

Configureer Cluster Servicability Verbeteringen in Firewall Management Center 7.4

Inhoud

[Inleiding](#)

[Nieuw](#)

[Voorwaarden, ondersteunde platforms, licentiëring](#)

[Minimale software- en hardwareplatforms](#)

[Gebruikte componenten](#)

[CCL Link-diagnostiek](#)

[Waarschuwing van MTU voor Cluster Control Link Interface in de overzichtspagina van het cluster](#)

[Probleem](#)

[MTU-grootteaanbevelingen per platform](#)

[Oplossing](#)

[CCL Ping Test in Cluster Live-status](#)

[Connectiviteit met CCL controleren](#)

[Oplossing](#)

[Toegevoegd CCL MTU maten voor Public Cloud](#)

[CLI's beschikbaar in FMC](#)

[Prompt voor apparaatverbinding beschikbaar in tabblad Apparaat/Cluster](#)

[Run Cluster Lina CLI's van FMC](#)

[Algemeen gebruikte CLI's standaard weergegeven](#)

[Vooraf gedefinieerde Cluster-CLI's](#)

[Handmatige invoer van opdrachten beschikbaar](#)

[Genereren van probleemoplossing](#)

[Automatische probleemoplossing Generation on Node Join Failure](#)

[Probleemoplossing - Trigger en Download-knop beschikbaar in de tabbladen Apparaten en Clusters](#)

[Eenvoudiger generatie van clusterprobleemoplossing](#)

[Generatie van clusterprobleemoplossing](#)

[Generatie van probleemoplossing voor knooppunt \(apparaat\)](#)

[Melding van Cluster Probleemoplossing Generatie voltooid](#)

[Vraag en antwoord](#)

[Revisiegeschiedenis](#)

Inleiding

In dit document wordt beschreven hoe u de verbetering van de service in FMC 7.4 kunt gebruiken

Nieuw

- Cluster Control Link (CCL) - linkdiagnostiek en hulp bij het controleren of de instellingen correct zijn.
- Cluster Lina CLI's zijn nu te zien in Firewall Management Center (FMC).
- Generatie voor probleemoplossing
 - Kan nu alles in één keer voor alle apparaten in een cluster worden gegenereerd.
 - Generatie van probleemoplossing is automatisch als een knooppunt zich niet bij een cluster aansluit.
 - Probleemoplossing voor generatie en navigatie vanuit het tabblad Apparaten > Cluster/apparaat.

Voorwaarden, ondersteunde platforms, licentiëring

Minimale software- en hardwareplatforms

Toepassing en minimale versie	Beheerde apparaten	Min. ondersteunde versie van beheerde apparaat vereist	Opmerkingen
Secure-firewall 7.4	<p>Allemaal die clustering op FTD ondersteunen</p> <p>Alleen verbetering in "Generation of Troubleshoots" vereist dat de FTD-versie 7.4 en hoger is</p>	<p>· FMC On-Prem + FMC REST API</p> <p>· FMC in de cloud</p>	Dit is een FMC-functie, zodat de configuratie kan worden toegepast op elk apparaat dat door FMC 7.4 kan worden beheerd.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco Firewall Management Center (FMC) met 7.4
- Cisco Firepower Threat Defence (FTD) met 7.4 of hoger.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

CCL Link-diagnostiek

Waarschuwing van MTU voor Cluster Control Link Interface in de overzichtspagina van het cluster

Probleem

- Clustering vereist een hogere MTU voor de clusterbesturingskoppeling dan datainterfaces.
- U stelt de MTU vaak niet op een voldoende hoge waarde in, wat betrouwbaarheidsproblemen veroorzaakt.
- Aanbeveling is CCL MTU moet 100 of 154 bytes meer dan de maximale data-interface MTU, gebaseerd op het platform, om de clusterstatus over de knooppunten te synchroniseren.

