Configurando el CSU para UNIX (Solaris)

Contenido

Introducción

El Cisco Secure ACS para el software de UNIX (CSU) ayuda a asegurar la Seguridad de la red y sigue la actividad de la gente que conecta con éxito con la red. El CSU actúa como un TACACS+ o servidor de RADIUS y utiliza el Authentication, Authorization, and Accounting (AAA) para proporcionar la seguridad de la red.

El CSU soporta estas opciones de base de datos de salvar al grupo y los perfiles del usuario y información de la cuenta:

- SQLAnywhere (incluido con el CSU).Esta versión del SQLAnywhere de SYBASE no tiene el cliente/soporte de servidor. Sin embargo, se optimiza para llevar a cabo los servicios esenciales AAA con el CSU.**Precaución:** La opción de la base de datos SQLAnywhere no soporta las bases de datos del perfil que exceden 5,000 usuarios, la replicación de la información del perfil entre los sitios de la base de datos, o la característica segura del Distribute Session Manager de Cisco (DSM).
- Oracle o Sybase Relational Database Management System (RDBMS).Para soportar las bases de datos seguras del perfil de Cisco de 5,000 o más usuarios, réplica de base de datos, o la característica segura de Cisco DSM, usted debe instalar previamente un Oracle (versión 7.3.2, 7.3.3, o 8.0.3) o al servidor SQL de SYBASE (versión 11) RDBMS para llevar a

cabo su información del perfil segura de Cisco. La réplica de base de datos requiere la configuración de RDBMS adicional después de que la instalación segura de Cisco sea completa.
- La actualización de una base de datos existente de una versión anterior (2.x) del CSU.Si usted actualiza de una versión anterior 2.x de Cisco segura, Cisco asegura el programa de instalación actualiza automáticamente la base de datos del perfil para ser compatible con CSU 2.3 para UNIX.
- Importación de una base de datos existente del perfil.Usted puede convertir el freeware existente TACACS+ o las bases de datos o los archivos planos del perfil de RADIUS para el uso con esta versión del CSU.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información en este documento se basa en el Cisco Secure ACS 2.3 para UNIX.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Para obtener más información sobre las convenciones del documento, consulte las Convenciones de Consejos Técnicos de Cisco.

Configuración de CSU

Utilice estos procedimientos para configurar el CSU.

Comience la Interfaz del administrador de CiscoSecure

Utilice este procedimiento para iniciar sesión al administrador seguro de Cisco.

1. De cualquier puesto de trabajo con una conexión Web al ACS, ponga en marcha a su buscador Web.
2. Ingrese uno de estos URL para el administrador de sitio Web seguro de Cisco:Si la característica del Security Socket Layer en su hojeador no se habilita, ingrese:`http://your_server/cs`donde está el nombre del host (o el nombre de dominio completo (FQDN) el your_server, si diferencian el nombre del host y el FQDN) del SPARCstation donde usted instaló el CSU. Usted puede también substituir la dirección IP del SPARCstation para el your_server.Si la característica del Security Socket Layer en su

navegador se habilita, especifique el “https” bastante que el “HTTP” como el protocolo de transmisión del hypertext. Ingrese:`https://your_server/cs`donde está el nombre del host (o el FQDN el your_server, si diferencian el nombre del host y el FQDN) del SPARCstation donde usted instaló el CSU. Usted puede también substituir la dirección IP del SPARCstation para el your_server.**Nota:** Los URL y los nombres de servidor son con diferenciación entre mayúsculas y minúsculas. Deben ser tecleados con el mayúscula y las letras minúsculas exactamente como se muestra.Se visualiza la página del inicio CSU.
3. Ingrese su nombre de usuario y contraseña. Haga clic en Submit (Enviar).**Nota:** El nombre de usuario predeterminado inicial es “superusuario.” La contraseña predeterminada inicial es “changeme.” Después de su conexión con el sistema inicial, usted necesita cambiar el nombre de usuario y contraseña inmediatamente para la seguridad máxima.Después de que usted inicie sesión, la página principal CSU se visualiza con la barra de menú principal a lo largo del top. Se visualiza la página de menú principal CSU solamente si el usuario proporciona un nombre y una contraseña que tengan privilegios del administrador-nivel. Si el usuario proporciona un nombre y una contraseña que tengan solamente privilegios del nivel de usuario, después se visualiza una diversa pantalla.

