使用MCD在AWS中部署FTDv网关

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

配置

- 在SCC租户上启用思科多云防御
- 注册AWS帐户（CSP帐户）
- 创建服务VPC
- 启动FTDv网关向导
- 配置网关属性
- 配置高级设置（可选）
- 审核和部署

验证

故障排除

摘要

相关信息

简介

本文档介绍如何使用Cisco MCD控制器将AWS账户注册到Cisco Multicloud Defense(MCD)并部署FTDv网关。

先决条件

- 为SCC租户调配的云交付防火墙管理中心(cdFMC)。
- AWS EC2密钥对可在针对部署的区域中使用。
- 具有足够的IAM权限以部署CloudFormation堆栈的AWS帐户。
- SCC租户上的活动思科多云防御订用/授权，以及适用的FTDv许可证类型和性能层授权。
- 具有管理平台订用和多云防御基础设施权限的SCC管理访问权限。
- 有权创建和监控CloudFormation堆栈和EC2资源的AWS控制台访问。

要求

Cisco 建议您了解以下主题：

- 思科安全云控制(SCC)导航
- 基本AWS网络概念（VPC、CIDR、传输网关、可用区）
- AWS CloudFormation堆栈部署和审核

使用的组件

- 思科安全云控制(SCC)
- 思科多云防御(MCD)
- 思科安全防火墙威胁防御虚拟(FTDv)
- 基于云的 Firewall Management Center (cdFMC)
- Amazon Web Services(AWS)- CloudFormation、EC2、VPC、传输网关

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。

背景信息

本文档介绍首次使用传输网关(TGW)网络类型将MCD部署到单个AWS账户和区域。AWS云广域网网络类型和入口网关部署不属于本文档的范围，因为MCD目前不支持入口网关。