CCL MTU = (maximale datainterface MTU) + 100 | 154

Bijvoorbeeld, voor een FTDv apparaat, als 1700 bytes de maximum gegevensinterface MTU is, dan zou de waarde van CCL interface MTU worden geplaatst als 1854:

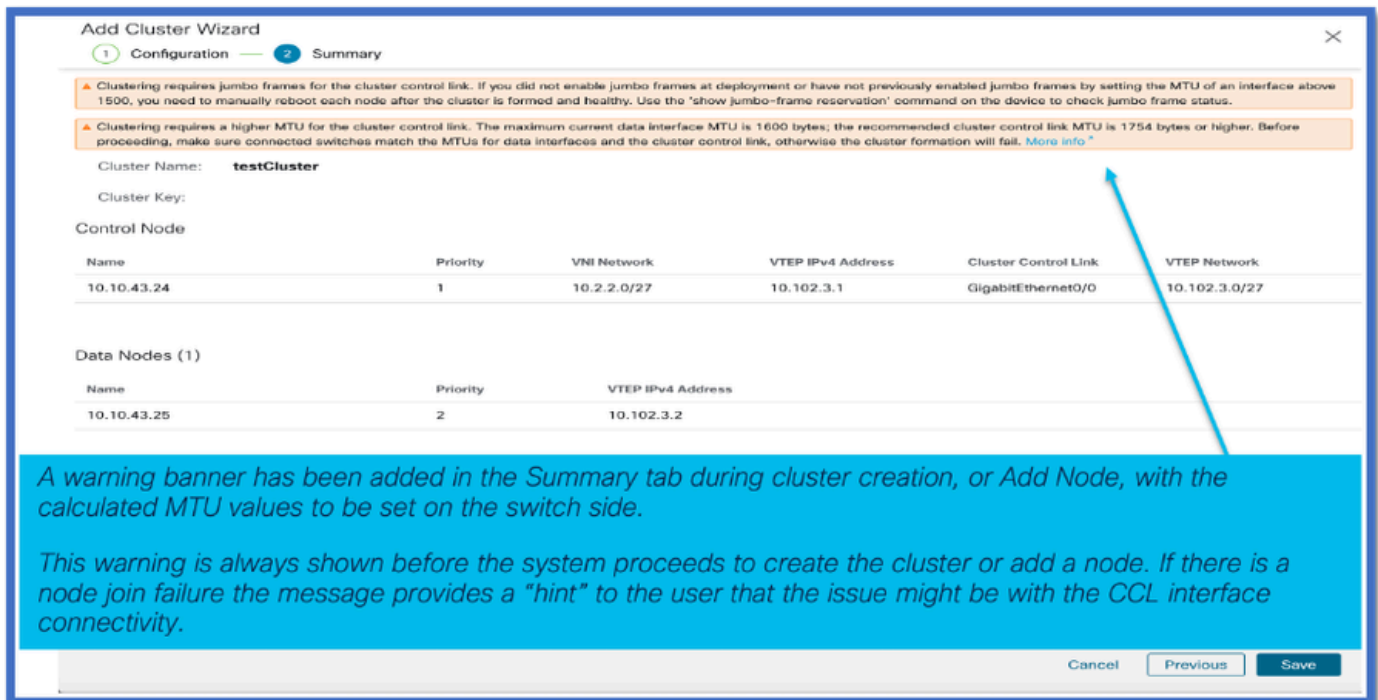
$$1854 = 1700 + 154$$

MTU-grootteaanbevelingen per platform

Platform	Maximum aantal gegevensinterfacemodule van voorbeeld	Toevoegen	Totaal aanbevolen instelling voor MTU voor CCL Link
SEC FW 3100 Series	1700	100	1800
FTDv	1700	154	1854

Oplossing

- Wanneer een cluster wordt gemaakt, wordt de MTU-waarde voor de CCL-link automatisch ingesteld op de aanbevolen waarde in de interface.
Maak de switch zijconfiguratie om deze waarde aan te passen.
- Waarschuwingsbericht:
Voor clustervorming is een hogere MTU nodig voor de koppeling voor clusterbesturing. De maximale huidige data-interface MTU is 1500 bytes; de aanbevolen cluster control link MTU is 1654 bytes of hoger. Alvorens verder te gaan, zorg ervoor dat de verbonden switches overeenkomen met de MTU's voor gegevensinterfaces en de clusterbesturingsverbinding, anders zou de clustervorming mislukken.
- Als de switch zijconfiguratie voor CCL-interface niet overeenkomt met deze waarde, kan het apparaat zich niet bij het cluster aansluiten.

