ASA 8.0: Configurar a autenticação RADIUS para usuários WebVPN

Índice

Introdução

Este documento demonstra como configurar a ferramenta de segurança adaptável de Cisco (ASA) para usar um servidor para autenticação do Remote Authentication Dial-In User Service (RADIUS) de usuários WebVPN. O servidor Radius neste exemplo é um server do Access Control Server de Cisco (ACS), versão 4.1 que esta configuração é executada com o Security Device Manager adaptável (ASDM) 6.0(2) em um ASA que execute a versão de software 8.0(2).

Nota: Neste exemplo a autenticação RADIUS é configurada para usuários WebVPN, mas esta configuração pode ser usada para outros tipos de acesso remoto VPN também. Atribua simplesmente o Grupo de servidores AAA ao perfil de conexão desejado (grupo de túneis) como mostrado.

Pré-requisitos

- Uma configuração básica WebVPN é exigida.
- Cisco ACS deve ter os usuários configurados para a autenticação de usuário. Refira adicionar uma seção básica da conta de usuário do gerenciamento de usuário para mais informação.

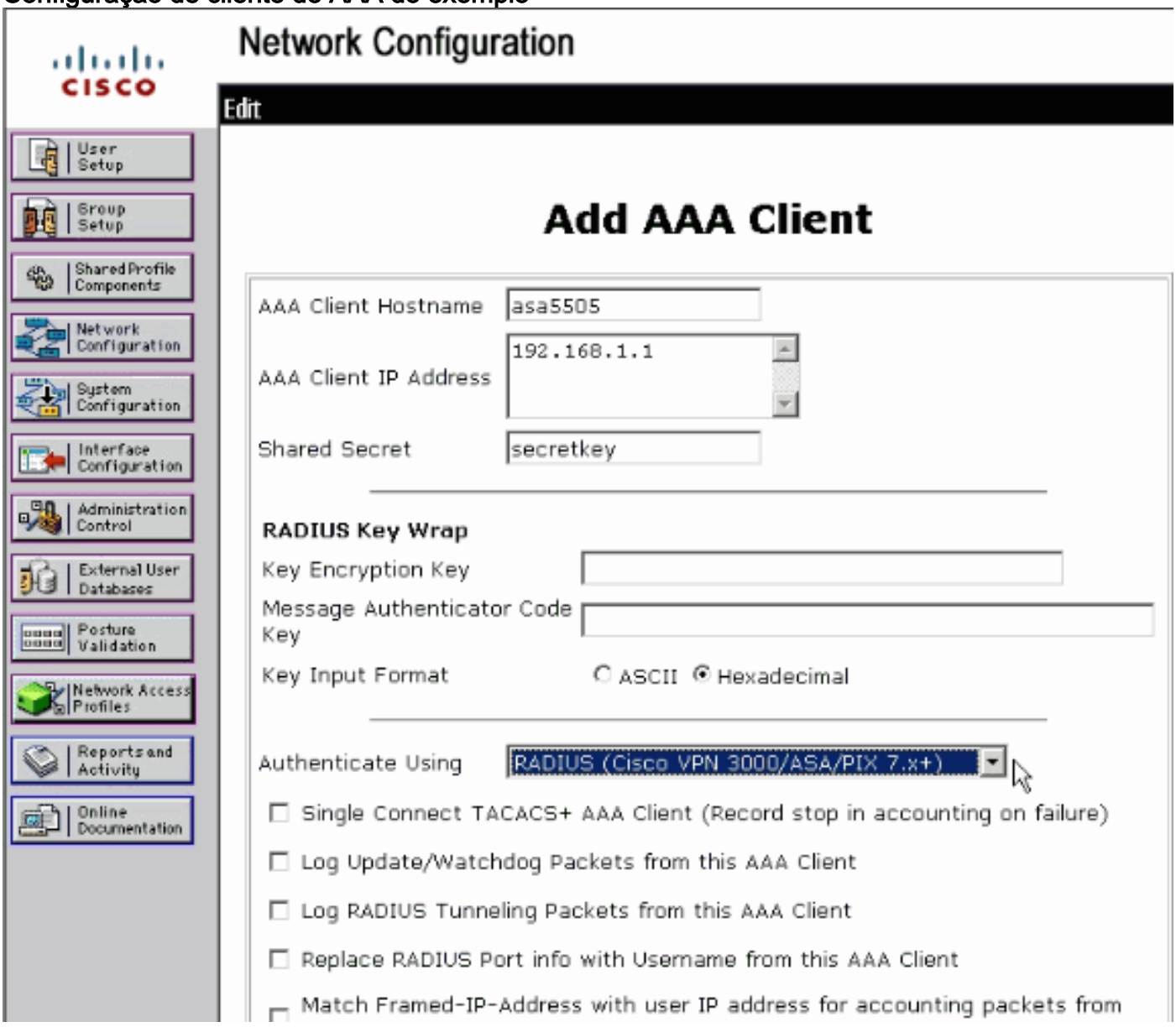
Configurar o servidor ACS

Nesta seção, você é presentado com a informação para configurar a autenticação RADIUS no ACS e no ASA.

Termine estas etapas a fim configurar o servidor ACS para comunicar-se com o ASA.

1. Escolha a **configuração de rede do** menu esquerdo da tela ACS.
2. Escolha **adicionam a entrada** sob **clientes de AAA**.
3. Forneça a informação cliente:**Nome de host do cliente AAA** — um nome de sua escolha**Endereço IP de Um ou Mais Servidores Cisco ICM NT do cliente de AAA** — o endereço de que a ferramenta de segurança contacta o ACS**Segredo compartilhado** — uma chave secreta configurada no ACS e na ferramenta de segurança
4. **Na utilização da autenticação** dropdown escolha o **RAIO (Cisco VPN 3000/ASA/PIX 7.x+)**.
5. Clique **Submit+Apply**.

Configuração de cliente de AAA do exemplo



Configurar a ferramenta de segurança

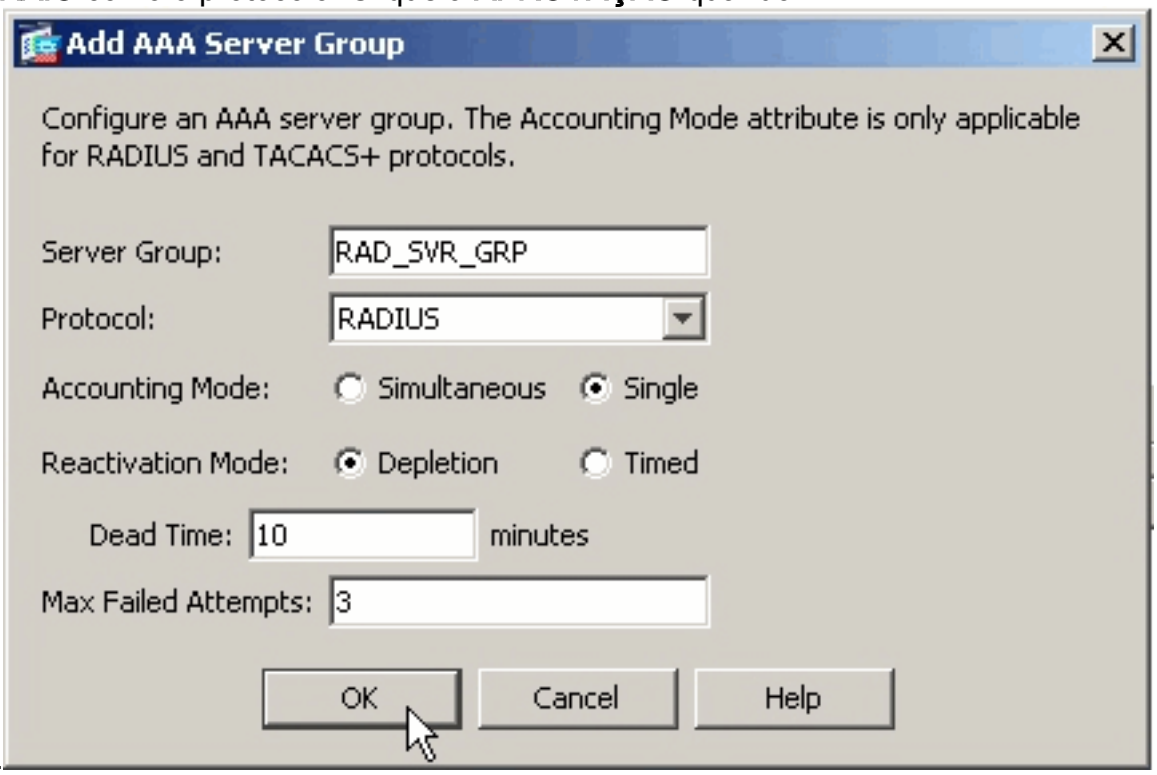
ASDM

Termine estas etapas no ASDM a fim configurar o ASA para comunicar-se com o servidor ACS e para autenticar clientes WebVPN.

