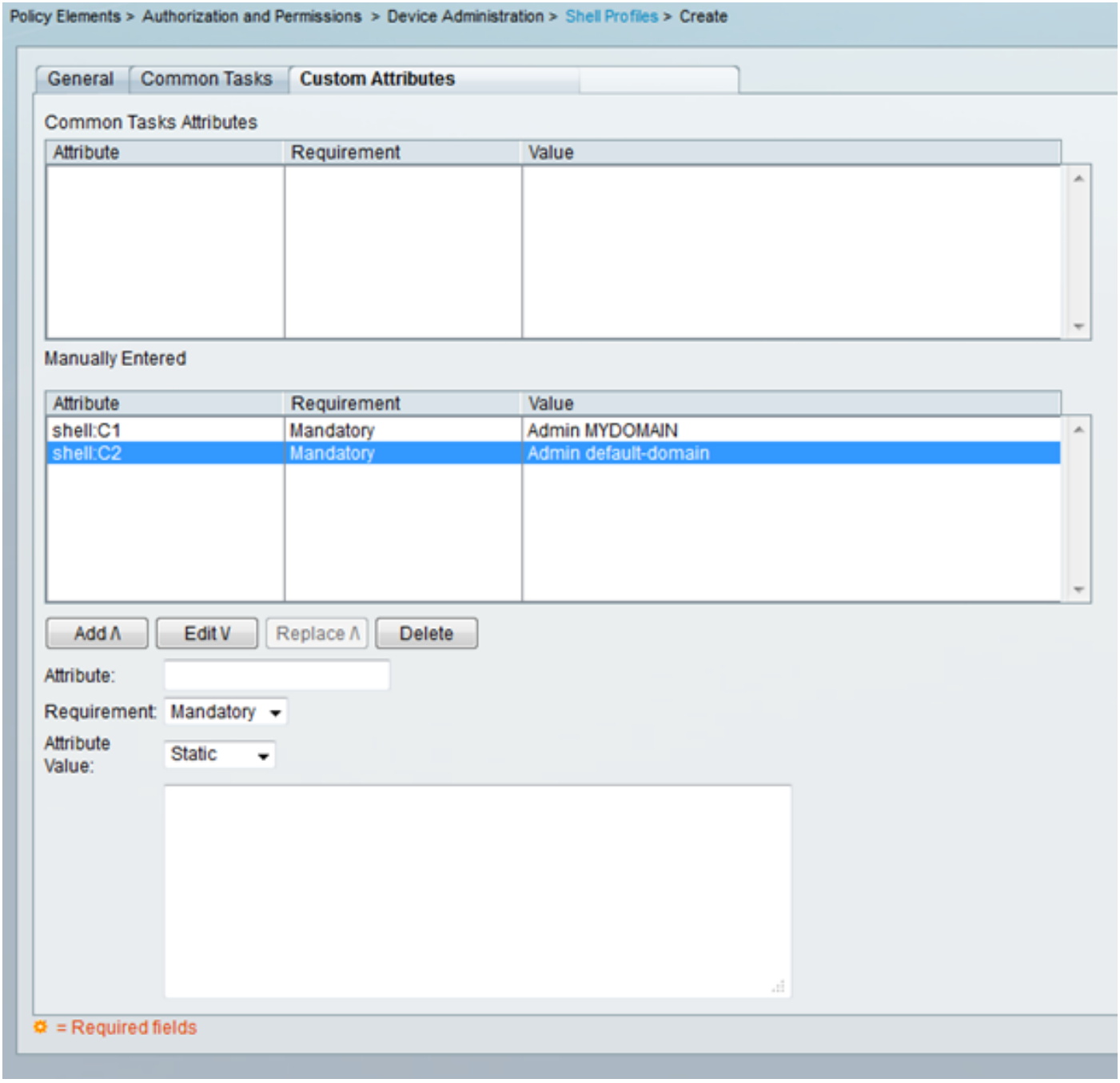
Ejemplo de configuración

Dispositivo: Motor del control de la aplicación (ACE)

Atributos: `shell: <context-name>`

Valor: `<Role-name> <domain-name1>`

Uso: El papel y el dominio son separados por un carácter de espacio. Usted puede configurar a un usuario (por ejemplo, USER1) para ser asignado un papel (por ejemplo, ADMIN) y un dominio (por ejemplo, MYDOMAIN) cuando el usuario abre una sesión a un contexto (por ejemplo, c1).



