Lock-and-Key: Listas de acceso dinámico

Contenido

Introducción Prerequisites Requirements Componentes Utilizados Convenciones Consideraciones de simulación Rendimiento Cuando utilizar el acceso Lock-and-Key Operación de acceso con cerrojo y llave Configuración de muestra y solución de problemas Diagrama de la red Uso de TACACS+ Uso de RADIUS Información Relacionada

Introducción

El acceso Lock-and-key (Llave y cerrojo) le permite configurar listas de acceso dinámicas que garantizan el acceso para cada usuario a un host de destino/origen específico mediante un proceso de autenticación de usuario. El acceso del usuario se permite a través de un Cisco IOS[®] Firewall dinámicamente, sin ningún riesgo en las restricciones de seguridad.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que se presenta en este documento se originó a partir de dispositivos dentro de un ambiente de laboratorio específico. En este caso, el entorno de laboratorio consistía en un router 2620 que ejecutaba la versión 12.3(1) del software del IOS® de Cisco. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Convenciones

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

Consideraciones de simulación

El acceso de bloqueo y llave permite que un evento externo coloque una apertura en el Cisco IOS Firewall. Luego de que exista esta apertura, el router es susceptible a la vigilancia de dirección de origen. Para evitar esto, proporcione soporte de cifrado usando el cifrado IP con autenticación o cifrado.

La simulación es un problema con todas las listas de acceso existentes. El acceso lock-and-key no trata este problema.

Debido a que el acceso lock-and-key introduce un camino potencial a través del firewall de la red, deberá analizar el acceso dinámico. Otro host, que falsifica su dirección autenticada, obtiene acceso detrás del firewall. Con el acceso dinámico, existe la posibilidad de que un host no autorizado, suplantando su dirección autenticada, obtenga acceso detrás del firewall. El acceso de bloqueo y llave no causa el problema de suplantación de dirección. El problema sólo se identifica aquí como una preocupación del usuario.

Rendimiento

El rendimiento se ve afectado en estas dos situaciones.

- Cada lista de acceso dinámica fuerza una reconstrucción de lista de acceso en el Motor de conmutación de silicio (SSE). Esto hace que el trayecto de conmutación SSE funcione más lento momentáneamente.
- Las listas de acceso dinámicas requieren la función de tiempo de espera inactivo (incluso si el tiempo de espera se deja en el valor predeterminado). Por lo tanto, las listas de acceso dinámicas no se pueden conmutar por SSE. Estas entradas se manejan en el trayecto de fast switching del protocolo.

Vea las configuraciones del router de borde. Los usuarios remotos crean entradas de lista de acceso en el router de borde. La lista de acceso crece y se reduce dinámicamente. Las entradas se eliminan dinámicamente de la lista luego de que caducan los períodos idle-timeout o maxtimeout. Listas de acceso grandes degradan el rendimiento de conmutación del paquete.

Cuando utilizar el acceso Lock-and-Key

A continuación se enumeran dos ejemplos de cuándo se utiliza el acceso de bloqueo y clave:

- Cuando desea que un host remoto pueda acceder a un host de la red interna a través de Internet. El acceso de bloqueo y llave limita el acceso más allá del firewall en un host individual o en una red.
- Cuando desea que un subgrupo de hosts en una red acceda a un host en una red remota protegido por un firewall. Por medio del acceso con cerrojo y llave, puede habilitar sólo un conjunto deseado de hosts para que tengan acceso. Para hacerlo, deberá autenticarlos a

través de un servidor TACACS+ o RADIUS.

Operación de acceso con cerrojo y llave

Este proceso describe la operación de acceso de bloqueo y llave.

- 1. Un usuario abre una sesión Telnet en un router de borde configurado para acceso con cerrojo y llave.
- El software Cisco IOS recibe el paquete Telnet. Realiza un proceso de autenticación de usuario. El usuario debe aprobar la autenticación antes de que se le permita el acceso. El proceso de autenticación lo realiza el router o un servidor de acceso central como un TACACS+ o un servidor RADIUS.

