

Analyser un déploiement de pare-feu sécurisé sur MCD

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Produits associés](#)

[Informations générales](#)

[Surveillance du déploiement](#)

[Vérifier](#)

[Dépannage](#)

[Informations connexes](#)

Introduction

Ce document décrit comment surveiller un déploiement de défense multicloud à l'aide des journaux système disponibles pour valider que le déploiement progresse.

Conditions préalables

Cette solution est destinée aux environnements cloud tels qu'AWS, Azure, GCP ou Oracle pour permettre une intégration transparente dans le connecteur cloud sécurisé et le centre de gestion Firepower déployé dans le cloud (cdFMC)

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Workflows de déploiement MCD (Multicloud Defense)
- Concepts de connectivité du réseau cloud et du connecteur cloud sécurisé (SCC)
- Surveillance FMC et validation de l'état pour les déploiements cloud

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions logicielles suivantes :

- Défense multicloud
- Environnement AWS
- Centre de gestion Firepower déployé dans le cloud (cdFMC)
- Connecteur cloud sécurisé (SCC)

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Produits associés

Ce document peut également être utilisé avec les versions matérielles et logicielles suivantes :

- Défense multicloud
- Connecteur cloud sécurisé (SCC)
- Centre de gestion Firepower déployé dans le cloud (cdFMC)

Informations générales

Lors du déploiement d'un périphérique sur une plate-forme cloud à l'aide de MCD, plusieurs points doivent être examinés afin de s'assurer que le déploiement progresse correctement. Ces outils permettent de surveiller le déploiement et fournissent un contexte supplémentaire en cas d'erreur. Les mêmes principes de surveillance s'appliquent aux déploiements AWS, Azure et GCP.

Les journaux système sont la principale source de visibilité du déploiement dans MCD. Il s'agit du meilleur endroit pour consulter les événements de création de cluster, l'activité de création de passerelle, les lancements d'instance et toutes les exceptions rencontrées au cours du workflow de déploiement. Le FMC déclenche également des alertes lorsqu'une étape d'enregistrement ou de déploiement échoue, ce qui permet de réduire la zone à examiner.



Conseil : Si un délai d'enregistrement expire, vérifiez les journaux système MCD avant de dépanner l'environnement lui-même. Les journaux identifient souvent l'étape ayant échoué.

Surveillance du déploiement

Vérifiez les journaux système dans MCD pour vous assurer que le déploiement progresse à travers les étapes prévues. Il s'agit du premier endroit utile pour vérifier l'état du déploiement, la création de la passerelle, l'activité de lancement de l'instance et toutes les erreurs enregistrées.

Naviguez jusqu'à l'adresse :

Défense multicloud > Enquêter > Journaux système

L'exemple illustre la création réussie d'une passerelle et l'emplacement de lancement des instances de cluster. Dans ce cas, les instances de passerelle sont hébergées dans la région US-east-2 et la zone de disponibilité 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...

Utilisez la page System Logs pour vérifier que le déploiement suit le cycle prévu et pour collecter des messages d'erreur détaillés en cas d'échec d'une étape.

Recherchez les erreurs de déploiement dans le FMC lorsqu'un événement de délai d'enregistrement ou d'échec de déploiement est signalé. Le FMC peut fournir une alerte de haut niveau qui indique que le déploiement ne s'est pas terminé correctement.

Les vérifications recommandées sont les suivantes :

1. Vérifiez la connectivité entre le réseau cloud et le connecteur cloud sécurisé (SCC).
2. Vérifiez que chaque étape de déploiement du guide de déploiement est terminée.
3. Vérifiez que le rôle IAM correct est configuré et utilisé.

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



Mise en garde : Un échec d'enregistrement peut se produire une ou plusieurs fois avant la fin de l'enregistrement. Ce comportement peut être provoqué par le comportement du minuteur cloud et n'est pas nécessairement un problème permanent.

Si le FMC du SCC signale un dépassement du délai d'enregistrement, les journaux système incluent généralement plus de détails sur la défaillance spécifique. Dans la plupart des cas, il s'agit d'une combinaison de problèmes de connectivité, de gestion de l'information ou de configuration, et les journaux sont la meilleure source pour limiter l'étape ayant échoué.

Vérifiez que le déploiement s'est terminé correctement en consultant l'événement de réussite final dans les journaux système MCD. Lorsque le déploiement réussit, les journaux peuvent afficher un événement d'achèvement réussi.

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...

Un déploiement réussi peut également être visible dans le FMC, où les périphériques déployés affichent un état connecté et les indicateurs d'état apparaissent en vert.

Device Management			
Devices		New device management UI ☒ Migrate Deployment history Add	
3 Normal 3			
Q Type to search		☆ Total: 3	⬆️ ⬇️ ⬇️
☐ Name	Version	Model	
☐ ▼ mcd-lab-cluster 2			
☐ ● cisco-mcd-mcd-lab-cluster-dfmnhqfi N/A - ROUTED	10.0.0	Firewall Threat Defense for AWS	
☐ ● cisco-mcd-mcd-lab-cluster-gcrpxvxq N/A - ROUTED	10.0.0	Firewall Threat Defense for AWS	

Cela confirme que le cluster a été créé avec succès et que le périphérique fonctionne dans l'environnement attendu.

Vérifier

Il existe des endroits à vérifier pour vérifier que le déploiement AWS est sain :

- Les journaux système indiquent une activité de déploiement normale et aucune erreur de blocage.
- Le périphérique ou la passerelle est créé dans la région et la zone de disponibilité attendues.
- Le FMC indique que le périphérique est connecté et en bon état.
- Aucun délai d'enregistrement ou avertissement d'échec de déploiement ne reste dans les journaux.

Lorsque toutes ces conditions sont remplies, le déploiement MCD peut être considéré comme réussi.

Dépannage

Si le déploiement n'atteint pas un état sain :

- Consultez les journaux système MCD pour connaître l'étape exacte qui a échoué.
- Consultez le FMC pour les alertes d'inscription ou de connectivité.
- Vérifiez la connectivité du réseau cloud et du connecteur cloud sécurisé.
- Validez le rôle IAM et toutes les conditions préalables du guide de déploiement.
- Vérifiez que le cluster est déployé dans la région et la zone de disponibilité attendues.

Informations connexes

- [Guide d'architecture de défense multicloud Cisco](#)
- [Livre blanc sur la défense multicloud Cisco](#)
- [Guide de l'utilisateur de Cisco Multicloud Defense : Journaux du système](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.