ASA 8.0: Autenticación de RADIUS de la configuración para los usuarios de WebVPN

Contenido

Introducción

Este documento demuestra cómo configurar el dispositivo de seguridad adaptante de Cisco (ASA) para utilizar a un servidor para autentificación del Remote Authentication Dial-In User Service (RADIUS) de los usuarios de WebVPN. El servidor de RADIUS en este ejemplo es un servidor del Access Control Server de Cisco (ACS), versión 4.1 que esta configuración se realiza con el Administrador de dispositivos de seguridad adaptante (ASDM) 6.0(2) en un ASA que funcione con la versión de software 8.0(2).

Nota: En este ejemplo la autenticación de RADIUS se configura para los usuarios de WebVPN, pero esta configuración se puede utilizar para otros tipos de VPN de acceso remoto también. Asigne simplemente al Grupo de servidores AAA al perfil de la conexión deseado (grupo de túnel) como se muestra.

prerrequisitos

- Se requiere una configuración básica del WebVPN.
- Cisco ACS debe tener los usuarios configurados para la autenticación de usuario. Refiera a agregar una sección básica de la cuenta de usuario de User Management (Administración de usuario) para más información.

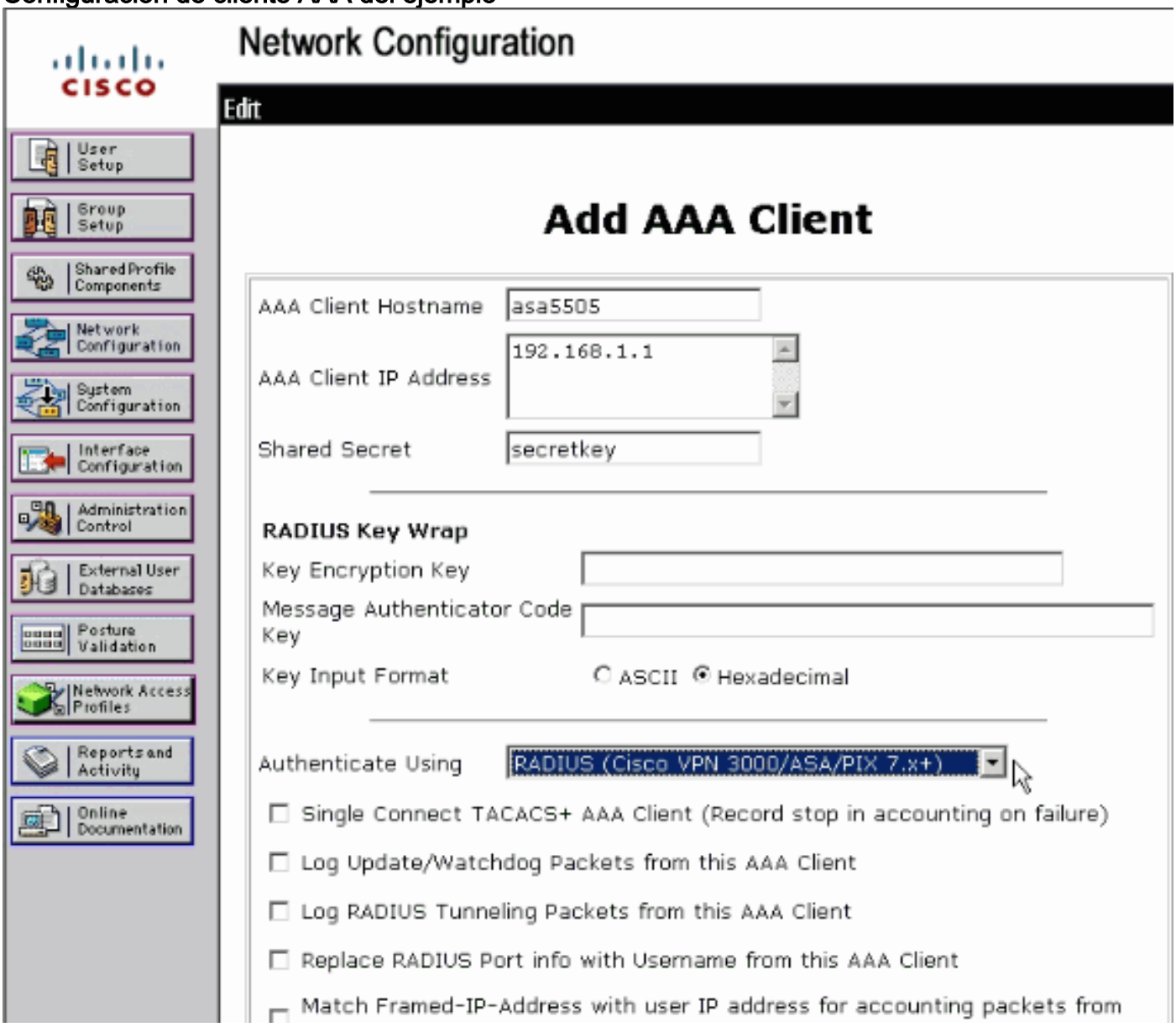
Configure al servidor ACS

En esta sección, le presentan con la información para configurar la autenticación de RADIUS en el ACS y el ASA.

Complete estos pasos para configurar al servidor ACS para comunicar con el ASA.

1. Elija la **configuración de red del** menú izquierdo de la pantalla ACS.
2. Elija **agregan la entrada** bajo los **clientes AAA**.
3. Proporcione la información del cliente:**Nombre del host del cliente AAA** — un nombre de su opción**Dirección IP del cliente AAA** — el direccionamiento del cual el dispositivo de seguridad entra en contacto el ACS**Secreto compartido** — una clave secreta configurada en el ACS y en el dispositivo de seguridad
4. En la **autenticidad usando** dropdown elija **RADIUS (Cisco VPN 3000/ASA/PIX 7.x+)**.
5. Haga clic **Submit+Apply**.