Encienda el programa de configuración avanzada

Encienda el programa de configuración avanzada seguro del administrador de Cisco de la Java basada de las páginas web unas de los del administrador CSU. De la barra de menú de la interfaz Web CSU, haga clic **avanzado**, y después haga clic **avanzado** otra vez.

Se visualiza el programa de configuración avanzada seguro del administrador de Cisco. Puede ser que tarde posiblemente algunos minutos para cargar.

Cree un perfil del grupo

Utilice el programa de configuración avanzada seguro del administrador de Cisco para crear y para configurar los perfiles del grupo. Cisco recomienda que usted crea los perfiles del grupo para configurar los requisitos detallados AAA para un gran número de usuarios similares. Después de que se defina el perfil del grupo, utilice el CSU agregan una página web del usuario para agregar rápidamente los perfiles del usuario al perfil del grupo. Los requerimientos avanzados configurados para el grupo se aplican a cada usuario miembro.

Utilice este procedimiento para crear un perfil del grupo.

1. En el programa de configuración avanzada seguro del administrador de Cisco, seleccione la lengueta de los **miembros**. En el panel Navigator (Navegador), no reelija como candidato la casilla de verificación de la **ojeada**. Las nuevas visualizaciones del icono del perfil del crear.
2. En el panel Navigator (Navegador), haga uno de éstos:Para crear un perfil del grupo sin el padre, localice y haga clic el icono de la carpeta del [Root].Para crear su perfil del grupo como el niño de otro perfil del grupo, localice al grupo que usted quiere como el padre y hace clic lo.Si el grupo que usted quisiera que fuera el padre es un grupo derivado, haga clic su carpeta del grupo de padre para visualizarla.
3. El tecleo **crea el nuevo perfil**. Las nuevas visualizaciones del cuadro de diálogo del perfil.
4. Seleccione el cuadro de **casilla del grupo**, teclee el nombre del grupo que usted quiere crear, y haga clic la **AUTORIZACIÓN**. Las nuevas visualizaciones del grupo en el árbol.
5. Después de que usted cree el perfil del grupo, asigne el TACACS+ o los atributos de

RADIUS para configurar las Propiedades AAA específicas.

Cree un perfil del usuario en el modo de la configuración avanzada

Utilice al modo de configuración del administrador de Secure de Cisco para crear y para configurar un perfil del usuario. Usted puede hacer esto para personalizar la autorización y los atributos relacionados a la contabilidad del perfil del usuario más detalladamente que posible con el agregar a la página del usuario.

Utilice este procedimiento para crear un perfil del usuario:

1. En el programa de configuración avanzada seguro del administrador de Cisco, seleccione la lengueta de los **miembros**. En el panel Navigator (Navegador), localice y no reelija como candidato **hojean**. Las nuevas visualizaciones del icono del perfil del crear.
2. En el panel Navigator (Navegador), haga uno de éstos:Localice y haga clic al grupo a quien el usuario pertenece.Si usted no quisiera que el usuario perteneciera a un grupo, haga clic el icono de la carpeta del [Root].
3. El tecleo **crea el perfil**. Las nuevas visualizaciones del cuadro de diálogo del perfil.
4. Aseegurese que el cuadro de **casilla del grupo** está no reelegido como candidato.
5. Ingrese el nombre del usuario que usted quiere crear y hacer clic la **AUTORIZACIÓN**. Las visualizaciones del usuario nuevo en el árbol.
6. Después de que usted cree el perfil del usuario, asigne el TACACS+ específico o los atributos de RADIUS para configurar las Propiedades AAA específicas:Para asignar los perfiles TACACS+ al perfil del usuario, vea para asignar los atributos TACACS+ a un grupo o perfil de usuario.Para asignar los perfiles de RADIUS al perfil del usuario, vea para asignar los atributos de RADIUS a un grupo o perfil de usuario.

Estrategias para aplicar los atributos

Utilice la característica del perfil del grupo CSU y el TACACS+ y los atributos de RADIUS para implementar la autenticación y autorización de los usuarios de la red con el CSU.

Planee los atributos para los grupos y los usuarios

La característica del perfil del grupo CSU le permite para definir al conjunto común de requerimientos AAA para un gran número de usuarios.

Usted puede asignar un conjunto de TACACS+ o los valores de atributo de RADIUS a un perfil del grupo. Estos valores de atributo asignados al grupo se aplican a cualquier usuario que sea un miembro o que se agregue como miembro de ese grupo.

