在Firewall Management Center 7.4中配置集群可维护性改进

目录

简介

本文档介绍如何使用FMC 7.4中的可维护性改进

新特性

- 集群控制链路(CCL)链路诊断并帮助确保设置正确。

- 现在可以在防火墙管理中心(FMC)中看到Cluster Lina CLI。
- 生成故障排除
  - 现在可一次为集群中的所有设备生成所有流量。
  - 如果节点无法加入集群，则生成故障排除是自动的。
  - 通过Devices > Cluster/Device选项卡排除生成和导航故障。

必备条件、支持的平台、许可

最低软件和硬件平台

应用和最低版本	受管设备	需要支持的最低受管设备版本	备注
安全防火墙7.4	所有这些都支持FTD上的集群 只有“Generation of Troubleshoots”增强功能要求FTD版本为7.4或更高版本	· FMC内部部署+ FMC REST API · 云交付的FMC	这是FMC功能，因此配置可以应用于FMC 7.4可以管理的任何设备。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行7.4的思科防火墙管理中心(FMC)
- 运行7.4或更高版本的Cisco Firepower威胁防御(FTD)。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

CCL链路诊断

集群控制链路接口MTU “集群摘要”(Cluster Summary)页面中的警告

问题

- 集群对集群控制链路的MTU要求高于数据接口。
- 您通常不会将MTU设置为足够高的值，这会导致可靠性问题。
- 建议根据平台，CCL MTU必须比最大数据接口MTU大100或154字节，才能在节点间同步集群状态。

CCL MTU =（最大数据接口MTU）+ 100 |154

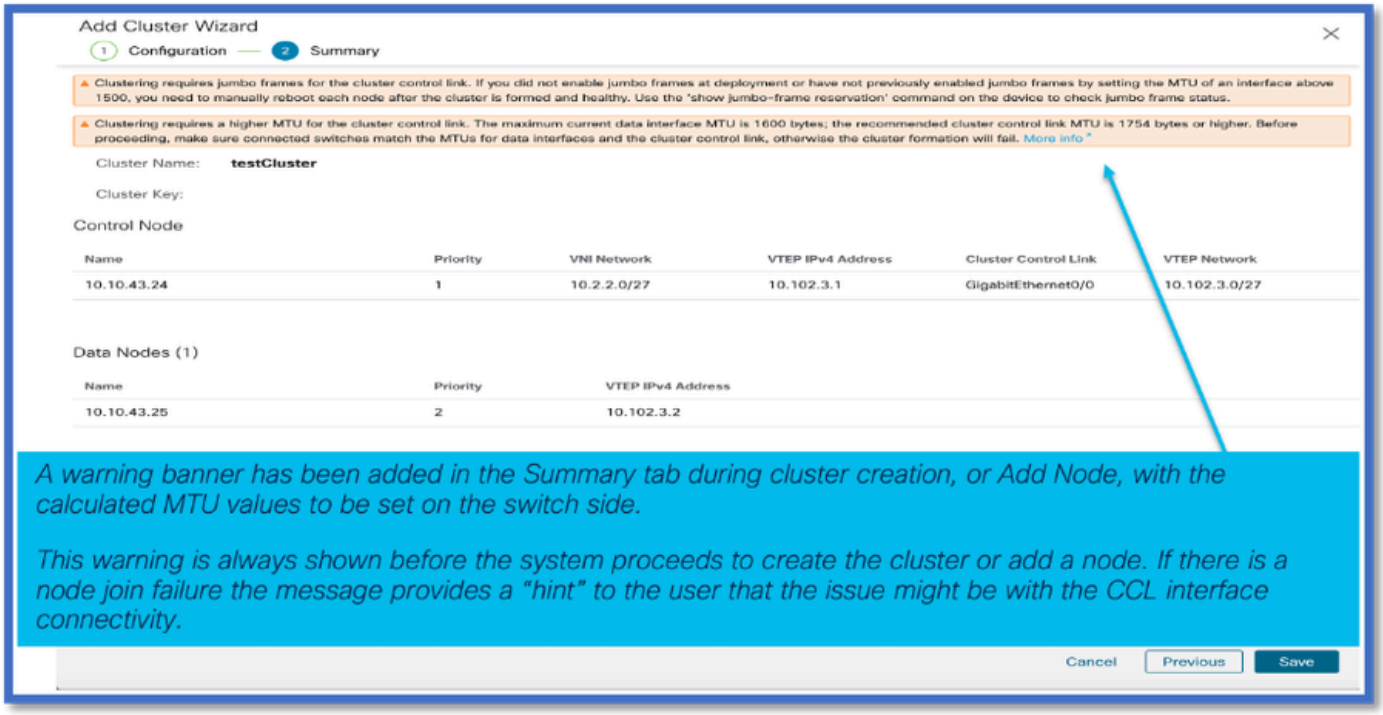
例如，对于FTDv设备，如果1700字节是最大数据接口MTU，则CCL接口MTU的值将设置为1854：1854 = 1700 + 154

