

Firewall Management Center 7.4でのクラスタサービスアビリティの改善の設定

内容

[はじめに](#)

[最新情報](#)

[前提条件、サポート対象プラットフォーム、ライセンス](#)

[最低限のソフトウェアおよびハードウェアプラットフォーム](#)

[使用するコンポーネント](#)

[CCLリンク診断](#)

[Cluster SummaryページのCluster Control Link Interface MTU警告](#)

[問題](#)

[プラットフォームごとの推奨MTUサイズ](#)

[解決方法](#)

[クラスタのライブステータスでのCCL pingテスト](#)

[CCL接続の確認](#)

[解決方法](#)

[パブリッククラウド用のCCL MTUサイズの追加](#)

[FMCで使用可能なCLI](#)

[デバイス/クラスタタブで使用可能なデバイスラインCLIプロンプト](#)

[FMCからのクラスタラインCLIの実行](#)

[一般的に使用されるCLI \(デフォルトで表示\)](#)

[定義済みクラスタCLI](#)

[使用可能なコマンドの手動入力](#)

[トラブルシューティングの生成](#)

[ノード結合失敗時の自動トラブルシューティング生成](#)

[デバイスタブとクラスタタブで使用可能な「トリガー」および「ダウンロード」ボタンのトラブルシューティング](#)

[クラスタトラブルシューティングの生成の簡素化](#)

[クラスタトラブルシューティングの生成](#)

[ノード \(デバイス\) のトラブルシューティングの生成](#)

[クラスタトラブルシューティング生成の通知の完了](#)

[Q & A](#)

[改訂履歴](#)

はじめに

このドキュメントでは、FMC 7.4でのサービスアビリティの向上の使用方法について説明します。

最新情報

- Cluster Control Link(CCL)リンクの診断と、設定が正しいことを確認するためのサポート。
- これで、Cluster Lina CLIがFirewall Management Center(FMC)で表示できるようになりました。
- 生成のトラブルシューティング
 - クラスタ内のすべてのデバイスに対して一度に生成できるようになりました。
 - トラブルシューティングの生成は、ノードがクラスタへの参加に失敗した場合に自動的に行われます。
 - Devices > Cluster/Deviceタブからのトラブルシューティングの生成とナビゲーション

前提条件、サポート対象プラットフォーム、ライセンス

最低限のソフトウェアおよびハードウェアプラットフォーム

アプリケーションと最小バージョン	管理対象デバイス	サポートされる管理対象デバイスの最小バージョンが必要	注意事項
Cisco Secure Firewall 7.4	FTDでのクラスタリングをサポートするすべて 「トラブルシューティングの生成」機能の拡張にのみ、FTDバージョン7.4以降が必要です	<ul style="list-style-type: none"> • FMCオンプレミス+FMC REST API • クラウド型FMC 	これはFMCの機能なので、FMC 7.4で管理できるすべてのデバイスに設定を適用できます。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- 7.4を実行するCisco Firewall Management Center(FMC)
- 7.4以降を実行するCisco Firepower Threat Defense(FTD)。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

CCLリンク診断

Cluster SummaryページのCluster Control Link Interface MTU警告

問題

- クラスタリングでは、クラスタ制御リンクにデータインターフェイスよりも大きなMTUが

必要です。

- MTUを十分に高い値に設定しないことが多いため、信頼性に問題が生じます。
- ノード間でクラスタ状態を同期させるには、プラットフォームに基づいて、CCL MTUを最大データインターフェイスMTUよりも100または154バイト多くする必要があります。

$$\text{CCL MTU} = (\text{最大データインターフェイスMTU}) + 100 | 154$$

たとえば、FTDvデバイスの場合、1700バイトが最大データインターフェイスMTUであれば、CCLインターフェイスMTUの値は1854に設定されます。

$$1854 = 1700 + 154$$

プラットフォームごとの推奨MTUサイズ

Platform	最大データインターフェイスMTUの例	追加	CCLリンクのMTUの推奨合計設定
Sec FW 3100シリーズ	1700	100	1800
FTDv	1700	154	1854

