Implante o conector de atributo dinâmico seguro no FMC

Contents

Introdução

Este documento descreve sobre o Cisco Secure Dynamic Attribute Connector no FMC.

Segundo Plano - Problema

O CSDAC (Cisco Secure Dynamic Attributes Connector) pode ser integrado ao FMC (Firepower Management Center), fornecendo o mesmo nível de funcionalidade que o aplicativo CSDAC independente e o CSDAC no CDO. Para o CSDAC autônomo, ele libera os clientes das despesas gerais de administração e manutenção de uma máquina separada para o CSDAC. Como administrador de rede, quero que as interfaces programáticas sejam fáceis de integrar e manter-se atualizadas com as alterações nos provedores de ambiente dinâmico externo. Essa integração resolve o problema de coletar atributos de ambientes de nuvem que mudam dinamicamente sem implantar uma política.

Solução (Resumo)

O CSDAC agora pode ser configurado no FMC para buscar atributos de marca do Azure, vCenter, AWS, GCP, Office 365 e etiquetas de serviço do Azure, fornecendo paridade de recursos com o CSDAC e o CSDAC autônomos no CDO.

- Agora você pode optar por usar
  - CSDAC no CVP (ou)
  - CSDAC em CDO (ou)
  - CSDAC independente
- Mercado-alvo: empresas, provedores de serviços

Conector de atributos dinâmicos no resumo do FMC

Conector de atributos dinâmicos do FMC:

- Painel para criar e operar os recursos do Conector de Atributo Dinâmico.
- IU do FMC para configurar Conectores de Carga de Trabalho de Origem (AWS, Azure, vCenter, Office 365, GCP)
- FMC UI para definir filtros de atributo dinâmico para criar objetos dinâmicos

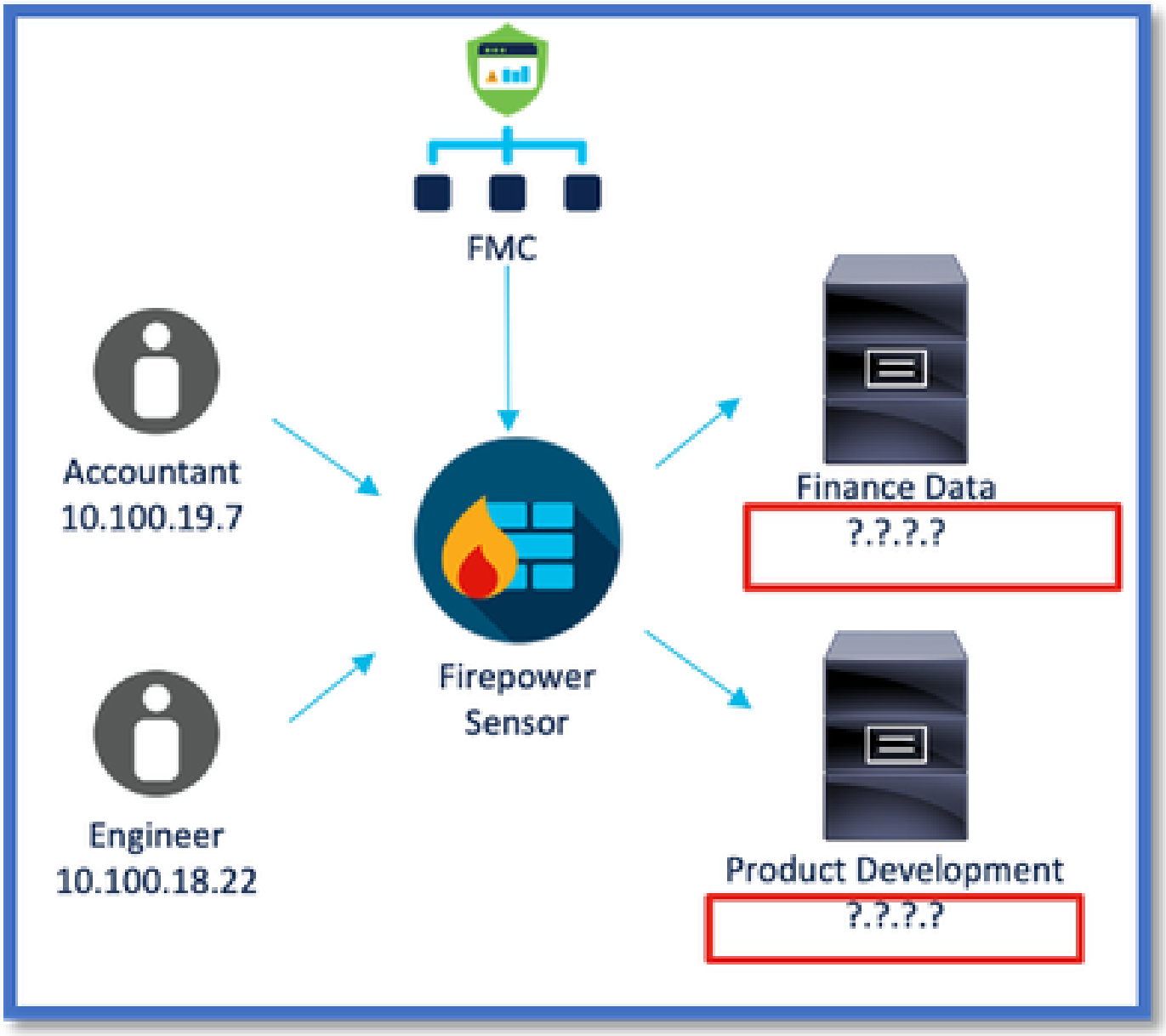
Exemplos de implantação

CSDAC no local

No ano passado, implantei uma VM dedicada para o CSDAC para coletar atributos de minhas contas do AWS e do Azure.

O problema

Agora, minha empresa mudou para a nuvem e não posso implantar e gerenciar uma máquina virtual dedicada para o CSDAC em meu ambiente.



Opção 1: Usar o conector de atributos dinâmicos integrado ao FMC

Você pode corrigir o problema usando o conector de atributos dinâmicos criado dentro do FMC. Os objetos dinâmicos criados por ele podem ser usados na Política de acesso.

Opção 2: usar o conector de atributos dinâmicos fornecido em nuvem no CDO

Você pode corrigir o problema usando o conector de atributos dinâmicos no CDO. Os objetos

dinâmicos criados por ele podem ser usados em

- FMC CDO fornecido em nuvem
- CDO no local

Pré-requisitos, plataformas suportadas, licenciamento

Plataformas mínimas de software e hardware suportadas

Mín. de Versão do Gerenciador com Suporte	Dispositivos gerenciados	Mín. de Dispositivos Gerenciados com Suporte Versão Necessária	Notas
CVP 7.4	Qualquer FTD suportado	Qualquer FTD 7.0+	

* O Conector de Atributos Dinâmicos não tem suporte em Dispositivos Gerenciados pelo FDM

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:
· Cisco Firewall Management Center executando a versão 7.4
· Cisco Firepower Threat Defense executando a versão 7.4 ou posterior.
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Detalhes do recurso

Visão geral do CSDAC independente (Lançado atualmente - 7.4)

O Cisco Secure Dynamic Attributes Connector permite usar marcas de várias plataformas de serviços em nuvem nas regras de controle de acesso do Centro de Gerenciamento de Firewall (FMC).

O CSDAC no local pode ser instalado em uma máquina Linux e oferece suporte à obtenção de atributos de:

- AWS,Azure,VMware vCenter e NSX-T,Office 365,Marcas de serviço do Azure,GCP,GitHub.

Visão geral do CSDAC no CDO (Lançado atualmente - 7.4)

Suporta a mesma funcionalidade do CSDAC no local sem a necessidade de instalar e manter um aplicativo dedicado.

O conector vCenter não é suportado no CDO.

Suporta o envio dos atributos recebidos para FMC fornecido na nuvem e FMC no local em CDO.

CSDAC no CVP

Suporta a mesma funcionalidade do CSDAC independente sem a necessidade de instalar e manter um aplicativo dedicado.

O CSDAC no FMC suporta a obtenção de atributos de:

- AWS,Azure,VMware vCenter e NSX-T,Office 365,Marcas de serviço do Azure,GCP,GitHub

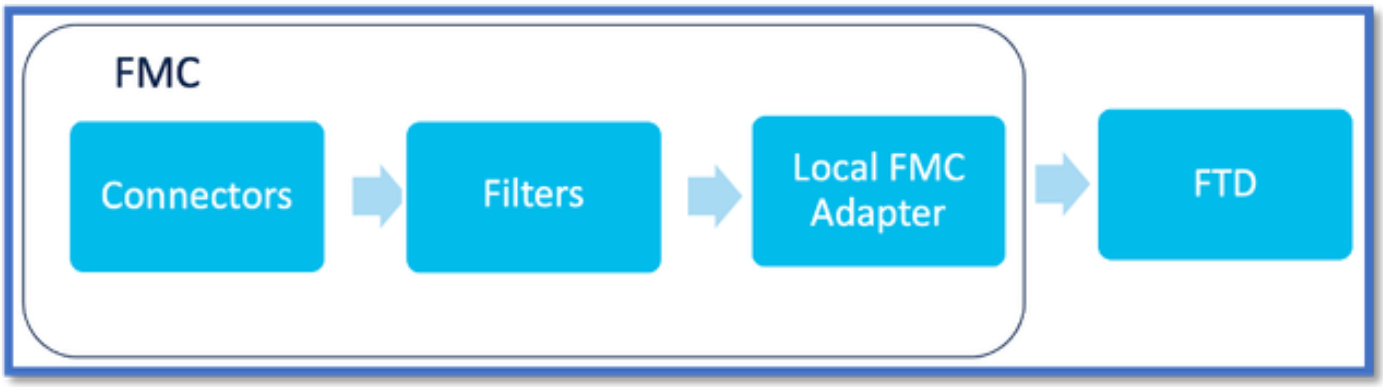
Não há configuração explícita do adaptador aqui, pois ele é local para o FMC.