注意：Multicloud Defense当前不支持入口网关。本文档仅介绍出口/东 — 西网关部署。

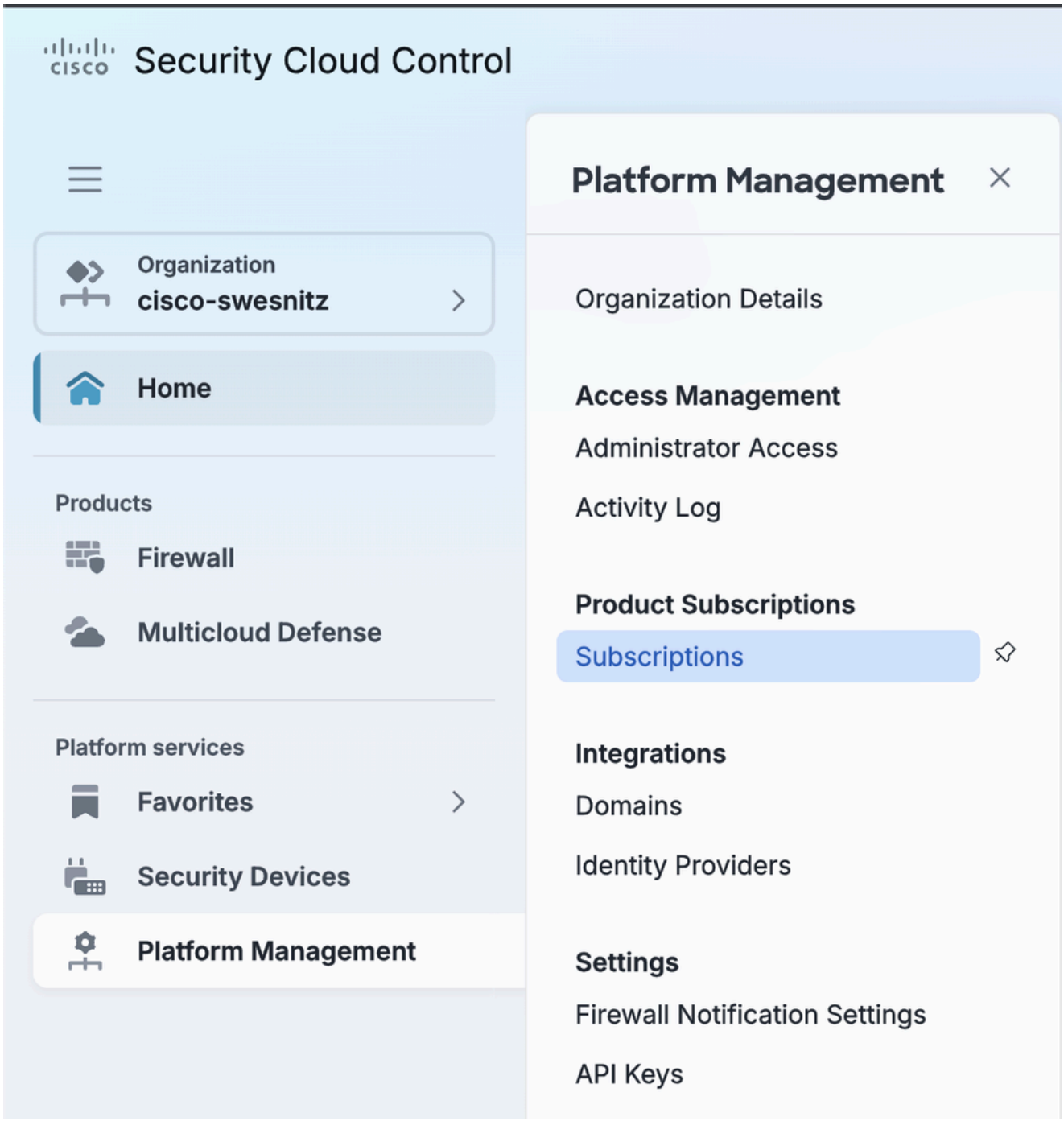


注意：如果初始cdFMC注册尝试失败或超时，则这是预期行为。在进一步排除故障之前，请为群集留出更多时间自动重试注册。

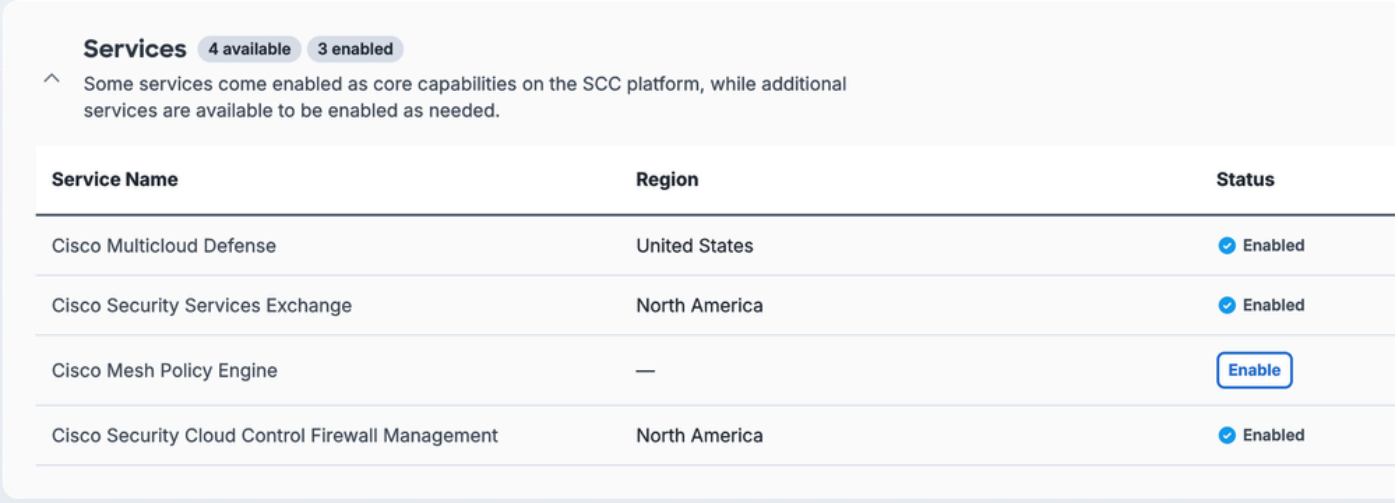
配置

在SCC租户上启用思科多云防御

1. 在Cisco Security Cloud Control(SCC)控制台中，导航到Home > Platform Management > Subscriptions。



