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

Table des matières

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	· 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.

Diagnostics 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

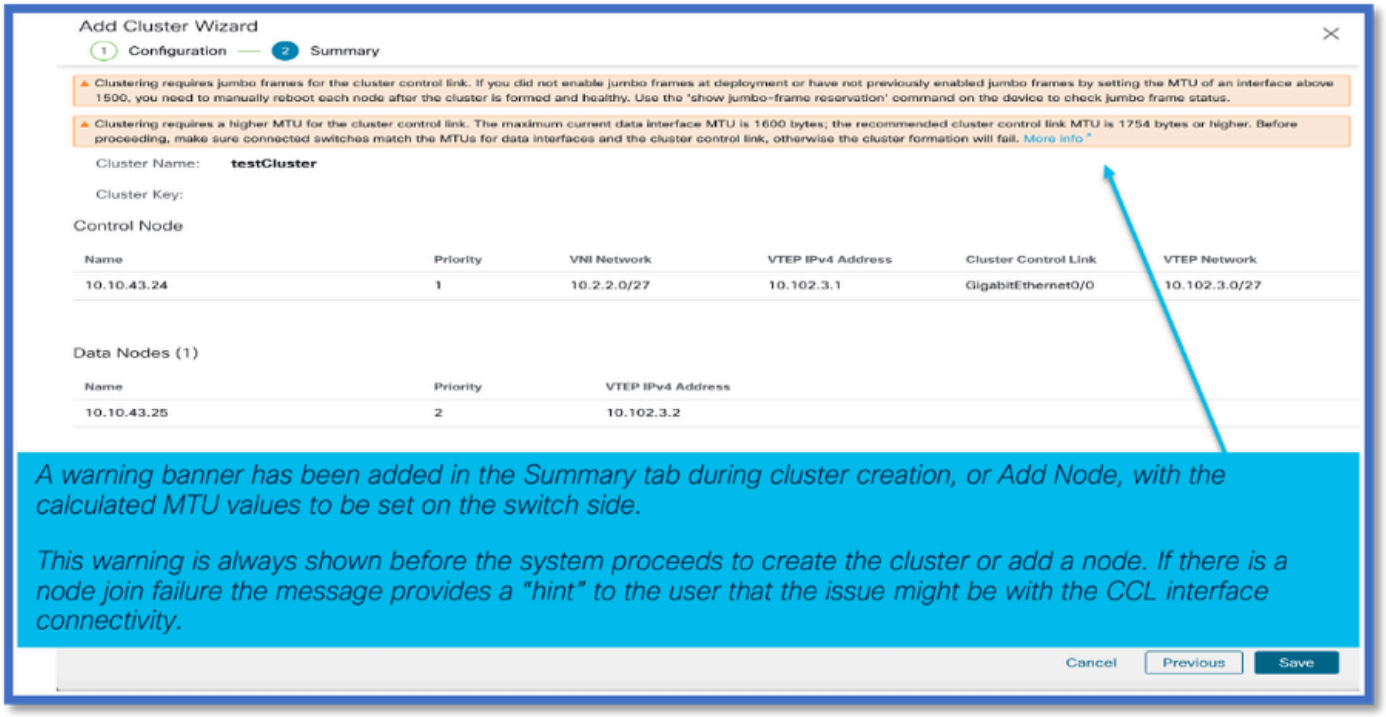
Recommandations de taille MTU par plate-forme

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.