Configuración de muestra y solución de problemas

Diagrama de la red



Cisco recomienda utilizar un servidor TACACS+ para el proceso de consulta de autenticación. TACACS+ proporciona servicios de autenticación, autorización y contabilidad. También proporciona soporte de protocolo, especificación de protocolo y una base de datos de seguridad centralizada.

Puede autenticar al usuario en el router o con un servidor TACACS+ o RADIUS.

Nota: Estos comandos son globales a menos que se indique lo contrario.

En el router, necesita un nombre de usuario para el usuario para la autenticación local.

username test password test

La presencia de login local en las líneas vty hace que se utilice este nombre de usuario.

Si no confía en que el usuario ejecute el comando **access-enable**, puede hacer una de estas dos cosas:

Asocie el tiempo de espera al usuario por usuario.

```
username test autocommand access-enable host timeout 10
```

or

• Obligar a todos los usuarios en los que se conecta Telnet a tener el mismo tiempo de espera.

```
line vty 0 4
login local
autocommand access-enable host timeout 10
```

Nota: El **10** en la sintaxis es el *tiempo de espera inactivo* de la lista de acceso. Se anula por el tiempo de espera absoluto en la lista de acceso dinámico.

Defina una lista de acceso ampliada que se aplica cuando un usuario (cualquier usuario) inicia sesión en el router y se ejecuta el comando **access-enable**. El tiempo absoluto máximo para este "agujero" en el filtro se establece en 15 minutos. Después de 15 minutos, el hoyo cierra si alguien lo usa o no. El nombre **testlist** necesita existir pero no es significativo. Limite las redes a las que el usuario tiene acceso mediante la configuración de la dirección de origen o de destino (aquí, el usuario no está limitado).

access-list 120 dynamic testlist timeout 15 permit ip any any

Defina la lista de acceso necesaria para bloquear todo excepto la capacidad de Telnet en el router (para abrir un agujero, el usuario necesita Telnet al router). La dirección IP aquí es la dirección IP Ethernet del router.

access-list 120 permit tcp any host 171.68.117.189 eq telnet

Hay una **negación** implícita al final (no introducida aquí).

Aplique esta lista de acceso a la interfaz en la que entran los usuarios.

```
interface ethernet1
ip access-group 120 in
```

Ya está.

Así es como se ve el filtro en el router en este momento:

```
Router#show access-lists
Extended IP access list 120
10 Dynamic testlist permit ip any any log
20 permit tcp any host 171.68.117.189 eq telnet (68 matches)
Los usuarios que obtienen acceso a su red interna no pueden ver nada hasta que se conectan
```

mediante Telnet al router.

Nota: El **10** aquí es el *tiempo de espera inactivo* de la lista de acceso. Se anula por el tiempo de espera absoluto en la lista de acceso dinámico.

%telnet 2514A
Trying 171.68.117.189 ...
Connected to 2514A.network.com.
Escape character is '^]'.

User Access Verification

Username: test Password: test

Connection closed by foreign host. El filtro se ve así.

Router#show access-lists
Extended IP access list 120
10 Dynamic testlist permit ip any any log
 permit ip host 171.68.109.158 any log (time left 394)
20 permit tcp any host 171.68.117.189 eq telnet (68 matches)

Hay un agujero en el filtro para este usuario basado en la dirección IP de origen. Cuando alguien más hace esto, se ven *dos agujeros*.

Router#show ip access-lists 120
Extended IP access list 120
10 Dynamic testlist permit ip any any log
 permit ip host 171.68.109.64 any log
 permit ip host 171.68.109.158 any log
20 permit tcp any host 171.68.117.189 eq telnet (288 matches)

Estos usuarios pueden tener acceso IP completo a cualquier dirección IP de destino desde su dirección IP *de origen*.