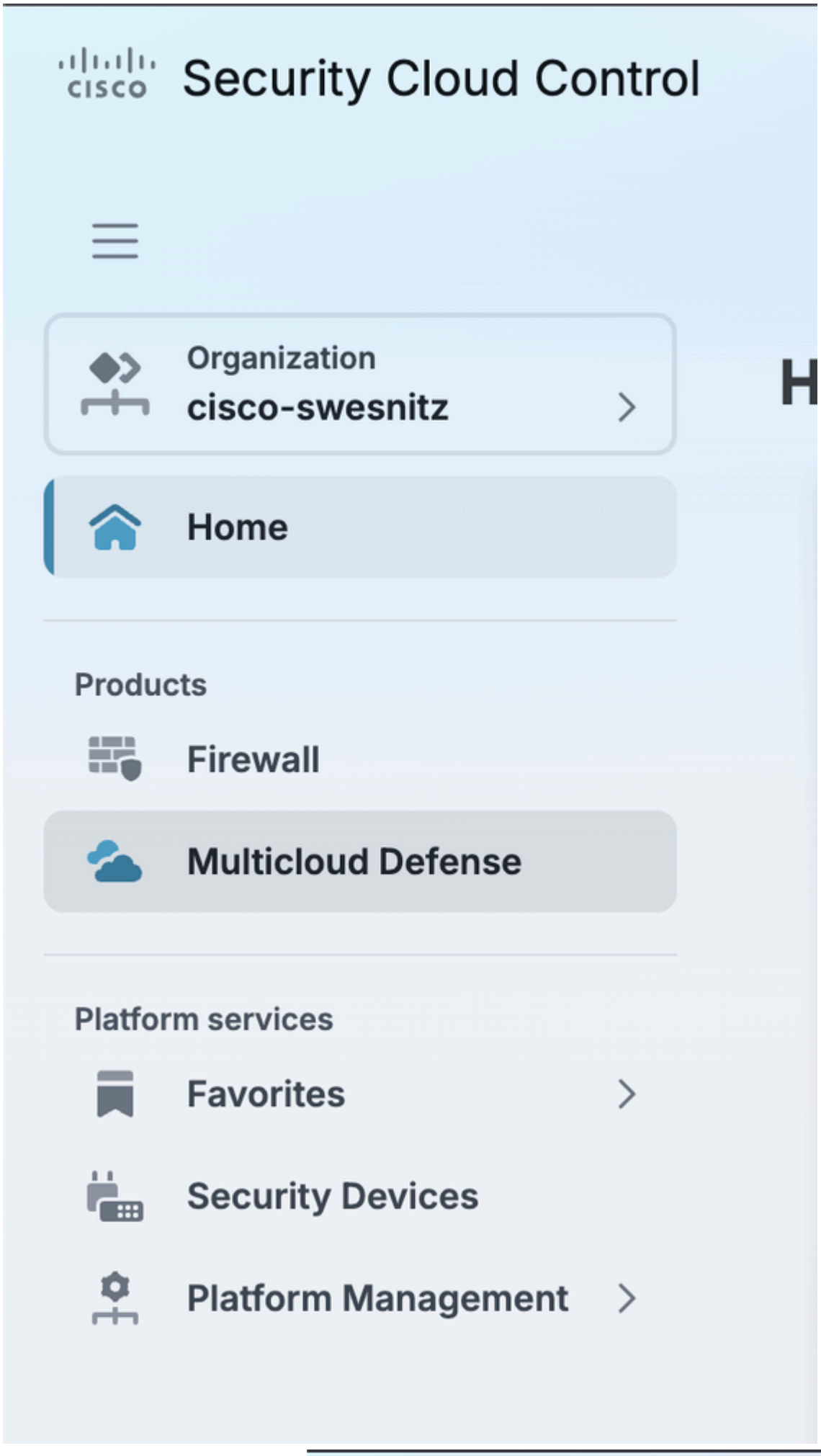
2. 为租户启用多云防御订用。



注册AWS帐户（CSP帐户）

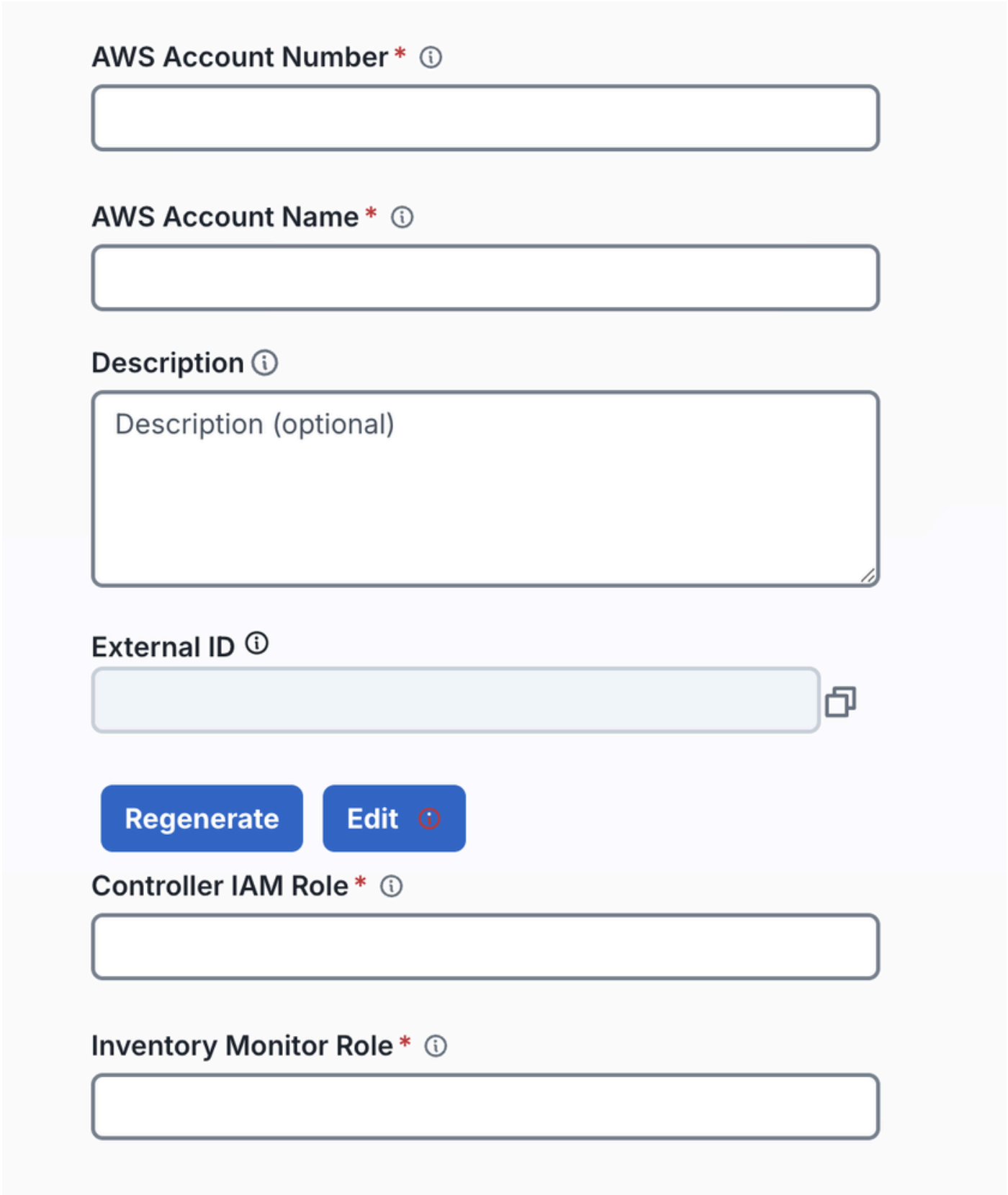
此步骤将AWS帐户连接到Multicloud Defense Controller，以便MCD可以代表其部署和管理资源。此示例使用AWS作为云服务提供商(CSP)。

1. 从SCC 左侧导航窗格中，选择Multicloud Defense。



Security Cloud Control

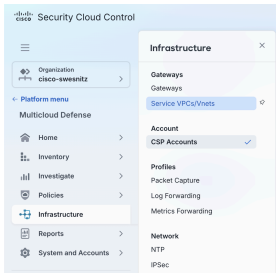
AWS帐号:CloudFormation堆栈的`AccountNumber`输出。
AWS账户名称:此AWS账户在MCD中的友好可识别名称。
控制器IAM角色:CloudFormation堆栈的`MCDControllerRoleArn`输出。
资产监控角色:CloudFormation堆栈的`MCDInventoryRoleArn`输出。



