Implementación del conector de atributos dinámicos seguros en FMC

Contenido

- Introducción
- Antecedentes - Problema
- Solución (resumen)
- Conector de atributos dinámicos en resumen de FMC
- Ejemplos de implementación
  - CSDAC in situ
  - El problema
    - Opción 1: Utilice el conector de atributos dinámicos incorporado en FMC
    - Opción 2: Utilice el conector de atributos dinámicos proporcionado por la nube en CDO
- Prerrequisitos, Plataformas Soportadas, Licencias
  - Plataformas de hardware y software admitidas mínimas
  - Componentes Utilizados
- Detalles de la función
  - Descripción general de CSDAC independiente (actualmente disponible: 7.4)
  - Descripción general de CSDAC en CDO (actualmente disponible: 7.4)
  - CSDAC en FMC
  - Cómo funciona
  - Configurar conectores
  - CSDAC en FMC
  - Objetos dinámicos
- Política de AC
  - Configuración: política de acceso
  - Límites de plataforma
- Resolución de problemas/Diagnóstico
  - Compruebe los conectores
  - Ver conectores desde la ficha Conectores
  - Comprobar los filtros de atributos
  - Comprobar los objetos dinámicos en la interfaz de usuario de FMC
  - Alertas de estado de CSDAC
- CSDAC en Troubleshooting
  - Generación de un Troubleshooting CSDAC
  - Troubleshooting de CLI
  - Modo de depuración CSDAC
  - Mensajes registrados con depuración
- Ejemplo de problema con la resolución de problemas
  - Descripción general de problemas y resolución de problemas
    - Problema:

Resolución de problemas:
Preparar paquete de solución de problemas
Observe los atributos de etiqueta de una dirección IP
Resumen de cheques
Preguntas y respuestas

Introducción

Este documento describe acerca de Cisco Secure Dynamic Attribute Connector en FMC.

Antecedentes - Problema

CSDAC (Cisco Secure Dynamic Attributes Connector) se puede integrar en FMC (Firepower Management Center), proporcionando el mismo nivel de funcionalidad que la aplicación CSDAC independiente y CSDAC en CDO. En el caso de CSDAC independiente, libera a los clientes de la sobrecarga que supone administrar y mantener una máquina independiente para CSDAC. Como administrador de red, deseo que las interfaces de programación sean fáciles de integrar y estén al día de los cambios en los proveedores de entornos dinámicos externos. Esta integración resuelve el problema de recopilar atributos de entornos de nube que cambian dinámicamente sin implementar una política.

Solución (resumen)

CSDAC se puede configurar ahora en FMC para obtener atributos de etiquetas de Azure, vCenter, AWS, GCP, Office 365 y Azure Service Tags, lo que proporciona paridad de funciones con CSDAC y CSDAC independientes en CDO.

- Ahora puede optar por utilizar
  - CSDAC en FMC (o)
  - CSDAC en CDO (o)
  - CSDAC independiente
- Mercado objetivo: empresa, proveedor de servicios

Conector de atributos dinámicos en resumen de FMC

Conector de atributos dinámicos de FMC:

- Pantalla del panel para crear y utilizar las funciones del conector de atributos dinámicos.
- Interfaz de usuario de FMC para configurar conectores de carga de trabajo de origen (AWS, Azure, vCenter, Office 365, GCP)
- Interfaz de usuario de FMC para definir filtros de atributos dinámicos para crear objetos dinámicos

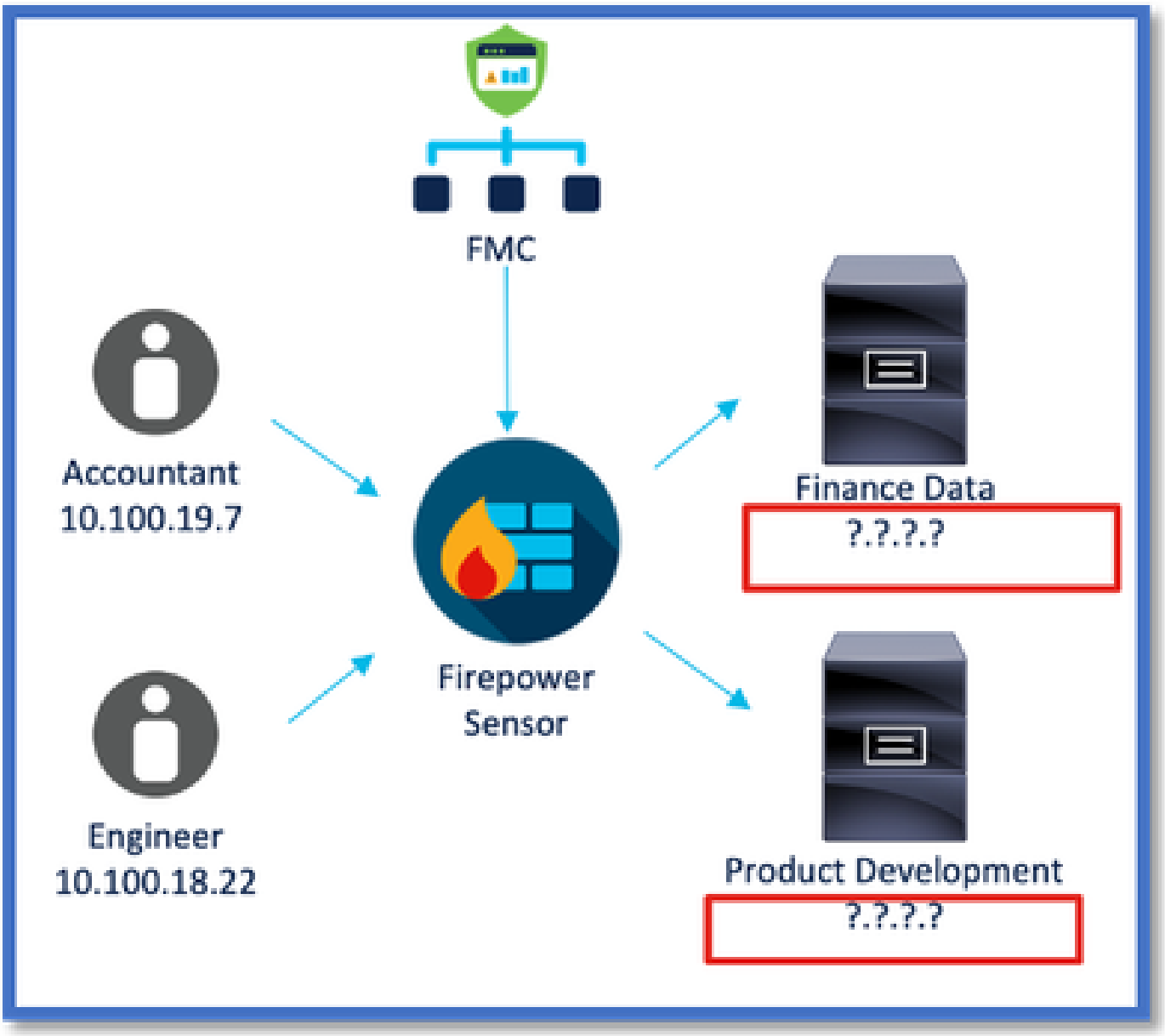
Ejemplos de implementación

CSDAC in situ

El año pasado, implementé una máquina virtual dedicada para CSDAC para recopilar atributos de mis cuentas de AWS y Azure.

El problema

Ahora, mi organización se ha pasado a la nube y no puedo implementar ni administrar una máquina virtual dedicada para CSDAC en mi entorno.



Opción 1: Utilice el conector de atributos dinámicos incorporado en FMC

Puede solucionar el problema mediante el conector de atributos dinámicos integrado en FMC. Los objetos dinámicos creados por él se pueden utilizar en la directiva de acceso.

Opción 2: Utilice el conector de atributos dinámicos proporcionado por la nube en CDO

Puede solucionar el problema utilizando Dynamic Attributes Connector en CDO. Los objetos dinámicos creados por ella se pueden utilizar en

- CDO Cloud-delivered FMC
- FMC en las instalaciones de CDO

Prerrequisitos, Plataformas Soportadas, Licencias

Plataformas de hardware y software admitidas mínimas

Versión mínima del administrador admitido	Dispositivos gestionados	Versión mínima de dispositivos administrados admitidos requerida	Notas
CSP 7.4	Cualquier FTD compatible	Cualquier FTD 7.0+	

* El conector de atributos dinámicos no es compatible con dispositivos administrados por FDM

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.
· Cisco Firewall Management Center con 7.4
· Cisco Firepower Threat Defence con versión 7.4 o superior.
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 tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Detalles de la función

Descripción general de CSDAC independiente (actualmente disponible: 7.4)

Cisco Secure Dynamic Attributes Connector permite utilizar etiquetas de varias plataformas de servicios en la nube en las reglas de control de acceso de Firewall Management Center (FMC).

CSDAC in situ se puede instalar en un equipo Linux y admite la obtención de atributos de:

- AWS,Azure,VMware vCenter y NSX-T,Office 365,Azure Service Tags,GCP,GitHub.

Descripción general de CSDAC en CDO (actualmente disponible: 7.4)

Admite la misma funcionalidad que CSDAC in situ sin necesidad de instalar y mantener una aplicación dedicada.

El conector vCenter no se admite actualmente en CDO.

Admite el envío de los atributos recibidos a FMC en la nube y a FMC in situ en CDO.

CSDAC en FMC

Admite la misma funcionalidad que CSDAC independiente sin necesidad de instalar y mantener una aplicación dedicada.

