群集技术：公共云

通过集群，您可以将多台 Firewall Threat Defense Virtual 组合成一个逻辑设备。集群具有单个设备的全部便捷性（管理、集成到一个网络中），同时还能实现吞吐量增加和多个设备的冗余性。使用以下公共云频台，您可以在公共云中部署 Firewall Threat Defense Virtual 集群：

- Amazon Web 服务 (AWS)
- Microsoft Azure
- Google Cloud Platform (GCP)

目前仅支持路由防火墙模式。

注释 使用集群时，有些功能不受支持。请参阅不支持的功能和集群，第 124 页。

- 关于公共云中的 Threat Defense Virtual 群集，第 2 页
- Threat Defense Virtual 集群的许可证，第 4 页
- Threat Defense Virtual 集群的要求和前提条件，第 4 页
- Threat Defense Virtual 集群的准则，第 6 页
- 在 AWS 中部署集群，第 8 页
- 在 Azure 中部署集群，第 37 页
- Azure 中的 Firewall Threat Defense Virtual 集群 Autoscale 解决方案，第 55 页
- 在 GCP 中部署集群，第 78 页
- GCP 中的 Threat Defense Virtual 集群 Autoscale 解决方案，第 87 页
- 将集群添加到管理中心（手动部署），第 100 页
- 配置集群运行状况监控设置，第 108 页
- 管理集群节点，第 112 页
- 监控集群，第 115 页
- 对集群进行故障排除，第 121 页
- 升级集群，第 123 页
- 集群参考，第 124 页
- 关于公共云中的 Threat Defense Virtual 集群的历史记录，第 135 页

关于公共云中的 Threat Defense Virtual 群集

本节介绍集群架构及其工作原理。

集群如何融入网络中

集群包含多台防火墙，作为单一设备工作。要用作集群，该防火墙需要以下基础设施：

- 独立的网络（称为集群控制链路），通过 VXLAN 接口用于集群内的通信。VXLAN 充当第 3 层物理网络上的第 2 层虚拟网络，让 Firewall Threat Defense Virtual 能够通过集群控制链路发送广播/组播消息。
- 负载均衡器 - 对于外部负载均衡，您有以下选择（具体取决于公共云）：
  - AWS 网关负载均衡器

    AWS 网关负载均衡器结合了透明网络网关和按需分配流量和扩展虚拟设备的负载均衡器。Firewall Threat Defense Virtual 支持使用 Geneve 接口单臂代理且具有分布式数据平面的网关负载均衡器集中控制平面（网关负载均衡器终端）。
  - Azure 网关负载均衡器

    在 Azure 服务链中， Firewall Threat Defense Virtual充当可以拦截互联网和客户服务之间的数据包的透明网关。 Firewall Threat Defense Virtual 通过已配对代理中的 VXLAN 网段在单个 NIC 上定义外部接口和内部接口。
  - 本地 GCP 负载均衡器，内部和外部
  - 使用内部和外部路由器（例如思科云服务路由器）的等价多路径路由 (ECMP)

    ECMP 路由可以通过路由指标并列最优的多条“最佳路径”转发数据包。它与 EtherChannel 一样，也可以使用源和目标 IP 地址及/或源和目标端口的散列值将数据包发送到下一跃点。如果将静态路由用于 ECMP 路由，则 Firewall Threat Defense 故障会导致问题；如果继续使用该路由，发往故障 Firewall Threat Defense 的流量将丢失。因此，如果使用静态路由，请务必要使用静态路由监控功能，例如对象跟踪。我们还建议使用动态路由协议来添加和删除路由，在这种情况下，您必须配置每台 Firewall Threat Defense 使之加入动态路由。

注释 负载均衡不支持第 2 层跨区以太网通道。

独立接口

您可以将集群接口配置为独立接口。

独立接口是正常的路由接口，每个接口都有自己的本地 IP 地址。接口的 IP 地址将通过 DHCP 自动配置。不支持静态 IP 配置。

控制和数据节点角色

一个集群成员是控制节点。如果多个集群节点同时上线，则控制节点由中的优先级设置决定；优先级可设置为 1 到 100，其中 1 为最高优先级。所有其他成员都是数据节点。 首次创建集群时，您可以指定要成为控制节点的节点，因为它是添加到集群的第一个节点，所以它将成为控制节点。

集群中的所有节点共享同一个配置。您最初指定为控制节点的节点将在数据节点加入集群时覆盖数据节点上的配置，因此您只需在形成集群之前在控制节点上执行初始配置。

有些功能在集群中无法扩展，控制节点将处理这些功能的所有流量。

集群控制链路

每个节点必须将一个接口作为集群控制链路的 VXLAN (VTEP) 接口。 有关 VXLAN 的详细信息，请参阅配置 VXLAN 接口。

VXLAN 隧道端点

VXLAN 隧道终端 (VTEP) 设备执行 VXLAN 封装和解封。每个 VTEP 有两种接口类型：一个或多个虚拟接口称为 VXLAN 网络标识符 (VNI) 接口；以及称为 VTEP 源接口的常规接口，用于为 VTEP 之间的 VNI 接口建立隧道。VTEP 源接口连接到传输 IP 网络，进行 VTEP 至 VTEP 通信。

VTEP 源接口

VTEP 源接口是一个计划要将其与 VNI 接口相关联的常规Firewall Threat Defense Virtual 接口。您可以将一个 VTEP 源接口配置为集群控制链路。源接口会被保留，以便仅供集群控制链路使用。每个 VTEP 源接口在同一子网上都有一个 IP 地址。此子网应与所有其他流量隔离，并且只包括集群控制链路接口。

VNI 接口

VNI 接口类似于 VLAN 接口：它是一个虚拟接口，通过使用标记，实现网络流量在给定物理接口上的分离。您只能配置一个 VNI 接口。每个 VNI 接口在同一子网上都有一个 IP 地址。

对等体 VTEP

与数据接口的常规 VXLAN 只允许单个 VTEP 对等体不同，Firewall Threat Defense Virtual 集群允许您配置多个对等体。

集群控制链路流量概述

集群控制链路流量包括控制流量和数据流量。

控制流量包括：

- 控制节点选举。
- 配置复制。
- 运行状况监控。

数据流量包括：

- 状态复制。
- 连接所有权查询和数据包转发。

配置复制

集群中的所有节点共享一个配置。您只能在控制节点上进行配置更改（引导程序配置除外），这些更改会自动同步到集群中的所有其他节点。

管理网络

您必须使用管理接口来管理每个节点；集群不支持从数据接口进行管理。

Threat Defense Virtual 集群的许可证

每个 Firewall Threat Defense Virtual 集群节点都需要相同的性能层许可证。我们建议为所有成员使用相同数量的CPU和内存，否则将限制所有节点上的性能，以匹配功能最低的成员。吞吐量级别将从控制节点复制到每个数据节点，以便它们匹配。

您可以将功能许可证分配到整个集群，而不是单个节点。但是，对于每个功能，集群中的每个节点都会使用一个单独的许可证。集群功能本身不需要任何许可证。

在将控制节点添加到 防火墙管理中心时，您可以指定要用于该集群的功能许可证。您可以在**设备** > **设备管理** 、**集群** > **许可证**区域中修改集群的许可证。

注释 如果在 防火墙管理中心 获得许可（并在评估模式下运行）之前添加了集群，当您许可 防火墙管理中心 时，会在将策略更改部署到集群时遇到流量中断的情况。更改为许可模式会导致所有数据单元先退出集群，然后重新加入。

Threat Defense Virtual 集群的要求和前提条件

型号要求

- FTDv5, FTDv10, FTDv20, FTDv30, FTDv50, FTDv100

注释 FTDv5 和 FTDv10 不支持 Amazon Web 服务 (AWS) 网关负载均衡器。

- 以下公共云服务：

  - Amazon Web 服务 (AWS)
  - Microsoft Azure
  - Google Cloud Platform (GCP)
- 最多 16 个节点

另请参阅 Cisco Secure Firewall Threat Defense Virtual 入门指南中的 Firewall Threat Defense Virtual 一般要求。

用户角色

- 管理员
- 访问管理员
- 网络管理员

硬件和软件要求

集群中的所有设备：

- 必须在同一个性能层。我们建议对所有节点都使用相同数量的CPU和内存，否则所有节点上的性能将受到限制，以匹配性能最低的节点。
- 必须从管理接口访问 防火墙管理中心；不支持数据接口管理。
- 除在映像升级时以外，必须运行完全相同的软件。支持无中断升级。
- 所有设备的集群控制链路接口必须位于同一子网中。

MTU

确保连接到集群控制链路的端口配置了正确（更高）的 MTU。如果存在不匹配的 MTU，则集群形成将失败。当某个节点加入集群时，它会向控制节点发送ping，其数据包大小与集群控制链路MTU匹配，从而检查 MTU 兼容性。如果初始 ping 失败，节点将使用较小的数据包大小（MTU 除以 2，然后除以 4，然后除以 8）尝试执行 ping，直到 ping 成功。如果 ping 失败，系统会生成通知，以便您纠正连接的交换机上 MTU 不匹配的问题，然后重试。

默认情况下，集群控制链路 MTU 会被设置为比数据接口高 154 字节。由于集群控制链路流量包括数据包转发，因此集群控制链路需要能够容纳完整大小的数据包以及集群流量开销（100 字节）加上 VXLAN 开销（54 字节）。

对于具有 GWLB 的 AWS，数据接口使用 Geneve 封装。在这种情况下，整个以太网数据报将被封装，因此，新数据包更大，需要更大的 MTU。您应将源接口 MTU 设置为网络 MTU + 306 字节。因此，对于标准的 1500 MTU 网络路径，源接口 MTU 应为 1806，而集群控制链路 MTU 应为 +154, 1960。

对于具有 GWLB 的 Azure，数据接口使用 VXLAN 封装。在这种情况下，整个以太网数据报将被封装，因此，新数据包更大，需要更大的 MTU。您应将集群控制链路 MTU 设置为源接口 MTU + 80 字节。

下表显示了集群控制链路 MTU 和数据接口 MTU 的默认值。

注释 我们不建议将集群控制链路 MTU 设置为介于 2561 和 8362 之间的值；由于块池处理，此 MTU 大小不是系统运行的最佳值。

表 *1:* 默认 ***MTU***

公共云	集群控制链路 **MTU**	数据接口 **MTU**
具有 GWLB 的 AWS	1980 年	1826
AWS	1654	1500
具有 GWLB 的 Azure	1454	1374
Azure	1454	1300
GCP	1554	1400

Threat Defense Virtual 集群的准则

高可用性

集群不支持高可用性。

IPv6

集群控制链路只有在使用 IPv4 时才受支持。

多区域集群

多区域集群最多支持三个区域。

其他准则

- 当拓扑发生重大更改时（例如添加或删除 EtherChannel 接口、启用或禁用 Firewall Threat Defense 或交换机上的接口、添加其他交换机以形成 VSS、vPC 或 VNet），应禁用运行状况检查功能，另外还应为禁用的接口禁用接口监控。当拓扑更改完成且配置更改已同步到所有设备后，您可以重新启用接口运行状态检查功能。

- 将节点添加到现有集群时或重新加载节点时，会有限地暂时丢弃数据包/断开连接；这是预期的行为。有些时候，丢弃的数据包会挂起连接；例如，丢弃 FTP 连接的 FIN/ACK 数据包将使 FTP 客户端挂起。在此情况下，您需要重新建立 FTP 连接。
- 请勿在节点上禁用集群之前关闭该节点。
- 对于解密的 TLS/SSL 连接，解密状态不同步，如果连接所有者失败，则解密的连接将重置。需要与新节点建立新的连接。未解密的连接（它们匹配“不解密”规则）不受影响，并且可以正确复制。
- 不支持动态扩展。
- 如果您使用的是 Cisco Secure Firewall 版本 7.2 或 7.3，则在 AWS 上部署集群时不支持状态目标故障切换。
- 在每个维护窗口完成后执行全局部署。
- 确保不要一次从自动扩展组 (AWS)/实例组 (GCP) /规模集 (Azure)中删除多个设备。我们还建议您先在设备上运行 **cluster disable** 命令，然后再从组东扩展组 (AWS) / 实例组 (GCP) / 规模集 (Azure)中删除设备。
- 如果要禁用集群中的数据节点和控制节点，我们建议您在禁用控制节点之前先禁用数据节点。如果在集群中有其他数据节点时禁用了某个控制节点，则必须将其中一个数据节点升级为控制节点。请注意，角色更改可能会对集群造成干扰。
- 在本指南中提供的自定义 Day 0 配置脚本中，您可以根据需要更改 IP 地址，提供自定义接口名称，并更改 CCL-Link 接口的顺序。
- 如果在云平台上部署 Threat Defense Virtual 集群后遇到 CCL 不稳定问题（例如间歇性 ping 失败），我们建议您解决导致 CCL 不稳定的原因。此外，您可以增加保持时间，作为在一定程度上缓解 CCL 不稳定问题的临时解决方法。有关如何更改保持时间的详细信息，请参阅 编辑集群运行状况监控设置。
- 为 Management Center Virtual 配置安全防火墙规则或安全组时，必须在源 IP 地址范围中包括 Firewall Threat Defense Virtual 的专用和公共 IP 地址。此外，请确保在 Firewall Threat Defense Virtual的安全防火墙规则或安全组中指定 Firewall Management Center Virtual 的专用和公共 IP 地址。这对于确保在集群部署期间正确注册节点非常重要。

集群默认设置

- 将自动生成 cLACP 系统 ID 且系统优先级默认为 1。
- 默认情况下，集群运行状况检查功能处于启用状态，保持时间为 3 秒。默认情况下，在所有接口上启用接口运行状况监控。
- 用于发生故障的集群控制链路的集群自动重新加入功能为每 5 分钟尝试无限次。
- 用于发生故障的数据接口的集群自动重新加入功能为每 5 分钟尝试 3 次，增量间隔设置为 2。
- 对于 HTTP 流量，默认启用 5 秒的连接复制延迟。

在 AWS 中部署集群

要在 AWS 中部署集群，您可以手动部署或使用 CloudFormation 模板来部署堆栈。您可以将集群与 AWS 网关负载均衡器或非本地负载均衡器（例如思科云服务路由器）配合使用。

从版本 10.0.0 开始，AWS Geneve 集群解决方案支持单臂和双臂部署模式，为网络架构提供更高的灵活性。

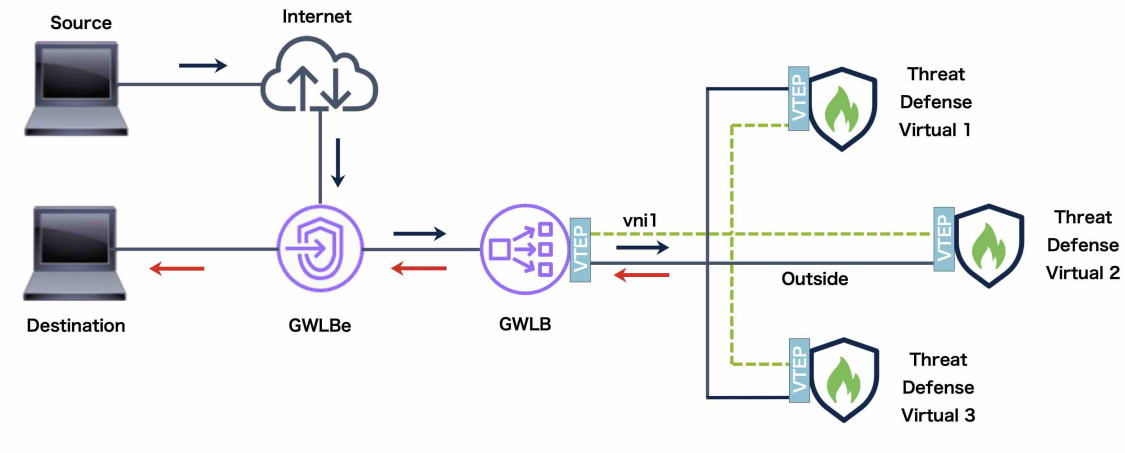
AWS 网关负载均衡器和 Geneve 单臂代理

注释 这是 Geneve 接口当前唯一支持的使用案例。

AWS 网关负载均衡器结合了透明网络网关和按需分配流量和扩展虚拟设备的负载均衡器。Threat Defense Virtual 支持具有分布式数据平面的网关负载均衡器集中控制平面（网关负载均衡器终端）。下图显示了从网关负载均衡器终端转发到网关负载均衡器的流量。网关负载均衡器会在多个 Threat Defense Virtual 流量之间进行均衡，这些流量在丢弃流量或将其发送回网关负载均衡器之前对其进行检查（掉头流量）。然后，网关负载均衡器会将流量发送回网关负载均衡器终端和目的地。

注释 AWS 上的 Geneve 单臂设置不支持传输层安全 (TLS) 服务器身份发现。

图 *1: Geneve* 单臂代理



拓扑示例

Firewall Threat Defense Virtual 在 AWS 区域的单个和多个可用性区域中使用自动扩展进行集群

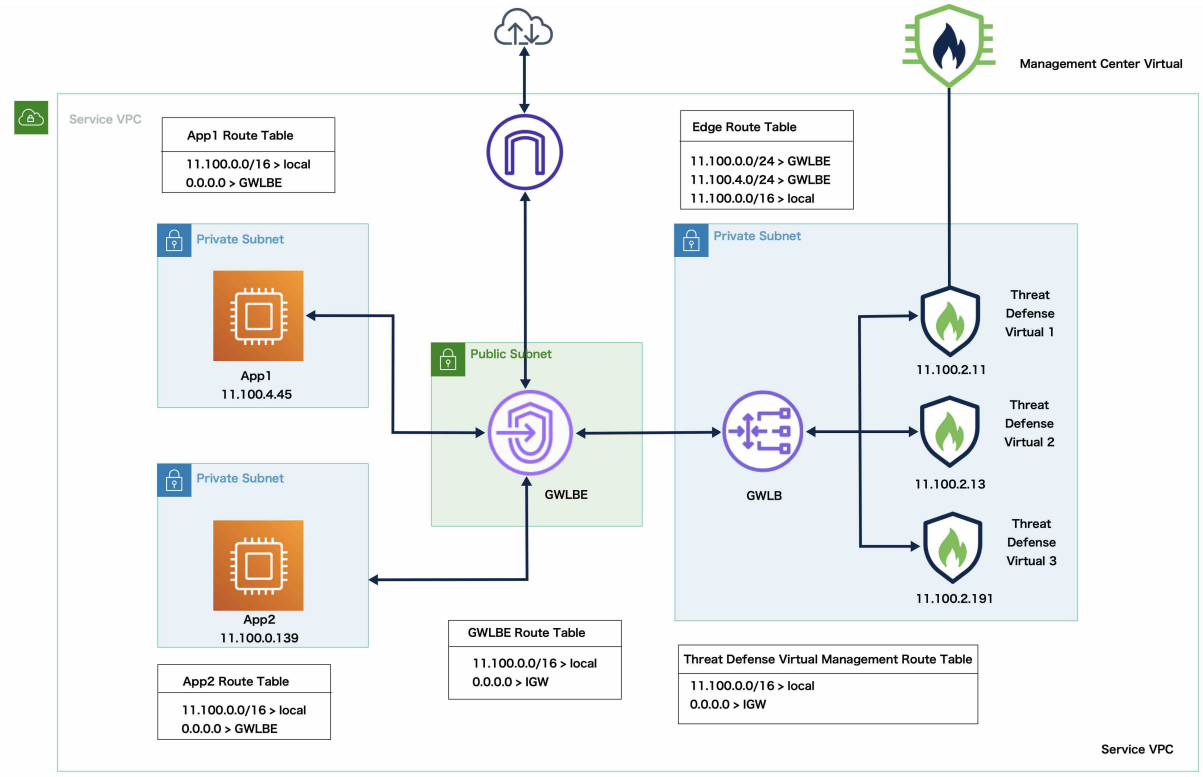
可用性区域是指一个 AWS 区域内独立运行的独立数据中心或一组独立数据中心。每个区域都有自己的网络基础设施、连接和电源，从而确保一个区域的故障不会影响到其他区域。为了提高冗余和可靠性，公司在灾难恢复计划中使用多个可用性区域。