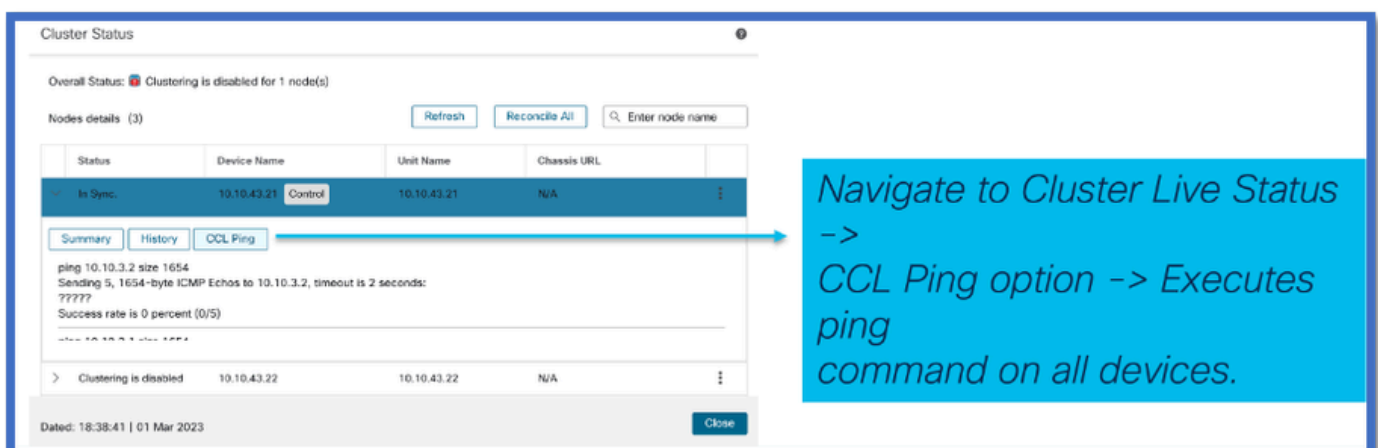


CCL Ping Test in Cluster Live-status

Connectiviteit met CCL controleren

- Behoeftte aan gebruikersvoorziening om de CCL-connectiviteit met de pakketgrootte van CCL MTU te verifiëren

Oplossing



Toegevoegd CCL MTU maten voor Public Cloud

AWS en Azure Cluster MTU-waarden

Er zijn nieuwe aanbevolen CCL en data interface MTU waarden voor 7.4 openbare cloud FTDv clusters.

	Aanbevolen CCL MTU in 7.3	Aanbevolen CCL MTU in 7.4	Aanbevolen Data-interface MTU in 7.3	Aanbevolen 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 werkt de CCL en data-interface MTU bij naar aanbevolen waarden na upgrade van een cluster naar 7.4 versie.

CLI's beschikbaar in FMC

Prompt voor apparaatverbinding beschikbaar in tabblad Apparaat/Cluster

Run Cluster Lina CLI's van FMC

- Het is nu mogelijk om CLI's voor probleemoplossing van cluster LINA uit te voeren vanuit FMC.

The screenshot shows the Cisco Firewall Management Center (FMC) interface for a cluster named 'clusterVFTD'. The 'General' tab is active, displaying various configuration parameters. A red box highlights a 'CLI' button located in the General section. A blue arrow points from this button to a text box on the right side of the image. The text box contains the following text: 'A CLI button is newly added in the General section on both the Cluster and Device Tabs'.

Algemeen gebruikte CLI's standaard weergegeven

```

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
clasp 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 : 59.20(0)180
Serial No.: 9AN9P5GHP2Q
CCL IP : 10.10.3.1
CCL MAC : 0050.468a.3d3e
Module : NCFW
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 : 59.20(0)180

```

- 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

Vooraf gedefinieerde Cluster-CLI's

- De CLI's die standaard worden uitgevoerd zijn:
 - toon in werking stellen-configuratiecluster
 - clusterinformatie tonen
 - gezondheid van clusterinfo tonen
 - toon cluster info transport cp
 - show version
 - druppel tonen
 - show counters
 - show arp
 - toon int ip samenvatting
 - blokken weergeven
 - cpu gedetailleerd weergeven
 - interface tonen <ccl_interface>
 - <ccl_ip> grootte pingen <ccl_mtu> herhaal 2