每个平台的MTU大小建议

Platform	最大数据接口MTU示例	Add（添加）	CCL链路MTU的总建议设置
安全FW 3100系列	1700	100	1800
FTDv	1700	154	1854

解决方案

- 创建集群时，CCL链路的MTU值会自动设置为接口上的建议值。
  使交换机端的配置与此值匹配。
- 警告消息示例：
  集群要求集群控制链路具有更高的MTU。当前最大数据接口MTU为1500字节；推荐的集群控制链路MTU为1654字节或更高。 在继续操作之前，请确保连接的交换机与数据接口和集群控制链路的MTU匹配，否则集群形成将失败。
- 如果CCL接口的交换机端配置与此值不匹配，则设备无法加入集群。

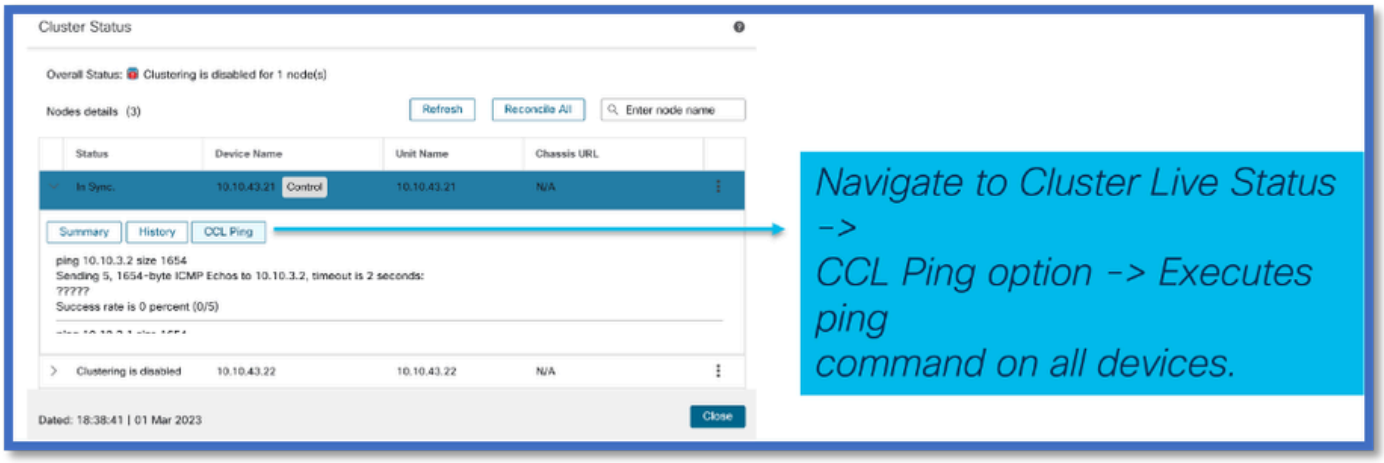


集群实时状态下的CCL Ping测试

检查CCL连接

- 需要用户调配以验证与CCL MTU数据包大小的CCL连接

解决方案



为公共云添加了CCL MTU大小

AWS和Azure群集MTU值

对于7.4公共云FTDv集群，有新的建议CCL和数据接口MTU值。

	7.3中建议的CCL MTU	推荐 7.4中的CCL MTU	7.3中推荐的数据接口MTU	推荐 7.4中的数据接口MTU
Azure NLB群集	1554	1454	1400	1300
Azure GWLB群集	1554	1454	1454	1374
AWS GWLB群集	1960	1980	1806	1826