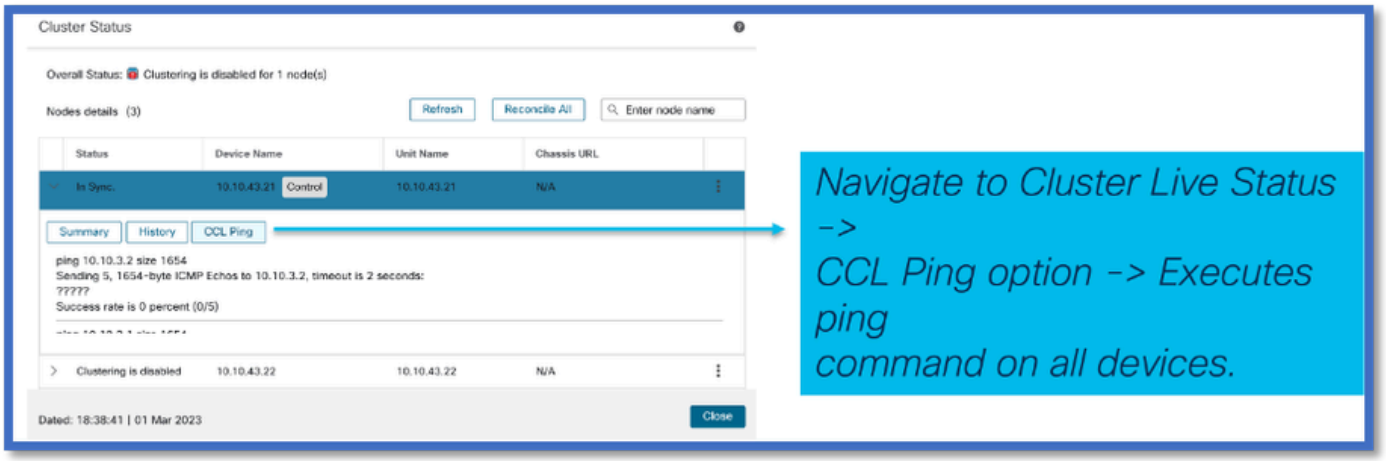


Test Ping CCL dans l'état actif du cluster

Vérifier la connectivité CCL

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

Solution



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

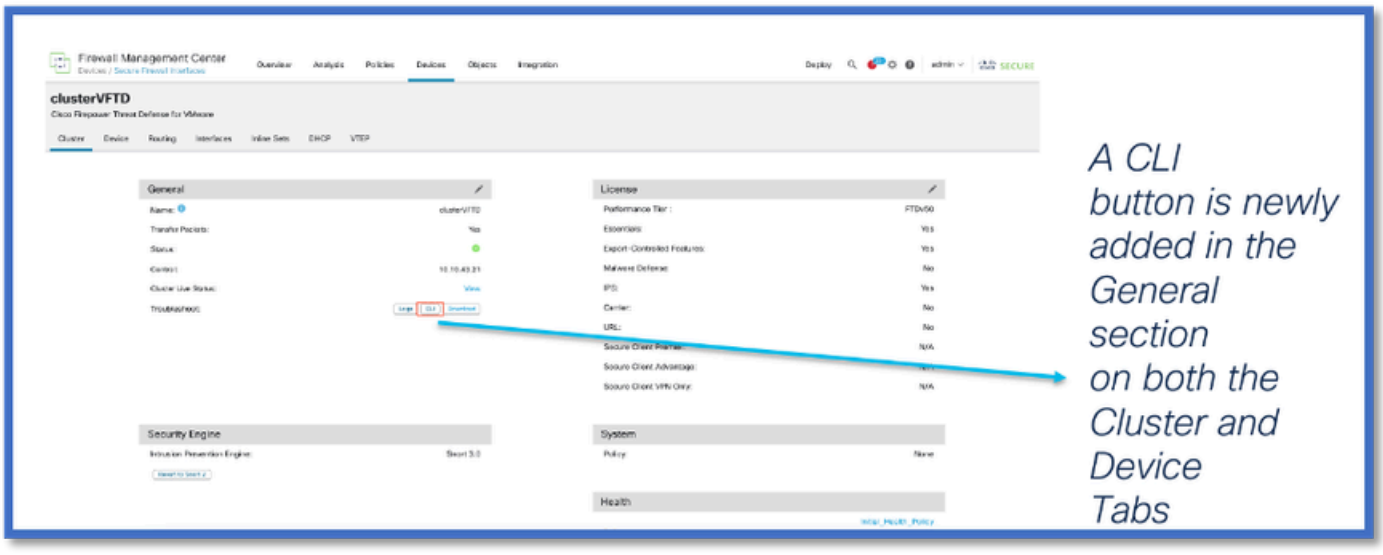
FMC met à jour le MTU de la CCL et de l'interface de données aux valeurs recommandées après la mise à niveau d'un cluster vers la version 7.4.