解決方法

- クラスタが作成されると、CCLリンクのMTU値は、インターフェイス上で自動的に推奨値に設定されます。
スイッチ側の設定をこの値に一致させます。
- 警告メッセージの例：
クラスタリングでは、クラスタ制御リンクに高いMTUが必要です。現在のデータインターフェイスMTUの最大値は1500バイトです。推奨されるクラスタ制御リンクMTUは1654バイト以上です。先に進む前に、接続されているスイッチがデータインターフェイスとクラスタ制御リンクのMTUに一致していることを確認してください。一致していないと、クラスタの形成に失敗します。
- CCLインターフェイスのスイッチ側の設定がこの値と一致しない場合、デバイスはクラスタに参加できません。

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

クラスタのライブステータスでのCCL pingテスト

CCL接続の確認

- CCL MTUパケットサイズでCCL接続を確認するためのユーザプロビジョニングが必要

解決方法

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 CCL 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)

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

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

パブリッククラウド用のCCL MTUサイズの追加

AWSおよびAzure Cluster MTU値

7.4パブリッククラウドFTDvクラスタでは、新たに推奨されるCCLおよびデータインターフェイスのMTU値があります。

	7.3での推奨される CCL MTU	推奨 7.4のCCL MTU	7.3での推奨される データインターフ ェイスMTU	推奨 7.4のデータインター フェイスMTU
Azure NLBクラス ター	1554	1454	1400	1300
Azure GWLBクラ スター	1554	1454	1454	1374
AWS GWLBクラス ター	1960	1980	1806	1826

