Configure Cluster Serviceability Improvements in Firewall Management Center 7.4

Contents

Introduction

This document describes how you can use serviceability improvements in FMC 7.4

What’s New

- Cluster Control Link (CCL) link diagnostics and assistance with ensuring settings are correct.
- Cluster Lina CLIs can now be seen in Firewall Management Center (FMC).

- Troubleshoot Generation
  - Can now be generated all at once for all devices in a cluster.
  - Troubleshoot generation is automatic if a node fails to join a cluster.
  - Troubleshoot generation and navigation from the Devices > Cluster/Device tab.

Prerequisites, Supported Platforms, Licensing

Minimum Software & Hardware Platforms

Application and Minimum Version	**Managed Devices**	**Min Supported Managed Device Version Required**	**Notes**
Secure Firewall 7.4	All which support clustering on FTD Only "Generation of Troubleshoots" enhancement requires FTD version to be 7.4 and higher	• FMC On-Prem + FMC REST API • cloud-delivered FMC	This is an FMC feature, so configuration can be applied to any device that FMC 7.4 can manage.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco Firewall Management Center (FMC) running 7.4
- Cisco Firepower Threat Defense (FTD) running 7.4 or higher.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

CCL Link Diagnostics

Cluster Control Link Interface MTU Warning in the Cluster Summary Page

Problem

- Clustering requires a higher MTU for the cluster control link than data interfaces.
- You often do not set the MTU to a high enough value, which causes reliability issues.
- Recommendation is CCL MTU must be 100 or 154 bytes more than the maximum data interface MTU, based on the platform, to sync the cluster state across the nodes.

CCL MTU = (Maximum Data Interface MTU) + 100 |154

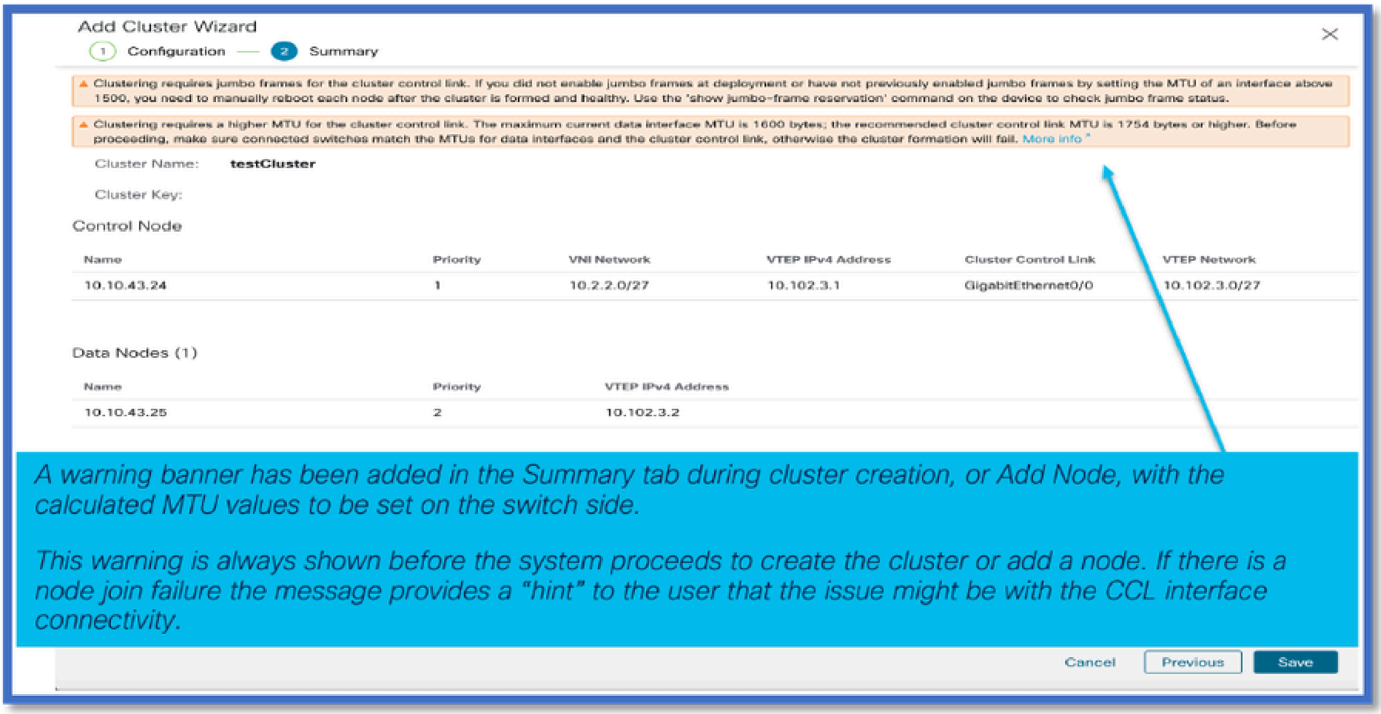
For example, for an FTDv device, if 1700 bytes is the maximum data interface MTU, then the value of CCL interface MTU would be set as 1854:
1854 = 1700 + 154