Handmatige invoer van opdrachten beschikbaar

CLI Troubleshoot

> Command: Execute Refresh Copy Device: 10.10.43.21

```

> show cluster history
-----
From State      To State      Reason
-----
97:40:17 UTC Feb 9 2023
DISABLED       DISABLED       Disabled at startup
98:47:44 UTC Feb 9 2023
DISABLED       ELECTION       Enabled from CLI
98:48:30 UTC Feb 9 2023
ELECTION       CONTROL_NODES_CONFIG  Enabled from CLI
98:48:30 UTC Feb 9 2023
CONTROL_NODES_CONFIG  CONTROL_NODES_POST_CFG Client progression done
98:48:31 UTC Feb 9 2023
CONTROL_NODES_POST_CFG CONTROL_NODES      Control mode post config done and waiting for ntpy
98:49:39 UTC Feb 9 2023
CONTROL_NODES      CONTROL_NODES      Event: Cluster unit 10.10.43.22 state
is DATA_MODE_COLD
98:49:39 UTC Feb 9 2023
CONTROL_NODES      CONTROL_NODES      Event: Cluster unit 10.10.43.22 state
is DATA_MODE_APP_SYNC
98:49:44 UTC Feb 9 2023
CONTROL_NODES      CONTROL_NODES      Event: Cluster new data node enrollment
is on hold for app 1 for
1800 s

```

Close

- 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.

Genereren van probleemoplossing

Automatische probleemoplossing Generation on Node Join Failure

- Wanneer een knooppunt zich niet bij het cluster aansluit, wordt automatisch een apparaatprobleemoplossing gegenereerd.
- Een melding wordt weergegeven in Taakbeheer.

Firewall Management Center

Overview Analysis Policies Devices Objects Integration

Deploy Search admin

Tasks

Name	Model	Version	Chassis	Status
10.10.43.27	FTDs for VMware	7.4.0	N/A	Success
10.10.43.21	FTDs for VMware	7.4.0	N/A	Success
10.10.43.22	FTDs for VMware	7.4.0	N/A	Failure