CLI disponibles dans FMC

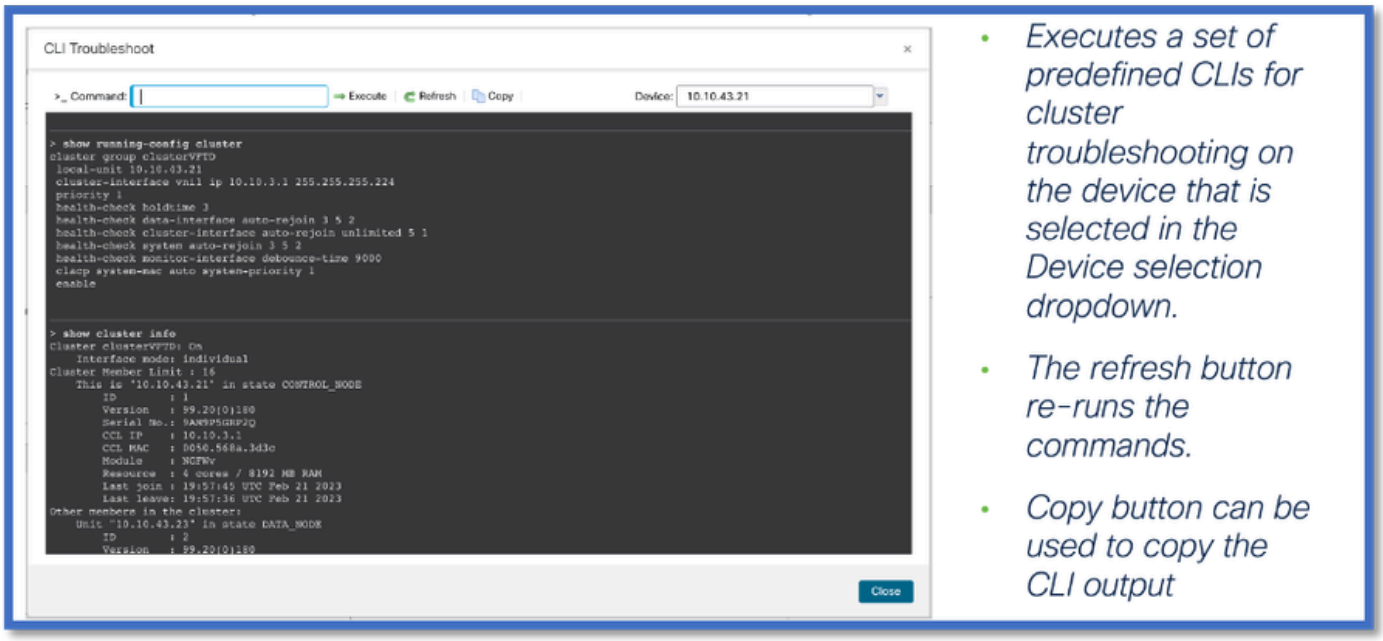
Invite CLI de la ligne de périphérique disponible dans l'onglet Périphérique/Cluster

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.



