CSM 3.x - Agregar sensores y módulos IDS al inventario

Contenido

Introducción

Este documento proporciona información sobre cómo agregar sensores y módulos del sistema de detección de intrusiones (IDS) (incluye IDSM en switches Catalyst 6500, NM-CIDS en routers y AIP-SSM en ASA) en Cisco Security Manager (CSM).

Nota: CSM 3.2 no admite IPS 6.2. Se admite en CSM 3.3.

Prerequisites

Requirements

Este documento asume que los dispositivos CSM e IDS están instalados y funcionan correctamente.

Componentes Utilizados

La información en este documento se basa en el CSM 3.0.1.

The information in this document was created from the devices in a specific lab environment. 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 TécnicosCisco para obtener más información sobre las convenciones del documento.

Agregar dispositivos al inventario de Security Manager

Al agregar un dispositivo al administrador de seguridad, se introduce una serie de información de identificación para el dispositivo, como su nombre DNS y su dirección IP. Después de agregar el dispositivo, aparece en el inventario de dispositivos del Administrador de seguridad. Sólo puede administrar un dispositivo en el Administrador de seguridad después de agregarlo al inventario.

Puede agregar dispositivos al inventario de Security Manager con estos métodos:

- Agregue un dispositivo de la red.
- Agregar un nuevo dispositivo que aún no está en la red
- Agregue uno o más dispositivos desde el repositorio de dispositivos y credenciales (DCR).
- Agregue uno o más dispositivos desde un archivo de configuración.

Nota: Este documento se centra en el método: Agregue un nuevo dispositivo que aún no esté en la red.

Pasos para agregar el sensor IDS y los módulos

Utilice la opción Add New Device para agregar un único dispositivo al inventario de Security Manager. Puede utilizar esta opción para el preaprovisionamiento. Puede crear el dispositivo en el sistema, asignar políticas al dispositivo y generar archivos de configuración antes de recibir el hardware del dispositivo.

Cuando reciba el hardware del dispositivo, debe preparar los dispositivos que administrará el administrador de seguridad. Refiérase a Preparación de los Dispositivos para que el Administrador de Seguridad Administre para obtener más información.

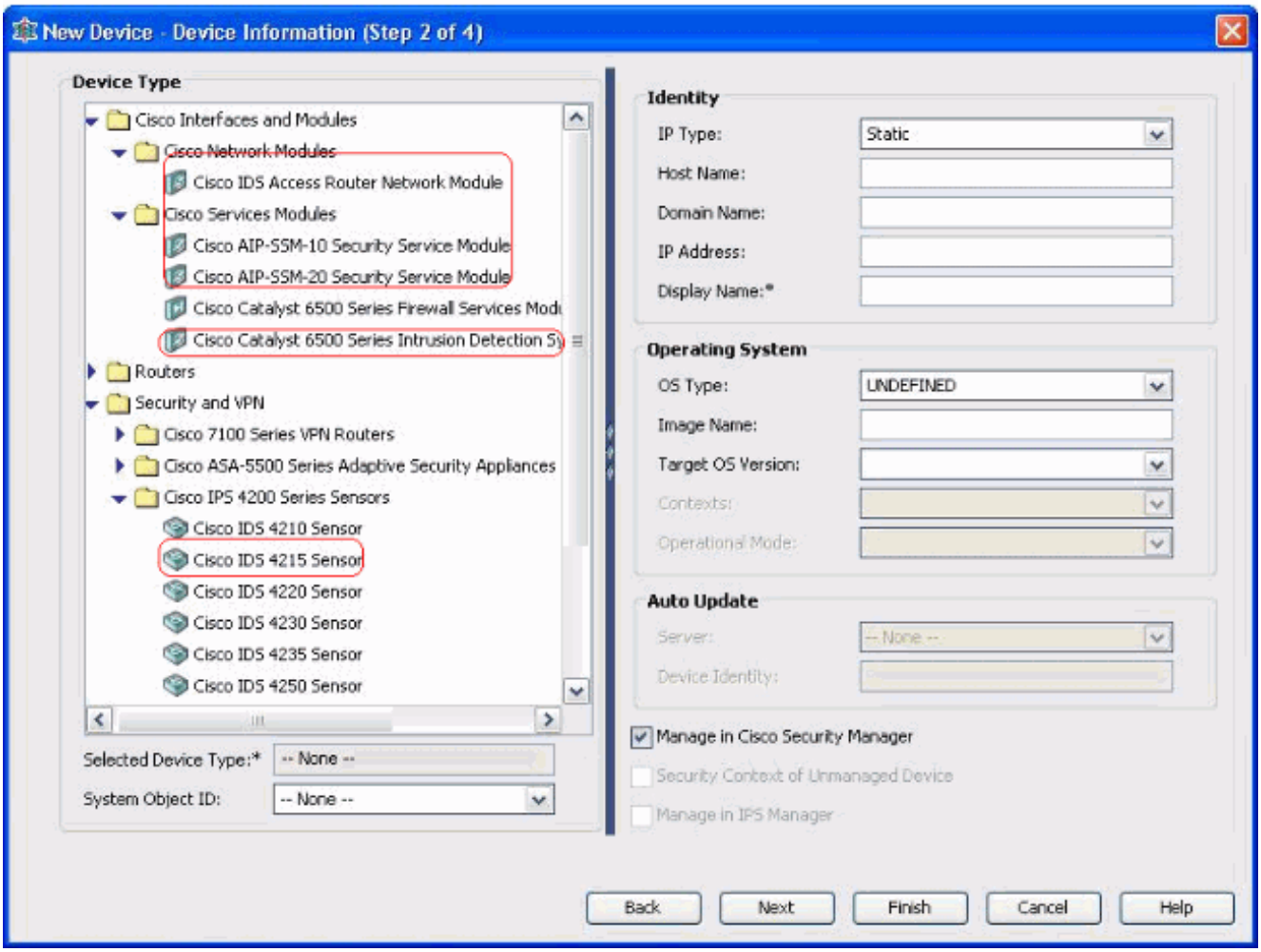
Este procedimiento muestra cómo agregar un nuevo sensor IDS y módulos:

1. Haga clic en el botón **Vista de dispositivo** de la barra de herramientas.Aparecerá la página Dispositivos.
2. Haga clic en el botón **Add** en el selector de dispositivos.Aparece la página Nuevo dispositivo - Elegir método con cuatro opciones.
3. Elija **Add New Device** y luego haga clic en **Next**.Aparecerá la página New Device - Device Information (Nuevo dispositivo - Información del dispositivo).
4. Introduzca la información del dispositivo en los campos correspondientes.Consulte la sección Proporcionar información del dispositivo—Nuevo dispositivo para obtener más información.
5. Haga clic en Finish (Finalizar).El sistema realiza las tareas de validación del dispositivo:Si los datos son incorrectos, el sistema genera mensajes de error y muestra la página en la que se produce el error con un icono de error rojo correspondiente.Si los datos son correctos, el dispositivo se agrega al inventario y aparece en el selector de dispositivos.

Proporcionar información del dispositivo: nuevo dispositivo

Complete estos pasos:

1. Seleccione el tipo de dispositivo para el nuevo dispositivo:Seleccione la carpeta de tipo de dispositivo de nivel superior para mostrar las familias de dispositivos compatibles.Seleccione la carpeta de la familia de dispositivos para mostrar los tipos de dispositivos admitidos.Seleccione **Cisco Interfaces and Modules > Cisco Network Modules** para agregar el **módulo de red del router de acceso IDS de Cisco**. Asimismo, seleccione **Cisco Interfaces and Modules > Cisco Services Modules** para agregar los módulos AIP-SSM e IDSM mostrados.Seleccione **Security and VPN > Cisco IPS 4200 Series Sensors** para agregar el sensor Cisco IDS 4210 al inventario
CSM.



Seleccione el tipo de dispositivo.**Nota:** Después de agregar un dispositivo, no puede cambiar el tipo de dispositivo.Los ID de objeto del sistema para ese tipo de dispositivo se muestran en el campo SysObjectId. El primer ID de objeto del sistema está seleccionado de forma predeterminada. Puede seleccionar otro si es necesario.

2. Introduzca la información de identidad del dispositivo, como el tipo de IP (estática o dinámica), el nombre de host, el nombre de dominio, la dirección IP y el nombre de visualización.
3. Introduzca la información del sistema operativo del dispositivo, como el tipo de sistema operativo, el nombre de la imagen, la versión del sistema operativo de destino, los contextos y el modo operativo.
4. Aparece el campo Auto Update o CNS-Configuration Engine, que depende del tipo de dispositivo que seleccione:Actualización automática: se muestra para los dispositivos PIX Firewall y ASA.CNS-Configuration Engine: se muestra para los routers Cisco IOS®.**Nota:** Este campo no está activo para los dispositivos Catalyst 6500/7600 y FWSM.
5. Complete estos pasos:Actualización automática: haga clic en la flecha para mostrar una lista

