

Firewall Management Center 7.4에서 클러스터 서비스 기능 개선 구성

목차

[소개](#)

[새로운 기능](#)

[사전 요구 사항, 지원되는 플랫폼, 라이선싱](#)

[최소 소프트웨어 및 하드웨어 플랫폼](#)

[사용되는 구성 요소](#)

[CCL 링크 진단](#)

[Cluster Summary\(클러스터 요약\) 페이지의 클러스터 제어 링크 인터페이스 MTU 경고](#)

[문제](#)

[플랫폼당 MTU 크기 권장 사항](#)

[솔루션](#)

[클러스터 라이브 상태의 CCL Ping 테스트](#)

[CCL 연결 확인](#)

[솔루션](#)

[퍼블릭 클라우드용 CCL MTU 크기 추가](#)

[FMC에서 사용 가능한 CLI](#)

[Device/Cluster 탭에서 Device Lina CLI 프롬프트 사용 가능](#)

[FMC에서 클러스터 Lina CLI 실행](#)

[일반적으로 사용되는 CLI가 기본적으로 표시됨](#)

[사전 정의된 클러스터 CLI](#)

[사용 가능한 명령의 수동 입력](#)

[트러블슈팅 생성](#)

[노드 가입 실패 시 자동 문제 해결](#)

[Device\(디바이스\) 및 Cluster\(클러스터\) 탭에서 Trigger\(트리거\) 및 Download\(다운로드\) 버튼 문제 해결](#)

[클러스터 문제 해결의 순서운 생성](#)

[클러스터 문제 해결 생성](#)

[노드\(장치\) 문제 해결 생성](#)

[클러스터 문제 해결 생성 완료 알림](#)

[Q & A](#)

[개정 이력](#)

소개

이 문서에서는 FMC 7.4의 향상된 서비스 기능을 사용하는 방법에 대해 설명합니다

새로운 기능

- CCL(Cluster Control Link) 링크 진단 및 설정이 올바른지 확인하는 지원
- 이제 FMC(Firewall Management Center)에서 클러스터 Lina CLI를 볼 수 있습니다.
- 문제 해결 생성
 - 이제 클러스터의 모든 디바이스에 대해 한 번에 생성할 수 있습니다.
 - 노드가 클러스터에 가입하지 못할 경우 자동으로 생성 문제를 해결합니다.
 - Devices > Cluster/Device 탭에서 생성 및 탐색 문제를 해결합니다.

사전 요구 사항, 지원되는 플랫폼, 라이선싱

최소 소프트웨어 및 하드웨어 플랫폼

애플리케이션 및 최소 버전	관리되는 디바이스	최소 지원 관리되는 디바이스 버전 필요	참고
Secure Firewall 7.4	FTD에서 클러스터링을 지원하는 모든 기능 "트러블슈팅 생성" 개선 사항만 적용되려면 FTD 버전이 7.4 이상이어야 합니다.	<ul style="list-style-type: none"> · FMC 온프레미스 + FMC REST API · 클라우드 기반 FMC 	이는 FMC 기능이므로 FMC 7.4에서 관리할 수 있는 모든 디바이스에 컨피그레이션을 적용할 수 있습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco FMC(Firewall Management Center) 실행 7.4
- 7.4 이상을 실행하는 Cisco Firepower FTD(Threat Defense).

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.

CCL 링크 진단

Cluster Summary(클러스터 요약) 페이지의 클러스터 제어 링크 인터페이스 MTU 경고

문제

- 클러스터링에는 데이터 인터페이스보다 클러스터 제어 링크에 더 높은 MTU가 필요합니다.
- MTU를 충분히 높게 설정하지 않을 때가 많습니다. 그러면 안정성 문제가 발생합니다.
- 노드 전체에서 클러스터 상태를 동기화하려면 CCL MTU가 플랫폼을 기준으로 최대 데이터 인터페이스 MTU보다 100바이트 또는 154바이트 커야 합니다.

$$\text{CCL MTU} = (\text{최대 데이터 인터페이스 MTU}) + 100 | 154$$

예를 들어 FTDv 디바이스의 경우 1700바이트가 최대 데이터 인터페이스 MTU이면 CCL 인터페이스 MTU 값은 1854로 설정됩니다.