MTU Size Recommendations Per Platform

Platform	Sample maximum Data Interface MTU	Add	Total Recommended Setting for MTU for CCL Link
Sec FW 3100 Series	1700	100	1800
FTDv	1700	154	1854

Solution

- When a cluster is created, the MTU value for the CCL link is automatically set to the recommended value on the interface.
  Make the switch side configuration to match this value.
- Sample warning message:
  Clustering requires a higher MTU for the cluster control link. The maximum current data interface MTU is 1500 bytes; the recommended cluster control link MTU is 1654 bytes or higher. Before proceeding, make sure connected switches match the MTUs for data interfaces and the cluster control link, otherwise the cluster formation would fail.
- If the switch side configuration for CCL interface does not match this value, the device fails to join the cluster.



▲ Clustering requires jumbo frames for the cluster control link. If you did not enable jumbo frames at deployment or have not previously enabled jumbo frames by setting the MTU of an interface above 1500, you need to manually reboot each node after the cluster is formed and healthy. Use the 'show jumbo-frame reservation' command on the device to check jumbo frame status.

▲ Clustering requires a higher MTU for the cluster control link. The maximum current data interface MTU is 1600 bytes; the recommended cluster control link MTU is 1754 bytes or higher. Before proceeding, make sure connected switches match the MTUs for data interfaces and the cluster control link, otherwise the cluster formation will fail. More info

Cluster Name: testCluster

Cluster Key:

Control Node

Name	Priority	VNI Network	VTEP IPv4 Address	Cluster Control Link	VTEP Network
10.10.43.24	1	10.2.2.0/27	10.102.3.1	GigabitEthernet0/0	10.102.3.0/27

Data Nodes (1)

Name	Priority	VTEP IPv4 Address
10.10.43.25	2	10.102.3.2

A warning banner has been added in the Summary tab during cluster creation, or Add Node, with the calculated MTU values to be set on the switch side.

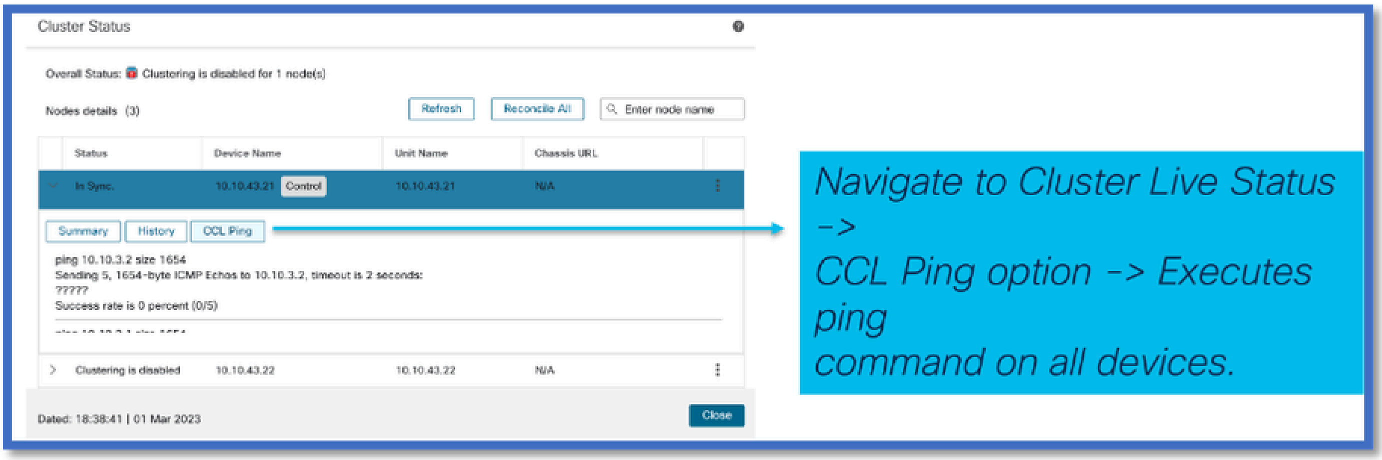
This warning is always shown before the system proceeds to create the cluster or add a node. If there is a node join failure the message provides a "hint" to the user that the issue might be with the CCL interface connectivity.

CCL Ping Test in Cluster Live Status

Check CCL Connectivity

- Need for user provision to verify the CCL connectivity with CCL MTU packet size

Solution



Overall Status: Clustering is disabled for 1 node(s)

Nodes details (3)

Status	Device Name	Unit Name	Chassis URL
In Sync.	10.10.43.21 Control	10.10.43.21	N/A
Clustering is disabled	10.10.43.22	10.10.43.22	N/A

```
ping 10.10.3.2 size 1654
Sending 5, 1654-byte ICMP Echos to 10.10.3.2, timeout is 2 seconds:
?????
Success rate is 0 percent (0/5)
```

Dated: 18:38:41 | 01 Mar 2023

Navigate to Cluster Live Status -> CCL Ping option -> Executes ping command on all devices.