跨多个可用性区域部署 Firewall Threat Defense Virtual 并配置支持动态扩展的集群可以显着增强基础设施的可用性和可扩展性。此外，在同一区域利用多个可用性区域可以提供额外的冗余，并在发生故障时保证高可用性。

您可以修改集群控制链路 (CCL) 的 IP 分配机制，以支持 AWS 上 Firewall Threat Defense Virtual 群集的单可用性区域和多可用性区域部署。下面给出的拓扑结构描述了具有自动扩展能力的单个和多个可用性区域中的入站和出站流量。

Firewall Threat Defense Virtual 在单个可用性区域中使用自动扩展进行集群

集群中有两个连接到 GWLB 的 Firewall Threat Defense Virtual 实例。

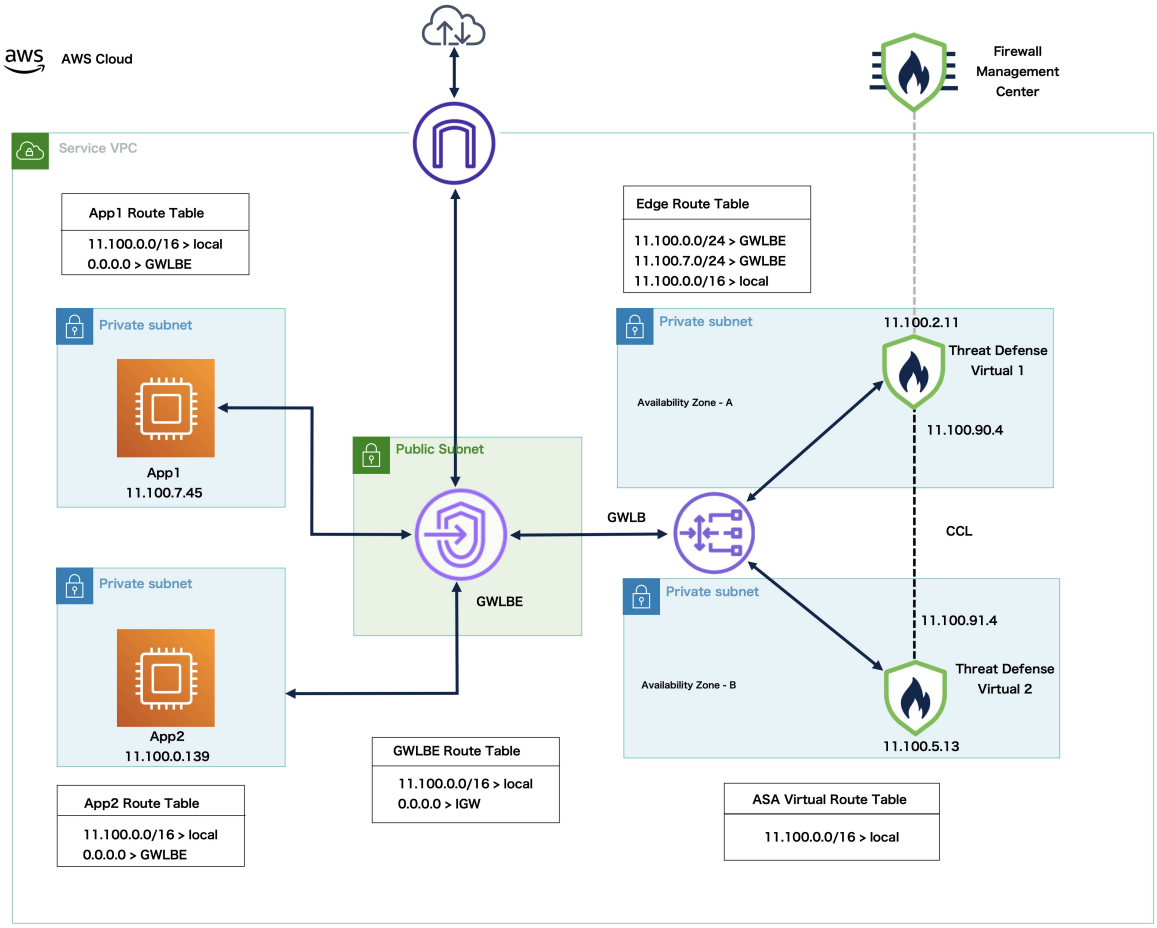


来自互联网的入站流量会进入GWLB端点，然后由端点将流量传输到GWLB。然后，流量被转发到 Firewall Threat Defense Virtual 集群。集群中的 Firewall Threat Defense Virtual 实例检测到流量后，将其转发到应用虚拟机 App1。

来自 App1 的出站流量将传输到 GWLB 终端 > GWLB > TDv > GWLB > GWLB 终端，然后由 GWLB 终端发送到互联网。

Firewall Threat Defense Virtual 在多个可用性区域中使用自动扩展进行集群

集群中有两个 Firewall Threat Defense Virtual 实例连接到 GWLB，它们位于不同的可用性区域。

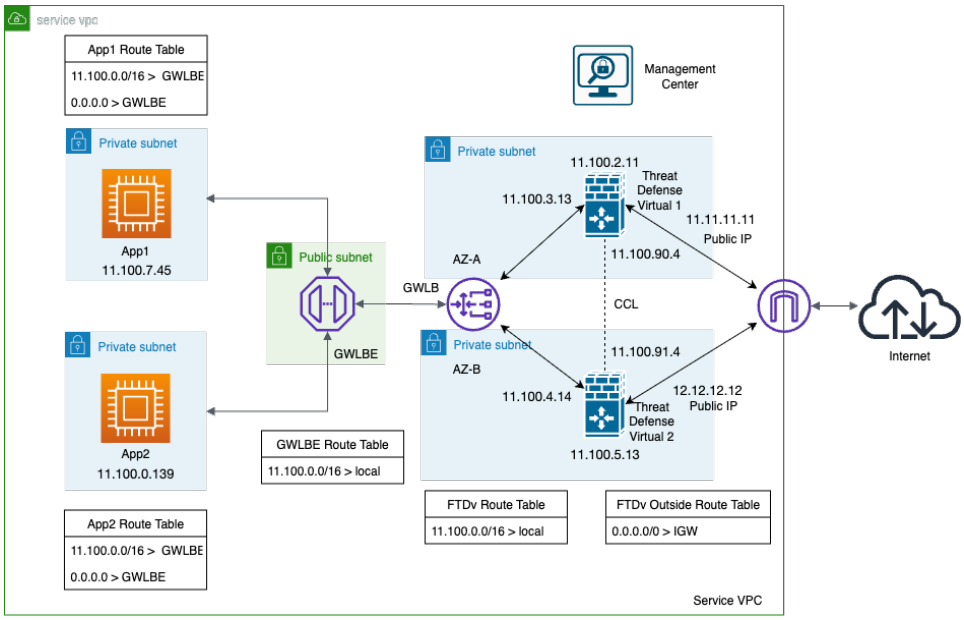


注释 从 Firewall Threat Defense Virtual 版本 7.6.0 及更高版本开始支持多可用性区域部署。

来自互联网的入站流量会进入GWLB端点，然后由端点将流量传输到GWLB。然后，根据可用性区域将流量路由到 Firewall Threat Defense Virtual 集群。集群中的 Firewall Threat Defense Virtual 实例检测到流量后，将其转发到应用虚拟机 App1。

AWS 网关负载均衡器和 Geneve 双臂代理

双臂代理是一种网络部署模式，可使 Threat Defense Virtual 检测流量，应用网络地址转换 (NAT)，并通过互联网网关将其从其外部接口直接发送到互联网。此直接出口路径会绕过 GWLB 及其出口终端，从而简化流量以提高效率。此方法在多 VPC 环境中特别有效，其中来自多个 VPC 的出站流量可以共享一个公共出口点。这降低了对基础设施的要求，从而使该解决方案更具成本效益。此外，它还支持集群，以提高流量处理效率。

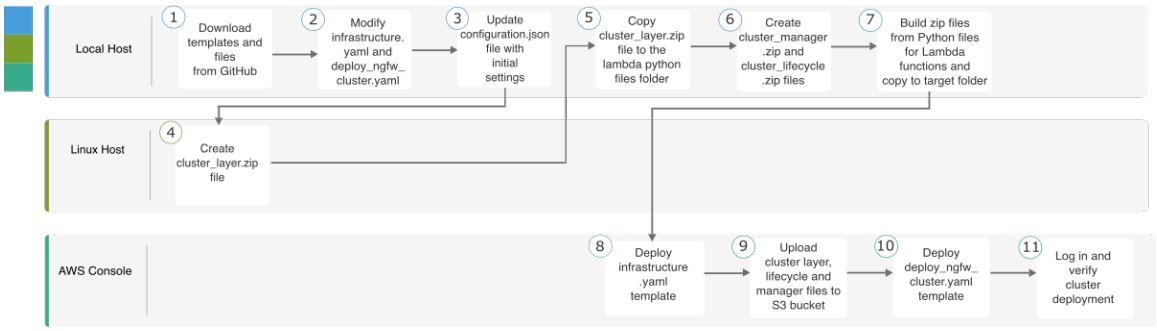


此部署的目的是使用双臂设计中跨单独可用区部署的集群 Threat Defense Virtual 实例，在应用程序将流量发送到互联网之前检查流量，其中内部接口处理入口流量，外部接口处理出口流量。在此流程中，来自 应用的流量将路由到 GWLB，由 GWLB 将流量转发到 Threat Defense Virtual 的内部接口进行检查。应用 NAT 后，Threat Defense Virtual 通过其外部接口将流量直接发送到互联网网关。

在 AWS 上部署 Threat Defense Virtual 集群的端到端流程

基于模板的部署

以下流程图说明了在 AWS 上基于模板部署 Threat Defense Virtual 集群的工作流程。



	工作空间	步骤
1	本地主机	从 Github 克隆存储库
2	本地主机	修改 *infrastructure.yaml* 和 *deploy_ngfw_cluster.yaml* 模板。

	工作空间	步骤
3	本地主机	使用 FMC 对象名称更新 *Configuration.json* 文件。
4	Linux 主机	创建 *cluster_layer.zip* 文件。
5	本地主机	将 *cluster_layer.zip* 文件复制到 Lambda python files 文件夹。
6	本地主机	创建 *cluster_manager.zip*、*custom_metrics_publisher.zip* 和 *cluster_lifecycle.zip* 文件。
7	本地主机	从 Python 文件为 Lambda 函数构建 zip 文件，并复制到目标文件夹。
8	AWS 控制台	部署 *Infrastructure.yaml* 模板。
9	AWS 控制台	将 *cluster_layer.zip*、*cluster_lifecycle.zip*、*custom_metrics_publisher.zip* 和 *cluster_manager.zip* 上传到 S3 存储桶。
10	AWS 控制台	部署 *deploy_ngfw_cluster.yaml* 模板。
11	AWS 控制台	登录并验证集群部署。

手动部署

以下流程图说明了在 AWS 上手动部署 Threat Defense Virtual 集群的工作流程。

	工作空间	步骤
1	本地主机	创建 Day 0 配置脚本。
2	AWS 控制台	部署 Threat Defense Virtual 实例。

	工作空间	步骤
3	AWS 控制台	将接口连接到实例。
4	AWS 控制台	验证节点是否已加入集群。
5	AWS 控制台	创建目标组和 GWLB；将目标组附加到 GWLB。
6	AWS 控制台	使用数据接口 IP 向目标组注册实例。
7	管理中心	注册控制节点。

模板

以下提供的模板可在GitHub中获取。参数值一目了然，包括模板中给出的参数名称、默认值、允许值和说明。

- Infrastructure.yaml - 基础设施部署模板。
- deploy_ngfw_cluster.yaml - 用于集群部署的模板。

注释 在部署集群节点之前，请确保检查支持的 AWS 实例类型列表。此列表可在 *deploy_ngfw_cluster.yaml* 模板中的参数 InstanceType 的允许值下找到。

使用 CloudFormation 模板在 AWS 中部署堆栈

使用自定义 CloudFormation 模板在 AWS 中部署堆栈。

开始之前

- 您需要安装了 Python 3 的 Amazon Linux 虚拟机。
- 要允许集群自动注册到 防火墙管理中心，您需要在 防火墙管理中心 上创建两个具有管理权限且可以使用 REST API 的用户。请参阅*Cisco Secure Firewall Management Center* 管理指南。
- 在 防火墙管理中心 中添加与您在 `Configuration.json` 中指定的策略名称匹配的访问策略。

过程

步骤 1 准备模板。

a) 将 GitHub 存储库克隆到本地文件夹。请参阅https://github.com/CiscoDevNet/cisco-ftdv/tree/master/cluster/aws。
b) 使用所需的参数修改 **infrastructure.yaml** 和 **deploy_ngfw_cluster.yaml**。
c) 使用初始设置修改 **cluster/aws/lambda-python-files/Configuration.json**。

例如：

```
{
  "licenseCaps": ["BASE", "MALWARE", "THREAT"],
  "performanceTier": "FTDv50",
  "fmcIpforDeviceReg": "DONTRESOLVE",
  "RegistrationId": "cisco",
  "NatId": "cisco",
  "fmcAccessPolicyName": "AWS-ACL"
}
```

- 将 fmcIpforDeviceReg 设置保留为 DONTRESOLVE。
- fmcAccessPolicyName 需要与 防火墙管理中心 上的访问策略匹配。

注释
不支持 FTDv5 和 FTDv10 层。

d) 创建名为 **cluster_layer.zip** 的文件，为 Lambda 函数提供必要的 Python 库。

我们建议使用安装了 Python 3.9 的 Amazon Linux 创建 **cluster_layer.zip** 文件。

注释
如果您需要 Amazon Linux 环境，可以使用 Amazon Linux 2023 AMI 或运行最新版本的 Amazon Linux 的 AWS Cloudshell 创建 EC2 实例。

要创建 cluster-layer.zip 文件，您需要先创建包含 python 库软件包详细信息的 **requirements.txt** 文件，然后运行 shell 脚本。

1. 通过指定 python 软件包详细信息来创建 **requirements.txt** 文件。

   以下是您在 **requirements.txt** 文件中提供的示例软件包详细信息：

   ```
   $ cat requirements.txt
   pycryptodome
   paramiko
   requests
   scp
   jsonschema
   cffi
   zipp
   importlib-metadata
   ```

2. 运行以下 shell 脚本以创建 **cluster_layer.zip**文件。

   ```
   $ pip3 install --platform manylinux2014_x86_64
   --target=./python/lib/python3.9/site-packages
   --implementation cp --python-version 3.9 --only-binary=:all:
   --upgrade -r requirements.txt
   $ zip -r cluster_layer.zip ./python
   ```

注释

如果在安装期间遇到依赖项冲突错误（例如 urllib3 或加密），建议您在 **requirements.txt** 文件中包含冲突软件包及其建议版本。之后，您可以再次运行安装来解决冲突。

e) 将生成的 **cluster_layer.zip** 文件复制到 lambda python files 文件夹 - `cluster/aws/lambda-python-files`。

f) 创建 **cluster_layer.zip**、**custom_metrics_publisher.zip**、 **cluster_manger.zip** 和 **lifecycle_ftdv.zip** 文件。

可以在克隆存储库 (`cluster/aws/make.py`) 中找到 **make.py** 文件。这样会将 python 文件压缩为 Zip 文件并复制到目标文件夹。

python3 make.py build

注释
如果您使用专用 IP 地址进行 Management Center Virtual 注册，请确保在 `cisco-ftdv/cluster/aws/lambda-python-files/constant.py` 文件中将 USE_PUBLIC_IP_FOR_FMC_CONN 设置为 False 。

步骤 2 部署 **Infrastructure.yaml** 并记下集群部署的输出值。 在部署基础设施堆栈之前，必须确定将使用的 AWS 区域和可用性区域。每个 AWS 区域都有一组不同的可用性区域和 VPC 基础设施，因此必须为部署选择正确的区域和可用性区域。

a) 在 AWS 控制台上，转到 **CloudFormation** 并点击**创建堆栈 (Create stack)**；选择**使用新资源（标准）(With new resources [standard])**。

b) 选择**上传模板文件 (Upload a template file)**，点击**选择文件 (Choose file)**，然后从目标文件夹中选择 **infrastructure.yaml**。