Uso de TACACS+

Configuración de TACACS+

Configure un servidor TACACS+ para forzar la autenticación y autorización a hacer en el servidor TACACS+ para utilizar TACACS+, como muestra este resultado:

aaa new-model
!
!
aaa authentication login default group tacacs+ local
aaa authorization exec default group tacacs+
tacacs-server host 10.48.66.53 key cisco123
Complete estos pasos para configurar TACACS+ en Cisco Secure ACS para Windows:

1. Abra un navegador web. Ingrese la dirección de su servidor ACS, que se encuentra en la forma de http://<IP_address o DNS_name>:2002. (Este ejemplo utiliza un puerto

predeterminado de 2002.) Inicie sesión como admin.

2. Haga clic en la configuración de red. Haga clic en **Agregar entrada** para crear un grupo de dispositivos de red que contenga los servidores de acceso a la red (NAS). Introduzca un nombre para el grupo y haga clic en

| Ciscolecure ACS - Microsoft Internet Explorer provided by Cisco Systems, Inc. | |
|--|--|
| in in my state you go the state of the state | |
| Agines a http://www.commerce.com | |
| Cases Strategy Network Configuration | |
| Stert | Help |
| New Network Device Group | <u>Network Device Group Name</u> |
| Burstitute Network Denice Group Name MyJWS | Network Device Group Name |
| Contention Contention Submit Concel | To add a new Network Device Group (NDG), the name of the new group, and then click Suba |
| 2 Bet to Wig | Names can control of any computation of manif- letters, or symbols. You can also assign users to NDG at the group level. |
| Control Control | Note: We recommend that you do not use spar NDG names. |
| C Appendix | [Back to Top] |
| Documentation | R Santas Manusco |
| | (Looine |

3. Haga clic en **Agregar entrada** para agregar un cliente de autenticación, autorización y contabilidad (AAA)

| Agabess Dhotp (Musi | S85(index2 htm | |
|--|--|--|
| Cinco Serrian | Network Configuration | |
| Betrop Setup Setup Setup Starug Starug Satured Profile Components Seturation Seturation Seturation Seturation Configuration Seturation Configuration | My_NAS AAA Clients AAA Client Hostname Address None Defined Add Enty | Network Device Groups Adding a Network Device Group Renaming a Network Device Group Deleting a Network Device Group Searching for Network Devices AAA Clients Adding a AAA Client Deleting a AAA Client AAA Servers Adding a AAA Server Editing a AAA Server |
| 10 (External User | 🍫 Q. My_NAS AAA Servers 💈 📃 | Deleting a AAA Server Proxy Distribution Table |
| BU Subdaces | AAA Server AAA Server IP AAA Server Name Address Type | Adding a Proxy Distribution Table Entry Sorting Proxy Distribution Table Entries |
| -Oliving | None Defined | Editing a Proxy Distribution Table Entry |

4. Introduzca el nombre de host, la dirección IP y la clave utilizada para cifrar la comunicación entre el servidor AAA y el NAS. Seleccione TACACS+ (Cisco IOS) como método de autenticación. Cuando haya terminado, haga clic en Enviar +Reiniciar para aplicar los cambios.



 Haga clic en User Setup, ingrese un ID de usuario y haga clic en Add/Edit

| Disconfecture ALS - 1 Ele Edit year fig 2-Back + | teronal Internet Explorer provided by Livia Systems, Brz. nates (Josh 1949) 2) 2) 2) Starth (Joseph Strates (Stada (S) () - () () - () Starter 2 Ma | العالي العالي عند العادي (العادي العادي العادي العادي (العادي العادي العادي) العادي (العادي العادي العادي العادي العادي ا |
|---|--|---|
| Cince States | User Setup Seter | Hiclp - |
| Carliportion | User. Sest Find Add/Edit List users beginning with letter/number: A R S P E F S B I X E L B B O F Q B S I U V M Z X Z Q A 2 2 5 5 2 5 2 | User Setup and External User Databases Finding a Specific User in the CiscoSecure User Database Adding a User to the CiscoSecure User Database Listing Usernames that Begin with a Particular Character Listing All Usernames in the CiscoSecure User Database Changing a Username in the CiscoSecure User Database |
| Additional Control Control Cherr Debetween Cherr Debetween Activity Declar Declar Declar Declar | Ent All Dawn | User Setup enables you to configure individual user information, add users, and delete users in the database. User Setup and External User Databases Before Cisco Secure ACS can authenticate users |