クラスターを7.4バージョンにアップグレードした後、FMCはCCLおよびデータインターフェイスMTUを推奨値に更新します。

FMCで使用可能なCLI

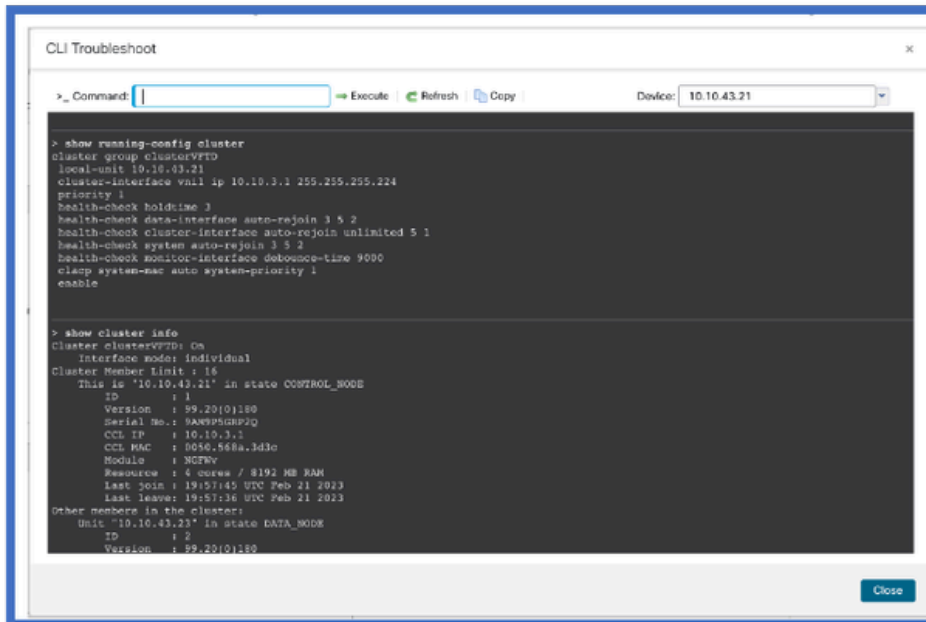
デバイス/クラスタータブで使用可能なデバイスラインCLIプロンプト

FMCからのクラスターラインCLIの実行

- FMCからクラスターLINAトラブルシューティングCLIを実行できるようになりました。

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

一般的に使用されるCLI (デフォルトで表示)



```
CLI Troubleshoot
> _ Command: | Execute Refresh Copy Device: 10.10.43.21
> show running-config cluster
cluster group clusterVFD
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 clusterVFD: 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.3d3c
Module : NCFEvy
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 clusters:
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

定義済みクラスタCLI

- デフォルトで実行されるCLIは次のとおりです。

show running-config cluster (推奨)

クラスタ情報の表示

クラスタ情報の状態の表示

