

MCD의 보안 방화벽 구축 분석

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[관련 제품](#)

[배경 정보](#)

[구축 모니터링](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[관련 정보](#)

소개

이 문서에서는 사용 가능한 시스템 로그를 사용하여 Multicholoud Defense 구축을 모니터링하여 구축이 진행 중인지 확인하는 방법에 대해 설명합니다.

사전 요구 사항

이는 AWS, Azure, GCP 또는 Oracle과 같은 클라우드 환경에서 Secure Cloud Connector 및 CDFMC(Cloud Deployed Firepower Management Center)와의 원활한 통합을 지원하기 위한 것입니다.

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- MCD(Multicoloud Defense) 구축 워크플로
- 클라우드 네트워크 및 SCC(Secure Cloud Connector) 연결 개념
- 클라우드 구축을 위한 FMC 모니터링 및 상태 검증

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

- 멀티 클라우드 방어
- AWS 환경
- 클라우드 구축 Firepower 관리 센터(cdFMC)
- SCC(Secure Cloud Connector)

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

관련 제품

이 문서는 다음 하드웨어 및 소프트웨어 버전에서도 사용할 수 있습니다.

- 멀티 클라우드 방어
- SCC(Secure Cloud Connector)
- 클라우드 구축 Firepower 관리 센터(cdFMC)

배경 정보

MCD를 사용하여 클라우드 플랫폼에 디바이스를 구축할 경우 구축이 올바르게 진행되는지 여러 곳에서 검토할 수 있습니다. 이러한 툴은 구축을 모니터링하고 오류 발생 시 추가 상황을 제공하는 데 도움이 됩니다. AWS, Azure 및 GCP 배포에도 동일한 모니터링 원칙이 적용됩니다.

시스템 로그는 MCD에서 구축 가시성의 기본 소스입니다. 클러스터 생성 이벤트, 게이트웨이 생성 활동, 인스턴스 시작 및 구축 워크플로 중에 발생한 모든 예외를 검토할 수 있는 최적의 위치입니다. 또한 FMC는 등록 또는 구축 단계가 실패할 경우 알림을 발생시켜 조사 영역을 좁히는 데 도움이 됩니다.



팁: 등록 시간 초과가 발생하면 환경 자체의 문제를 해결하기 전에 MCD 시스템 로그를 확인하십시오. 로그에서는 실패한 단계를 확인하는 경우가 많습니다.

구축 모니터링

MCD의 시스템 로그를 검토하여 예상 단계를 통해 구축이 진행되고 있는지 확인합니다. 구축 상태, 게이트웨이 생성, 인스턴스 실행 활동 및 기록된 오류를 확인하는 가장 유용하고 첫 번째 장소입니다.

다.

다음으로 이동합니다.

Multicloud Defense > Investigate > System Logs

이 예에서는 성공적인 게이트웨이 생성 및 클러스터 인스턴스가 시작되는 위치를 보여 줍니다. 이 경우 게이트웨이 인스턴스는 US-east-2 지역 및 us-east-2b 가용 영역에서 호스팅됩니다.

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	

[시스템 로그] 페이지에서는 구축이 예상 주기를 따라 이동하고 있는지 확인하고 단계가 실패할 경우 자세한 오류 메시지를 수집할 수 있습니다.

등록 시간 초과 또는 실패한 구축 이벤트가 보고될 때 FMC에서 구축 오류를 확인합니다. FMC는 구축이 성공적으로 완료되지 않았음을 나타내는 높은 수준의 알림을 제공할 수 있습니다.

권장 검사 항목은 다음과 같습니다.

1. 클라우드 네트워크와 SCC(Secure Cloud Connector) 간의 연결을 확인합니다.
2. 구축 설명서의 각 구축 단계가 완료되었는지 확인합니다.
3. 올바른 IAM 역할이 구성되어 사용 중인지 확인합니다.