CSDAC en FMC admite la obtención de atributos de:

- AWS,Azure,VMware vCenter y NSX-T,Office 365,Azure Service Tags,GCP,GitHub

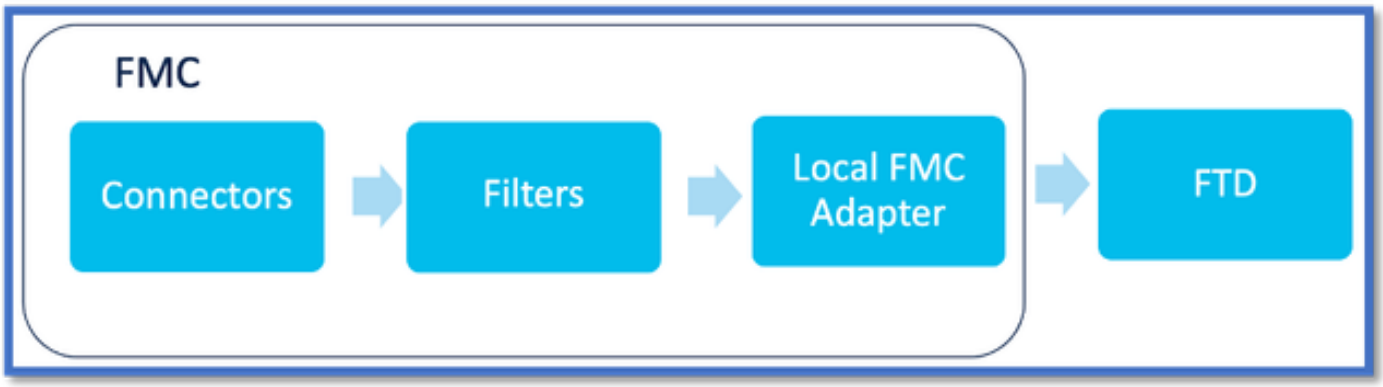
No hay ninguna configuración de adaptador explícita aquí, ya que es local para FMC.

Cómo funciona

Los conectores se utilizan para obtener atributos de AWS, Azure, o365, vCenter.

A continuación, se utiliza el adaptador local para guardar estos atributos simplificados y sus asignaciones IP en FMC como objetos dinámicos.

FMC envía la asignación en tiempo real al FTD (sin implementar).



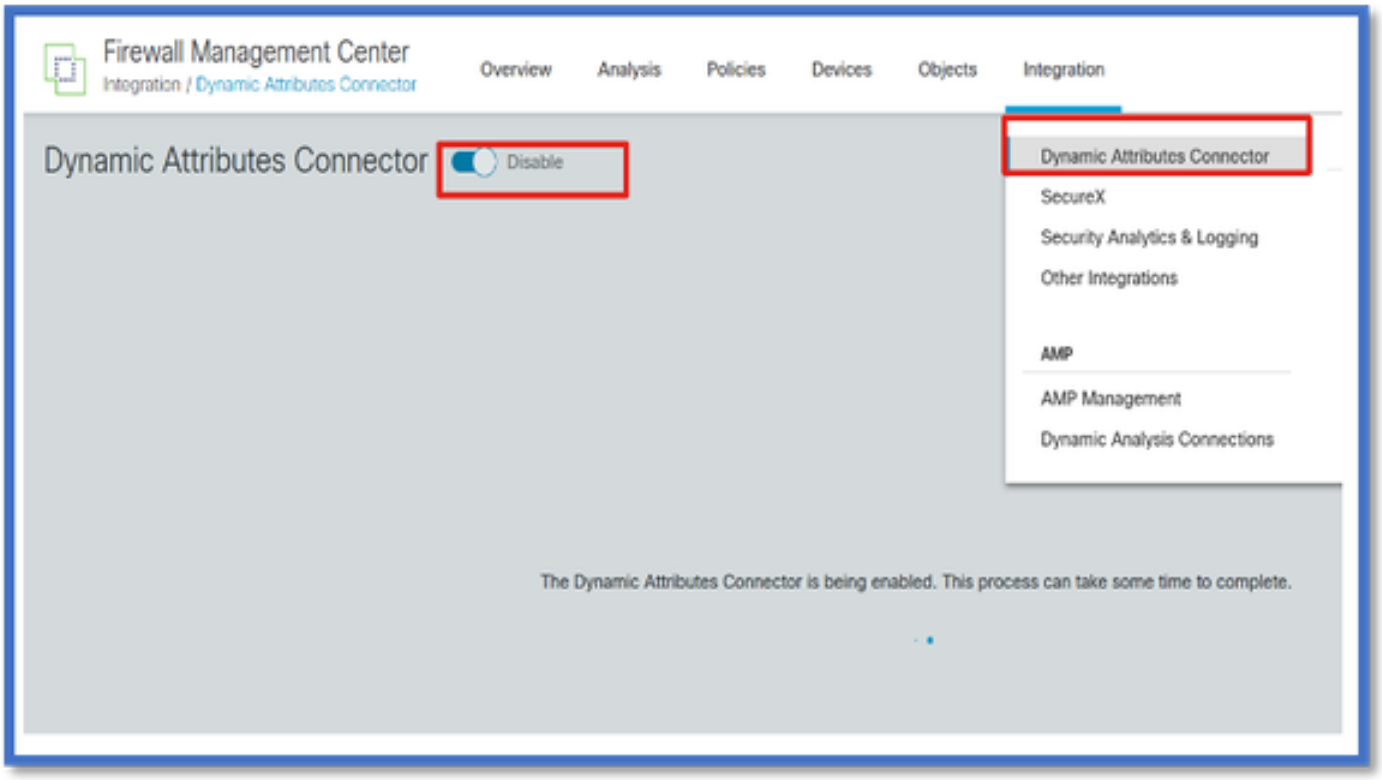
Activar CSDAC en FMC

Vaya a Integración > Conector de atributos dinámicos.

Utilice el botón de alternancia para activar el conector.

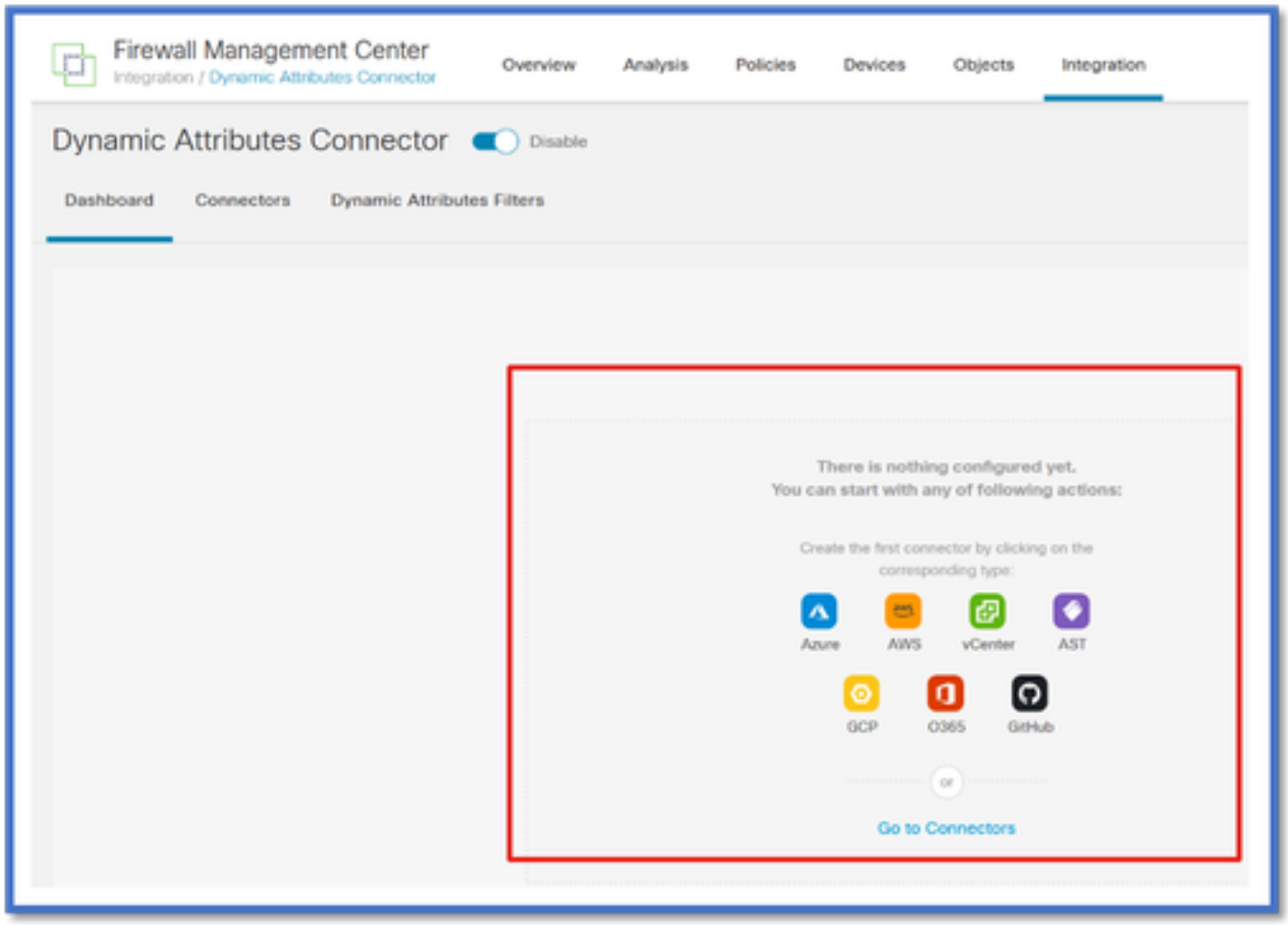
FMC tarda unos minutos en descargar y mostrar las imágenes y los contenedores del acoplador.