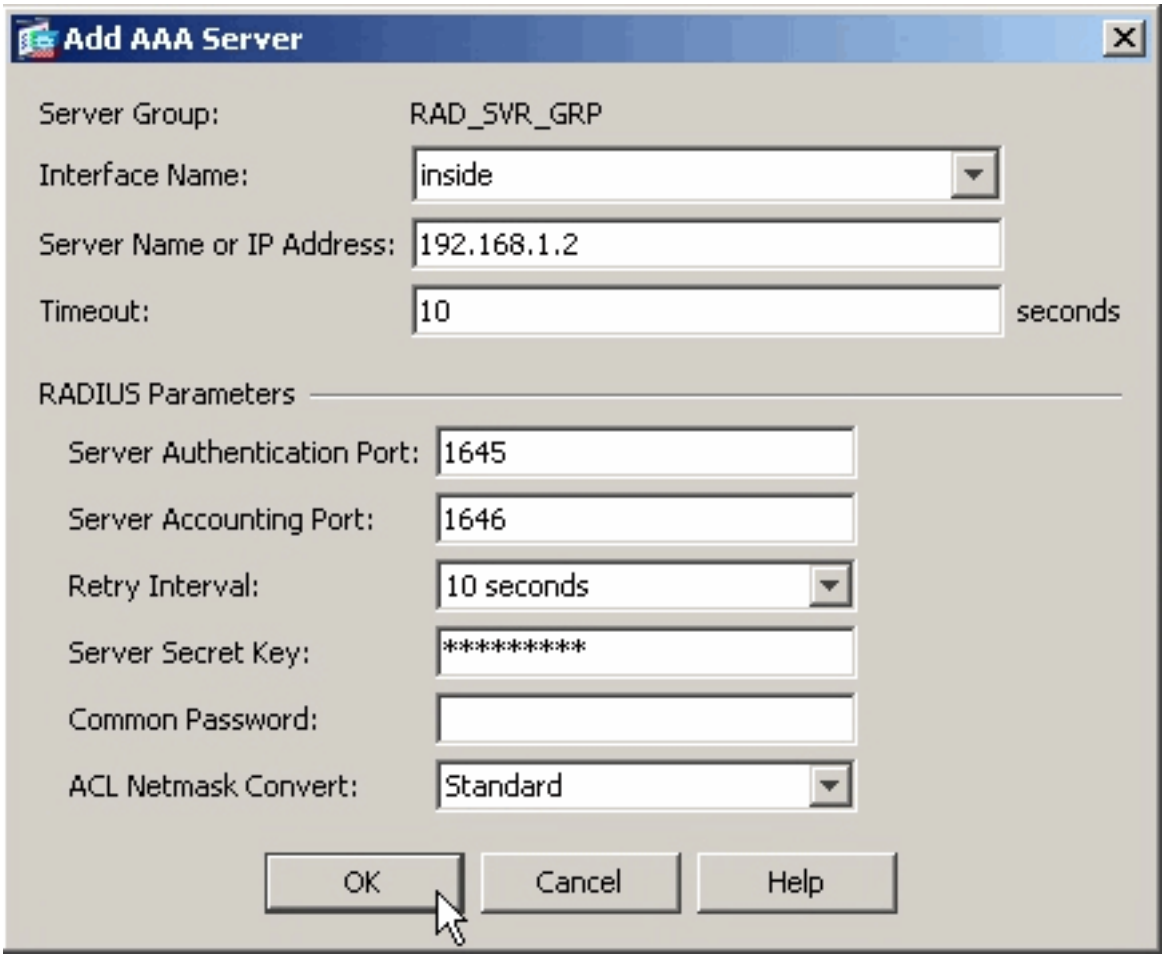
1. Escolha a **configuração > o acesso remoto VPN > o AAA Setup > Grupos de servidores**

AAA.