6. Elija una base de datos para autenticar al usuario. (En este ejemplo, el usuario es "test" y la base de datos interna del ACS se utiliza para la autenticación). Introduzca una contraseña para el usuario y



7. Elija el grupo al que está asignado el usuario y marque **Usar configuración de grupo**. Haga clic en Submit



8. Haga clic en Group Setup. Seleccione el grupo al que se asignó el usuario en el paso 7.

Haga clic en Editar

configuración.

| CiscoSecure ACS - Microsoft Internet Diplarer provided by Cisco Systems, Iac. | | | | |
|--|---|---|--|--|
| file fall year Fyrontes Jook 1940 | | | | |
| -tak | | | | |
| Address Attp://flut? | Sitt/index2.htm | 🛫 Pilo Unis ** | | |
| Cisco Secremo | Group Setup | × | | |
| | Select | Help | | |
| Uter Setup Setup Setup Barry Profile Composents Detroyof Configure at las | Group : D Group (1 user) Users in Group Edit Settings Periame Group | Default Group Group Users in Group Edit Settings Rename Group | | |
| Configuration | | Default Group | | |
| Admission Centremation Control Detabaser Detabaser Reports and Activity Decementation | 2 East rooms | If group mapping has not been configured, usernames that are not configured in the CiscoSecure Database are assigned to the Default Group by Cisco Secure ACS the first time they log in. The privileges and restrictions for the default group- are applied to first-time users. If you have upgraded from a previous version of Cisco Secure ACS and kept your database information, users will map as configured in the previous version. | | |

 Desplácese hacia abajo hasta la sección Configuración de TACACS+. Marque la casilla para Shell exec. Marque la casilla para Auto command. Ingrese el auto-comando que se ejecutará tras la autorización exitosa del usuario. (Este ejemplo utiliza el comando access-enable host timeout 10.) Haga clic en Enviar+Reiniciar

| CiscoSecure ACS - M | terosoft Internet Explorer provider | l by Cisco Systems, loc. | | |
|---------------------------|-------------------------------------|--|---|------------------|
| Ele Edt you Fgr | orites jools Help | | | 10 M |
| 4-8ak - → · 🧿 | 3 3 Seath Bravates | 8meda 3 3. 3 3. | • 🖸 | |
| Address 10 http://flur25 | 85/index2.htm | | | • 12% Links * |
| Cisco Statems | Group Setup | | | × |
| adhaatha. | Jump To Access | Restrictions | Help | - |
| User Setup | 🗵 Shell (exec) | | X | |
| | C Access control list | | Group Settings Vaire must TP (VaTP) Support | |
| 1 Satur | R Auto command | access-enable ho | Default Time-of-Day Access Setting | B 🕌 |
| Ca Sharedinafie | C. Callback Inc. | | Callback | - 18 |
| Camposing | E Chillender and | | Network Access Restrictions | |
| Service Configuration | 1.5 Calback rotary | and the second sec | Max Sessions Usage Ougtas | |
| (Sixian) | 🖾 Ide time | L | Enable Options | |
| Certipration | 🖾 No caliback verify | Enabled | Taken Card Settings | |
| Confinentiate | No escape | C Enabled | Password Aging Rules | |
| (Carl Construction) | No hangup | C Enabled | <u>IP Assignment</u> | |
| Administration Control | C Privilege level | | Downloadable ACLs TACACS+ Settings | |
| A A I External User | C. Treasure | | TACACS+ Shell Command Authory | ation. |
| 90 Databases | C Incos | La construction and | Command Authorization for Network | k Device |
| Reports and | C Custom attributes | | Management Applications | 1 |
| Spr 1 Activity | | 2 | TACACS+ Unknown Services | |
| Designmentation | - | and the second second | IETF RADIUS Attributes | |
| - | Submit Submit | Pestart Cancel | RADIUS Vendor-Specific Attributes | interesting with |
| 0 | | | | ocal intranet |

Solución de problemas de TACACS+

Utilice estos comandos debug en el NAS para resolver problemas con TACACS+.

