Integración del administrador de seguridad con el ACS

Contenido

Introducción
prerrequisitos
Requisitos
Componentes Utilizados
Convenciones
Integre al Cisco Security Manager con el Cisco Secure ACS
Procedimientos de la integración realizados en el Cisco Secure ACS
Defina los usuarios y a los grupos de usuarios en el Cisco Secure ACS
Agregue los dispositivos administrados como clientes AAA en el Cisco Secure ACS
Agregue los dispositivos como clientes AAA sin NDGs
Configure a los grupos de dispositivos de red para el uso en el administrador de seguridad
Procedimientos de la integración realizados en los CiscoWorks
Cree a un usuario local en los CiscoWorks
Defina al usuario de la identidad del sistema
Configure al modo de configuración AAA en los CiscoWorks
Recomience al administrador de Daemon
Asigne los papeles a los grupos de usuarios en el Cisco Secure ACS
Asigne los papeles a los grupos de usuarios sin NDGs
Asocie NDGs y los papeles a los grupos de usuarios
Troubleshooting
Información Relacionada

Introducción

Este documento describe cómo integrar al Cisco Security Manager con el Cisco Secure Access Control Server (ACS).

El Cisco Secure ACS proporciona el comando authorization para los usuarios que utilizan las aplicaciones de administración, tales como Cisco Security Manager, para configurar los dispositivos de la red administrada. El soporte para el comando authorization es proporcionado por los tipos únicos del conjunto del comando authorization, llamados los papeles en el Cisco Security Manager, que contienen un conjunto de los permisos. Estos permisos, los privilegios también llamados, determinan las acciones que los usuarios con los rol específicos pueden realizar dentro del Cisco Security Manager.

Aplicaciones TACACS+ del Cisco Secure ACS para comunicar con las aplicaciones de administración. Para que el Cisco Security Manager comunique con el Cisco Secure ACS, usted

debe configurar Servidor CiscoWorks adentro el Cisco Secure ACS como cliente AAA que utilice el TACACS+. Además, usted debe proporcionar Servidor CiscoWorks con el nombre y la contraseña del administrador que usted utiliza para registrar en el Cisco Secure ACS. Cuando usted satisface estos requisitos, asegura la validez de las comunicaciones entre el Cisco Security Manager y el Cisco Secure ACS.

Cuando el Cisco Security Manager comunica inicialmente con el Cisco Secure ACS, dicta a Cisco ACS la creación de los papeles predeterminados, que aparecen en la sección de los componentes del perfil compartidos de la interfaz de HTML del Cisco Secure ACS. También dicta un servicio de encargo que se autorizará por el TACACS+. Este servicio de encargo aparece en la página TACACS+ (Cisco IOS®) en la sección de configuración de la interfaz de la interfaz de HTML. Usted puede después modificar los permisos incluidos en cada papel del Cisco Security Manager y aplicar estos papeles a los usuarios y a los grupos de usuarios.

Nota: No es posible integrar el CS con ACS 5.2 pues no se soporta.

prerrequisitos

Requisitos

Para utilizar el Cisco Secure ACS, aseegurese que:

- Usted define los papeles que incluyen los comandos required para realizar las funciones necesarias en el Cisco Security Manager.
- La restricción del acceso a la red (NAR) incluye el grupo de dispositivos (o los dispositivos) ese usted quiere administrar, si usted aplica un NAR al perfil.
- Los nombres de dispositivo administrado se deletrean y se capitalizan idénticamente en el Cisco Secure ACS y en el Cisco Security Manager.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Versión 3.0 del Cisco Security Manager
- Versión 3.3 del Cisco Secure ACS

Nota: Aseegurese que usted elige el CS y los ACS versión compatibles antes de que usted instale en su entorno de red. Por ejemplo, Cisco probó ACS 3.3 con solamente el 3.0 CS y paró para CSM versión posteriores. Así pues, le recomiendan para utilizar el 3.0 CS con ACS 3.3. Vea la tabla de matrices de Compatabilty para más información sobre las diversas versiones de software.