Utilice la característica del perfil del grupo eficazmente

Para configurar el CSU para manejar a diversos y númerosos tipos de usuarios con los requerimientos de AAA complejos, Cisco recomienda que usted utiliza las características del programa de configuración avanzada seguro del administrador de Cisco para crear y para configurar los perfiles del grupo.

El perfil del grupo necesita contener todos los atributos que no sean específicos al usuario. Esto

significa generalmente todos los atributos a excepción de la contraseña. Usted puede entonces utilizar el agregar una página del usuario del administrador seguro de Cisco para crear los perfiles del usuario simples con los atributos de la contraseña y para asignar estos perfiles del usuario al perfil del grupo apropiado. Las características y los valores de atributo definidos para un grupo determinado entonces se aplican a sus usuarios miembros.

Grupos y grupos derivados de padre

Usted puede crear una jerarquía de los grupos. Dentro de un perfil del grupo, usted puede crear los perfiles de grupo derivado. Los valores de atributo asignados al perfil del grupo del padre son valores predeterminados para los perfiles de grupo derivado.

La administración del nivel de grupo

Un administrador de sistema seguro de Cisco puede asignar el estatus individual del administrador del grupo de Usuarios usuarios seguros de Cisco. El estatus del administrador del grupo permite a los usuarios individuales para administrar cualquier perfil de grupo derivado y los perfiles del usuario que son subordinados a su grupo. Sin embargo, él no permite que él administre a ninguna grupos o los usuarios que bajan fuera de la jerarquía de su grupo. Así, el administrador de sistema empaqueta hacia fuera la tarea de administrar una Red grande a otros individuos sin la concesión cada uno de ellos de la autoridad igual.

¿Qué atributos defino para los usuarios individuales?

Cisco recomienda que usted asigna a usuarios individuales los valores de atributo de la autenticación básica que son únicos al usuario, tal como atributos que definan el nombre de usuario, la contraseña, el tipo de contraseña, y el privilegio de la red. Asigne los valores de atributo de la autenticación básica a sus usuarios con el Edit a User CSU o agregue las páginas del usuario.

¿Qué atributos defino para los perfiles del grupo?

Cisco recomienda que usted define la calificación, la autorización, y los atributos relacionados a la contabilidad en el nivel de grupo.

En este ejemplo, el perfil del grupo nombrado los “usuarios de dial in” se asigna los pares de valor de atributo Frame-Protocol=PPP y Service-Type=Framed.

¿Cuáles son atributos absolutos?

Un subconjunto del TACACS+ y los atributos de RADIUS en el CSU se pueden asignar el estado absoluto en el nivel del perfil del grupo. Un valor de atributo habilitado para el estado absoluto en el nivel del perfil del grupo reemplaza cualquier valor de atributo contendiente en un nivel del perfil del perfil de grupo derivado o de usuario miembro.

Dentro de las redes de niveles múltiples con varios niveles de administradores del grupo, los atributos absolutos permiten a un administrador de sistema para fijar los valores de atributo del grupo seleccionados que agrupan a los administradores en los niveles inferiores no pueden reemplazar.

Atributos que se pueden asignar a visualización de estado absoluto una casilla de selección absoluta en el cuadro de los atributos del programa de configuración avanzada seguro del administrador de Cisco. Seleccione la casilla de verificación para habilitar el estado absoluto.

¿Pueden los valores de atributo del grupo y los valores de atributo de usuario estar en conflicto?

La resolución de conflicto entre los valores de atributo asignados para parent los perfiles del grupo, los perfiles de grupo derivado, y los perfiles de usuario miembro depende encendido si los valores de atributo son absolutos y si son TACACS+ o atributos de RADIUS:

- TACACS+ o valores de atributo de RADIUS asignados a un perfil del grupo con la invalidación del estado absoluto cualquier valores de atributo contendiente fijados en un grupo derivado o un nivel del perfil del usuario.
- Si no habilitan al estado absoluto de un valor de atributo TACACS+ en el nivel del perfil del grupo, es reemplazado por cualquier valor de atributo contendiente fijado en un grupo derivado o un nivel del perfil del usuario.
- Si no habilitan a un estado absoluto del valor de atributo de RADIUS en el nivel de grupo de padre, después cualquier valor de atributo contendiente fija en un resultado del grupo derivado en un resultado impredecible. Cuando usted define los valores de atributo de RADIUS para un grupo y sus usuarios miembros, evite asignar el mismo atributo al usuario y a los perfiles del grupo.