Nota: Consulte Información Importante sobre Comandos Debug antes de utilizar los comandos debug.

- debug tacacs authentication—Muestra información sobre el proceso de autenticación TACACS+. Sólo disponible en algunas versiones de software. Si no está disponible, utilice debug tacacs solamente.
- debug tacacs authorization—Muestra información sobre el proceso de autorización TACACS+. Sólo disponible en algunas versiones de software. Si no está disponible, utilice debug tacacs solamente.
- debug tacacs events—Muestra información del proceso de ayudante TACACS+. Sólo disponible en algunas versiones de software. Si no está disponible, utilice debug tacacs solamente.

Utilice estos comandos para resolver problemas de AAA:

- debug aaa authentication Muestra información sobre autenticación de AAA/TACACS+.
- debug aaa authorization—Muestra información sobre la autorización AAA/TACACS+.

El ejemplo de **resultado de debug** aquí muestra un proceso exitoso de autenticación y autorización en el servidor ACS TACACS+.

```
Router#show debug
General OS:
 TACACS+ events debugging is on
 TACACS+ authentication debugging is on
 TACACS+ authorization debugging is on
 AAA Authentication debugging is on
 AAA Authorization debugging is on
_____
Router#
AAA/BIND(0000009): Bind i/f
AAA/AUTHEN/LOGIN (0000009): Pick method list 'default'
TPLUS: Queuing AAA Authentication request 9 for processing
TPLUS: processing authentication start request id 9
TPLUS: Authentication start packet created for 9()
TPLUS: Using server 10.48.66.53
TPLUS(0000009)/0/NB WAIT/82A2E088: Started 5 sec timeout
TPLUS(0000009)/0/NB_WAIT: socket event 2
TPLUS(0000009)/0/NB_WAIT: wrote entire 36 bytes request
TPLUS(0000009)/0/READ: socket event 1
TPLUS(0000009)/0/READ: Would block while reading
TPLUS(0000009)/0/READ: socket event 1
TPLUS(0000009)/0/READ: read entire 12 header bytes
   (expect 16 bytes data)
TPLUS(0000009)/0/READ: socket event 1
TPLUS(0000009)/0/READ: read entire 28 bytes response
TPLUS(0000009)/0/82A2E088: Processing the reply packet
TPLUS: Received authen response status GET_USER (7)
TPLUS: Queuing AAA Authentication request 9 for processing
TPLUS: processing authentication continue request id 9
TPLUS: Authentication continue packet generated for 9
TPLUS(0000009)/0/WRITE/8347F3FC: Started 5 sec timeout
TPLUS(0000009)/0/WRITE: wrote entire 22 bytes request
TPLUS(0000009)/0/READ: socket event 1
```