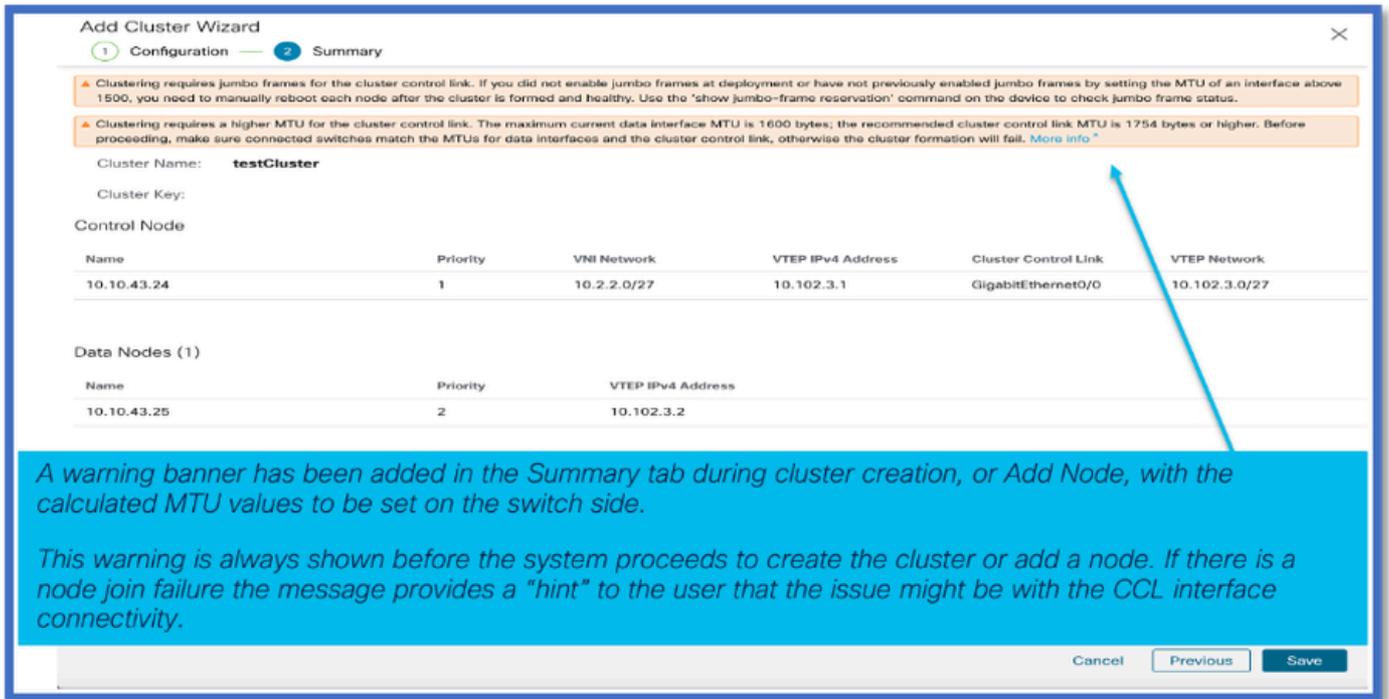
$$1854 = 1700 + 154$$

플랫폼당 MTU 크기 권장 사항

플랫폼	샘플 최대 데이터 인터페이스 MTU	추가	CCL 링크의 MTU에 대한 총 권장 설정
Sec FW 3100 시리즈	1700	100	1800
FTDv	1700	154	1854

솔루션

- 클러스터가 생성되면 CCL 링크의 MTU 값이 인터페이스의 권장 값으로 자동 설정됩니다. 이 값과 일치하도록 스위치측 컨피그레이션을 설정합니다.
- 샘플 경고 메시지:
클러스터링에는 클러스터 제어 링크에 더 높은 MTU가 필요합니다. 최대 현재 데이터 인터페이스 MTU는 1500바이트이며, 권장되는 클러스터 제어 링크 MTU는 1654바이트 이상입니다. 계속하기 전에 연결된 스위치가 데이터 인터페이스 및 클러스터 제어 링크의 MTU와 일치하는지 확인하십시오. 일치하지 않으면 클러스터 형성이 실패합니다.
- CCL 인터페이스에 대한 스위치측 컨피그레이션이 이 값과 일치하지 않으면 디바이스가 클러스터에 조인하지 못합니다.

