

Een beveiligde firewallimplementatie op MCD analyseren

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Verwante producten](#)

[Achtergrondinformatie](#)

[Monitoring van de implementatie](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Gerelateerde informatie](#)

Inleiding

In dit document wordt beschreven hoe u een Multicloud Defense-implementatie kunt bewaken met behulp van de beschikbare systeemlogboeken om te bevestigen dat de implementatie vordert.

Voorwaarden

Dit is voor cloudomgevingen zoals AWS, Azure, GCP of Oracle om naadloze integratie in de Secure Cloud Connector en Cloud Deployed Firepower Management Center (cdFMC) mogelijk te maken

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Implementatieworkflows voor Multicloud Defense (MCD)
- Concepten voor cloudnetwerk en Secure Cloud Connector (SCC)-connectiviteit
- FMC-bewaking en gezondheidsvalidatie voor cloudimplementaties

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende softwareversies:

- multicloud-verdediging
- AWS-omgeving
- Cloud Deployed Firepower Management Center (cdFMC)
- Secure Cloud Connector (SCC)

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Verwante producten

Dit document kan ook worden gebruikt voor de volgende hardware- en softwareversies:

- multicloud-verdediging
- Secure Cloud Connector (SCC)
- Cloud Deployed Firepower Management Center (cdFMC)

Achtergrondinformatie

Bij het implementeren van een apparaat in een cloudplatform met behulp van MCD, zijn er meerdere plaatsen om te controleren of de implementatie correct verloopt. Deze tools helpen de implementatie te bewaken en bieden extra context wanneer zich een fout voordoet. Dezelfde monitoringprincipes zijn van toepassing op AWS-, Azure- en GCP-implementaties.

Systeemlogboeken zijn de belangrijkste bron van zichtbaarheid van implementatie in MCD. Dit is de beste plaats om gebeurtenissen voor het maken van clusters, activiteiten voor het maken van gateways, instantielancerings en eventuele uitzonderingen tijdens de implementatieworkflow te bekijken. Het VCC waarschuwt ook wanneer een registratie- of implementatiestap mislukt, waardoor het te onderzoeken gebied wordt verkleind.



Tip: Als er een time-out voor de registratie optreedt, controleert u de MCD-systeemlogboeken voordat u het probleem met de omgeving zelf oplost. De logs identificeren vaak de mislukte stap.

Monitoring van de implementatie

Controleer de systeemlogboeken in MCD om te bevestigen dat de implementatie de verwachte fasen doorloopt. Dit is de eerste en meest nuttige plaats om te controleren op de implementatiestatus, het maken van gateways, de activiteiten voor het starten van instanties en eventuele geregistreerde fouten.

Navigeer naar:

Multicloud Defense > Onderzoeken > Systeemlogboeken

Het voorbeeld toont de succesvolle gateway-creatie en waar de clusterinstanties worden gestart. In dit geval worden de gateway-instanties gehost in de US-East-2-regio en de US-East-2b-beschikbaarheidszone.

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 Gateway...

Gebruik de pagina Systeemlogboeken om te controleren of de implementatie de verwachte cyclus doorloopt en om gedetailleerde foutmeldingen te verzamelen wanneer een stap mislukt.

Controleer het VCC op implementatiefouten wanneer een time-out voor registratie of een mislukte implementatie wordt gemeld. Het VCC kan een waarschuwing op hoog niveau geven dat aangeeft dat de implementatie niet met succes is voltooid.

Aanbevolen controles zijn onder meer:

1. Controleer de connectiviteit tussen het cloudnetwerk en de Secure Cloud Connector (SCC).
2. Bevestig dat elke implementatiestap in de implementatiegids is voltooid.
3. Valideren dat de juiste IAM-rol is geconfigureerd en in gebruik is.

 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



Let op: een registratiefout kan een of meerdere keren optreden voordat een succesvolle registratie is voltooid. Dit gedrag kan worden veroorzaakt door het gedrag van de cloudtimer en is niet noodzakelijk een permanent probleem.

Als de FMC in het SCC een time-out voor de registratie meldt, bevatten de systeemlogboeken meestal meer details over de specifieke storing. In de meeste gevallen is het probleem een combinatie van connectiviteits-, IAM- of configuratieproblemen en de logs zijn de beste bron voor het verkleinen van de mislukte stap.

Bevestig dat de implementatie met succes is voltooid door de laatste succesgebeurtenis in de MCD-systeemlogboeken te bekijken. Wanneer de implementatie slaagt, kunnen de logs een succesvolle voltooiingsgebeurtenis weergeven.

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		
AWS-CXLABS-RTP-FW	mcd-lab-cluster	Info		FTDv instance i-0e880723d...

Een succesvolle implementatie kan ook zichtbaar zijn in het FMC, waar de geïmplementeerde apparaten een aangesloten status tonen en de gezondheidsindicatoren groen verschijnen.

Device Management			
Devices		New device management UI ☐ Migrate Deployment history Add	
3 Normal 3			
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	⌵

Dit bevestigt dat het cluster met succes is gemaakt en dat het apparaat in de verwachte omgeving werkt.

Verifiëren

Er zijn enkele plaatsen om te controleren of de AWS-implementatie gezond is:

- De systeemlogboeken tonen normale implementatieactiviteit en geen blokkeringsfouten.
- Het apparaat of de gateway wordt gemaakt in de verwachte regio en beschikbaarheidszone.
- Het FMC meldt het apparaat als verbonden en gezond.
- Er blijven geen time-out voor registratie of waarschuwingen voor mislukte implementatie in de logboeken.

Wanneer al deze voorwaarden juist zijn, kan de MCD-implementatie als succesvol worden beschouwd.

Problemen oplossen

Als de inzet niet tot een gezonde staat leidt:

- Controleer de MCD-systeemlogboeken voor de exacte stap die is mislukt.
- Controleer de FMC voor registratie- of connectiviteitswaarschuwingen.
- Bevestig het cloudnetwerk en de Secure Cloud Connector-connectiviteit.
- Valideer de IAM-rol en alle vereisten uit de implementatiegids.
- Bevestig dat het cluster wordt geïmplementeerd in de verwachte regio en beschikbaarheidszone.

Gerelateerde informatie

- [Cisco Multicloud Defense Architecture Guide](#)
- [Cisco Multicloud Defense-witboek](#)
- [Cisco Multicloud Defense-gebruikershandleiding: systeemlogboeken](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.