

Configuration de la facilité de maintenance du cluster dans Firewall Management Center 7.4

Table des matières

[Introduction](#)

[Nouveautés de Cisco](#)

[Conditions préalables, plates-formes prises en charge, licences](#)

[Plates-formes logicielles et matérielles minimales](#)

[Composants utilisés](#)

[Diagnostics de liaison CCL](#)

[Avertissement MTU de l'interface de liaison de contrôle de cluster dans la page Récapitulatif du cluster](#)

[Problème](#)

[Recommandations de taille MTU par plate-forme](#)

[Solution](#)

[Test Ping CCL dans l'état actif du cluster](#)

[Vérifier la connectivité CCL](#)

[Solution](#)

[Ajout de tailles CCL MTU pour le cloud public](#)

[CLI disponibles dans FMC](#)

[Inviter CLI de la ligne de périphérique disponible dans l'onglet Périphérique/Cluster](#)

[Exécuter les CLI de ligne de cluster depuis FMC](#)

[CLI couramment utilisées affichées par défaut](#)

[CLI de cluster prédéfinis](#)

[Saisie manuelle des commandes disponibles](#)

[Génération de dépannages](#)

[Génération automatique de dépannage en cas d'échec de jonction de noeud](#)

[Dépannage du déclencheur et bouton de téléchargement disponibles dans les onglets Périphérique et Cluster](#)

[Génération plus facile de dépannages de cluster](#)

[Génération de dépannage de cluster](#)

[Génération de dépannage de noeud \(périphérique\)](#)

[Notification de la génération du dépannage de cluster terminée](#)

[Questions et réponses](#)

[Historique de révision](#)

Introduction

Ce document décrit comment utiliser les améliorations de la facilité de maintenance dans FMC 7.4

Nouveautés de Cisco

- Diagnostic de la liaison CCL (Cluster Control Link) et assistance pour vérifier que les paramètres sont corrects.
- Les interfaces CLI de la ligne de cluster sont désormais visibles dans Firewall Management Center (FMC).
- Dépannage de la génération
 - Peut désormais être généré en une seule fois pour tous les périphériques d'une grappe.
 - La génération du dépannage est automatique si un noeud ne parvient pas à joindre un cluster.
 - Dépannez la génération et la navigation à partir de l'onglet Périphériques > Cluster/Périphérique.

Conditions préalables, plates-formes prises en charge, licences

Plates-formes logicielles et matérielles minimales

Application et version minimale	Périphériques gérés	Version minimale du périphérique géré prise en charge requise	Remarques
Pare-feu sécurisé 7.4	Tous les qui prennent en charge le clustering sur FTD Seule l'amélioration « Génération de dépannages » nécessite que la version FTD soit 7.4 et supérieure	<ul style="list-style-type: none"> · FMC On-Prem + FMC REST API · FMC fourni dans le cloud 	Il s'agit d'une fonctionnalité FMC, de sorte que la configuration peut être appliquée à n'importe quel périphérique que FMC 7.4 peut gérer.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco Firewall Management Center (FMC) 7.4
- Cisco Firepower Threat Defense (FTD) version 7.4 ou ultérieure.

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Diagnostiques de liaison CCL

Avertissement MTU de l'interface de liaison de contrôle de cluster dans la page Récapitulatif du cluster

Problème

- La mise en grappe nécessite un MTU plus élevé pour la liaison de contrôle de grappe que les interfaces de données.
- Souvent, vous ne définissez pas le MTU à une valeur suffisamment élevée, ce qui entraîne des problèmes de fiabilité.
- La recommandation est que le MTU de la liste de contrôle d'accès doit être supérieur de 100 ou 154 octets au MTU maximal de l'interface de données, basé sur la plate-forme, pour synchroniser l'état du cluster sur les noeuds.

CCL MTU = (MTU d'interface de données maximum) + 100 |154

Par exemple, pour un périphérique FTDv, si 1700 octets est la valeur MTU maximale de l'interface de données, la valeur de MTU de l'interface CCL serait définie sur 1854 :

$$1\ 854 = 1\ 700 + 154$$

Recommandations de taille MTU par plate-forme

Plateforme	Exemple de MTU d'interface de données maximale	Ajouter	Paramètre total recommandé pour MTU pour la liaison CCL
Sec FW, série 3100	1700	100	1800
FTDv	1700	154	1854