Esto solo se puede configurar en el dominio global FMC.



Panel CSDAC

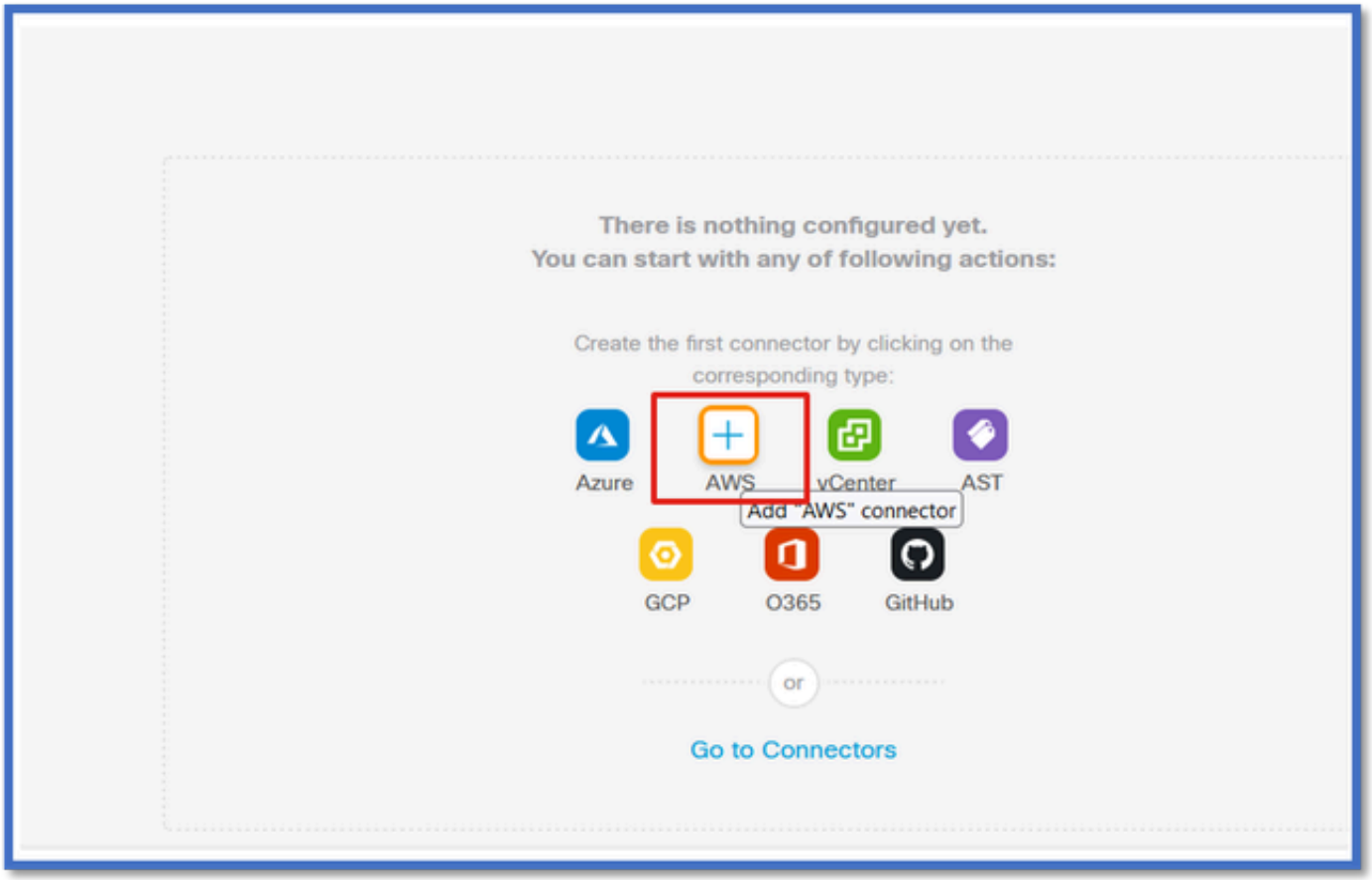
Después de activar CSDAC, se muestra al usuario la página Panel de CSDAC. El panel se utiliza para configurar y ver conectores y filtros consolidados.



Configurar conectores

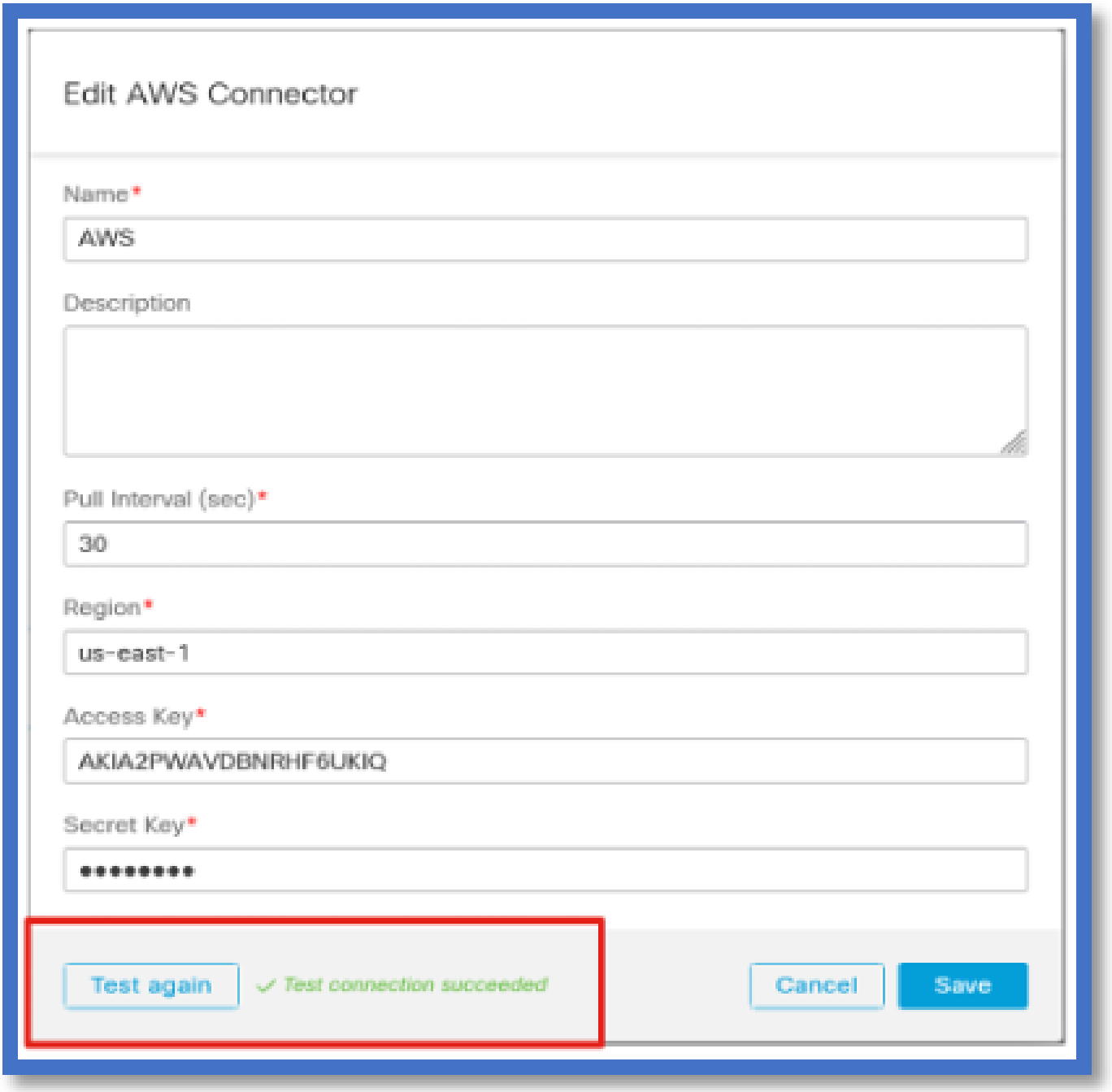
Agregar conectores desde el panel

En el panel, haga clic en el icono del conector que desee para agregarlo.



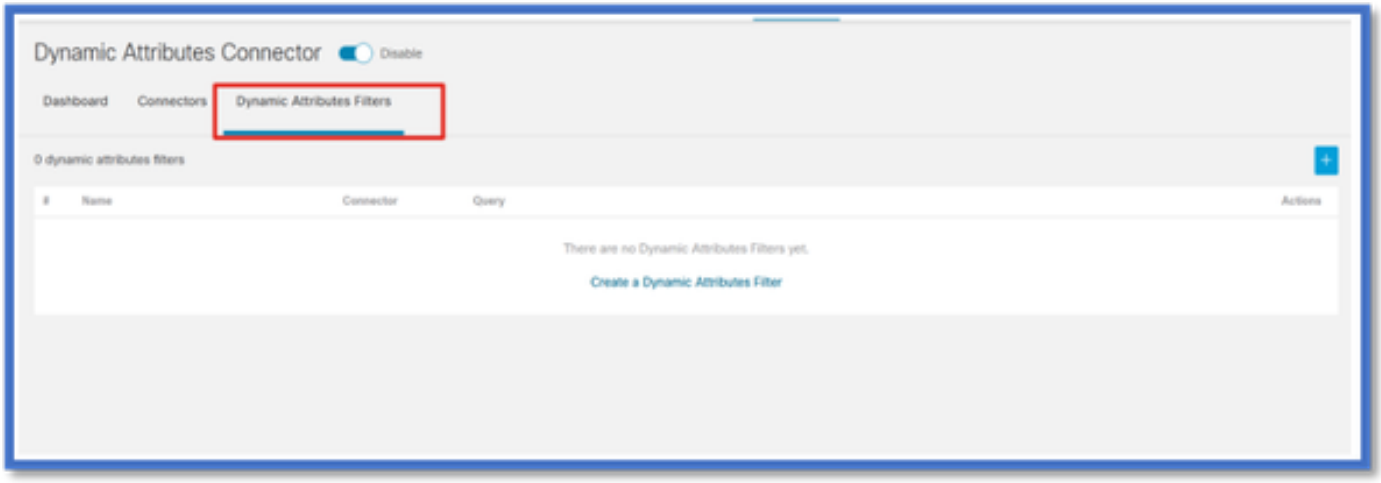
Configure un intervalo de tiempo (en el campo Intervalo de extracción) para que los conectores puedan obtener información de los proveedores con la periodicidad configurada.