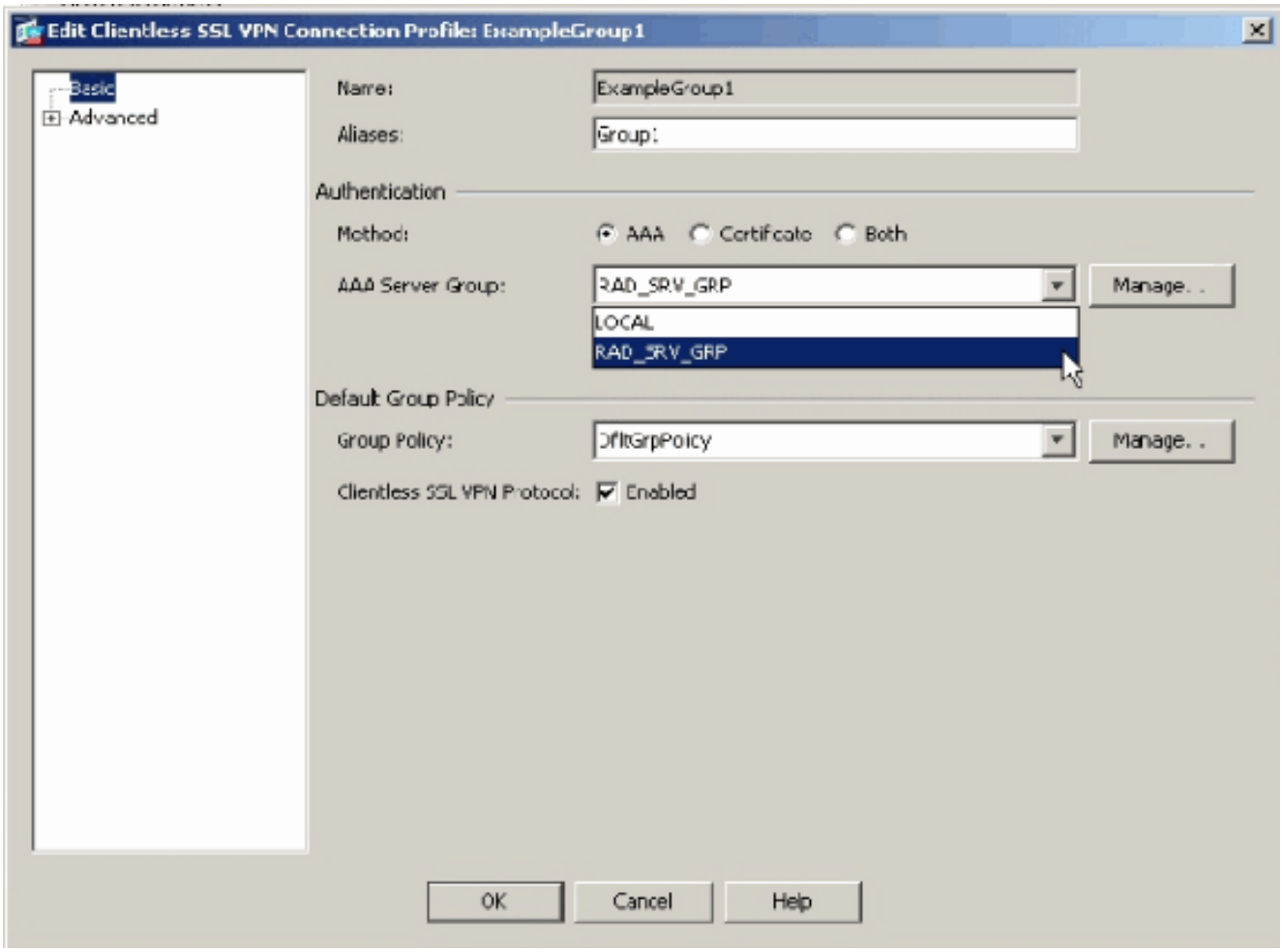
2. O clique **adiciona** ao lado dos Grupos de servidores AAA.
3. No indicador que aparece, especifique um nome para o Grupo de servidores AAA novo e escolha o **RAIO** como o protocolo. Clique a **APROVAÇÃO** quando terminado.



