

TACACS+ e atributos RADIUS para vários Cisco e o exemplo de configuração dos dispositivos que não é da Cisco

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Crie um perfil do shell \(o TACACS+\)](#)

[Exemplo de configuração](#)

[Crie um perfil da autorização \(o RAI0\)](#)

[Exemplo de configuração](#)

[Lista de dispositivos](#)

[A agregação presta serviços de manutenção ao Roteadores \(o ASR\)](#)

[Motor do controle de aplicativo \(ACE\)](#)

[Shaper do pacote de BlueCoat](#)

[Switches de brocado](#)

[Cisco Unity Express \(SUGESTÃO\)](#)

[Infoblox](#)

[Intrusion Prevention System \(IPS\)](#)

[Zimbro](#)

[Switches do nex0](#)

[Leito fluvial](#)

[Controlador do Wireless LAN \(WLC\)](#)

[Informações Relacionadas](#)

[Introdução](#)

Este documento fornece uma compilação dos atributos que vários Cisco e o Produtos não-Cisco esperam receber de um servidor de Autenticação, Autorização, and Accounting (AAA); neste caso, o servidor AAA é um Access Control Server (ACS). O ACS pode retornar estes atributos junto com uma aceitação de acesso enquanto parte de um perfil do shell (TACACS+) ou perfil da autorização (RAIO).

Este documento fornece instruções passo a passo em como adicionar atributos feitos sob encomenda para descascar perfis e perfis da autorização. Este documento igualmente contém uma lista de dispositivos e o TACACS+ e os atributos RADIUS que os dispositivos esperam ver retornado do servidor AAA. Todos os assuntos incluem exemplos.

A lista de atributos fornecidos neste documento não é exaustiva ou competente e pode mudar a qualquer hora sem uma atualização a este documento.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

A informação neste documento é baseada na versão de ACS 5.2/5.3.

Convenções

Consulte as [Convenções de Dicas Técnicas da Cisco](#) para obter mais informações sobre convenções de documentos.

Crie um perfil do shell (o TACACS+)

Um perfil do shell é um recipiente básico das permissões para o acesso TACACS+-based. Você pode especificar que TACACS+ atribui e os valores de atributo devem ser retornados com a aceitação de acesso, além do que o nível de privilégio do [®] IO de Cisco, o timeout de sessão, e os outros parâmetros.

Termine estas etapas a fim adicionar atributos feitos sob encomenda a um perfil novo do shell:

1. Entre à relação ACS.
2. Navegue aos **elementos da política > à autorização e às permissões > à administração > ao shell do dispositivo perfis**.
3. Clique o **botão Create**.
4. Nomeie o perfil do shell.
5. Clique a aba dos **atributos feitos sob encomenda**.
6. Dê entrada com o nome do atributo no campo do **atributo**.
7. Escolha se a exigência é **imperativa** ou **opcional** da lista de drop-down da exigência.
8. Deixe a gota-para baixo para o valor de atributo ajustado à **estática**. Se o valor é estático, você pode incorporar o valor ao campo seguinte. Se o valor é dinâmico, você não pode incorporar o atributo manualmente; em lugar de atribuído é traçado a um atributo em uma das lojas da identidade.
9. Incorpore o valor do atributo ao último campo.
10. Clique o **botão Add** a fim adicionar a entrada à tabela.
11. Repita para configurar todos os atributos que você precisa.
12. Clique o **botão Submit Button** na parte inferior da tela.

Exemplo de configuração

Dispositivo: Motor do controle de aplicativo (ACE)

Atributos: shell: <context-name>

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

Uso: O papel e o domínio são separados por um caractere de espaço. Você pode configurar um usuário (por exemplo, USUÁRIO1) para ser atribuído um papel (por exemplo, ADMIN) e um domínio (por exemplo, MYDOMAIN) quando o usuário entra a um contexto (por exemplo, C1).

[Crie um perfil da autorização \(o RAI0\)](#)

Um perfil da autorização é um recipiente básico das permissões para o acesso Raio-baseado. Você pode especificar que atributos RADIUS e valores de atributo devem ser retornados com a aceitação de acesso, além do que os VLAN, o Access Control Lists (ACLs), e os outros parâmetros.