TPLUS(0000009)/0/READ: read entire 12 header bytes (expect 16 bytes data) TPLUS(0000009)/0/READ: socket event 1 TPLUS(0000009)/0/READ: read entire 28 bytes response TPLUS(0000009)/0/8347F3FC: Processing the reply packet TPLUS: Received authen response status GET_PASSWORD (8) TPLUS: Queuing AAA Authentication request 9 for processing TPLUS: processing authentication continue request id 9 TPLUS: Authentication continue packet generated for 9 TPLUS(0000009)/0/WRITE/8347EE4C: Started 5 sec timeout TPLUS(0000009)/0/WRITE: wrote entire 25 bytes request TPLUS(0000009)/0/READ: socket event 1 TPLUS(0000009)/0/READ: read entire 12 header bytes (expect 6 bytes data) TPLUS(0000009)/0/READ: socket event 1 TPLUS(0000009)/0/READ: read entire 18 bytes response TPLUS(0000009)/0/8347EE4C: Processing the reply packet TPLUS: Received authen response status PASS (2) AAA/AUTHOR (0x9): Pick method list 'default' TPLUS: Queuing AAA Authorization request 9 for processing TPLUS: processing authorization request id 9 TPLUS: Protocol set to NoneSkipping TPLUS: Sending AV service=shell TPLUS: Sending AV cmd TPLUS: Authorization request created for 9(tne-1) TPLUS: using previously set server 10.48.66.53 from group tacacs+ TPLUS(0000009)/0/NB_WAIT/8347F508: Started 5 sec timeout TPLUS(0000009)/0/NB_WAIT: socket event 2 TPLUS(0000009)/0/NB_WAIT: wrote entire 60 bytes request TPLUS(0000009)/0/READ: socket event 1 TPLUS(0000009)/0/READ: Would block while reading TPLUS(0000009)/0/READ: socket event 1 TPLUS(0000009)/0/READ: read entire 12 header bytes (expect 44 bytes data) TPLUS(0000009)/0/READ: socket event 1 TPLUS(0000009)/0/READ: read entire 56 bytes response TPLUS(0000009)/0/8347F508: Processing the reply packet TPLUS: Processed AV autocmd=access-enable host timeout 10 TPLUS: received authorization response for 9: PASS AAA/AUTHOR/EXEC(00000009): processing AV cmd= AAA/AUTHOR/EXEC(00000009): processing AV autocmd=access-enable host timeout 10 AAA/AUTHOR/EXEC(0000009): Authorization successful

Uso de RADIUS

Configurar RADIUS

Para utilizar RADIUS, configure un servidor RADIUS para forzar que la autenticación se realice en el servidor RADIUS con los parámetros de autorización (el comando automático) que se enviarán en el atributo específico del proveedor 26, como se muestra aquí:

aaa new-model
!
!
aaa authentication login default group radius local
aaa authorization exec default group radius local
radius-server host 10.48.66.53 auth-port 1645
 acct-port 1646 key cisco123

Complete estos pasos para configurar RADIUS en Cisco Secure ACS para Windows:

- 1. Abra un navegador web e ingrese la dirección de su servidor ACS, que se encuentra en la forma de http://<IP_address o DNS_name>:2002. (Este ejemplo utiliza un puerto predeterminado de 2002.) Inicie sesión como admin.
- 2. Haga clic en la configuración de red. Haga clic en **Add Entry** para crear un grupo de dispositivos de red que contenga el NAS. Introduzca un nombre para el grupo y haga clic en



3. Haga clic en Agregar entrada para agregar un cliente AAA

| | T C Closenty T | gravortes grieda | 2 | - |
|-------------------------|-----------------------------|------------------|-----------------------|---|
| Agdress 👔 Nttp://flui25 | 85/index2.htm | | | 12 |
| Cinco Systems | Network Conf | iguration | | |
| AA | Select | | - | Help |
| User Setup | | | | |
| | | | | Network Device Groups |
| Safup | 0 | Mr. NAS AAA (S | inter 191 | Annung a Network Device Group Renaming a Network Device Group |
| d. Shareditotte | | My_POAS ANA CI | Annual Constants | Deleting a Network Device Group |
| - i Camponanta | AAA Client | AAA Client IP | Authenticate | Searching for Network Devices |
| Configuration | Hostname | Address | Using | AAA Clients Adding a AAA Client |
| 21st Suten | rocaldorem concernen | None Defined | nuture for the second | Editing a AAA Client |
| Contribuction | | Add Fatry Search | a i | Deleting a AAA Client |
| Configuration | 1 | | a - 1 | AAA Servers Adding a AAA Surrow |
| Administration | | | | Editing a AAA Server |
| Contral | % Q | My_NAS AAA Se | rvers 👔 | Deleting a AAA Server |
| BO Dutations | AAA Server | AAA Server IP | AAA Server | Adding a Proxy Distribution Table Entry |
| Experts and | Name | Address | Type | Sorting Proxy Distribution Table Entries |
| -Children | - Committee Contraction | None Defined | | Editing a Proxy Distribution Table Entry |
| Documentation | Dates Grand Descent Control | | I Second | Deleting a Proxy Distribution Table Entry |

4. Introduzca el nombre de host, la dirección IP y la clave utilizada para cifrar la comunicación entre el servidor AAA y el NAS. Seleccione RADIUS (Cisco IOS/PIX) como método de autenticación. Cuando haya terminado, haga clic en Enviar +Reiniciar para aplicar los cambios.