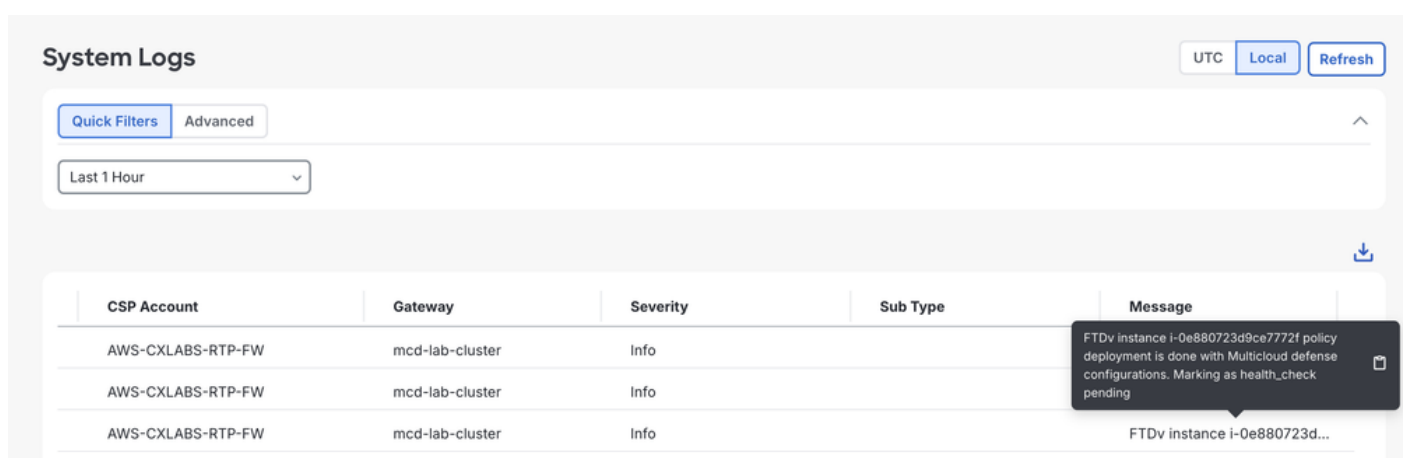
Register	Registration ciscomcd-mcd-lab-cluster-gcrpxvxq: Established secure connection	27s
Register	Registration ciscomcd-mcd-lab-cluster-gcrpxvxq: Registration timed out. Please check connectivity and registration id	2m 6s X
Register	Registration ciscomcd-mcd-lab-cluster-dfmnhqfi: Established secure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



주의: 등록 실패는 등록이 완료되기 전에 한 번 이상 발생할 수 있습니다. 이 동작은 클라우드 타이머 동작으로 인해 발생할 수 있으며 반드시 영구적인 문제는 아닙니다.

SCC의 FMC에서 등록 시간 초과를 보고하는 경우 일반적으로 시스템 로그에 특정 오류에 대한 자세한 내용이 포함됩니다. 대부분의 경우 연결, IAM 또는 컨피그레이션 문제의 조합이 문제이며, 실패한 단계를 좁히는 데 로그는 최적의 소스가 됩니다.

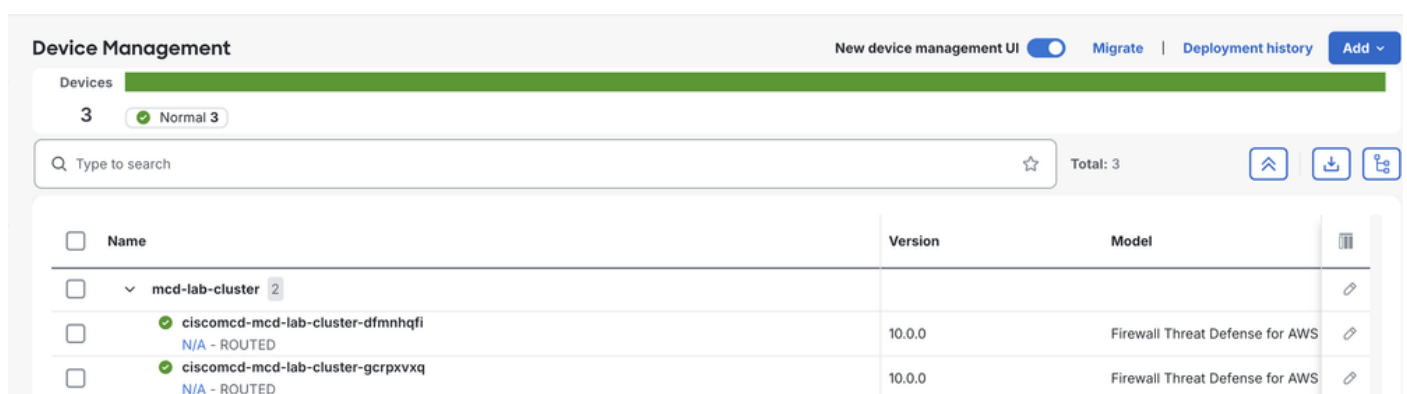
MCD 시스템 로그에서 최종 성공 이벤트를 검토하여 구축이 성공적으로 완료되었는지 확인합니다. 구축이 성공하면 로그에 성공적인 완료 이벤트가 표시될 수 있습니다.