Cree un perfil de la autorización (el RADIUS)

Un perfil de la autorización es un envase básico de los permisos para el acceso basado en RADIUS. Usted puede especificar qué atributos de RADIUS y valores de atributo se deben volver con el access-accept, además de los VLA N, del Listas de control de acceso (ACL), y de otros parámetros.

Complete estos pasos para agregar los atributos personalizados a un nuevo perfil de la autorización:

1. Inicie sesión a la interfaz ACS.
2. Navegue a los **elementos de la directiva** > a la **autorización y a los permisos** > a los **perfiles del acceso a la red** > de la **autorización**.
3. Haga clic el **botón Create**.
4. Nombre el perfil de la autorización.
5. Haga clic la lengueta de los **atributos de RADIUS**.
6. Seleccione un diccionario del menú desplegable del **tipo de diccionario**.
7. Para fijar el selecto el atributo para el campo del atributo de RADIUS, hace clic el botón **selecto**. Una nueva ventana aparece.
8. Revise los atributos disponibles, haga su selección, y haga clic la **AUTORIZACIÓN**. El valor del **tipo del atributo** se fija por abandono, sobre la base de la selección del atributo que usted acaba de hacer.
9. Deje el descenso-abajo por el valor de atributo fijado a los **parásitos atmosféricos**. Si el valor es estático, usted puede ingresar el valor en el campo siguiente. Si el valor es dinámico, usted no puede ingresar el atributo manualmente; en lugar atribuido se asocia a un atributo en uno de los almacenes de la identidad.
10. Ingrese el valor del atributo en el campo más reciente.
11. Haga clic el **botón Add** para agregar la entrada a la tabla.
12. Relance para configurar todos los atributos que usted necesita.
13. Haga clic el **botón Submit Button** en la parte inferior de la pantalla.