Configuración de cliente AAA del ejemplo

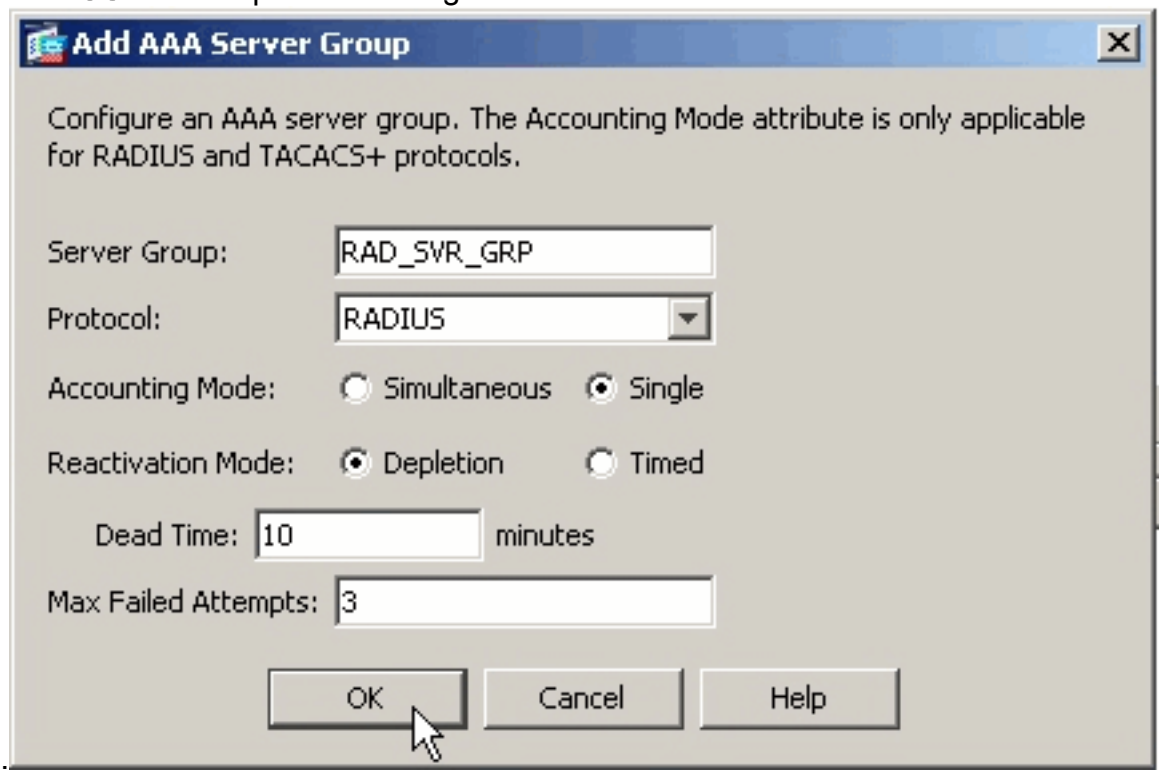


Configure el dispositivo de seguridad

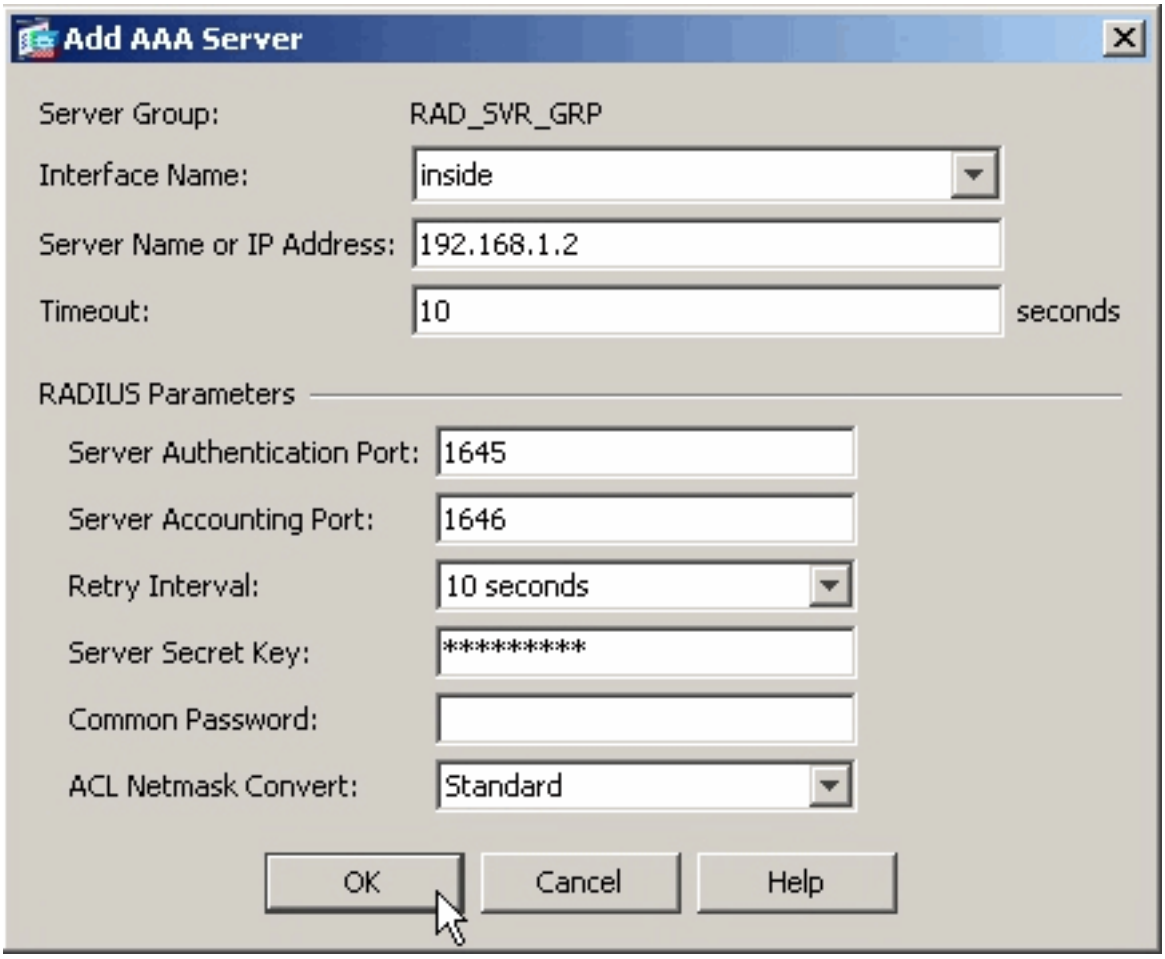
ASDM

Complete estos pasos en el ASDM para configurar el ASA para comunicar con el servidor ACS y para autenticar a los clientes del WebVPN.