Added CCL MTU Sizes for Public Cloud

AWS and Azure Cluster MTU Values

There are new recommended CCL and data interface MTU values for 7.4 public cloud FTDv clusters.

	Recommended CCL MTU in 7.3	Recommended CCL MTU in 7.4	Recommended Data interface MTU in 7.3	Recommended Data interface MTU in 7.4
Azure NLB cluster	1554	1454	1400	1300
Azure GWLB cluster	1554	1454	1454	1374
AWS GWLB cluster	1960	1980	1806	1826

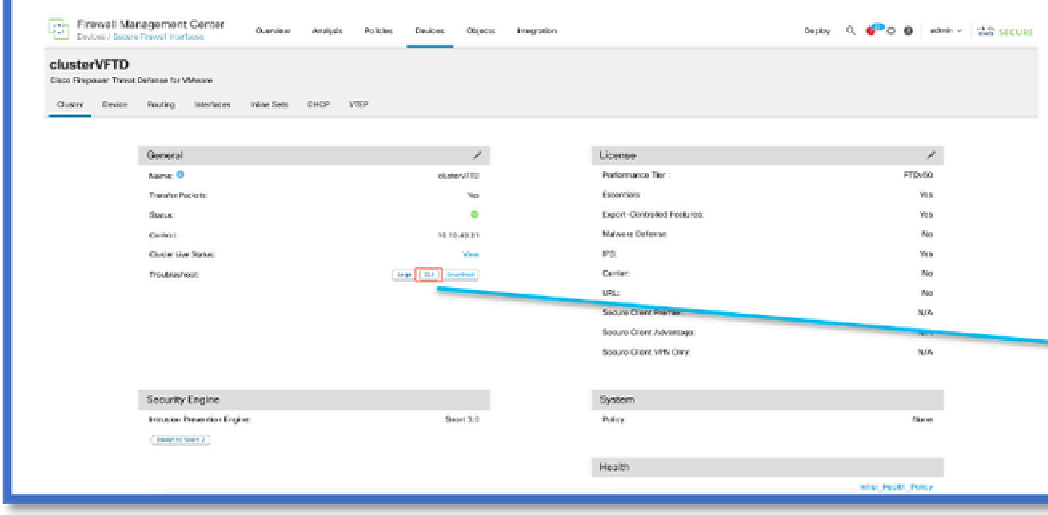
FMC updates the CCL and data interface MTU to recommended values after upgrade of a cluster to 7.4 version.

CLIs Available in FMC

Device Lina CLI Prompt Available in Device/Cluster Tab

Run Cluster Lina CLIs from FMC

- It is now possible to execute cluster LINA troubleshoot CLIs from FMC.



Firewall Management Center
Devices / Secure Firewall Interfaces

Overview Analysis Policies Devices Objects Integration

Deploy admin SECURE

clusterVFTD
Cisco Firepower Threat Defense for VMware

Cluster Device Routing Interfaces Inline Sets DHCP VTEP

General

Name: clusterVFTD
Transfer Packets: Yes
Status:
Control: 10.10.43.21
Cluster Live Status: View
Troubleshoot: Logs CLI Download

License

Performance Tier : FTDv50
Essentials: Yes
Export-Controlled Features: Yes
Malware Defense: No
IPS: Yes
Carrier: No
URL: No
Secure Client Premier: N/A
Secure Client Advantage: N/A
Secure Client VPN Only: N/A

