

Analisar uma implantação de firewall segura no MCD

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Produtos Relacionados](#)

[Informações de Apoio](#)

[Monitorando a implantação](#)

[Verificar](#)

[Troubleshooting](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve como monitorar uma implantação do Multicloud Defense usando os logs de sistema disponíveis para validar o andamento da implantação.

Pré-requisitos

Isso é para ambientes de nuvem, como AWS, Azure, GCP ou Oracle, para permitir a integração perfeita no conector de nuvem seguro e no Firepower Management Center implantado na nuvem (cdFMC)

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Fluxos de trabalho de implantação de Defesa em várias nuvens (MCD)
- Conceitos de rede em nuvem e conectividade do conector de nuvem seguro (SCC)
- Monitoramento e validação de integridade do FMC para implantações de nuvem

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

- Defesa em várias nuvens
- Ambiente AWS
- Firepower Management Center implantado em nuvem (cdFMC)
- Conector de nuvem seguro (SCC)

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.

Produtos Relacionados

Este documento também pode ser usado com as seguintes versões de hardware e software:

- Defesa em várias nuvens
- Conector de nuvem seguro (SCC)
- Firepower Management Center implantado em nuvem (cdFMC)

Informações de Apoio

Ao implantar um dispositivo em uma plataforma de nuvem usando o MCD, há vários lugares a serem analisados para garantir que a implantação esteja progredindo corretamente. Essas ferramentas ajudam a monitorar a implantação e fornecem contexto adicional quando ocorre um erro. Os mesmos princípios de monitoramento se aplicam às implantações AWS, Azure e GCP.

Os registros do sistema são a principal fonte de visibilidade de implantação no MCD. Este é o melhor local para revisar eventos de criação de cluster, atividade de criação de gateway, inicializações de instância e quaisquer exceções encontradas durante o fluxo de trabalho de implantação. O CVP também emite alertas quando um registro ou uma fase de implantação falha, o que ajuda a restringir a área a ser investigada.



Tip: Se ocorrer um tempo limite de registro, verifique os registros do sistema MCD antes de solucionar o problema do ambiente em si. Os registros frequentemente identificam a etapa que falhou.

Monitorando a implantação

Revise os Logs do sistema no MCD para confirmar se a implantação está progredindo pelos estágios esperados. Esse é o primeiro e mais útil local para verificar o status da implantação, a criação do gateway, a atividade de inicialização da instância e todos os erros registrados.

Navegue até:

Defesa em várias nuvens > Investigar > Logs do sistema

O exemplo mostra a criação bem-sucedida de gateway e onde as instâncias de cluster estão sendo inicializadas. Nesse caso, as instâncias de gateway são hospedadas na região US-east-2 e na zona de disponibilidade us-east-2b.

AWS-CXLABS-RTP-FW	mcd-lab-cluster	Info	FTDv instance i-0bdd9ff657...
AWS-CXLABS-RTP-FW	mcd-lab-cluster	Info	Gateway Enabled for Gateway mcd-lab-cluster. Newly created instances in this gateway are 1 in region us-east-2 availability zone us-east-2b
AWS-CXLABS-RTP-FW	mcd-lab-cluster	Info	
AWS-CXLABS-RTP-FW	mcd-lab-cluster	Info	
AWS-CXLABS-RTP-FW	mcd-lab-cluster	Info	Gateway Enabled for Gatew...

Use a página Logs do sistema para verificar se a implantação está se movendo pelo ciclo esperado e para coletar mensagens de erro detalhadas quando uma etapa falhar.

Verifique se há erros de implantação no FMC quando um evento de tempo limite de registro ou de implantação com falha for relatado. O FMC pode fornecer um alerta de alto nível que indica que a implantação não foi concluída com êxito.

As verificações recomendadas incluem:

1. Verifique a conectividade entre a rede de nuvem e o conector de nuvem seguro (SCC).
2. Confirme se cada etapa de implantação no guia de implantação foi concluída.
3. Valide se a função IAM correta está configurada e em uso.

 Register Registration ciscoecd-mcd-lab-cluster-gcrpxvxq: Established secure connection	27s
 Register Registration ciscoecd-mcd-lab-cluster-gcrpxvxq: Registration timed out. Please check connectivity and registration id	2m 6s 
 Register Registration ciscoecd-mcd-lab-cluster-dfmnhqfi: Established secure connection	2m 32s



Caution: Uma falha de registro pode ocorrer uma ou mais vezes antes da conclusão de um registro bem-sucedido. Esse comportamento pode ser causado pelo comportamento do temporizador da nuvem e não é necessariamente um problema permanente.

Se o FMC no SCC relatar um tempo limite de registro, os registros do sistema geralmente incluirão mais detalhes sobre a falha específica. Na maioria dos casos, o problema é uma combinação de problemas de conectividade, IAM ou configuração, e os registros são a melhor fonte para restringir a etapa com falha.

Confirme se a implantação foi concluída com êxito, revisando o evento final de êxito nos Logs do sistema MCD. Quando a implantação for bem-sucedida, os logs poderão mostrar um evento de conclusão bem-sucedida.

System Logs

UTC
Local
Refresh

Quick Filters
Advanced

Last 1 Hour

CSP Account	Gateway	Severity	Sub Type	Message
AWS-CXLABS-RTP-FW	mcd-lab-cluster	Info		FTDv instance i-0e880723d9ce7772f policy deployment is done with Multicloud defense configurations. Marking as health_check pending
AWS-CXLABS-RTP-FW	mcd-lab-cluster	Info		FTDv instance i-0e880723d...

Uma implantação bem-sucedida também pode ser visível no FMC, onde os dispositivos implantados mostram um status conectado e os indicadores de integridade aparecem verdes.

Device Management

New device management UI

Migrate

Deployment history

Add

Devices

3

Normal 3

Q Type to search

☆

Total: 3

Name	Version	Model	
▼ mcd-lab-cluster 2			
ciscomcd-mcd-lab-cluster-dfmnhqfi N/A - ROUTED	10.0.0	Firewall Threat Defense for AWS	
ciscomcd-mcd-lab-cluster-gcrpxvxq N/A - ROUTED	10.0.0	Firewall Threat Defense for AWS	

Isso confirma que o cluster foi criado com êxito e que o dispositivo está operando no ambiente esperado.

Verificar

Há alguns locais para verificar se a implantação do AWS está íntegra:

- Os registros do sistema mostram atividades normais de implantação e nenhum erro de bloqueio.
- O dispositivo ou gateway é criado na região e na zona de disponibilidade esperadas.
- O FMC informa o dispositivo como conectado e íntegro.
- Nenhum tempo limite de registro ou avisos de falha de implantação permanecem nos logs.

Quando todas essas condições forem verdadeiras, a implantação do MCD poderá ser considerada bem-sucedida.

Troubleshooting

Se a implantação não atingir um estado íntegro:

- Verifique os registros do sistema MCD para saber a etapa exata que falhou.
- Verificar se há alertas de registro ou conectividade no FMC.
- Confirme a rede em nuvem e a conectividade do conector de nuvem seguro.
- Valide a função do IAM e todos os pré-requisitos do guia de implantação.
- Confirme se o cluster está sendo implantado na região e na zona de disponibilidade esperadas.

Informações Relacionadas

- [Guia de arquitetura de defesa em várias nuvens da Cisco](#)
- [White paper sobre a defesa em várias nuvens da Cisco](#)
- [Manual do usuário do Cisco Multicloud Defense: Registros de sistema](#)

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.