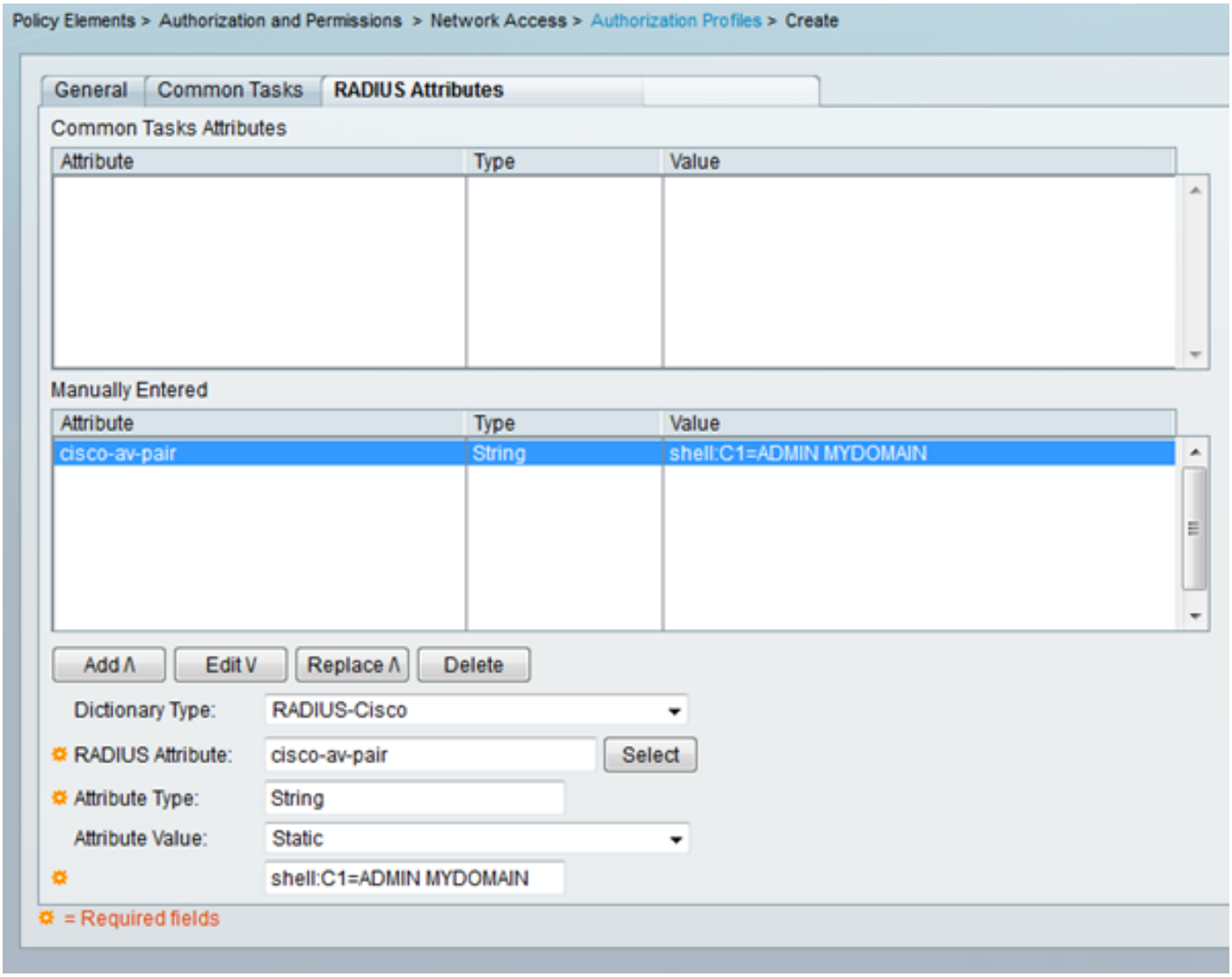
Ejemplo de configuración

Dispositivo: ACE

Atributos: `Cisco-av-pair`

Valor: `shell: <context-name>=<Role-name> <domain-name1> <domain-name2>`

Uso: Cada valor después del signo igual es separado por un carácter de espacio. Usted puede configurar a un usuario (por ejemplo, USER1) para ser asignado un papel (por ejemplo, ADMIN) y un dominio (por ejemplo, MYDOMAIN) cuando el usuario abre una sesión a un contexto (por ejemplo, c1).



Lista de dispositivos

La agregación mantiene al Routers (el ASR)

RADIUS (perfil de la autorización)

Atributos: `Cisco-av-pair`

Valor: `shell: #<role-name> del tasks= ", <permission>: <process>”`

Uso: Fije los valores del `<role-name> al` nombre de un papel localmente definido en el router. La jerarquía del papel se puede describir en términos de árbol, donde está el `#root del` papel en la cima del árbol, y el `#leaf del` papel agrega los comandos adicionales. Estos dos papeles pueden ser combinados y ser devueltos si: `shell: tasks= " #root, #leaf”`.

Los permisos se pueden también devolver sobre una base del proceso individual, de modo que un usuario pueda ser concedido leído, escribir, y ejecutar los procesos de los privilegios con certeza. Por ejemplo, para conceder a un usuario lea y escriba los privilegios para el proceso BGP, fijan el valor a: `shell: #root del tasks= ", RW: BGP”`. La orden de los atributos no importa; el resultado es lo mismo si el valor está fijado `para descascar: #root del tasks= ", RW: shell BGP”` o ro`: tasks= " RW: BGP, #root”`.

Ejemplo – *Agregue el atributo a un perfil de la autorización*

Tipo de diccionario	Atributo de RADIUS	Tipo del atributo	Valor de atributo
RADIUS-Cisco	`cisco-av-pair`	String (cadena)	`shell:tasks="#root,#leaf,rwx:bgp,r:ospf"`

Motor del control de la aplicación (ACE)

TACACS+ (perfil del shell)

Atributos: `shell: <context-name>`

Valor: `<Role-name> <domain-name1>`

Uso: El papel y el dominio son separados por un carácter de espacio. Usted puede configurar a un usuario (por ejemplo, USER1) para ser asignado un papel (por ejemplo, ADMIN) y un dominio (por ejemplo, MYDOMAIN) cuando el usuario abre una sesión a un contexto (por ejemplo, c1).

Ejemplo – *Agregue el atributo a un perfil del shell*

Atributo	Requisito	Valor de atributo
`shell:C1`	Obligatorio	`Admin MYDOMAIN`

Si el USER1 abre una sesión con el contexto del c1, asignan ese usuario automáticamente el papel y el dominio MYDOMAIN (a condición de que se ha configurado una regla de la autorización donde, una vez que el USER1 abre una sesión, ellos ADMIN se asignan este perfil de la autorización).

Si el USER1 abre una sesión con un diverso contexto, que no se vuelve en el valor del atributo que el ACS envía detrás, que asignan usuario automáticamente el papel predeterminado (Network Monitor) y el Default Domain (Default Domain).