Utilice las opciones de prohibición y permiso

Para el TACACS+, reemplace la Disponibilidad de los valores heredados del servicio prefijando la palabra clave **prohíben** o **permiten a la** especificación del servicio. La palabra clave del **permiso** permite los servicios especificados. La palabra clave del **prohibir** rechaza los servicios especificados. Con el uso de estas palabras claves junto, usted puede construir “todo excepto” las configuraciones. Por ejemplo, esta configuración permite el acceso de todos los servicios excepto el X.25:

```
default service = permit
prohibit service = x25
```

Asigne los atributos TACACS+ a un grupo o perfil de usuario

Para asignar los servicios específicos y los atributos TACACS+ a un grupo o perfil de usuario, siga los siguientes pasos:

1. En el programa de configuración avanzada seguro del administrador de Cisco, seleccione la lengueta de los **miembros**. En el panel Navigator (Navegador), haga clic el icono para el grupo o perfil de usuario al cual se asignan los atributos TACACS+.
2. En caso necesario, en el cristal del perfil, haga clic el icono del **perfil** para ampliarlo.Una lista o un cuadro de diálogo que contienen los atributos aplicables al perfil o al servicio seleccionado visualiza en la ventana en la inferior derecha de la pantalla. La información en esta ventana cambia basado en qué perfil o manténgale seleccionan en el cristal del perfil.
3. Haga clic el servicio o el protocolo que usted quiere agregar y el tecleo **se aplican**. El servicio se agrega al perfil.
4. Ingrese o seleccione el texto necesario en la ventana del atributo.Las entradas válidas se explican en las estrategias para aplicar la sección de los atributos del CSU 2.3 para el guía

de referencia de UNIX.**Nota:** Si usted asigna un valor de atributo en el nivel del perfil del grupo, y el atributo que usted especifica las visualizaciones una **casilla de selección absoluta**, seleccione esa casilla de verificación para asignar el estado absoluto del valor. Un estado absoluto con valor asignado no puede ser reemplazado por ninguna valores de afirmación asignada en el perfil de grupo subordinado o los niveles del perfil del usuario.
5. Relance los pasos 1 a través para cada servicio adicional o protocolo que usted necesita agregar.
6. Cuando se realizan todos los cambios, el tecleo **somete**.

Asigne los atributos de RADIUS a un grupo o perfil de usuario

Para asignar los atributos de RADIUS específicos a un grupo o perfil de usuario:

1. Asigne un diccionario de RADIUS al perfil del grupo:En la página de los miembros del programa de configuración avanzada seguro del administrador de Cisco, haga clic el **grupo** o el **icono Usuario**, después haga clic el icono del **perfil** en el cristal de los perfiles. En el cristal de los atributos, las visualizaciones del menú de opciones.En el **menú de opciones**, haga clic el nombre del diccionario de RADIUS que usted quisiera que el grupo o el usuario utilizara. (Por ejemplo, RADIUS - Cisco.) Haga clic en Apply (Aplicar).
2. Agregue los elementos de verificación requeridos y conteste los atributos al perfil de RADIUS:**Nota:** Los elementos de verificación son atributos requeridos para la autenticación, tal como identificación del usuario y contraseña. Los atributos de la contestación son atributos enviados al servidor de acceso a la red (NAS) después de que el perfil haya pasado el procedimiento de autenticación, tal como Protocolo Entramado. Para las listas y las explicaciones de los elementos de verificación y de los atributos de la contestación, refiera a los Pares valor-atributo de RADIUS y a la administración del diccionario en el CSU 2.3 para el guía de referencia de UNIX.En la ventana del perfil, haga clic el RADIUS - icono de la carpeta del dictionaryname. (Usted necesita probablemente hacer clic el perfil + el símbolo para ampliar la carpeta RADIUS.) Los elementos de verificación y la visualización de las opciones de los atributos de la contestación en la ventana de grupo de atributos.Para utilizar uno o más de estos atributos, hacer clic los atributos que usted quiere utilizar, después hacer clic **apliqúese**. Usted puede agregar más de un en un momento del atributo.Haga clic **+** símbolo para el RADIUS - dictionaryname para ampliar la carpeta.**Nota:** Si usted selecciona la opción RADIUS-Cisco11.3, aseegurese que la versión del Cisco IOS ® Software 11.3.3(T) o más adelante está instalada en sus NAS de conexión y agregue las líneas de comando new a sus Configuraciones de NAS. Refiera completamente a habilitar el diccionario RADIUS-Cisco11.3 en el CSU 2.3 para el guía de referencia de UNIX.
3. Especifique los valores para los elementos de verificación agregados y conteste los atributos:**Precaución:** Para el protocolo RADIUS, la herencia es aditiva en comparación con jerárquico. (El protocolo TACACS+ utiliza la herencia jerárquica). Por ejemplo, si usted asigna los mismos atributos de la contestación al usuario y a los perfiles del grupo, la autorización falla porque el NAS recibe dos veces el número de atributos. No puede tener sentido de los atributos de la contestación. No asigne el mismo atributo del elemento de verificación o de la contestación al grupo y a los perfiles del usuario.Haga clic los **elementos de verificación** o **conteste los atributos**, o haga clic ambos. Una lista de elementos de verificación y de valores de atributos aplicables de la contestación aparece en la ventana de la derecha más baja. Haga clic **+** símbolo para ampliar la carpeta.Haga clic los valores que