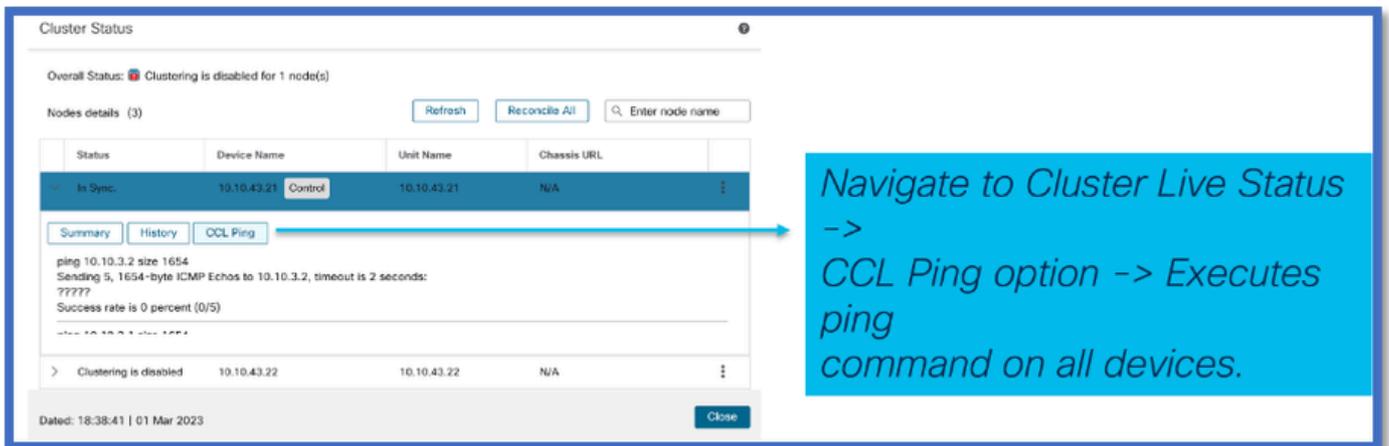


클러스터 라이브 상태의 CCL Ping 테스트

CCL 연결 확인

- CCL MTU 패킷 크기로 CCL 연결을 확인하기 위해 사용자 프로비저닝이 필요함

솔루션



퍼블릭 클라우드용 CCL MTU 크기 추가

AWS 및 Azure 클러스터 MTU 값

7.4 퍼블릭 클라우드 FTDv 클러스터에는 새로운 권장 CCL 및 데이터 인터페이스 MTU 값이 있습니다.

	7.3의 권장 CCL MTU	권장 7.4의 CCL MTU	7.3의 권장 데이터 인터페이스 MTU	권장 7.4의 데이터 인터페이스 MTU
Azure NLB 클러스터	1554	1454	1400	1300
Azure GWLB 클러스터	1554	1454	1454	1374
AWS GWLB 클러스터	1960	1980	1806	1826

FMC는 클러스터를 7.4 버전으로 업그레이드한 후 CCL 및 데이터 인터페이스 MTU를 권장 값으로 업데이트합니다.