show cluster info transport cp (隠しコマンド)

show version

show asp drop

show counters

show arp

show int ip brief (隠しコマンド)

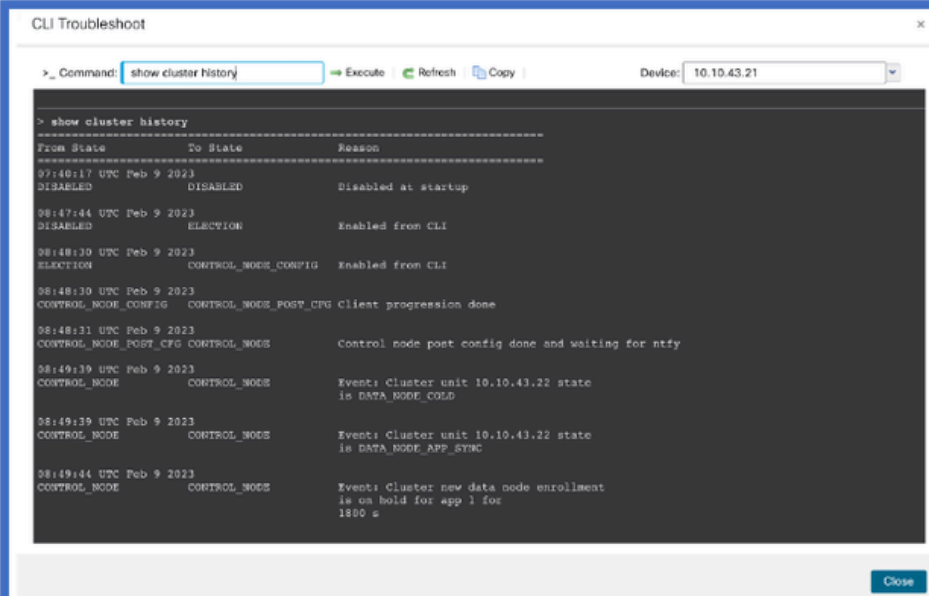
show blocks

show cpu detailed (隠しコマンド)

show interface <ccl_interface>

ping <ccl_ip> size <ccl_mtu> repeat 2

使用可能なコマンドの手動入力

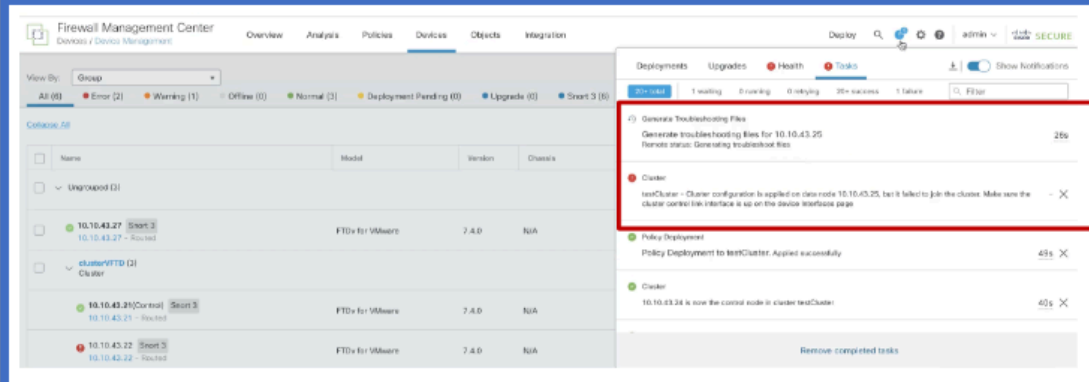


- Alternatively, the user can manually enter the CLI command to be run on the device.
- Enter the command and click the Execute link.
- Refresh and copy are also available.

トラブルシューティングの生成

ノード結合失敗時の自動トラブルシューティング生成

- ノードがクラスタへの参加に失敗すると、デバイスのトラブルシューティングが自動的に生成されます。
- タスクマネージャに通知が表示されます。



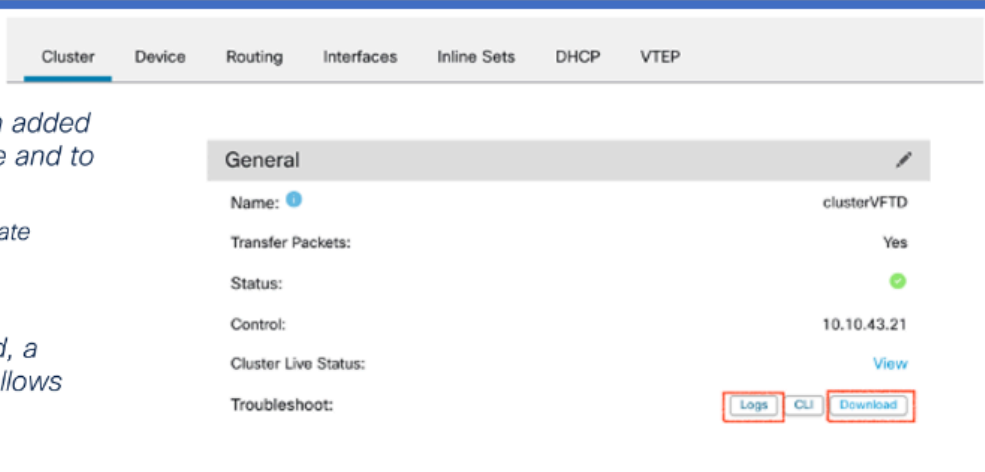
Task manager shows

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

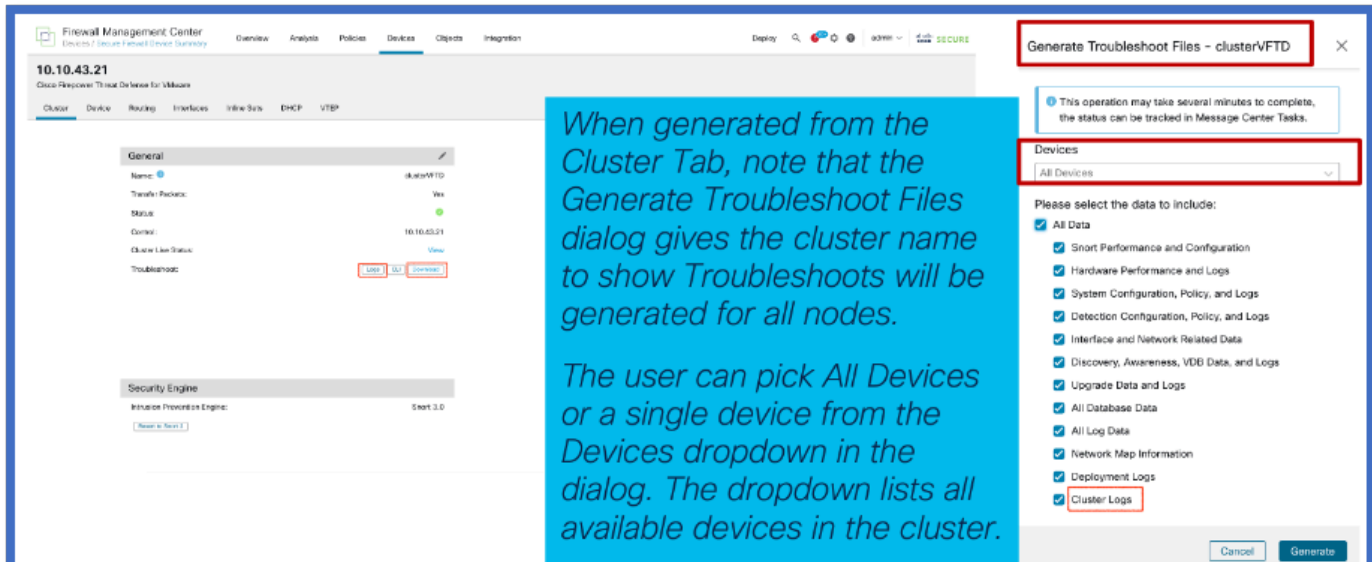
デバイスタブとクラスタブで使用可能なトリガーとダウンロードボタンのトラブルシューティング