Versiones del Cisco Security Manager	ACS versión CS probados
3.0.0 3.0.0 SP1	Windows 3.3(3) y 4.0(1)
3.0.1 3.0.1 SP1 3.0.1 SP2	Motor de las soluciones 4.0(1) Windows 4.0(1)
3.1.0 3.0.2	Motor de las soluciones 4.0(1) Windows 4.1(1) y 4.1(3)

3.1.1 3.0.2 SP1 3.0.2 SP2	Motor de las soluciones v4.0(1) Windows 4.1(2), 4.1(3) y 4.1(4)
3.1.1 SP1	Motor de las soluciones 4.0(1) Windows 4.1(4)
3.1.1 SP2	Motor de las soluciones 4.0(1) Windows 4.1(4) y 4.2(0)
3.2.0	Motor de las soluciones 4.1(4) Windows 4.1(4) y 4.2(0)
3.2.1	Motor de las soluciones 4.1(4) Windows 4.2(0)

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

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

Integre al Cisco Security Manager con el Cisco Secure ACS

Esta sección describe los pasos requeridos para integrar al Cisco Security Manager con el Cisco Secure ACS. Algunos pasos contienen varios substeps. Estos pasos y substeps se deben realizar en la orden. Esta sección también contiene las referencias a los procedimientos específicos usados para realizar cada paso.

Complete estos pasos:

1. **Planee su modelo de la autenticación administrativa y de la autorización.**Usted debe decidir sobre su modelo administrativo antes de que usted utilice al Cisco Security Manager. El incluye la definición de los papeles administrativos y las cuentas que usted planea utilizar.**Consejo:** Cuando usted define los papeles y los permisos de los posibles administradores, también considere independientemente de si habilitar el flujo de trabajo. Influencias de esta selección cómo usted puede restringir el acceso.
2. **Instale el Cisco Secure ACS, el Cisco Security Manager, y el CiscoWorks Common Services.**Instale la versión 3.3 del Cisco Secure ACS en Windows 2000/2003 servidor. Instale el CiscoWorks Common Services y al Cisco Security Manager en un diverso servidor de Windows 2000/Windows 2003.Si desea más información, consulte estos documentos:Guía de instalación para el Cisco Security Manager 3.0Guía de instalación para el Cisco Secure ACS for Windows 3.3**Nota:** Vea la tabla de la Matriz de compatibilidad para más información antes de que usted elija las versiones CS y del software ACS.
3. **Realice los procedimientos de la integración en el Cisco Secure ACS.**Defina a los usuarios del Cisco Security Manager como usuarios de ACS y asígnelos a los grupos de usuarios basados en su papel previsto, agregue todos sus dispositivos administrados (así como el servidor de los CiscoWorks/del administrador de seguridad) como clientes AAA, y cree Administration Control (Control de administración) a un usuario. Vea los procedimientos de

la integración realizados en el Cisco Secure ACS para más información.

4. **Realice los procedimientos de la integración en el CiscoWorks Common Services.**Configure a un usuario local que haga juego al administrador definido en el Cisco Secure ACS, definen que el mismo usuario para la configuración de la identidad del sistema, y la configuración ACS como el modo de configuración AAA.Vea los procedimientos de la integración realizados en los CiscoWorks para más información.
5. **Asigne los papeles a los grupos de usuarios en el Cisco Secure ACS.**Asigne los papeles a cada grupo de usuarios configurado en el Cisco Secure ACS. El procedimiento que usted utiliza depende encendido si usted tiene grupos de dispositivos de la red configurada (NDGs).Vea para asignar los papeles a los grupos de usuarios en el Cisco Secure ACS para más información.

Procedimientos de la integración realizados en el Cisco Secure ACS

Esta sección describe los pasos que usted debe completar en el Cisco Secure ACS para integrarlo con el Cisco Security Manager:

1. Defina los usuarios y a los grupos de usuarios en el Cisco Secure ACS
2. Agregue los dispositivos administrados como clientes AAA en el Cisco Secure ACS
3. Cree Administration Control (Control de administración) a un usuario en el Cisco Secure ACS

Defina los usuarios y a los grupos de usuarios en el Cisco Secure ACS

Todos los usuarios del Cisco Security Manager deben ser definidos en el Cisco Secure ACS y asignaron un papel apropiado a su función de trabajo. La manera más fácil de hacer esto es dividir a los usuarios en diversos grupos basados en cada papel predeterminado disponible en el ACS. Por ejemplo, asigne a todos los administradores de sistema a un grupo, todos los operadores de la red a otro grupo, y así sucesivamente. Refiera al Cisco Secure ACS omiten los papeles de más información sobre los papeles predeterminados en el ACS.