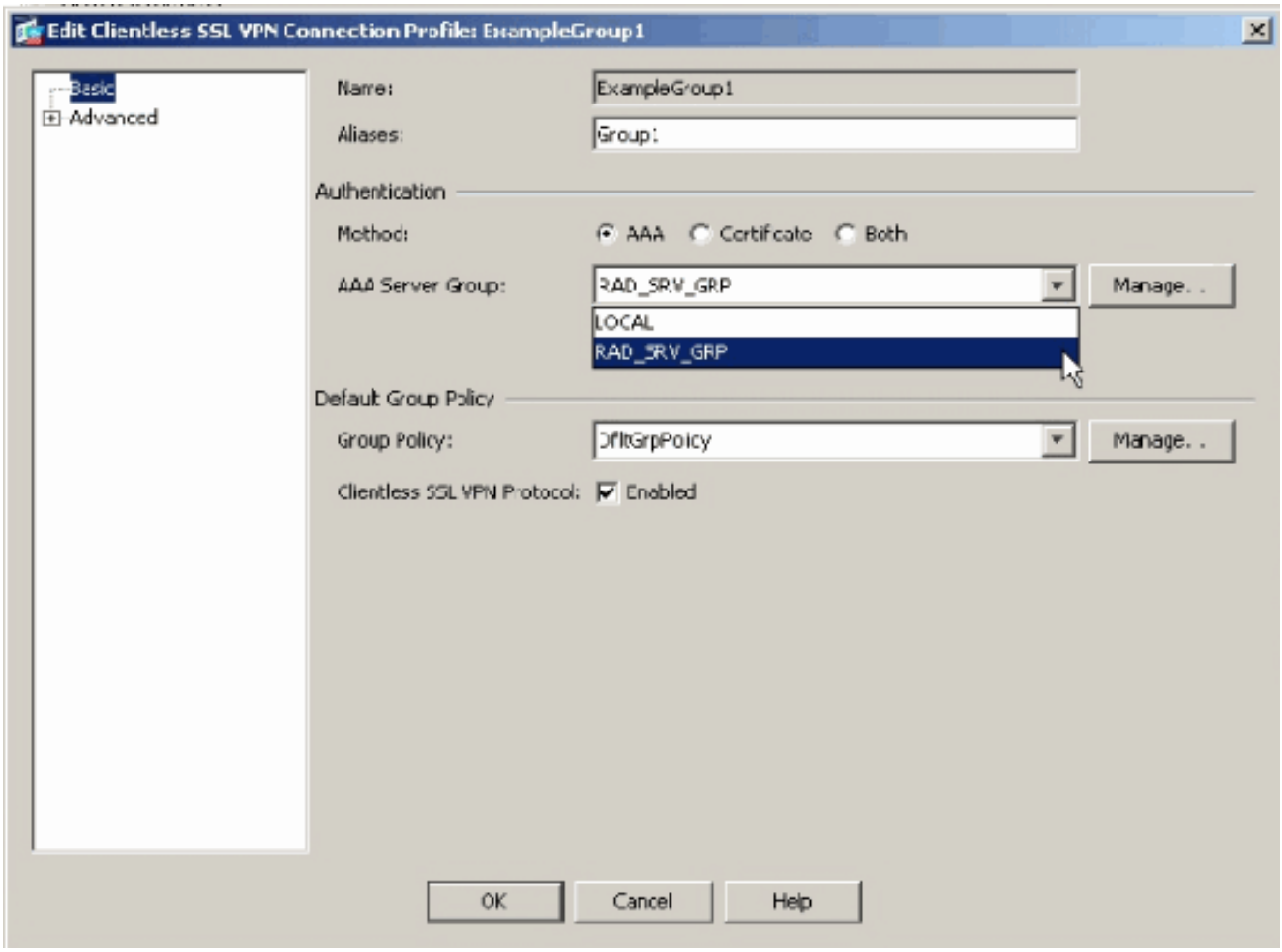
1. Elija la **configuración > el VPN de acceso remoto >AAA ponen >AAA a los grupos de servidores**.
2. El tecleo **agrega** al lado de los Grupos de servidores AAA.
3. En la ventana que aparece, especifique un nombre para el nuevo Grupo de servidores AAA y elija el **RADIUS** como el protocolo. Haga Click en OK cuando está acabado.