5. Haga clic en **User Setup**, ingrese un ID de usuario y haga clic en **Add/Edit**.

| Cisco Secure ACS - Microsoft Internet Explorer provided by Lisco Systems, Inc. | | | | |
|--|--|--|--|--|
| Bie Edit jeen Agrontes jook 1940 | | | | |
| -tax | | | | |
| Address 🔊 http://flu:2585/index2.Mm | 🔹 👌 🔂 Laka 🛎 | | | |
| User Setup Select | | | | |
| Other Setup Discred Fundle Setup Discred Fundle Setup < | User Setup and External User Databases Finding a Specific User in the CiscoSecure User Database Adding a User to the CiscoSecure User Database Listing Usernames that Regin with a Particular Character Listing All Usernames in the CiscoSecure User Database Changing a Username in the CiscoSecure User Database | | | |
| Attributer Distance Distance Reports and Actively Distance D | User Setup enables you to configure individual user information, add users, and delete users in the database. User Setup and External User Databases Before Cisco Secure ACS can asthemicate users | | | |

6. Elija una base de datos para autenticar al usuario. (En este ejemplo, el usuario es "test" y la base de datos interna del ACS se utiliza para la autenticación). Introduzca una contraseña para el usuario y

| datest 🚺 http://Nur2585 | Inder2 htm | 💌 🥐 Go Unia |
|--|--|---|
| Cisco Statema | User Setup | 0 |
| | User Setup | Help |
| Serve Starve Starve | Password Authentication: CiscoSecure Database CiscoSecure PAP (Also used for CHAP/MS- CHAP/ARAP, if the Separate field is not checked.) Password Confirm Password Separate (CHAP/MS-CHAP/ARAP) Password Confirm Password When a token server is used for authentication, | Account Disabled Deleting a Username Supplementary User Info Password Authentication Group to which the user is assigned Callback Client IP Address Assignment Advanced Settings Network Access Restrictions Max Sessions Usage Quotas Account Disable Downloadable ACLs Advanced TACACS+ Settings TACACS+ Enable Control TACACS+ Enable Password |

 Elija el grupo al que está asignado el usuario y marque Usar configuración de grupo. Haga clic en Submit (Enviar).



8. Haga clic en **Group Setup** y seleccione el grupo al que se asignó al usuario en el paso anterior. Haga clic en **Editar**

| configuració | n. | |
|--|--|---|
| CiscoSecure ACS - M | icrosoft Internet Explorer provided by Cisco Systems, Iac. | |
| the tide your figur | ordes Jook Belp | |
| -Back O. | 2 2 Queen Elevater Steda 3 2 3 2 - 3 | |
| Address Attp://fluc25 | 05/index2.htm | er والمن المنه المن المنه المن المنه ال |
| Cisco Secretos | Group Setup | × |
| | Select | Help 🔒 |
| Uter Setup Setup Setup Setup Compounds Compounds Set work Configuration | Group : FGroup J (1 user) Users in Group Edit Settings Percarre Group | Default Group Group Users in Group Edit Settings Rename Group |
| Configuration | | Default Group |
| Configuration Administration Configuration C | 2 Back to Holo | If group mapping has not been configured, usernames that are not configured in the CiscoSecure Database are assigned to the Default Group by Cisco Secure ACS the first time they log in. The privileges and restrictions for the default group- are applied to first-time users. If you have upgraded from a previous version of Cisco Secure ACS and kept your database information, users will map as configured in the previous version. |
| Done | | Cocol extranet |

Desplácese hacia abajo hasta la sección Atributos RADIUS de Cisco IOS/PIX. Marque la casilla para par cisco-av. Ingrese el comando shell que se ejecutará tras la autorización exitosa del usuario. (Este ejemplo utiliza shell:autocmd=access-enable host timeout 10.) Haga clic en Enviar+Reiniciar.