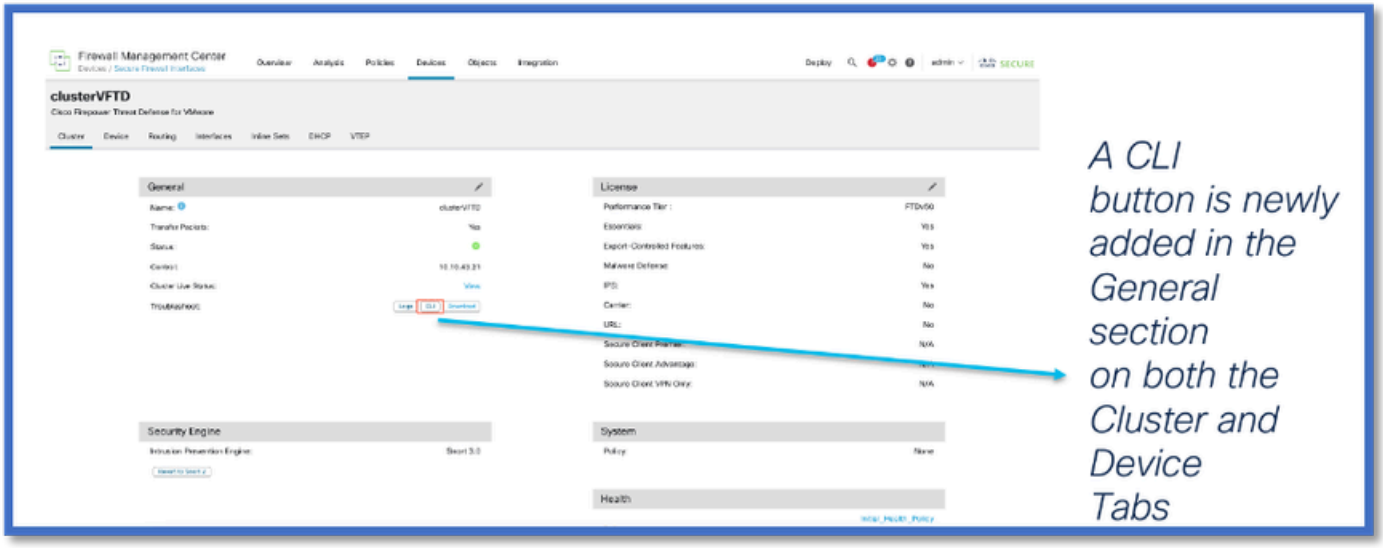
在将集群升级到7.4版后，FMC会将CCL和数据接口MTU更新为建议的值。

FMC中可用的CLI

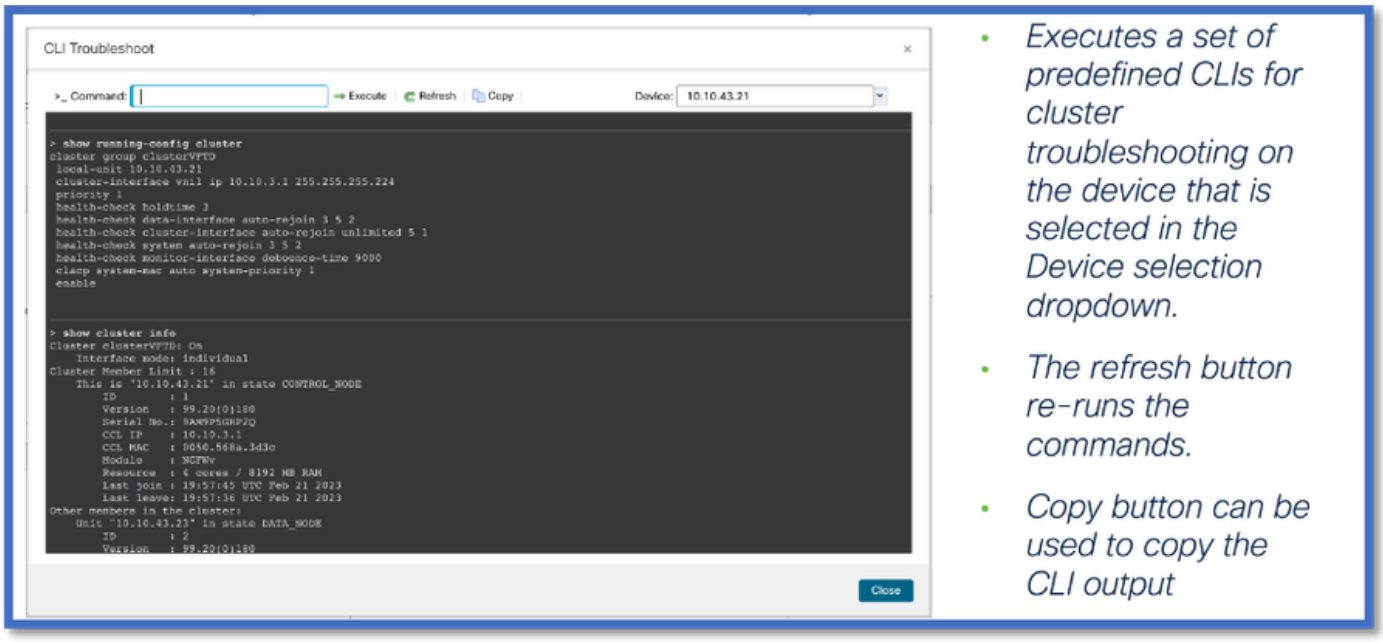
Device Lina CLI提示可在Device/Cluster选项卡中找到

从FMC运行集群Lina CLI

- 现在可以从FMC执行集群LINA故障排除CLI。



默认显示的常用CLI



预定义的集群CLI

- 默认情况下运行的CLI包括：

  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