Además, usted debe crear a un usuario adicional que se asigne el papel del administrador de sistema con los permisos completos. Las credenciales establecidas para este usuario se utilizan más adelante en la página de configuración de la identidad del sistema en los CiscoWorks. Vea para definir al usuario de la identidad del sistema para más información.

Observe que usted asigna en esta etapa simplemente a los usuarios a diversos grupos. La asignación real de los papeles a estos grupos se realiza más adelante, después de los CiscoWorks, Cisco Security Manager, y cualquier otra aplicación se registra al Cisco Secure ACS.

Consejo: Antes de que usted proceda, instale el CiscoWorks Common Services y al Cisco Security Manager en un Windows 2000/2003 servidor. Instale el Cisco Secure ACS en diverso Windows 2000/2003 servidor.

1. Inicie sesión al Cisco Secure ACS.
2. Configure a un usuario con los permisos completos:Haga clic la **configuración de usuario** en la barra de navegación.En la página de la configuración de usuario, ingrese un nombre para el usuario nuevo, después haga clic **agregan/editan**.Seleccione un método de autentificación

de la lista de la autenticación de contraseña bajo configuración de usuario.Ingrese y confirme la contraseña para el usuario nuevo.Seleccione el **group1** pues el grupo a quien asignan el usuario.El tecleo **somete** para crear la cuenta de usuario.

3. Relance el paso 2 para cada usuario del Cisco Security Manager. Cisco recomienda que usted divide a los usuarios en los grupos basados en el papel que asignan cada usuario:Group1 — Administradores de sistemaGroup2 — Administradores de seguridadGroup3 — Seguridad ApproversGrupo 4 — Administradores de la redGrupo 5 — ApproversGrupo 6 — Operadores de la redGrupo 7 — Escritorio de ayudaVea la tabla para más información sobre los permisos predeterminados asociados a cada papel. Refiera a personalizar los papeles del Cisco Secure ACS de más información sobre personalizar los rol del usuario.**Nota:** En esta etapa, los grupos ellos mismos son conjuntos de usuarios sin ningunas definiciones del papel. Usted asigna los papeles a cada grupo después de que usted complete el proceso de integración. Vea para asignar los papeles a los grupos de usuarios en el Cisco Secure ACS para más información.
4. Cree a un usuario adicional y asigne a este usuario al grupo de los administradores de sistema. Las credenciales establecidas para este usuario se utilizan más adelante en la página de configuración de la identidad del sistema en los CiscoWorks. Vea para definir al usuario de la identidad del sistema para más información.
5. Continúe con agregan los dispositivos administrados como clientes AAA en el Cisco Secure ACS.

Agregue los dispositivos administrados como clientes AAA en el Cisco Secure ACS

Antes de que usted pueda comenzar a importar los dispositivos en el Cisco Security Manager, usted debe primero configurar cada dispositivo como cliente AAA en su Cisco Secure ACS. Además, usted debe configurar el servidor de los CiscoWorks/del administrador de seguridad como cliente AAA.

Si el Cisco Security Manager maneja los contextos de seguridad configurados en los dispositivos del Firewall, que incluye los contextos de seguridad configuró en los FWSM para los dispositivos del Catalyst 6500/7600, cada contexto se debe agregar individualmente al Cisco Secure ACS.

El método que usted utiliza para agregar los dispositivos administrados depende encendido si usted quiere restringir a los usuarios para manejar un conjunto de dispositivos determinado con los grupos de dispositivos de red (NDGs). Vea una de estas secciones:

- Si usted quisiera que los usuarios tuvieran acceso a todos los dispositivos, agregue los dispositivos como descrito adentro agregue los dispositivos como clientes AAA sin NDGs.
- Si usted quisiera que los usuarios tuvieran acceso solamente a cierto NDGs, agregue los dispositivos según lo descrito en los grupos de dispositivos de red de la configuración para el uso en el administrador de seguridad.