Como funciona

Os conectores são usados para obter atributos do AWS, Azure, o365, vCenter.

O adaptador local é usado para salvar esses atributos dinamizados e seus mapeamentos IP no FMC como objetos dinâmicos.

O FMC envia o mapeamento em tempo real para o FTD (sem implantação).



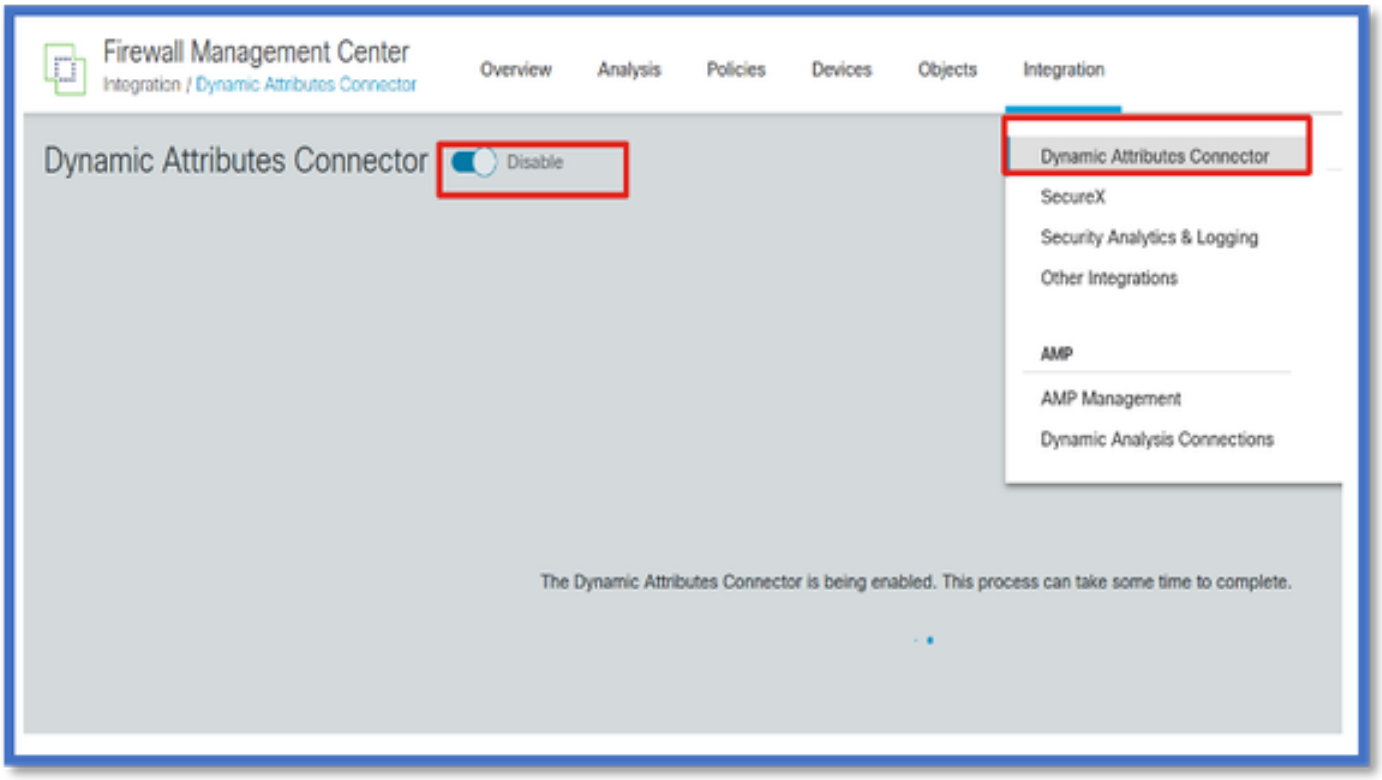
Habilitar CSDAC no FMC

Navegue até Integração > Conector de Atributos Dinâmicos.

Use o botão de alternância para ativar o conector.

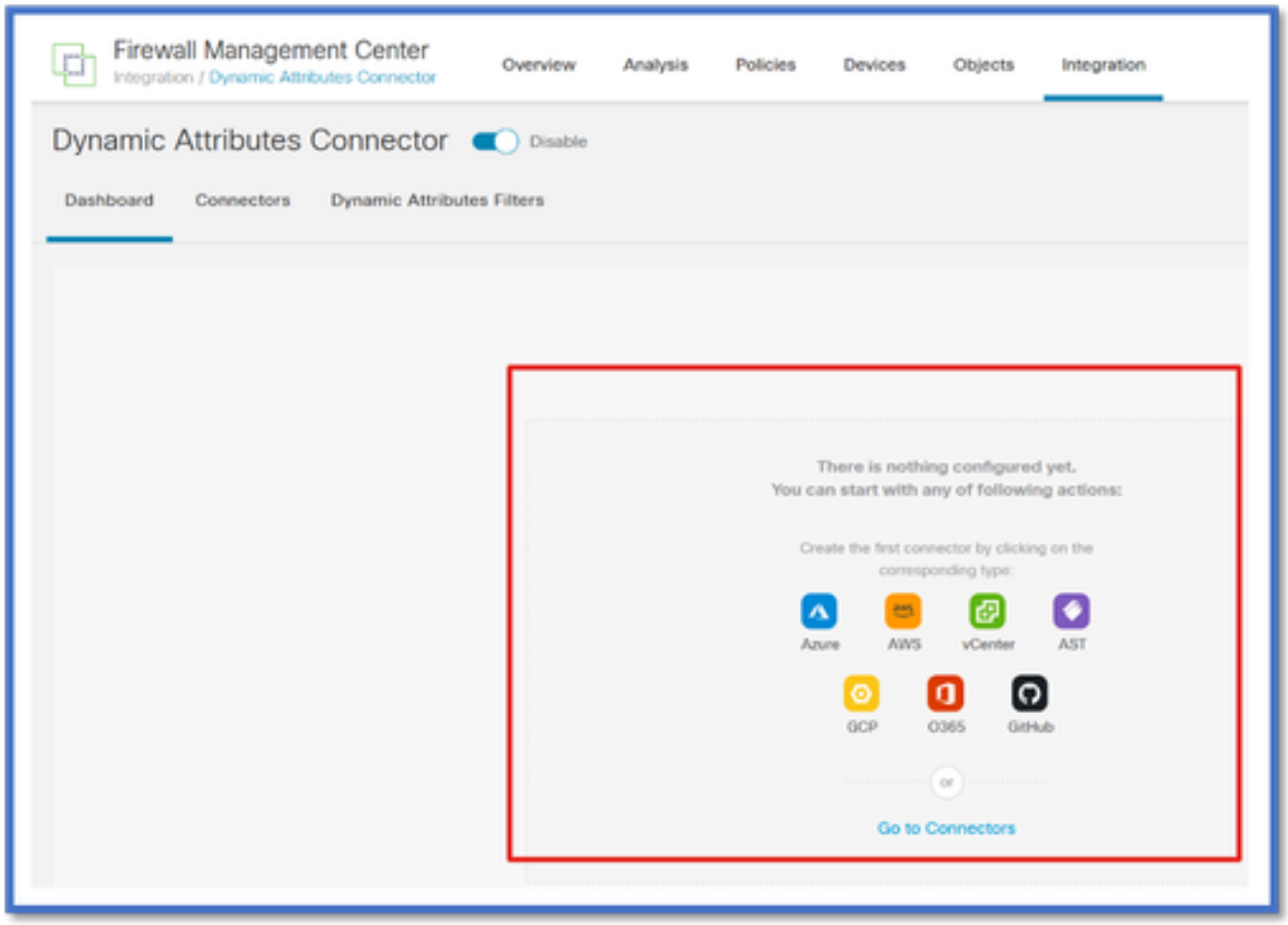
O FMC leva alguns minutos para fazer o download e exibir as imagens e os contêineres do docker.

Isso só pode ser configurado no domínio global do FMC.