RADIUS (perfil de la autorización)

Atributos: `Cisco-av-pair`

Valor: `shell: <context-name>=<Role-name> <domain-name1> <domain-name2>`

Uso: Cada valor después del signo igual es separado por un carácter de espacio. Usted puede configurar a un usuario (por ejemplo, USER1) para ser asignado un papel (por ejemplo, ADMIN) y un dominio (por ejemplo, MYDOMAIN) cuando los registros de usuario en un contexto (por ejemplo, c1).

Ejemplo – *Agregue el atributo a un perfil de la autorización*

Tipo de diccionario	Atributo de RADIUS	Tipo del atributo	Valor de atributo
RADIUS-Cisco	`cisco-av-pair`	String (cadena)	`shell:C1=ADMIN MYDOMAIN`

Si el USER1 abre una sesión con el contexto del c1, asignan ese usuario automáticamente el papel y el dominio MYDOMAIN (a condición de que se ha configurado una regla de la autorización donde, una vez que el USER1 abre una sesión, ellos ADMIN se asignan este perfil de la autorización).

Si el USER1 abre una sesión con un diverso contexto, que no se vuelve en el valor del atributo que el ACS envía detrás, que asignan usuario automáticamente el papel predeterminado (Network Monitor) y el Default Domain (Default Domain).

Shaper del paquete de BlueCoat

RADIUS (perfil de la autorización)

Atributos: `Packeteer-AVPair`

Valor: `access=<level>`

Uso: `el <level>` es el nivel de acceso a conceder. El acceso del tacto es equivalente a de lectura/grabación, mientras que el acceso de la mirada es equivalente a solo lectura.

El BlueCoat VSA no existe en los diccionarios ACS por abandono. Para utilizar el atributo de BlueCoat en un perfil de la autorización, usted debe crear un diccionario de BlueCoat y agregar los atributos de BlueCoat a ese diccionario.

Cree el diccionario:

1. Navegue a la **administración del sistema** > a la **configuración** > a los **diccionarios** > a los **protocolos** > al **RADIUS** > a **RADIUS VSA**.
2. El tecleo **crea**.
3. Ingrese los detalles del diccionario:Nombre: BlueCoatVendor ID: 2334Prefijo del atributo: Packeteer-
4. Haga clic en Submit (Enviar).

Cree un atributo en el nuevo diccionario:

1. Navegue a la **administración del sistema** > a la **configuración** > a los **diccionarios** > a los **protocolos** > a **RADIU** S > **RADIUS VSA** > **BlueCoat**.
2. El tecleo **crea**.
3. Ingrese los detalles del atributo:Atributo: `Packeteer-AVPair`Descripción: Utilizado para especificar el nivel de accesoAtributo del vendedor ID: 1Dirección: SALIENTEMúltiplo permitido: FalsoIncluya el atributo en el registro: MarcadoTipo del atributo: String (cadena)
4. Haga clic en Submit (Enviar).

Ejemplo – ***Agregue el atributo a un perfil de la autorización (para acceso de sólo lectura)***

Tipo de diccionario	Atributo de RADIUS	Tipo del atributo	Valor de atributo
RADIUS-BlueCoat	`Packeteer-AVPair`	String (cadena)	`access=look`

Ejemplo – ***Agregue el atributo a un perfil de la autorización (para el acceso de lectura/escritura)***

Tipo de	Atributo de	Tipo del	Valor de

diccionario	RADIUS	atributo	atributo
RADIUS-BlueCoat	`Packeteer-AVPair`	String (cadena)	`access=touch`

Switches del brocado

RADIUS (perfil de la autorización)

Atributos: `TÚNEL-SOLDADO-GRUPO-ID`

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

Uso: Fije `<VLAN1> al` valor del VLAN de dato. Fije `<VLAN2> al` valor del VLA N de la Voz. En este ejemplo, el VLAN de dato es VLAN10, y el VLA N de la Voz es el VLA N 21.

Ejemplo – ***Agregue el atributo a un perfil de la autorización***

Tipo de diccionario	Atributo de RADIUS	Tipo del atributo	Valor de atributo
RADIUS-IETF	`Tunnel-Private-Group-ID`	Cadena marcada con etiqueta	`U:10;T:21`

Cisco Unity Express (SEÑAL)

RADIUS (perfil de la autorización)

Atributos: `Cisco-av-pair`

Valor: `fndn: groups=<group-name>`

Uso: `<group-name>` está el nombre del grupo con los privilegios que usted quiere conceder al usuario. Este grupo debe ser configurado en el Cisco Unity Express (SEÑAL).