Agregue los dispositivos como clientes AAA sin NDGs

Este procedimiento describe cómo agregar los dispositivos como clientes AAA de un Cisco Secure ACS. Refiera a la *sección de configuración del cliente AAA de la* configuración de red para toda la información sobre todas las opciones disponibles.

Nota: Recuerde agregar el servidor de los CiscoWorks/del administrador de seguridad como

cliente AAA.

1. Haga clic la **configuración de red** en la barra de navegación del Cisco Secure ACS.
2. El tecleo **agrega la entrada** debajo de la tabla de los clientes AAA.
3. Ingrese Nombre del host del cliente AAA (hasta 32 caracteres) en la página del cliente AAA del agregar. El nombre de host del cliente AAA debe hacer juego el nombre de la visualización que usted planea utilizar para el dispositivo en el Cisco Security Manager.Por ejemplo, si usted se prepone añadir un Domain Name al final del fichero al Nombre del dispositivo en el Cisco Security Manager, Nombre del host del cliente AAA adentro el ACS debe ser **<device_name>.<domain_name>**.Cuando usted nombra Servidor CiscoWorks, se recomienda para utilizar el nombre de host calificado completamente. Esté seguro de deletrear el nombre de host correctamente. El nombre de host no es con diferenciación entre mayúsculas y minúsculas.Cuando usted nombra los contextos de seguridad, añada el nombre del contexto al final del fichero (_**<context_name>**) al Nombre del dispositivo. Para los FWSM, ésta es la convención para nombres:Cuchilla FWSM — **<chassis_name>_FW_<slot_number>**Contextos de seguridad — **<chassis_name>_FW_<slot_number>_<context_name>**
4. Ingrese el IP Address del dispositivo de red en el campo del IP Address del cliente AAA.
5. Ingrese el secreto compartido en el campo clave.
6. Seleccione **TACACS+ (Cisco IOS) de la** autenticidad usando la lista.
7. El tecleo **somete** para salvar sus cambios. El dispositivo que usted agregó aparece en la tabla de los clientes AAA.
8. Relance los pasos 1 a 7 para agregar los dispositivos adicionales.
9. Después de que usted agregue todos los dispositivos, haga clic **Submit + Restart**.
10. Continúe con crean Administration Control (Control de administración) a un usuario en el Cisco Secure ACS.

Configure a los grupos de dispositivos de red para el uso en el administrador de seguridad

El Cisco Secure ACS le permite para configurar a los grupos de dispositivos de red (NDGs) que contienen los dispositivos específicos que se manejarán. Por ejemplo, usted puede crear NDGs para cada región geográfica o NDGs que hagan juego su estructura de organización. Cuando están utilizados con el Cisco Security Manager, permiso de NDGs usted para proporcionar a los usuarios con diversos niveles de permisos, sobre la base de los dispositivos necesitan manejar. Por ejemplo, con NDGs usted puede asignar los permisos del administrador de sistema del usuario A a los dispositivos situados en los permisos de Europa y del escritorio de ayuda a los dispositivos situados en Asia. Usted puede entonces asignar los permisos opuestos al usuario B.

NDGs no se asigna directamente a los usuarios. Bastante, NDGs se asigna a los papeles que usted define para cada grupo de usuarios. Cada NDG se puede asignar a un solo papel solamente, pero cada papel puede incluir NDGs múltiple. Estas definiciones se guardan como parte de la configuración para el grupo de usuario seleccionado.

Estos temas delinean los pasos básicos requeridos para configurar NDGs:

- Active la característica NDG
- Cree NDGs
- Asocie NDGs y los papeles a los grupos de usuarios

Active la característica NDG

Usted debe activar la característica NDG antes de que usted pueda crear NDGs y poblarlos con los dispositivos.

1. **Configuración de la interfaz del** tecleo en la barra de navegación del Cisco Secure ACS.
2. Haga clic en **Advanced Options**.
3. Navegue hacia abajo, después marque la casilla de verificación de los **grupos de dispositivos de red**.
4. Haga clic en Submit (Enviar).
5. Continúe con crean NDGs.