Introduzca las credenciales del proveedor para obtener los atributos de etiqueta. Una vez configurado el conector, puede probarlo haciendo clic en el botón Test (Probar).



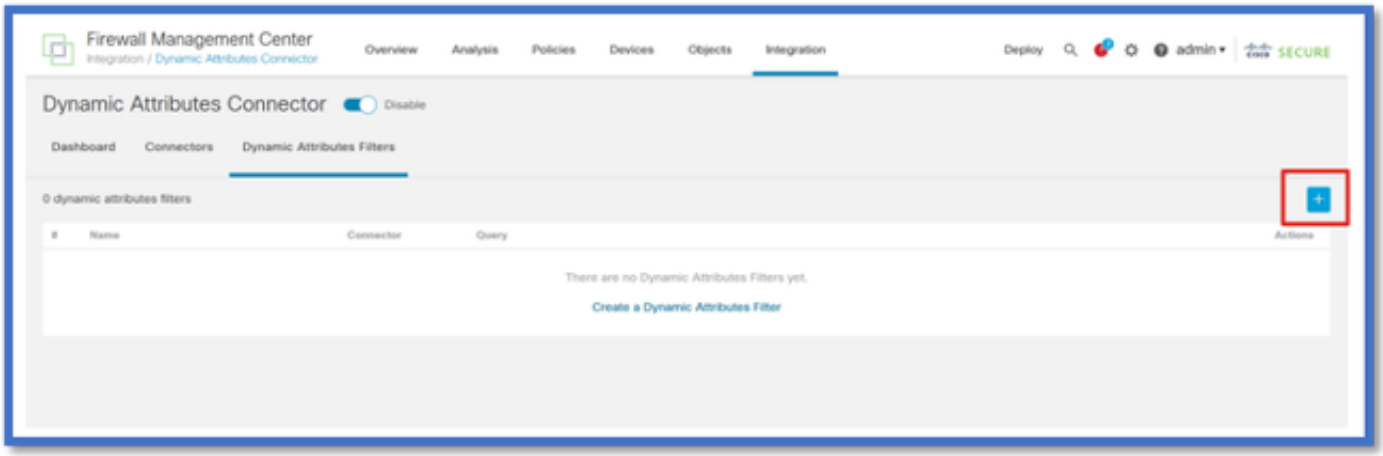
Configurar filtros

Haga clic en la ficha "Dynamic Attribute Filters" (Filtros de atributos dinámicos) del menú "Dynamic Attributes Connector" (Conector de atributos dinámicos) para ir a la página Dynamic Attributes Filters (Filtros de atributos dinámicos).



Adición de filtros

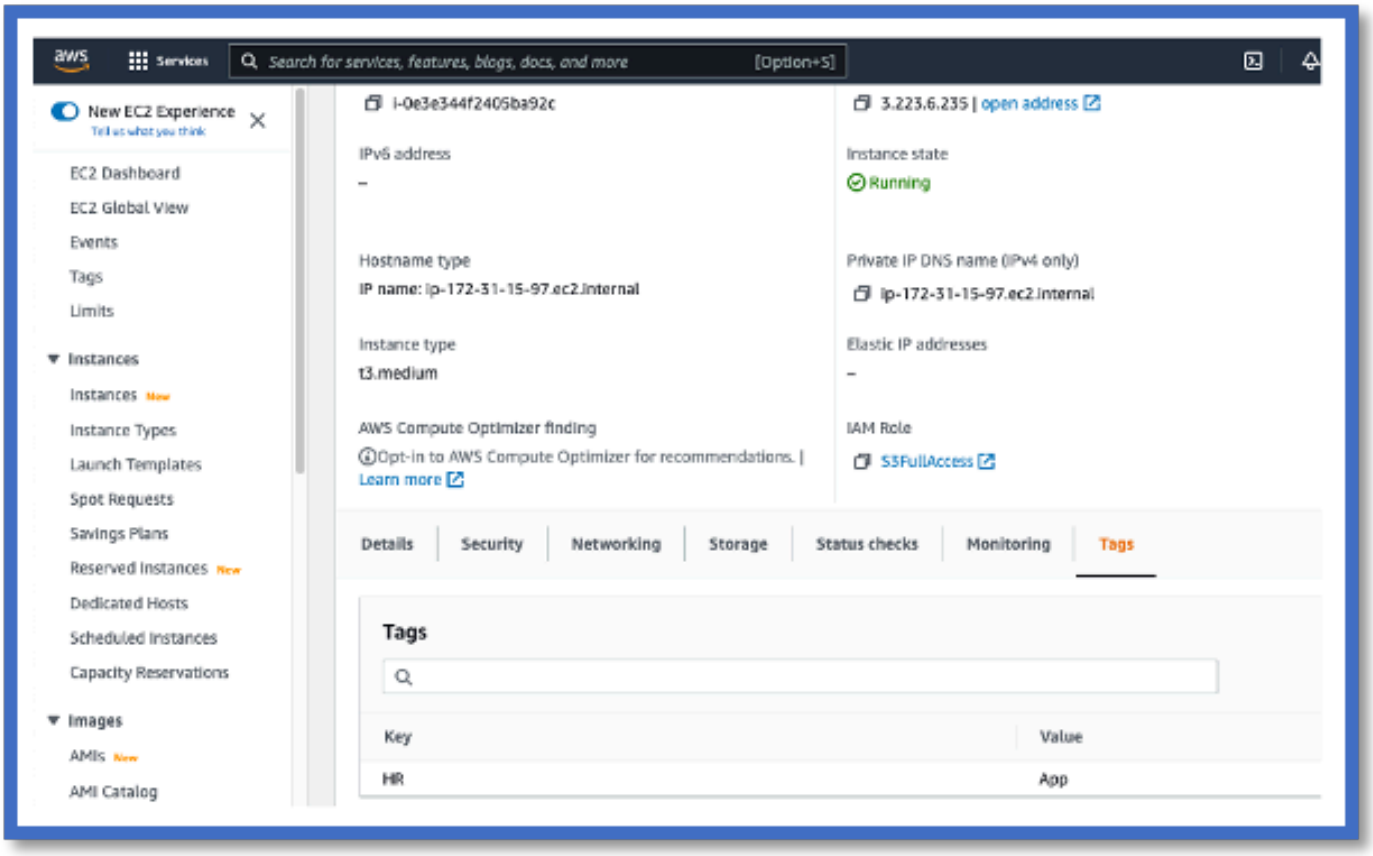
Haga clic en el botón + para crear un filtro para conectores de atributos.



Agregar etiquetas AWS

Por ejemplo, podemos suponer que está interesado en la clave "RR. HH." y el valor "Aplicación" en las cargas de trabajo de AWS.

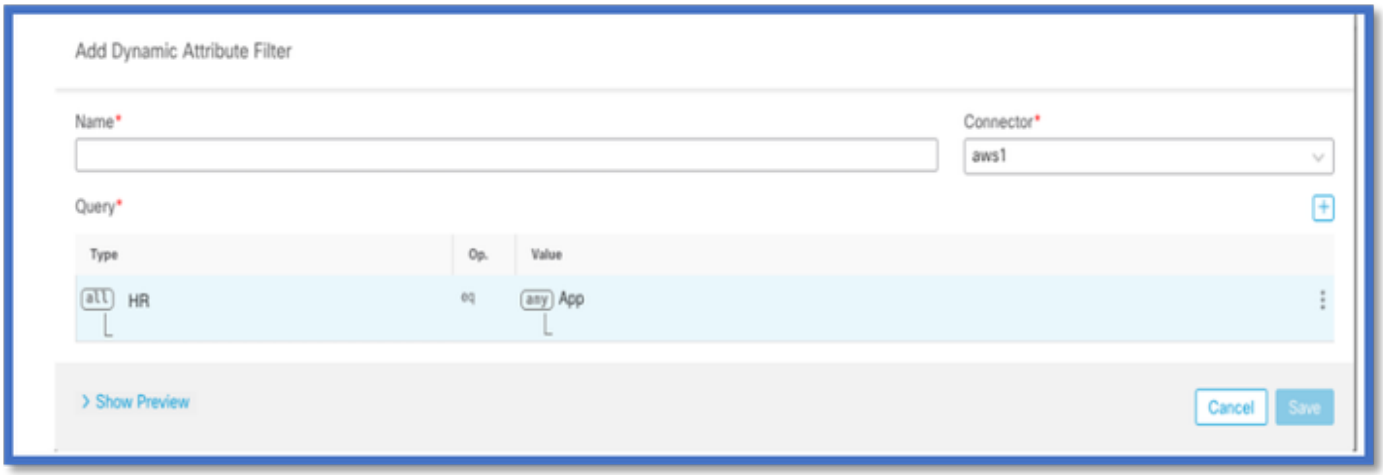
Así es como se vería en AWS.