de servidores. Seleccione el servidor que está administrando el dispositivo. Si el servidor no aparece en la lista, complete estos pasos:Haga clic en la flecha y, a continuación, seleccione **+ Agregar servidor**... Aparecerá el cuadro de diálogo Propiedades del servidor.Introduzca la información en los campos obligatorios.Click OK. El nuevo servidor se agrega a la lista de servidores disponibles.CNS-Configuration Engine: se muestra información diferente, que depende de si selecciona un tipo IP estático o dinámico:**Estático**: haga clic en la flecha para mostrar una lista de motores de configuración. Seleccione el motor de configuración que está administrando el dispositivo. Si el motor de configuración no aparece en la lista, complete estos pasos:Haga clic en la flecha y, a continuación, seleccione **+ Agregar motor de configuración**... Aparecerá el cuadro de diálogo Propiedades del motor de configuración.Introduzca la información en los campos obligatorios.Click OK. El nuevo motor de configuración se agrega a la lista de motores de configuración disponibles.**Dinámico**: haga clic en la flecha para mostrar una lista de servidores. Seleccione el servidor que está administrando el dispositivo. Si el servidor no aparece en la lista, complete estos pasos:Haga clic en la flecha y, a continuación, seleccione **+ Agregar servidor**... Aparecerá el cuadro de diálogo Propiedades del servidor.Introduzca la información en el campo correspondiente.Click OK. El nuevo servidor se agrega a la lista de servidores disponibles.

6. Complete estos pasos:Para administrar el dispositivo en el Administrador de seguridad, marque la casilla de verificación **Administrar en Cisco Security Manager**. Este es el valor predeterminado.Si la única función del dispositivo que está agregando es servir como punto final de VPN, desmarque la casilla de verificación **Administrar en Cisco Security Manager**.Security Manager no administrará configuraciones ni cargará ni descargará configuraciones en este dispositivo.
7. Marque la casilla de verificación Contexto de seguridad de dispositivo no administrado para administrar un contexto de seguridad, cuyo dispositivo primario (Firewall PIX, ASA o FWSM) no está administrado por el Administrador de seguridad.Puede dividir un firewall PIX, ASA o FWSM en varios firewalls de seguridad, también conocidos como contextos de seguridad. Cada contexto es un sistema independiente, con su propia configuración y políticas. Puede administrar estos contextos independientes en el Administrador de seguridad, aunque el administrador de seguridad no administre el principal (Firewall PIX, ASA o FWSM).**Nota:** Este campo está activo sólo si el dispositivo que seleccionó en el selector de dispositivos es un dispositivo de firewall, como PIX Firewall, ASA o FWSM, que soporta el contexto de seguridad.
8. Marque la casilla de verificación **Administrar en IPS Manager** para administrar un router Cisco IOS en IPS Manager.Este campo está activo sólo si seleccionó un router Cisco IOS en el selector de dispositivos.**Nota:** IPS Manager puede administrar las funciones IPS solamente en un router Cisco IOS que tenga capacidades IPS. Para obtener más información, consulte la documentación de IPS.Si marca la casilla de verificación Administrar en IPS Manager, también debe marcar la casilla de verificación Administrar en Cisco Security Manager.Si el dispositivo seleccionado es IDS, este campo no está activo. Sin embargo, la casilla de verificación está marcada porque IPS Manager administra los sensores IDS.Si el dispositivo seleccionado es Firewall PIX, ASA o FWSM, este campo no está activo porque el administrador IPS no administra estos tipos de dispositivo.
9. Haga clic en Finish (Finalizar).El sistema realiza las tareas de validación del dispositivo:Si los datos introducidos son incorrectos, el sistema genera mensajes de error y muestra la página en la que se produce el error.Si los datos introducidos son correctos, el dispositivo se agrega al inventario y aparece en el selector de dispositivos.

Troubleshoot

Use esta sección para resolver problemas de configuración.

Mensajes de error

Cuando agrega IPS a CSM, el `dispositivo no válido: No se pudo deducir el` mensaje de error `SysObjId para el tipo de plataforma`.

Solución

Complete estos pasos para resolver este mensaje de error.

1. Detenga el servicio CSM Daemon en Windows y luego elija **Archivos de Programa > CSCOpx > MDC > Athena > config > Directory**, donde puede encontrar `VMS-SysObjID.xml`.
2. En el sistema CSM, reemplace el archivo VMS-SysObjID.xml original ubicado de forma predeterminada en `C:\Program Files\CSCOpx\MDC\athena\config\directory` por el último archivo `VMS-SysObjID.xml`.
3. Reinicie el servicio CSM Daemon Manager (CRMDmgtd) y vuelva a intentar agregar o descubrir los dispositivos afectados de nuevo.

Información Relacionada

- Página de soporte de Cisco Security Manager
- Página de soporte del sistema de detección de intrusiones de Cisco
- Soporte Técnico y Documentación - Cisco Systems