Painel CSDAC

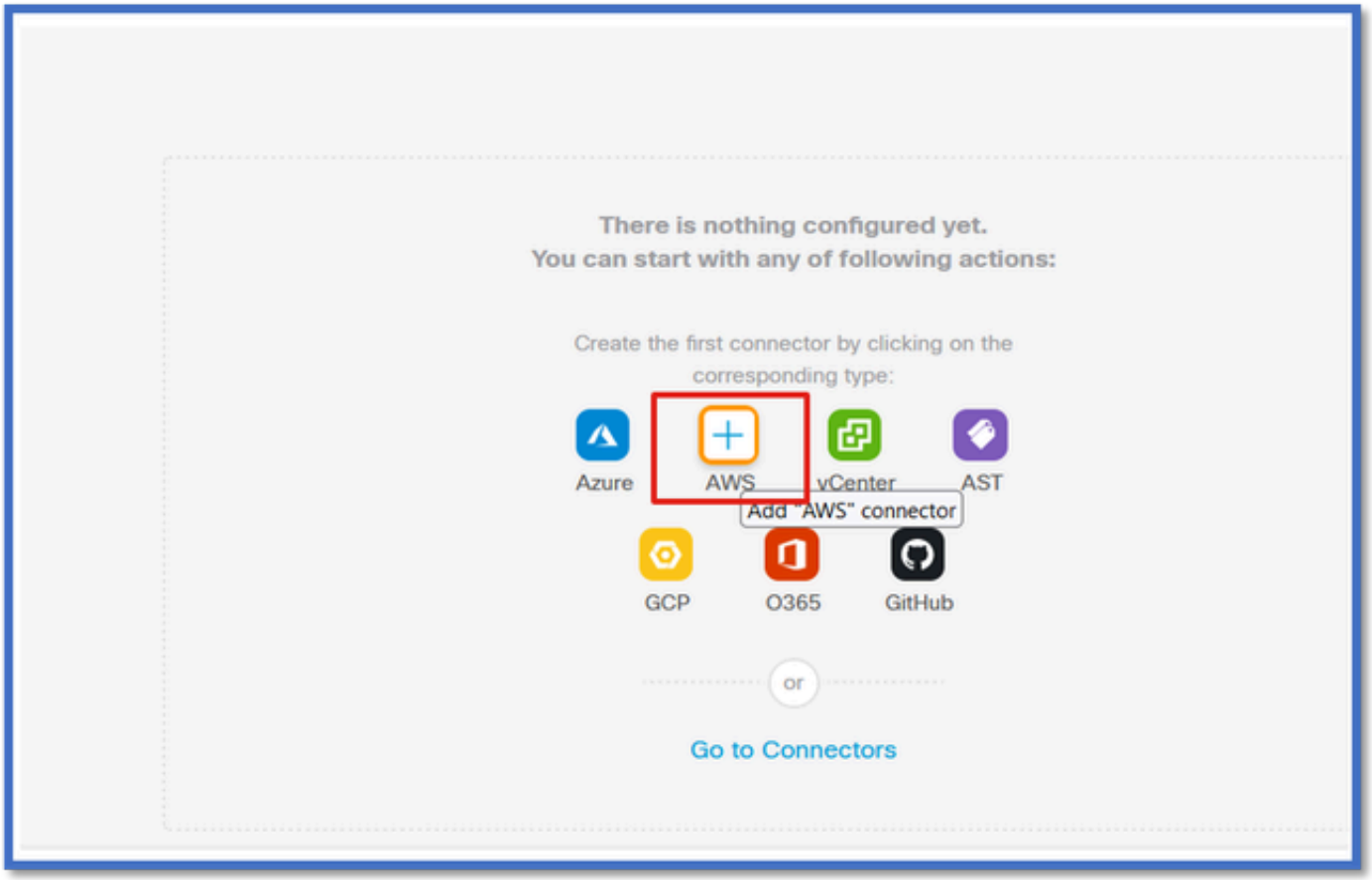
Depois de ativar o CSDAC, o usuário verá a página Painel do CSDAC. O painel é usado para configurar e exibir conectores e filtros consolidados.



Configurar conectores

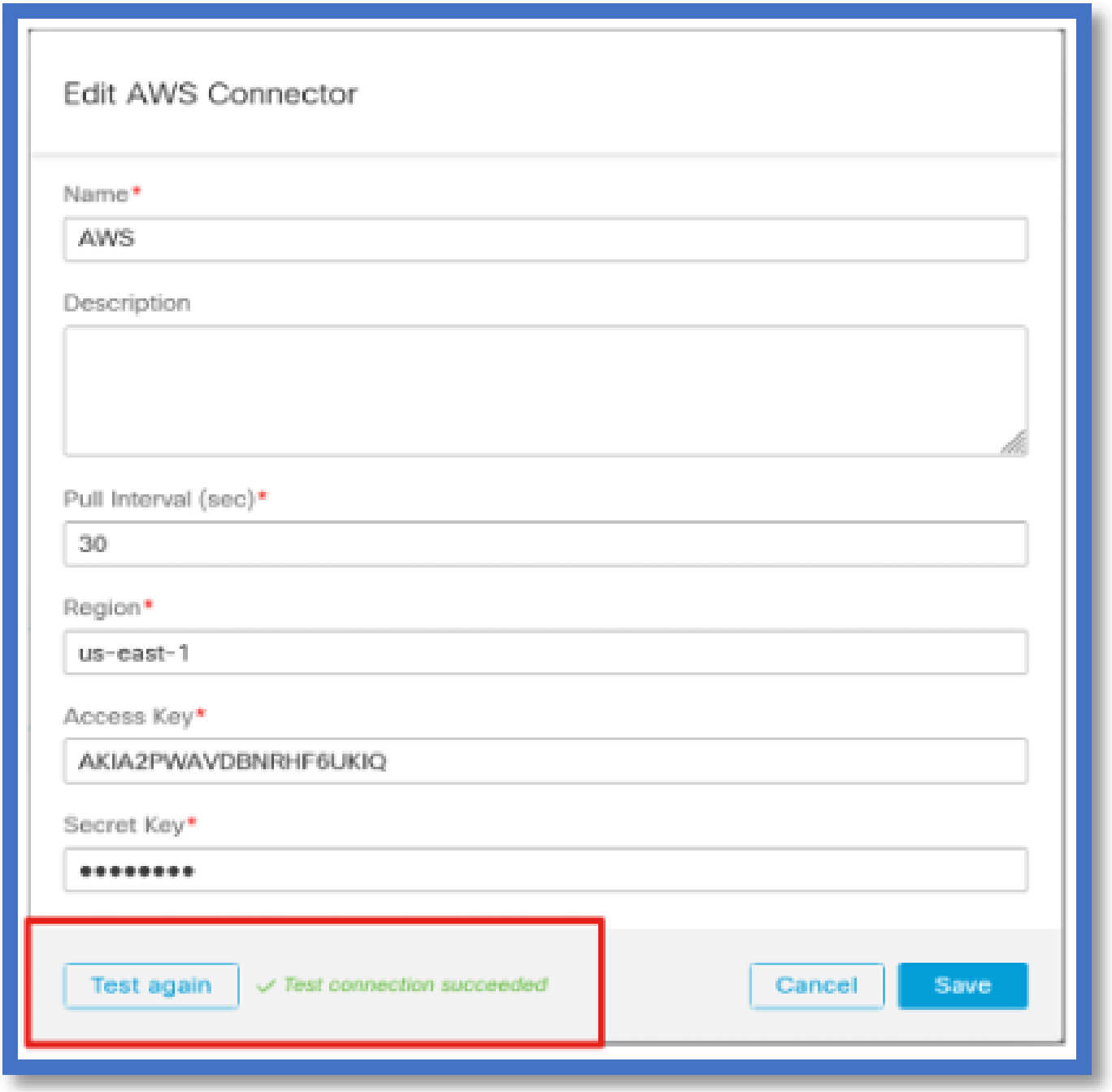
Adicionar Conectores do Painel

No Painel, clique no ícone do conector desejado para adicioná-lo.



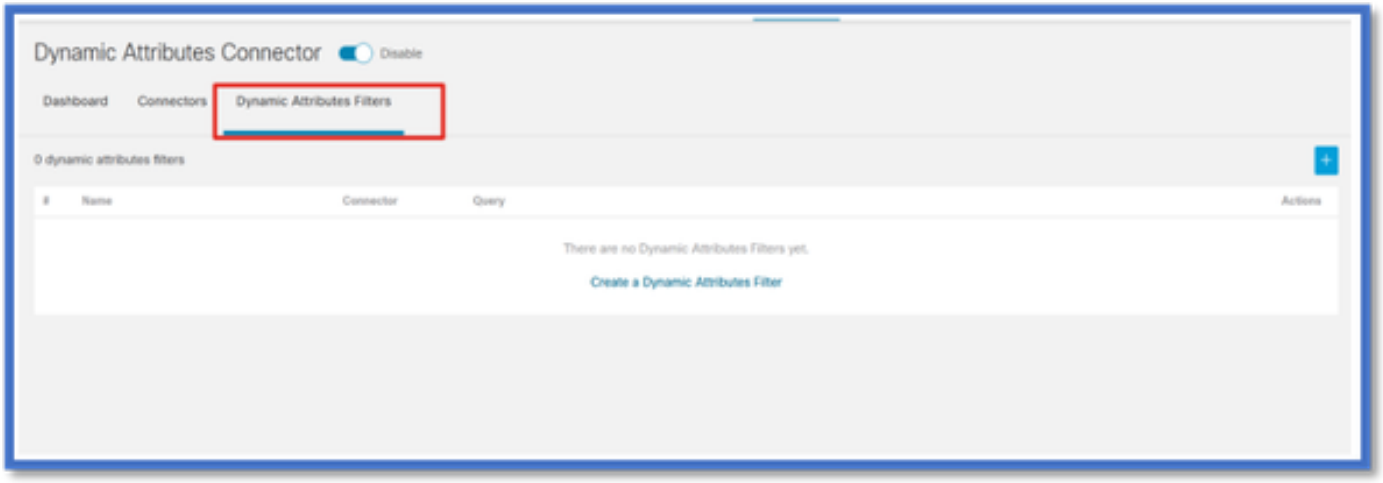
Configure um intervalo de tempo (no campo Intervalo de Recebimento) para que os conectores possam receber informações de provedores com a periodicidade configurada.