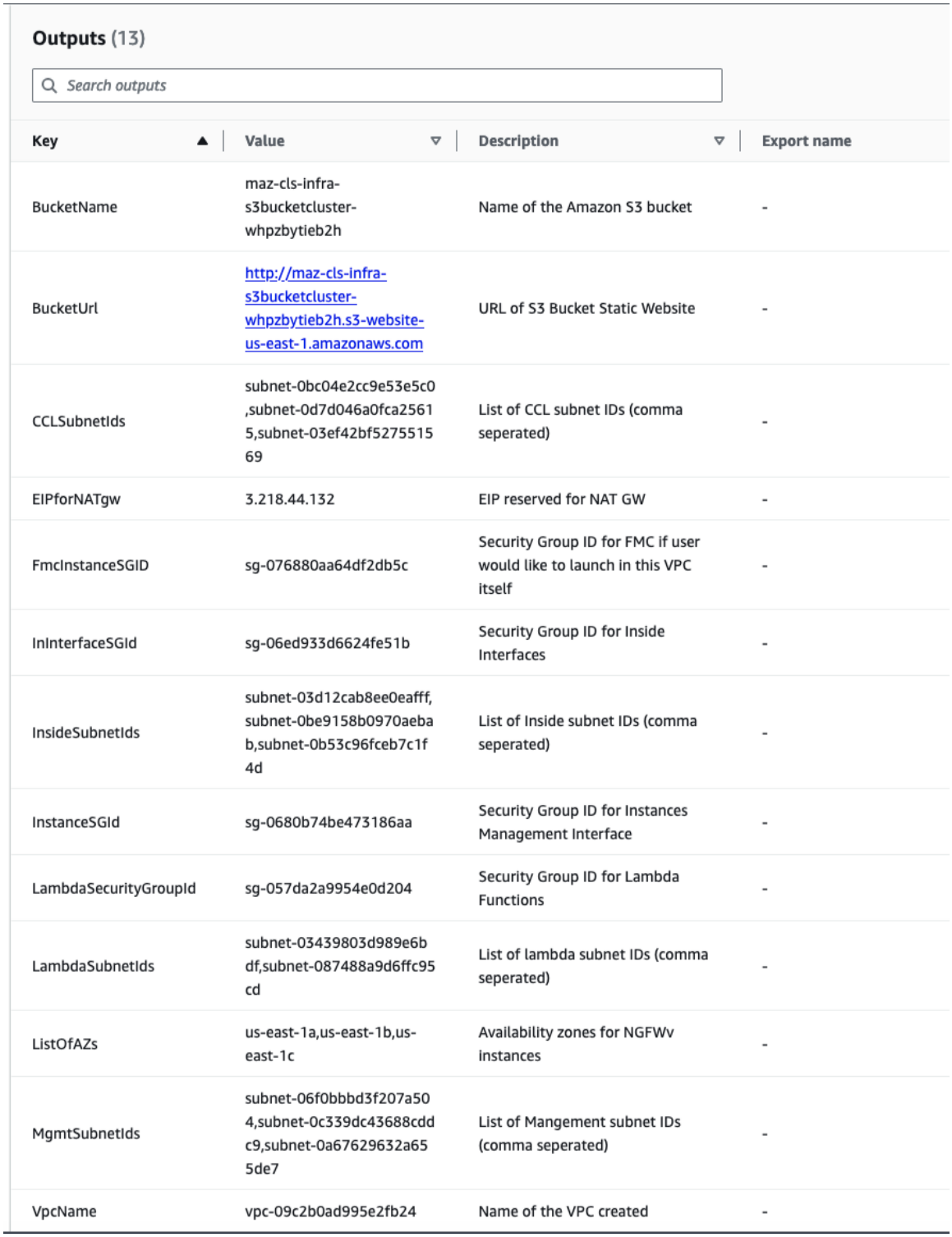
c) 点击**下一步 (Next)** 并提供所需的信息。

参数	允许的值/类型	说明
ClusterName	字符串	输入唯一的集群名称。
ClusterNumber	数字	输入唯一的集群编号。
DeploymentType	字符串	指定是否需要“单臂”或“双臂”部署。 注释 双臂模式支持 10.0.0 及更高版本。
VpcCidr	字符串	为新 VPC 输入 CIDR 块
NoOfAZs	数字	对于 7.6.0 及更高版本，选择 2 或 3 个可用区 (AZ)；对于较低版本，选择 1AZ。 管理、内部、外部和CCL 子网将相应地分布在所选 AZ 中。
ListOfAZs	名单	选择可用区（数量应与可用区数量匹配）
MgmtSubnetNames	CommaDelimitedList	管理子网名称（路由为“互联网 GW”）

参数	允许的值/类型	说明
MgmtSubnetCidrs	CommaDelimitedList	管理子网 Cidr 列表
InsideSubnetNames	CommaDelimitedList	内部子网名称（路由为专用）
InsideSubnetCidrs	CommaDelimitedList	内部子网 Cidr 列表
OutsideSubnetNames	CommaDelimitedList	外部子网名称（路由为“互联网 GW”）（仅双臂模式）
OutsideSubnetCidrs	CommaDelimitedList	输入外部子网 Cidr 列表（仅双臂模式）
CCLSubnetNames	CommaDelimitedList	输入 CCL 子网名称
CCLSubnetCidrs	CommaDelimitedList	输入 CCL 子网 CIDR
LambdaAZs	名单	为 Lambda 选择 2 个可用区
LambdaSubnetNames	CommaDelimitedList	输入 Lambda 子网名称（路由为 NAT GW），用于 Lambda 函数
LambdaSubnetCidrs	CommaDelimitedList	输入 Lambda 子网 CIDR

d) 为集群输入唯一的**集群名称**和**集群编号**。
e) 从**可用性区域 (Availability Zone)** 列表中选择可用性区域。此字段仅列出基于 AWS 区域的可用性区域，您选择该区域是为了使用 ClusterFormation 模板部署基础设施堆栈。
f) 点击**下一步 (Next)**，然后点击**创建堆栈 (Create stack)**。
g) 在部署完成后，转到**输出 (Outputs)** 并记下 S3 **BucketName**。

图 *2: infrastructure.yaml* 的输出



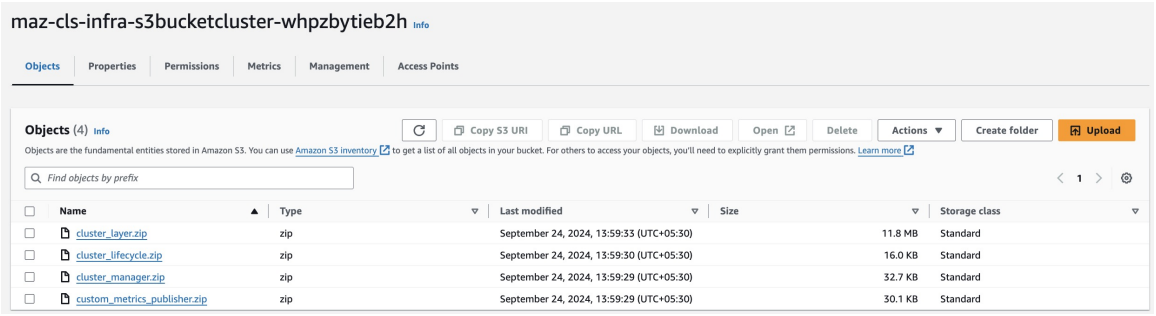
Outputs (13)

Search outputs

Key	Value	Description	Export name
BucketName	maz-cls-infra-s3bucketcluster-whpzbytieb2h	Name of the Amazon S3 bucket	-
BucketUrl	http://maz-cls-infra-s3bucketcluster-whpzbytieb2h.s3-website-us-east-1.amazonaws.com	URL of S3 Bucket Static Website	-
CCLSubnetIds	subnet-0bc04e2cc9e53e5c0,subnet-0d7d046a0fca25615,subnet-03ef42bf527551569	List of CCL subnet IDs (comma seperated)	-
EIPforNATgw	3.218.44.132	EIP reserved for NAT GW	-
FmcInstanceSGID	sg-076880aa64df2db5c	Security Group ID for FMC if user would like to launch in this VPC itself	-
InInterfaceSGId	sg-06ed933d6624fe51b	Security Group ID for Inside Interfaces	-
InsideSubnetIds	subnet-03d12cab8ee0eafff,subnet-0be9158b0970aebab,subnet-0b53c96fceb7c1f4d	List of Inside subnet IDs (comma seperated)	-
InstanceSGId	sg-0680b74be473186aa	Security Group ID for Instances Management Interface	-
LambdaSecurityGroupId	sg-057da2a9954e0d204	Security Group ID for Lambda Functions	-
LambdaSubnetIds	subnet-03439803d989e6bdf,subnet-087488a9d6ffc95cd	List of lambda subnet IDs (comma seperated)	-
ListOfAZs	us-east-1a,us-east-1b,us-east-1c	Availability zones for NGFWv instances	-
MgmtSubnetIds	subnet-06f0bbbd3f207a504,subnet-0c339dc43688cddc9,subnet-0a67629632a655de7	List of Mangement subnet IDs (comma seperated)	-
VpcName	vpc-09c2b0ad995e2fb24	Name of the VPC created	-

步骤 3 将 **cluster_layer.zip**、**cluster_manager.zip**、**custom_metrics_publisher.zip** 和 **cluster_lifecycle.zip** 上传到由 **infrastructure.yaml** 创建的 S3 存储桶。

图 *3: S3* 桶



注释
确保 Lambda NAT 网关的弹性 IP 地址已添加到与 Management Center Virtual 相关联的安全组。

步骤 4 部署 **deploy_ngfw_cluster.yaml**。

a) 转到 **CloudFormation** 并点击**创建堆栈 (Create stack)**；选择**使用新资源（标准）(With new resources [standard])**。

b) 选择**上传模板文件 (Upload a template file)**，点击**选择文件 (Choose file)**，然后从目标文件夹中选择 **deploy_ngfw_cluster.yaml**。

c) 点击**下一步 (Next)** 并提供所需的信息。

d) 提供以下集群和基础设施配置信息。

参数	允许的值/类型	说明
集群配置		
ClusterGrpNamePrefix	字符串	这是集群名称前缀。集群编号将作为后缀添加。
ClusterNumber	字符串	这是集群编号。这将作为集群名称的后缀 (msa-ftdv-infra)。例如，如果此值为 **1**，则组名称将为 *msa-ftdv-infra-1*。 它应至少为 1 个数字，但不超过 3 个数字。默认值：1。
集群大小	数字	这是集群中 Firewall Threat Defense Virtual 节点的总数。 最小值：1 最大值：16
DeploymentType	字符串	指定是否需要“单臂”或“双臂”部署。 **注释** 双臂模式支持 10.0.0 及更高版本。

参数	允许的值/类型	说明
DiagnosticInterface	字符串	指定是否需要诊断接口。 "ON" - 将附加诊断接口。 “OFF”- 不会附加诊断接口。 **注释** “OFF”支持 10.0.0 及更高版本。
基础设施详细信息		
NoOfAZs	字符串	这是部署 Firewall Threat Defense Virtual 的可用性区域总数。（根据地区的不同，可用性区域的数量从最少 1 个到最多 3 个不等）。 子网将在这些可用性区域内创建。 此列表中可用的可用性区域基于为部署集群而选择的区域。 **注释** 根据此参数在三个可用性区域中创建管理、内部和集群控制链路 (CCL) 子网。
AZ	字符串	可用性区域列表基于您计划部署的区域。 在可用性区域列表中，选择有效的可用性区域（1 个或 2 个可用性区域或 3 个可用性区域）。 计数应与可用性区域数量参数的值匹配。
NotifyEmailID	字符串	集群事件邮件将发送到的邮件地址。您必须接受订用电子邮件请求，才能收到此电子邮件通知。 示例：admin@company.com
VpcId	字符串	集群组的 VPC ID。 类型：AWS::EC2::VPC::Id
S3BktName	字符串	包含已上传的 Lambda zip 文件的 S3 存储桶。您必须指定正确的存储桶名称。
MgmtSubnetIds	名单	每个可用性区域只能输入一个子网。 如果从同一可用性区域选择多个子网，则选择不正确的子网可能会导致部署 Firewall Threat Defense Virtual 实例时出现问题。 类型：List<AWS::EC2::Subnet::Id>
InsideSubnetIds	名单	为每个可用性区域至少输入一个子网。

参数	允许的值/类型	说明
		如果选择来自同一可用性区域的多个子网，则选择不正确的子网可能会导致部署 Firewall Threat Defense Virtual 实例时出现问题。 类型：List<AWS::EC2::Subnet::Id>
OutsideSubnetIds	CommaDelimitedList	（仅双臂模式） 每个 AZ 仅提供一个子网。如果选择了来自同一 AZ 的多个子网，错误的子网选择将在部署 NGFWv 实例时导致问题。 确保添加来自所提供 AZ 的子网。
LambdaSubnets	列表	为 Lambda 函数输入至少两个子网。您输入的两个子网必须具有 NAT 网关，以使 Lambda 函数能够与 AWS 服务（即公共 DNS）通信。 类型：List<AWS::EC2::Subnet::Id>
CCLSubnetIds	字符串	为每个可用性区域至少输入一个子网。 如果选择来自同一可用性区域的多个子网，则选择不正确的子网可能会导致部署 Firewall Threat Defense Virtual 实例时出现问题。 类型：List<AWS::EC2::Subnet::Id>
CCLSubnetRanges	字符串	输入不同可用性区域的 CCL 子网的 IP 地址范围。 排除前 4 个保留的 IP 地址。集群控制链路 (CCL) 的 IP 地址池。 IP 地址从 CCL IP 地址池分配给 Firewall Threat Defense Virtual 实例的 CCL 接口。
MgmtInterfaceSG	名单	为 Firewall Threat Defense Virtual 实例选择安全组 ID。 类型：List<AWS::EC2::SecurityGroup::Id>
InsideInterfaceSG	名单	为 Firewall Threat Defense Virtual 实例的内部接口选择安全组 ID。 类型：List<AWS::EC2::SecurityGroup::Id>
OutsideInterfaceSG	字符串	（仅双臂模式） 为 NGFWv 实例外部接口提供安全组 ID。
LambdaSG	列表	为 Lambda 函数选择一个安全组。 确保出站连接设置为 **ANYWHERE**。

参数	允许的值/类型	说明
		类型：List<AWS::EC2::SecurityGroup::Id>
CCLInterfaceSG	名单	为 Firewall Threat Defense Virtual 实例的 CCL 接口选择安全组 ID。
DualArmAppCidrList	CommaDelimitedList	（仅双臂模式） 输入用于东西向流量的双臂应用 CIDR。
GWLB 配置		
DeployGWLBE	字符串	点击**是**部署 GWLB 端点。 默认情况下，该值设置为**否**。
VpcIdLBE	字符串	输入 VPC 以部署网关负载均衡器终端。 **注释** 如果不部署GWLB终端，请不要在此字段中输入任何值。
GWLBESubnetId	字符串	仅输入一个子网 ID。 **注释** 如果不部署GWLB终端，请不要在此字段中输入任何值。 确保子网属于正确的 VPC 以及您指定的可用性区域。
TargetFailover	字符串	当目标发生故障或取消注册时，启用目标故障转移支持。（默认情况下，此参数的值设置为 **rebalance**）。 • **no_rebalance**：将现有流量导向故障目标，将新流量导向健康目标，从而确保向后兼容性。 • **rebalance**：重新分配现有流量，同时确保新流量流向正常运行的目标。 从 Firewall Threat Defense Virtual 版本7.4.1 及更高版本开始支持 *rebalance*。
TgHealthPort	字符串	输入 GWLB 的运行状况检查端口。 **注释** 默认情况下，此端口不得用于流量。 确保您提供的值是有效的 TCP 端口。默认值：8080

参数	允许的值/类型	说明
思科 NGFWv 实例配置		
InstanceType	字符串	思科 Firewall Threat Defense Virtual EC2 实例类型。 确保 AWS 区域支持您选择的实例类型。 默认情况下，**c5.xlarge** 处于选中状态。 **注释** 当诊断接口为“ON”时，双臂部署仅支持 _.4xlarge。
LicenseType	字符串	选择思科 Firewall Threat Defense Virtual EC2 实例许可证类型。确保您在 **AMI-ID** 参数中输入的 AMI ID 的许可类型相同。 默认情况下，选择 **BYOL**。
AssignPublicIP	字符串	将该值设置为 **true** 可从 AWS IP 地址池为 Firewall Threat Defense Virtual 分配公共 IP 地址。
AmiID	字符串	根据地区、版本和许可证类型（BYOL 或 PAYG）选择正确的 AMI ID。 Firewall Threat Defense Virtual 7.2 及更高版本支持集群，Firewall Threat Defense Virtual 7.6 及更高版本支持自动扩展和多个可用性区域增强功能。 类型：AWS::EC2::Image::Id
ngfwPassword	字符串	Firewall Threat Defense Virtual 实例密码。 所有 Firewall Threat Defense Virtual 实例都提供一个默认密码，该密码位于启动模板（集群组）的 Userdata 字段中。 密码将在 Firewall Threat Defense Virtual 可访问后激活。 最小长度必须为 8 个字符。密码可以是纯文本密码，也可以是 KMS 加密密码。
KmsArn	字符串	输入现有 KMS（用于静态加密的 AWS KMS 密钥）的 ARN。 如果在此字段中指定值，则 Firewall Threat Defense Virtual 实例的**管理员**密码必须是加密密码。 生成加密密码示例：*“aws kms encrypt --key-id <KMS ARN> --plaintext <password>”*

参数	允许的值/类型	说明
		密码加密必须仅使用指定的 ARN 进行。
FMC 自动化配置		
fmcDeviceGrpName	字符串	在管理中心中输入集群组的唯一名称。
fmcPublishMetrics	字符串	选择 **true** 以创建 Lambda 函数以轮询管理中心，并将特定设备组指标发布到 AWS CloudWatch。 允许的值： • true • false 默认情况下，该值设置为 **true**。
fmcMetricsUsername	字符串	输入用于从管理中心轮询内存指标的唯一内部用户名。 用户必须具有**网络管理员**和**维护用户**权限或更高权限。
fmcMetricsPassword	字符串	输入密码。 如果您提到了 KMS 主密钥 ARN 参数，请确保提供加密密码。 确保输入正确的密码，因为输入错误的密码可能会导致指标收集失败。
fmcServer	字符串	IP 地址可以是外部 IP 地址，也可以是在 VPC 的 Firewall Threat Defense Virtual 管理子网中可访问的 IP 地址。 最小长度：7 最大长度：15
fmcOperationsUsername	字符串	为 CloudWatch 的 Firewall Management Center Virtual 提供唯一的内部用户名。 用户必须拥有**管理员**权限。
fmcOperationsPassword	字符串	输入密码。 如果您提到了 KMS 主密钥 ARN 参数，请确保提供加密密码。
扩展配置		

参数	允许的值/类型	说明
CpuThresholds	CommaDelimitedList	（可选）指定非零的下阈值和上阈值将创建比例策略。如果选择(0,0)，则不会创建CPU扩展警报或策略。评估点和数据点采用默认值或建议值。 默认情况下，此模板中启用**自动扩展**。部署后可以禁用自动扩展。
MemoryThresholds	CommaDelimitedList	指定非零下限和上限阈值将创建扩展策略。如果选择 (0,0)，则不会创建内存扩展警报或策略。评估点和数据点采用默认值或建议值。

e) 点击**下一步**。
f) 点击以确认所有 AWS CloudFormation 选项。
g) 点击**提交 (Submit)** 以部署集群。
h) 点击**下一步 (Next)**，然后点击**创建堆栈 (Create stack)**。