Termine estas etapas a fim adicionar atributos feitos sob encomenda a um perfil novo da autorização:

1. Entre à relação ACS.
2. Navegue aos **elementos da política > à autorização e às permissões > aos perfis do acesso de rede > da autorização**.
3. Clique o **botão Create**.
4. Nomeie o perfil da autorização.
5. Clique a aba dos **atributos RADIUS**.
6. Selecione um dicionário do menu suspenso do **tipo de dicionário**.
7. A fim ajustar o seletor do atributo para o campo do atributo RADIUS, clique o botão **seleto**. Uma nova janela aparece.
8. Reveja os atributos disponíveis, faça sua seleção, e clique a **APROVAÇÃO**. O **tipo** valor do **atributo** é ajustado à revelia, com base na seleção do atributo que você apenas fez.
9. Deixe a gota-para baixo para o valor de atributo ajustado à **estática**. Se o valor é estático, você pode incorporar o valor ao campo seguinte. Se o valor é dinâmico, você não pode incorporar o atributo manualmente; em lugar de atribuído é traçado a um atributo em uma das lojas da identidade.
10. Incorpore o valor do atributo ao último campo.
11. Clique o **botão Add** a fim adicionar a entrada à tabela.
12. Repita para configurar todos os atributos que você precisa.
13. Clique o **botão Submit Button** na parte inferior da tela.

[Exemplo de configuração](#)

Dispositivo: ACE

Atributos: Cisco-av-pair

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

Uso: Cada valor após o sinal de igual é separado por um caractere de espaço. Você pode configurar um usuário (por exemplo, USUÁRIO1) para ser atribuído um papel (por exemplo, ADMIN) e um domínio (por exemplo, MYDOMAIN) quando o usuário entra a um contexto (por

exemplo, C1).

Lista de dispositivos

A agregação presta serviços de manutenção ao Roteadores (o ASR)

RAIO (perfil da autorização)

Atributos: Cisco-av-pair

Valor: shell: #<role-name> do tasks= ", <permission>: <process>"

Uso: Ajuste os valores do <role-name> ao nome de um papel definido localmente no roteador. A hierarquia do papel pode ser descrita em termos de uma árvore, onde o #root do papel esteja na parte superior da árvore, e o #leaf do papel adicione comandos adicionais. Estes dois papéis podem ser combinados e passado para trás se: shell: tasks= " #root, #leaf".

As permissões podem igualmente ser passadas para trás em uma base do processo individual, de modo que um usuário possa ser concedido lido, escrito, e executado processos dos privilégios com certeza. Por exemplo, a fim conceder um usuário leia e escreva privilégios para o processo BGP, ajustam o valor a: shell: #root do tasks= ", RW: BGP". A ordem dos atributos não importa; o resultado é o mesmo se o valor está ajustado para descascar: #root do tasks= ", RW: shell BGP" OU RO: tasks= " RW: BGP, #root".

Exemplo – Adicionar o atributo a um perfil da autorização

Tipo de dicionário	Atributo RADIUS	Tipo do atributo	Valor de atributo
Raio-Cisco	cisco-av-pair	Série	shell:tasks="#root,#leaf,rwx:bgp,r:ospf"

Motor do controle de aplicativo (ACE)

TACACS+ (perfil do shell)

Atributos: shell: <context-name>

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

Uso: O papel e o domínio são separados por um caractere de espaço. Você pode configurar um usuário (por exemplo, USUÁRIO1) para ser atribuído um papel (por exemplo, ADMIN) e um domínio (por exemplo, MYDOMAIN) quando o usuário entra a um contexto (por exemplo, C1).

Exemplo – Adicionar o atributo a um perfil do shell

Atributo	Exigência	Valor de atributo
shell:C1	Obrigatório	Admin MYDOMAIN

Se o USUÁRIO1 entra com o contexto C1, esse usuário está atribuído automaticamente o papel

ADMIN e o domínio MYDOMAIN (contanto que uma regra da autorização esteve configurada onde, uma vez que o USUÁRIO1 entra, eles são atribuídos este perfil da autorização).