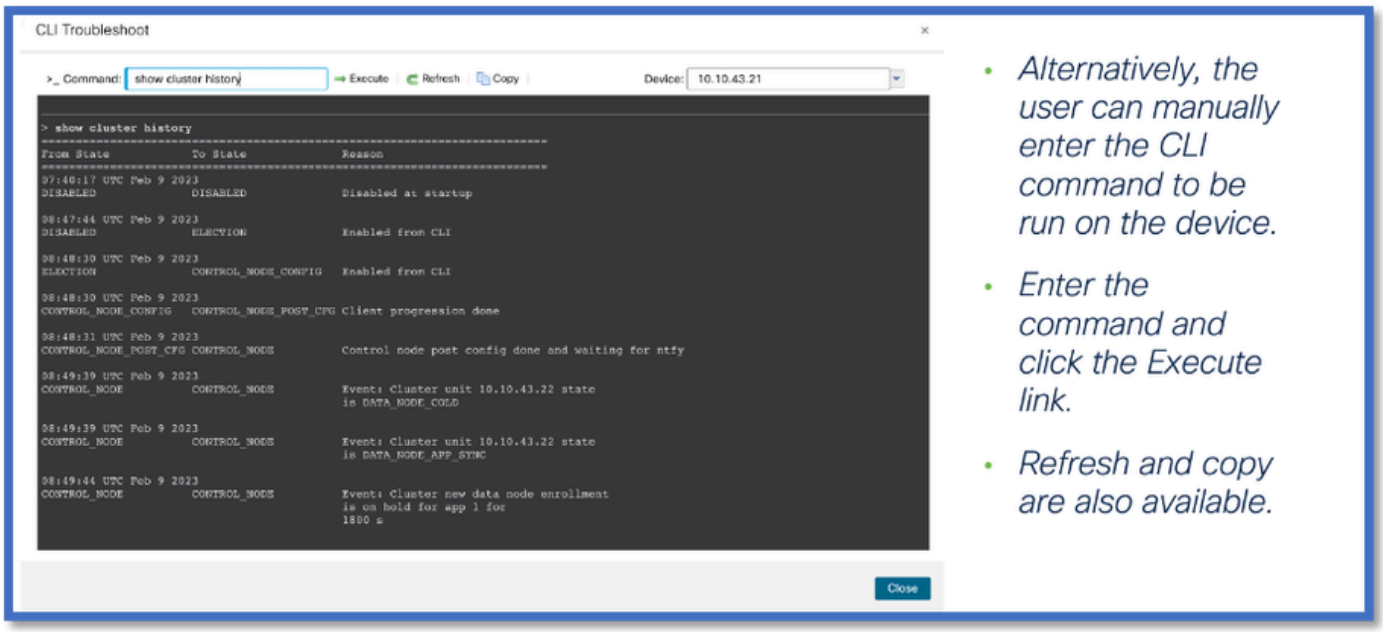
show blocks

show cpu detailed

show interface <ccl_interface>

ping <ccl_ip> size <ccl_mtu> repeat 2

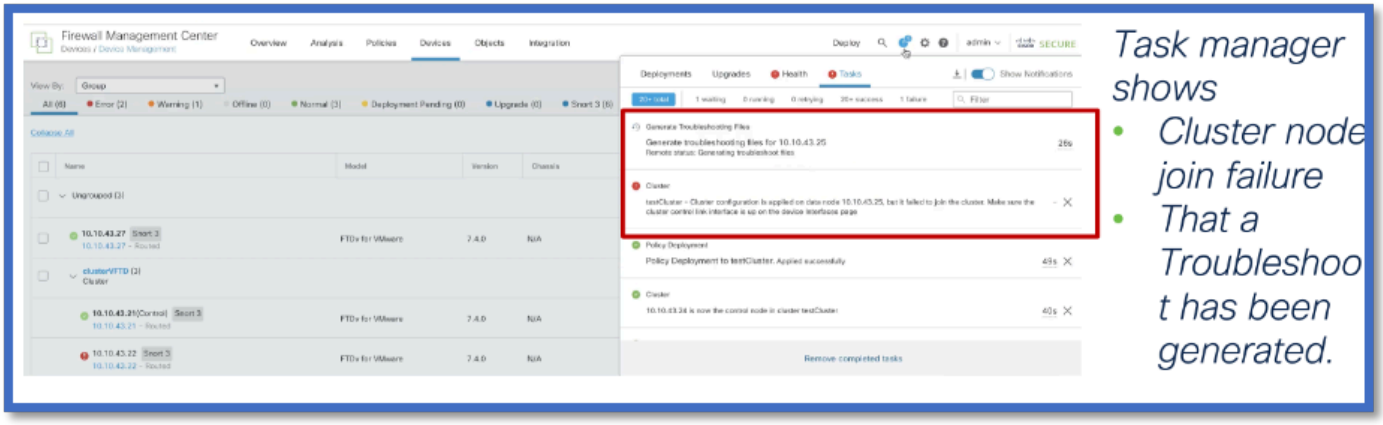
手动输入可用的命令



故障排除的生成

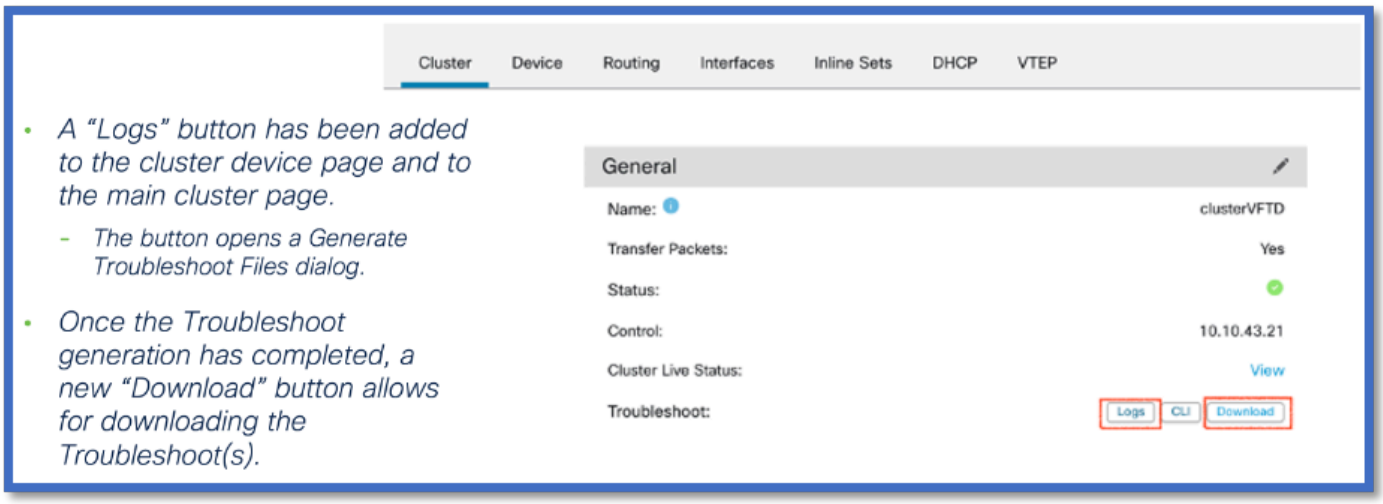
在节点加入失败时自动生成故障排除