Ejemplo – ***Agregue el atributo a un perfil de la autorización***

Tipo de diccionario	Atributo de RADIUS	Tipo del atributo	Valor de atributo
RADIUS-Cisco	`cisco-av-pair`	String (cadena)	`fndn:groups=Administrators`

Infoblox

RADIUS (perfil de la autorización)

Atributos: `Infoblox-Grupo-Info`

Valor: `<group-name>`

Uso: `<group-name>` está el nombre del grupo con los privilegios que usted quiere conceder al usuario. Este grupo debe ser configurado en el dispositivo de Infoblox. En este ejemplo de configuración, el nombre del grupo es MyGroup.

El Infoblox VSA no existe en los diccionarios ACS por abandono. Para utilizar el atributo de Infoblox en un perfil de la autorización, usted debe crear un diccionario de Infoblox y agregar los atributos de Infoblox a ese diccionario.

Cree el diccionario:

1. Navegue a la **administración del sistema** > a la **configuración** > a los **diccionarios** > a los **protocolos** > al **RADIUS** > a **RADIUS VSA**.
2. El tecleo **crea**.
3. Haga clic la pequeña flecha al lado de las **opciones de distribuidor avanzadas uso**.
4. Ingrese los detalles del diccionario:Nombre: InfobloxVendor ID: 7779Tamaño de extensión del campo del vendedor: 1Tamaño de campo del tipo de vendedor: 1
5. Haga clic en Submit (Enviar).

Cree un atributo en el nuevo diccionario:

1. Navegue a la **administración del sistema** > a la **configuración** > a los **diccionarios** > a los **protocolos** > al **RADIUS** > al **RADIUS VSA** > **Infoblox**.
2. El tecleo **crea**.
3. Ingrese los detalles del atributo:Atributo: `Infoblox-Grupo-Info`Atributo del vendedor ID: 009Dirección: SALIENTEMúltiplo permitido: FalsoIncluya el atributo en el registro: MarcadoTipo del atributo: String (cadena)
4. Haga clic en Submit (Enviar).

Ejemplo – ***Agregue el atributo a un perfil de la autorización***

Tipo de diccionario	Atributo de RADIUS	Tipo del atributo	Valor de atributo
RADIUS-Infoblox	`Infoblox-Group-Info`	String (cadena)	`MyGroup`

Sistema de prevención de intrusiones (IPS)

RADIUS (perfil de la autorización)

Atributos: `IPS-papel`

Valor: `name> del <role`

Uso: `El name> del <role del` valor puede ser de los cuatro rol del usuario del Sistema de prevención de intrusiones (IPS): Visualizador, operador, administrador, o servicio. Refiera a la guía de configuración para su versión del IPS para los detalles de los permisos concedidos a cada rol del usuario del tipo.

- Guía de configuración del administrador de dispositivo del Cisco Intrusion Prevention System

para IPS 7.0
- Guía de configuración del administrador de dispositivo del Cisco Intrusion Prevention System para IPS 7.1

Ejemplo – *Agregue el atributo a un perfil de la autorización*

Tipo de diccionario	Atributo de RADIUS	Tipo del atributo	Valor de atributo
RADIUS-Cisco	`cisco-av-pair`	String (cadena)	`ips-role:administrator`

Enebro

TACACS+ (perfil del shell)

Atributos: `permitir-comandos`; `permitir-configuración`; `nombre de usuario local`; `comandos deny`; `negar-configuración`; `permisos del usuario`

Valor: `<allow-commands-regex>`; `<allow-configuration-regex>`; `<local-username>`; `<deny-commands-regex>`; `<deny-configuration-regex>`

Uso: Fije el valor del `<local-username>` (es decir, el valor del atributo de nombre de usuario local) a un nombre de usuario que exista localmente en el dispositivo del enebro. Por ejemplo, usted puede configurar a un usuario (por ejemplo, USER1) para ser asignado la misma plantilla del usuario que un usuario (por ejemplo, JUSER) que exista localmente en el dispositivo del enebro cuando usted fija el valor del atributo de nombre de usuario local a JUSER. Los valores de los permitir-comandos, de la permitir-configuración, de los comandos deny, y de los atributos de la negar-configuración se pueden ingresar en el formato del regex. Los valores que estos atributos están fijados a están además del operativo/de los comandos configuration mode autorizados por los bits de los permisos de la clase del login del usuario.