4. Seja certo que seu grupo novo está selecionado na placa superior e o clique **adiciona** à direita da placa mais baixa.
5. Forneça a informação do servidor:**Nome da relação** — a relação que o ASA deve usar para alcançar o servidor ACS**Nome do servidor ou endereço IP de Um ou Mais Servidores Cisco ICM NT** — o endereço que o ASA deve usar para alcançar o servidor ACS**Chave do segredo de servidor** — a chave secreta compartilhada configurada para o ASA no servidor ACS**Configuração do servidor AAA do exemplo no ASA**



6. Uma vez que você configurou o Grupo de servidores AAA e o server, navegue à configuração > ao acesso remoto VPN > ao acesso > aos perfis de conexão dos sem clientes SSL VPN a fim configurar o WebVPN para usar a configuração de AAA nova.**Nota:** Mesmo que este exemplo use o WebVPN, você pode ajustar todo o perfil da conexão de acesso remoto (grupo de túneis) para usar esta instalação AAA.
7. Escolha o perfil para que você quer configurar o AAA, e o clique **edita**.
8. Sob a **autenticação** escolha o grupo de servidor Radius que você criou mais cedo. Clique a **APROVAÇÃO** quando
terminado.



Interface da linha de comando

Termine estas etapas no comando line interface(cli) a fim configurar o ASA para comunicar-se com o servidor ACS e para autenticar clientes WebVPN.

```
ciscoasa#configure terminal !--- Configure the AAA Server group. ciscoasa(config)# aaa-server
RAD_SRV_GRP protocol RADIUS ciscoasa(config-aaa-server-group)# exit !--- Configure the AAA
Server. ciscoasa(config)# aaa-server RAD_SRV_GRP (inside) host 192.168.1.2 ciscoasa(config-aaa-
server-host)# key secretkey ciscoasa(config-aaa-server-host)# exit !--- Configure the tunnel
group to use the new AAA setup. ciscoasa(config)# tunnel-group ExampleGroup1 general-attributes
ciscoasa(config-tunnel-general)# authentication-server-group RAD_SRV_GRP
```

Verificar

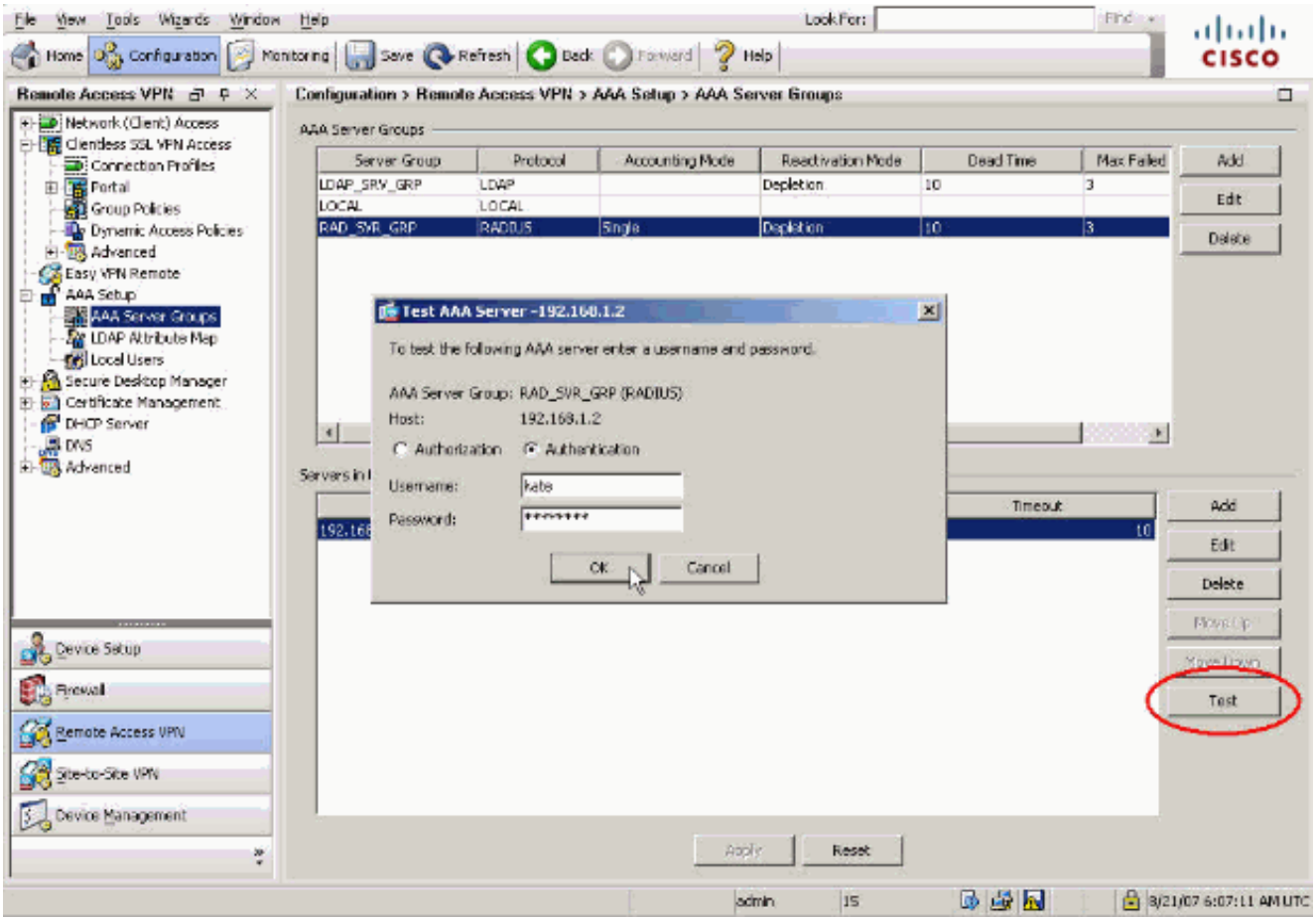
Use esta seção para confirmar se a sua configuração funciona corretamente.