Lambda 函数将管理该过程的其余部分，并且 Firewall Threat Defense Virtual 将自动注册到 防火墙管理中心。

图 *4:* 已部署的资源

状态从 **CREATE_IN_PROGRESS** 更改为 **CREATE COMPLETE**，表示部署成功。

步骤 5 通过登录到任何一个节点并使用 **show cluster info** 命令来验证集群部署。

图 *5:* 集群节点

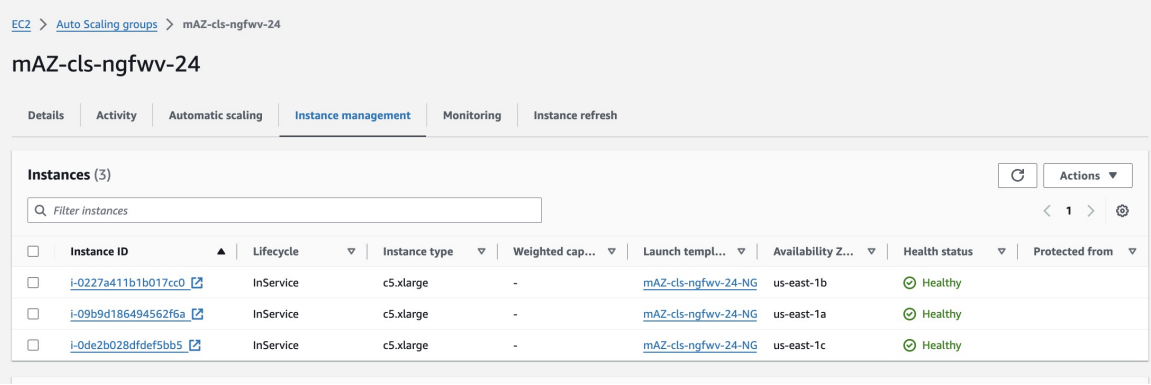
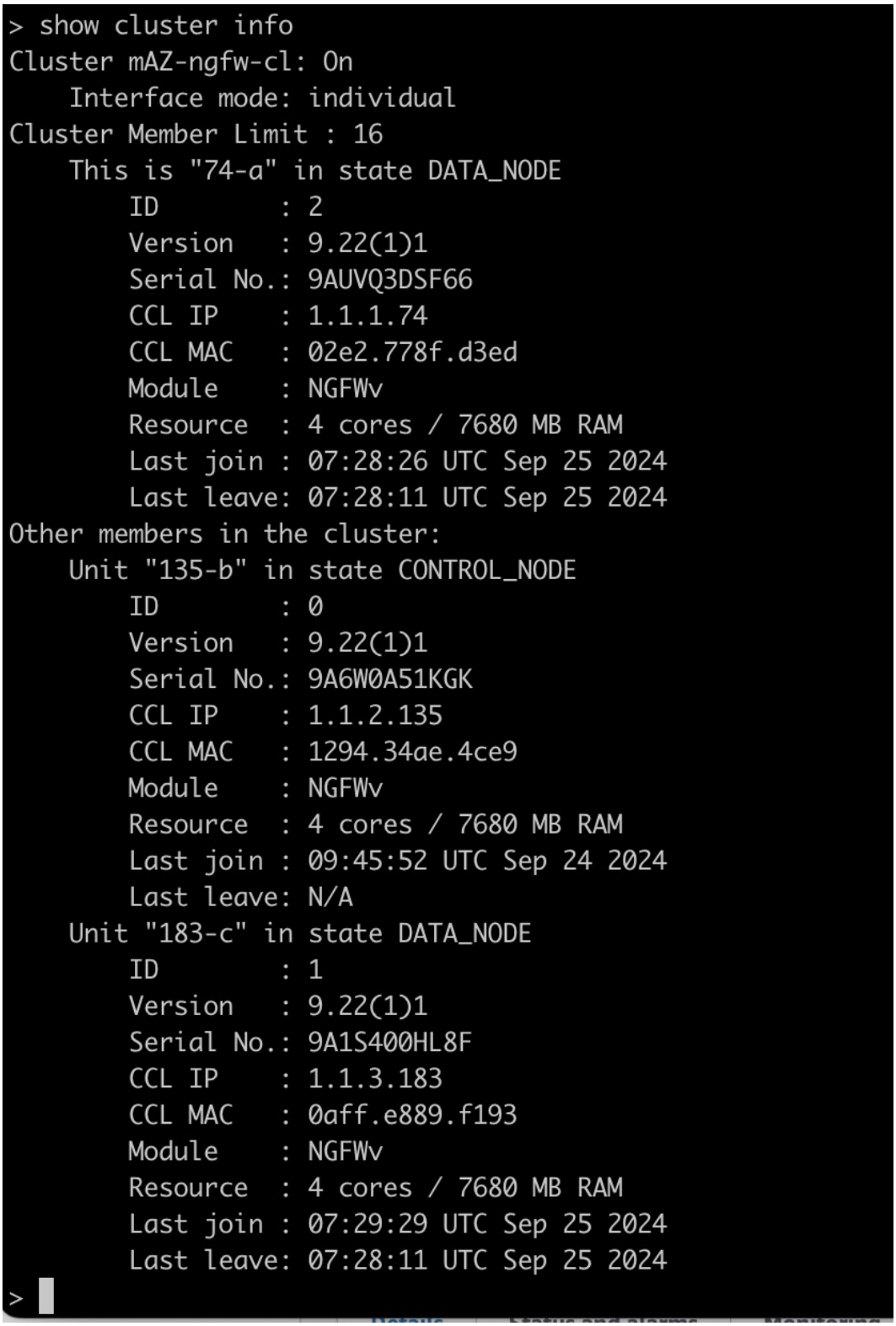


图 *6: show cluster info*



管理中心双臂部署的 NAT 配置

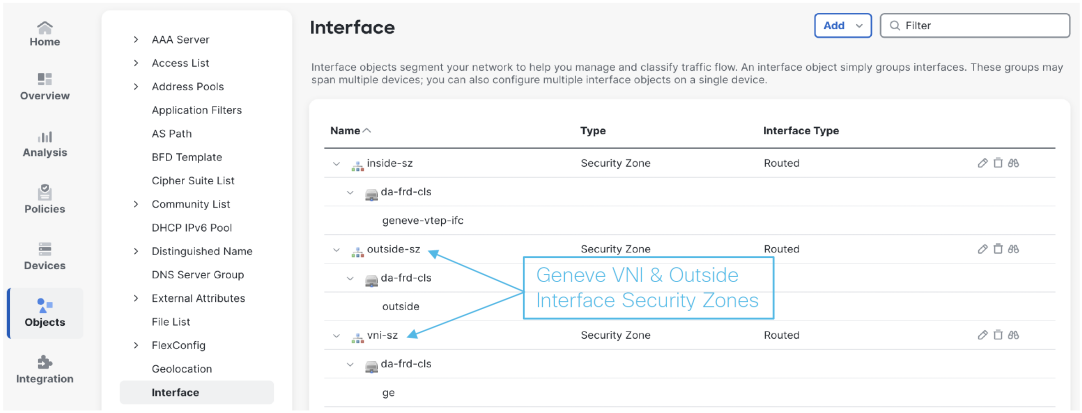
过程

步骤 1 创建安全区域。

安全区域允许您将访问控制、NAT 和检查策略统一应用于一组接口，而无需单独配置它们。

在管理中心中，导航至“对象 > 接口 > 添加 > 安全区域”。

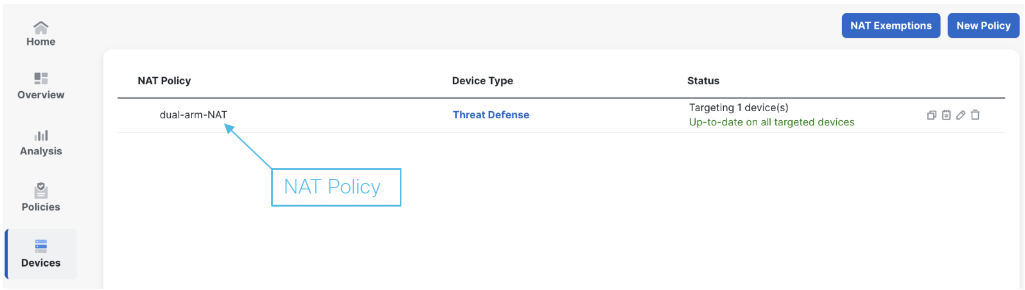
- **内部安全区域** → 用于内部或入口接口（来自应用程序的流量）。
- **VNI 安全区域** → 用于 Geneve VNI 隧道接口（来自 GWLB 的流量）。
- **外部安全区域** → 用于通向互联网网关的出口接口。



步骤 2 配置 NAT 政策。

NAT 政策（双臂 NAT）定义了源和目标地址转换规则，这些规则需要将流量从内部接口（经防火墙检查后）直接转发到外部接口以访问互联网，在出口时绕过 GWLB。

导航至“设备 > NAT > 新建政策”。

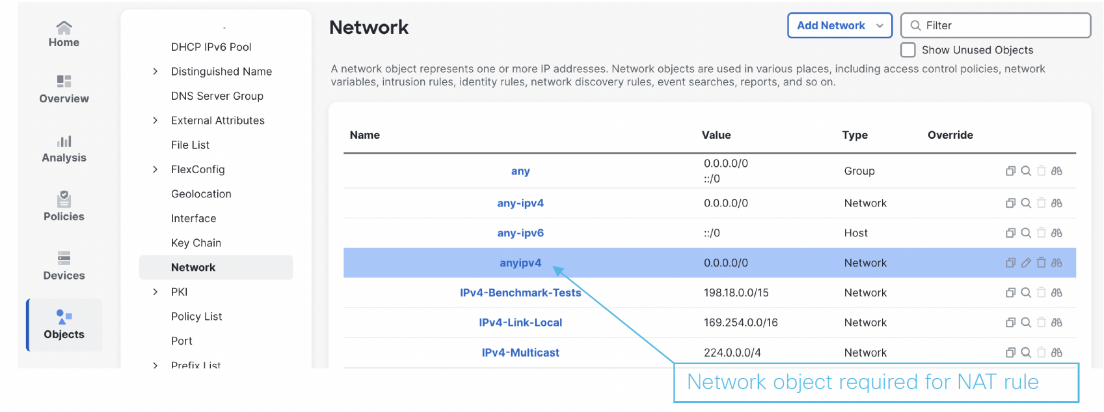


步骤 3 为您的源网络创建一个网络对象。

网络对象代表一个或多个 IP 地址或范围。这些对象用于 NAT 规则、访问控制政策和网络发现规则等多个地方。

导航至“对象 > 网络 > 添加网络”。

- **名称**：赋予网络对象的逻辑名称。
- **值**：实际的 IP 地址范围或 CIDR 格式的网段（例如，`0.0.0.0/0` 代表所有 IPv4 地址）。
- **类型**：指定对象是组、网络还是主机。

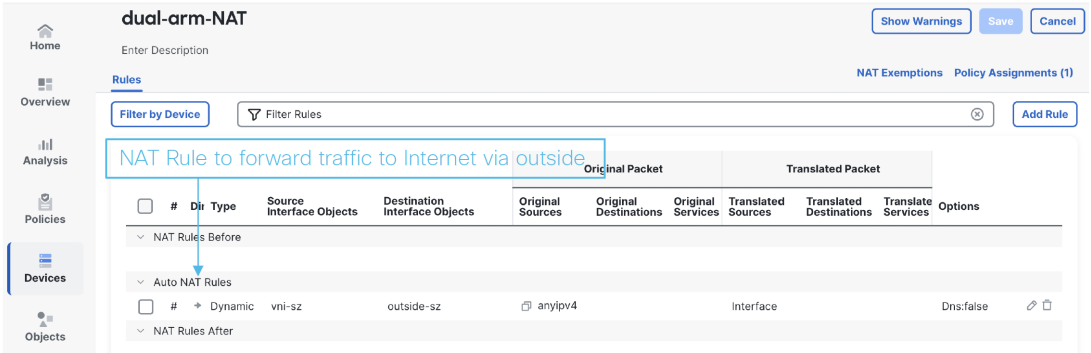


步骤 4 添加 NAT 规则

NAT 策略是为双臂部署配置的，以将流量通过外部接口转发到互联网。

导航至“设备 → NAT → 双臂 NAT → 添加规则”

完成配置后，按照“部署 > 选择集群组 > 全部部署”的路径将策略部署到集群组。

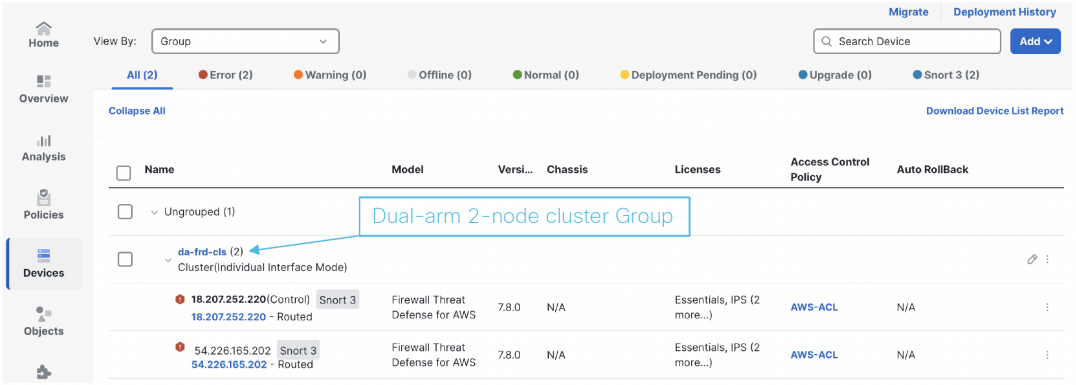


步骤 5 部署后检查

a) 验证双臂 2 节点集群组。

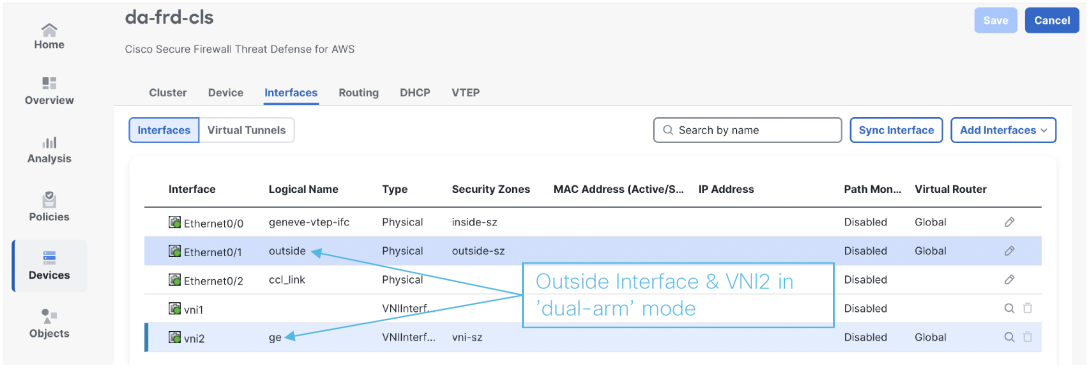
此步骤旨在验证集群是否包含在双臂模式下运行的两个 Threat Defense Virtual 实例,其中每个实例至少使用两个专用网络接口来处理单独的流量路径。

导航到“设备 → 设备管理”，然后验证集群组。



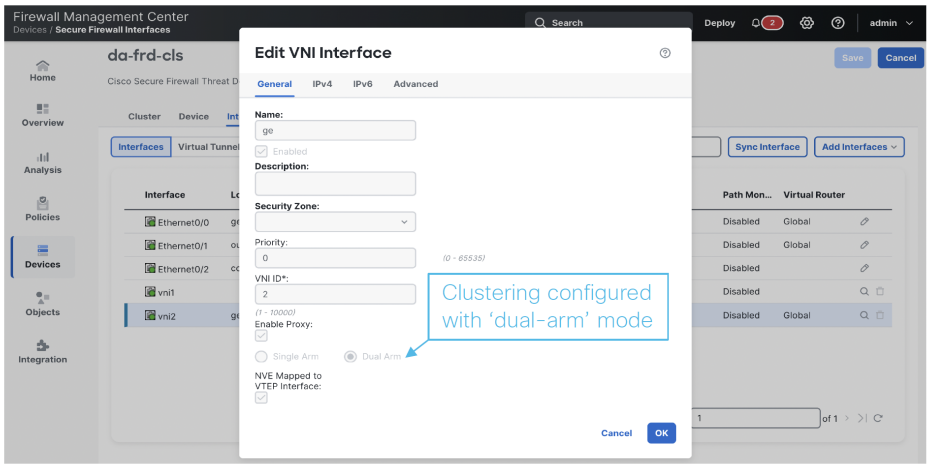
b) 验证 Cisco Secure Firewall Threat Defense Virtual 集群的接口和配置。

导航到“设备 > 设备管理 > 集群组 > 接口”，然后验证双臂部署所用的接口。



c) 确认双臂配置。

导航到“设备 > 设备管理 > 集群组 > 接口 > vni2”。点击“编辑 VNI 接口”以验证双臂配置。

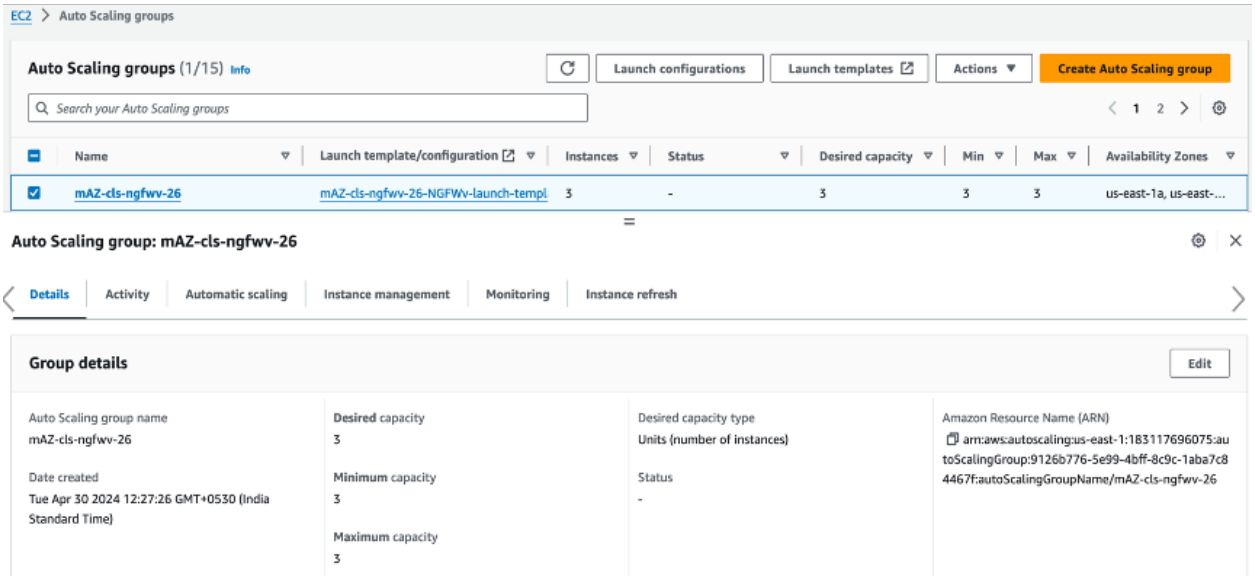


自动扩展参数配置

部署完成后，必须指定 Firewall Threat Defense Virtual Autoscale 组的**最小 (Minimum)**、**最大 (Maximum)** 和**期望 (Desired)** 容量。您必须验证自动扩展功能。