FMC에서 사용 가능한 CLI

Device/Cluster 탭에서 Device Lina CLI 프롬프트 사용 가능

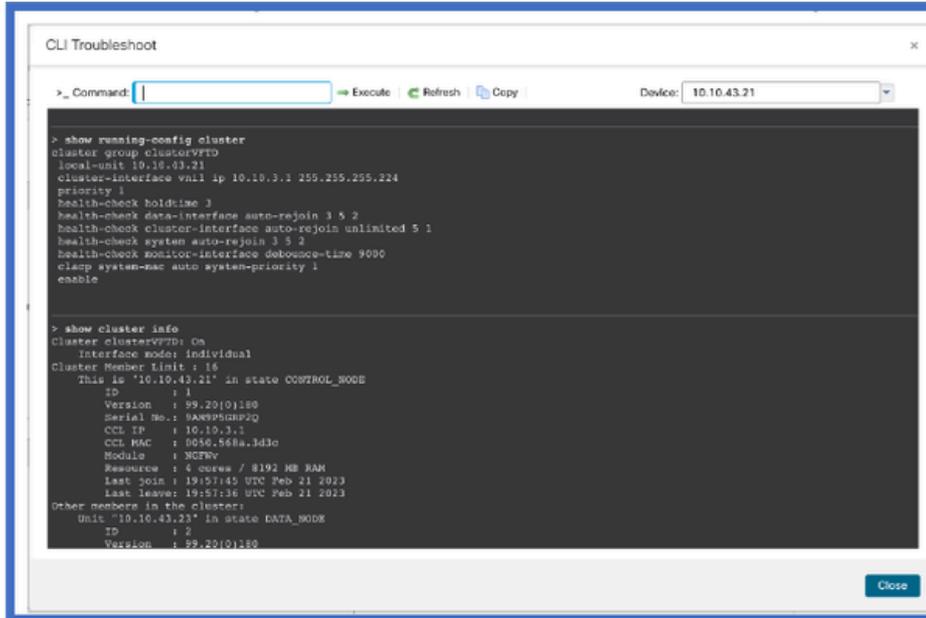
FMC에서 클러스터 Lina CLI 실행

- 이제 FMC에서 클러스터 LINA 문제 해결 CLI를 실행할 수 있습니다.

The screenshot shows the FMC configuration page for 'clusterVFTD'. In the 'General' section, under 'Troubleshoot', there is a 'CLI' button highlighted with a red box. A blue arrow points from this button to a text box on the right side of the image.

A CLI button is newly added in the General section on both the Cluster and Device Tabs

일반적으로 사용되는 CLI가 기본적으로 표시됨



- Executes a set of predefined CLIs for cluster troubleshooting on the device that is selected in the Device selection dropdown.
- The refresh button re-runs the commands.
- Copy button can be used to copy the CLI output

사전 정의된 클러스터 CLI

- 기본적으로 실행되는 CLI는 다음과 같습니다.

show running-config 클러스터

클러스터 정보 표시

클러스터 정보 상태 표시

클러스터 정보 전송 cp 표시

show version

asp 드롭 표시

show counters

arp 표시

int ip brief 표시

블록 표시

show cpu detailed

show interface <ccl_interface>

ping <ccl_ip> 크기 <ccl_mtu> 반복 2

사용 가능한 명령의 수동 입력

- Alternatively, the user can manually enter the CLI command to be run on the device.
- Enter the command and click the Execute link.
- Refresh and copy are also available.

트러블슈팅 생성

노드 가입 실패 시 자동 문제 해결

- 노드가 클러스터에 가입하지 못하면 디바이스 문제 해결이 자동으로 생성됩니다.
- 작업 관리자에 알림이 표시됩니다.

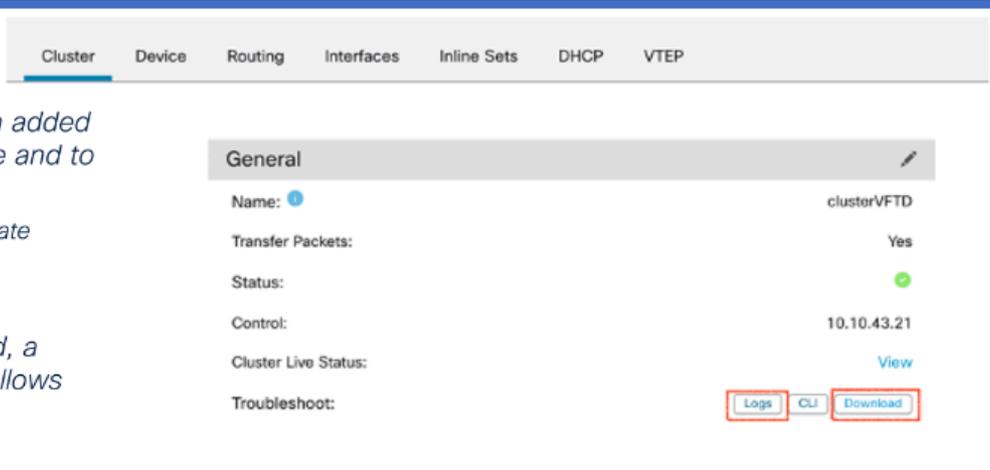
Task manager shows

- Cluster node join failure
- That a Troubleshoot has been generated.