Teste com ASDM

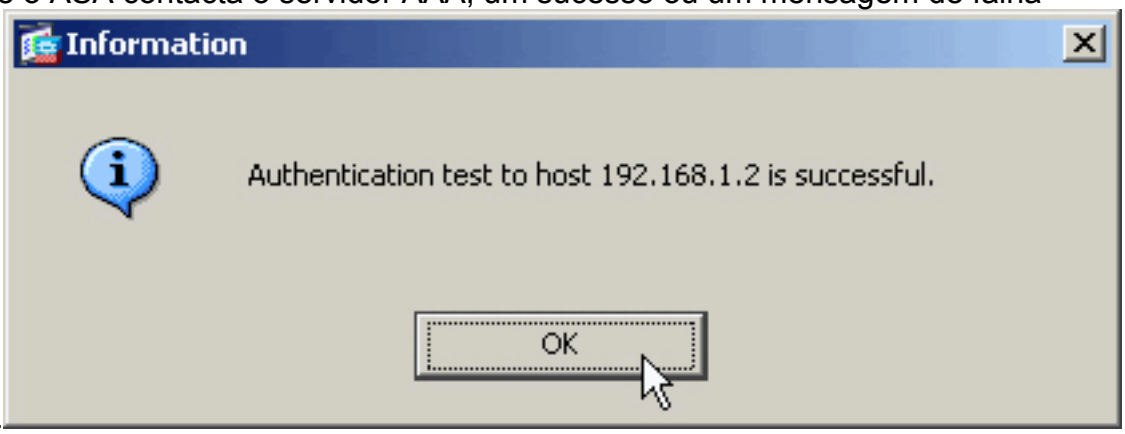
Verifique sua configuração RADIUS com o **botão Test Button na** tela de configuração dos Grupos de servidores AAA. Uma vez que você fornece um nome de usuário e senha, este botão permite que você envie um pedido da autenticação de teste ao servidor ACS.

1. Escolha a **configuração > o acesso remoto VPN > o AAA Setup > Grupos de servidores AAA**.
2. Selecione seu Grupo de servidores AAA desejado na placa superior.
3. Selecione o servidor AAA que você quer testar na placa mais baixa.

4. Clique o **botão Test Button** à direita da placa mais baixa.
5. No indicador que aparece, clique o botão de rádio da **autenticação**, e forneça as credenciais com que você quer testar. Clique a **APROVAÇÃO** quando terminado.