过程

步骤 1 在 AWS 控制台中，依次选择 **服务 (Services)** > **EC2** > **自动扩展组 (Auto Scaling groups)** > **已创建 ClusterAutoscale 组 (Created ClusterAutoscale group)**。



步骤 2 选中自动扩展组复选框。

步骤 3 点击**操作 (Actions)** 以编辑自动扩展组容量。

步骤 4 配置**所需容量 (Desired capacity)**，然后设置**扩展限制 (Scaling limits)** 容量。

步骤 5 在 AWS Cloudwatch 警报中检查 CPU 和内存指标数据是否可用，缩放是否按预期进行。

通过更新堆叠在 Firewall Threat Defense Virtual 集群中配置所需的 IMDSv2 模式

您可以为 AWS 上已部署的 Firewall Threat Defense Virtual 个自动扩展组实例配置 IMDSv2 必需模式。

Before you begin

仅 Firewall Threat Defense Virtual 版本 7.6 及更高版本支持 IMDSv2 必需模式。在为部署配置 IMDSv2 模式之前，您必须确保现有实例版本与 IMDSv2 模式兼容（升级到版本 7.6）。

Procedure

步骤 1 在 AWS 控制台上，转到 **CloudFormation** ，然后点击 **堆栈**。

步骤 2 选择初始部署的集群实例的堆栈。

步骤 3 点击**更新**。

步骤 4 在 **更新堆栈** 页面上，点击 **替换现有模板**。

步骤 5 在 **指定模板** 部分下，点击 **上传模板文件**。

步骤 6 选择并上传支持 IMDSv2 的模板。

步骤 7 为模板中的输入参数提供值。

步骤 8 更新堆栈。

在 AWS 中手动部署集群

要手动部署集群，请准备 day 0 配置，部署每个节点，然后将控制节点添加到 防火墙管理中心。

注释 从版本 7.6.4-69 和 10.0.0 开始，对于内部集群配置，每个集群节点都需要一个唯一的 AWS 实例标记“cluster-node-id”，其值范围为 1 到 16。请确保在设备启动之前添加标签。

例如：键“cluster-node-id” -> 值“1”

此外，请确保将“在实例元数据中允许标记”设置为“已启用”。

创建 AWS 的 Day0 配置

您可以使用固定配置或自定义配置。我们建议使用固定配置。

使用 AWS 的固定配置创建 Day0 配置

固定配置将自动生成集群引导程序配置。

单个可用性区域 - 第 0 天配置与 AWS 的固定配置

```
{
    "AdminPassword": "password",
    "Hostname": "hostname",
    "FirewallMode": "Routed",
    "ManageLocally": "No",
    "Cluster": {
        "CclSubnetRange": "ip_address_start ip_address_end",
        "ClusterGroupName": "cluster_name",
        [For Gateway Load Balancer] "Geneve": "{Yes | No}",
        [For Gateway Load Balancer] "HealthProbePort": "port"
```

```
    }
}
```

例如：

```
{
 "AdminPassword": "Sup3rnatural",
 "Hostname": "ciscoftdv",
 "FirewallMode": "Routed",
 "ManageLocally": "No",
 "Cluster": {
              "CclSubnetRange": "10.5.90.4 10.5.90.30",
  "ClusterGroupName": "ftdv-cluster",
  "Geneve": "Yes",
  "HealthProbePort": "7777"
 }
}
```

多个可用性区域 - 第 0 天配置与 AWS 的固定配置

```
{
    "AdminPassword": "password",
    "Hostname": "hostname",
    "FirewallMode": "Routed",
    "ManageLocally": "No",
    "Cluster": {
    "CclSubnetRange":[
    "ip_address_start_AZ1 ip_address_end_AZ1",
    "ip_address_start_AZ2 ip_address_end_AZ2",
    "ip_address_start_AZ3 ip_address_end_AZ3"
     ],
   "ClusterGroupName": "cluster_name",
        [For Gateway Load Balancer] "Geneve": "{Yes | No}",
        [For Gateway Load Balancer] "HealthProbePort": "port"
    }
}
```

例如：两个可用性区域

```
{
 "AdminPassword": "Sup4rnatural",
 "Hostname": "ftdvcluster",
 "FirewallMode": "Routed",
 "ManageLocally": "No",
 "Cluster": {
        "CclSubnetRange": [
            "10.5.90.4  10.5.90.30",
            "10.5.91.4  10.5.91.30"
        ],
  "ClusterGroupName": "ftdv-cluster",
  "Geneve": "Yes",
  "HealthProbePort": "8080"
 }
}
```

例如：三个可用性区域

```
{
 "AdminPassword": "Sup4rnatural",
 "Hostname": "ftdvcluster",
```

```
 "FirewallMode": "Routed",
 "ManageLocally": "No",
 "Cluster": {
        "CclSubnetRange": [
            "10.5.90.4  10.5.90.30",
            "10.5.91.4  10.5.91.30",
            "10.5.92.4  10.5.92.30"
        ],
  "ClusterGroupName": "ftdv-cluster",
  "Geneve": "Yes",
  "HealthProbePort": "8080"
 }
}
```

双臂部署的单个或多个可用性区域 Day0 配置

```
{
    "AdminPassword": "password",
    "Hostname": "hostname",
    "FirewallMode": "Routed",
    "ManageLocally": "No",
    "Diagnostic": "OFF",
    "Cluster": {
    "CclSubnetRange":[
    "ip_address_start_AZ1 ip_address_end_AZ1",
    "ip_address_start_AZ2 ip_address_end_AZ2",
    "ip_address_start_AZ3 ip_address_end_AZ3"
     ],
    "ProxyType": "dual-arm"
    "DualArmAppCidrList":[
    "CIDR_BLOCK_1",
    "CIDR_BLOCK_2",
    "CIDR_BLOCK_3"
     ],
   "ClusterGroupName": "cluster_name",
        [For Gateway Load Balancer] "Geneve": "{Yes | No}",
        [For Gateway Load Balancer] "HealthProbePort": "port"
    }
}
```

例如：

```
{
"AdminPassword": "FtDv_ClU3TeR44",
"Hostname": "ftdvcluster",
"FirewallMode": "routed",
"ManageLocally": "No",
"Diagnostic": "OFF",
"Cluster": {
"CclSubnetRange": [
"10.5.90.4 10.5.90.30",
"10.5.91.4 10.5.91.30",
"10.5.92.4 10.5.92.30"
],
"ProxyType": "dual-arm",
"DualArmAppCidrList": [
"10.0.0.0/8",
"172.16.0.0/12",
"192.168.0.0/16"
],
"Geneve": "Yes",
"HealthProbePort": "8080",
"ClusterGroupName": "ftdv-cluster"
```

```
}
}
```

对于 **CclSubnetRange** 变量，请指定从 xxx4 开始的 IP 地址范围。确保您至少有 16 个可用于集群的 IP 地址。下面给出了开始 (*ip_address_start*) 和结束 (*ip_address_end*) IP 地址的一些示例。

表 *2:* 开始和结束 *IP* 地址示例

CIDR	起始 IP 地址	结束 IP 地址
10.1.1.0/27	10.1.1.4	10.1.1.30
10.1.1.32/27	10.1.1.36	10.1.1.62
10.1.1.64/27	10.1.1.68	10.1.1.94
10.1.1.96/27	10.1.1.100	10.1.1.126
10.1.1.128/27	10.1.1.132	10.1.1.158
10.1.1.160/27	10.1.1.164	10.1.1.190
10.1.1.192/27	10.1.1.196	10.1.1.222
10.1.1.224/27	10.1.1.228	10.1.1.254

注释 所有集群基础设施子网都必须使用 /27 CIDR

部署集群节点

部署集群节点，以便它们形成集群。

过程

步骤 1 使用具有所需数量的接口的集群 Day 0 配置部署 Threat Defense Virtual 实例 - 如果使用网关负载均衡器 (GWLB)，则为四个接口；如果使用非本地负载均衡器，则为五个接口。在 **配置实例详细信息** > **高级详细信息** 部分中，粘贴您的 day0 配置。

注释
确保按以下顺序将接口连接到实例。

- AWS 网关负载均衡器 - 四个接口 - 管理、诊断、内部和集群控制链路。
- 非本地负载均衡器 - 五个接口 - 管理、诊断、内部、外部和集群控制链路。

有关在 AWS 上部署 Threat Defense Virtual 的更多信息，请参阅 在 AWS 上部署 Threat Defense Virtual。

步骤 2 重复步骤 1 以部署所需数量的其他节点。

步骤 3 使用 Threat Defense Virtual 控制台上的 **show cluster info** 命令验证是否所有节点都已成功加入集群。

注意
多可用区部署中的集群形成问题 (Threat Defense Virtual 7.6.2)：

在使用由管理中心 7.6.2.1 管理的 Threat Defense Virtual 7.6.2 的 AWS 多可用区部署中，一个已知问题可能会阻止成功形成集群。在这种情况下，无法配置第二个 VTEP，并且 VNI 配置可能缺失。

解决方法：

从管理中心取消注册现有集群，然后在所有集群节点上逐个运行以下 CLI 命令：

```
cluster reset-interface-mode
```

重新注册并重新配置集群。

此操作将解决 VNI 配置缺失的问题，并允许成功建立集群。

步骤 4 配置 AWS 网关负载均衡器。

a) 创建目标组和 GWLB。
b) 将目标组连接到 GWLB。

注释
确保将 GWLB 配置为使用正确的安全组、侦听程序配置和运行状况检查设置。

c) 使用 IP 地址向目标组注册数据接口（内部接口）。

有关详细信息，请参阅创建网关负载均衡器。

步骤 5 将控制节点添加到管理中心。请参阅将集群添加到管理中心（手动部署），第 100 页。

在 AWS 中使用 GWLB 配置 Cisco Secure Firewall Threat Defense Virtual 集群的目标故障转移

AWS 中的 Threat Defense Virtual 集群利用网关负载均衡器 (GWLB) 来均衡网络数据包并将其转发到指定的 Threat Defense Virtual 节点。GWLB 用于在目标节点发生故障切换或取消注册的情况下，继续向该节点发送网络数据包。

AWS 中的目标故障转移功能使 GWLB 能够在计划维护期间取消注册或目标节点发生故障的情况下将网络数据包重定向到正常运行的目标节点。它利用集群的状态故障切换。

在 AWS 中，您可以通过 AWS 弹性负载均衡 (ELB) API 或 AWS 控制台来配置目标故障转移。

注释 如果目标节点在 GWLB 使用某些协议（例如 SSH、SCP、CURL 等）路由流量时发生故障，则将流量重定向到正常目标可能会出现延迟。此延迟是由于流量的重新平衡和重新路由造成的。

在 AWS 中，您可以通过 AWS ELB API 或 AWS 控制台来配置目标故障转移。

- AWS API - 在 AWS 弹性负载均衡 (ELB) API - *modify-target-group-attributes* 中，您可以通过修改以下两个新参数来定义流量处理行为。
  - target_failover.on_unhealthy - 定义当目标变得运行不正常时 GWLB 如何处理网络流量。
  - target_failover.on_deregistration - 定义当目标取消注册时 GWLB 如何处理网络流量。

  以下命令显示了定义这两个参数的 API 参数配置示例。

```
aws elbv2 modify-target-group-attributes \
--target-group-arn arn:aws:elasticloadbalancing:…/my-targets/73e2d6bc24d8a067 \
--attributes \
Key=target_failover.on_unhealthy, Value=rebalance[no_rebalance] \
Key=target_failover.on_deregistration, Value=rebalance[no_rebalance]
```

  有关详细信息，请参阅 AWS 文档中的 TargetGroupAttribute。

- AWS 控制台 – 在 EC2 控制台中，您可以通过配置以下选项来启用目标组页面上的目标故障转移选项。
  - 编辑目标组属性
  - 启用目标故障转移
  - 验证再平衡流量

  有关如何启用目标故障转移的详细信息，请参阅 在 AWS 中启用 Cisco Secure Firewall Threat Defense Virtual 集群的目标故障转移，第 36 页。

在 AWS 中启用 Cisco Secure Firewall Threat Defense Virtual 集群的目标故障转移

Firewall Threat Defense Virtual 的数据接口已注册到 AWS 中的 GWLB 目标组。在 Firewall Threat Defense Virtual 集群中，每个实例都与一个目标组关联。GWLB 进行负载平衡，并将流量发送到该运行状况正常的实例，而该实例已被识别或注册为目标组中目标节点。

开始之前

您必须已通过手动方法或使用 CloudFormation 模板在 AWS 中部署集群。

如果您使用 CloudFormation 模板部署集群，您还可以通过分配集群部署文件 `deploy_ftdv_clustering.yaml` 的 **GWLB 配置**部分下提供的 **rebalance** 属性来启用 **Target Failover** 参数。在模板中，默认情况下，此参数的值设置为 **rebalance**。但在 AWS 控制台上，此参数的默认值设置为 **no_rebalance**。

其中，

- **no_rebalance** - GWLB 继续将网络流量发送到发生故障或已取消注册的目标。
- **rebalance** - 当现有目标发生故障或取消注册时，GWLB 将网络流量发送到另一个正常运行的目标。

有关在 AWS 中部署堆栈的信息，请参阅：

- 在 AWS 中手动部署集群
- 使用 CloudFormation 模板在 AWS 中部署堆栈

过程

步骤 1 在 AWS 控制台上，转到 **服务 > EC2**

步骤 2 点击**目标组 (Target Groups)** 以查看目标组页面。

步骤 3 选择向其注册 Firewall Threat Defense Virtual 数据接口 IP 的目标组。系统将显示目标组详细信息页面，您可以在其中启用目标故障转移属性。

步骤 4 转到**属性 (Attributes)** 菜单。

步骤 5 点击**编辑 (Edit)** 以编辑属性。

步骤 6 将 **重新平衡流量** 滑块按钮切换到右侧，以便启用目标故障转移，从而将 GWLB 配置为在发生故障转移或取消注册时重新平衡现有网络数据包，并将其转发到正常运行的目标节点。

在 Azure 中部署集群

您可以将集群与 Azure 网关负载均衡器 (GWLB) 或非本地负载均衡器配合使用。要在 Azure 中部署集群， 可使用 Azure 资源管理器 (ARM) 模板来部署虚拟机规模集。

基于 GWLB 的集群部署的拓扑示例

图 *7: GWLB* 的入站流量使用案例和拓扑

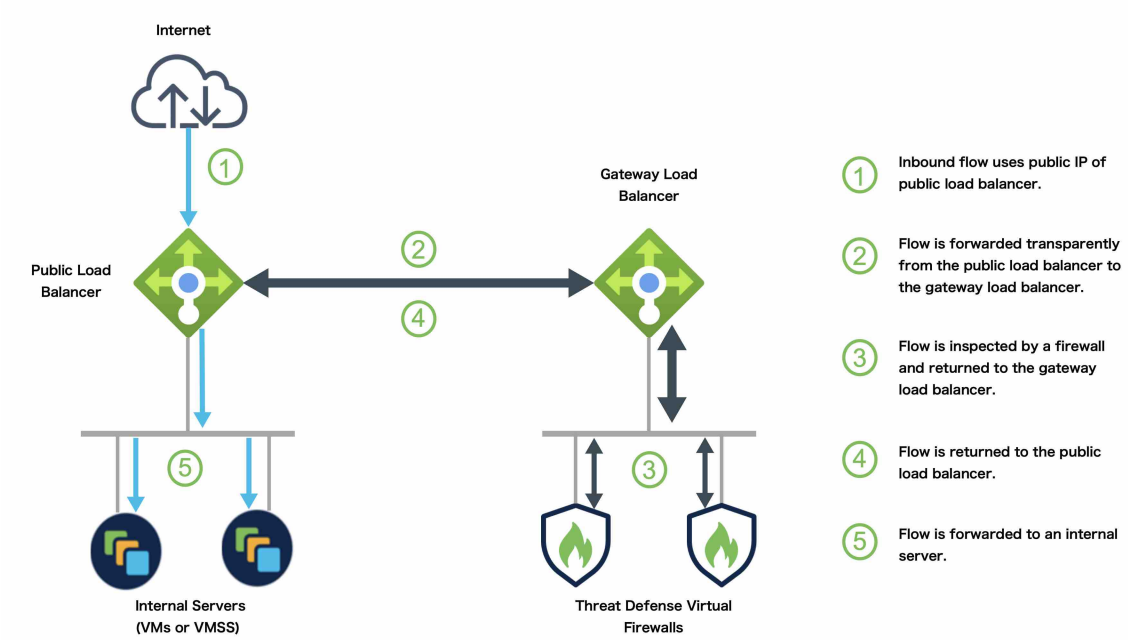
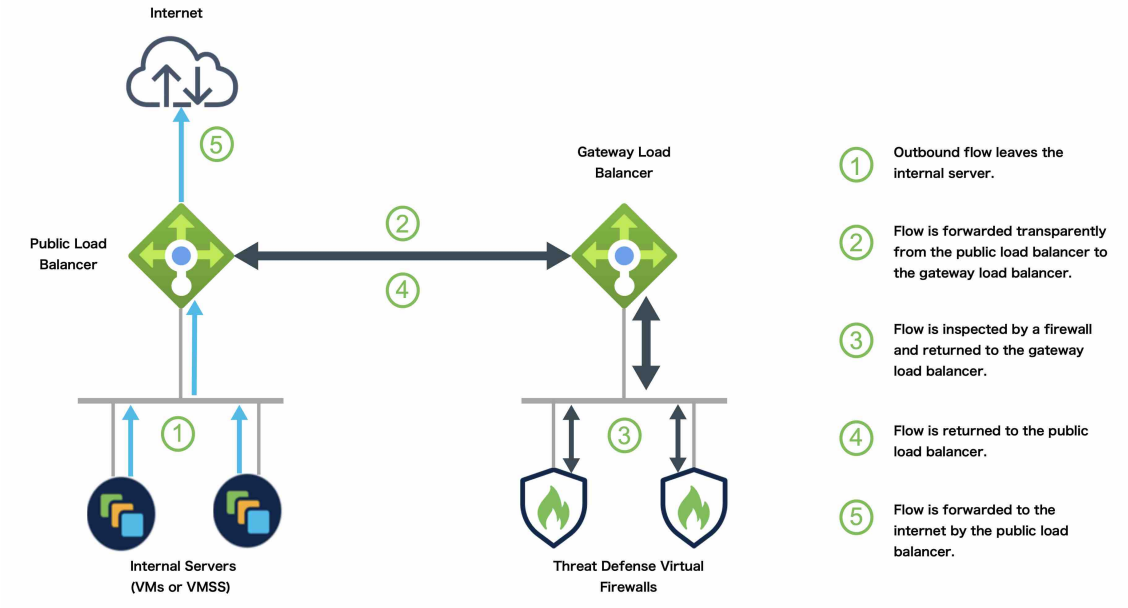