Cree NDGs

Este procedimiento describe cómo crear NDGs y poblarlos con los dispositivos. Cada dispositivo puede pertenecer a solamente un NDG.

Nota: Cisco recomienda que usted crea un NDG especial que contenga el servidor de los CiscoWorks/del administrador de seguridad.

1. **Configuración de red del** tecleo en la barra de navegación.Todos los dispositivos se ponen inicialmente bajo no asignado, que lleva a cabo todos los dispositivos que no fueron puestos en un NDG. Tenga presente que no asignado no es un NDG.
2. Cree NDGs:El tecleo **agrega la entrada**.Ingrese un nombre para el NDG en la nueva página del grupo de dispositivos de red. El Largo máximo es 24 caracteres. Se permiten los espacios.**Opcional cuando con la versión 4.0 o posterior:** Ingrese una clave que se utilizará por todos los dispositivos en el NDG. Si usted define una clave para el NDG, reemplaza cualquier clave definida para los dispositivos individuales en el NDG.El tecleo **somete** para salvar el NDG.Relance los pasos a d para crear más NDGs.
3. Pueble el NDGs con los dispositivos:Haga clic el nombre del NDG en el área de los grupos de dispositivos de red.El tecleo **agrega la entrada** en el área de los clientes AAA.Defina los detalles del dispositivo para agregar al NDG, después haga clic **someten**. Vea para agregar los dispositivos como clientes AAA sin NDGs para más información.Relance los pasos b y c para agregar el resto de los dispositivos a NDGs. El único dispositivo que usted puede dejar en la categoría no asignada es el servidor de AAA predeterminado.Después de que usted configure el dispositivo más reciente, haga clic **Submit + Restart**.
4. Continúe con crean Administration Control (Control de administración) a un usuario en el Cisco Secure ACS.

Cree Administration Control (Control de administración) a un usuario en el Cisco Secure ACS

Utilice Administration Control (Control de administración) la página en el Cisco Secure ACS para definir la cuenta del administrador se utiliza que al definir al modo de configuración AAA en el CiscoWorks Common Services. Vea la configuración el modo de configuración AAA en los CiscoWorks para más información.

1. Haga clic **Administration Control (Control de administración)** en la barra de navegación del Cisco Secure ACS.
2. El tecleo **agrega al administrador**.

3. En la página del administrador del agregar, ingrese un nombre y una contraseña para el administrador.
4. Haga clic a **Grant todo** en el área de los privilegios de administrador para proporcionar los permisos administrativos completos a este administrador.
5. El tecleo **somete** para crear al administrador.

Nota: Refiera a los administradores y a la directiva administrativa para más información sobre las opciones disponibles cuando usted configura a un administrador.

Procedimientos de la integración realizados en los CiscoWorks

Esta sección describe los pasos para completar en el CiscoWorks Common Services para integrarlo con el Cisco Security Manager:

- Cree a un usuario local en los CiscoWorks
- Defina al usuario de la identidad del sistema
- Configure al modo de configuración AAA en los CiscoWorks

Complete estos pasos después de que usted complete los procedimientos de la integración realizados en el Cisco Secure ACS. Los servicios comunes realizan el registro real de cualquier aplicación instalada, tal como Cisco Security Manager, Auto Update Server, y administrador IPS en el Cisco Secure ACS.

Cree a un usuario local en los CiscoWorks

Utilice la página de configuración del usuario local en el CiscoWorks Common Services para crear una cuenta de usuario local que duplique al administrador que usted creó previamente en el Cisco Secure ACS. Esta cuenta de usuario local se utiliza más adelante para la configuración de la identidad del sistema. Vea para más información.

Nota: Antes de que usted proceda, cree a un administrador en el Cisco Secure ACS. Vea para definir los usuarios y a los grupos de usuarios en el Cisco Secure ACS para las instrucciones.

1. Registro en los CiscoWorks con la cuenta de **Usuario administrador** predeterminada.
2. Elija la **Seguridad del server> de los** servicios comunes, después elija al **usuario local puesto del** TOC.
3. Haga clic en Add (Agregar).
4. Ingrese el mismo nombre y contraseña que usted ingresó cuando usted creó al administrador en el Cisco Secure ACS. Vea el paso 4 adentro definir los usuarios y a los grupos de usuarios en el Cisco Secure ACS.
5. Marque todas las casillas de verificación bajo papeles excepto los datos de la exportación.
6. Haga Click en OK para crear al usuario.