Solution

- Lors de la création d'un cluster, la valeur MTU de la liaison CCL est automatiquement définie sur la valeur recommandée sur l'interface.
Définissez la configuration côté commutateur pour qu'elle corresponde à cette valeur.
- Exemple de message d'avertissement :
La mise en grappe nécessite un MTU plus élevé pour la liaison de contrôle de grappe. La MTU maximale actuelle de l'interface de données est de 1 500 octets ; la MTU recommandée de la liaison de contrôle de cluster est de 1 654 octets ou plus. Avant de continuer, assurez-vous que les commutateurs connectés correspondent aux MTU pour les interfaces de données et la liaison de contrôle de cluster, sinon la formation du cluster échouerait.
- Si la configuration côté commutateur pour l'interface CCL ne correspond pas à cette valeur,

le périphérique ne parvient pas à joindre le cluster.

Add Cluster Wizard

1 Configuration — 2 Summary

▲ 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.

Cancel Previous Save

Test Ping CCL dans l'état actif du cluster

Vérifier la connectivité CCL

- Nécessité d'un provisionnement utilisateur pour vérifier la connectivité CCL avec la taille de paquet MTU CCL

Solution

Cluster Status

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

Nodes details (3) Refresh Reconcile All Enter node name

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

Summary History **OCL Ping**

```
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)
```

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

Dated: 18:38:41 | 01 Mar 2023 Close

Ajout de tailles CCL MTU pour le cloud public

Valeurs MTU de cluster AWS et Azure

Il existe de nouvelles valeurs recommandées de MTU de CCL et d'interface de données pour les clusters FTDv de cloud public 7.4.

	MTU CCL recommandé dans 7.3	Recommandé CCL MTU dans 7.4	MTU d'interface de données recommandée dans 7.3	Recommandé MTU de l'interface de données dans 7.4
Cluster NLB Azure	1554	1454	1400	1300
Cluster Azure GWLb	1554	1454	1454	1374
Cluster GWLB AWS	1960	1980	1806	1826

FMC met à jour le MTU de la CCL et de l'interface de données aux valeurs recommandées après la mise à niveau d'un cluster vers la version 7.4.

CLI disponibles dans FMC

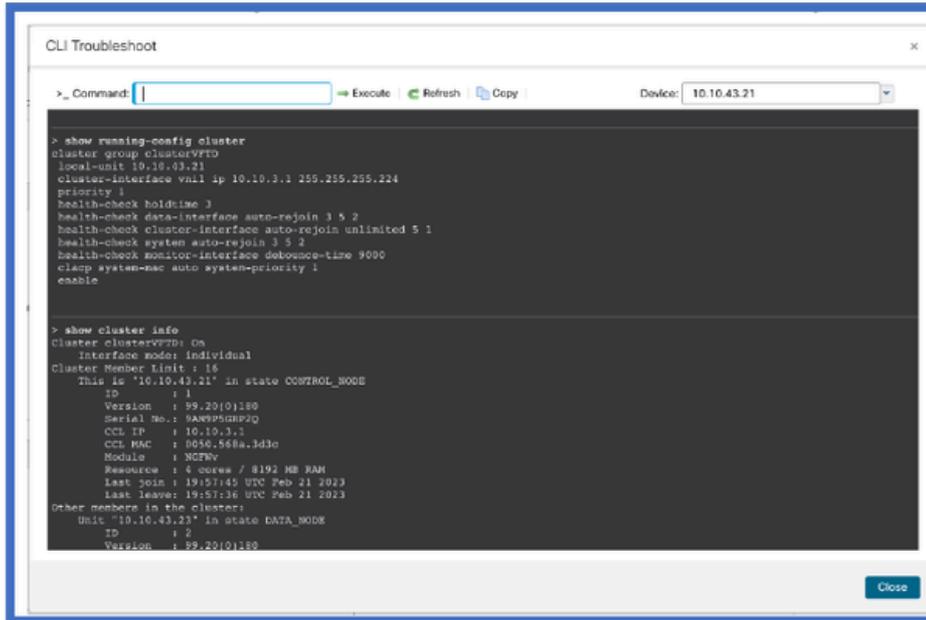
Invite CLI de la ligne de périphérique disponible dans l'onglet Périphérique/Cluster

Exécuter les CLI de ligne de cluster depuis FMC

- Il est désormais possible d'exécuter des CLI de dépannage LINA de cluster à partir de FMC.

