

Analyse einer sicheren Firewall-Bereitstellung auf MCD

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Verwandte Produkte](#)

[Hintergrundinformationen](#)

[Überwachen der Bereitstellung](#)

[Überprüfung](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird beschrieben, wie eine Multicloud Defense-Bereitstellung mithilfe der verfügbaren Systemprotokolle überwacht wird, um zu überprüfen, ob die Bereitstellung weiter voranschreitet.

Voraussetzungen

Dies gilt für Cloud-Umgebungen wie AWS, Azure, GCP oder Oracle, um eine nahtlose Integration in Secure Cloud Connector und Cloud Deployed FirePOWER Management Center (cdFMC) zu ermöglichen.

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Multicloud Defense (MCD)-Bereitstellungs-Workflows
- Konzepte für Cloud-Netzwerke und Secure Cloud Connector (SCC)-Verbindungen
- FMC-Überwachung und Integritätsvalidierung für Cloud-Bereitstellungen

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf folgenden Software-Versionen:

- Multicloud-Schutz
- AWS-Umgebung
- Cloud-basiertes FirePOWER Management Center (cdFMC)
- Secure Cloud Connector (SCC)

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Verwandte Produkte

Dieses Dokument kann auch mit folgenden Hardware- und Softwareversionen verwendet werden:

- Multicloud-Schutz
- Secure Cloud Connector (SCC)
- Cloud-basiertes FirePOWER Management Center (cdFMC)

Hintergrundinformationen

Wenn Sie ein Gerät mithilfe von MCD in einer Cloud-Plattform bereitstellen, müssen Sie mehrere Stellen überprüfen, um sicherzustellen, dass die Bereitstellung ordnungsgemäß verläuft. Diese Tools unterstützen Sie bei der Überwachung der Bereitstellung und bieten zusätzlichen Kontext, wenn ein Fehler auftritt. Dieselben Überwachungsgrundsätze gelten für AWS-, Azure- und GCP-Bereitstellungen.

Systemprotokolle sind die wichtigste Quelle für die Bereitstellungstransparenz bei MCD. Dies ist der beste Ort, um Cluster-Erstellungsereignisse, Gateway-Erstellungsaktivitäten, Instanzstarts und alle Ausnahmen zu überprüfen, die während des Bereitstellungs-Workflows aufgetreten sind. Das FMC gibt auch Warnungen aus, wenn ein Registrierungs- oder Bereitstellungsschritt fehlschlägt, wodurch der Untersuchungsbereich eingegrenzt werden kann.



Tipp: Wenn bei der Registrierung ein Timeout auftritt, überprüfen Sie die MCD-Systemprotokolle, bevor Sie die Umgebung selbst reparieren. Die Protokolle identifizieren

häufig den fehlgeschlagenen Schritt.

Überwachen der Bereitstellung

Überprüfen Sie die Systemprotokolle in MCD, um zu bestätigen, dass die Bereitstellung die erwarteten Schritte durchläuft. Dies ist der erste und hilfreichste Ort, um den Bereitstellungsstatus, die Gateway-Erstellung, die Aktivität zum Starten von Instanzen und aufgezeichnete Fehler zu überprüfen.

Navigieren Sie zu:

Multicloud-Schutz > Untersuchen > Systemprotokolle

Das Beispiel zeigt die erfolgreiche Gateway-Erstellung und den Ort, an dem die Cluster-Instanzen gestartet werden. In diesem Fall werden die Gateway-Instanzen in der Ost-2-Region (USA) und der Verfügbarkeitszone (US-Ost-2b) gehostet.

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	
			Gateway Enabled for Gatew...

Auf der Seite "System Logs" (Systemprotokolle) können Sie überprüfen, ob die Bereitstellung den erwarteten Zyklus durchläuft, und detaillierte Fehlermeldungen sammeln, wenn ein Schritt fehlschlägt.