Digite as credenciais do provedor para obter os atributos da tag. Depois de configurar o conector, você pode testá-lo clicando no botão Testar.



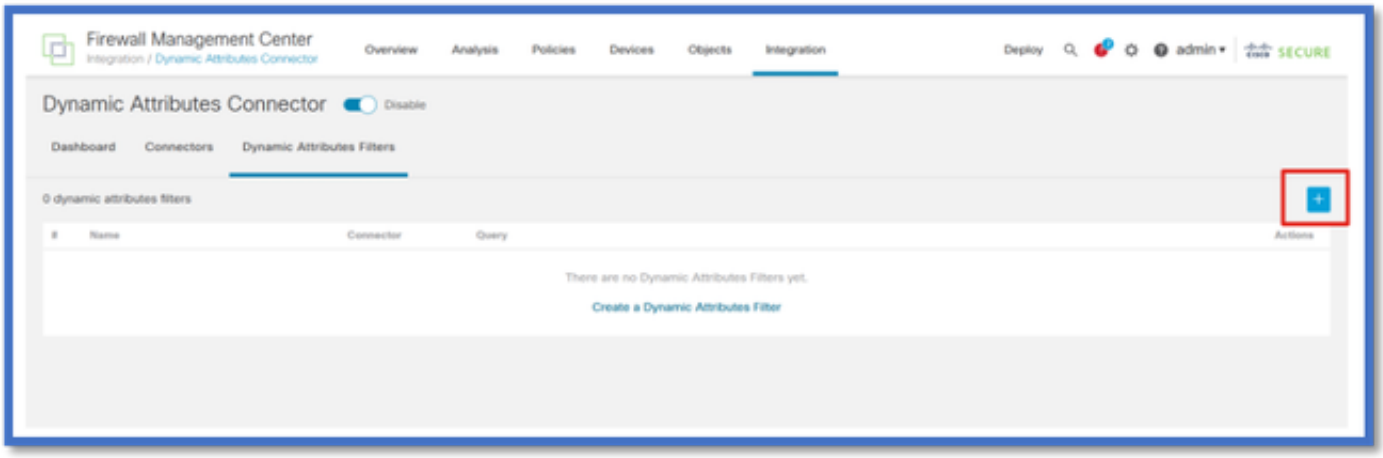
Configurar filtros

Clique na guia "Filtros de atributos dinâmicos" no menu "Conector de atributos dinâmicos" para ir para a página Filtros de atributos dinâmicos.



Adicionando filtros

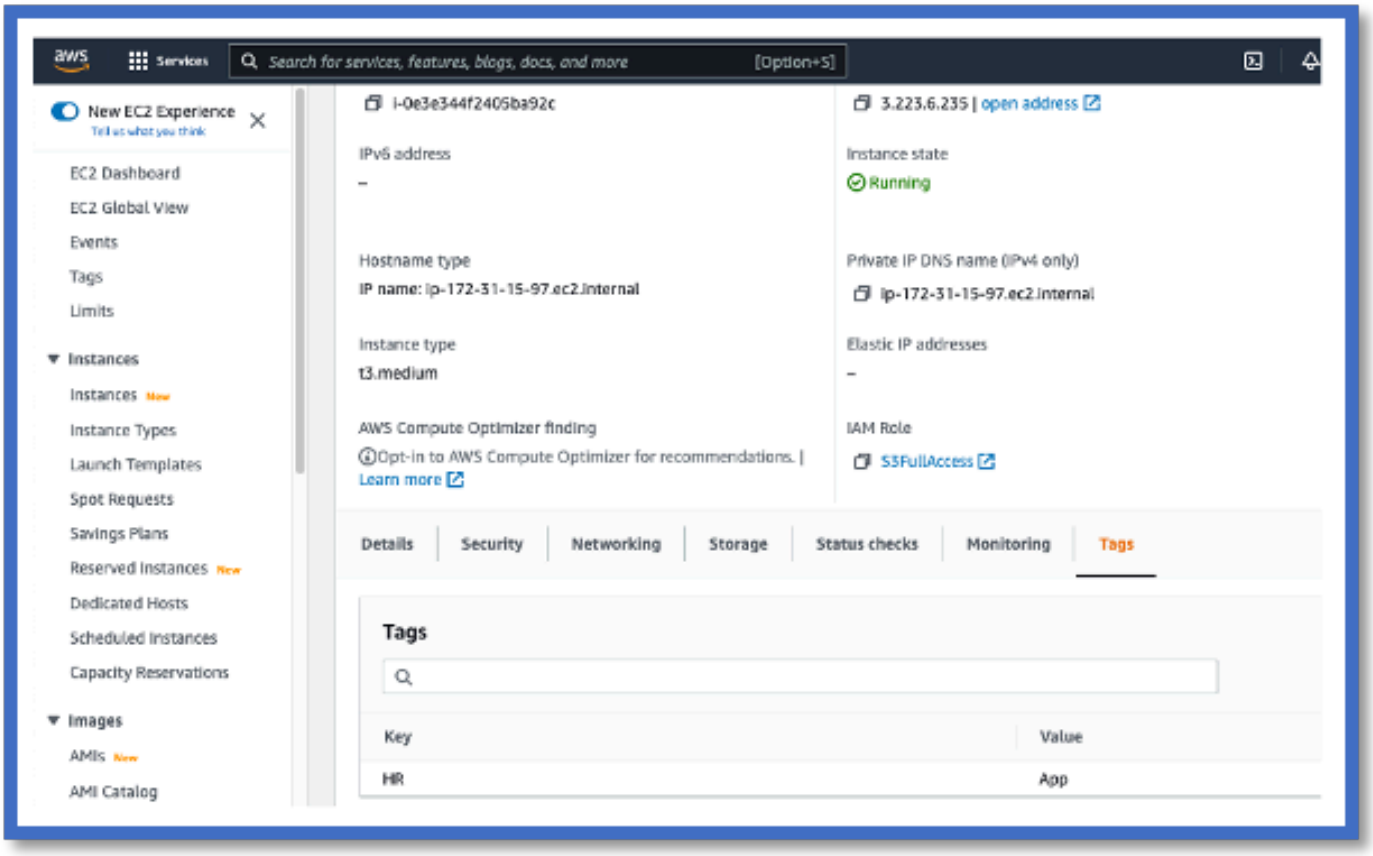
Clique no botão + para criar um filtro para conectores de atributo.



Adicionar marcas AWS

Por exemplo, podemos supor que você está interessado na chave ‘HR’ e no valor ‘App’ nas cargas de trabalho do AWS.

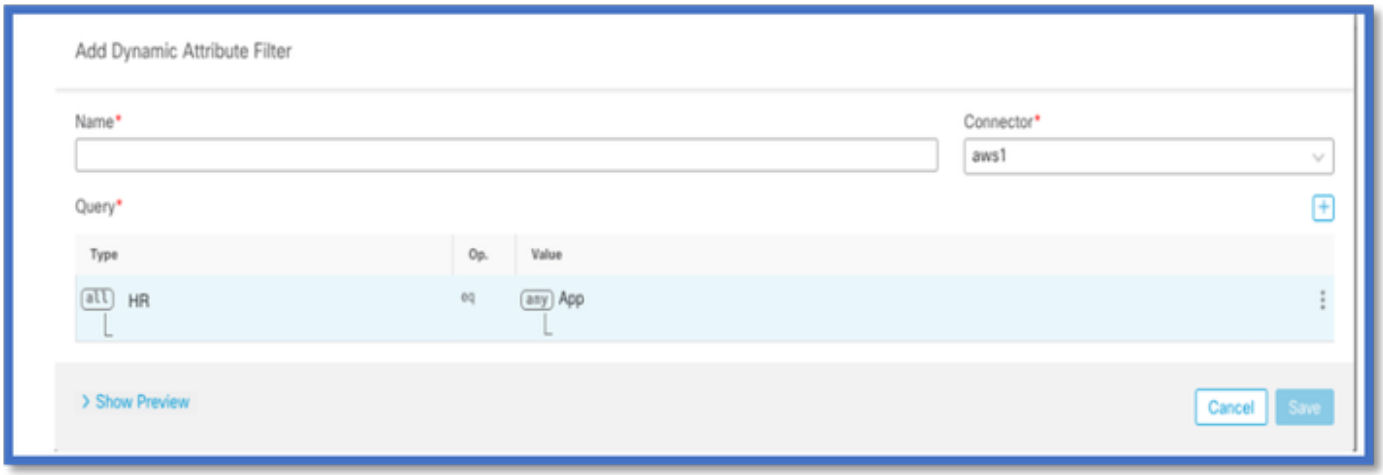
Isto é como se pareceria no AWS.