Se o USUÁRIO1 entra com um contexto diferente, que não esteja retornado no valor do atributo que o ACS envia para trás, que usuário está atribuído automaticamente o papel do padrão (monitor de rede) e o domínio padrão (domínio padrão).

RAIO (perfil da autorização)

Atributos: Cisco-av-pair

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

Uso: Cada valor após o sinal de igual é separado por um caractere de espaço. Você puder configurar um usuário (por exemplo, USUÁRIO1) para ser atribuído um papel (por exemplo, ADMIN) e um domínio (por exemplo, MYDOMAIN) quando os log de usuário em um contexto (por exemplo, C1).

Exemplo – Adicionar o atributo a um perfil da autorização

Tipo de dicionário	Atributo RADIUS	Tipo do atributo	Valor de atributo
Raio-Cisco	cisco-av-pair	Série	shell:C1=ADMIN MYDOMAIN

Se o USUÁRIO1 entra com o contexto C1, esse usuário está atribuído automaticamente o papel ADMIN e o domínio MYDOMAIN (contanto que uma regra da autorização esteve configurada onde, uma vez que o USUÁRIO1 entra, eles são atribuídos este perfil da autorização).

Se o USUÁRIO1 entra com um contexto diferente, que não esteja retornado no valor do atributo que o ACS envia para trás, que usuário está atribuído automaticamente o papel do padrão (monitor de rede) e o domínio padrão (domínio padrão).

[Shaper do pacote de BlueCoat](#)

RAIO (perfil da autorização)

Atributos: Packeteer-AVPair

Valor: access=<level>

Uso: o <level> é o nível do acesso a conceder. O acesso do toque é equivalente a de leitura/gravação, quando o acesso do olhar for equivalente a de leitura apenas.

O BlueCoat VSA não existe nos dicionários ACS à revelia. A fim usar o atributo de BlueCoat em um perfil da autorização, você deve criar um dicionário de BlueCoat e adicionar os atributos de BlueCoat a esse dicionário.

Crie o dicionário:

1. Navegue à **administração do sistema > à configuração > aos dicionários > aos protocolos > ao RAIO > ao RAIO VSA.**
2. O clique **cria**.

- Incorpore os detalhes do dicionário: Nome: BlueCoat Vendor ID: 2334 Prefixo do atributo: Packeteer-
- Clique em Submit.

Crie um atributo no dicionário novo:

- Navegue à **administração do sistema** > à **configuração** > aos **dicionários** > aos **protocolos** > ao **RADIUS** > **RAIO VSA** > **BlueCoat**.
- O clique **cria**.
- Incorpore os detalhes do atributo: Atributo: Packeteer-AVPair Descrição: Usado a fim especificar o nível de acesso Atributo de fornecedor ID: 1 Direção: SAÍDA Múltiplo permitido: Falso Inclua o atributo no log: Verificado Tipo do atributo: Série
- Clique em Submit.

Exemplo – Adicionar o atributo a um perfil da autorização (para o acesso somente leitura)

Tipo de dicionário	Atributo RADIUS	Tipo do atributo	Valor de atributo
Raio-BlueCoat	Packeteer-AVPair	Série	access=look

Exemplo – Adicionar o atributo a um perfil da autorização (para o acesso de leitura/gravação)

Tipo de dicionário	Atributo RADIUS	Tipo do atributo	Valor de atributo
Raio-BlueCoat	Packeteer-AVPair	Série	access=touch

[Switches de brocado](#)

RAIO (perfil da autorização)

Atributos: Túnel-Privado-Grupo-ID

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

Uso: Ajuste <VLAN1> ao valor do VLAN de dados. Ajuste <VLAN2> ao valor da Voz VLAN. Neste exemplo, o VLAN de dados é VLAN10, e a Voz VLAN é VLAN 21.

Exemplo – Adicionar o atributo a um perfil da autorização

Tipo de dicionário	Atributo RADIUS	Tipo do atributo	Valor de atributo
RADIUS-IETF	Tunnel-Private-Group-ID	Corda etiquetada	U:10;T:21

[Cisco Unity Express \(SUGESTÃO\)](#)

RAIO (perfil da autorização)

Atributos: Cisco-av-pair

Valor: fndn: groups=<group-name>

Uso: o <group-name> é o nome do grupo com os privilégios que você quer conceder ao usuário. Este grupo deve ser configurado no Cisco Unity Express (SUGESTÃO).