Defina al usuario de la identidad del sistema

Utilice la página de configuración de la identidad del sistema en el CiscoWorks Common Services para crear a un usuario de la confianza, conocido como el usuario de la identidad del sistema, que habilita la comunicación entre los servidores que son parte del mismo dominio y los procesos de la aplicación que están situados en el mismo servidor. Las aplicaciones utilizan al usuario de la identidad del sistema para autenticar los procesos en los servidores locales o remotos de los CiscoWorks. Esto es especialmente útil cuando las aplicaciones deben sincronizar antes de que

cualquier usuario haya abierto una sesión.

Además, el usuario de la identidad del sistema es de uso frecuente para realizar una subtarea cuando la tarea primaria se autoriza ya para el usuario autenticado. Por ejemplo, para editar un dispositivo en el Cisco Security Manager, la comunicación del interapplication se requiere entre el Cisco Security Manager y el DCR de los servicios del campo común. Después de que autoricen al usuario a realizar la tarea que edita, utilizan al usuario de la identidad del sistema para invocar el DCR.

El usuario de la identidad del sistema que usted configura aquí debe ser idéntico al usuario con los permisos (completos) administrativos que usted configuró en el ACS. El error hacer tan puede dar lugar a una incapacidad para ver todos los dispositivos y directivas configurados en el Cisco Security Manager.

Nota: Antes de que usted proceda, cree a un usuario local con el mismo nombre y contraseña que este administrador en el CiscoWorks Common Services. Vea para crear a un usuario local en los CiscoWorks para las instrucciones.

1. Elija la **Seguridad del server>**, después elija la **Administración de confianza multiservidora > la identidad del sistema puestas del** TOC.
2. Ingrese el nombre del administrador que usted creó para el Cisco Secure ACS. Vea el paso 4 adentro definir los usuarios y a los grupos de usuarios en el Cisco Secure ACS.
3. Ingrese y verifique la contraseña para este usuario.
4. Haga clic en Apply (Aplicar).

Configure al modo de configuración AAA en los CiscoWorks

Utilice la página del modo de configuración AAA en el CiscoWorks Common Services para definir su Cisco Secure ACS como el servidor de AAA, que incluye el puerto y la clave secreta compartida requeridos. Además, usted puede definir a hasta dos servidores de backup.

Estos pasos realizan el registro real de los CiscoWorks, Cisco Security Manager, administrador IPS (y opcionalmente, Auto Update Server) en el Cisco Secure ACS.

1. Elija la **Seguridad del server>**, después elija el **modo AAA puesto del** TOC.
2. Marque la casilla de verificación **TACACS+** bajo los módulos disponibles del login.
3. Seleccione el **ACS** como el tipo AAA.
4. Ingrese los IP Addresses de hasta tres servidores del Cisco Secure ACS en el área de los detalles del servidor. Los servidores secundarios y terciarios actúan como respaldos en caso de que el servidor primario falle.**Nota:** Si todos los servidores configurados TACACS+ no pueden responder, usted debe iniciar sesión con la cuenta local de los CiscoWorks admin, después cambia el modo AAA de nuevo al NON-ACS/a los CiscoWorks locales. Después de que los servidores TACACS+ se restablezcan para mantener, usted debe cambiar el modo AAA de nuevo al ACS.
5. En el área del login, ingrese el nombre del administrador que usted definió en Administration Control (Control de administración) la página del Cisco Secure ACS. Vea para crear Administration Control (Control de administración) a un usuario en el Cisco Secure ACS para más información.
6. Ingrese y verifique la contraseña para este administrador.
7. Ingrese y verifique la clave secreta compartida que usted ingresó cuando usted agregó el

servidor del administrador de seguridad como cliente AAA del Cisco Secure ACS. Vea el paso 5 adentro agregar los dispositivos como clientes AAA sin NDGs.