The screenshot shows the FMC configuration page for a cluster. The 'General' section includes fields for Name, Transfer Packets, Status, Control, and Cluster Use Status. A red box highlights a 'CLI' button in the 'Troubleshoot' area. A blue arrow points from this button to a text box on the right that reads: "A CLI button is newly added in the General section on both the Cluster and Device Tabs".

CLI couramment utilisées affichées par défaut



```
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 vml 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
cleanup 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.: 9AN9P5GHPJQ
CCL IP : 10.10.3.1
CCL MAC : 0950.568a.3d3c
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 : 99.20(0)180
```

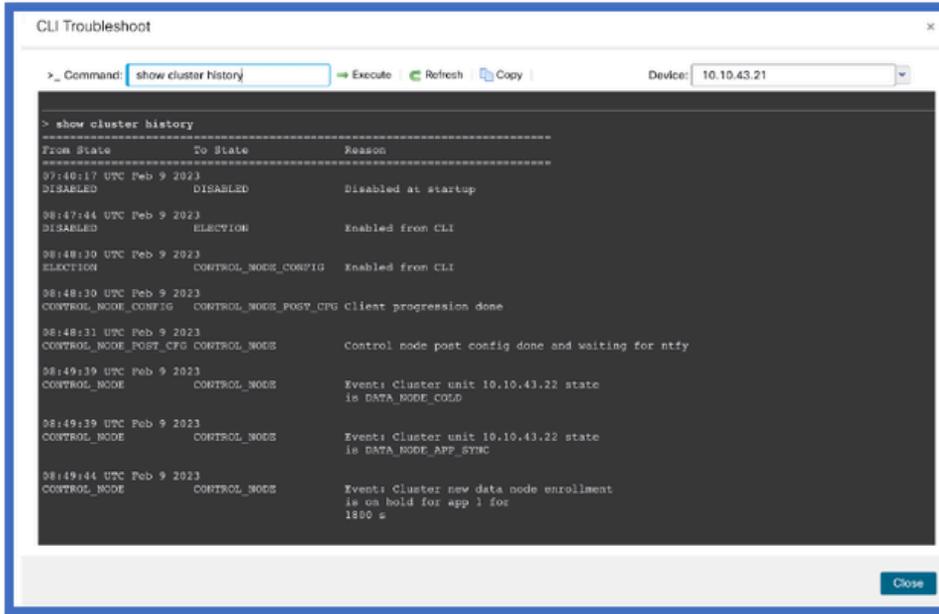
- Executes a set of predefined CLIs for cluster troubleshooting on the device that is selected in the Device selection dropdown.
- The refresh button re-runs the commands.
- Copy button can be used to copy the CLI output

CLI de cluster prédéfinis

- Les CLI exécutées par défaut sont les suivantes :

```
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
```

Saisie manuelle des commandes disponibles



The screenshot shows a terminal window titled 'CLI Troubleshoot' with the command 'show cluster history' entered. The output displays a table of state transitions for a cluster unit. The table has columns for 'From State', 'To State', and 'Reason'. The output shows the cluster unit starting as 'DISABLED', then transitioning to 'ELECTION' and 'CONTROL_NODES_CONFIG', and finally to 'CONTROL_NODES_POST_CFG'. It also shows events for 'DATA_NODE_COLD' and 'DATA_NODE_APP_SYNC'.

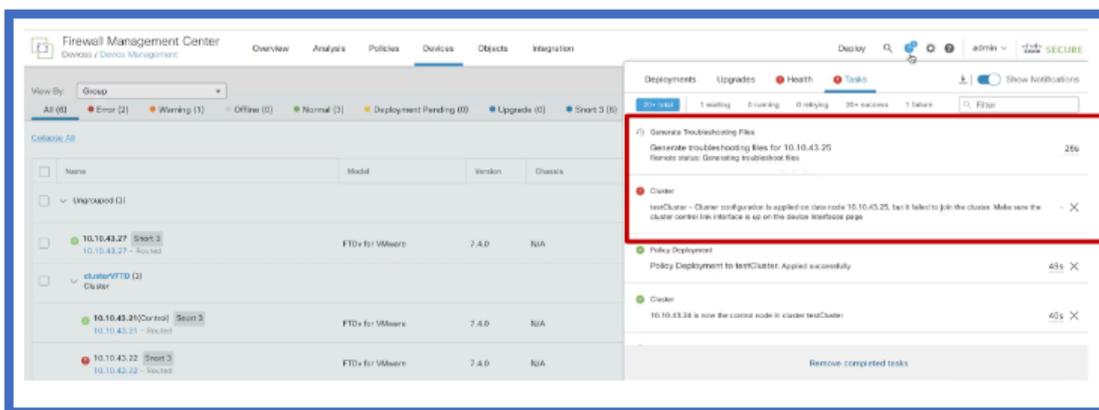
From State	To State	Reason
DISABLED	DISABLED	Disabled at startup
DISABLED	ELECTION	Enabled from CLI
ELECTION	CONTROL_NODES_CONFIG	Enabled from CLI
CONTROL_NODES_CONFIG	CONTROL_NODES_POST_CFG	client progression done
CONTROL_NODES_POST_CFG	CONTROL_NODES	Control node post config done and waiting for ntpy
CONTROL_NODES	CONTROL_NODES	Event: Cluster unit 10.10.43.22 state is DATA_NODE_COLD
CONTROL_NODES	CONTROL_NODES	Event: Cluster unit 10.10.43.22 state is DATA_NODE_APP_SYNC
CONTROL_NODES	CONTROL_NODES	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.