CSDAC no CVP

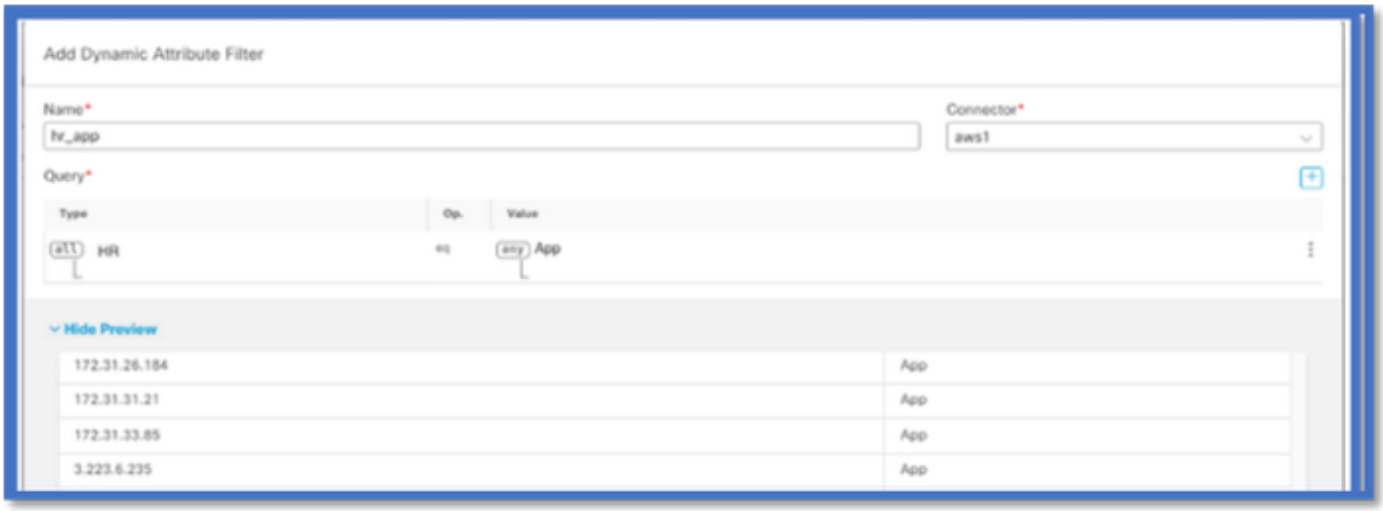
Você pode criar uma regra "RH igual a Aplicativo" clicando no botão +.

O adaptador FMC local enviaria os endereços IP correspondentes como mapeamentos de objetos dinâmicos ao FMC



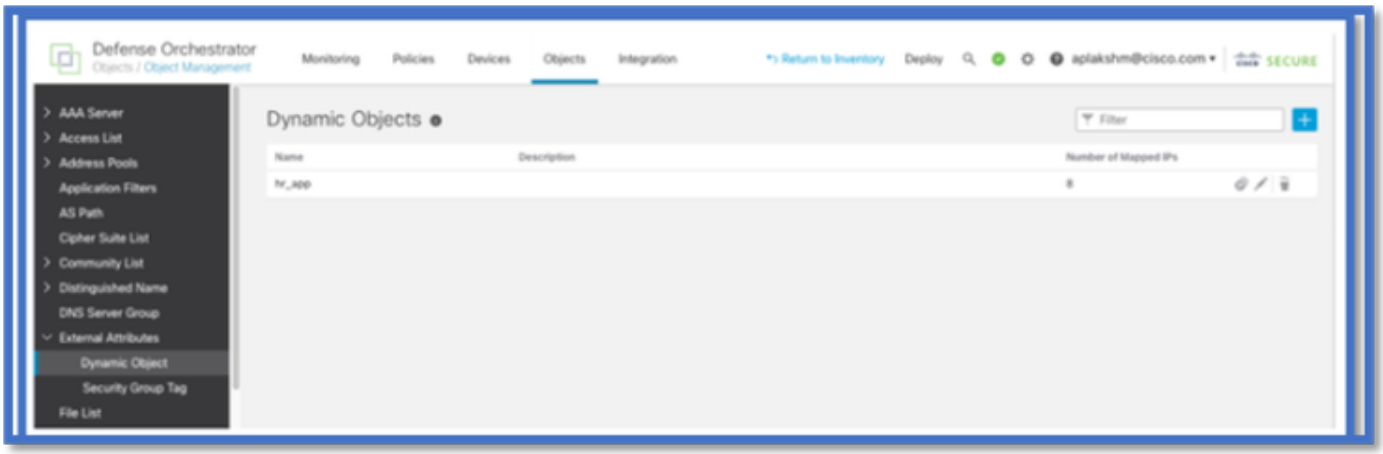
Visualização

Você também pode exibir os endereços IP correspondentes de uma regra de atributo específica clicando no botão ‘Mostrar | Ocultar o botão Visualizar.



Objetos dinâmicos

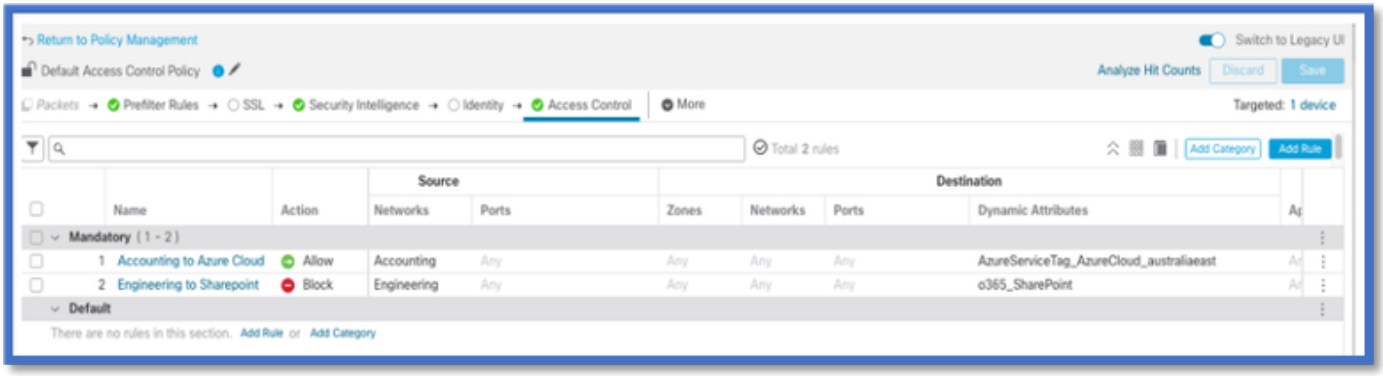
Exibir os objetos dinâmicos criados pelo CSDAC em Objetos > Atributos externos, Objeto dinâmico no FMC



Política de CA

Configuração: política de acesso

No FMC, adicione uma política de acesso para permitir ou bloquear os objetos dinâmicos recebidos do conector de atributo dinâmico.



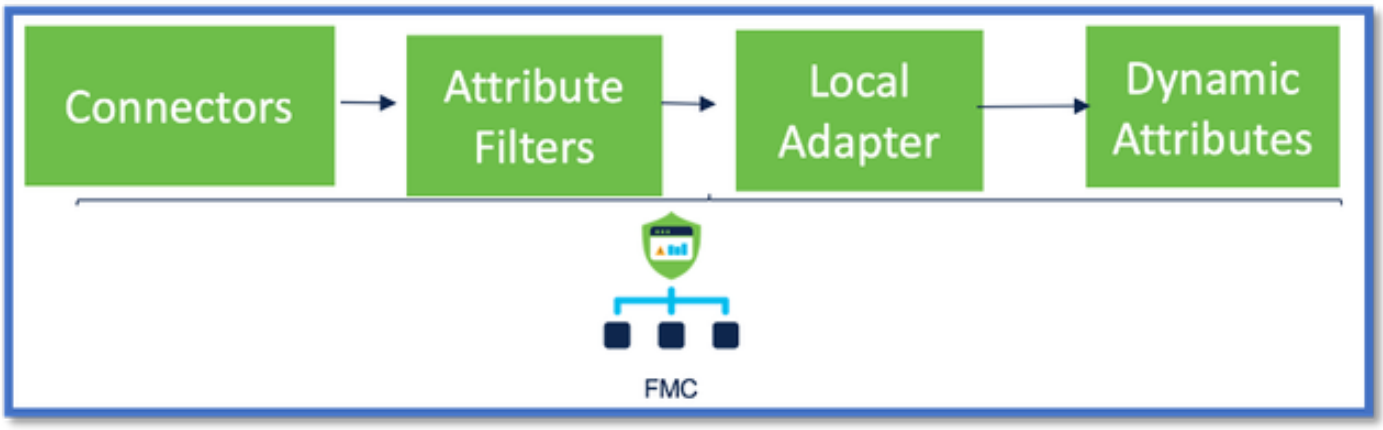
Limites da plataforma

- Os limites do conector se baseiam na memória FMC disponível.
- O vFMC precisaria de uma memória extra de 1 GB para suportar 5 conectores
- O realm do Azure AD também está incluído no limite, pois também é um contêiner do CSDAC.