クラストラブルシューティングの生成の簡素化

- 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).



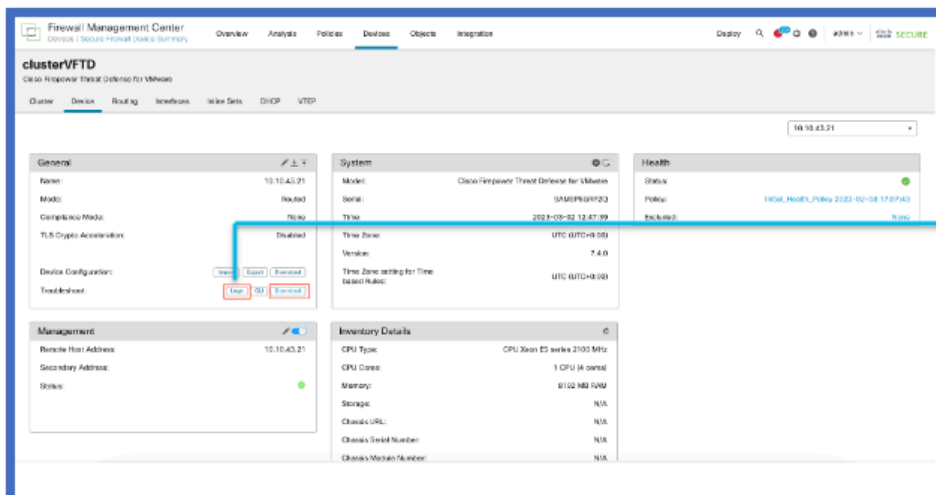
クラスタトラブルシューティングの生成



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.

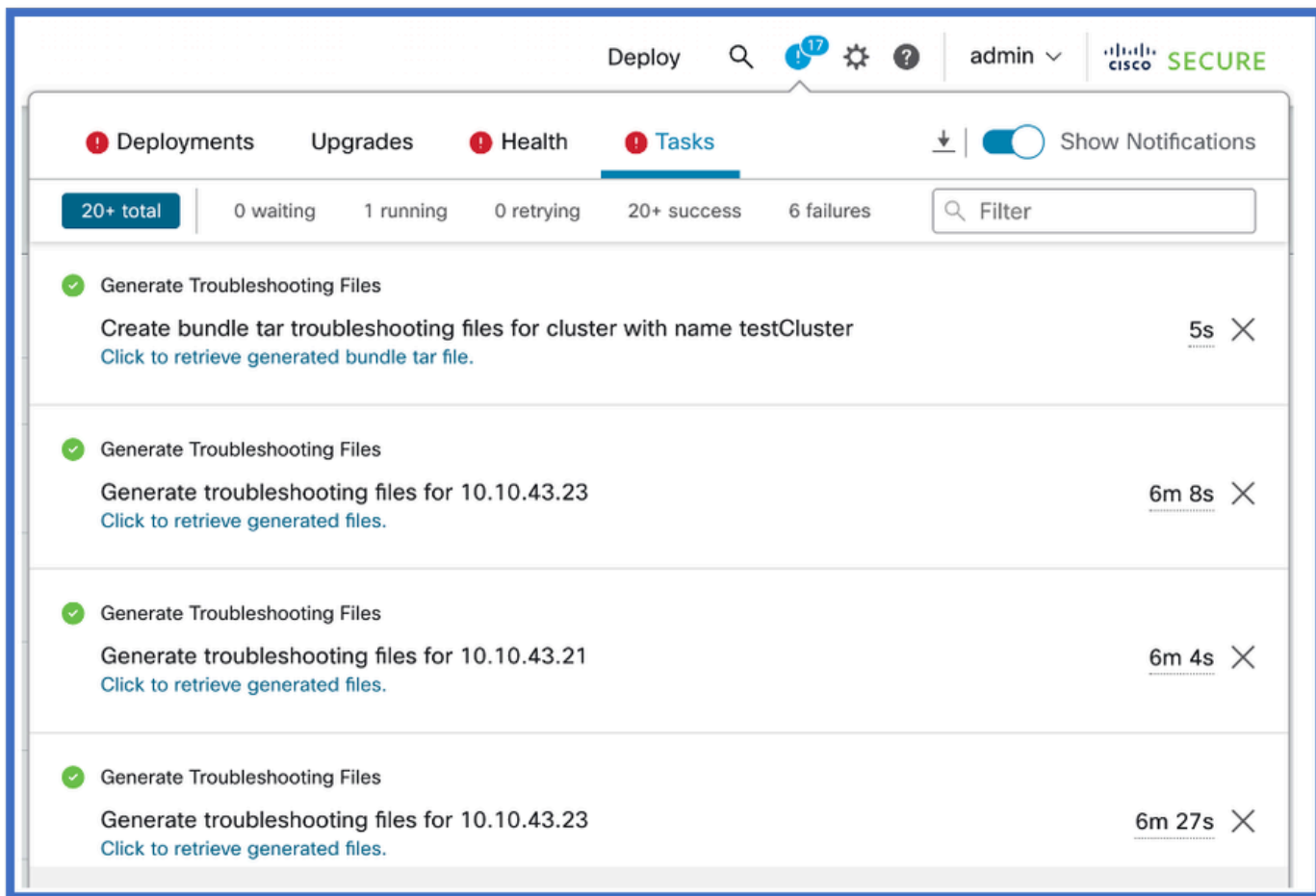
ノード (デバイス) のトラブルシューティングの生成



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

クラスタトラブルシューティング生成の通知の完了

タスクマネージャには、クラスタ内の各ノードのトラブルシューティング生成の進行状況が表示されます。それを待ってからDownloadをクリックします。



Q & A

Q: Azureでは、MTUに対してAWSでは減少しますが増加しますか？

A: パブリッククラウドの新しいMTU値については、Azureでは推奨されるMTUが減りますが、AWSでは増えます。

Q: アップグレード中にMTUが自動的に変更される場合、Syslogエントリはありますか。

A: いいえ。現時点ではSyslogエントリは作成されていません。これが必要な場合は、見直すことができます。

Q: 各ノードのMTU値はどこに表示されていますか。

A: Clusterタブのdevice management > interfacesページで、MTU値を列で表示します。

Q：この障害は、スイッチが設定されていないか、または他のノードが設定されていないために発生していますか。

A：いいえ。これは警告メッセージであり、ユーザにはいつも表示されます。