Überprüfen Sie das FMC auf Bereitstellungsfehler, wenn ein Registrierungstimeout oder ein fehlgeschlagenes Bereitstellungsereignis gemeldet wird. Das FMC kann eine allgemeine Warnung ausgeben, die besagt, dass die Bereitstellung nicht erfolgreich abgeschlossen wurde.

Folgende Prüfungen werden empfohlen:

1. Überprüfen der Verbindung zwischen dem Cloud-Netzwerk und dem Secure Cloud Connector (SCC)
2. Bestätigen Sie, dass alle Bereitstellungsschritte im Bereitstellungsleitfaden abgeschlossen wurden.
3. Überprüfen Sie, ob die richtige IAM-Rolle konfiguriert ist und gerade verwendet wird.

 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



Vorsicht: Ein Registrierungsfehler kann ein- oder mehrmals auftreten, bevor die Registrierung erfolgreich abgeschlossen wird. Dieses Verhalten kann durch das Verhalten von Cloud-Timern verursacht werden und ist nicht unbedingt ein dauerhaftes Problem.

Wenn das FMC im SCC einen Registrierungstimeout meldet, enthalten die Systemprotokolle in der Regel weitere Details zu dem jeweiligen Fehler. In den meisten Fällen handelt es sich um eine Kombination aus Verbindungs-, IAM- oder Konfigurationsproblemen, und die Protokolle sind die beste Quelle zur Eingrenzung des fehlgeschlagenen Schritts.

Bestätigen Sie, dass die Bereitstellung erfolgreich abgeschlossen wurde, indem Sie das endgültige Erfolgsereignis in den MCD-Systemprotokollen überprüfen. Wenn die Bereitstellung erfolgreich abgeschlossen wurde, können die Protokolle ein Ereignis für den erfolgreichen Abschluss anzeigen.

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...			

Eine erfolgreiche Bereitstellung kann auch im FMC angezeigt werden, wo die bereitgestellten Geräte einen Verbindungsstatus anzeigen und die Statusanzeigen grün leuchten.

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			
☐ ✓ cisco-mcd-lab-cluster-dfmmhqi N/A - ROUTED	10.0.0	Firewall Threat Defense for AWS	
☐ ✓ cisco-mcd-lab-cluster-gcrpxvq N/A - ROUTED	10.0.0	Firewall Threat Defense for AWS	

Dadurch wird bestätigt, dass der Cluster erfolgreich erstellt wurde und das Gerät in der erwarteten Umgebung arbeitet.

Überprüfung

Es gibt einige Stellen, an denen Sie überprüfen können, ob die AWS-Bereitstellung fehlerfrei ist:

- Die Systemprotokolle zeigen normale Bereitstellungsaktivitäten und keine Blockierungsfehler an.
- Das Gerät oder Gateway wird in der erwarteten Region und Verfügbarkeitszone erstellt.
- Das FMC meldet das Gerät als verbunden und inaktiv.
- Es verbleiben keine Timeouts für die Registrierung oder fehlerhafte Bereitstellungswarnungen in den Protokollen.

Wenn alle diese Bedingungen zutreffen, kann die MCD-Bereitstellung als erfolgreich angesehen werden.

Fehlerbehebung

Wenn die Bereitstellung keinen fehlerfreien Zustand erreicht:

- Überprüfen Sie die MCD-Systemprotokolle auf den genauen Schritt, der fehlgeschlagen ist.
- FMC auf Registrierungs- oder Verbindungswarnungen überprüfen
- Bestätigen Sie das Cloud-Netzwerk und die Verbindung mit Secure Cloud Connector.
- Validieren Sie die IAM-Rolle und alle Voraussetzungen aus dem Bereitstellungsleitfaden.
- Bestätigen Sie, dass der Cluster in der erwarteten Region und Verfügbarkeitszone bereitgestellt wird.

Zugehörige Informationen

- [Cisco Multicloud Defense - Architekturleitfaden](#)
- [Cisco Multicloud Defense - Whitepaper](#)
- [Cisco Multicloud Defense Benutzerhandbuch: Systemprotokolle](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.