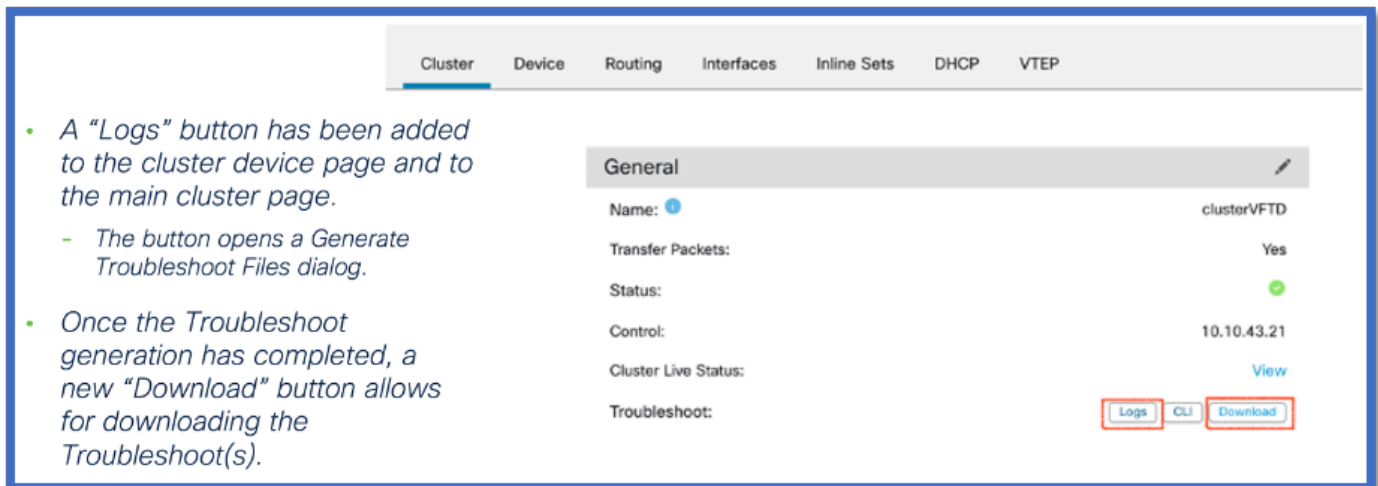
Task manager shows

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

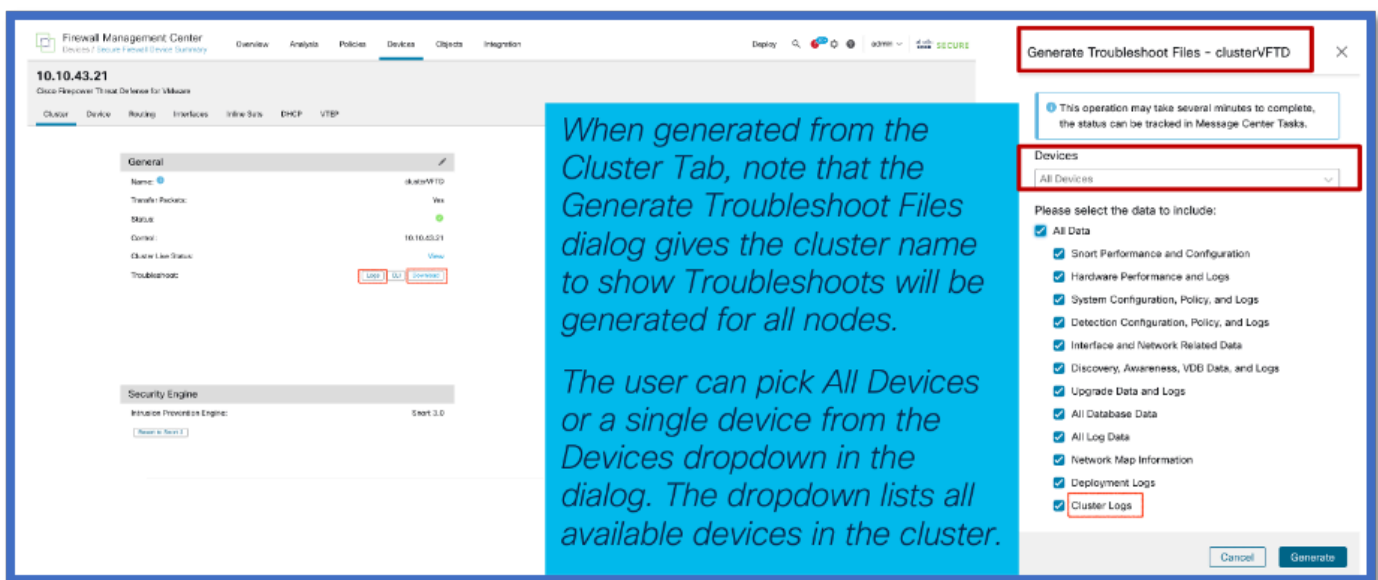
Probleemoplossing Trigger en Download-knop beschikbaar in de tabbladen Apparaat en Cluster

Eenvoudiger generatie van clusterprobleemoplossing

- 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).



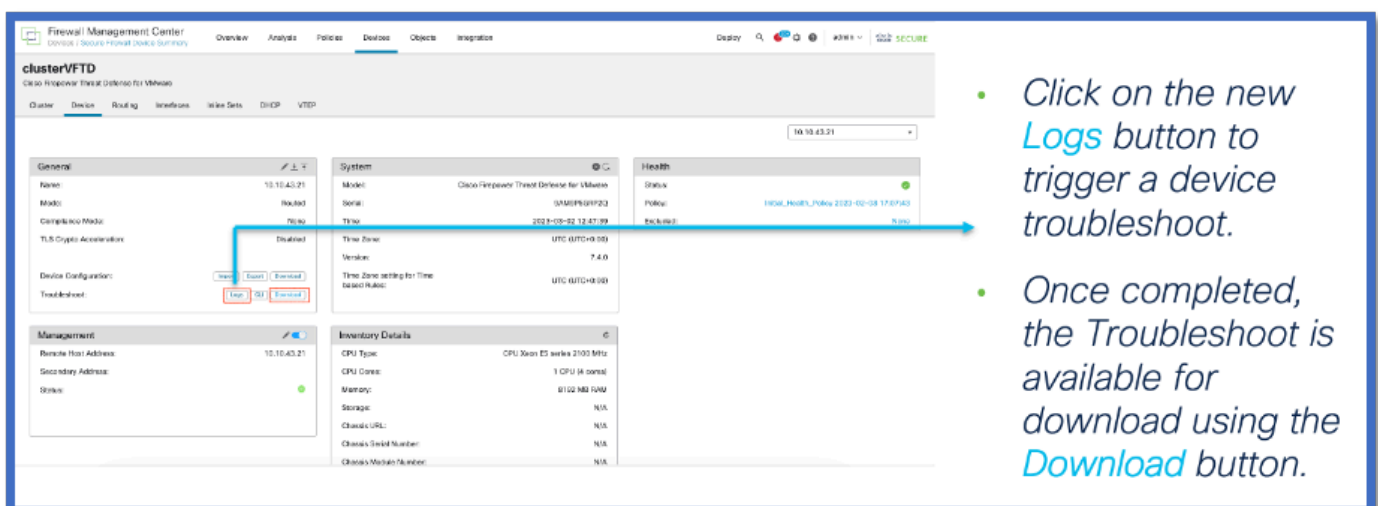
Generatie van clusterprobleemoplossing



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.