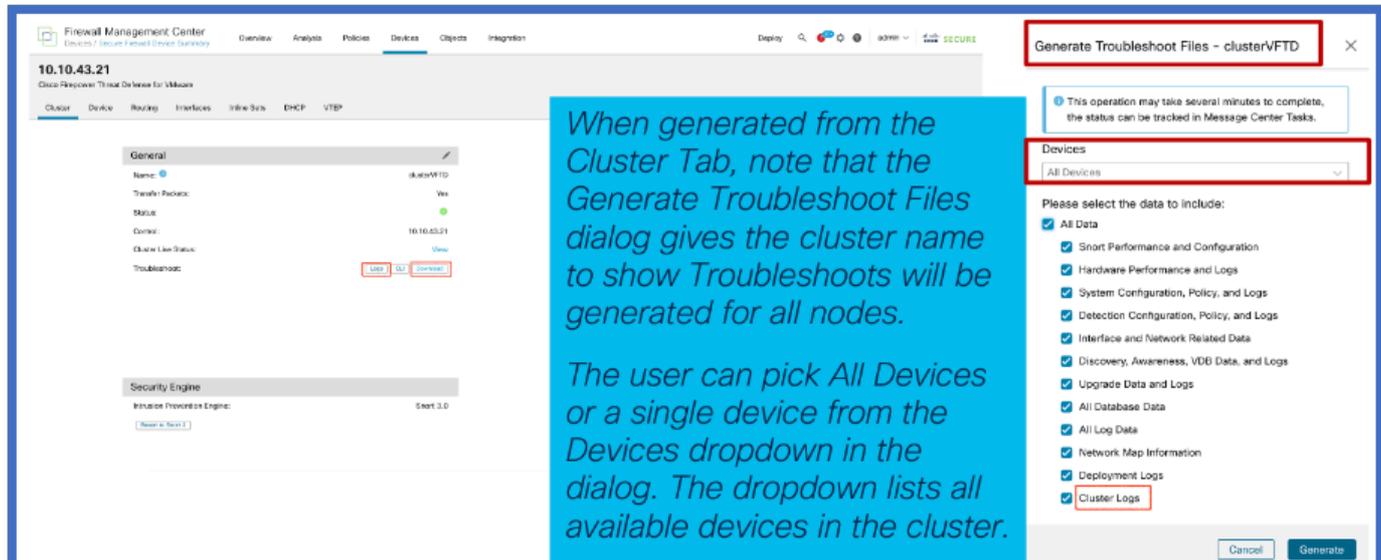
Device(디바이스) 및 Cluster(클러스터) 탭에서 Troubleshoot Trigger and Download(트리거 및 다운로드 문제 해결) 버튼 사용 가능

클러스터 문제 해결의 손쉬운 생성

- A "Logs" button has been added to the cluster device page and to the main cluster page.
 - The button opens a Generate Troubleshoot Files dialog.
- Once the Troubleshoot generation has completed, a new "Download" button allows for downloading the Troubleshoot(s).



