

分析MCD上的安全防火墙部署

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[相关产品](#)

[背景信息](#)

[监控部署](#)

[验证](#)

[故障排除](#)

[相关信息](#)

简介

本文档介绍如何使用可用的系统日志来监控多云防御部署，以验证部署是否正在进行。

先决条件

这适用于AWS、Azure、GCP或Oracle等云环境，允许无缝集成到安全云连接器和云部署的Firepower管理中心(cdFMC)

要求

Cisco 建议您了解以下主题：

- 多云防御(MCD)部署工作流程
- 云网络和安全云连接器(SCC)连接概念
- 云部署的FMC监控和运行状况验证

使用的组件

本文档中的信息基于以下软件版本：

- 多云防御
- AWS环境
- 云部署的Firepower管理中心(cdFMC)
- 安全云连接器(SCC)

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。

相关产品

本文档还可与以下硬件和软件版本一起使用：

- 多云防御
- 安全云连接器(SCC)
- 云部署的Firepower管理中心(cdFMC)

背景信息

使用MCD在云平台中部署设备时，需要查看多个位置以确保部署正确进行。这些工具可帮助监控部署，并在发生错误时提供额外的情景。同样的监控原则适用于AWS、Azure和GCP部署。

系统日志是MCD中部署可视性的主要来源。这是查看集群创建事件、网关创建活动、实例启动以及部署工作流程期间遇到的任何异常的最佳位置。FMC还会在注册或部署步骤失败时发出警报，这有助于缩小调查范围。



提示：如果注册超时，请在排除环境故障之前检查MCD系统日志。日志通常用于识别失败步骤。

监控部署

查看MCD中的系统日志，确认部署正在经历预期阶段。这是检查部署状态、网关创建、实例启动活动和所有已记录错误的第一个、也是最有用的位置。

导航至：

Multicloud Defense > Investigate > System Logs

此示例显示了成功的网关创建以及集群实例启动的位置。在本例中，网关实例托管在US-east-2区域和us-east-2b可用性区域。

AWS-CXLABS-RTP-FW	mcd-lab-cluster	Info	FTDv instance i-0bdd9ff657...
AWS-CXLABS-RTP-FW	mcd-lab-cluster	Info	
AWS-CXLABS-RTP-FW	mcd-lab-cluster	Info	
AWS-CXLABS-RTP-FW	mcd-lab-cluster	Info	Gateway Enabled for Gateway...

使用“系统日志”(System Logs)页面验证部署正在经历预期周期，并在步骤失败时收集详细的错误消息。

当报告注册超时或失败的部署事件时，检查FMC是否存在部署错误。FMC可提供高级警报，指示部署未成功完成。

建议的检查包括：

- 1. 验证云网络和安全云连接器(SCC)之间的连接。
- 2. 确认已完成部署指南中的每个部署步骤。
- 3. 验证已配置且正在使用的IAM角色是否正确。

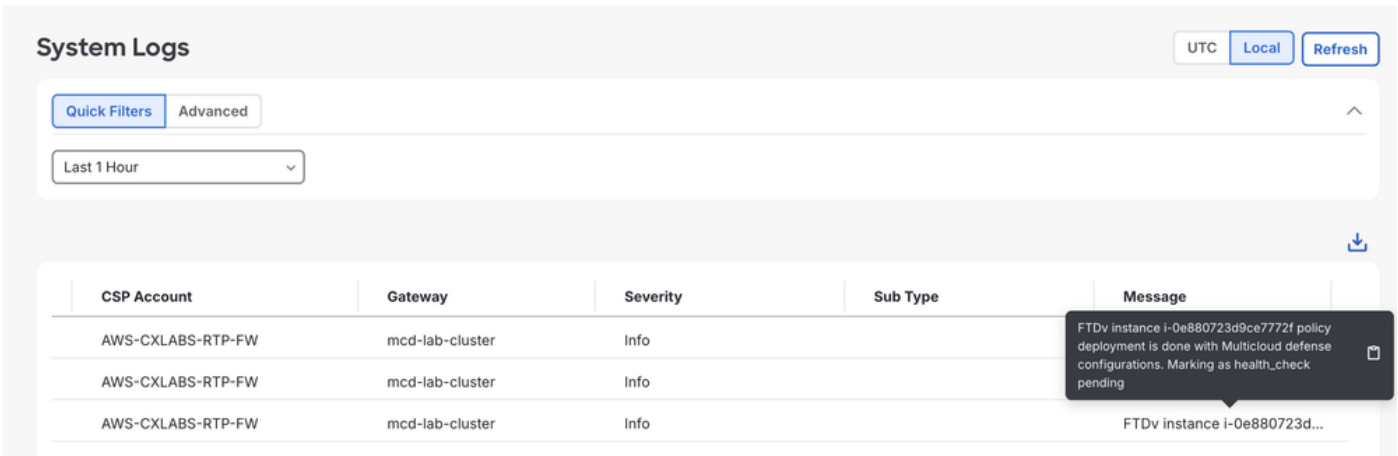
Register	Registration	27s
ciscomcd-mcd-lab-cluster-gcrpxvxq: Established secure connection		
Register	Registration	2m 6s
ciscomcd-mcd-lab-cluster-gcrpxvxq: Registration timed out. Please check connectivity and registration id		
Register	Registration	2m 32s
ciscomcd-mcd-lab-cluster-dfmnhqfi: Established secure connection		