图 *8: GWLB* 的出站流量使用案例和拓扑

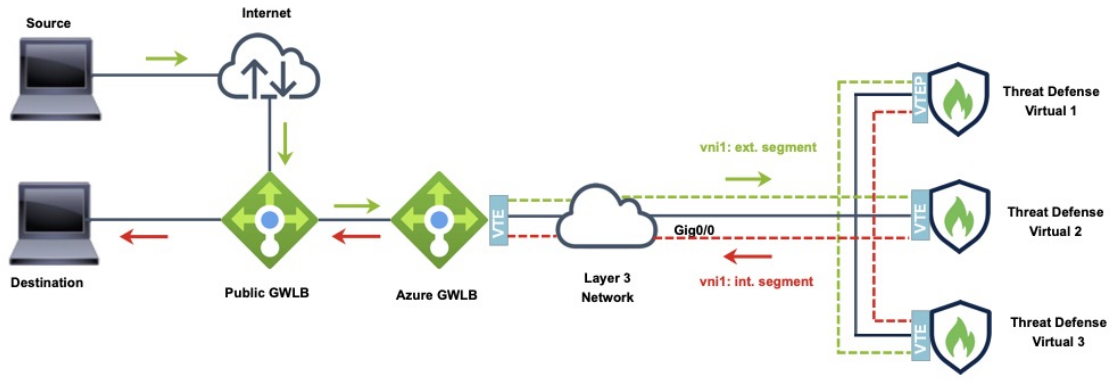


Azure 网关负载均衡器和配对代理

在 Azure 服务链中，Threat Defense Virtual 充当可以拦截互联网和客户服务之间的数据包的透明网关。Threat Defense Virtual 通过利用成对代理中的 VXLAN 网段在单个 NIC 上定义外部接口和内部接口。

下图显示了从外部 VXLAN 网段上的公共网关负载均衡器转发到 Azure 门户负载均衡器的流量。网关负载均衡器会在多个 Threat Defense Virtual 流量之间进行均衡，这些流量在丢弃流量或将其发送回在内部 VXLAN 部分的网关负载均衡器之前对其进行检查。然后，Azure 网关负载均衡器会将流量发送回公共网关负载均衡器和目的地。

图 *9: Azure* 网关负载均衡器和配对代理

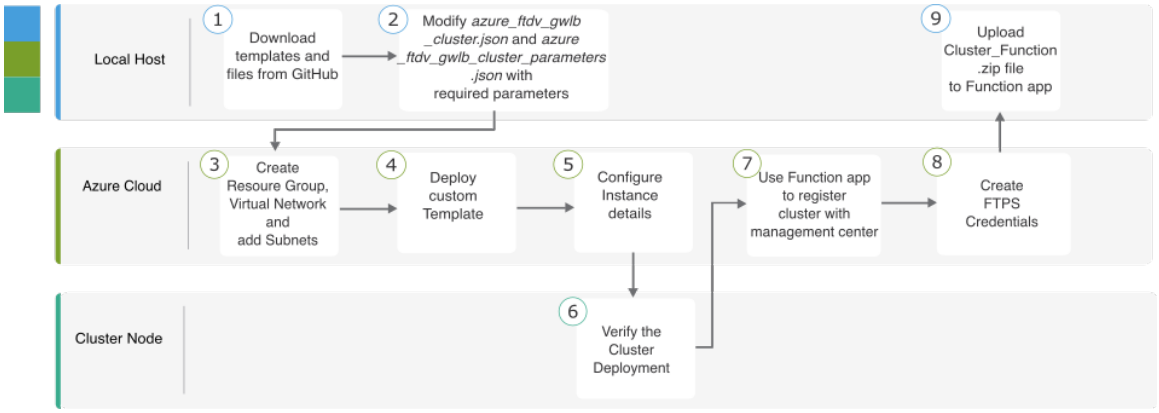


Traffic flow between GWLBe to GWLB (Geneve Single-Arm Proxy) in Azure

使用 GWLB 在 Azure 中部署 Threat Defense Virtual 集群的端到端流程

基于模板的部署

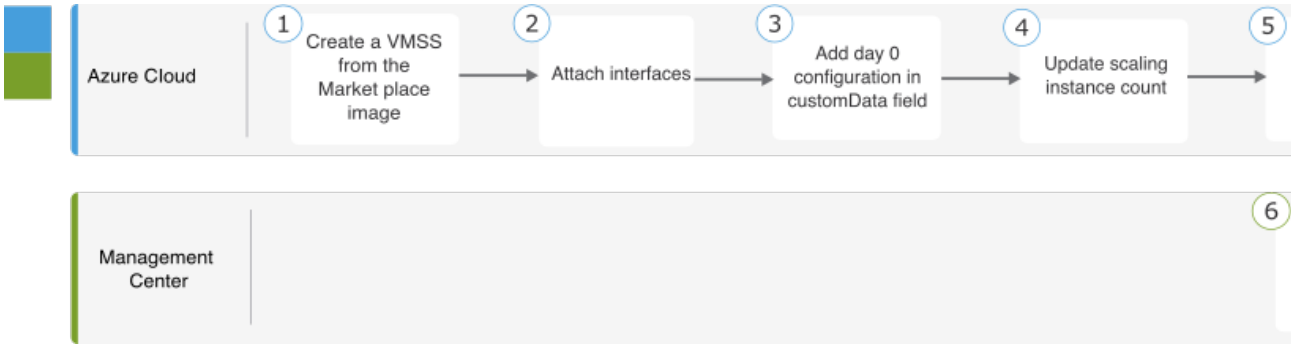
以下流程图说明使用 GWLB 在 Azure 中基于模板部署 Threat Defense Virtual 集群的工作流程。



	工作空间	步骤
1	本地主机	从 GitHub 下载模板和文件。
2	本地主机	使用所需的参数来修改 *azure_ftdv_gwlb_cluster.json* 和 *azure_ftdv_gwlb_cluster_parameters.json*。
3	Azure Cloud	创建资源组、虚拟网络和子网。
4	Azure Cloud	部署自定义模板。
5	Azure Cloud	配置实例详细信息。
6	集群节点	验证集群部署。
7	Azure Cloud	使用函数应用向管理中心注册集群。
8	Azure Cloud	创建 FTPS 凭证。
9	本地主机	将 *Cluster_Function.zip* 文件上传到 Function 应用。

手动部署

以下流程图说明了使用 GWLB 在 Azure 中手动部署 Threat Defense Virtual 集群的工作流程。



	工作空间	步骤
1	本地主机	从市场映像创建 VMSS。
2	本地主机	连接接口。
3	本地主机	在 customData 字段中添加 Day 0 配置。
4	本地主机	更新扩展实例计数。

	工作空间	步骤
5	本地主机	配置 GWLB。
6	管理中心	添加控制节点。

模板

以下提供的模板可在 GitHub 中获取。参数值是不言自明的，参数名称和值在模板中给出。

- azure_ftdv_gwlb_cluster_parameters.json - 用于为 Firewall Threat Defense Virtual 集群输入参数的模板
- azure_ftdv_gwlb_cluster.json - 用于部署 Firewall Threat Defense Virtual 集群的模板。

前提条件

- 要允许集群自动注册到管理中心，请在管理中心创建具有网络管理员和维护用户权限的用户。具有这些权限的用户可以使用 REST API。请参阅 Cisco Secure Firewall Management Center 管理指南。
- 在管理中心添加与您将在模板部署期间指定的策略名称匹配的访问策略。
- 确保 Management Center Virtual 已获得适当许可。
- 将集群添加到 Management Center Virtual 后，执行以下步骤：
  1. 使用管理中心中的运行状况检查端口号配置平台设置。有关配置此功能的详细信息，请参阅平台设置。
  2. 为数据流量创建静态路由。有关创建静态路由的详细信息，请参阅 添加静态路由。

     静态路由配置示例：

```
Network: any-ipv4
Interface: vxlan_tunnel
Leaked from Virtual Router: Global
Gateway: vxlan_tunnel_gw
Tunneled: false
Metric: 2
```

注释 *vxlan_tunnel_gw* 是数据子网的网关 IP 地址。

使用 GWLB 在 Azure 中部署 Threat Defense Virtual 集群的端到端流程

使用自定义的 Azure 资源管理器 (ARM) 模板为 Azure GWLB 部署虚拟机规模集。请注意，以下步骤中提到的模板可从 GitHub 上获取。

过程

步骤 1 准备模板。

a) 将 github 存储库克隆到本地文件夹。请参阅https://github.com/CiscoDevNet/cisco-ftdv/tree/master/cluster/azure。

b) 使用所需的参数来修改 azure_ftdv_gwlb_cluster.json 和 azure_ftdv_gwlb_cluster_parameters.json 。

步骤 2 登录到 Azure 门户：https://portal.azure.com。

步骤 3 创建一个资源组。

a) 在**基本 (Basics)** 选项卡中，从下拉列表中选择**订用 (Subscription)** 和**资源组 (Resource Group)**。

b) 选择所需的**区域 (Region)**。

步骤 4 创建一个包含三个子网的虚拟网络：管理子网、数据子网和集群控制链路 (CCL) 子网。

a) 创建虚拟网络。

1. 在**基本 (Basics)** 选项卡中，从下拉列表中选择**订用 (Subscription)** 和**资源组 (Resource Group)**。
2. 选择所需的**区域 (Region)**。点击 **下一个：IP 地址**。

在 **IP 地址** 选项卡中，点击 **添加子网** ，然后添加以下子网 - 管理、数据和集群控制链路。

b) 添加子网。

步骤 5 部署自定义模板。

a) 点击 **创建** > **模板部署**（**使用自定义模板部署**）。

b) 点击 **在编辑器中生成自己的模板**。

c) 点击 **加载文件**，然后上传 **azure_ftdv_gwlb_cluster.json**。

d) 点击**保存**。

步骤 6 配置实例详细信息。

a) 输入所需的值，然后点击**查看 + 创建 (Review + create)**。

b) 在验证通过后，点击**创建 (Create)**。

步骤 7 在实例开始运行后，通过登录到任何一个节点并输入 **show cluster info** 命令来验证集群部署。

图 *10: show cluster info*

```
> show cluster info
Cluster gwlb-cluster-template-with-AN: On
    Interface mode: individual
Cluster Member Limit : 16
    This is "12" in state CONTROL_NODE
        ID        : 0
        Version   : 99.19(1)180
        Serial No.: 9AKGFV8VH4G
        CCL IP    : 10.1.1.12
        CCL MAC   : 000d.3a55.5470
        Module    : NGFWv
        Resource  : 8 cores / 28160 MB RAM
        Last join : 11:13:24 UTC Sep 5 2022
        Last leave: N/A
```

步骤 8 在 Azure 门户中，点击函数应用以将集群注册到 防火墙管理中心。

注释
如果您不想使用函数应用，也可以使用 **添加** > **设备**（而不是**添加** > **集群**）直接将控制节点注册到 防火墙管理中心 。其余集群节点将自动注册。

步骤 9 通过点击 **部署中心** > **FTPS 凭证** > **用户范围** > **配置用户名和密码** 来创建 FTPS 凭证，然后点击 **保存**。

步骤 10 通过在本地终端中执行以下 **curl** 命令，将 Cluster_Function.zip 文件上传到 Function 应用。

curl -X POST -u *username* **--data-binary @"Cluster_Function.zip" https://** *Function_App_Name***.scm.azurewebsites.net/api/zipdeploy**

注释
curl 命令可能需要几分钟（约 2 到 3 分钟）才能完成命令执行。

函数将被上传到函数应用。功能将启动，而您可以在存储帐户的出站队列中看到日志。系统将向管理中心发起设备注册。

图 *11:* 功能

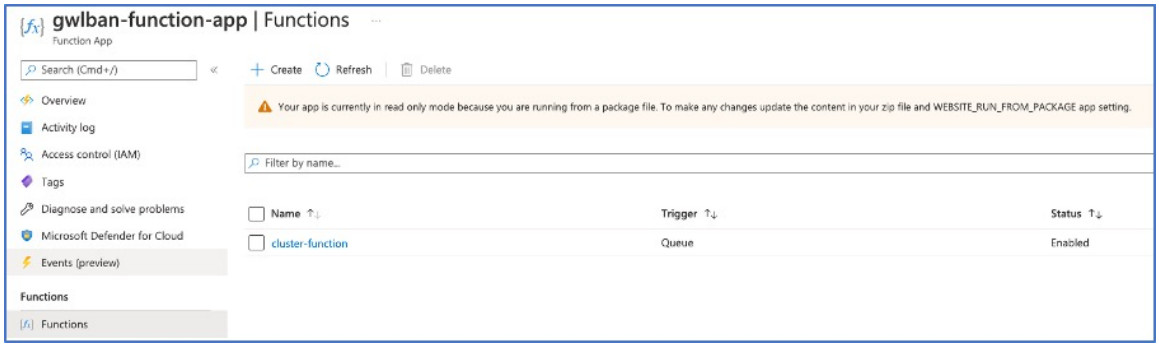


图 *12:* 队列

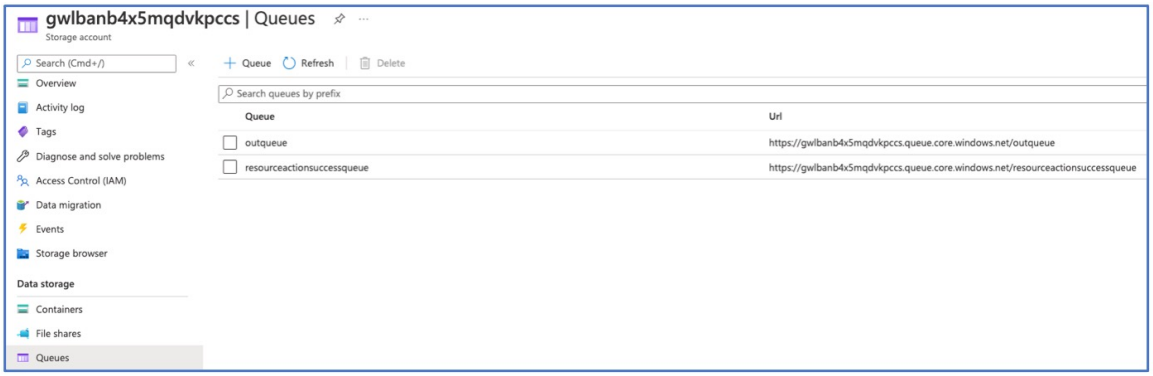
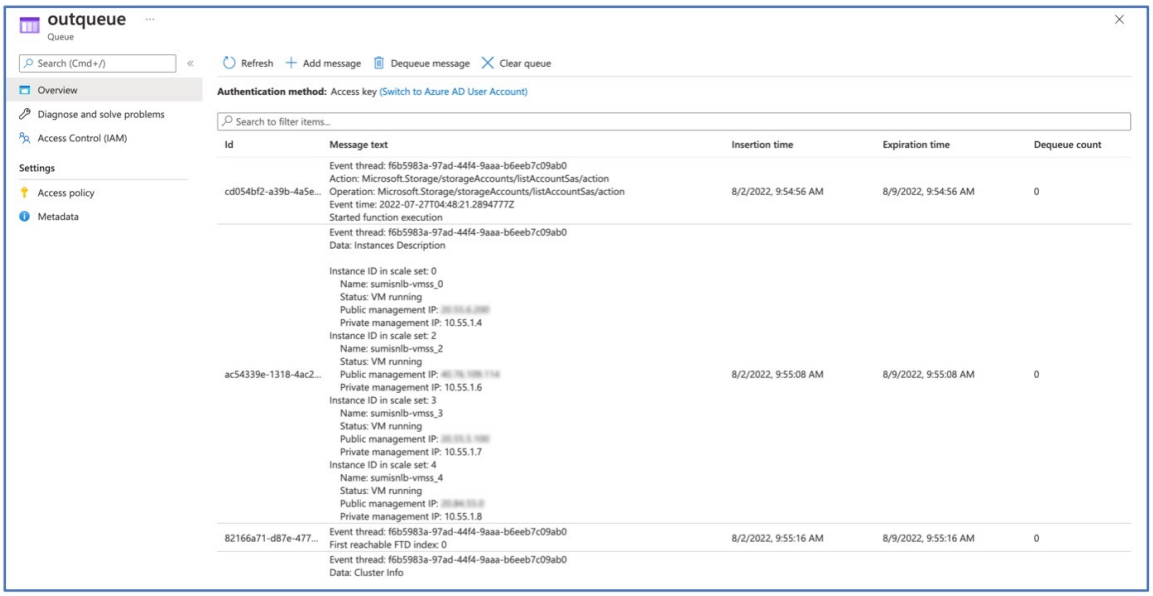
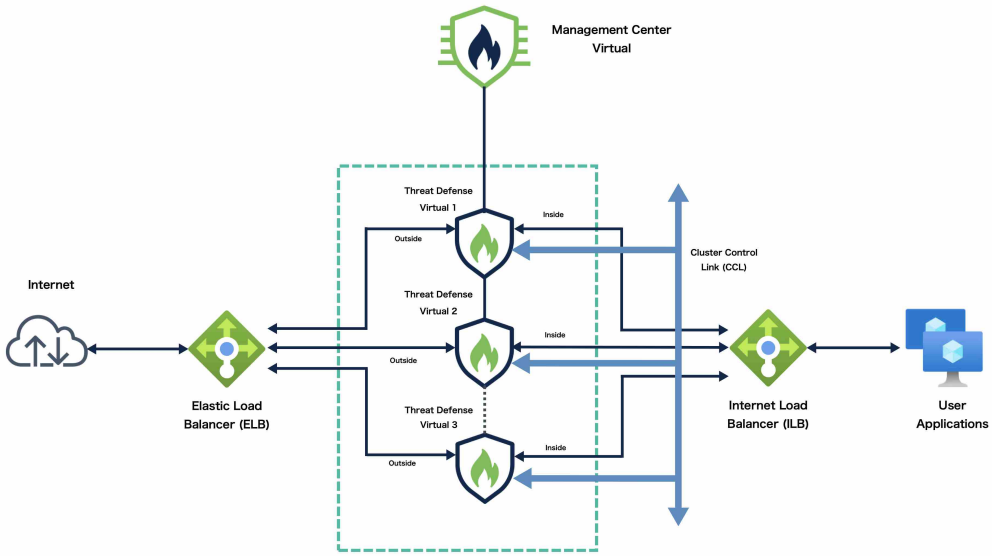


图 *13:* 出站队列



基于 NLB 的集群部署拓扑示例



此拓扑描述入站和出站流量。Threat Defense Virtual 集群夹在内部和外部负载均衡器之间。Management Center Virtual 实例用于管理集群。