Exemplo – Adicionar o atributo a um perfil da autorização

Tipo de dicionário	Atributo RADIUS	Tipo do atributo	Valor de atributo
Raio-Cisco	cisco-av-pair	Série	fndn:groups=Administrators

Infoblox

RAIO (perfil da autorização)

Atributos: Infoblox-Grupo-informação

Valor: <group-name>

Uso: o <group-name> é o nome do grupo com os privilégios que você quer conceder ao usuário. Este grupo deve ser configurado no dispositivo de Infoblox. Neste exemplo de configuração, o nome do grupo é MyGroup.

O Infoblox VSA não existe nos dicionários ACS à revelia. A fim usar o atributo de Infoblox em um perfil da autorização, você deve criar um dicionário de Infoblox e adicionar os atributos de Infoblox a esse dicionário.

Crie o dicionário:

1. Navegue à **administração do sistema > à configuração > aos dicionários > aos protocolos > ao RAIO > ao RAIO VSA.**
2. O clique **cria.**
3. Clique a seta pequena ao lado das **opções de fornecedor avançadas uso.**
4. Incorpore os detalhes do dicionário: Nome: InfobloxVendedor ID: 7779 Tamanho de campo de comprimento do vendedor: 1 Tipo de vendedor tamanho de campo: 1
5. Clique em Submit.

Crie um atributo no dicionário novo:

1. Navegue à **administração do sistema > à configuração > aos dicionários > aos protocolos > ao RAIO > ao RAIO VSA > Infoblox.**
2. O clique **cria.**
3. Incorpore os detalhes do atributo: Atributo: Infoblox-Grupo-informação Atributo de fornecedor ID: 009 Direção: SAÍDA Múltiplo permitido: Falso Inclua o atributo no log: Verificado Tipo do atributo: Série
4. Clique em Submit.

Exemplo – Adicionar o atributo a um perfil da autorização

Tipo de dicionário	Atributo RADIUS	Tipo do atributo	Valor de atributo
Raio-Infoblox	Infoblox-Group-Info	Série	MyGroup

Intrusion Prevention System (IPS)

RAIO (perfil da autorização)

Atributos: IP-papel

Valor: name> do <role

Uso: O name> do <role do valor pode ser qualquer dos quatro papéis de usuário do Intrusion Prevention System (IPS): visor, operador, administrador, ou serviço. Refira o manual de configuração para sua versão do IPS para os detalhes das permissões concedidas a cada papel de usuário do tipo.

- [Manual de configuração do gerenciador de dispositivo do Sistema de prevenção de intrusões da Cisco para IPS 7.0](#)
- [Manual de configuração do gerenciador de dispositivo do Sistema de prevenção de intrusões da Cisco para IPS 7.1](#)

Exemplo – Adicionar o atributo a um perfil da autorização

Tipo de dicionário	Atributo RADIUS	Tipo do atributo	Valor de atributo
Raio-Cisco	cisco-av-pair	Série	ips-role:administrator

Zimbro

TACACS+ (perfil do shell)

Atributos: permitir-comandos; permitir-configuração; nome de usuário local; comandos deny; negar-configuração; USER-permissões

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

Uso: Ajuste o valor do <local-username> (isto é, o valor do atributo de nome de usuário local) a um username que exista localmente no dispositivo do zimbro. Por exemplo, você pode configurar um usuário (por exemplo, USUÁRIO01) para ser atribuído o mesmo molde do usuário que um usuário (por exemplo, JUSER) que exista localmente no dispositivo do zimbro quando você ajusta o valor do atributo de nome de usuário local a JUSER. Os valores dos permitir-comandos, da permitir-configuração, dos comandos deny, e dos atributos da negar-configuração podem ser incorporados ao formato do regex. Os valores que estes atributos estão ajustados a são além do que o operacional/comandos configuration mode autorizados pelos bit das permissões da classe do início de uma sessão do usuário.