Modelos	Número de conectores suportados	Plataformas	Limite baseado na memória
Básico	Somente Azure AD	1600	32 GB
Pequeno	5	vFMC	> 32 GB
Médio	10	vFMC 300, 2600	>= 64 GB
Grande	20	4600	>= 128 GB

Solução de problemas/diagnósticos

A melhor forma de solucionar problemas é rastrear objetos dinâmicos de Conectores CSDAC para Atributos Dinâmicos no FMC.Muitos registros internos se referem a esse recurso como "reunião". Você pode observar o estado do sistema ao longo da cadeia de broadcast para isolar os problemas. O CSDAC usa contêineres Docker. As mensagens e os nomes de registros e outros arquivos devem ser chamados de "docker"



Verifique os conectores

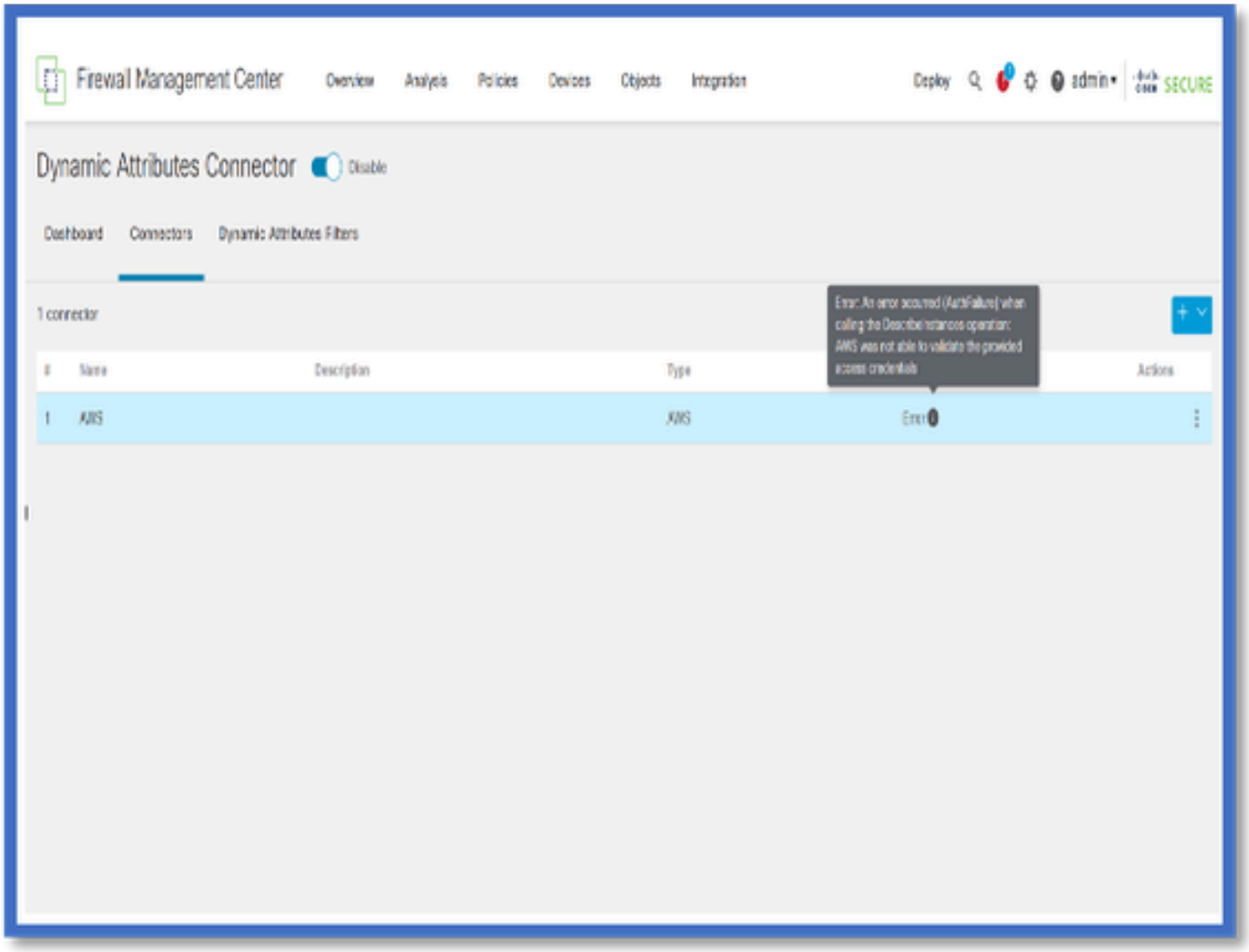
Primeiro, verifique se os Conectores podem se conectar aos servidores vCenter, AWS ou Azure.

Se os conectores não estiverem configurados corretamente, os processos de downstream não poderão obter informações de marcação.

Exibir conectores na guia Conectores

O status do conector é exibido no campo de status e atualizado a cada 15 segundos.

Aqui, vemos que o conector não pôde autenticar usando as credenciais fornecidas.



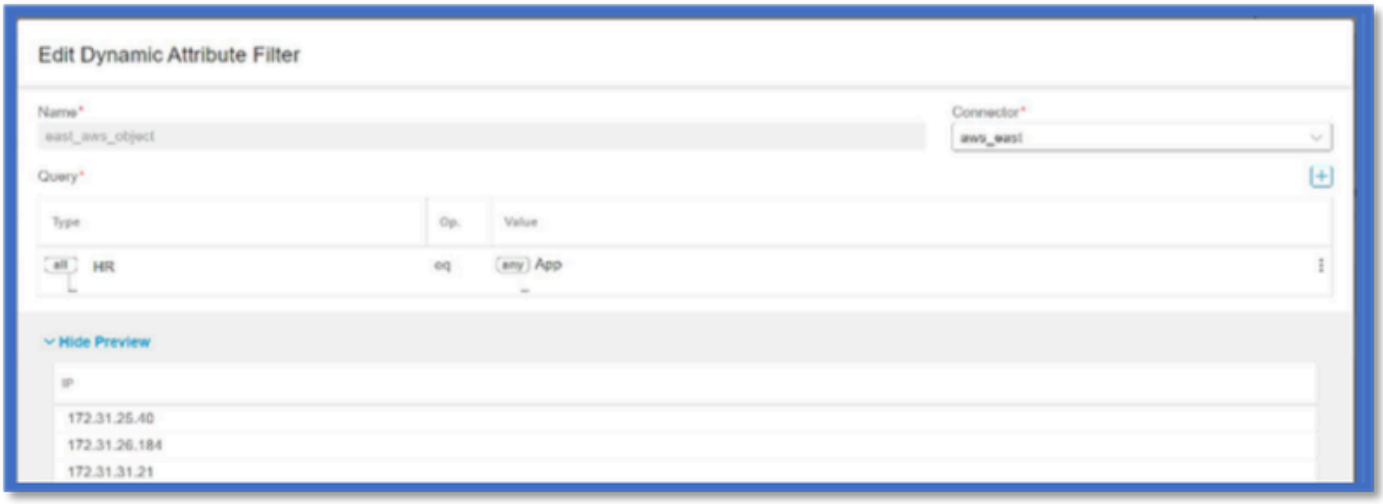
Verificar os Filtros de Atributo

Verifique se a visualização Rule (Regra) mostra os endereços IP correspondentes para a condição da consulta.

Se não houver endereços IP correspondentes, o FMC não poderá obter os mapeamentos de objetos dinâmicos.

Verificando os Filtros de Atributos

Verifique se os mapeamentos de IP de atributo dinâmico estão disponíveis em Visualização. O botão Mostrar visualização está disponível no pop-up de edição do Filtro de Atributos Dinâmicos.



Verifique os objetos dinâmicos na interface do usuário do FMC

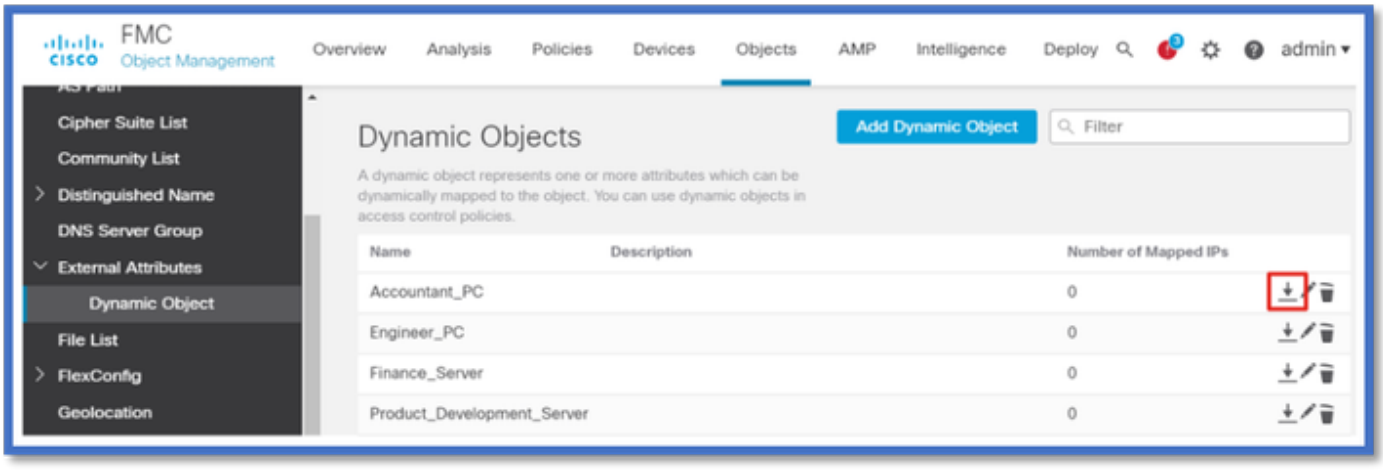
Primeiro, certifique-se de que o servidor FMC contenha as vinculações esperadas.