Génération de dépannages

Génération automatique de dépannage en cas d'échec de jonction de noeud

- Lorsqu'un noeud ne parvient pas à rejoindre le cluster, un dépannage de périphérique est automatiquement généré.
- Une notification s'affiche dans le Gestionnaire des tâches.



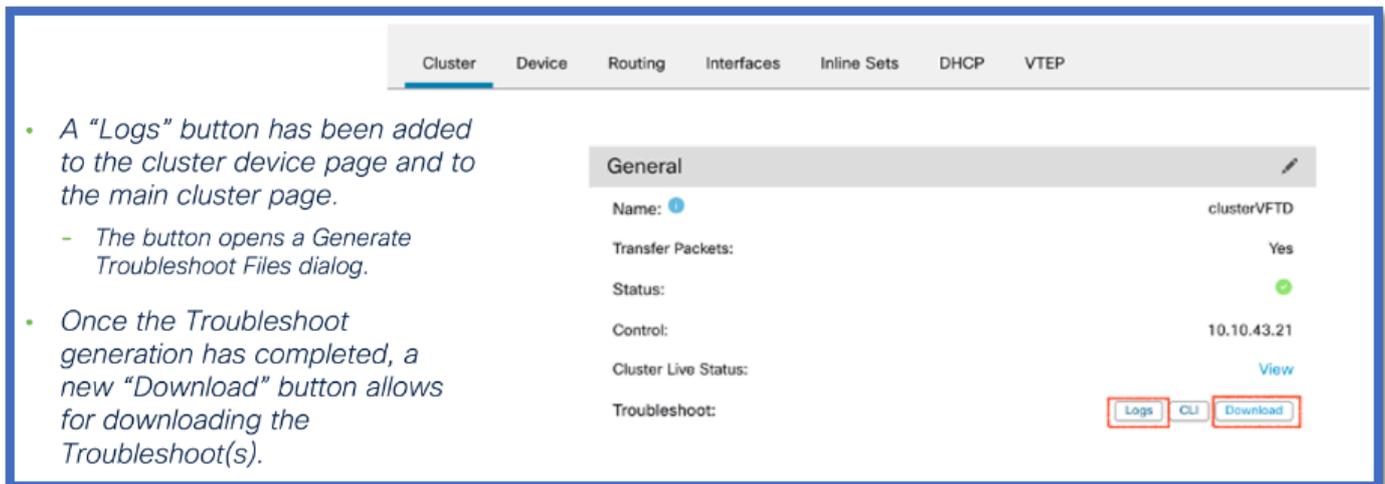
The screenshot shows the 'Task manager' section of the Firewall Management Center. A notification is highlighted in a red box, indicating a 'Cluster' task that failed to join the cluster. The notification text reads: 'Cluster - testCluster - Cluster configuration is applied on data node 10.10.43.25, but it failed to join the cluster. Make sure the cluster control interface is up on the device interface page.' The notification also shows a 'Generate Troubleshooting Files' button and a 'Remove completed tasks' button.