Exemplo – Adicionar atributos a um perfil 1 do shell

Atributo	Exigência	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	

Exemplo – Adicionar atributos a um perfil 2 do shell

Atributo	Exigência	Valor de atributo
allow-commands	Opcional	"monitor help show ping tracertoute"
allow-configuration	Opcional	
local-user-name	Opcional	engineering
deny-commands	Opcional	"configure"
deny-configuration	Opcional	

Switches do nexa

RAIO (perfil da autorização)

Atributos: Cisco-av-pair

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

Uso: Ajuste os valores de <role1> e de <role2> aos nomes dos papéis definidos localmente no interruptor. Quando você adiciona papéis múltiplos, separe-os com um caractere de espaço. Quando os papéis múltiplos são passados para trás do servidor AAA ao nexa comute, o resultado é que o usuário tem o acesso aos comandos definidos pela união de todos os três papéis.

Os papéis do acessório são definidos em [configurar contas de usuário e RBAC](#).

Exemplo – Adicionar o atributo a um perfil da autorização

Tipo de dicionário	Atributo RADIUS	Tipo do atributo	Valor de atributo
Raio-Cisco	cisco-av-pair	Série	shell:roles="network-admin vdc-admin vdc-operator"

Leito fluvial

TACACS+ (perfil do shell)

Atributos: serviço; nome de usuário local

Valor: RBT-EXEC; <username>

Uso: A fim conceder o acesso somente leitura do usuário, o valor do <username> deve ser ajustado para monitorar. A fim conceder o acesso de leitura/gravação do usuário, o valor do <username> deve ser ajustado ao admin. Se você tem uma outra conta definida além do que o admin e o

monitor, configurar que nome a ser retornado.

Exemplo – Adicionar atributos a um perfil do shell (para o acesso somente leitura)

Atributo	Exigência	Valor de atributo
service	Obrigatório	rbt-exec
local-user-name	Obrigatório	monitor

Exemplo – Adicionar atributos a um perfil do shell (para o acesso de leitura/gravação)

Atributo	Exigência	Valor de atributo
service	Obrigatório	rbt-exec
local-user-name	Obrigatório	admin

Controlador do Wireless LAN (WLC)

RAIO (perfil da autorização)

Atributos: Tipo de serviço

Valor: (6) administrativo/alerta (7)

Uso: A fim conceder ao usuário o acesso de leitura/gravação ao controlador do Wireless LAN (WLC), o valor deve ser administrativo; para o acesso somente leitura, o valor deve ser NAS-alerta.

Para detalhes, veja a [autenticação de servidor Radius de usuários do Gerenciamento no exemplo de configuração do controlador do Wireless LAN \(WLC\)](#)

Exemplo – Adicionar o atributo a um perfil da autorização (para o acesso somente leitura)

Tipo de dicionário	Atributo RADIUS	Tipo do atributo	Valor de atributo
RADIUS-IETF	Service-Type	Enumeração	NAS-Prompt

Exemplo – Adicionar o atributo a um perfil da autorização (para o acesso de leitura/gravação)

Tipo de dicionário	Atributo RADIUS	Tipo do atributo	Valor de atributo
RADIUS-IETF	Service-Type	Enumeração	Administrative

Gerente de rede do centro de dados (DCNM)

DCNM deve ser reiniciado depois que o método de autenticação é mudado. Se não, pode atribuir o privilégio do operador de rede em vez do rede-admin.

Papel DCNM	Cisco-av-pair do RAIO	Cisco-av-pair de Tacacs
Usuário	shell:roles = "network-operator"	cisco-av-pair=shell:roles="network-operator"
Administr	shell:roles	cisco-av-

ador	= "network-admin"	pair=shell:roles="network-admin"
------	-------------------	----------------------------------

Informações Relacionadas

- [Suporte Técnico e Documentação - Cisco Systems](#)
- [Terminal Access Controller Access Control System \(TACACS+\)](#)
- [Remote Authentication Dial-In User Service \(RADIUS\)](#)
- [Solicitações de Comentários \(RFCs\)](#)