- Procure em Gerenciamento de objetos, guia Objetos externos, verifique Objetos dinâmicos para vinculações.
- Se o FMC não obtiver as vinculações, o FTD não poderá obtê-las.

Verifique o Monitor de integridade do FMC e as notificações para alertas de integridade do CSDAC.

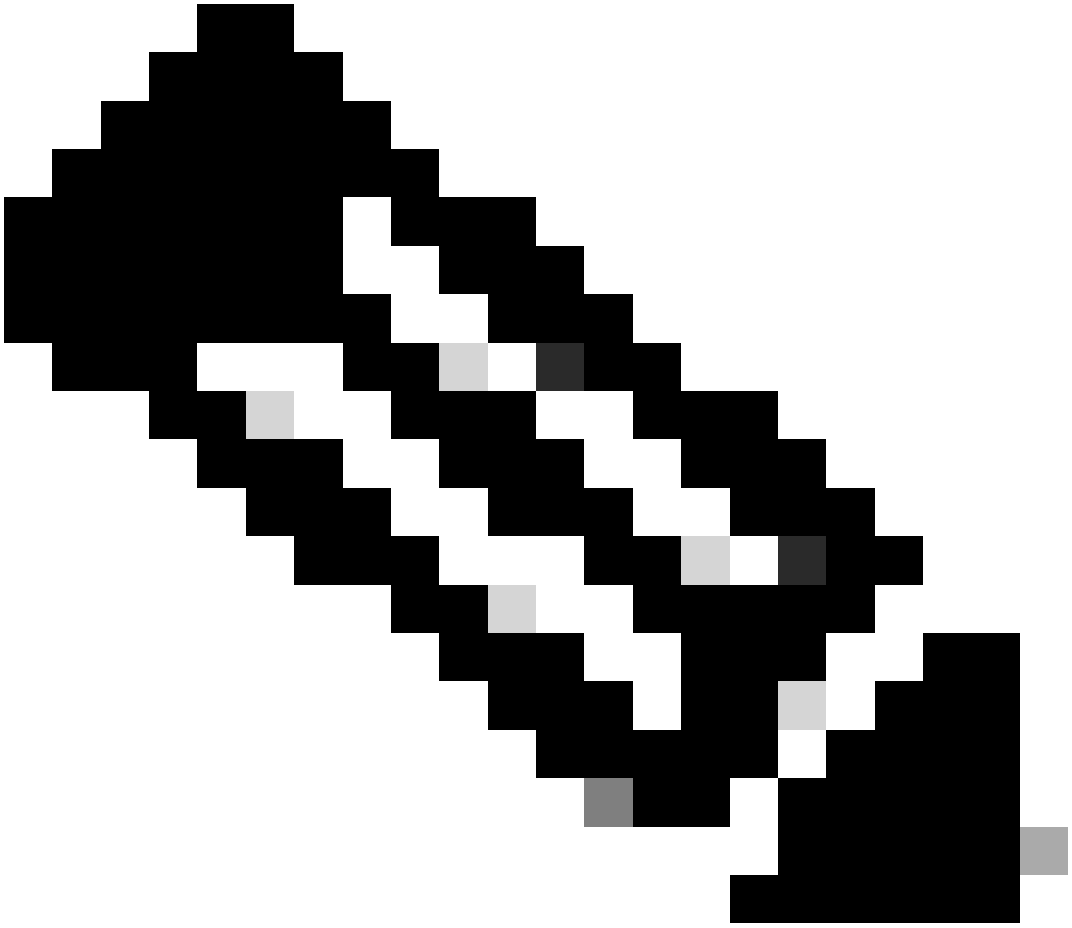
Verificando Objetos Dinâmicos

O FMC Object Manager permite que você faça download dos endereços IP atuais de objetos dinâmicos.

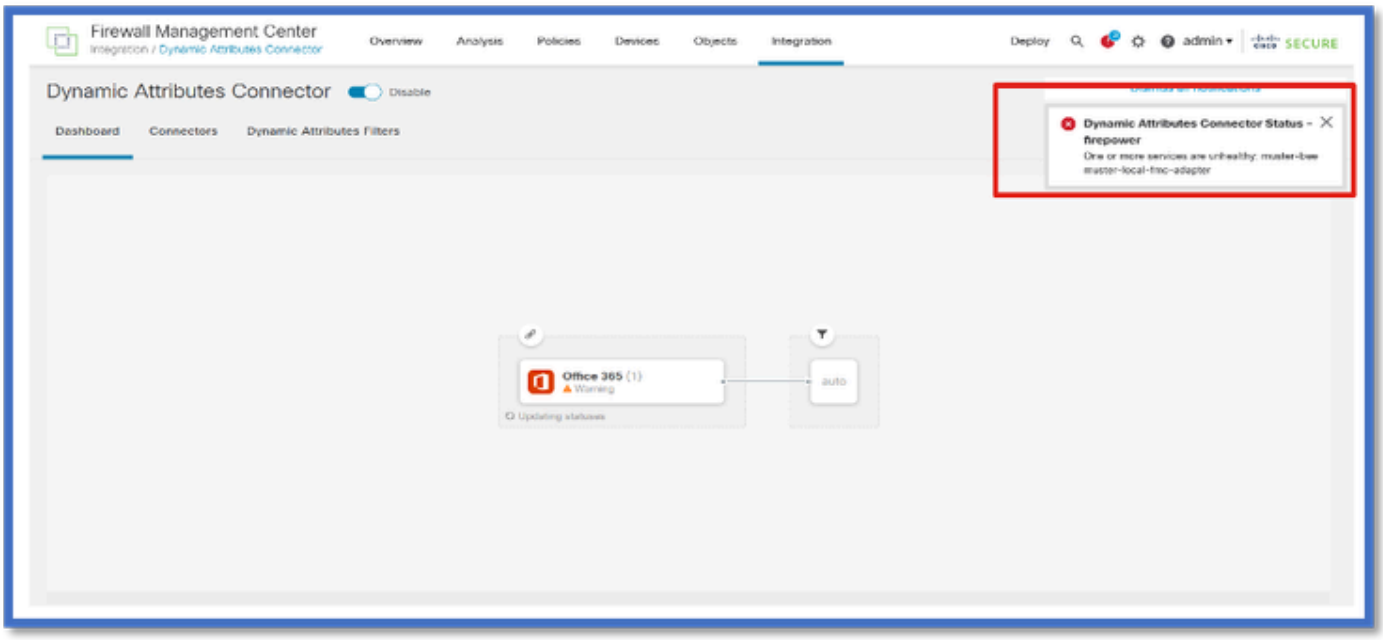


Alertas de integridade do CSDAC

O Gerenciador de tarefas do FMC exibe alertas de integridade se algum serviço principal, incluindo o conector de atributos dinâmicos, estiver inoperante. O Alerta contém informações sobre o nome e o status do serviço.