Security Engine

Intrusion Prevention Engine: Snort 3.0
Revert to Snort 2

System

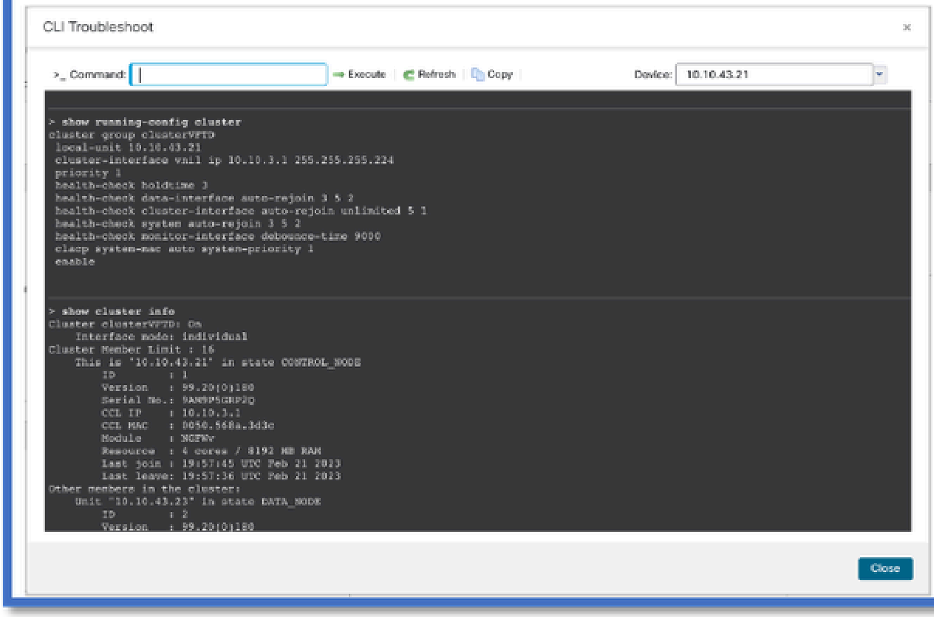
Policy: None

Health

Initial_Health_Policy

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

Commonly Used CLIs Shown by Default



CLI Troubleshoot

>_ Command: | Execute | Refresh | Copy | Device: 10.10.43.21

```
> show running-config cluster
cluster group clusterVFTD
 local-unit 10.10.43.21
 cluster-interface vni1 ip 10.10.3.1 255.255.255.224
 priority 1
 health-check holdtime 3
 health-check data-interface auto-rejoin 3 5 2
 health-check cluster-interface auto-rejoin unlimited 5 1
 health-check system auto-rejoin 3 5 2
 health-check monitor-interface debounce-time 9000
 clacp system-mac auto system-priority 1
 enable
```

```
> show cluster info
Cluster clusterVFTD: On
    Interface mode: individual
Cluster Member Limit : 16
    This is '10.10.43.21' in state CONTROL_NODE
        ID        : 1
        Version   : 99.20(0)180
        Serial No.: 9AN9P5GRP2Q
        CCL IP    : 10.10.3.1
        CCL MAC   : 0050.568a.3d3c
        Module    : NGFWv
        Resource  : 4 cores / 8192 MB RAM
        Last join : 19:57:45 UTC Feb 21 2023
        Last leave: 19:57:36 UTC Feb 21 2023
Other members in the cluster:
    Unit "10.10.43.23" in state DATA_NODE
        ID        : 2
        Version   : 99.20(0)180
```

Close

- *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*

Predefined Cluster CLIs

- The CLIs which are run by default are:

  show running-config cluster

  show cluster info

  show cluster info health

  show cluster info transport cp

  show version

  show asp drop

  show counters

show arp

show int ip brief

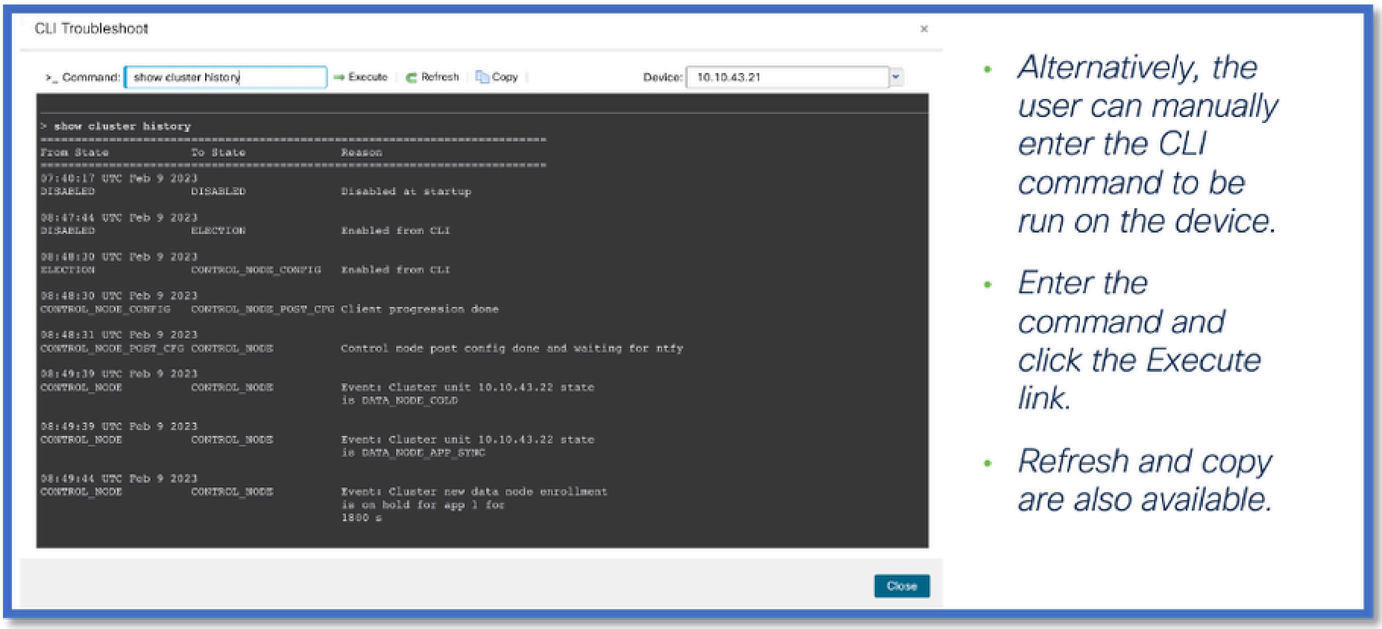
show blocks

show cpu detailed

show interface <ccl_interface>

ping <ccl_ip> size <ccl_mtu> repeat 2

Manual Entry of Commands Available



Command: show cluster history

Device: 10.10.43.21

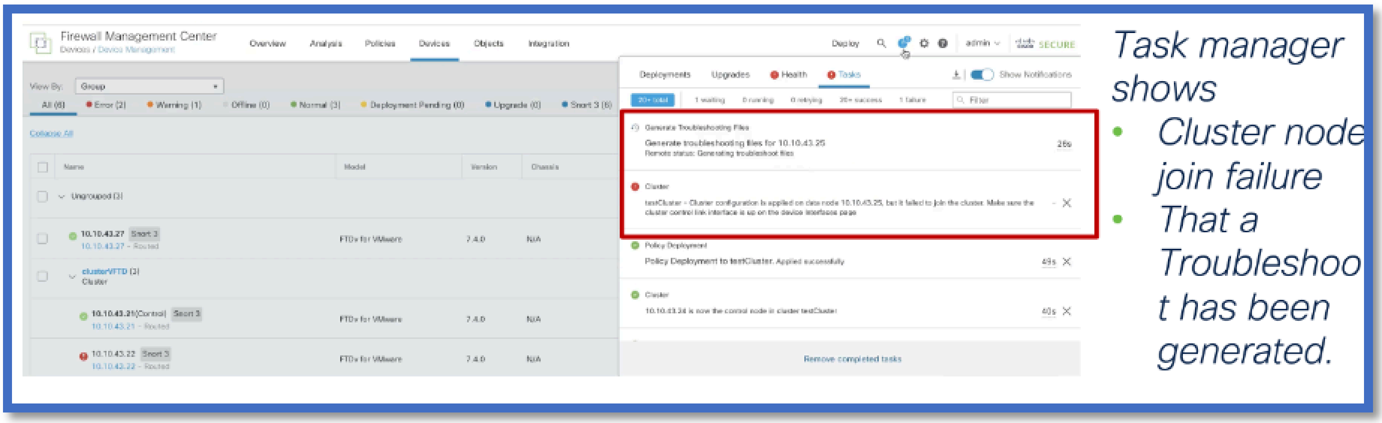
```
> show cluster history
==========================================================================
From State           To State             Reason
==========================================================================
07:40:17 UTC Feb 9 2023
DISABLED             DISABLED             Disabled at startup

08:47:44 UTC Feb 9 2023
DISABLED             ELECTION             Enabled from CLI

08:48:30 UTC Feb 9 2023
ELECTION             CONTROL_NODE_CONFIG  Enabled from CLI

08:48:30 UTC Feb 9 2023
CONTROL_NODE_CONFIG  CONTROL_NODE_POST_CFG Client progression done

08:48:31 UTC Feb 9 2023
CONTROL_NODE_POST_CFG CONTROL_NODE        Control node post config done and waiting for ntfy

08:49:39 UTC Feb 9 2023
CONTROL_NODE         CONTROL_NODE         Event: Cluster unit 10.10.43.22 state
                                          is DATA_NODE_COLD

08:49:39 UTC Feb 9 2023
CONTROL_NODE         CONTROL_NODE         Event: Cluster unit 10.10.43.22 state
                                          is DATA_NODE_APP_SYNC

08:49:44 UTC Feb 9 2023
CONTROL_NODE         CONTROL_NODE         Event: Cluster new data node enrollment
                                          is on hold for app 1 for
                                          1800 s
```

- *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.*

Generation of Troubleshoots

Automatic Troubleshoot Generation on Node Join Failure

- When a node fails to join the cluster, a device Troubleshoot is automatically generated.
- A notification is shown in Task Manager.