Resolución de problemas de RADIUS

Utilice estos comandos debug en el NAS para resolver problemas RADIUS.

Nota: Consulte Información Importante sobre Comandos Debug antes de utilizar los comandos debug.

• debug radius: muestra información asociada con RADIUS.

Utilice estos comandos para resolver problemas de AAA:

• debug aaa authentication — Muestra información sobre autenticación de AAA/TACACS+.

• debug aaa authorization-Muestra información sobre la autorización AAA/TACACS+.

El ejemplo de **salida debug** aquí muestra un proceso exitoso de autenticación y autorización en el ACS configurado para RADIUS.

```
Router#show debug
General OS:
 AAA Authentication debugging is on
 AAA Authorization debugging is on
Radius protocol debugging is on
Radius packet protocol debugging is on
_____
Router#
AAA/BIND(0000003): Bind i/f
AAA/AUTHEN/LOGIN (0000003): Pick method list 'default'
RADIUS/ENCODE(0000003): ask "Username: "
RADIUS/ENCODE(0000003): send packet; GET_USER
RADIUS/ENCODE(0000003): ask "Password: "
RADIUS/ENCODE(0000003): send packet; GET_PASSWORD
RADIUS: AAA Unsupported
                          [152] 5
```

```
74 74 79
RADIUS:
                                       [ttv]
RADIUS(0000003): Storing nasport 66 in rad_db
RADIUS/ENCODE(0000003): dropping service type,
 "radius-server attribute 6 on-for-login-auth" is off
RADIUS(0000003): Config NAS IP: 0.0.0.0
RADIUS/ENCODE(0000003): acct_session_id: 1
RADIUS(0000003): sending
RADIUS/ENCODE: Best Local IP-Address 172.18.124.1
 for Radius-Server 10.48.66.53
RADIUS(0000003): Send Access-Request to 10.48.66.53:1645
 id 21645/1, len 77
RADIUS: authenticator 5A 95 1F EA A7 94 99 E5 -
 BE B5 07 BD E9 05 5B 5D
                          [1] 7
                                   "test"
RADIUS: User-Name
RADIUS: User-Password
                          [2]
                               18 *
RADIUS: NAS-Port
                          [5] 6
                                    66
RADIUS: NAS-Port-Type
                          [61] 6
                                    Virtual
                                               [5]
RADIUS: Calling-Station-Id [31] 14 "171.68.109.158"
RADIUS: NAS-IP-Address [4] 6 171.68.117.189
RADIUS: Received from id 21645/1 10.48.66.53:1645,
 Access-Accept, len 93
RADIUS: authenticator 7C 14 7D CB 33 19 97 19 -
 68 4B C3 FC 25 21 47 CD
RADIUS: Vendor, Cisco
                          [26] 51
RADIUS: Cisco AVpair
                          [1] 45
 "shell:autocmd=access-enable host timeout 10"
RADIUS: Class
                          [25] 22
RADIUS: 43 49 53 43 4F 41 43 53 3A 61 63 31 32 37 63 30
 [CISCOACS:ac127c0]
RADIUS: 31 2F 36 36
                                    [1/66]
RADIUS(0000003): Received from id 21645/1
AAA/AUTHOR/EXEC(0000003): processing AV
 autocmd=access-enable host timeout 10
AAA/AUTHOR/EXEC(0000003): Authorization successful
```

Información Relacionada

- <u>Seguridad Lock-and-Key de Cisco IOS</u>
- Página de soporte de TACACS/TACACS+
- <u>TACACS+ en documentación de IOS</u>
- Página de soporte de RADIUS
- Solicitudes de Comentarios (RFC)
- Soporte Técnico y Documentación Cisco Systems