- 当节点无法加入集群时，会自动生成设备故障排除。
- 任务管理器中显示通知。

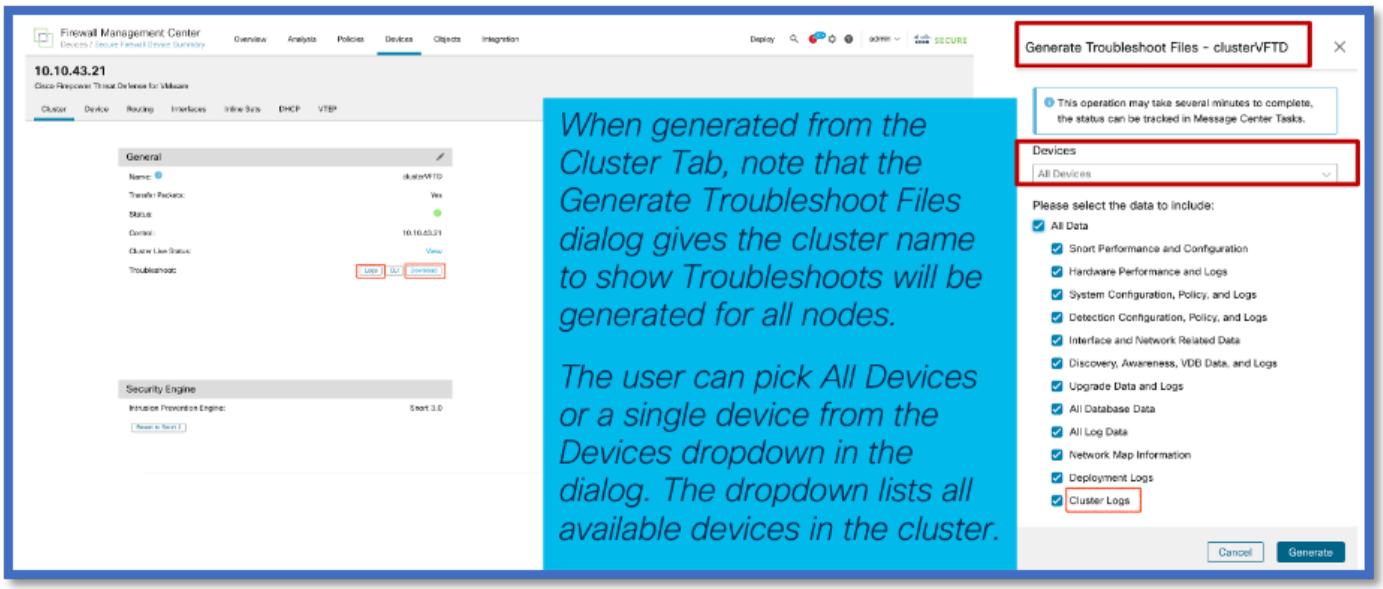


Device和Cluster选项卡中提供Troubleshoot Trigger and Download按钮

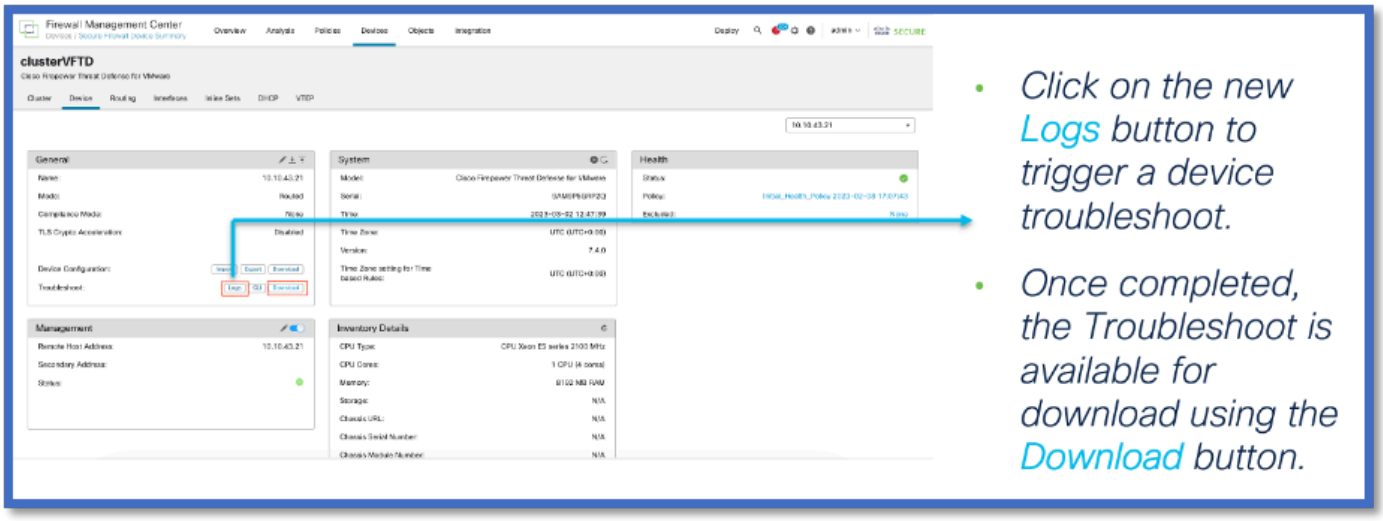
更轻松生成群集故障排除



群集故障排除生成

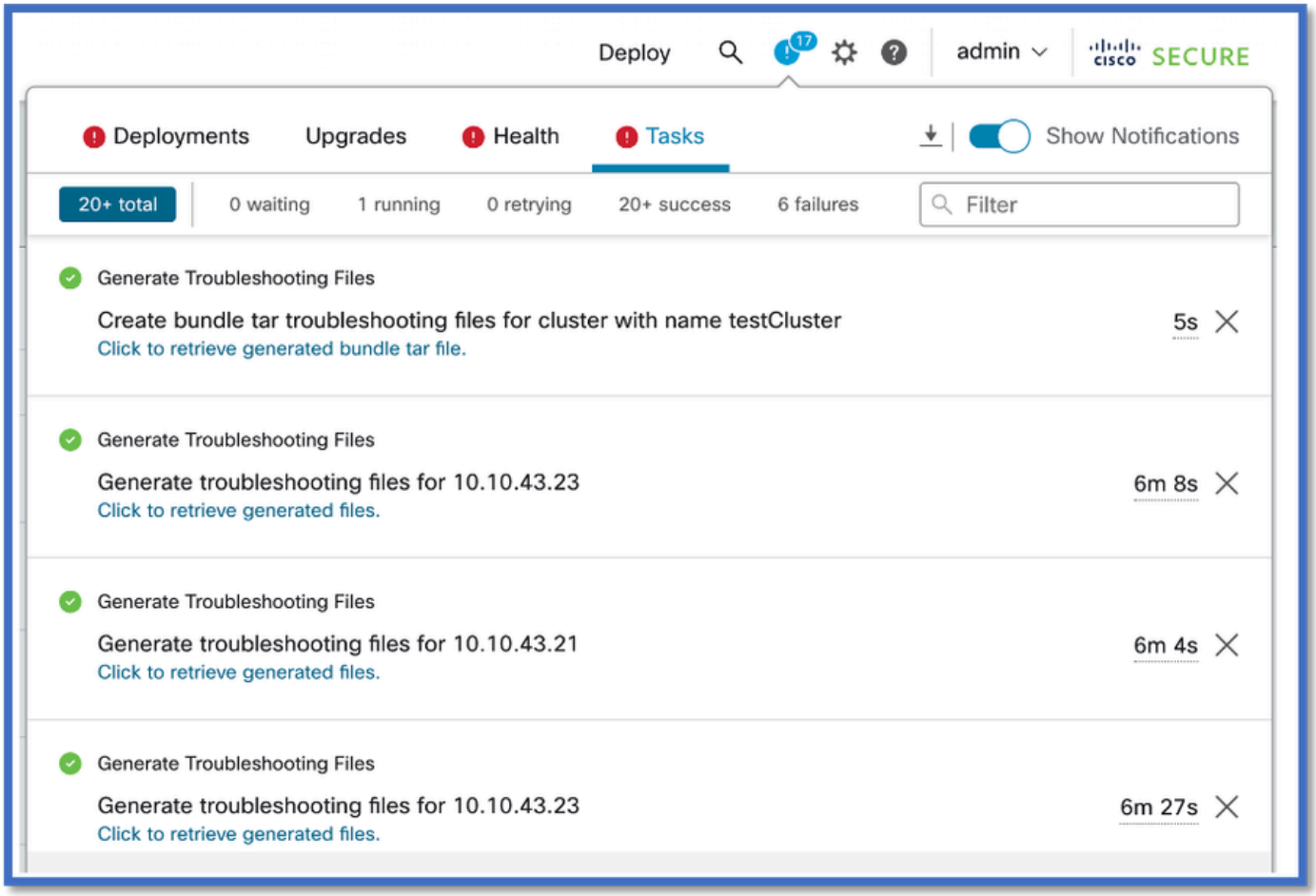


节点（设备）故障排除生成



集群故障排除生成完成通知

任务管理器显示集群中每个节点的故障排除生成进度。稍等片刻，然后再单击下载。