	Name	Model	Version	Chassis
□	Ungrouped (1)			
□	10.10.43.27 Snort 3 10.10.43.27 - Routed	FTDv for VMware	7.4.0	N/A
□	clusterVFTD (3) Cluster			
	10.10.43.21(Control) Snort 3 10.10.43.21 - Routed	FTDv for VMware	7.4.0	N/A
	10.10.43.22 Snort 3 10.10.43.22 - Routed	FTDv for VMware	7.4.0	N/A

Generate Troubleshooting Files
Generate troubleshooting files for 10.10.43.25 — 28s
Remote status: Generating troubleshoot files

Cluster
testCluster - Cluster configuration is applied on data node 10.10.43.25, but it failed to join the cluster. Make sure the cluster control link interface is up on the device interfaces page

Policy Deployment
Policy Deployment to testCluster. Applied successfully — 49s

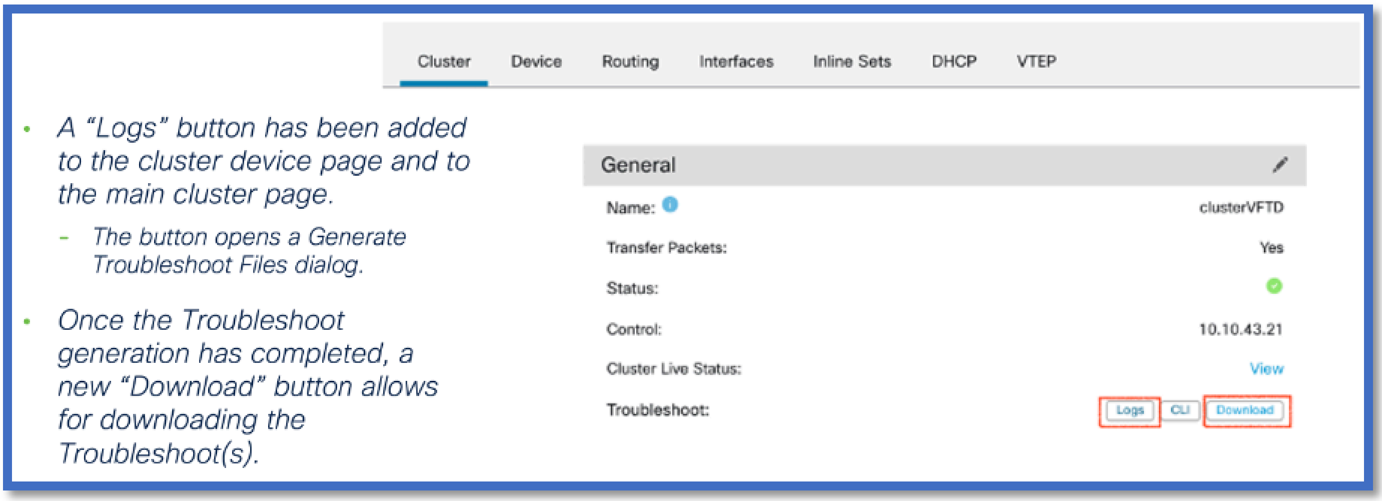
Cluster
10.10.43.24 is now the control node in cluster testCluster — 40s

Task manager shows

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

Troubleshoot Trigger and Download Button Available in Device and Cluster Tabs

Easier Generation of Cluster Troubleshoots



- *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).*

General

Name: clusterVFTD

Transfer Packets: Yes

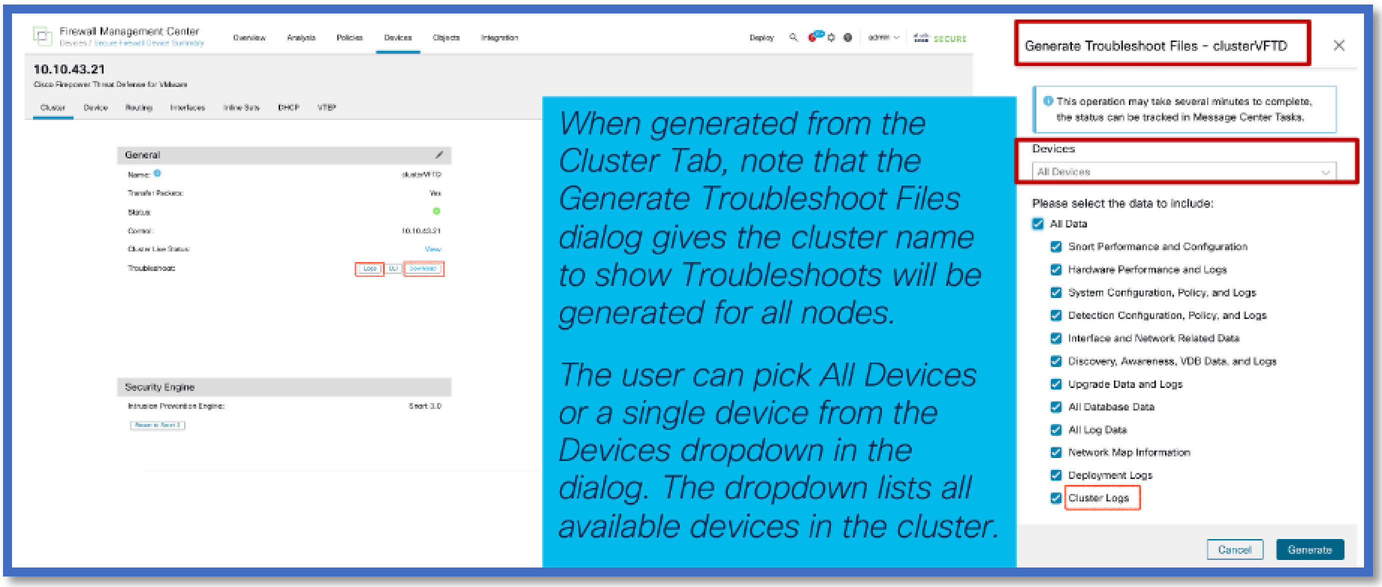
Status:

Control: 10.10.43.21

Cluster Live Status: View

Troubleshoot: Logs CLI Download

Cluster Troubleshoot Generation



10.10.43.21

Cisco Firepower Threat Defense for VMware

General

Name: clusterVFTD

Transfer Packets: Yes

Status:

Control: 10.10.43.21

Cluster Live Status: View

Troubleshoot:

Security Engine

Intrusion Prevention Engine: Snort 3.0

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.

Generate Troubleshoot Files - clusterVFTD

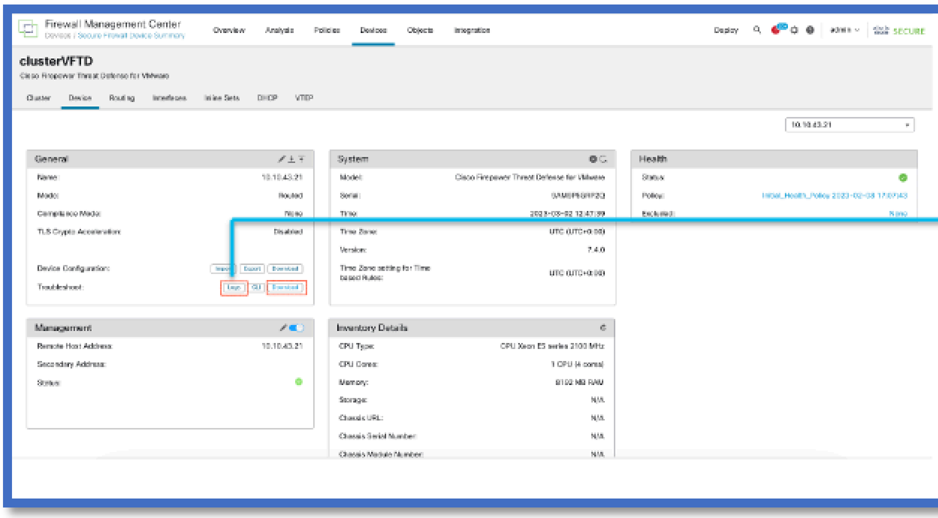
This operation may take several minutes to complete, the status can be tracked in Message Center Tasks.

Devices: All Devices

Please select the data to include:

- ☑ All Data
  - ☑ Snort Performance and Configuration
  - ☑ Hardware Performance and Logs
  - ☑ System Configuration, Policy, and Logs
  - ☑ Detection Configuration, Policy, and Logs
  - ☑ Interface and Network Related Data
  - ☑ Discovery, Awareness, VDB Data, and Logs
  - ☑ Upgrade Data and Logs
  - ☑ All Database Data
  - ☑ All Log Data
  - ☑ Network Map Information
  - ☑ Deployment Logs
  - ☑ Cluster Logs