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

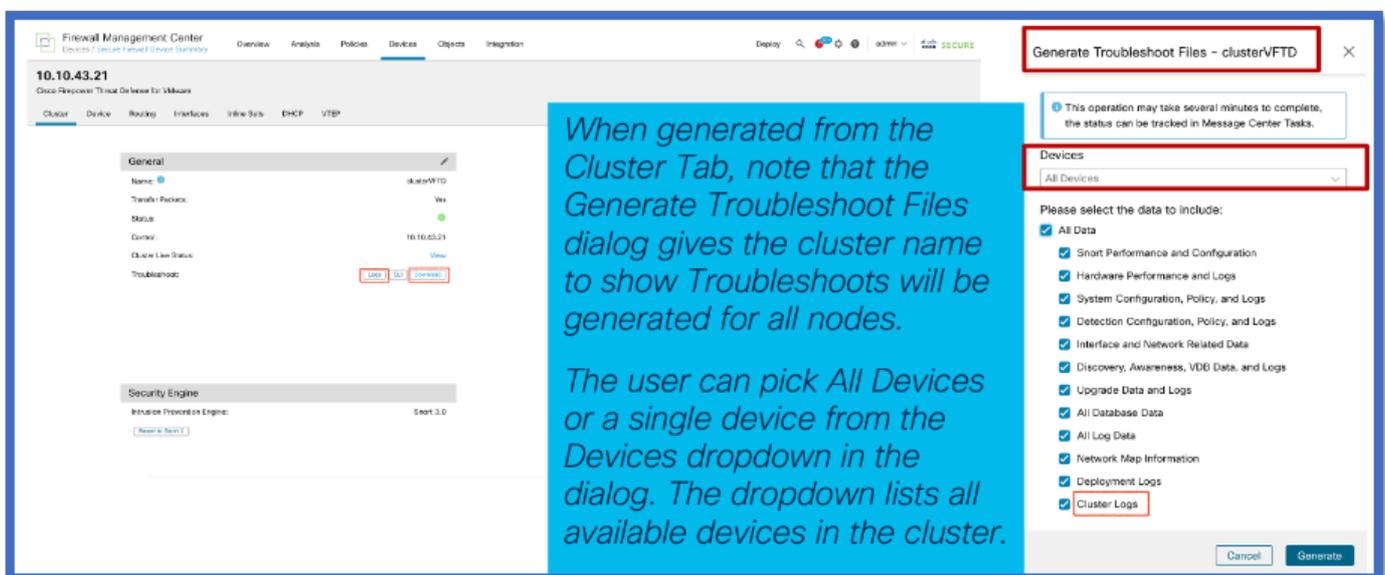
Dépannage du déclencheur et bouton de téléchargement disponibles dans les onglets Device et Cluster

Génération plus facile de dépannages de cluster

- 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).



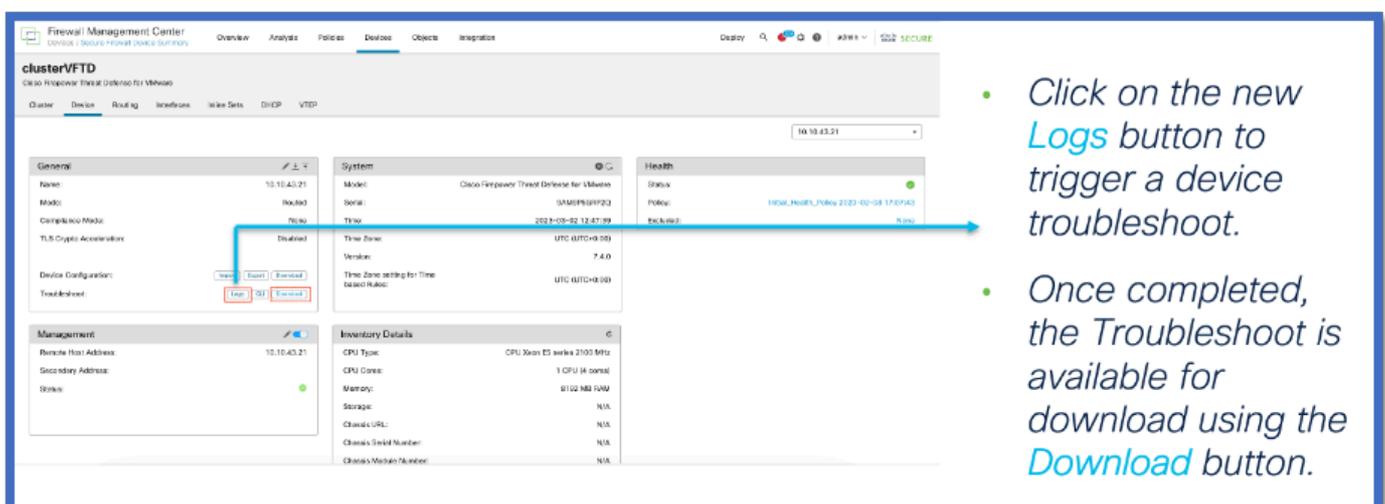
Génération de dépannage de cluster



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.