CSDAC en FMC

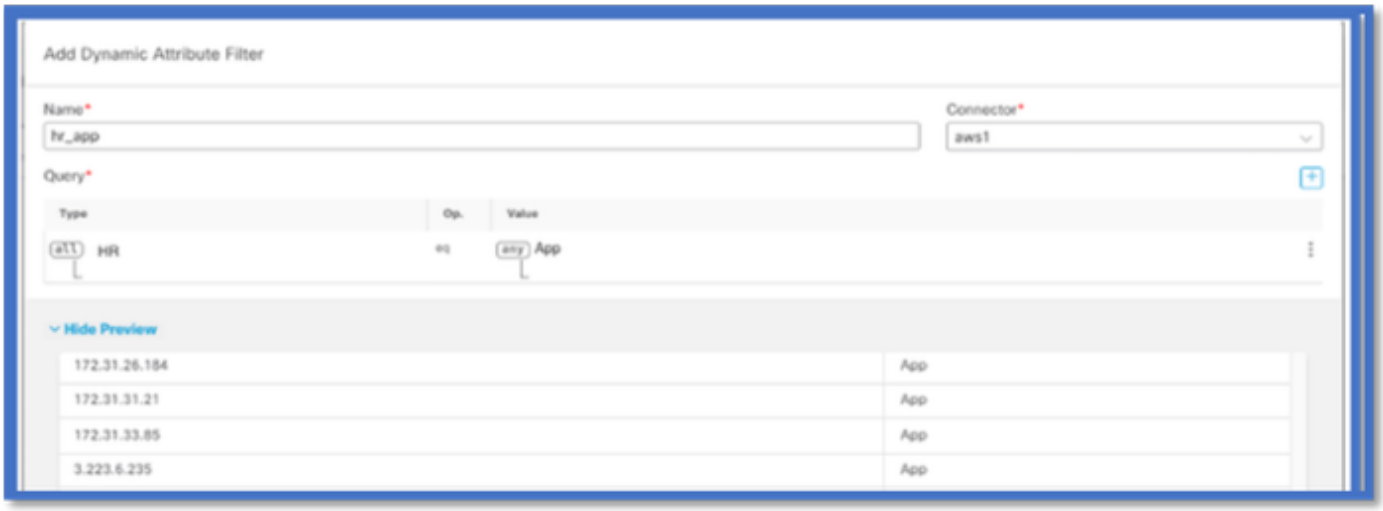
Puede crear una regla de "RR. HH. igual a aplicación" haciendo clic en el botón +.

El adaptador FMC local enviaría las direcciones IP coincidentes como asignaciones de objetos dinámicos a FMC



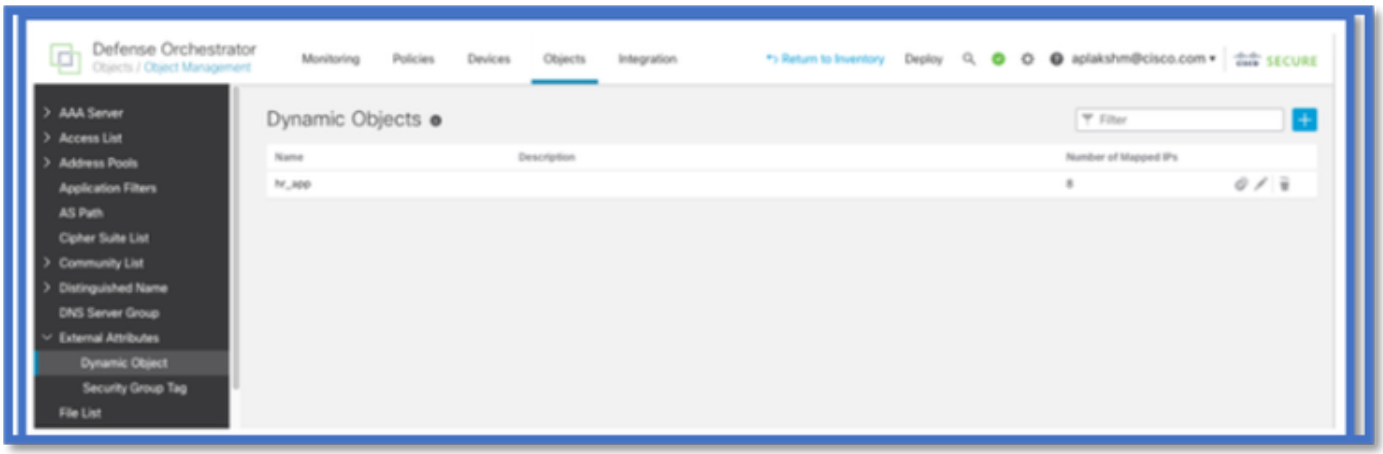
Vista previa

También puede ver las direcciones IP coincidentes de una regla de atributo determinada haciendo clic en el botón | Ocultar el botón "Vista previa".



Objetos dinámicos

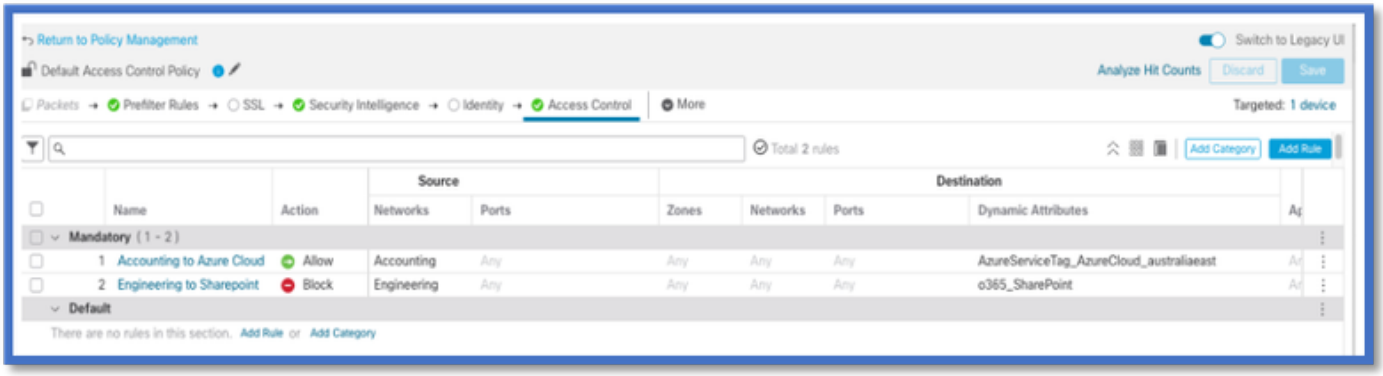
Ver los objetos dinámicos creados por CSDAC en Objetos > Atributos externos, Objeto dinámico en FMC



Política de AC

Configuración: política de acceso

En FMC, agregue una política de acceso para permitir o bloquear los objetos dinámicos recibidos desde el Conector de atributos dinámicos.



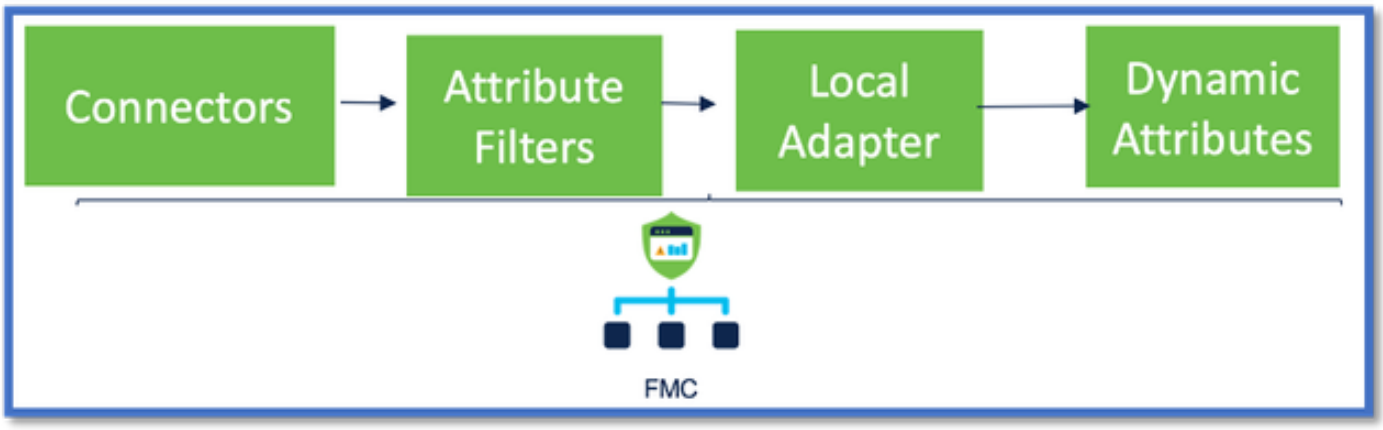
Límites de plataforma

- Los límites de los conectores se basan en la memoria FMC disponible.
- vFMC necesitaría una memoria de 1 GB adicional para admitir 5 conectores
- El rango de Azure AD también se incluye en el límite, ya que también es un contenedor CSDAC.