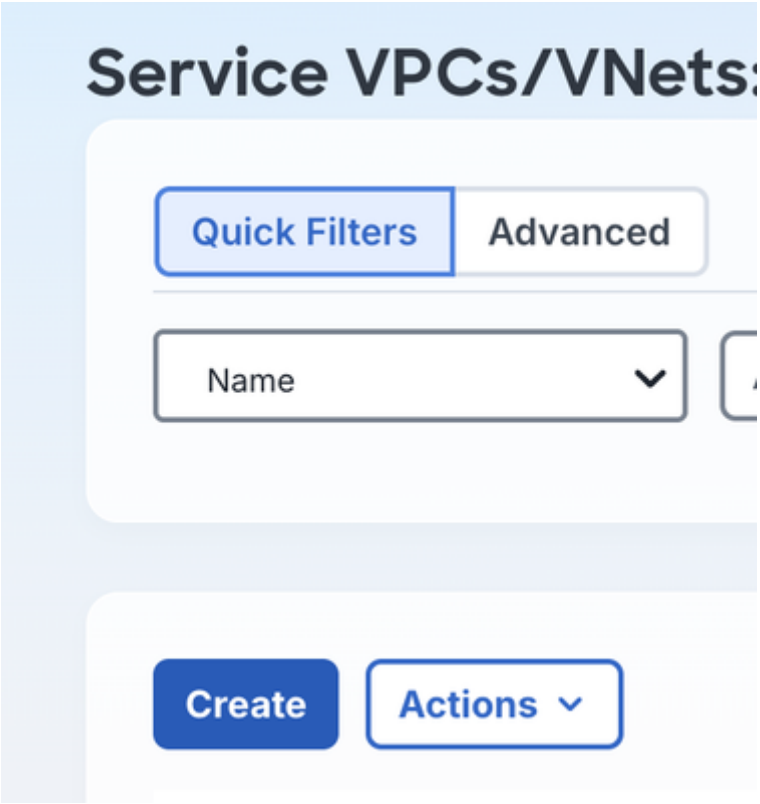
9.保存帐户。AWS账户已注册到MCD。

创建服务VPC

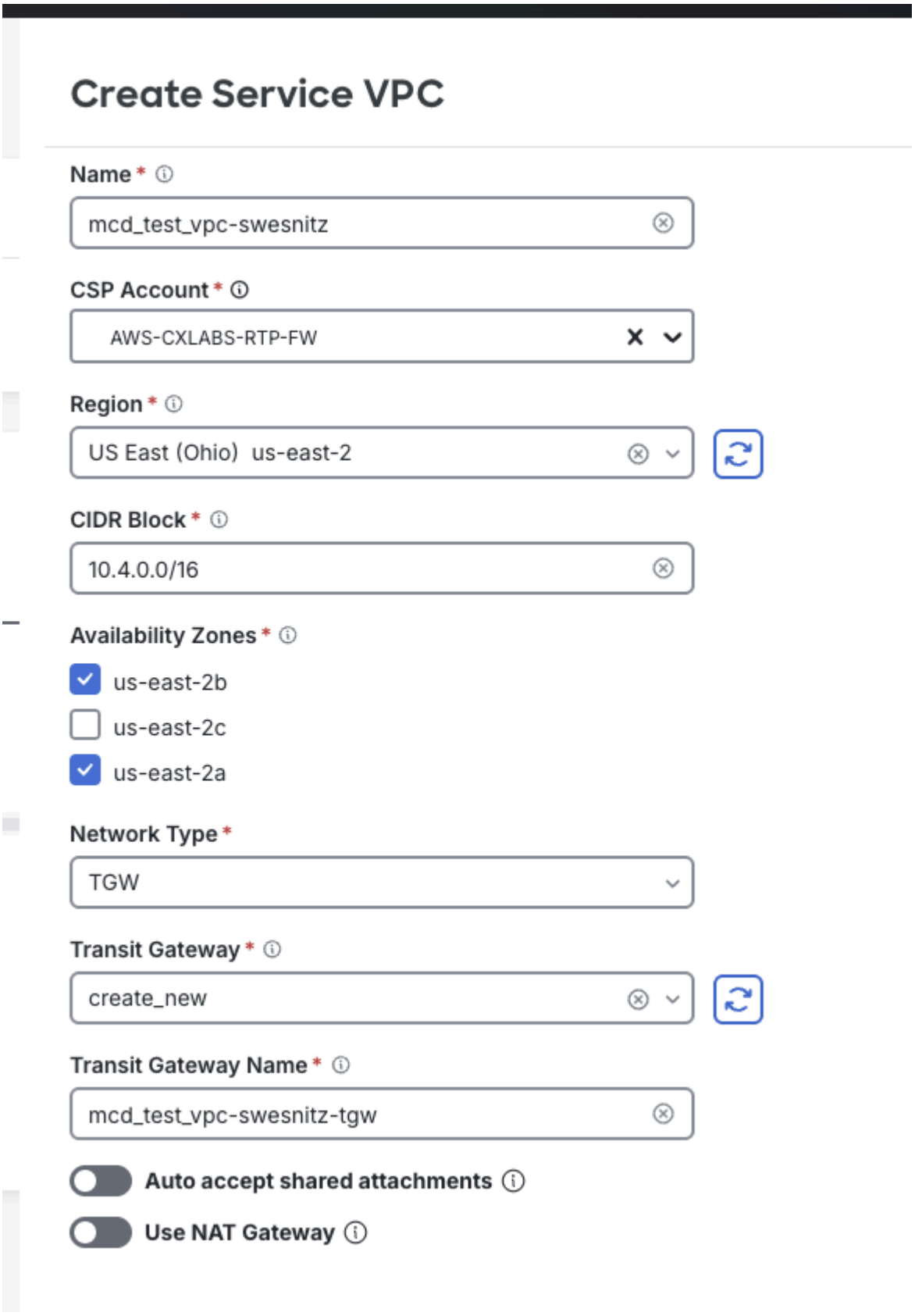
服务VPC托管FTDv网关使用的网络基础设施（子网、路由表、传输网关）。



1. 导航到Multicloud Defense > Infrastructure > Service VPCs/VNets。



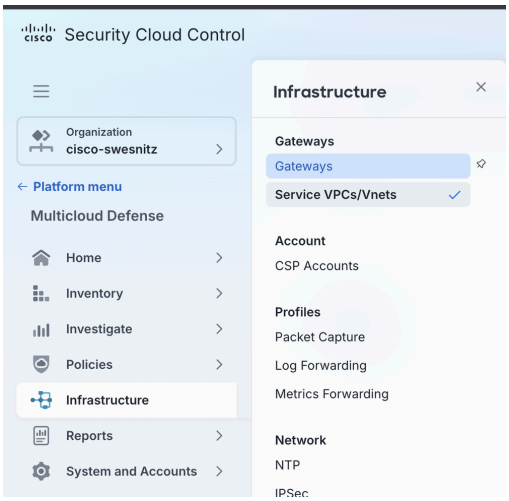
2. 选择创建。
3. 配置VPC设置：
   名称：VPC的唯一易识别名称。
   CSP帐户:第2步集成的AWS账户。
   地区:启动FTDv集群的AWS区域。
   CIDR块:专用于此MCD部署的CIDR范围（不得与现有VPC重叠）。
   可用区:至少一个AZ;建议使用两个作为冗余。
   网络类型:选择传输网关(TGW)。 CloudWAN是专门用于AWS云广域网部署的独立网络类型，不在本文档的讨论范围之内。
   传输网关:选择create_new，为新的传输网关指定唯一的名称。
   NAT网关（可选）：允许所有出口流量通过NAT网关路由。在本示例中未启用；NAT网关配置不在本文档的讨论范围之内。