CLI couramment utilisées affichées par défaut



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

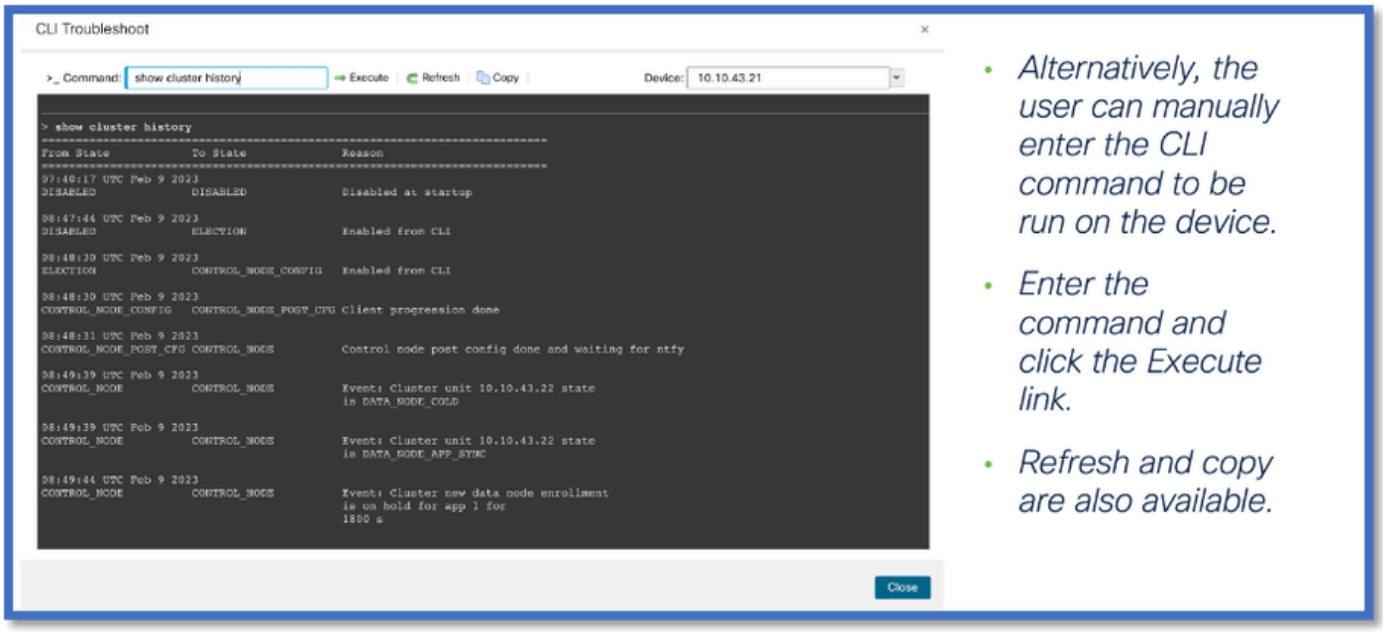
  show blocks

  show cpu detailed

  show interface <ccl_interface>

  ping <ccl_ip> size <ccl_mtu> repeat 2

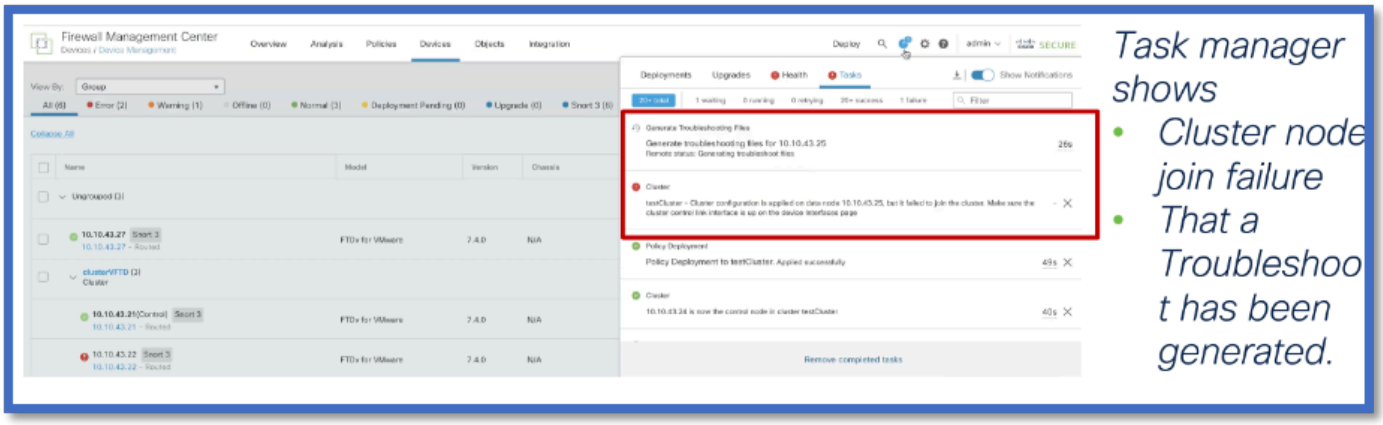
Saisie manuelle des commandes disponibles