Modelos	Número de conectores admitidos	Plataformas	Límite basado en la memoria
Básico	Solo Azure AD	1600	32 GB
Pequeño	5	vFMC	> 32 GB
Medio	10	vFMC 300 y 2600	>= 64 GB
Grande	20	4600	>= 128 GB

Resolución de problemas/Diagnóstico

La resolución de problemas se realiza mejor trazando los objetos dinámicos desde conectores CSDAC a atributos de Dynamics en FMC.Muchos registros internos se refieren a esta función como "recopilación". Puede observar el estado del sistema a lo largo de la cadena de difusión para aislar los problemas. CSDAC utiliza contenedores Docker. Los mensajes y los nombres de los registros y otros archivos deben denominarse "docker"



Compruebe los conectores

En primer lugar, asegúrese de que Connectors se pueden conectar a servidores vCenter, AWS o

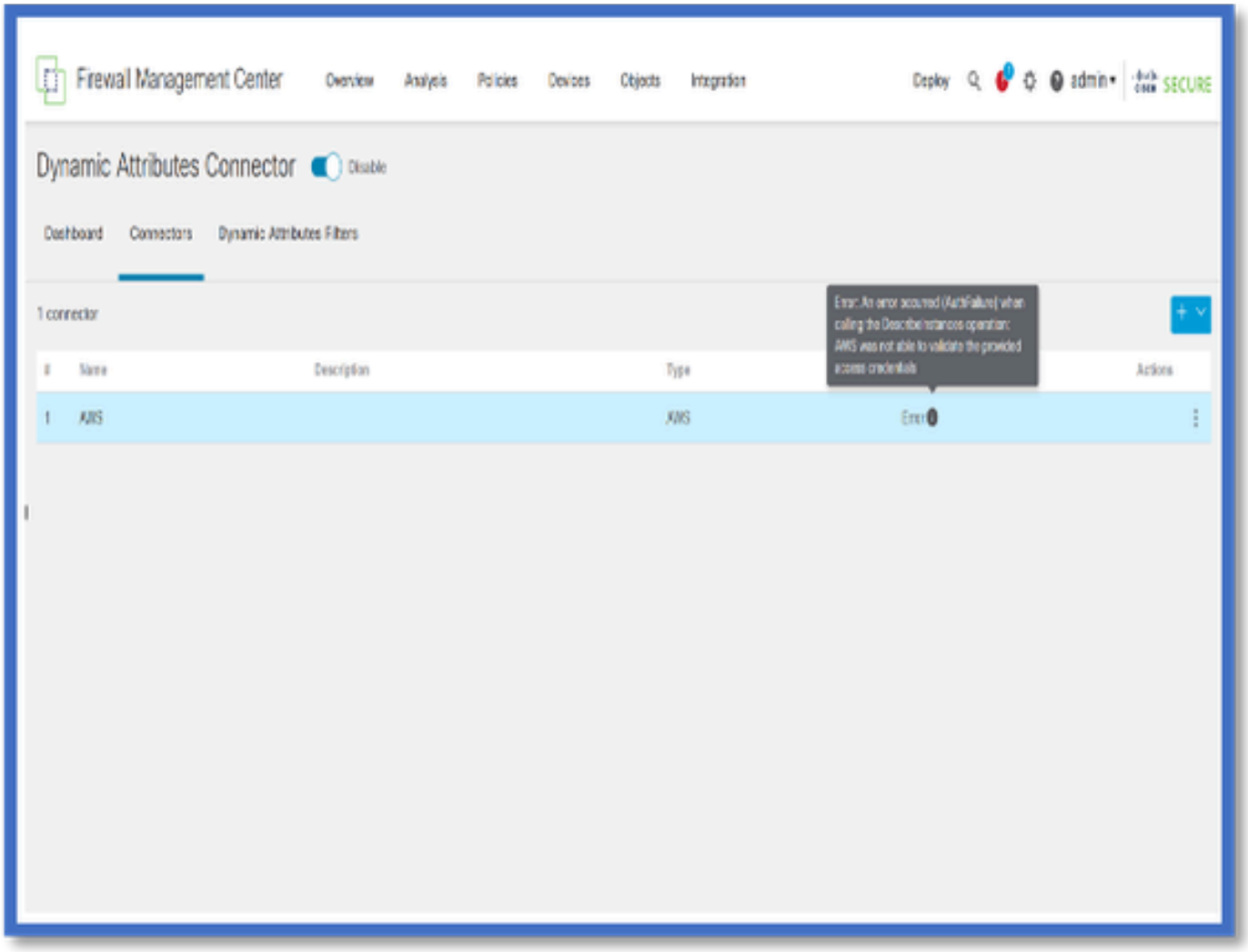
Azure.

Si los conectores no están configurados correctamente, los procesos descendentes no pueden obtener información de etiquetas.

Ver conectores desde la ficha Conectores

El estado del conector se muestra en el campo de estado y se actualiza cada 15 segundos.

Aquí, vemos que el conector no pudo autenticarse con las credenciales proporcionadas.



Comprobar los filtros de atributos

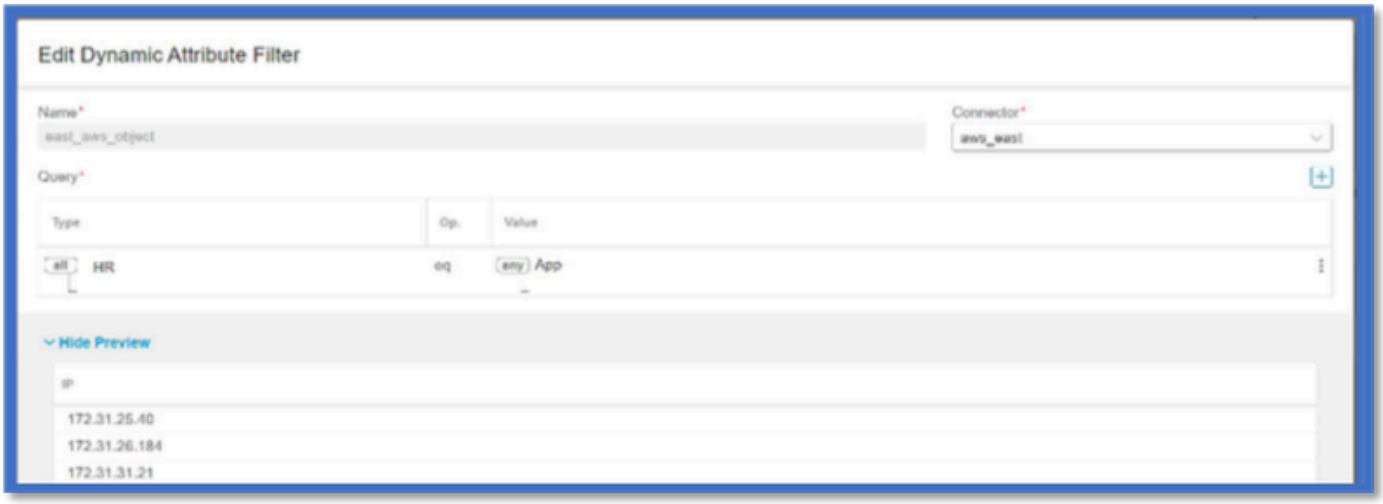
Asegúrese de que la vista previa de la regla muestre las direcciones IP coincidentes para la condición de consulta.

Si no hay direcciones IP coincidentes, FMC no puede obtener las asignaciones de objetos dinámicos.

Comprobación de los filtros de atributos

Compruebe que las asignaciones de IP de atributos dinámicos están disponibles en la vista

previa. El botón Mostrar vista previa está disponible en la ventana emergente Editar filtro de atributos dinámicos.



Comprobar los objetos dinámicos en la interfaz de usuario de FMC

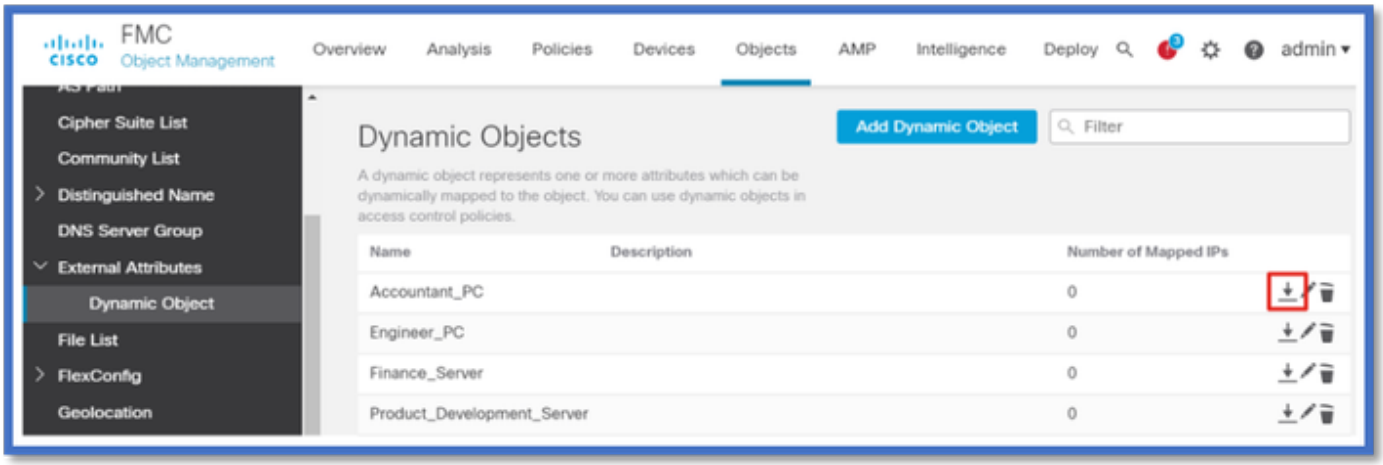
En primer lugar, asegúrese de que el servidor FMC contiene los enlaces que espera.

- Busque en Administración de objetos, pestaña Objetos externos, y verifique Objetos dinámicos para encontrar enlaces.
- Si el FMC no consigue las fijaciones, el FTD no podrá obtenerlas.

Verifique FMC Health Monitor y Notifications para las alertas de estado CSDAC.