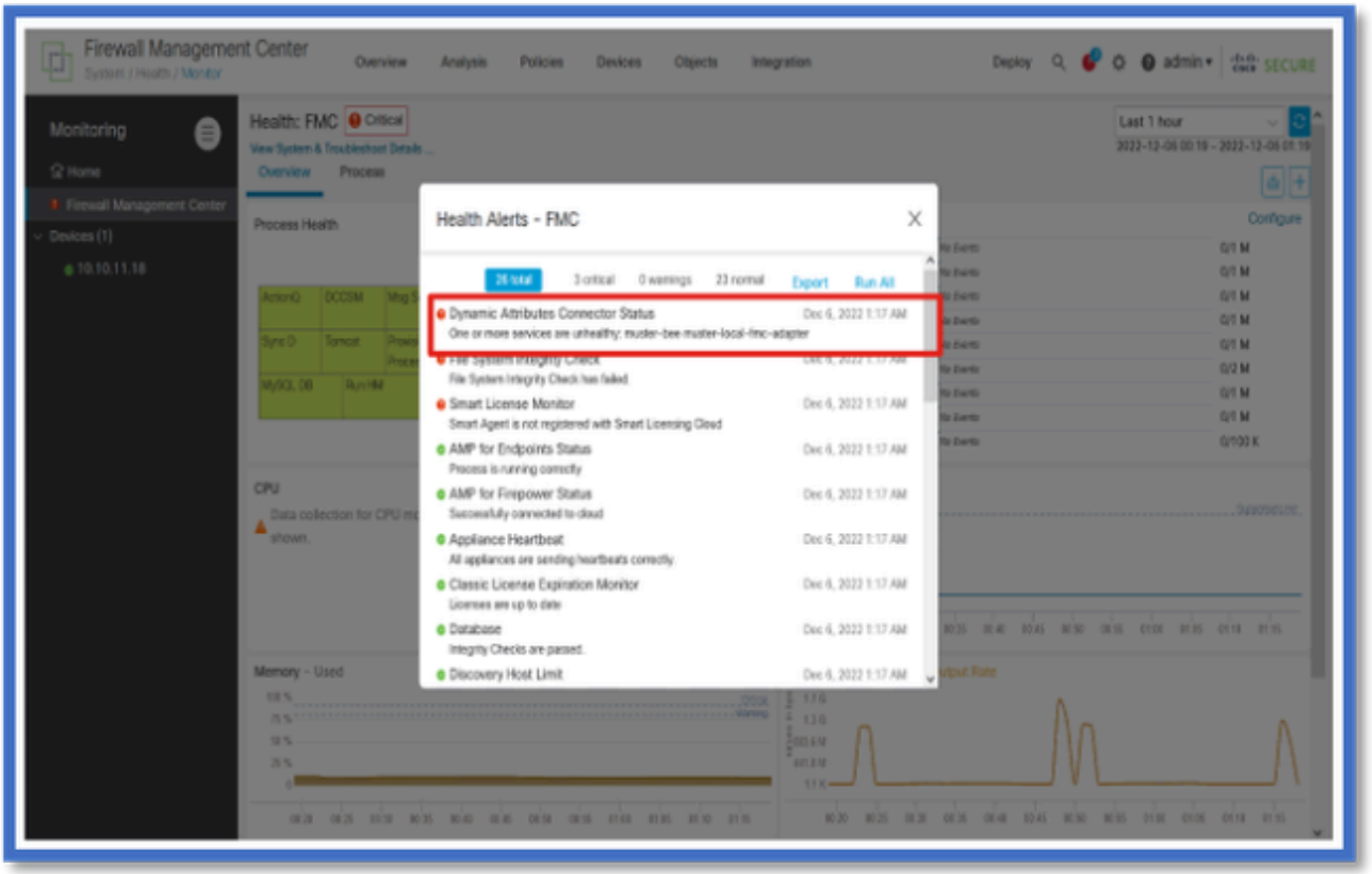


Observação: ainda temos o nome "de reunião" em várias notificações e é necessário fornecer aqui o nome do serviço para obter informações detalhadas.



Aqui vemos que o muster-bee e o muster-local-fmc-adapter são "não saudáveis".

Se o erro indicar qualquer um dos serviços principais, os logs de solução de problemas precisam ser coletados para a depuração.



CSDAC em soluções de problemas

Gerando uma solução de problemas do CSDAC

- Os logs do CSDAC são coletados automaticamente durante a geração de Troubleshooting do FMC. O pacote contém o status do Docker, logs e dados necessários para depurar o problema off-line.
- A prática recomendada é ativar o modo de depuração CSDAC antes de reproduzir o erro para o qual os logs de solução de problemas são coletados .

A partir de /usr/local/sf/csdac, chame ./muster-cli debug-on

Localize os logs do CSDAC em Solução de problemas não-tarred nestas pastas:

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

Contém os dados armazenados no banco de dados etcd.

/results-XX/saída-comando/solução_de_problemas_csdac /log

Contém os logs dos contêineres do docker.

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

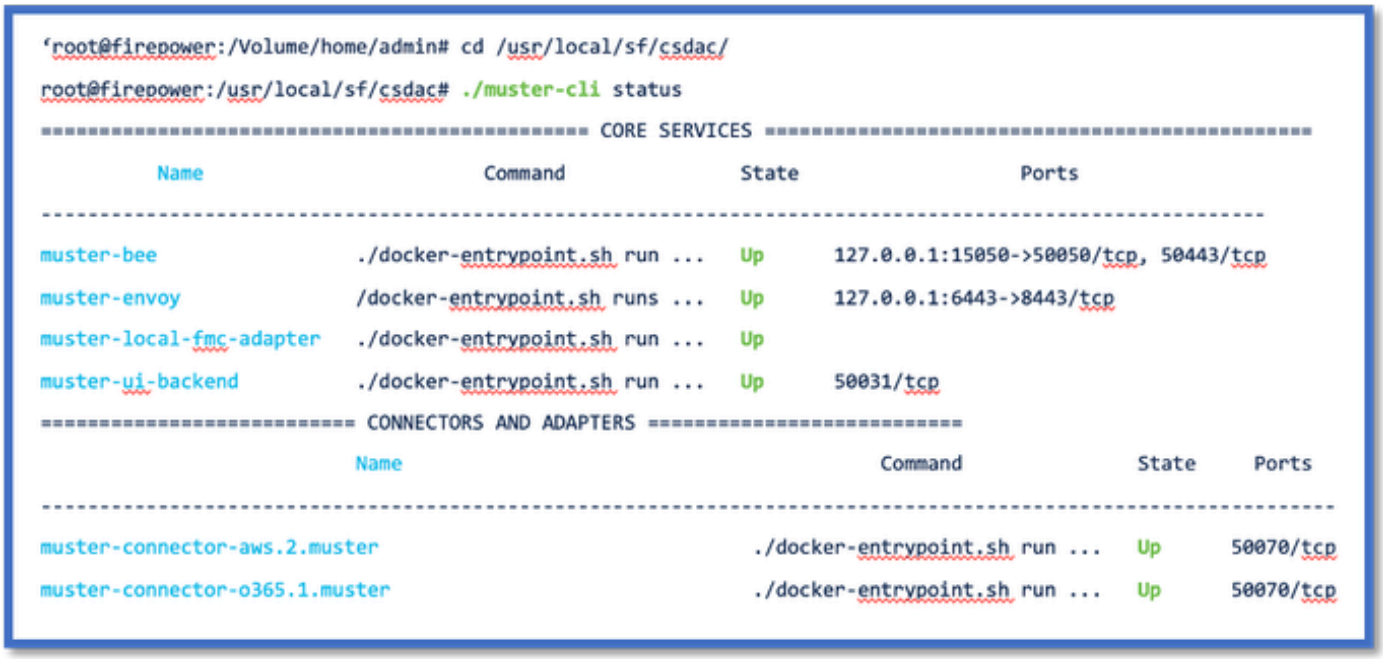
Mostra o status do contêiner, as versões e os detalhes da imagem de encaixe.

Solução de problemas de CLI

O script muster-cli pode ser usado para verificar o status do CSDAC na CLI do FMC.

Se o status de qualquer serviço for "Saindo" ou diferente de "Ativo", comece verificando os logs desse contêiner.

O Nome do contêiner é necessário para obter logs; ele pode ser obtido da saída.



Modo de depuração CSDAC

O script ‘muster-cli’ pode ser usado para ativar e desativar os logs de depuração.Por padrão, os contêineres são registrados no INFO level.INFO e DEBUG são os únicos níveis suportados.

Para ativar o nível de DEPURAÇÃO user: ./muster-cli debug-on.

Isso forneceria mais informações para geração de solução de problemas e ajuda na depuração.Essa opção deve ser habilitada durante a reprodução de um problema.

Para retornar ao nível INFO, use: ./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
```

Mensagens registradas com Depuração

Quando o modo de depuração estiver habilitado, todos os logs do contêiner do docker também conterão mensagens de depuração

Obtenha registros em tempo real usando comandos docker: docker logs -f <container_name>

No exemplo abaixo, a mensagem de depuração mostra o que acionou um erro 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
```

Exemplo de problema com Troubleshooting de Passo a Passo

Visão geral de problemas e solução de problemas

Problema:

O problema mais comum que encontramos é que o FMC não recebe todos os mapeamentos de

objetos dinâmicos.

Troubleshooting:

Para solucionar o problema,

- Ativar o modo de depuração a partir de "muster-cli"
- Arquivo de solução de problemas gerado da interface do usuário do FMC
- Verificados os registros do CSDAC AWS Connector no coletaram a Solução de problemas.
- Descobriu que o CSDAC AWS Connector somente consultou o primeiro IP nas instâncias do AWS.

Preparar pacote de solução de problemas

- Na CLI do FMC, ativamos o modo de depuração usando ./muster-cli debug-on. A ferramenta muster-cli está disponível em /usr/local/sf/csdac.
- Recriado o problema aguardando que o conector tenha o status OK e verificando os Filtros de atributo dinâmico.
- Coletados os logs de solução de problemas da interface do usuário do FMC e extraídos.Verificados os logs do AWS Connector quanto ao conteúdo do instantâneo

Examine os atributos de tag para um IP

Os atributos de tag para um determinado IP são registrados nos registros de Troubleshooting. Para o AWS Connector, examinamos muster-connector-aws.1.muster-docker.log.gz

Resumo das verificações

O status do conector e do adaptador parece bom?

Verifique os status nas páginas Connector, Adapter correspondentes.

Os Conectores obtiveram todos os mapeamentos?

Verifique se há endereços IP correspondentes na visualização da regra.

Verifique os logs do encaixe do conector para ver se ele está consultando os mapeamentos corretamente.

O servidor REST recebeu mapeamentos de marcas dinâmicas do conector?

Verifique a página de objetos dinâmicos do FMC.

Verifique os logs do USMS (em /opt/CSCOpx/MDC/log/operation/usmsharedsvcs.log) para ver se o servidor FMC REST processou corretamente a solicitação da API do CSDAC.

Perguntas e respostas

P: Que versão do CSDAC local oferece suporte a um conector ISE? Também não vejo esse conector na versão 7.4.0 (build 1494)?

R: Ele está no CSDAC autônomo e não no FMC ou no CDO. você precisaria de um pacote CSDAC Ansible para testá-lo.

P: Quando lançada, qual seria a versão CSDAC local?

R: Provavelmente 2.1.0.

P: Uma tela com uma engrenagem que tem API colocada sobre ela foi mostrada. Acho que é CSDAC; o que isso significa?

R: O explorador de API está integrado neste CSDAC, você pode fazer chamadas de API para o CSDAC a partir dessa página.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.