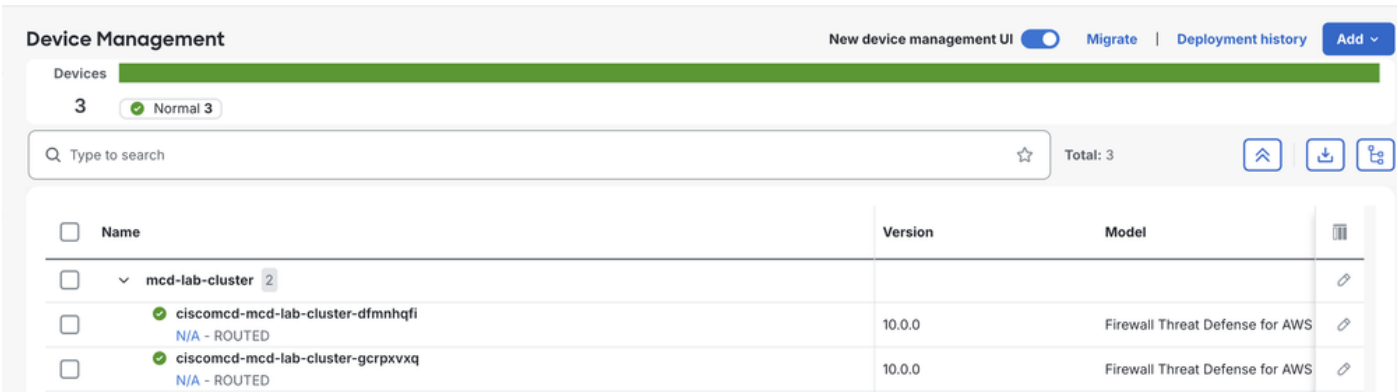
警告：注册失败可能会在成功注册完成之前发生一次或多次。此行为可能是由云计时器行为导致的，并且不一定是一个永久性问题。

如果SCC中的FMC报告注册超时，则系统日志通常会包含有关特定故障的更多详细信息。在大多数情况下，问题是连接、IAM或配置问题的组合，而日志是缩小失败步骤范围的最佳来源。

通过查看MCD系统日志中的最终成功事件，确认部署已成功完成。部署成功后，日志会显示成功的完成事件。



在FMC中也可以看到成功的部署，其中已部署的设备显示已连接状态，并且运行状况指示器显示为绿色。



这确认已成功创建集群，并且设备在预期环境中运行。

验证

有一些地方可以检查以验证AWS部署是否正常：

- 系统日志显示正常部署活动，且没有阻止错误。
- 设备或网关在预期区域和可用区域创建。
- FMC报告设备已连接且运行正常。
- 日志中不会保留注册超时或失败部署警告。

当所有这些条件都成立时，可以认为MCD部署是成功的。

故障排除

如果部署未达到正常状态：

- 查看MCD系统日志，了解失败的准确步骤。
- 检查FMC的注册或连接警报。
- 确认云网络和安全云连接器连接。
- 从部署指南验证IAM角色和所有必备条件。
- 确认群集正在部署到预期区域和可用性区域。

相关信息

- [思科多云防御架构指南](#)
- [思科多云防御白皮书](#)
- [思科多云防御用户指南：系统日志](#)

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）。