Q:MTUサイズを表示するには、どのコマンドをshow clusterで使用しますか。

A:CCL pingはデフォルトで、CLIのデフォルトで表示されます。

Q: AWSの場合、スイッチのMTUを増やす手順をドキュメント化できますか？

A：テクニカルパブで確認します。

Q:HWについては、3100シリーズのみをリストしていますが、4K/9K/2K/1Kについてはどうですか。

A:9300、4100、3100でのクラスタリングと仮想のみ。3100はFMCから実行できますが、4100と9300のクラスタはFMCではなくシャーシマネージャで実行されます。

Q：デバイスのアップグレード後に変更を有効にするには、FMCから導入する必要がありますか。

A：はい。アップグレード後に導入する必要があります。推奨されるMTU値を使用する必要があります。

Q:FTDがGREトンネルが構築されるパスの途中で、トンネルのフラッピングやダウンが見られるかのように、MTUが変更されたことを示す警告メッセージをユーザに表示しますか。

A：ドキュメントに記載されています。警告メッセージを処理できます。ノードは制御ノードに合わせて調整されます。スイッチを新しい値に調整する必要があります。制御ノードのアップグレード後に値が変更される。MTU値は制御によって送信されます。

Q：アップグレード後にMTUを変更する場合、FTDデバイスをリブートしますか。

A：アップグレード時にMTU値が変更されても、FTDでは明示的なリブートはトリガーされません。

改訂履歴

改訂	発行日	注釈
2.0	2024年7月17日	代替テキストが追加されました。更新された書式。
1.0	2024年7月17日	初版リリース

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。