Génération de dépannages

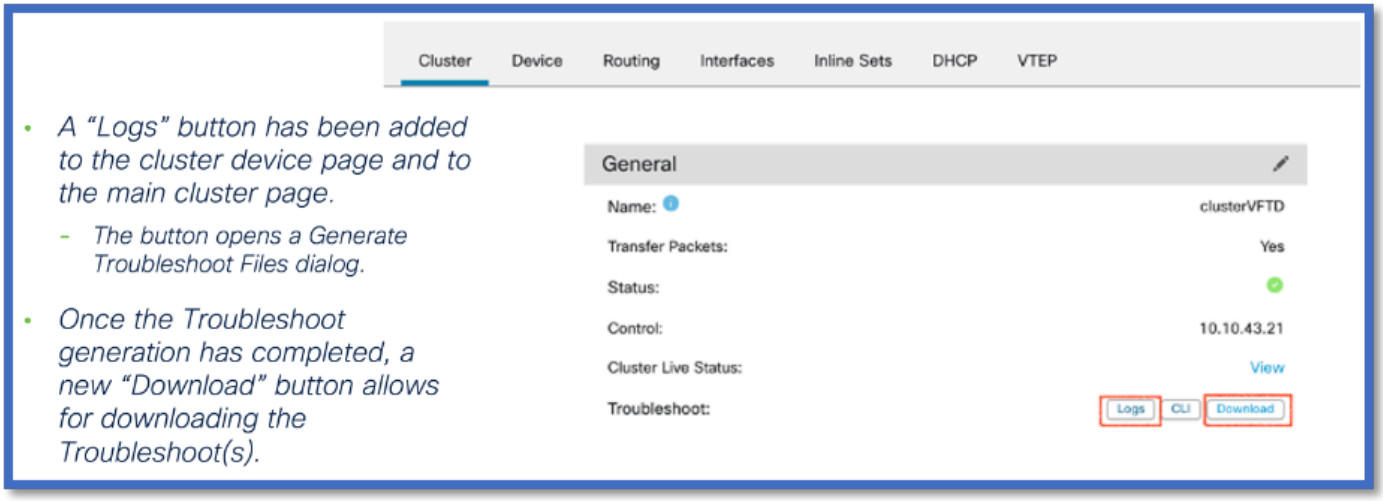
Génération automatique de dépannage en cas d'échec de jonction de noeud

- 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.