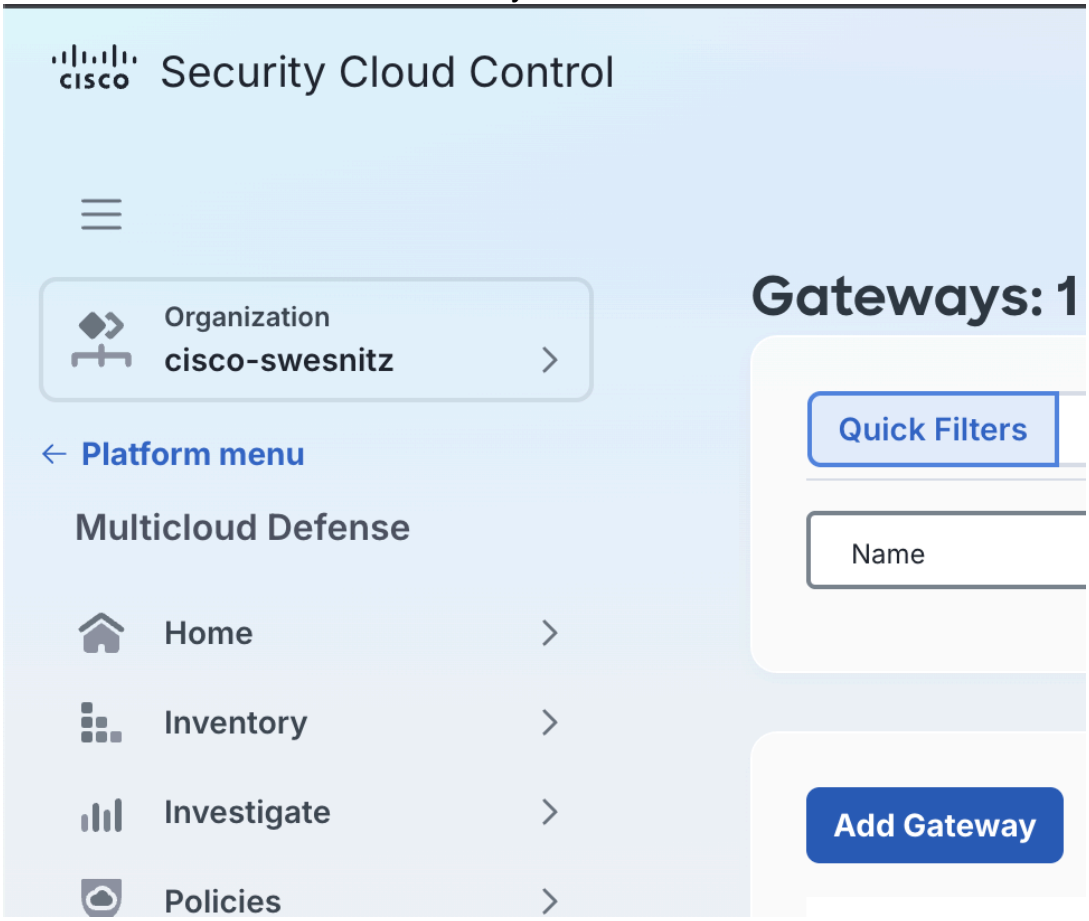


4.选择保存。

启动FTDv网关向导

1. 导航到Multicloud Defense > Infrastructure > Gateways。





2. 选择添加网关。
3. 配置初始设置：

   帐户:第2步中集成了CSP帐户。

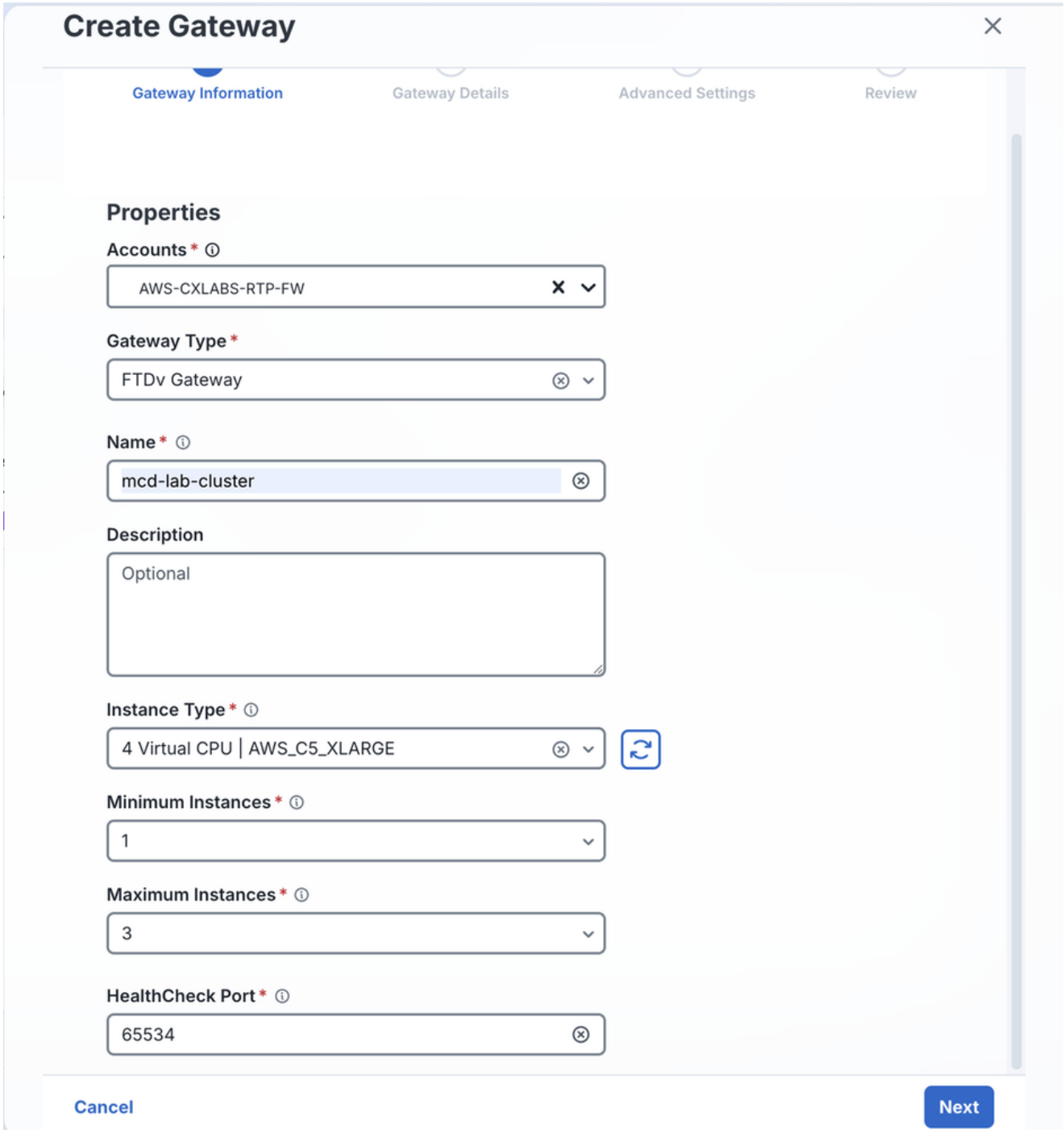
   网关类型:选择FTDv Gateway。

   名称：此群集在MCD中的显示名称。

   实例类型:符合所需吞吐量和性能需求的实例大小。此示例使用支持的最小类型C5_XLARGE。

   最小/最大实例:所需的缩放范围。最小值为1个实例；最大值为10。

   运行状况检查端口：默认值为 65534；仅在为MCD负载均衡器指定了其他端口时进行更改。如果更改，则端口必须在与FTDv实例关联的任何数据路径安全组中允许。