6. Depois que o ASA contacta o servidor AAA, um sucesso ou um mensagem de falha aparecem.



Teste com CLI

Você pode usar o **comando test na** linha de comando a fim testar sua instalação AAA. Um pedido do teste é enviado ao servidor AAA, e o resultado aparece na linha de comando.

```
ciscoasa#test aaa-server authentication RAD_SVR_GRP host 192.168.1.2 username kate password
cisco123 INFO: Attempting Authentication test to IP address <192.168.1.2> (timeout: 12 seconds)
INFO: Authentication Successful
```

Troubleshooting

O comando debug radius pode ajudá-lo a pesquisar defeitos problemas de autenticação nesta encenação. Este comando permite a eliminação de erros da sessão do RAIO assim como a descodificação do pacote de informação de RADIUS. Em cada resultado do debug apresentado, o primeiro pacote descodificado é o pacote enviado do ASA ao servidor ACS. O segundo pacote é a resposta do servidor ACS.

Nota: Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos **debug**.

Quando a autenticação é bem sucedida, o servidor Radius envia uma mensagem da **aceitação de acesso**.

```
ciscoasa#debug radius !--- First Packet. Authentication Request. ciscoassa#radius mkreq: 0x88
alloc_rip 0xd5627ae4 new request 0x88 --> 52 (0xd5627ae4) got user '' got password add_req
0xd5627ae4 session 0x88 id 52 RADIUS_REQUEST radius.c: rad_mkpkt RADIUS packet decode
(authentication request) ---------------------------------- Raw packet data (length =
62)..... 01 34 00 3e 18 71 56 d7 c4 ad e2 73 30 a9 2e cf | .4.>.qV....s0... 5c 65 3a eb 01 06 6b
61 74 65 02 12 0e c1 28 b7 | \e:...kate....(. 87 26 ed be 7b 2c 7a 06 7c a3 73 19 04 06 c0 a8 |
.&..{,z.|.s..... 01 01 05 06 00 00 00 34 3d 06 00 00 00 05 | .......4=..... Parsed packet
data..... Radius: Code = 1 (0x01) Radius: Identifier = 52 (0x34) Radius: Length = 62 (0x003E)
Radius: Vector: 187156D7C4ADE27330A92ECF5C653AEB Radius: Type = 1 (0x01) User-Name Radius:
Length = 6 (0x06) Radius: Value (String) = 6b 61 74 65 | kate Radius: Type = 2 (0x02) User-
Password Radius: Length = 18 (0x12) Radius: Value (String) = 0e c1 28 b7 87 26 ed be 7b 2c 7a 06
7c a3 73 19 | ..(..&..{,z.|.s. Radius: Type = 4 (0x04) NAS-IP-Address Radius: Length = 6 (0x06)
Radius: Value (IP Address) = 192.168.1.1 (0xC0A80101) Radius: Type = 5 (0x05) NAS-Port Radius:
Length = 6 (0x06) Radius: Value (Hex) = 0x34 Radius: Type = 61 (0x3D) NAS-Port-Type Radius:
Length = 6 (0x06) Radius: Value (Hex) = 0x5 send pkt 192.168.1.2/1645 rip 0xd5627ae4 state 7 id
52 rad_vrfy() : response message verified rip 0xd544d2e8 : chall_state '' : state 0x7 : timer
0x0 : reqauth: 18 71 56 d7 c4 ad e2 73 30 a9 2e cf 5c 65 3a eb : info 0x88 session_id 0x88
request_id 0x34 user 'kate' response '***' app 0 reason 0 skey 'secretkey' sip 192.168.1.2 type
1 !--- Second Packet. Authentication Response. RADIUS packet decode (response) ----------------
---------------------- Raw packet data (length = 50)..... 02 34 00 32 35 a1 88 2f 8a bf 2a 14 c5
31 78 59 | .4.25../..*..1xY 60 31 35 89 08 06 ff ff ff ff 19 18 43 41 43 53 | `15.........CACS
3a 30 2f 32 61 36 2f 63 30 61 38 30 31 30 31 2f | :0/2a6/c0a80101/ 35 32 | 52 Parsed packet
data..... Radius: Code = 2 (0x02) Radius: Identifier = 52 (0x34) Radius: Length = 50 (0x0032)
Radius: Vector: 35A1882F8ABF2A14C531785960313589 Radius: Type = 8 (0x08) Framed-IP-Address
Radius: Length = 6 (0x06) Radius: Value (IP Address) = 255.255.255.255 (0xFFFFFFFF) Radius: Type
= 25 (0x19) Class Radius: Length = 24 (0x18) Radius: Value (String) = 43 41 43 53 3a 30 2f 32 61
36 2f 63 30 61 38 30 | CACS:0/2a6/c0a80 31 30 31 2f 35 32 | 101/52 rad_procpkt: ACCEPT
RADIUS_ACCESS_ACCEPT: normal termination RADIUS_DELETE remove_req 0xd5627ae4 session 0x88 id 52
free_rip 0xd5627ae4 radius: send queue empty
```