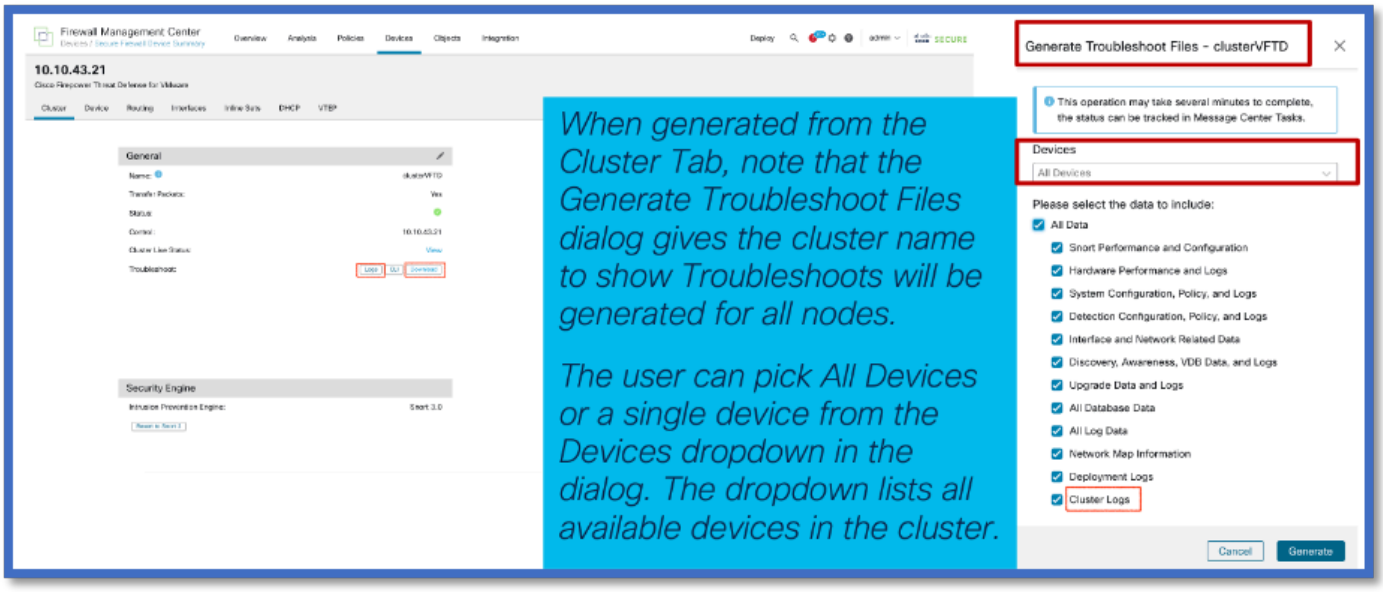


Dépannage du déclencheur et bouton de téléchargement disponibles dans les onglets Device et Cluster

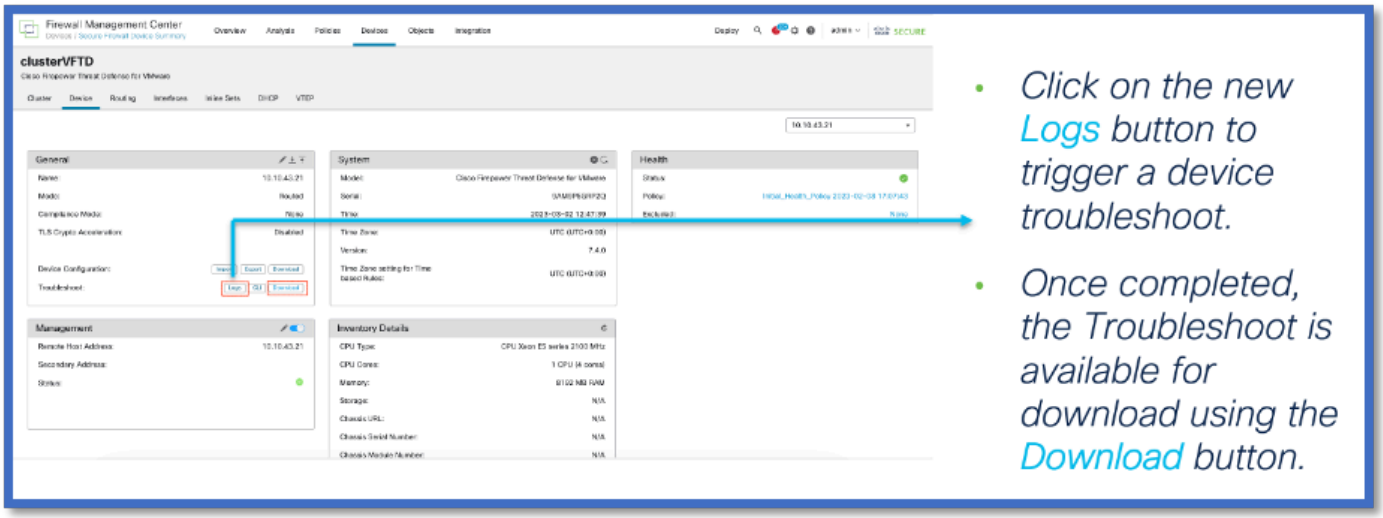
Génération plus facile de dépannages de cluster