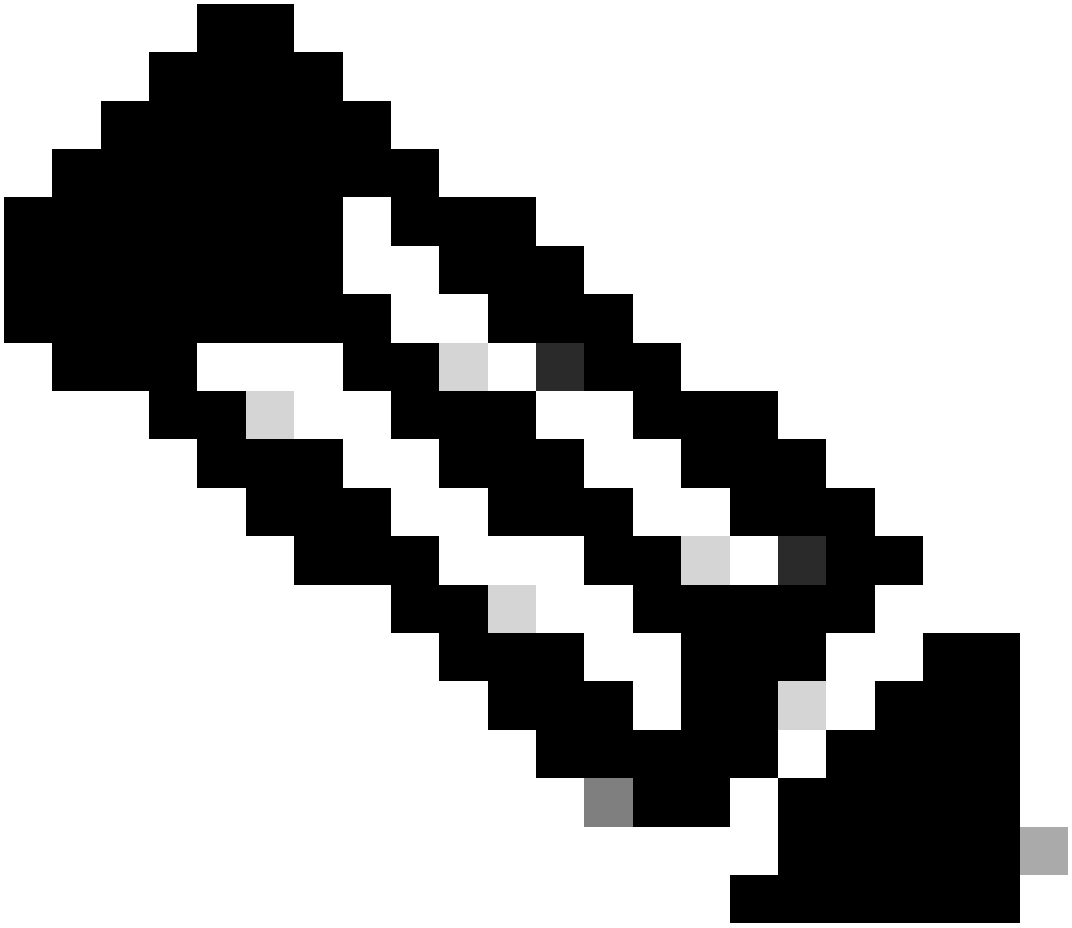
Comprobación de objetos dinámicos

FMC Object Manager le permite descargar las direcciones IP de objetos dinámicos actuales.

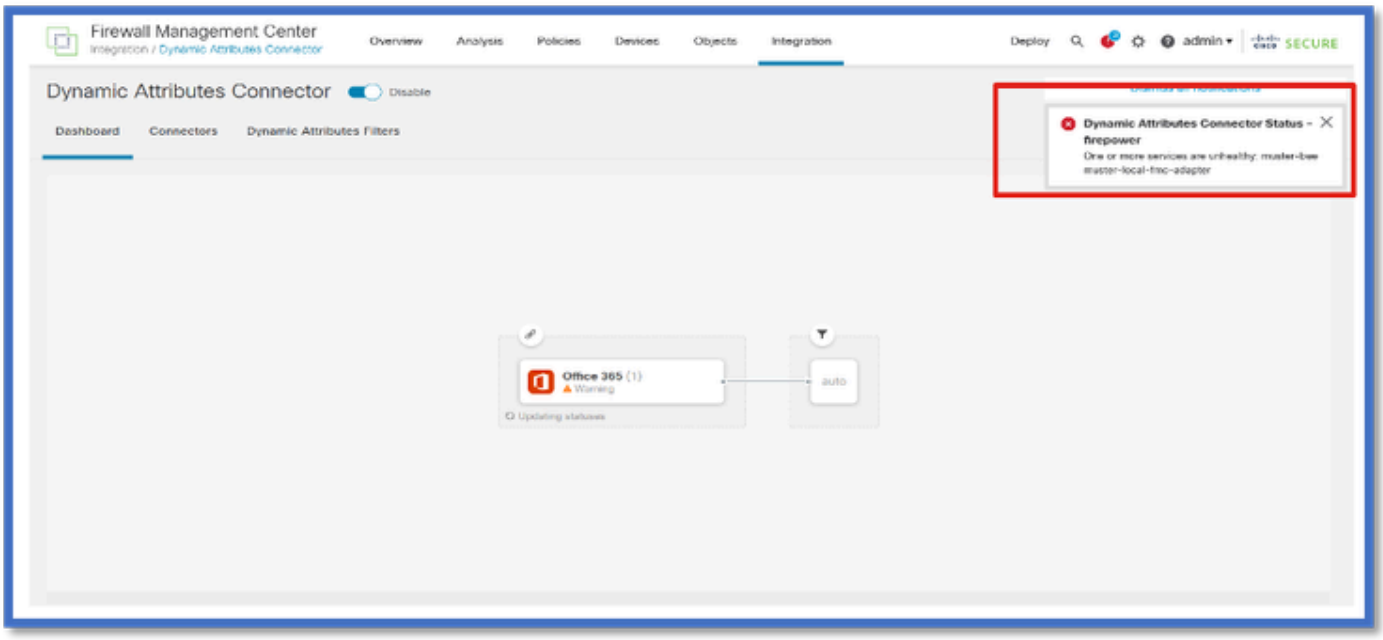


Alertas de estado de CSDAC

El administrador de tareas de FMC muestra alertas de estado si algún servicio principal, incluido el conector de atributos dinámicos, está inactivo. La alerta contiene información relativa al nombre y el estado del servicio.

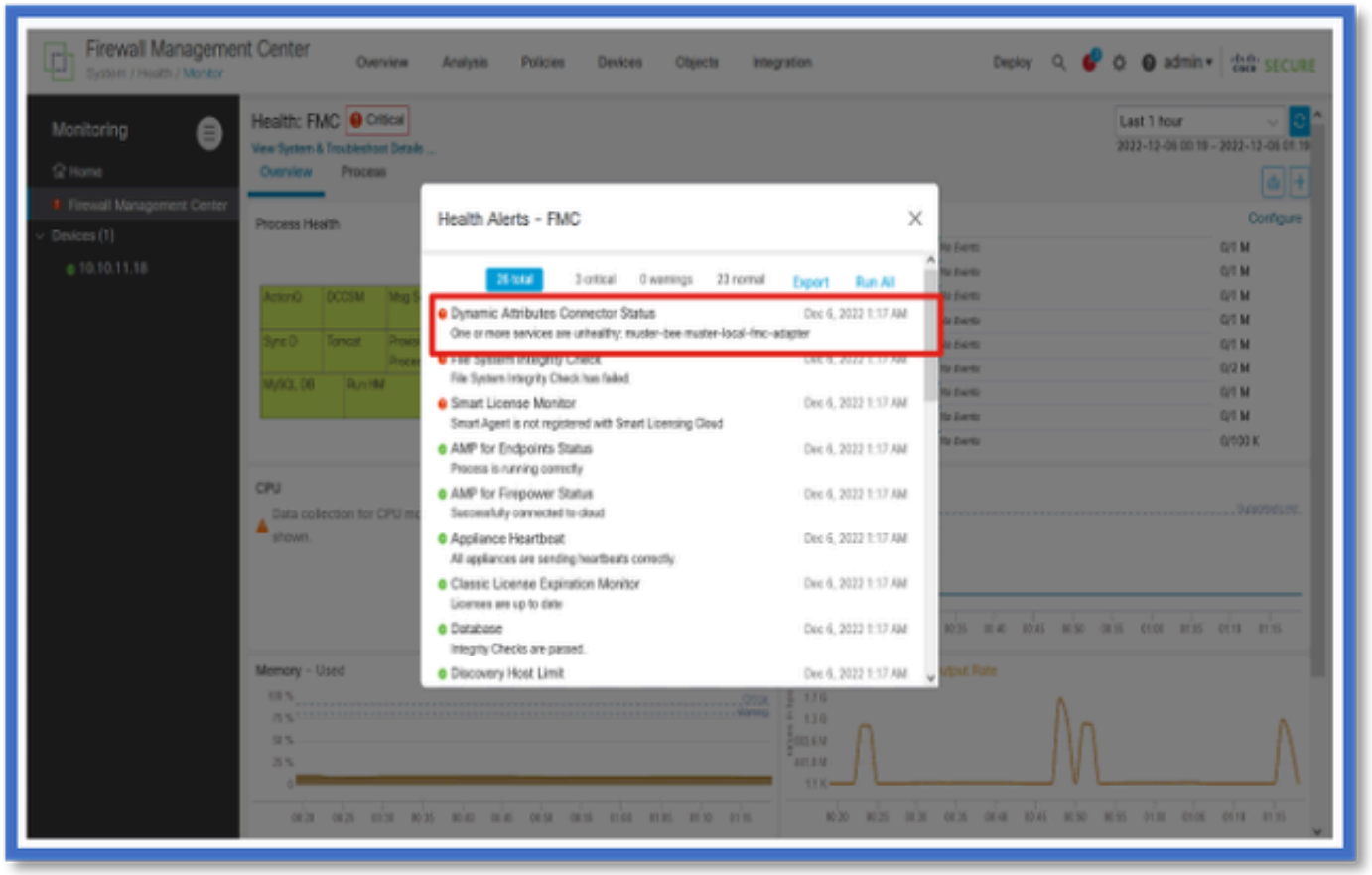


Nota: seguimos teniendo el nombre de "reunión" en varias notificaciones y es necesario proporcionar aquí el nombre del servicio para obtener información detallada.