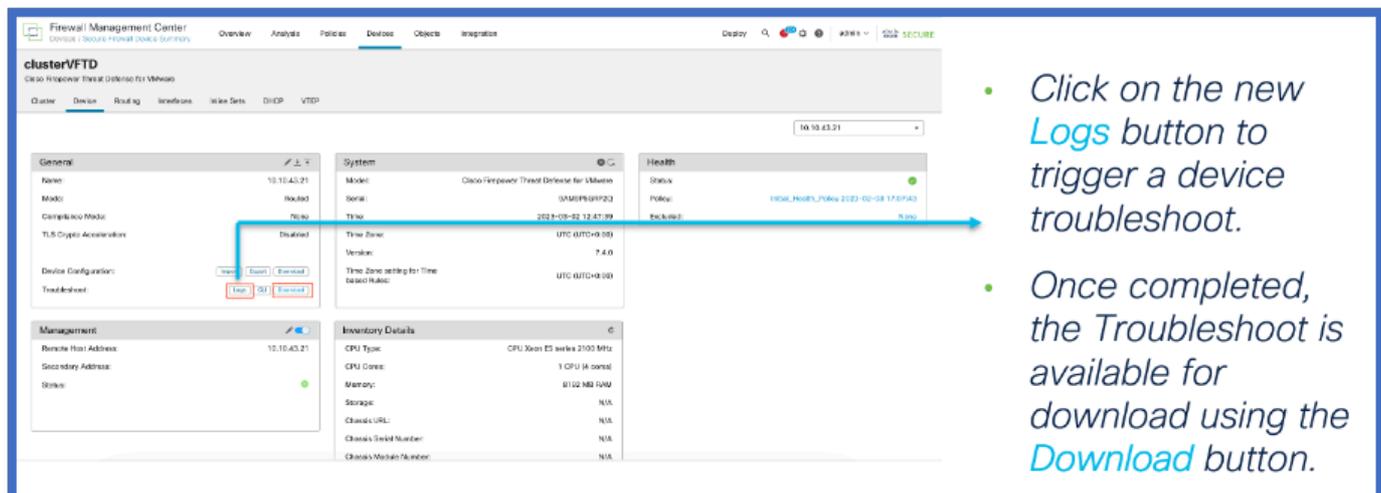
클러스터 문제 해결 생성



When generated from the Cluster Tab, note that the Generate Troubleshoot Files dialog gives the cluster name to show Troubleshoots will be generated for all nodes.

The user can pick All Devices or a single device from the Devices dropdown in the dialog. The dropdown lists all available devices in the cluster.