4. Esté seguro que seleccionan a su nuevo grupo en el cristal superior y el tecleo **agrega** a la derecha del cristal más bajo.
5. Proporcione la información del servidor:**Nombre de la interfaz** — la interfaz que el ASA debe utilizar para alcanzar al servidor ACS**Nombre del servidor o dirección IP** — el direccionamiento que el ASA debe utilizar para alcanzar al servidor ACS**Clave del Secreto de servidor** — la clave secreta compartida configurada para el ASA en el servidor ACS**Configuración de servidor AAA del ejemplo en el ASA**



6. Una vez que usted ha configurado el Grupo de servidores AAA y el servidor, navegue a la configuración > al VPN de acceso remoto > al acceso > a los perfiles de la conexión del clientless SSL VPN para configurar el WebVPN para utilizar la nueva configuración AAA.**Nota:** Aunque este ejemplo utiliza el WebVPN, usted puede fijar cualquier perfil de la conexión de acceso remoto (grupo de túnel) para utilizar esta configuración AAA.
7. Elija el perfil para el cual usted quiere configurar el AAA, y el tecleo **edita**.
8. Bajo **autenticación** elija al grupo de servidor de RADIUS que usted creó anterior. Haga Click en OK cuando está
acabado.



Interfaz de la línea de comandos

Complete estos pasos en el comando line interface(cli) para configurar el ASA para comunicar con el servidor ACS y para autenticar a los clientes del 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
```

Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

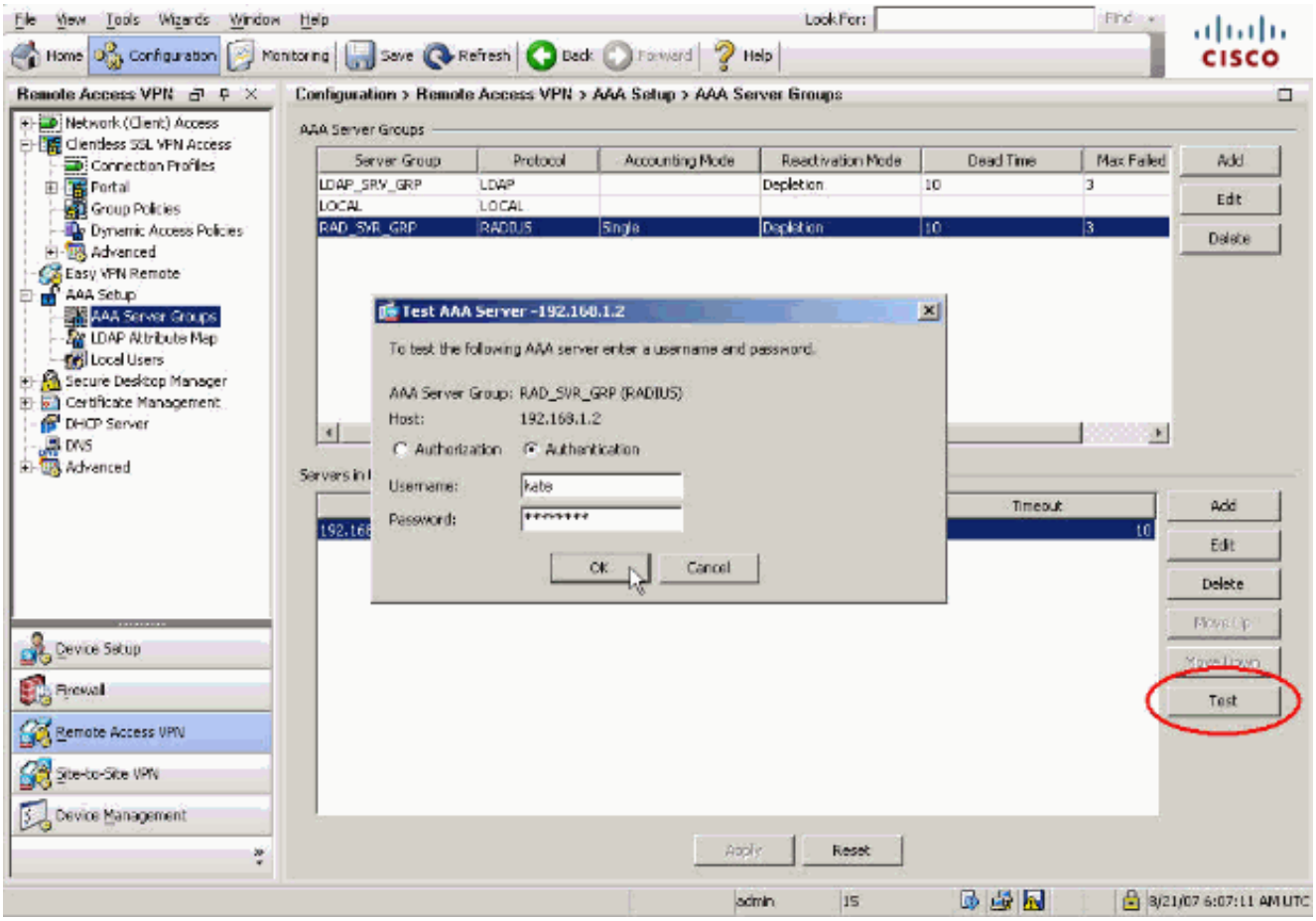
Pruebe con el ASDM

Verifique su configuración de RADIUS con el **botón Test Button** en la pantalla de configuración de los Grupos de servidores AAA. Una vez que usted suministra un nombre de usuario y contraseña, este botón permite que usted envíe una petición de la prueba de la autentificación al servidor ACS.