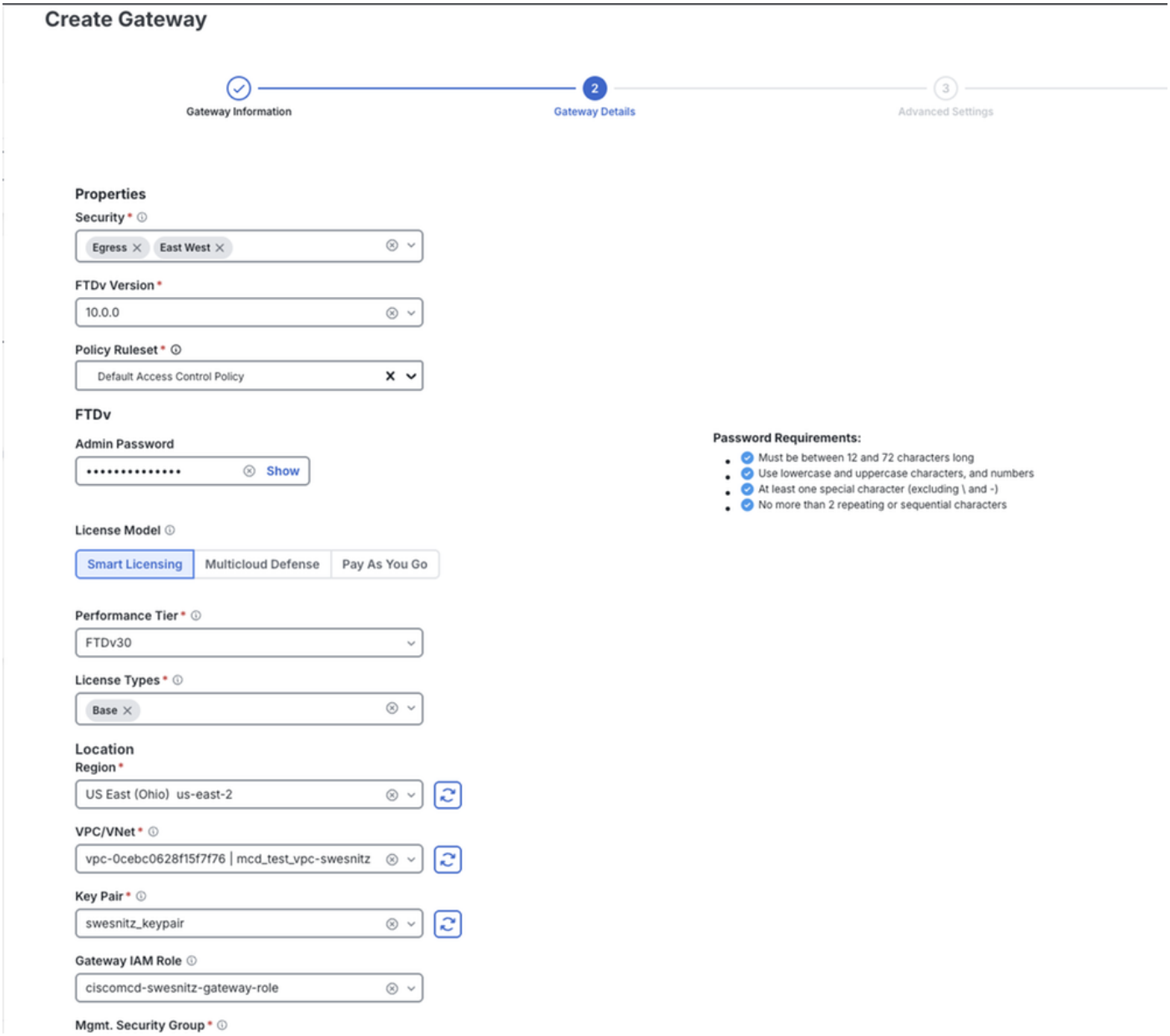
4. 选择 Next（下一步）。

配置网关属性

属性:选择Egress/East-West.当前不支持入口网关。
FTDv版本:最适合该环境的软件版本。
策略规则集:要应用于此FTDv集群的访问控制策略(ACP)。
密码:FTDv实例的密码。
许可证型号:所需的许可模式。
性能层:适合预期设备吞吐量的层。

许可证类型:为此部署购买的许可证类型。
地区:部署这些FTDv实例的区域。
VPC/VNet ID:第3步中创建的服务VPC。
密钥对:现有AWS密钥对。
网关IAM角色:在其名称中包含网关的角色，与MCDFirewallRoleName对应 第2步中CloudFormation堆栈的值。选择此角色会自动填充关联的安全组。
EBS加密:默认情况下选择AWS管理的加密。Amazon EBS自动且透明地加密块存储卷、传输数据和快照。