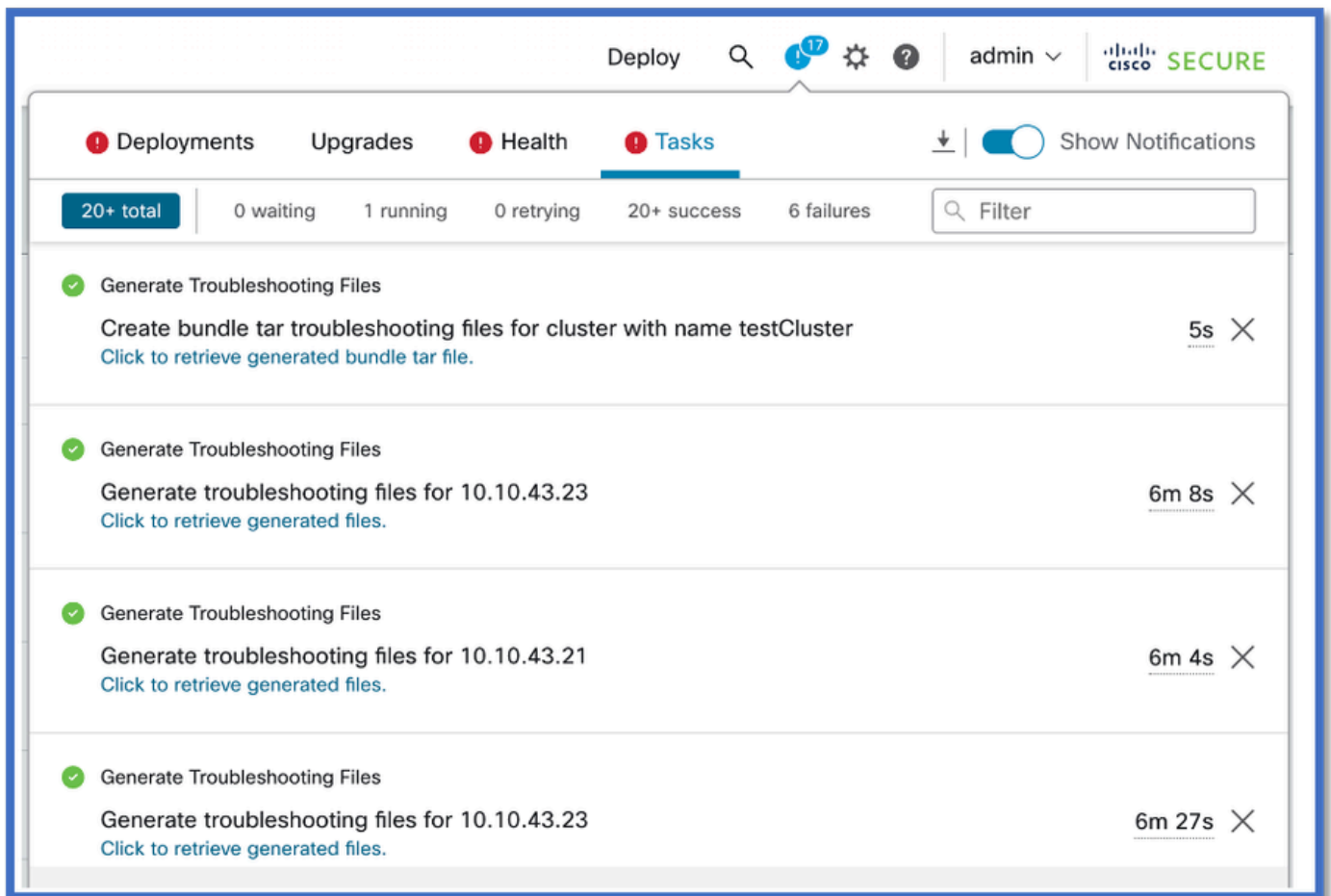
Generatie van probleemoplossing voor knooppunt (apparaat)



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

Melding van Cluster Probleemoplossing Generatie voltooid

De taakmanager toont de voortgang van de probleemoplossingsgeneratie voor elk knooppunt in het cluster. Wacht daarop voordat u op Downloaden klikt.