Génération de dépannage de noeud (périphérique)



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

Notification de la génération du dépannage de cluster terminée

Le Gestionnaire des tâches affiche la progression de la génération du dépannage pour chaque noeud du cluster. Attendez-le avant de cliquer sur Télécharger.

The screenshot shows the Cisco Secure Task Manager interface. The top navigation bar includes 'Deploy', search, settings, and user 'admin'. The main navigation bar shows 'Deployments', 'Upgrades', 'Health', and 'Tasks' (selected). A summary bar indicates '20+ total' tasks, with '0 waiting', '1 running', '0 retrying', '20+ success', and '6 failures'. A 'Filter' search box is also present. The task list shows four completed tasks for generating troubleshooting files for a cluster named 'testCluster'.

Task Name	Description	Duration
Generate Troubleshooting Files	Create bundle tar troubleshooting files for cluster with name testCluster Click to retrieve generated bundle tar file.	5s
Generate Troubleshooting Files	Generate troubleshooting files for 10.10.43.23 Click to retrieve generated files.	6m 8s
Generate Troubleshooting Files	Generate troubleshooting files for 10.10.43.21 Click to retrieve generated files.	6m 4s
Generate Troubleshooting Files	Generate troubleshooting files for 10.10.43.23 Click to retrieve generated files.	6m 27s

Questions et réponses

Q : Dans Azure, il a diminué mais augmenté dans AWS pour MTU ?

R : Pour les nouvelles valeurs MTU dans les clouds publics, dans Azure, le MTU recommandé est réduit, mais il est augmenté dans AWS.

Q : Lors de la mise à niveau si MTU est modifié automatiquement - y a-t-il une entrée Syslog ?

R : Non, il n'y a pas d'entrée Syslog pour le moment. Nous pouvons y revenir si cela s'avère nécessaire.

Q : Où la valeur MTU de chaque noeud est-elle affichée ?

R : Affichez la valeur MTU sous la forme d'une colonne sur la page Device Management > interfaces, dans l'onglet Cluster.

Q : Cet échec est-il visible parce que le commutateur n'est pas défini ou parce que l'autre noeud n'est pas défini ?

R : Non, c'est un message d'avertissement comme précaution qui est affiché tout le temps à l'utilisateur.

Q : Quelle commande - show cluster - affiche la taille de MTU ?

R : La commande ping CCL est utilisée par défaut et apparaît dans les valeurs par défaut de l'interface de ligne de commande.

Q : Dans le cas d'AWS, pouvons-nous documenter les étapes sur la façon d'augmenter la MTU sur le commutateur ?

R : Pour les pubs de technologie à vérifier.

Q : Pour le matériel - vous n'avez répertorié que les gammes 3100 - qu'en est-il des gammes 4K/9K/2K/1K ?

R : Mise en grappe sur 9300, 4100, 3100 et virtuel uniquement. 3100 peut être effectué à partir de FMC, mais les clusters 4100 et 9300 sont effectués dans le gestionnaire de châssis, pas FMC.

Q : Devez-vous déployer à partir du FMC pour que les modifications prennent effet, après la mise à niveau du périphérique ?

R : Oui, besoin de déployer après la mise à niveau. Vous devez utiliser les valeurs MTU recommandées.

Q : Fournissons-nous un message d'avertissement à l'utilisateur indiquant que la MTU a changé, comme si FTD était au milieu du chemin où le tunnel GRE a été construit, l'utilisateur verrait-il le tunnel basculer ou tomber en panne ?

R : Il est dans la documentation. Peut travailler sur les messages d'avertissement. Les noeuds s'ajustent au noeud de contrôle. Le commutateur doit être ajusté aux nouvelles valeurs. La valeur est modifiée après la mise à niveau du noeud de contrôle. La valeur MTU est envoyée par le contrôle.

Q : Allons-nous redémarrer le périphérique FTD si, après la mise à niveau, nous modifions le MTU ?

R : Aucun redémarrage explicite n'est déclenché sur FTD lors de la mise à niveau lorsque les valeurs MTU sont modifiées.

Historique de révision

Révision	Date de publication	Commentaires
2.0	17-juil-2024	Texte de remplacement ajouté. Mise en forme mise à jour.
1.0	17-juil-2024	Première publication

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.