1.选择下一步。



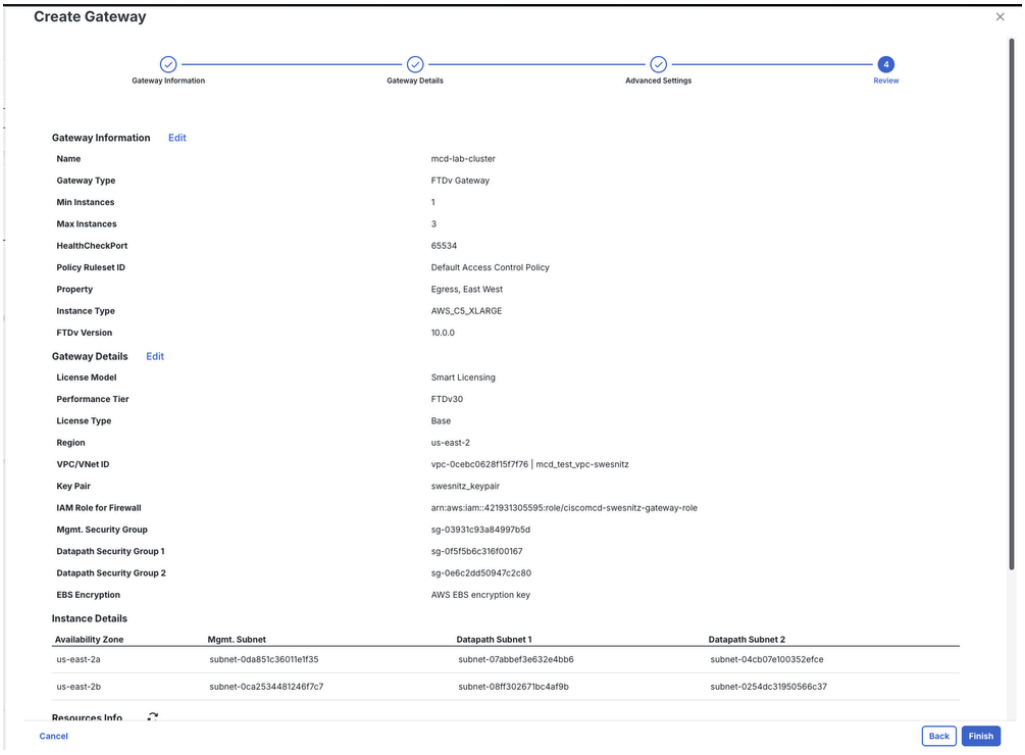


配置高级设置（可选）

高级设置允许配置选项，例如禁用FTDv实例的公共IP地址。本示例中未配置高级设置。

审核和部署

1. 检查所有配置的设置是否准确。



2. 选择完成开始部署。

注意：部署最多可能需要30分钟。在此期间，MCD调配和集群指定数量的FTDv实例并将其

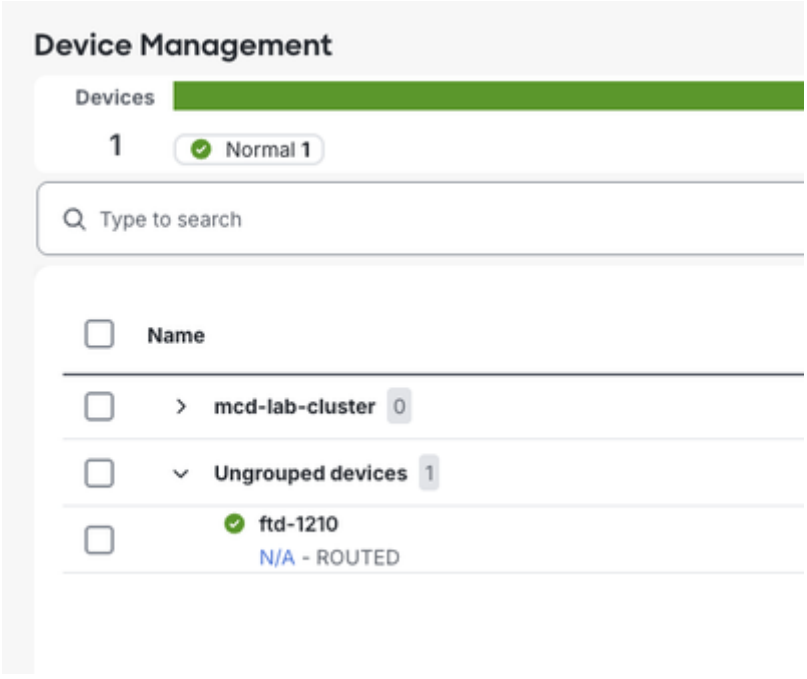
注册到cdFMC。

验证

使用本部分可确认配置能否正常运行。

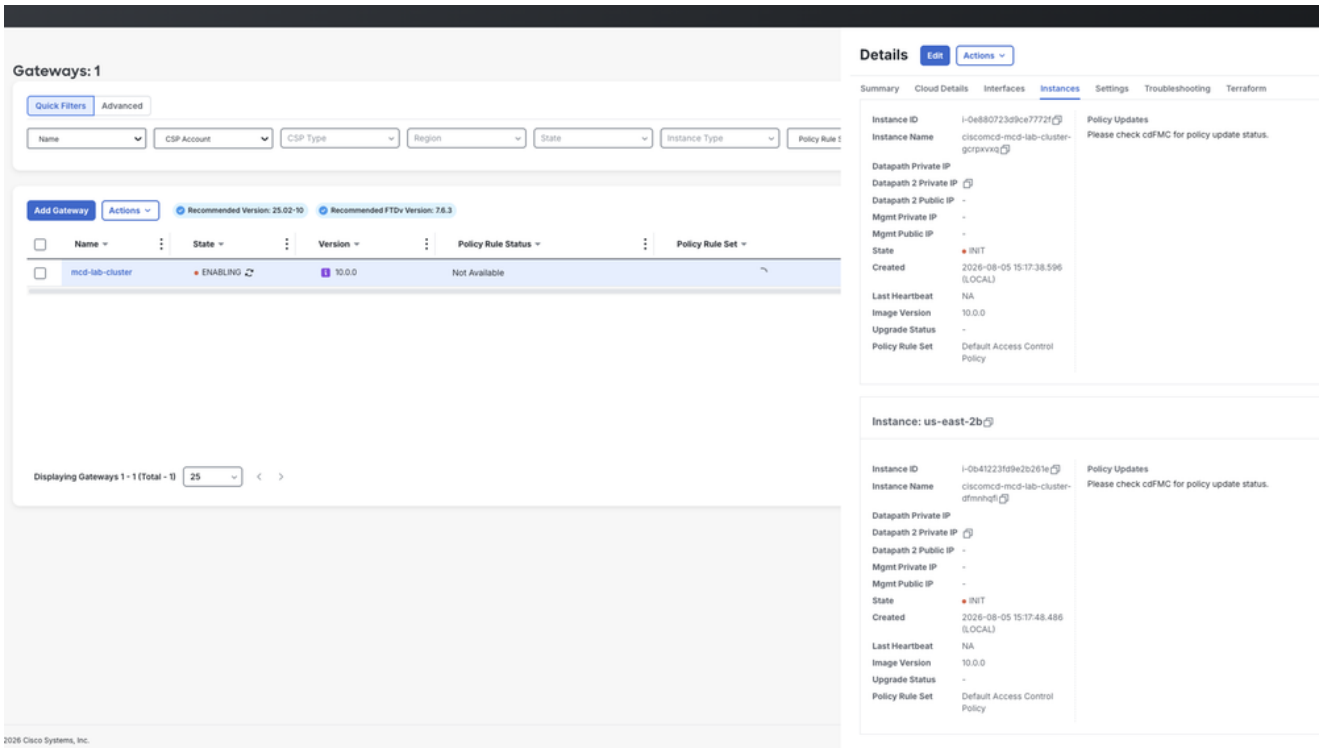
可从多个位置确认部署和注册成功：

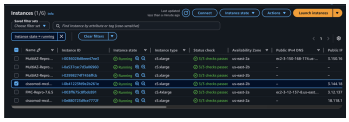
- cdFMC:选择Finish后，新集群即会在cdFMC中的Devices > Device Management下显示（处于挂起状态）。