Quando a autenticação falha, o servidor ACS envia um **mensagem de rejeição de acesso**.

```
ciscoasa#debug radius !--- First Packet. Authentication Request. ciscoasa# radius mkreq: 0x85
alloc_rip 0xd5627ae4 new request 0x85 --> 49 (0xd5627ae4) got user '' got password add_req
0xd5627ae4 session 0x85 id 49 RADIUS_REQUEST radius.c: rad_mkpkt RADIUS packet decode
(authentication request) ---------------------------------- Raw packet data (length =
62)..... 01 31 00 3e 88 21 46 07 34 5d d2 a3 a0 59 1e ff | .1.>.!F.4]...Y.. cc 15 2a 1b 01 06 6b
61 74 65 02 12 60 eb 05 32 | ..*...kate..`..2 87 69 78 a3 ce d3 80 d8 4b 0d c3 37 04 06 c0 a8 |
.ix.....K..7.... 01 01 05 06 00 00 00 31 3d 06 00 00 00 05 | .......1=..... Parsed packet
data..... Radius: Code = 1 (0x01) Radius: Identifier = 49 (0x31) Radius: Length = 62 (0x003E)
Radius: Vector: 88214607345DD2A3A0591EFFCC152A1B Radius: Type = 1 (0x01) User-Name Radius:
Length = 6 (0x06) Radius: Value (String) = 6b 61 74 65 | kate Radius: Type = 2 (0x02) User-
Password Radius: Length = 18 (0x12) Radius: Value (String) = 60 eb 05 32 87 69 78 a3 ce d3 80 d8
4b 0d c3 37 | `..2.ix.....K..7 Radius: Type = 4 (0x04) NAS-IP-Address Radius: Length = 6 (0x06)
Radius: Value (IP Address) = 192.168.1.1 (0xC0A80101) Radius: Type = 5 (0x05) NAS-Port Radius:
Length = 6 (0x06) Radius: Value (Hex) = 0x31 Radius: Type = 61 (0x3D) NAS-Port-Type Radius:
Length = 6 (0x06) Radius: Value (Hex) = 0x5 send pkt 192.168.1.2/1645 rip 0xd5627ae4 state 7 id
49 rad_vrfy() : response message verified rip 0xd544d2e8 : chall_state '' : state 0x7 : timer
0x0 : reqauth: 88 21 46 07 34 5d d2 a3 a0 59 1e ff cc 15 2a 1b : info 0x85 session_id 0x85
request_id 0x31 user 'kate' response '***' app 0 reason 0 skey 'secretkey' sip 192.168.1.2 type
```

```
1 !--- Second packet. Authentication Response. RADIUS packet decode (response) ----------
---------- Raw packet data (length = 32)..... 03 31 00 20 70 98 50 af 39 cc b9 ba df
a7 bd ff | .1. p.P.9....... 06 af fb 02 12 0c 52 65 6a 65 63 74 65 64 0a 0d | ......Rejected..
Parsed packet data..... Radius: Code = 3 (0x03) Radius: Identifier = 49 (0x31) Radius: Length =
32 (0x0020) Radius: Vector: 709850AF39CCB9BADFA7BDFF06AFFB02 Radius: Type = 18 (0x12) Reply-
Message Radius: Length = 12 (0x0C) Radius: Value (String) = 52 65 6a 65 63 74 65 64 0a 0d |
Rejected.. rad_procpkt: REJECT RADIUS_DELETE remove_req 0xd5627ae4 session 0x85 id 49 free_rip
0xd5627ae4 radius: send queue empty
```

Informações Relacionadas

- Remote Authentication Dial-In User Service (RADIUS)
- Solicitações de Comentários (RFCs)
- Suporte Técnico e Documentação - Cisco Systems