usted quiere asignar, después haga clic **se aplican**. Para más información sobre los valores, refiera a los Pares valor-atributo de RADIUS y a la administración del diccionario en el CSU 2.3 para el guía de referencia de UNIX.**Nota:** Si usted asigna un valor de atributo en el nivel del perfil del grupo, y el atributo que usted especifica las visualizaciones una casilla de selección absoluta, seleccione esa casilla de verificación para asignar el estado absoluto del valor. Un valor asignado el estado absoluto no se puede reemplazar por ninguna valores de afirmación asignada en el perfil de grupo subordinado o los niveles del perfil del usuario.Cuando usted ha acabado de realizar los cambios, el tecleo **somete**.
4. Para utilizar uno o más de estos atributos, hacer clic los atributos que usted quiere utilizar, después hacer clic **apliqúese**. Usted puede aplicar más de un en un momento del atributo.

Asigne los niveles de privilegio de control de acceso

El administrador del superusuario utiliza el atributo del privilegio de la red para asignar un nivel de privilegio de control de acceso a los Usuarios usuarios seguros de Cisco.

1. En el programa de configuración avanzada seguro del administrador de Cisco, haga clic al usuario cuyo privilegio de control de acceso usted quiere asignar, después hace clic el icono del perfil en el cristal de los perfiles.
2. En el menú de opciones, haga clic el **privilegio de la red** y seleccione uno de estos valores.**0** - Niega a usuario cualquier privilegio de control de acceso que incluya la capacidad de cambiar la contraseña segura de Cisco del usuario.**1** - Concede el acceso del usuario a la página web de CSUser. Esto permite que los Usuarios usuarios seguros de Cisco cambien sus contraseñas seguras de Cisco. Para más información sobre cómo cambiar las contraseñas, refiera a las funciones del nivel de usuario (que cambian una contraseña) en la administración de ACS y usuario simple.**12** - Concede los privilegios de administrador del grupo de usuario.**15** - Concede los privilegios de administrador del sistema del usuario.**Nota:** Si usted selecciona alguna opción de privilegio Web con excepción de 0, usted debe también especificar una contraseña. Para satisfacer el requisito de contraseña del privilegio de la red, un solo espacio en blanco es como mínimo aceptable.

Comience y pare el CSU

Generalmente, el CSU comienza automáticamente cuando usted comienza o recomienza el SPARCstation donde está instalado. Sin embargo, usted puede comenzar el CSU manualmente, o cerrarlo sin apagar el SPARCstation entero.

Inicie sesión como [Root] al SPARCstation donde usted instaló el CSU.

Para comenzar el CSU manualmente, teclee:

```
# /etc/rc2.d/S80CiscoSecure
```

Para parar el CSU manualmente, teclee:

```
# /etc/rc0.d/K80CiscoSecure
```

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshooting

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- Página de soporte de Cisco Secure ACS para Windows
- Página de soporte TACACS/TACACS+
- Página de soporte de RADIUS
- Solicitudes de Comentarios (RFC)
- Soporte Técnico y Documentación - Cisco Systems