- MCD网关详细信息:选择网关名称将打开一个显示启动进度的详细信息面板。

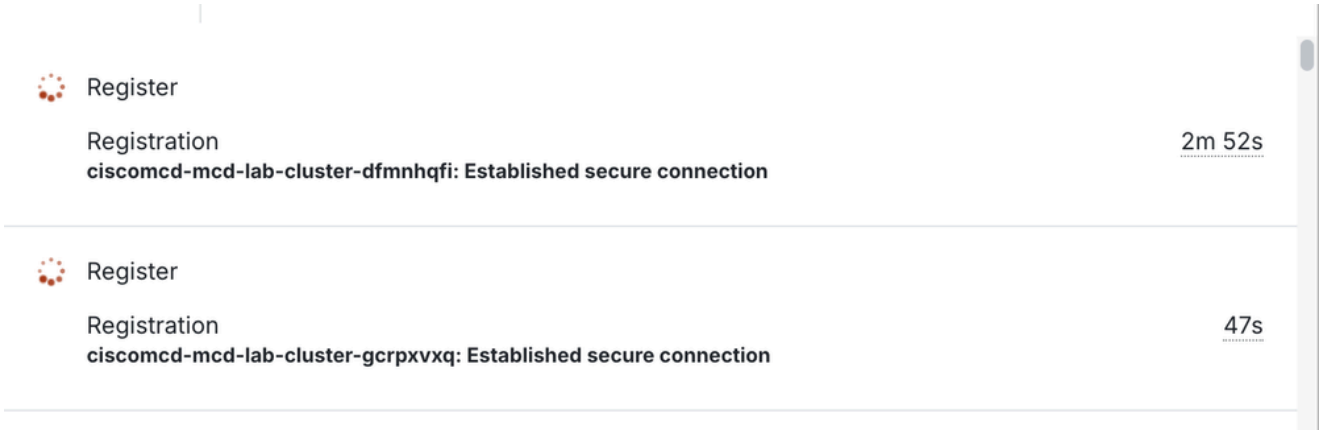
  选择指定名称，然后单击实例选项卡。



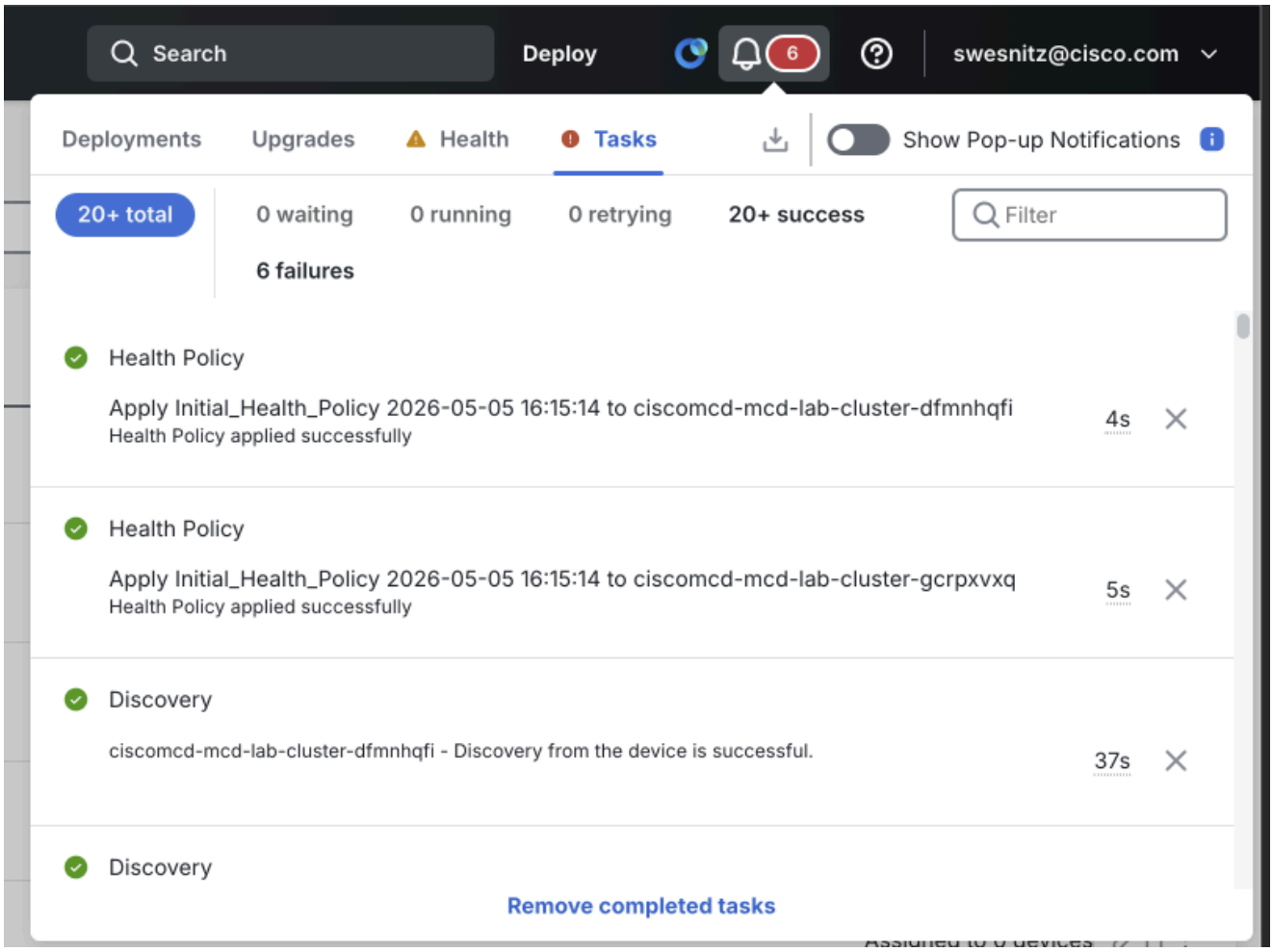


- AWS EC2控制台:可以在EC2 > Instances中直接监控单个实例状态。
- cdFMC任务选项卡:在以下位置跟踪注册进度：

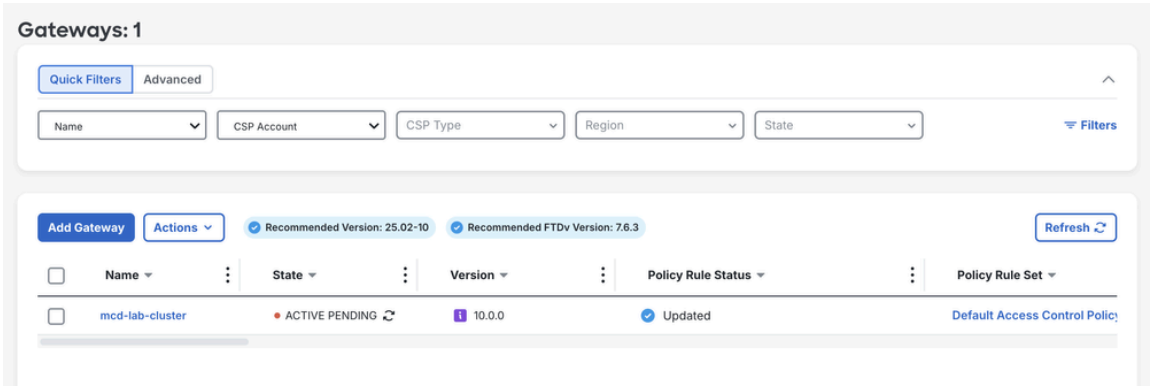
注册继续：



注册成功：



- 最终状态:成功注册后，网关在转换到完全活动之前显示活动 — 待定状态，确认集群已部署且运行正常。



故障排除

本部分提供了可用于对配置进行故障排除的信息。

- 在cdFMC Tasks（cdFMC任务）选项卡中，初始注册尝试失败或超时 — 首次注册尝试时的预期行为。在进一步进行故障排除之前，请为群集留出更多时间自动重试注册。
- CloudFormation堆栈无法完成 — 验证部署堆栈的AWS IAM用户/角色是否具有足够的权限，然后查看Events选项卡以了解具体的故障原因。
- 网关IAM角色或安全组未填充在网关向导中 — 确认第2步中的CloudFormation堆栈已成功完成，并且选择了正确的CSP帐户和区域。

摘要

完成此过程将导致：

- 在SCC租户上启用多云防御。
- 通过CloudFormation注册AWS帐户。
- 使用传输网关创建的服务VPC。
- 群集FTDv网关已部署并注册到cdFMC。

FTDv网关处于活动状态，可用于策略配置和流量检测。

相关信息

- 防火墙威胁防御虚拟
- 从Multicloud Defense Dashboard将AWS账户连接到Multicloud Defense Controller
- 创建服务VPC或VNet
- 创建FTDv网关
- 技术支持和文档 - Cisco Systems

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）。