Q & A

问：在Azure中，MTU的AWS中的流量减少但增加？

答：对于公共云中的新MTU值，在Azure中，建议的MTU会减少，但在AWS中会增加。

问：在升级过程中，如果MTU自动更改-是否有Syslog条目？

答：否，此时没有创建系统日志条目。如果需要，我们可以重新查看它。

问：显示的每个节点的MTU值在哪里？

答：在集群选项卡的“设备管理”(device management) >“接口”(interfaces)页面上，以列形式显示MTU值。

问：是否由于未设置交换机或未设置其他节点而出现此故障？

答：不是，这是一条警告消息，作为警告，会始终显示给用户。

问：哪个命令- show cluster -显示MTU大小？

答：CCL ping处于默认状态，显示在CLI的默认设置中。

问：对于AWS，我们能否记录如何增加交换机上的MTU的步骤？

答：技术酒吧需要检查。

问：对于硬件-您只列出了3100系列-关于4K/9K/2K/1K呢？

答：仅在9300、4100、3100和虚拟交换机上进行集群。3100可以从FMC完成，但4100和9300集群在机箱管理器中完成，而不是FMC。

问：您是否必须从FMC进行部署才能使更改在设备升级后生效？

答：是，需要在升级后部署。您必须使用建议的MTU值。

问：我们是否向用户提供任何有关MTU已更改的警告消息，就像FTD位于GRE隧道构建路径的中间，用户是否看到隧道抖动或关闭？

答：在文档中。可以处理警告消息。节点将调整到控制节点。必须将交换机调整为新值。在升级控制节点后更改值。MTU值由控件发送。

问：如果升级后我们更改MTU，是否重新启动FTD设备？

答：当MTU值更改时，升级时不会在FTD上触发显式重新启动。

修订历史纪录

修订版	发布日期	备注
2.0	2024年7月17日	添加了Alt文本。更新的格式。
1.0	2024年7月17日	首次公开发布

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。