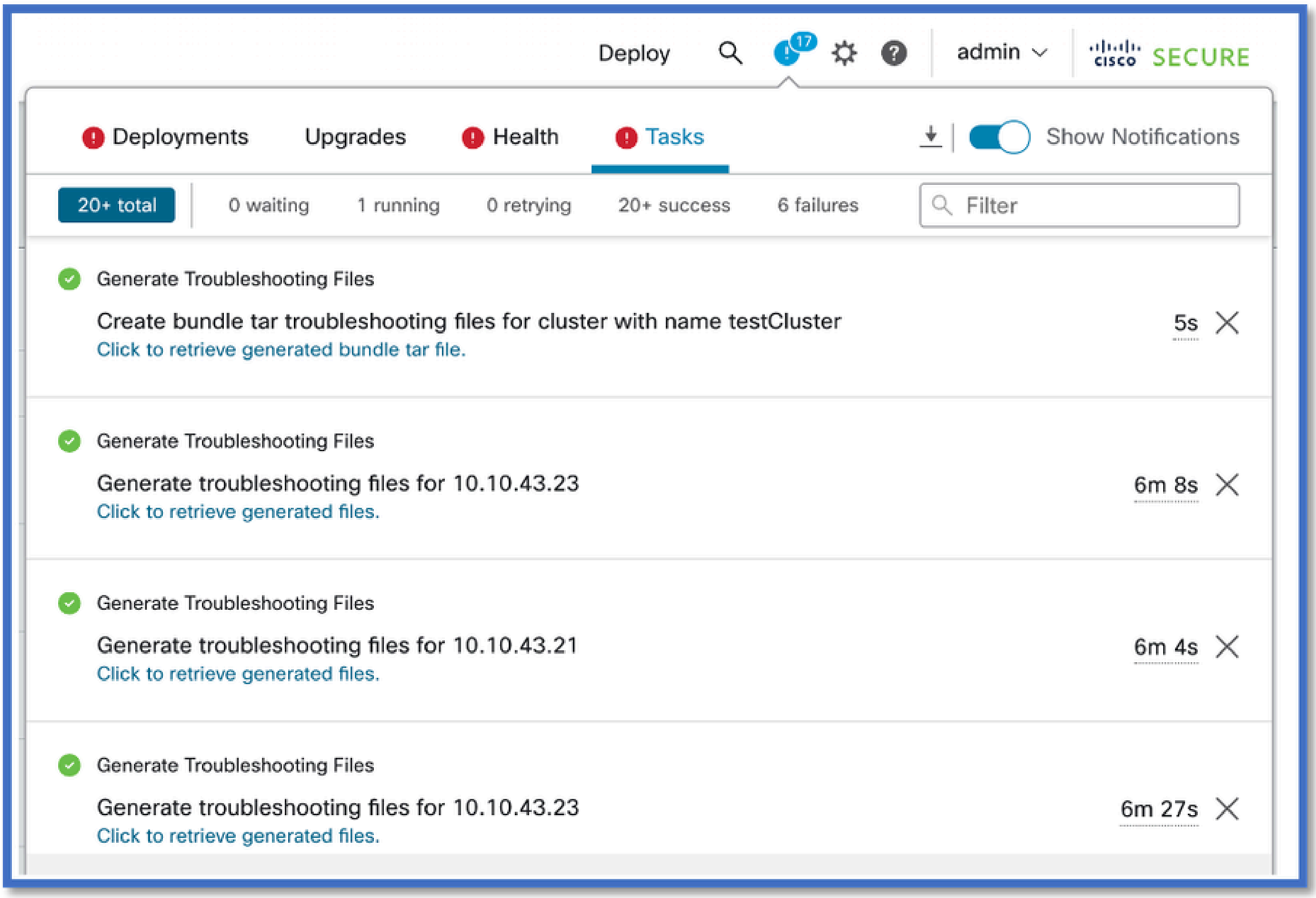
Node (Device) Troubleshoot Generation



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

Notification of Cluster Troubleshoot Generation Complete

The Task manager shows the progress of the troubleshoot generation for each node in the cluster. Wait for that before clicking **Download**.



Generate Troubleshooting Files
Create bundle tar troubleshooting files for cluster with name testCluster — 5s
Click to retrieve generated bundle tar file.

Generate Troubleshooting Files
Generate troubleshooting files for 10.10.43.23 — 6m 8s
Click to retrieve generated files.

Generate Troubleshooting Files
Generate troubleshooting files for 10.10.43.21 — 6m 4s
Click to retrieve generated files.

Generate Troubleshooting Files
Generate troubleshooting files for 10.10.43.23 — 6m 27s
Click to retrieve generated files.

Q & A

Q: In Azure it reduced but increased in AWS for MTU?

A: For the new MTU values in public clouds, in Azure the recommended MTU is reduced, but it is increased in AWS.

Q: During Upgrade if MTU is changed automatically - is there a Syslog entry?

A: No, there is no Syslog entry made at this time. We can relook at it if this is needed.

Q: Where is the MTU value of each node shown?

A: Show the MTU value as a column on the device management > interfaces page, on the cluster tab.

Q: Is this failure showing because Switch is not set, or the other node is not set?

A: No, it is a warning message as precaution which is displayed all the time to user.

Q: Which command - show cluster - shows the MTU size?

A: CCL ping is in the default and shows in the CLI defaults.

Q: In case of AWS, can we document the steps on how to increase the MTU on switch?

A: For tech pubs to check.

Q: For HW - you only listed 3100 series -what about 4K/9K/2K/1K?

A: Clustering on 9300, 4100, 3100 and virtual only. 3100 can be done from FMC, but 4100 and 9300 clusters are done in the chassis manager, not FMC.

Q: Do you have to deploy from the FMC for the changes to take effect, post-device upgrade?

A: Yes, need to deploy after upgrade. You must use the recommended MTU values.

Q: Are we providing any warning message to user that MTU is changed, as if FTD is middle of path where GRE tunnel build, would user see the tunnel flapping or went down?

A: It is in the documentation. Can work on warning message. Nodes wiould adjust to control node. Switch would have to be adjusted to the new values. Value is changed after control node is upgraded. MTU value is sent by control.

Q: Are we going to reboot the FTD device if post upgrade we are changing the MTU?

A: No explicit reboot is triggered on FTD on upgrade when MTU values are changed.

Revision History

Revision	Publish Date	Comments
2.0	17-Jul-2024	Added Alt Text. Updated Formatting.
1.0	17-Jul-2024	Initial Release