

Analisi di una distribuzione sicura del firewall su MCD

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Prodotti correlati](#)

[Premesse](#)

[Monitoraggio della distribuzione](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come monitorare una distribuzione di Multicast Defense utilizzando i registri di sistema disponibili per convalidare l'avanzamento della distribuzione.

Prerequisiti

Questa funzionalità è destinata agli ambienti cloud, ad esempio AWS, Azure, GCP o Oracle, per consentire l'integrazione completa in Secure Cloud Connector e Cloud Deployed Firepower Management Center (cdFMC)

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Flussi di lavoro di distribuzione di Multicast Defense (MCD)
- Nozioni di connettività rete cloud e Secure Cloud Connector (SCC)
- Monitoraggio FMC e convalida dell'integrità per installazioni cloud

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software:

- Multicast Defense
- Ambiente AWS
- CdFMC (Cloud Deployed Firepower Management Center)
- SCC (Secure Cloud Connector)

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Prodotti correlati

Il presente documento può essere utilizzato anche per le seguenti versioni hardware e software:

- Multicast Defense
- SCC (Secure Cloud Connector)
- CdFMC (Cloud Deployed Firepower Management Center)

Premesse

Quando si distribuisce un dispositivo in una piattaforma cloud utilizzando MCD, è necessario controllare più punti per verificare che la distribuzione avvenga correttamente. Questi strumenti consentono di monitorare la distribuzione e di fornire contesto aggiuntivo quando si verifica un errore. Gli stessi principi di monitoraggio si applicano alle distribuzioni AWS, Azure e GCP.

I registri di sistema sono la principale fonte di visibilità della distribuzione in MCD. Questa è la posizione migliore per esaminare gli eventi di creazione del cluster, l'attività di creazione del gateway, gli avvisi dell'istanza e le eventuali eccezioni rilevate durante il flusso di lavoro di distribuzione. Il CCP emette inoltre avvisi quando una fase di registrazione o installazione non riesce, il che consente di restringere l'area da analizzare.



Suggerimento: Se si verifica un timeout durante la registrazione, controllare i registri di sistema MCD prima di risolvere i problemi dell'ambiente stesso. I registri spesso identificano il passaggio non riuscito.

Monitoraggio della distribuzione

Esaminare i registri di sistema in MCD per verificare che la distribuzione stia procedendo nelle fasi previste. Questa è la prima e più utile posizione in cui verificare lo stato della distribuzione, la creazione del gateway, l'attività di avvio dell'istanza e gli eventuali errori registrati.

Accedere a:

Difesa di Multicast > Analizza > Registri di sistema

Nell'esempio viene illustrata la creazione del gateway e la posizione in cui vengono avviate le istanze del cluster. In questo caso, le istanze del gateway sono ospitate nella regione US-East-2 e nella zona di disponibilità 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...

Utilizzare la pagina Log di sistema per verificare che la distribuzione si stia spostando nel ciclo previsto e per raccogliere messaggi di errore dettagliati quando un passo non riesce.

Verificare la presenza di errori di distribuzione nel FMC quando viene segnalato un timeout di registrazione o un evento di distribuzione non riuscita. Il CCP può fornire un avviso di alto livello che indica che la distribuzione non è stata completata correttamente.

I controlli consigliati includono:

1. Verificare la connettività tra la rete cloud e Secure Cloud Connector (SCC).
2. Confermare il completamento di ogni fase di distribuzione nella guida alla distribuzione.
3. Verificare che sia configurato e in uso il ruolo IAM corretto.

 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



Attenzione: Un errore di registrazione può verificarsi una o più volte prima del completamento della registrazione. Questo comportamento può essere causato dal comportamento del timer del cloud e non è necessariamente un problema permanente.

Se il CCP segnala un timeout di registrazione, i registri di sistema solitamente includono maggiori dettagli sull'errore specifico. Nella maggior parte dei casi, il problema è dovuto a una combinazione di problemi di connettività, IAM o configurazione e i registri rappresentano la migliore fonte per restringere il passaggio non riuscito.

Confermare il completamento della distribuzione esaminando l'evento finale nei registri di sistema MCD. Se la distribuzione ha esito positivo, nei registri può essere visualizzato un evento di completamento corretto.

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...			

Una distribuzione corretta può essere visibile anche nel CCP, dove i dispositivi distribuiti mostrano uno stato connesso e gli indicatori di stato appaiono verdi.

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-lab-cluster-dfmnhqfi N/A - ROUTED	10.0.0	Firewall Threat Defense for AWS	
☐ ● cisco-mcd-lab-cluster-gcrpxvxq N/A - ROUTED	10.0.0	Firewall Threat Defense for AWS	

Ciò conferma che il cluster è stato creato correttamente e che il dispositivo funziona nell'ambiente previsto.

Verifica

Per verificare che la distribuzione di AWS sia integra, è necessario controllare alcune posizioni:

- I registri di sistema mostrano la normale attività di distribuzione e nessun errore di blocco.
- La periferica o il gateway è stato creato nella zona prevista e nella zona di disponibilità.
- Il FMC segnala il dispositivo come connesso e integro.
- Nei log non rimangono timeout di registrazione o avvisi di distribuzione non riusciti.

Se tutte queste condizioni sono vere, la distribuzione di MCD può essere considerata riuscita.

Risoluzione dei problemi

Se la distribuzione non raggiunge uno stato integro:

- Esaminare i registri di sistema MCD per individuare la fase non riuscita.
- Controllare gli avvisi relativi alla registrazione o alla connettività nel CCP.
- Confermare la rete cloud e la connettività Secure Cloud Connector.
- Convalidare il ruolo IAM e tutti i prerequisiti dalla guida alla distribuzione.
- Confermare la distribuzione del cluster nella zona prevista e nella zona di disponibilità.

Informazioni correlate

- [Guida all'architettura di difesa multicolore Cisco](#)

- [White paper su Cisco Multicast Defense](#)
- [Guida per l'utente di Cisco Multicast Defense: Log di sistema](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).