The screenshot shows the 'System Logs' interface. At the top, there are tabs for 'UTC', 'Local', and 'Refresh'. Below these are 'Quick Filters' and 'Advanced' tabs, and a dropdown menu set to 'Last 1 Hour'. A table displays log entries with the following columns: CSP Account, Gateway, Severity, Sub Type, and Message. The table contains three entries, all with 'Info' severity. A tooltip is visible over the 'Message' column, showing a detailed log message: 'FTDv instance i-0e880723d9ce7772f policy deployment is done with Multicloud defense configurations. Marking as health_check pending'. The message in the table is truncated: 'FTDv instance i-0e880723d...'.

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...
AWS-CXLABS-RTP-FW	mcd-lab-cluster	Info		

성공적인 구축은 구축된 디바이스가 연결된 상태를 표시하고 상태 표시기가 녹색으로 표시되는 FMC에서도 볼 수 있습니다.



The screenshot shows the 'Device Management' interface. At the top, there are tabs for 'New device management UI', 'Migrate', and 'Deployment history', and an 'Add' button. Below these is a 'Devices' section showing '3' devices and a 'Normal 3' status. A search bar is present with the text 'Type to search'. A table displays device information with the following columns: Name, Version, and Model. The table contains three entries, all with '10.0.0' version and 'Firewall Threat Defense for AWS' model. The first entry is expanded, showing a dropdown menu with 'mcd-lab-cluster' and a count of '2'. The other two entries are 'ciscomcd-mcd-lab-cluster-dfmnhqfi' and 'ciscomcd-mcd-lab-cluster-gcrpxvxq', both with 'N/A - ROUTED' status.

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

이렇게 하면 클러스터가 성공적으로 생성되었고 디바이스가 예상 환경에서 작동하고 있음을 확인할 수 있습니다.

다음을 확인합니다.

AWS 구축이 정상적인지 확인하기 위해 몇 가지 확인할 수 있는 곳이 있습니다.

- 시스템 로그에는 정상적인 구축 작업이 표시되며 차단 오류가 없습니다.
- 디바이스 또는 게이트웨이는 예상 영역 및 가용 영역에서 생성됩니다.
- FMC에서 디바이스가 연결되어 있고 정상이라고 보고합니다.
- 등록 시간 초과 또는 실패한 구축 경고가 로그에 남아 있지 않습니다.

이 모든 조건이 참인 경우 MCD 구축이 성공한 것으로 간주할 수 있습니다.

문제 해결

구축이 정상 상태에 도달하지 않는 경우:

- MCD 시스템 로그에서 실패한 정확한 단계를 검토합니다.
- FMC에서 등록 또는 연결 알림을 확인합니다.
- 클라우드 네트워크 및 보안 클라우드 커넥터 연결을 확인합니다.
- 구축 가이드에서 IAM 역할 및 모든 사전 요구 사항을 검증합니다.
- 클러스터가 예상 지역 및 가용 영역으로 구축되고 있는지 확인합니다.

관련 정보

- [Cisco Multicholoud Defense 아키텍처 가이드](#)
- [Cisco Multicloud Defense 백서](#)
- [Cisco Multicholoud Defense 사용 설명서: 시스템 로그](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.