The screenshot displays the Cisco Secure task manager interface. At the top, there is a navigation bar with 'Deploy', a search icon, a notification bell with '17', a settings gear, a help icon, and a user profile 'admin'. The main header includes tabs for 'Deployments', 'Upgrades', 'Health', and 'Tasks', with 'Tasks' selected. A 'Show Notifications' toggle is also present. Below the header, a summary bar shows '20+ total' tasks, with sub-counts for '0 waiting', '1 running', '0 retrying', '20+ success', and '6 failures'. A 'Filter' search box is available. The task list shows four completed tasks, each with a green checkmark and a close button (X). The tasks are: 'Generate Troubleshooting Files' for cluster 'testCluster' (5s), 'Generate Troubleshooting Files' for IP '10.10.43.23' (6m 8s), 'Generate Troubleshooting Files' for IP '10.10.43.21' (6m 4s), and 'Generate Troubleshooting Files' for IP '10.10.43.23' (6m 27s). Each task includes a link to 'Click to retrieve generated files.'

Vraag en antwoord

Q: In Azure is het verlaagd maar verhoogd in AWS voor MTU?

A: Voor de nieuwe MTU-waarden in openbare clouds wordt in Azure de aanbevolen MTU verlaagd, maar in AWS wordt deze verhoogd.

V: Tijdens upgrade als MTU automatisch wordt gewijzigd - is er een Syslog-vermelding?

A: Nee, er is op dit moment geen inzending van Syslog gemaakt. We kunnen er nog eens naar kijken als dat nodig is.

V: Waar wordt de MTU-waarde van elk knooppunt weergegeven?

A: Laat de MTU-waarde zien als een kolom op de pagina Apparaatbeheer > Interfaces, op het tabblad Cluster.

V: Is deze fout zichtbaar omdat de Switch niet is ingesteld of omdat het andere knooppunt niet is ingesteld?

A: Nee, het is een waarschuwingsbericht als voorzorgsmaatregel die de hele tijd wordt weergegeven aan de gebruiker.

Q: Welke opdracht - toon cluster - toont de grootte MTU?

A: CCL ping staat standaard en wordt in de CLI-standaardwaarden weergegeven.

Q: In het geval van AWS, kunnen wij de stappen op hoe te verhogen MTU op switch documenteren?

A: Voor tech pubs om te controleren.

Q: Voor HW - u alleen vermeld 3100 reeks - wat over 4K/9K/2K/1K?

A: Clustering op 9300, 4100, 3100 en alleen virtueel. 3100 kan worden gedaan van het VCC, maar 4100 en 9300 clusters worden gedaan in de chassisbeheerder, niet VCC.

V: Moet u van het VCC inzetten om de wijzigingen van kracht te laten worden, na de upgrade van het apparaat?

A: Ja, moet na de upgrade worden geïmplementeerd. U moet de aanbevolen MTU-waarden gebruiken.

V: Gaan we de gebruiker waarschuwen dat MTU wordt gewijzigd, alsof FTD het midden is van een pad waar GRE-tunnel gebouwd wordt, zou de gebruiker de tunnel zien flappen of daalde?

A: Dat staat in de documentatie. Kan aan waarschuwingsbericht werken. De knooppunten worden aangepast om de controleknooppunt te selecteren. De switch zou aan de nieuwe waarden moeten worden aangepast. De waarde wordt gewijzigd nadat het besturingsknooppunt is bijgewerkt. De waarde MTU wordt verzonden door controle.

V: Gaan we het FTD-apparaat opnieuw opstarten als we na de upgrade de MTU veranderen?

A: Geen expliciete reboot wordt geactiveerd op FTD op upgrade wanneer MTU-waarden worden gewijzigd.

Revisiegeschiedenis

Herziening	Publicatiedatum	Opmerkingen
2.0	17 jul.-2024	Toegevoegd Alt Text. Bijgewerkte opmaak.
1.0	17 jul.-2024	Eerste vrijgave

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.