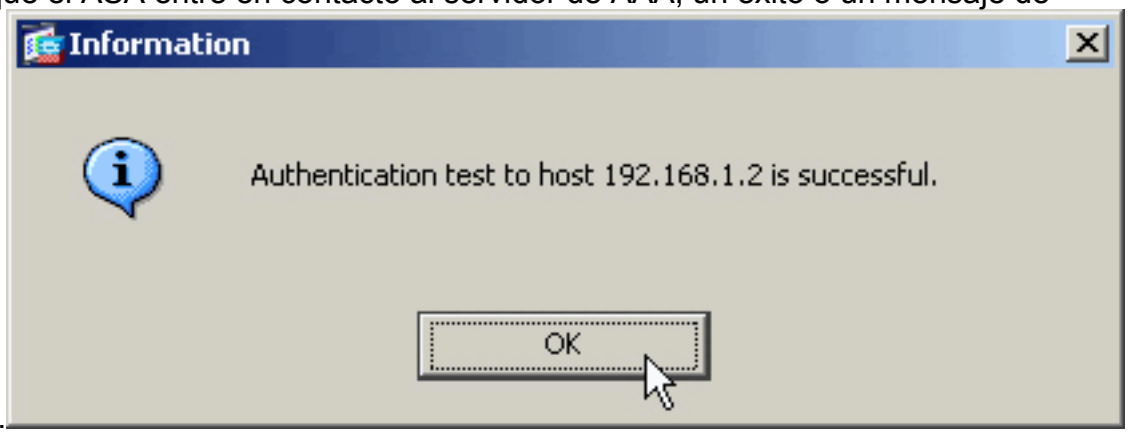
1. Elija la **configuración > el VPN de acceso remoto >AAA ponen >AAA a los grupos de**

servidores.

2. Seleccione a su Grupo de servidores AAA deseado en el cristal superior.
3. Seleccione al servidor de AAA que usted quiere probar en el cristal más bajo.
4. Haga clic el **botón Test Button** a la derecha del cristal más bajo.
5. En la ventana que aparece, haga clic el botón de radio de la **autenticación**, y suministre las credenciales con las cuales usted quiere probar. Haga Click en OK cuando está acabado.



6. Después de que el ASA entre en contacto al servidor de AAA, un éxito o un mensaje de error aparece.



Pruebe con el CLI

Usted puede utilizar el **comando test** en la línea de comando para probar su configuración AAA. Una petición de la prueba se envía al servidor de AAA, y el resultado aparece en la línea 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

El comando debug radius puede ayudarle a resolver problemas los problemas de autenticación en este escenario. Este comando habilita el debugging de la sesión RADIUS así como decodificar del paquete RADIUS. En cada salida de los debugs presentada, el primer paquete decodificado es el paquete enviado del ASA al servidor ACS. El segundo paquete es la respuesta del servidor ACS.

Nota: Consulte Información Importante sobre Comandos de Debug antes de usar un **comando debug**.

Cuando la autenticación es acertada, el servidor de RADIUS envía un mensaje del **access-accept**.

```
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
```

Cuando la autenticación falla, el servidor ACS envía los **mensajes de rechazo de acceso**.

```
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

Información Relacionada

- Remote Authentication Dial-In User Service (RADIUS)
- Solicitudes de Comentarios (RFC)
- Soporte Técnico y Documentación - Cisco Systems