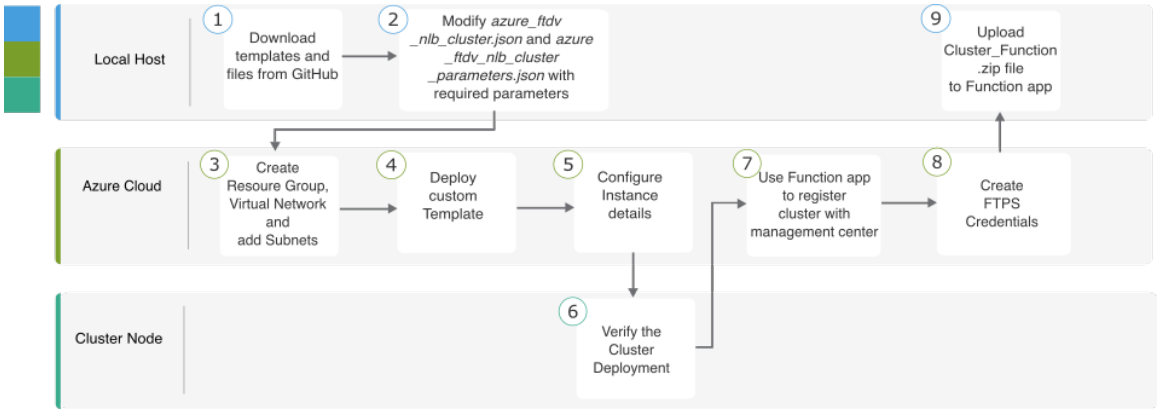
来自互联网的入站流量会进入外部负载均衡器，然后该负载均衡器会将流量传输到 Threat Defense Virtual 集群。集群中的 Threat Defense Virtual 实例检测到流量后，会将其转发到应用虚拟机。

来自应用虚拟机的出站流量将传输到内部负载均衡器。然后，流量会被转发到 Threat Defense Virtual 集群，然后再发送到互联网。

使用 NLB 在 Azure 中部署 Threat Defense Virtual 集群的端到端流程

基于模板的部署

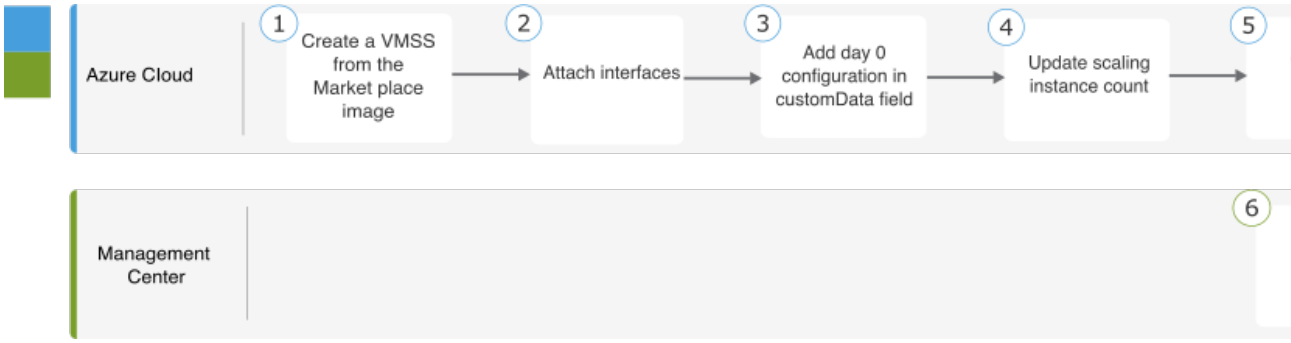
以下流程图说明了使用 NLB 在 Azure 中部署基于模板的 Threat Defense Virtual 集群的工作流程。



	工作空间	步骤
1	本地主机	从 GitHub 下载模板和文件。
2	本地主机	使用所需的参数来修改 *azure_ftdv_nlb_cluster.json* 和 *azure_ftdv_nlb_cluster_parameters.json* 。
3	Azure Cloud	创建资源组、虚拟网络和子网。
4	Azure Cloud	部署自定义模板。
5	Azure Cloud	配置实例详细信息。
6	集群节点	验证集群部署。
7	Azure Cloud	使用函数应用向管理中心注册集群。
8	Azure Cloud	创建 FTPS 凭证。
9	本地主机	将 *Cluster_Function.zip* 文件上传到 Function 应用。

手动部署

以下流程图说明了使用 NLB 在 Azure 中手动部署 Threat Defense Virtual 集群的工作流程。



	工作空间	步骤
1	本地主机	从市场映像创建 VMSS。
2	本地主机	连接接口。
3	本地主机	在 customData 字段中添加 Day 0 配置。
4	本地主机	更新扩展实例计数。

	工作空间	步骤
5	本地主机	配置 NLB。
6	管理中心	添加控制节点。

模板

以下提供的模板可在 GitHub 中获取。参数值是不言自明的，参数名称和值在模板中给出。

- azure_ftdv_nlb_cluster_parameters.json - 用于为具有 GWLB 的 Firewall Threat Defense Virtual 集群输入参数的模板
- azure_ftdv_nlb_cluster.json - 使用 GWLB 部署 Firewall Threat Defense Virtual 集群的模板。

前提条件

- 要允许集群自动注册到管理中心，请在管理中心创建具有网络管理员和维护用户权限的用户。具有这些权限的用户可以使用 REST API。请参阅 Cisco Secure Firewall Management Center 管理指南。
- 在管理中心添加与您将在模板部署期间指定的策略名称匹配的访问策略。
- 确保 Management Center Virtual 已获得适当许可。
- 将集群添加到 Management Center Virtual 后：
  1. 使用管理中心中的运行状况检查端口号配置平台设置。有关配置此功能的详细信息，请参阅平台设置。
  2. 为来自外部和内部接口的流量创建静态路由。有关创建静态路由的详细信息，请参阅 添加静态路由。

     外部接口的静态路由配置示例：

```
Network: any-ipv4
Interface: outside
Leaked from Virtual Router: Global
Gateway: ftdv-cluster-outside
Tunneled: false
Metric: 10
```

注释 *ftdv-cluster-outside* 是外部子网的网关 IP 地址。

     内部接口的静态路由配置示例：

```
Network: any-ipv4
Interface: inside
```

```
Leaked from Virtual Router: Global
Gateway: ftdv-cluster-inside-gw
Tunneled: false
Metric: 11
```

注释 *ftdv-cluster-inside-gw*是内部子网的网关 IP 地址。

3. 为数据流量配置 NAT 规则。有关配置 NAT 规则的详细信息，请参阅 网络地址转换。

使用 Azure 资源管理器模板通过 NLB 在 Azure 上部署集群

使用自定义的 Azure 资源管理器 (ARM) 模板为 Azure NLB 部署集群。请注意，以下步骤中提到的模板可从 GitHub 上获取。

过程

步骤 1 准备模板。

a) 将 github 存储库克隆到本地文件夹。请参阅https://github.com/CiscoDevNet/cisco-ftdv/tree/master/cluster/azure。

b) 使用所需的参数来修改 azure_ftdv_nlb_cluster.json 和 azure_ftdv_nlb_cluster_parameters.json。

步骤 2 登录到 Azure 门户：https://portal.azure.com。

步骤 3 创建一个资源组。

a) 在**基本 (Basics)** 选项卡中，从下拉列表中选择**订用 (Subscription)** 和**资源组 (Resource Group)**。

b) 选择所需的**区域 (Region)**。

步骤 4 创建具有四个子网的虚拟网络：管理、诊断、内部、外部和集群控制链路。

a) 创建虚拟网络。

1. 在**基本 (Basics)** 选项卡中，从下拉列表中选择**订用 (Subscription)** 和**资源组 (Resource Group)**。
2. b) 选择所需的 **区域**。点击 **下一个：IP 地址**。

b) 添加子网。

在 **IP 地址** 选项卡中，点击 **添加子网** 并添加以下子网 - 管理、诊断、内部、外部和集群控制链路。

步骤 5 部署自定义模板。

a) 点击 **创建** > **模板部署**（**使用自定义模板部署**）。

b) 点击 **在编辑器中生成自己的模板**。

c) 点击 **加载文件**，然后上传 **azure_ftdv_nlb_cluster.json**。

d) 点击**保存**。

步骤 6 配置实例详细信息。

a) 输入所需的值，然后点击**查看 + 创建 (Review + create)**。

注释
对于集群控制链路的起始地址和结束地址，仅指定所需数量的地址（最多 16 个）。较大的范围可能会影响性能。

b) 在验证通过后，点击**创建 (Create)**。

步骤 7 在实例开始运行后，通过登录到任何一个节点并使用 **show cluster info** 命令来验证集群部署。

图 *14: show cluster info*

```
> show cluster info
Cluster gwlb-cluster-template-with-AN: On
    Interface mode: individual
Cluster Member Limit : 16
    This is "12" in state CONTROL_NODE
        ID        : 0
        Version   : 99.19(1)180
        Serial No.: 9AKGFV8VH4G
        CCL IP    : 10.1.1.12
        CCL MAC   : 000d.3a55.5470
        Module    : NGFWv
        Resource  : 8 cores / 28160 MB RAM
        Last join : 11:13:24 UTC Sep 5 2022
        Last leave: N/A
```

步骤 8 在 Azure 门户中，点击函数应用以将集群注册到 防火墙管理中心。

注释
如果您不想使用函数应用，也可以使用 **添加 > 设备** （而不是 **添加 > 集群**）直接将控制节点注册到管理中心。其余集群节点将自动注册。

步骤 9 通过点击 **部署中心 > FTPS 凭证 > 用户范围 > 配置用户名和密码** 来创建 FTPS 凭证，然后点击 **保存**。

步骤 10 通过在本地终端中执行以下 **curl** 命令，将 Cluster_Function.zip 文件上传到 Function 应用。

curl -X POST -u *username* **--data-binary @"Cluster_Function.zip" https://** *Function_App_Name***.scm.azurewebsites.net/api/zipdeploy**

注释
curl 命令可能需要几分钟（约 2 到 3 分钟）才能完成命令执行。

函数将被上传到函数应用。功能将启动，而您可以在存储帐户的出站队列中看到日志。系统将向管理中心发起设备注册。

在 Azure 中手动部署集群

要手动部署集群，请准备 day0 配置，部署每个节点，然后将控制节点添加到 防火墙管理中心。

创建 Azure 的 Day0 配置

您可以使用固定配置或自定义配置。

使用 Azure 的固定配置创建 Day0 配置

固定配置将自动生成集群引导程序配置。

```
"Cluster": {
"CclSubnetRange": "ip_address_start ip_address_end",
"ClusterGroupName": "cluster_name",
"HealthProbePort": "port_number",
"GatewayLoadBalancerIP": "ip_address",
"EncapsulationType": "vxlan",
"InternalPort": "internal_port_number",
"ExternalPort": "external_port_number",
"InternalSegId": "internal_segment_id",
"ExternalSegId": "external_segment_id"
}
```

示例

下面给出了第 0 天的配置示例。

```
"Cluster": {
"CclSubnetRange": "10.45.3.4 10.45.3.30",     //mandatory user input
"ClusterGroupName": "ngfwv-cluster",          //mandatory user input
"HealthProbePort": "7777",                    //mandatory user input
"GatewayLoadBalancerIP": "10.45.2.4",         //mandatory user input
"EncapsulationType": "vxlan",
"InternalPort": "2000",
"ExternalPort": "2001",
"InternalSegId": "800",
"ExternalSegId": "801"
}
```

注释 如果要复制并粘贴上面给出的配置，请确保从配置中删除 **//mandatory user input**

对于 Azure 运行状况检查设置，请务必指定您在此处设置的 **HealthProbePort**。

对于 **CclSubnetRange** 变量，请指定从 xxx4 开始的 IP 地址范围。确保您至少有 16 个可用于集群的 IP 地址。下面给出了开始和结束 IP 地址的一些示例。

注释 所有集群基础设施子网都必须使用 /27 CIDR

表 *3:* 开始和结束 *IP* 地址示例

CIDR	起始 IP 地址	结束 IP 地址
10.1.1.0/27	10.1.1.4	10.1.1.30
10.1.1.32/27	10.1.1.36	10.1.1.62

CIDR	起始 IP 地址	结束 IP 地址
10.1.1.64/27	10.1.1.68	10.1.1.94
10.1.1.96/27	10.1.1.100	10.1.1.126
10.1.1.128/27	10.1.1.132	10.1.1.158
10.1.1.160/27	10.1.1.164	10.1.1.190
10.1.1.192/27	10.1.1.196	10.1.1.222
10.1.1.224/27	10.1.1.228	10.1.1.254

使用 Azure 的自定义配置创建 Day0 配置

您可以使用命令来输入整个集群引导程序配置。

```
"Cluster": {
"CclSubnetRange": "ip_address_start ip_address_end",
"ClusterGroupName": "cluster_name",
"HealthProbePort": "port_number",
"GatewayLoadBalancerIP": "ip_address",
"EncapsulationType": "vxlan",
"InternalPort": "internal_port_number",
"ExternalPort": "external_port_number",
"InternalSegId": "internal_segment_id",
"ExternalSegId": "external_segment_id"
}
```

手动部署集群节点 - 基于 GWLB 的部署

部署集群节点，以便它们形成集群。

过程

步骤 1 登录到 Azure 门户：https://portal.azure.com

步骤 2 创建一个资源组。

1. 在**基本 (Basics)** 选项卡中，从下拉列表中选择**订用 (Subscription)** 和**资源组 (Resource Group)**。
2. 选择所需的**区域 (Region)**。

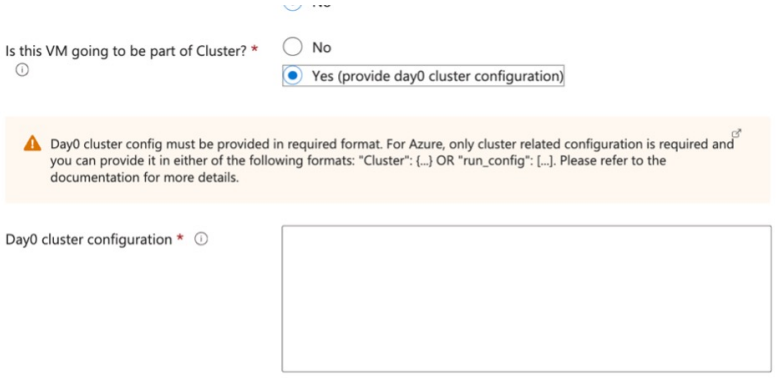
步骤 3 创建具有必要子网的虚拟网络：管理、数据和集群控制链路 (CCL)。

注释
根据需要使用最小子网配置 CCL。较宽的子网可能会影响性能。

请参阅有关创建虚拟网络和子网的 Azure 文档：https://learn.microsoft.com/en-us/azure/virtual-network/quickstart-create-virtual-network?tabs=portal

步骤 4 转到应用市场，搜索 **Cisco Secure Firewall Threat Defense Virtual - BYOL 和 PAYG**，然后点击**创建**。

步骤 5 填写必填详细信息，并为**此虚拟机是否将成为集群的一部分？**选择**是**。



将以下集群相关配置粘贴到文本框中。

```
"Cluster": {
"CclSubnetRange": "ip_address_start ip_address_end", //mandatory user input
"ClusterGroupName": "cluster_name", //mandatory user input
"HealthProbePort": "port_number", //mandatory user input
"GatewayLoadBalancerIP": "ip_address",  //mandatory user input
"EncapsulationType": "vxlan",
"InternalPort": "internal_port_number",
"ExternalPort": "external_port_number",
"InternalSegId": "internal_segment_id",
"ExternalSegId": "external_segment_id"
}
```

步骤 6 点击**下一步**，然后选择**虚拟网络和子网**。

步骤 7 点击**查看 + 创建**。等待 Threat Defense Virtual 部署完成。

步骤 8 连接到 Threat Defense Virtual 设备并使用 **show cluster info** 命令确认集群已成功建立。

```
> show cluster info
Cluster ngfwv-cluster: On
    Interface mode: individual
Cluster Member Limit : 16
    This is "4" in state CONTROL_NODE
        ID        : 0
        Version   : 9.23(1)
        Serial No.: 9AC1VMGJKAQ
        CCL IP    : 169.254.200.4
        CCL MAC   : 6045.bda8.e07b
        Module    : NGFWv
        Resource  : 4 cores / 14336 MB RAM
        Last join : 05:22:55 UTC Jul 14 2025
        Last leave: N/A
Other members in the cluster:
    There is no other unit in the cluster
>
```

步骤 9 配置 Azure 网关负载均衡器。有关详细信息，请参阅 Auto Scale 与 Azure 网关负载均衡器使用案例。

步骤 10 将控制节点添加到 防火墙管理中心。请参阅将集群添加到管理中心（手动部署），第 100 页。

手动部署集群节点 - 基于 NLB 的部署

部署集群节点，以便它们形成集群。

过程

步骤 1 登录到 Azure 门户：https://portal.azure.com

步骤 2 创建一个资源组。

1. 在**基本 (Basics)** 选项卡中，从下拉列表中选择**订用 (Subscription)** 和**资源组 (Resource Group)**。
2. 选择所需的**区域 (Region)**。

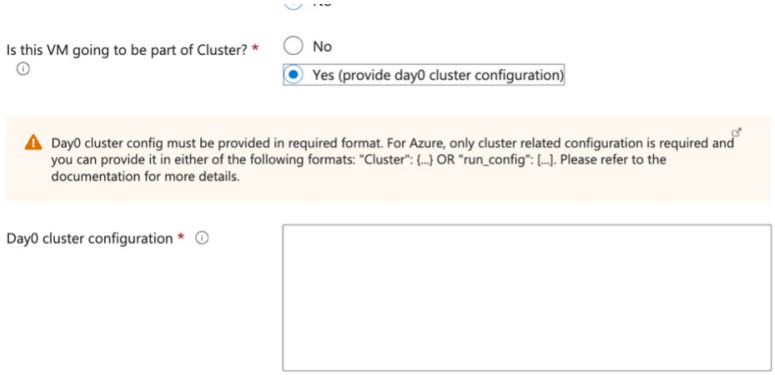
步骤 3 创建具有必要子网的虚拟网络：管理、内部、外部和集群控制链路 (CCL)。

注释
根据需要使用最小子网配置 CCL。较宽的子网可能会影响性能。

请参阅有关创建虚拟网络和子网的 Azure 文档：https://learn.microsoft.com/en-us/azure/virtual-network/quickstart-create-virtual-network?tabs=portal

步骤 4 转到应用市场，搜索 **Cisco Secure Firewall Threat Defense Virtual – BYOL 和 PAYG**，然后点击**创建**。