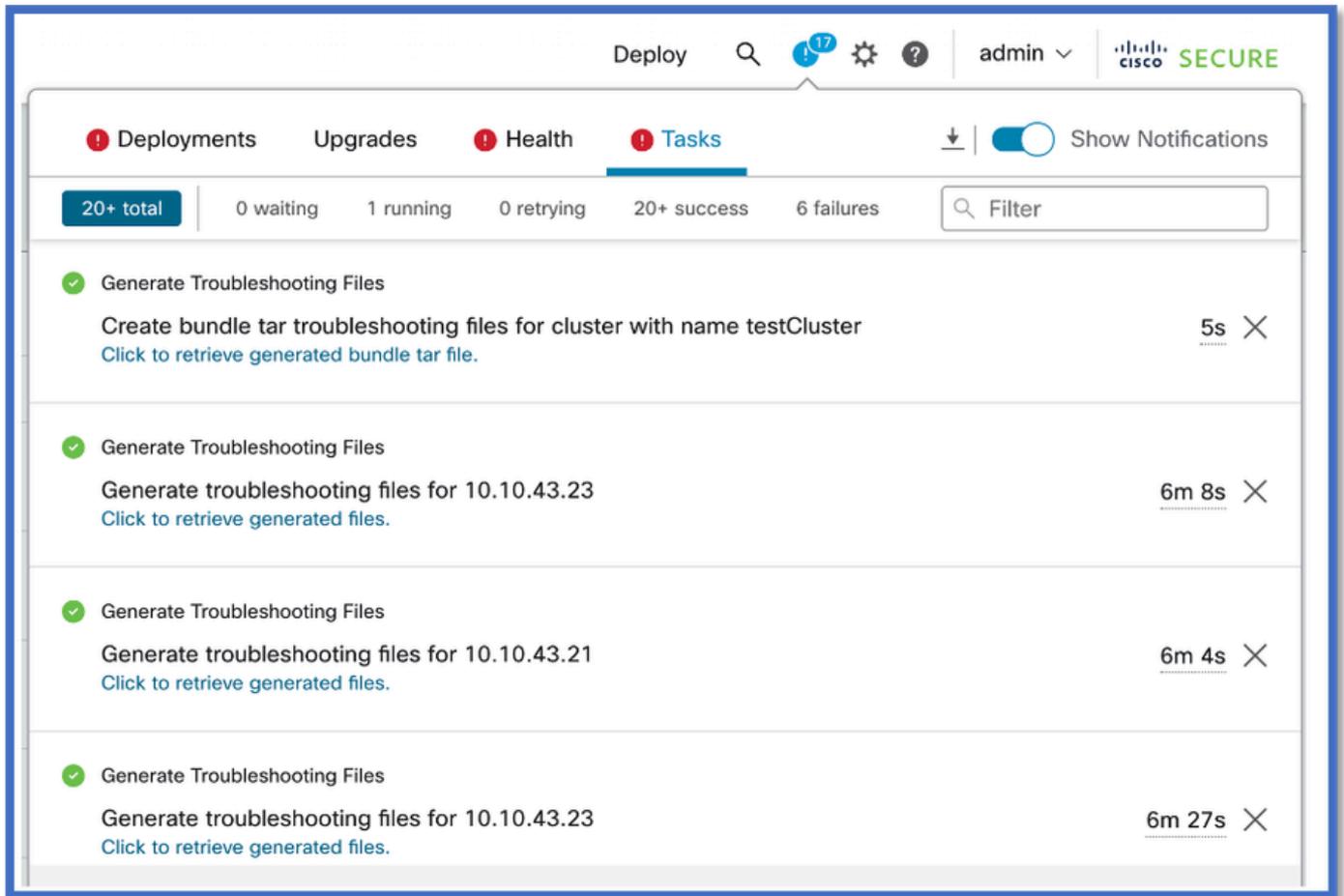
노드(장치) 문제 해결 생성



- Click on the new Logs button to trigger a device troubleshoot.
- Once completed, the Troubleshoot is available for download using the Download button.

클러스터 문제 해결 생성 완료 알림

작업 관리자는 클러스터의 각 노드에 대한 문제 해결 생성 진행 상황을 표시합니다. Download(다운로드)를 클릭하기 전에 기다립니다.



Q & A

Q: Azure에서는 MTU에 대한 AWS가 감소했지만 증가했습니까?

A: 퍼블릭 클라우드의 새 MTU 값에 대해 Azure에서는 권장 MTU가 감소하지만 AWS에서는 증가합니다.

Q: 업그레이드 과정에서 MTU가 자동으로 변경되는 경우 Syslog 항목이 있습니까?

A: 아니요. 현재 작성된 Syslog 항목이 없습니다. 필요하다면 다시 살펴볼 수 있습니다.

Q: 각 노드의 MTU 값은 어디에 표시됩니까?

A: 클러스터 탭의 device management > interfaces 페이지에 MTU 값을 열로 표시합니다.

Q: 스위치가 설정되지 않았거나 다른 노드가 설정되지 않았기 때문에 이 오류가 표시됩니까?

A: 아닙니다. 사용자에게 항상 표시되는 예방 조치로서의 경고 메시지입니다.

Q: show cluster - MTU 크기를 표시하는 명령은 무엇입니까?

A: CCL ping은 기본값이며 CLI 기본값에 표시됩니다.

Q: AWS의 경우, 스위치에서 MTU를 늘리는 방법에 대한 단계를 문서화할 수 있습니까?

A: 테크 팝에서 확인하려고요.

Q: HW의 경우 - 3100 시리즈만 나열했으며 4K/9K/2K/1K는 어떻습니까?

A: 9300, 4100, 3100에서 클러스터링하고 가상 전용입니다. FMC에서 3100을 수행할 수 있지만, 4100 및 9300 클러스터는 FMC가 아니라 새시 관리자에서 수행됩니다.

Q: 변경 사항을 적용하려면 FMC에서 구축해야 합니까? 디바이스 이후 업그레이드를 수행해야 합니까?

A: 예. 업그레이드 후 구축해야 합니다. 권장 MTU 값을 사용해야 합니다.

Q: FTD가 GRE 터널을 생성하는 경로의 중간인 것처럼 MTU가 변경되었다는 경고 메시지를 사용자에게 제공합니까? 사용자가 터널이 플래핑되거나 다운된 것을 볼 수 있습니까?

A: 문서에 있습니다. 경고 메시지에 대해 작업할 수 있습니다. 노드는 제어 노드로 조정됩니다. 스위치는 새로운 값으로 조정되어야 할 것이다. 제어 노드가 업그레이드된 후 값이 변경됩니다. MTU 값은 제어에 의해 전송됩니다.

Q: 업그레이드 후에 MTU를 변경하는 경우 FTD 디바이스를 재부팅합니까?

A: MTU 값이 변경될 때 업그레이드 시 FTD에서 명시적 재부팅이 트리거되지 않습니다.

개정 이력

개정	게시 날짜	의견
2.0	2024년 7월 17일	대체 텍스트를 추가했습니다. 서식이 업데이트되었습니다.
1.0	2024년 7월 17일	최초 릴리스

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.