8. Marque el **registro todas las aplicaciones instaladas con la** casilla de verificación **ACS** para registrar el Cisco Security Manager y cualquier otra aplicación instalada con el Cisco Secure ACS.
9. Haga clic en **Apply** para guardar sus configuraciones. Una barra de progreso visualiza el progreso del registro. Un mensaje aparece cuando el registro es completo.
10. Si usted integra al Cisco Security Manager con cualquier ACS versión, recomience el servicio del administrador de Daemon del Cisco Security Manager. Vea el reinicio el administrador de Daemon para las instrucciones.**Nota:** Después de CS 3.0.0, Cisco prueba no más con ACS 3.3(x) porque se parchea pesadamente y su fin de vida (EOL) se ha anunciado. Por lo tanto, usted necesita utilizar el ACS versión apropiado para el CSM versión 3.0.1 y posterior. Vea la tabla de la Matriz de compatibilidad para más información.
11. Registro nuevamente dentro del Cisco Secure ACS para asignar los papeles a cada grupo de usuarios. Vea para asignar los papeles a los grupos de usuarios en el Cisco Secure ACS para las instrucciones.**Nota:** La configuración AAA configurada aquí no se conserva si usted desinstala el CiscoWorks Common Services o al Cisco Security Manager. Además, esta configuración no se puede sostener y restablecer después de la reinstalación. Por lo tanto, si usted actualiza a una nueva versión de cualquier aplicación, usted debe configurar de nuevo al modo de configuración AAA y reregistrar al Cisco Security Manager con el ACS. Este proceso no se requiere para las actualizaciones graduales. Si usted instala las aplicaciones adicionales, tales como AU, encima de los CiscoWorks, usted debe reregistrar las nuevas aplicaciones y al Cisco Security Manager.

Recomience al administrador de Daemon

Este procedimiento describe cómo recomenzar al administrador de Daemon del servidor del Cisco Security Manager. Usted debe hacer esto para que las configuraciones AAA que usted configuró para tomar el efecto. Usted puede entonces registrar nuevamente dentro de los CiscoWorks con las credenciales definidas en el Cisco Secure ACS.

1. Registro en la máquina en la cual el servidor del Cisco Security Manager está instalado.
2. Elija el **Start (Inicio) > Programs (Programas) > Administrative Tools (Herramientas administrativas) > Services (Servicios)** para abrir la ventana de los servicios.
3. De la lista de servicios visualizados en el panel derecho, seleccione al **administrador de Daemon del Cisco Security Manager**.
4. Haga clic el botón del **servicio del reinicio** en la barra de herramientas.
5. Continúe con asignan los papeles a los grupos de usuarios en el Cisco Secure ACS.

Asigne los papeles a los grupos de usuarios en el Cisco Secure ACS

Después de que usted registre los CiscoWorks, el Cisco Security Manager y otras aplicaciones instaladas al Cisco Secure ACS, usted puede asignar los papeles a cada uno de los grupos de usuarios que usted configuró previamente en el Cisco Secure ACS. Estos papeles determinan las acciones que permiten los usuarios en cada grupo para realizarse en el Cisco Security Manager.

El procedimiento que usted utiliza para asignar los papeles a los grupos de usuarios depende

encendido si NDGs está utilizado:

- Asigne los papeles a los grupos de usuarios sin NDGs
- Asocie NDGs y los papeles a los grupos de usuarios

Asigne los papeles a los grupos de usuarios sin NDGs

Este procedimiento describe cómo asignar los papeles predeterminados a los grupos de usuarios cuando NDGs no se define. Refiera al Cisco Secure ACS omiten los papeles de más información.

Nota: Antes de que usted proceda:

- Cree a un grupo de usuarios para cada papel predeterminado. Vea para definir los usuarios y a los grupos de usuarios en el Cisco Secure ACS para las instrucciones.
- Complete los procedimientos descritos en los procedimientos de la integración realizados en el Cisco Secure ACS y los procedimientos de la integración realizados en los CiscoWorks.

Complete estos pasos:

1. Inicie sesión al Cisco Secure ACS.
2. Haga clic la **configuración de grupo** en la barra de navegación.
3. Seleccione al grupo de usuarios para los administradores de sistema de la lista. Vea el paso 2 de los usuarios y de los grupos de usuarios Define en el Cisco Secure ACS, después haga clic **editan las configuraciones**.

