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. Es compatible con CSM 3.3.

Prerequisites

Requirements

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

Componentes Utilizados

La información de este documento se basa en CSM 3.0.1.

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). 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 incluye una serie de datos de identificación del dispositivo, como el nombre DNS y la dirección IP. Después de agregar el dispositivo, aparece en el inventario de dispositivos de Security Manager. 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 desde la red.
- Agregar un nuevo dispositivo que aún no está en la red
- Agregue uno o más dispositivos desde el repositorio de credenciales y dispositivos (DCR).
- Agregue uno o más dispositivos desde un archivo de configuración.

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

Pasos para agregar el sensor IDS y los módulos

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

Cuando reciba el hardware del dispositivo, debe preparar los dispositivos para que el Administrador de seguridad los administre. Consulte Preparación de los Dispositivos para que el Administrador de Seguridad los Gestione para obtener más información.

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

1. Haga clic en el botón Device View de la barra de herramientas.

   Aparecerá la página Dispositivos.

2. Haga clic en el botón Add en el selector Device.

   Aparecerá la página Nuevo dispositivo - Elegir método con cuatro opciones.

3. Elija Add New Device, luego haga clic en Next.

   Aparecerá la página 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 tareas de validación de dispositivos:

   - 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 que se corresponde con él.
   - Si los datos son correctos, el dispositivo se agrega al inventario y aparece en el selector Dispositivo.

Proporcionar información sobre el dispositivo—Nuevo dispositivo

Complete estos pasos:

1. Seleccione el tipo de dispositivo para el nuevo dispositivo:

   a. Seleccione la carpeta de tipo de dispositivo de nivel superior para mostrar las familias de dispositivos soportados.

   b. Seleccione la carpeta de la familia de dispositivos para mostrar los tipos de dispositivos admitidos.

      a. Seleccione Cisco Interfaces and Modules > Cisco Network Modules para agregar el Cisco IDS Access Router Network Module. Del mismo modo, seleccione Cisco Interfaces and Modules > Cisco Services Modules para agregar los módulos AIP-SSM e IDSM que se muestran.

      b. Seleccione Security and VPN > Cisco IPS 4200 Series Sensors para agregar el Cisco IDS 4210 Sensor al inventario CSM.

   c. Seleccione el tipo de dispositivo.

      Nota: Después de agregar un dispositivo, no puede cambiar el tipo de dispositivo.

      Los ID de objetos 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. Si es necesario, puede seleccionar otro.

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 para mostrar.

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 Firewall PIX 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 administra el dispositivo. Si el servidor no aparece en la lista, siga estos pasos:

     a. Haga clic en la flecha y, a continuación, seleccione + Agregar servidor... Aparecerá el cuadro de diálogo Propiedades del servidor.

     b. Introduzca la información en los campos obligatorios.

     c. 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 el tipo de IP estática o dinámica:

     Estático: haga clic en la flecha para mostrar una lista de motores de configuración. Seleccione el motor de configuración que administra el dispositivo. Si el motor de configuración no aparece en la lista, siga estos pasos:

     a. Haga clic en la flecha y, a continuación, seleccione + Add Configuration Engine... Aparecerá el cuadro de diálogo Propiedades del motor de configuración.

     b. Introduzca la información en los campos obligatorios.

     c. 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 administra el dispositivo. Si el servidor no aparece en la lista, siga estos pasos:

     a. Haga clic en la flecha y, a continuación, seleccione + Agregar servidor... Aparecerá el cuadro de diálogo Propiedades del servidor.

     b. Introduzca la información en el campo obligatorio.

     c. 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 el Administrador de seguridad de Cisco. Este es el valor

predeterminado.

- Si la única función del dispositivo que está agregando es servir como punto final de VPN, desactive la casilla de verificación Administrar en Cisco Security Manager.

  Security Manager no administrará las 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 principal (Firewall PIX, ASA o FWSM) no esté 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 principal (Firewall PIX, ASA o FWSM) no esté administrado por el Administrador de seguridad.

   Nota: Este campo solo está activo si el dispositivo seleccionado en el selector de dispositivo es un dispositivo de firewall, como PIX Firewall, ASA o FWSM, que admite 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 ha seleccionado un router Cisco IOS en el selector de dispositivos.

   Nota: IPS Manager sólo puede gestionar las funciones de IPS en un router de Cisco IOS que tenga funciones de 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 activada porque IPS Manager gestiona los sensores IDS.

   Si el dispositivo seleccionado es PIX Firewall, ASA o FWSM, este campo no está activo porque IPS Manager no gestiona estos tipos de dispositivos.

9. Haga clic en Finish (Finalizar).

   El sistema realiza tareas de validación de dispositivos:

   - 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 dispositivo.

Troubleshoot

Use esta sección para resolver problemas de configuración.

Mensajes de error

Cuando agrega IPS a CSM, aparece el mensaje de error `Invalid device: Failed deduce el 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 Program Files > 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 archivo `VMS-SysObjID.xml` más reciente.
3. Reinicie el servicio Administrador de demonios CSM (CRMDmgtd) y vuelva a intentar agregar o detectar los dispositivos afectados.

Información Relacionada

- Página de soporte de Cisco Security Manager
- Página de soporte de Cisco Intrusion Detection System
- Soporte Técnico y Documentación - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).