Génération de dépannage de cluster

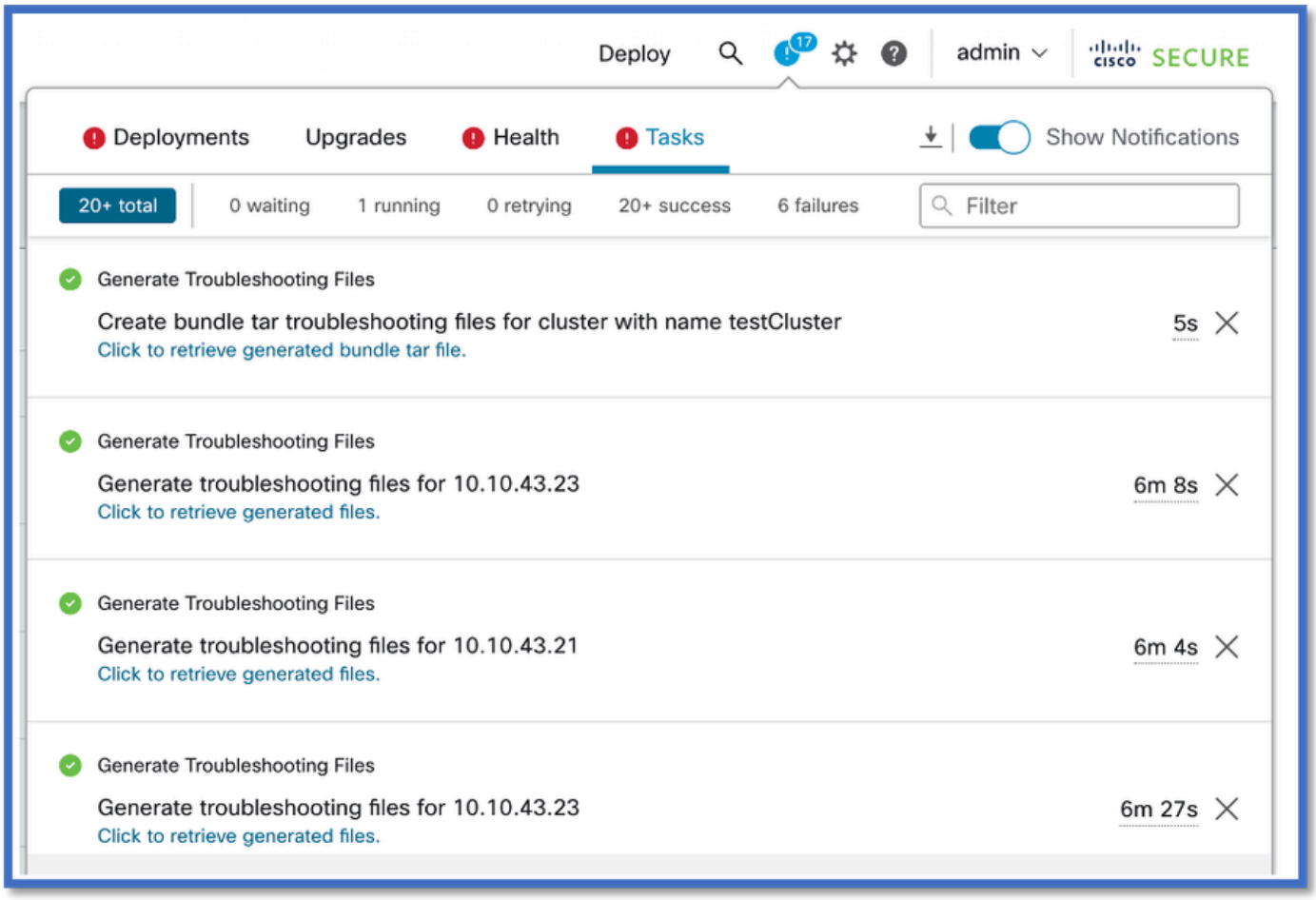


Génération de dépannage de noeud (périphérique)



Notification de la génération du dépannage de cluster terminée

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



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.