Aquí vemos que muster-bee y muster-local-fmc-adapter son "insalubres".

Si el error indica cualquiera de los servicios centrales, entonces los registros de troubleshooting deben ser recolectados para el debug.



CSDAC en Troubleshooting

Generación de un Troubleshooting CSDAC

- Los registros de CSDAC se recopilan automáticamente durante la generación de la solución de problemas de FMC. El paquete contiene el estado del Docker, los registros y los datos necesarios para depurar el problema sin conexión.
- Una buena práctica es habilitar el modo de depuración CSDAC antes de reproducir el error para el cual se recopilan los registros de solución de problemas .

Desde /usr/local/sf/csdac call ./muster-cli debug-on

Busque los registros CSDAC en untarred Solución de problemas en estas carpetas:

/results-XX/command-outputs/csdac_troubleshoot/info

Contiene los datos almacenados en la base de datos etcd.

/results-XX/command-output/csdac_troubleshoot /log

Contiene los registros de los contenedores de acoplamiento.

/results-XX/command-outputs/csdac_troubleshoot/status.log

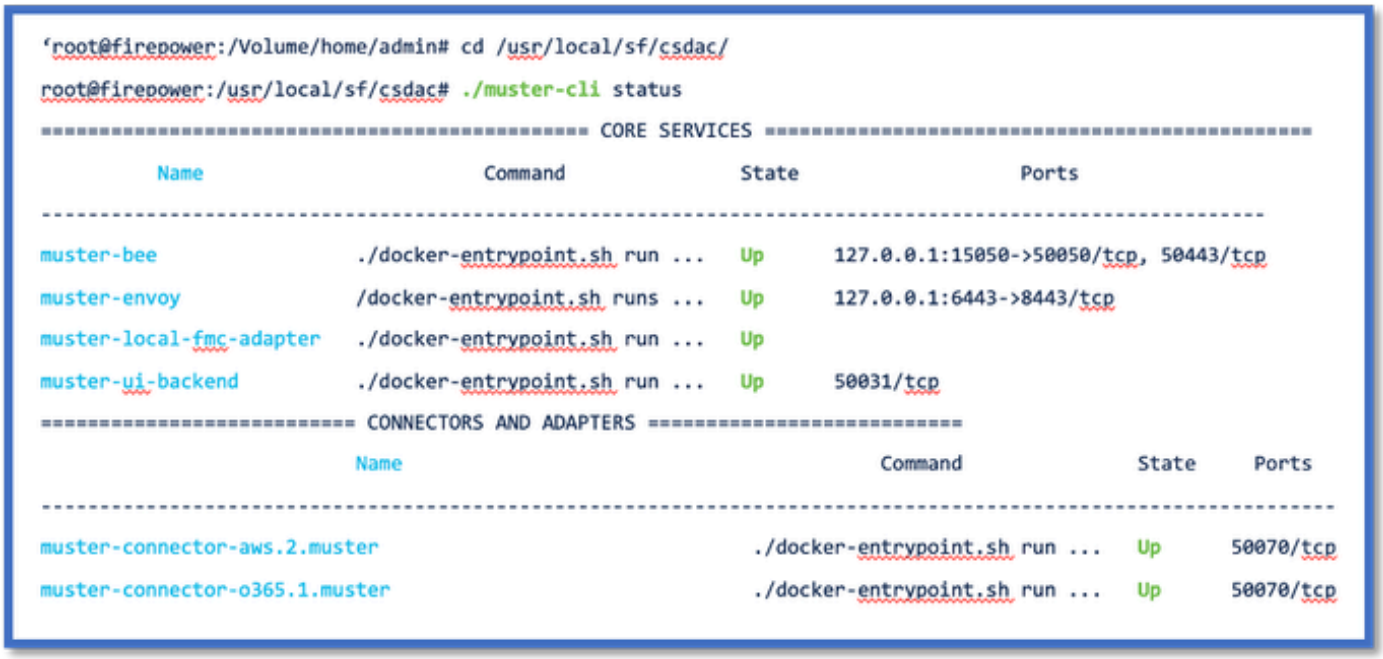
Muestra el estado del contenedor, las versiones y los detalles de la imagen del acoplador.

Troubleshooting de CLI

El script muster-cli se puede utilizar para comprobar el estado de CSDAC desde la CLI de FMC.

Si el estado de cualquier servicio es "Salido" o diferente de "Activo", comience comprobando los registros de ese contenedor.

El nombre del contenedor es necesario para obtener registros; se puede obtener de la salida.



Modo de depuración CSDAC

El script ‘muster-cli’ se puede utilizar para activar y desactivar los registros de depuración.De forma predeterminada, los contenedores se registran en INFO level.INFO y DEBUG son los únicos niveles admitidos.

Para habilitar el usuario de nivel DEBUG: ./muster-cli debug-on.

Esto proporcionaría más información para la generación de problemas y ayuda con debug.Esta opción debe estar habilitada mientras se reproduce un problema.

Para volver al nivel INFO, utilice: ./muster-cli debug-off.

<#root>

```
root@firepower:/usr/local/sf/csdac# ./muster-cli debug-on


Recreating muster-bee ...
Recreating muster-bee ... done
Recreating muster-user-analysis     ... done
Recreating muster-local-fmc-adapter ... done
Recreating muster-ui-backend        ... done
```

Mensajes registrados con depuración

Cuando el modo de depuración está habilitado, todos los registros del contenedor de docker también contendrían mensajes de depuración

Obtenga registros en tiempo real mediante los comandos de docker: docker logs -f <nombre_contenedor>

En el siguiente ejemplo, el mensaje de depuración muestra qué desencadenó un error gRPC

<#root>

```
2022-12-12 14:33:29,649 [status_storage] DEBUG: Loading status from /app/status/aws.1_status.json...
2022-12-12 14:33:29,650 [status_storage] DEBUG: Loading status from /app/status/gcp.1_status.json...
2022-12-12 14:33:29,651 [status_storage] DEBUG: Loading status from /app/status/github.1_status.json...
2022-12-12 14:33:29,651 [status_storage] DEBUG: Loading status from /app/status/o365.1_status.json...
2022-12-12 14:33:43,279 [server] DEBUG: Got health status request.

2022-12-12 14:33:43,280 [bee_api] WARNING: Got gRPC error from BEE: StatusCode.UNAVAILABLE failed to cor
```

Ejemplo de problema con la resolución de problemas

Descripción general de problemas y resolución de problemas

Problema:

El problema más común que encontramos es que FMC no recibe todos los mapeos de objetos dinámicos.

Resolución de problemas:

Para solucionar el problema,

- Habilitar el modo de depuración desde "muster-cli"
- Archivo de solución de problemas generado desde la interfaz de FMC
- Se comprobaron los registros del conector CSDAC AWS y se recopiló la solución de problemas.
- Descubrió que el conector CSDAC AWS solo consultaba la primera IP en las instancias de AWS.

Preparar paquete de solución de problemas

- Desde la CLI de FMC habilitamos el modo de depuración mediante ./muster-cli debug-on. la herramienta muster-cli está disponible en /usr/local/sf/csdac.
- Se volvió a crear el problema al esperar a que el conector tuviera el estado OK y luego verificar los filtros de atributos dinámicos.
- Recopiló los registros de solución de problemas de la interfaz de usuario de FMC y los extrajo.Comprobó los registros del conector de AWS para ver el contenido de la instantánea

Observe los atributos de etiqueta de una dirección IP

Los atributos de etiqueta para una IP dada se registran en los registros de Troubleshooting. Para el conector AWS, analizamos muster-connector-aws.1.muster-docker.log.gz

Resumen de cheques

¿Se ve bien el estado del conector y el adaptador?

Compruebe los estados en las páginas Conector, Adaptador correspondientes.

¿Consiguieron los conectores todos los mapeos?

Compruebe la vista previa de la regla para ver si hay direcciones IP coincidentes.

Verifique los registros del acoplador del conector para ver si está consultando las asignaciones correctamente.

¿Recibió el servidor REST asignaciones de etiquetas dinámicas del conector?

Compruebe la página de objetos dinámicos de FMC.

Compruebe los registros de USMS (en /opt/CSCOpx/MDC/log/operation/usmsharedsvcs.log) para ver si el servidor FMC REST ha procesado correctamente la solicitud de API de CSDAC.

Preguntas y respuestas

P: ¿Qué versión de CSDAC in situ admite un conector ISE? Tampoco veo un conector de este tipo en la versión 7.4.0 (compilación 1494).

R.: Se encuentra en CSDAC independiente y no en FMC ni en CDO. Para probarlo, necesitará un paquete CSDAC ansible.

P: Cuando se publique, ¿qué versión de CSDAC in situ sería?

R: Probablemente 2.1.0.

P: Se ha mostrado una pantalla con un engranaje que tiene API colocada sobre ella. Creo que es CSDAC; ¿qué significa eso?

R: El explorador de API está incorporado en este CSDAC. Desde esta página puede realizar llamadas de API a CSDAC.

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).