Ejemplo – *Agregue los atributos a un perfil 1 del shell*

Atributo	Requisito	Valor de atributo
`allow-commands`	Opcional	`"(request system) | (show rip neighbor)"`
`allow-configuration`	Opcional	
`local-user-name`	Opcional	`sales`
`deny-commands`	Opcional	`"<^clear"`
`deny-configuration`	Opcional	

Ejemplo – *Agregue los atributos a un perfil 2 del shell*

Atributo	Requisito	Valor de atributo
`allow-commands`	Opcional	`"monitor | help | show | ping | traceroute"`
`allow-configuration`	Opcional	
`local-user-name`	Opcional	`engineering`
`deny-commands`	Opcional	`"configure"`
`deny-configuration`		

	Opcional	

Switches del nexo

RADIUS (perfil de la autorización)

Atributos: `Cisco-av-pair`

Valor: `shell:roles="<role1> el <role2>"`

Uso: Fije los valores de `<role1>` y de `<role2> a los` nombres de los papeles localmente definidos en el Switch. Cuando usted agrega los papeles múltiples, sepárelos con un carácter de espacio. Cuando los papeles múltiples se devuelven del servidor de AAA al Switch del nexo, el resultado es que el usuario tiene acceso a los comandos definidos por la unión de los tres papeles.

Los papeles incorporados se definen en configurar las cuentas de usuario y RBAC.

Ejemplo – ***Agregue el atributo a un perfil de la autorización***

Tipo de diccionario	Atributo de RADIUS	Tipo del atributo	Valor de atributo
RADIUS-Cisco	`cisco-av-pair`	String (cadena)	`shell:roles="network-admin vdc-admin vdc-operator"`

Cauce del río

TACACS+ (perfil del shell)

Atributos: `servicio`; `nombre de usuario local`

Valor: `RBT-EXEC`; `<username>`

Uso: Para conceder al usuario acceso de sólo lectura, el valor del `<username>` se debe fijar para monitorear. Para conceder el acceso de lectura/escritura del usuario, el valor del `<username>` se debe fijar al admin. Si usted tiene otra cuenta definida además del admin y del monitor, configure que nombre que se volverá.

Ejemplo – ***Agregue los atributos a un perfil del shell (para acceso de sólo lectura)***

Atributo	Requisito	Valor de atributo
`service`	Obligatorio	`rbt-exec`
`local-user-name`	Obligatorio	`monitor`

Ejemplo – ***Agregue los atributos a un perfil del shell (para el acceso de lectura/escritura)***

Atributo	Requisito	Valor de atributo
`service`	Obligatorio	`rbt-exec`
`local-user-name`	Obligatorio	`admin`

Regulador del Wireless LAN (WLC)

RADIUS (perfil de la autorización)

Atributos: `Tipo de servicio`

Valor: `(6) administrativo`/NAS-`prompt (7)`

Uso: Para conceder al usuario el acceso de lectura/grabación al regulador del Wireless LAN (WLC), el valor debe ser administrativo; para acceso de sólo lectura, el valor debe ser NAS-prompt.

Para los detalles, vea la autenticación de servidor de RADIUS de los usuarios de administración en el ejemplo de configuración del regulador del Wireless LAN (WLC)

Ejemplo – ***Agregue el atributo a un perfil de la autorización (para acceso de sólo lectura)***

Tipo de diccionario	Atributo de RADIUS	Tipo del atributo	Valor de atributo
RADIUS-IETF	`Service-Type`	Enumeración	`NAS-Prompt`

Ejemplo – ***Agregue el atributo a un perfil de la autorización (para el acceso de lectura/escritura)***

Tipo de diccionario	Atributo de RADIUS	Tipo del atributo	Valor de atributo
RADIUS-IETF	`Service-Type`	Enumeración	`Administrative`

Administrador de la red del centro de datos (DCNM)

DCNM debe ser recomenzado después de que se cambie el método de autentificación. Si no, puede asignar el privilegio del operador de la red en vez del red-admin.

Papel DCNM	Cisco-av-pair RADIUS	Cisco-av-pair de Tacacs
Usuario	`shell:roles = "network-operator"`	`cisco-av-pair=shell:roles="network-operator"`
Administrador	`shell:roles = "network-admin"`	`cisco-av-pair=shell:roles="network-admin"`

Información Relacionada

- Soporte Técnico y Documentación - Cisco Systems
- Terminal Access Controller Access Control System (TACACS+)
- Remote Authentication Dial-In User Service (RADIUS)
- Solicitudes de Comentarios (RFC)