Asocie NDGs y los papeles a los grupos de usuarios

Cuando usted asocia NDGs a los papeles del uso en el Cisco Security Manager, usted debe crear las definiciones en dos lugares en la página de la configuración de grupo:

- Área de los CiscoWorks
- Área del Cisco Security Manager

Las definiciones en la cada área deben hacer juego lo más posible. Cuando usted asocia los rol personalizado o los papeles ACS que no existen en el CiscoWorks Common Services, intente definir como se cierran un equivalente como sea posible basado en los permisos asignados a ese papel.

Usted debe crear las asociaciones para que cada grupo de usuarios sea utilizado con el Cisco Security Manager. Por ejemplo, si usted tiene un grupo de usuarios que contenga el personal de servicio técnico para la región occidental, usted puede seleccionar a ese grupo de usuarios, después asocia el NDG que contiene los dispositivos en esa región con el papel del escritorio de ayuda.

Nota: Antes de que usted proceda, active la característica NDG y cree NDGs. Vea a los grupos de dispositivos de red de la configuración para el uso en el administrador de seguridad para más información.

1. Haga clic la **configuración de grupo** en la barra de navegación.
2. Seleccione a un grupo de usuarios de la lista del grupo, después haga clic **editan las configuraciones**.
3. Asocie NDGs y los papeles del uso en los CiscoWorks:En la página de la configuración de

grupo, navegue hacia abajo a los CiscoWorks el área bajo configuraciones TACACS+.Selecto **asigne los CiscoWorks en a por la base del grupo de dispositivos de red**.Seleccione un NDG de la lista del grupo de dispositivos.Seleccione el papel al cual este NDG debe ser asociado de la segunda lista.El tecleo **agrega la asociación**. La asociación aparece en el cuadro de grupo de dispositivos.Relance los pasos c a e para crear las asociaciones adicionales.**Nota:** Para quitar una asociación, seleccionarla del grupo de dispositivos, entonces para hacer clic quita la asociación.

4. Navegue hacia abajo al área del Cisco Security Manager y cree las asociaciones que corresponden con tan de cerca como sea posible las asociaciones definidas en el paso 3.**Nota:** Cuando usted selecciona los papeles de la Seguridad Approver o del administrador de seguridad en el Cisco Secure ACS, se recomienda que usted selecciona al administrador de la red como el papel equivalente más cercano de los CiscoWorks.
5. El tecleo **somete** para salvar sus configuraciones.
6. Relance los pasos 2 a 5 para definir NDGs para el resto de los grupos de usuarios.
7. Después de que usted asocie NDGs y los papeles a cada grupo de usuarios, haga clic **Submit + Restart**.

Troubleshooting

1. Antes de que usted pueda comenzar a importar los dispositivos en el Cisco Security Manager, usted debe primero configurar cada dispositivo como cliente AAA en su Cisco Secure ACS. Además, usted debe configurar el servidor de los CiscoWorks/del administrador de seguridad como cliente AAA.
2. Si usted recibe un registro de los intentos fallidos, el autor falló con el error en el Cisco Secure ACS.
   ```
   "service=Athena cmd=OGS authorize-deviceGroup*(Not Assigned) authorize-deviceGroup*Test Devices authorize-deviceGroup*HQ Routers authorize-deviceGroup*HQ Switches authorize-deviceGroup*HQ Security Devices authorize-deviceGroup*Agent Routers authoriz"
   ```
   Para resolver este problema, aseegurese que el nombre del dispositivo en el ACS necesita ser un Nombre de dominio totalmente calificado (FQDN).

Información Relacionada

- Access Control Server del Cisco Security para la página de soporte de Windows
- Página de soporte del Cisco Security Manager
- Cisco Secure Access Control Server para Windows
- Guía de configuración para el Cisco Secure ACS 4.1
- Guía de Troubleshooting en línea del Cisco Secure ACS, 4.1
- Avisos de campos de productos de seguridad (incluido CiscoSecure ACS para Windows)
- Soporte Técnico y Documentación - Cisco Systems