步骤 5 填写必填详细信息，并为**此虚拟机是否将成为集群的一部分？**选择**是**。



将以下集群相关配置粘贴到文本框中。

```
"Cluster": {
"CclSubnetRange": "ip_address_start ip_address_end", //mandatory user input
"ClusterGroupName": "cluster_name" //mandatory user input
}
```

步骤 6 点击**下一步**，然后选择**虚拟网络和子网**。

步骤 7 点击**查看 + 创建**。等待 Threat Defense Virtual 部署完成。

步骤 8 连接到 Threat Defense Virtual 设备并使用 **show cluster info** 命令确认集群已成功建立。

```
> show cluster info
Cluster ngfwv-cluster: On
    Interface mode: individual
Cluster Member Limit : 16
    This is "4" in state CONTROL_NODE
        ID        : 0
        Version   : 9.23(1)
        Serial No.: 9AC1VMGJKAQ
        CCL IP    : 169.254.200.4
        CCL MAC   : 6045.bda8.e07b
        Module    : NGFWv
        Resource  : 4 cores / 14336 MB RAM
        Last join : 05:22:55 UTC Jul 14 2025
        Last leave: N/A
Other members in the cluster:
    There is no other unit in the cluster
>
```

步骤 9 将控制节点添加到管理中心。请参阅将集群添加到管理中心（手动部署），第 100 页。

Azure 中的集群部署故障排除

- 问题：无流量

  故障排除：

  - 检查使用 GWLB 部署的 Threat Defense Virtual 实例的运行状况探测状态是否正常。
  - 如果 Threat Defense Virtual 实例的运行状况探测状态为不正常 -
    - 检查是否在 Management Center Virtual 中配置了静态路由。
    - 验证默认网关是否为数据子网的网关 IP。
    - 检查 Threat Defense Virtual 实例是否正在接收运行状况探测流量。
    - 检查在 Management Center Virtual 中配置的访问列表是否允许运行状况探测流量。

- 问题：集群未组建

  故障排除：

  - 检查 nve-only 集群接口的 IP 地址。确保您可以 ping 其他节点的仅 NVE 集群接口。
  - 检查仅 NVE 集群接口的 IP 地址是对象组的一部分。
  - 确保通过对象组来配置 NVE。
  - 集群组中的集群接口具有正确的 VNI 接口。此 VNI 接口具有相应对象组的 NVE。
  - 确保节点之间可相互 ping 通。由于每个节点都有自己的集群接口 IP，因此应该可以相互 ping 通。

- 验证模板部署期间提及的CCL子网的开始地址和结束地址是否正确。起始地址必须以子网中的第一个可用的 IP 地址开头。例如，如果子网为 192.168.1.0/27。那么起始地址应为 192.168.1.4（前三个 IP 地址由 Azure 保留）
- 检查 Management Center Virtual 是否具有有效的许可证。

- 问题：在同一资源组中再次部署资源时出现任何与角色相关的错误。

  故障排除：在终端上使用以下命令删除下面给出的角色。

  错误消息：

```
"error": {
"code": "RoleAssignmentUpdateNotPermitted",
"message": "Tenant ID, application ID, principal ID, and scope are not allowed to be
updated.” }
```

  - **az role assignment delete --resource-group** <资源组名称> **--role "Storage Queue Data Contributor"**
  - **az role assignment delete --resource-group** <资源组名称> **--role "Contributor"**

Azure 中的 Firewall Threat Defense Virtual 集群 Autoscale 解决方案

Azure 区域中的典型集群部署包括规定数量的 Firewall Threat Defense Virtual 实例（节点）。当 Azure 区域流量变化时，如果没有动态扩展（自动扩展）节点，这种集群安排中的资源利用率可能未充分利用资源或导致延迟。思科在 7.7 及更高版本中为 Firewall Threat Defense Virtual 集群提供自动扩展解决方案，支持动态扩展 Azure 区域中的节点。它允许您根据网络流量从集群内向内扩展或横向扩展节点。它使用基于 Azure VMSS 指标（如 CPU 和内存指标）的资源利用率统计信息的逻辑，动态添加或删除集群中的节点。

Azure 中使用自动扩展解决方案的 Firewall Threat Defense Virtual 集群同时支持网络负载均衡器（NLB 或三明治拓扑）和网关负载均衡器 (GWLB)。请参阅拓扑示例，第 55 页

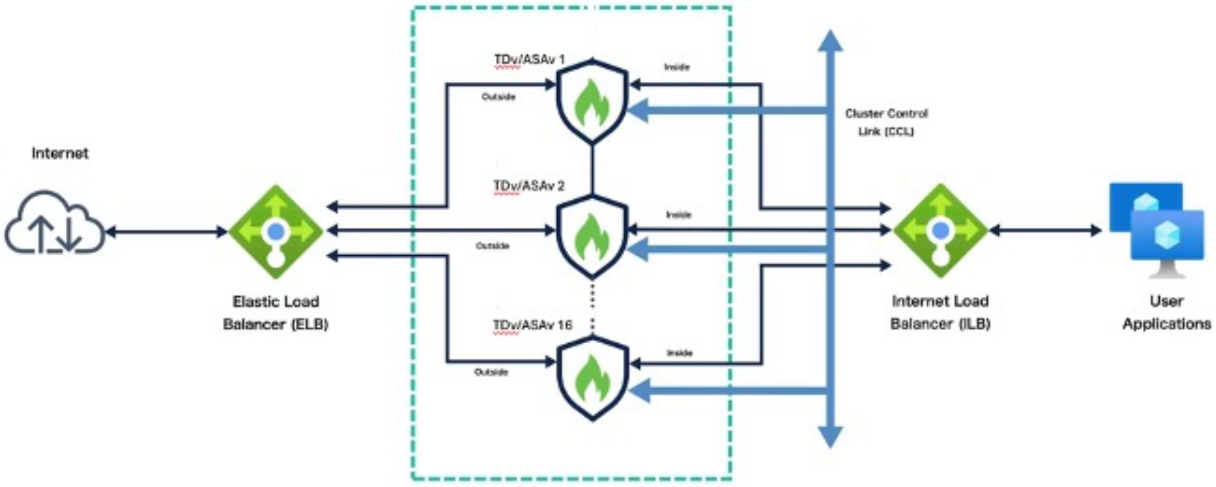
思科提供单独的 Azure 资源管理器 (ARM) 模板用于使用 NLB 和 GWLB 在 Azure 中部署具有自动扩展功能的 Firewall Threat Defense Virtual 集群，并提供基础设施和配置模板用于部署函数应用和逻辑应用等 Azure 服务。

拓扑示例

Firewall Threat Defense Virtual 使用三明治拓扑（网络负载均衡器）在 Azure 中通过自动扩展建立集群

Azure 中使用三明治拓扑结构 (NLB) 的自动扩展的 Firewall Threat Defense Virtual 集群用例是一种自动水平缩放解决方案，它将 Firewall Threat Defense Virtual 规模集置于 Azure 内部负载均衡器 (ILB) 与 Azure 外部负载均衡器 (ELB) 之间。

在此拓扑中，Firewall Threat Defense Virtual 仅使用四个接口：管理、内部、外部和 CCL 子网。



Firewall Threat Defense Virtual 使用三明治拓扑 (NLB) 在 Azure 中通过自动扩展建立集群

下面简要介绍了 Firewall Threat Defense Virtual集群如何使用 NLB 功能在 Azure 中进行自动扩展：

- ELB 将流量从互联网分发到规模集中的 Firewall Threat Defense Virtual 实例；然后，防火墙将流量转发到应用。
- ILB 将出站互联网流量从应用分发到规模集中的 Firewall Threat Defense Virtual 实例；然后，防火墙将流量转发到互联网。
- 网络数据包决不会在一个连接中同时穿过（内部和外部）负载均衡器。
- 规模集中的 Firewall Threat Defense Virtual实例数将根据负载条件自动进行扩展和配置。

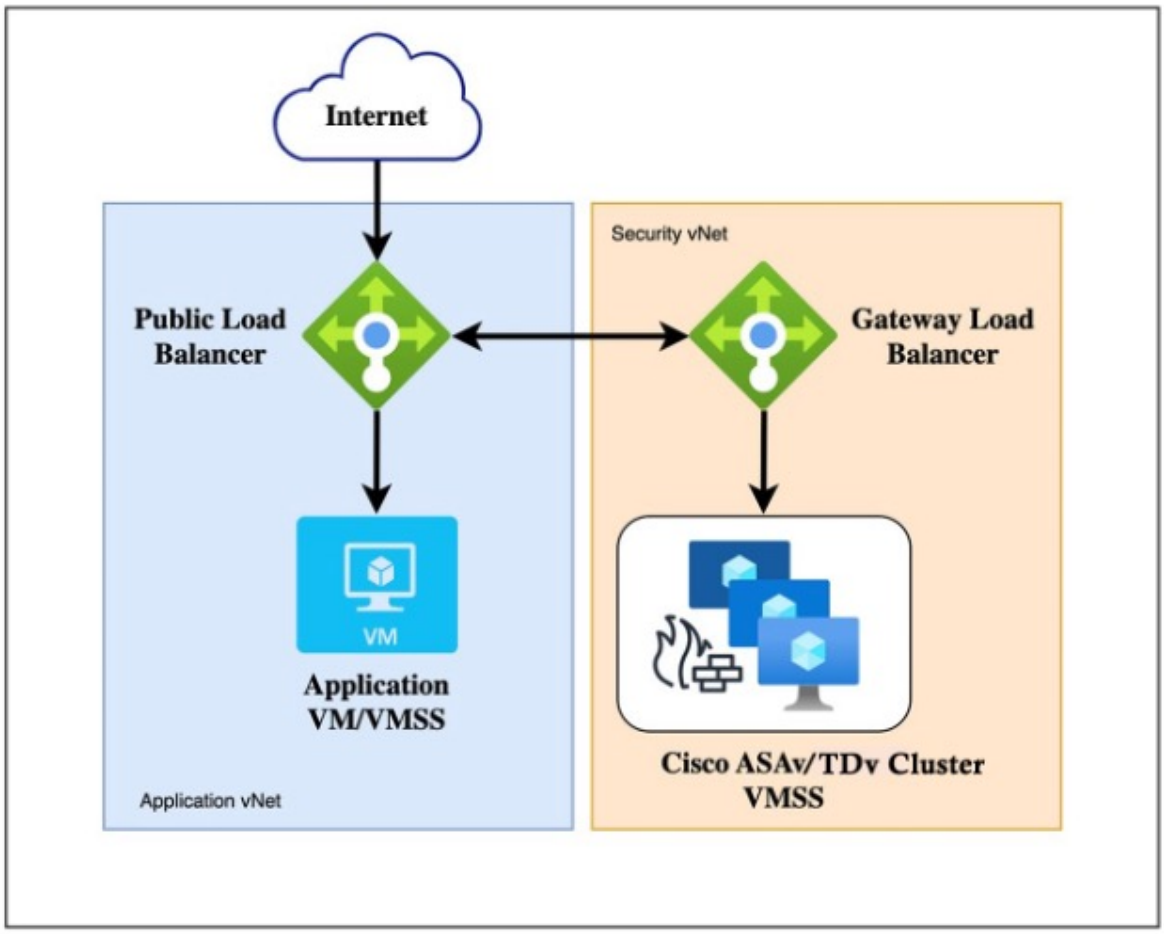
Firewall Threat Defense Virtual 使用网关负载均衡器在 Azure 中建立自动扩展集群

使用自动扩展解决方案的 Azure 网关负载均衡器 (GWLB) 与 Firewall Threat Defense Virtual 集群集成可简化集群设置中的实例部署、管理和扩展。Azure 网关负载均衡器 (GWLB) 可确保 Cisco Secure Firewall 检查进出 Azure VM（例如应用服务器）的互联网流量，而无需更改任何路由。这种集成还降低了操作复杂性，并为防火墙上的流量提供了单一的入口和出口点。应用和基础设施可以保持源 IP 地址的可视性，而这在某些环境中至关重要。

Firewall Threat Defense Virtual 在此使用案例中仅使用三个接口：管理、数据和 CCL 接口。

注释

- 如果要部署 Azure GWLB，则不需要网络地址转换 (NAT)。
- 仅支持 IPv4。



下面简要介绍了 Firewall Threat Defense Virtual集群如何使用 GWLB 功能在 Azure 中进行自动扩展：

- 来自互联网的入站流量会进入 GWLB 端点，然后由端点将流量传输到 GWLB。
- 然后，流量将路由到 Firewall Threat Defense Virtual 集群。
- 集群中的 Firewall Threat Defense Virtual 实例检测到流量后，将其转发到应用虚拟机。

前提条件

- 确保您在 Azure 订阅中具有所有者角色。
- 创建 Azure 资源组。确保已创建 Azure 虚拟网络以及必要的子网。
  - 基于 NLB 的集群接口：管理、诊断、内部、外部、CCL 和函数应用。
  - 基于 GWLB 的集群接口：管理、诊断、数据、CCL 和函数应用。
- 在管理中心上：

- 确保 Management Center Virtual 已正确授权。
- 创建访问控制策略。
- 为接口创建安全区域(SZ)对象。对于基于NLB的集群，为内部和外部接口创建安全区域。对于基于 GWLB 的集群，为数据接口创建安全区域。
- 为 Azure 函数创建单独的用户名和密码，以将 Threat Defense Virtual 实例添加到 Management Center Virtual 并配置这些实例。

- 在本地系统上安装 Azure CLI。
- 从 GitHub 将 Azure 集群自动扩展存储库下载到本地计算机，并运行命令 **python3 make.py build** 创建 Azure 函数 zip 文件。

Azure 中的 Firewall Threat Defense Virtual 集群自动扩展逻辑

扩展策略

在具有自动扩展的集群中，节点的扩展根据以下策略确定：

- 扩展策略 1 - 当一个集群节点超过资源使用限制时。
- 扩展策略 2 - 所有节点的总体平均资源利用率。

横向扩展

横向扩展是指当流量负载阈值超过任何一个集群节点上配置的CPU或内存限制时，向集群添加新节点的过程。

以下是在横向扩展期间向集群添加新节点的过程：

1. 已启动一个新的 Firewall Threat Defense Virtual 实例。
2. 相应配置将被应用于 Firewall Threat Defense Virtual。
3. 已应用适当的许可证。
4. 一个新的 Firewall Threat Defense Virtual 实例将被添加到集群中。

如果在横向扩展过程中，新的 Firewall Threat Defense Virtual 实例的配置失败（低概率），则会终止失败的实例，并启动和配置一个新实例。

内向扩展

内向扩展是指当配置的内向扩展阈值和群集实例总数超过最小集群规模时，将节点从群集中移除的过程。

以下是在内向扩展过程中终止集群中一个节点的过程：

1. 使用 VMSS 指标确定 CPU 或内存使用率最低的 Firewall Threat Defense Virtual 实例。
2. 如果有多个实例具有相同的最低利用率，则选择 VMSS 中 VM 索引较高的实例进行内向扩展。

3. 通过适当的配置和策略，该实例的任何新连接都会被禁用。
4. 实例会从智能许可中注销（适用于 BYOL）。
5. 实例将被终止。

Azure Functions（函数应用）

Function 应用可帮助启用 Firewall Threat Defense Virtual 群集并在管理中心注册。Function 应用还可以帮助您为支持自动扩展部署的 Firewall Threat Defense Virtual 集群选择托管计划。

提供以下两种类型的托管计划：

- 使用量
  - 这是具有自动扩展功能的 Firewall Threat Defense Virtual 集群的默认托管计划。
  - 该计划允许 Function 应用通过打开 SSH 端口连接到该区域的 Azure 数据中心 IP 地址，从而连接到 Firewall Threat Defense Virtual 实例。
- 高级
  - 您可以在部署期间为 Function 应用选择此托管计划。
  - 此计划支持将网络地址转换 (NAT) 网关添加到 Function 应用，以控制 Function 应用的出站 IP 地址。此计划仅允许从 NAT 网关的固定 IP 地址对 Firewall Threat Defense Virtual 实例进行 SSH 访问，从而增强安全性。

有关自动扩展解决方案组件概述的详细信息，请参阅《*Cisco Secure Firewall Threat Defense Virtual* 入门指南》中的自动扩展解决方案组件。

GitHub 上的部署和基础设施模板

思科提供 Azure 资源管理器 (ARM) 模板和脚本，用于使用多个 Azure 服务（包括函数应用、逻辑应用、自动扩展组等）部署 Firewall Threat Defense Virtual 集群的自动扩展组。

Firewall Threat Defense Virtual 集群的自动扩展解决方案是基于 ARM 模板的部署，可提供：

- 使用 Function 应用与管理中心进行完全自动化的 Firewall Threat Defense Virtual 实例注册和注销注册。
- 自动应用到横向扩展 Threat Defense Virtual 实例的 NAT 策略、访问控制策略和路由。
- 支持 GWLB 和 NLB 负载均衡器。
- 仅适用于管理中心；不支持设备管理器。

使用自动扩展解决方案模板的 Firewall Threat Defense Virtual 集群

Azure 资源管理器 (ARM) 模板

根据您在 Azure 中为集群使用的（NLB 或 GWLB）负载均衡器，为自动扩展解决方案提供了两套模板。

GitHub 上提供了以下模板：

- 使用 NLB 的 Firewall Threat Defense Virtual 集群的自动扩展解决方案模板：`azure_ftdv_nlb_cluster.json.json`，可从文件夹 `arm-templates` 获取。
- 使用 GWLB 的 Firewall Threat Defense Virtual 集群的自动扩展解决方案模板：`azure_ftdv_gwlb_cluster.json`，可从文件夹 `arm-templates` 获取。

设置 Azure 基础架构和配置

- 用于在 Firewall Threat Defense Virtual 实例上启用集群的函数应用：`cluster_functions.zip`。
- Firewall Threat Defense Virtual 用于部署、缩容和扩容工作流的逻辑应用代码：`logical_app.txt`。

输入参数

下表定义了模板参数并提供了示例。确定这些值后，就可以在将 Azure 资源管理器 (ARM) 模板部署到 Azure 订阅时使用这些参数来创建 Firewall Threat Defense Virtual 设备。在使用 GWLB for Azure 的自动扩展集群中，还创建了网络基础设施，因此必须在模板中配置额外的输入参数。参数说明的含义不言自明。

表 *4:* 模板参数

参数名	允许的值/类型	说明	资源创建类型
resourceNamePrefix	字符串*（3-10 个字符）	所有资源都使用包含此前缀的名称创建。 注：只能使用小写字母。 示例：ftdv	New
virtualNetworkRg	字符串	虚拟网络资源组名称。 示例：cisco-virtualnet-rg	现有
virtualNetworkName	字符串	虚拟网络名称（已创建）。 示例：cisco-virtualnet	现有
virtualNetworkCidr	CIDR 格式 x.x.x.x/y	虚拟网络的 CIDR（已创建）	现有
mgmtSubnet	字符串	管理子网名称（已创建） 示例：cisco-mgmt-subnet	现有

参数名	允许的值/类型	说明	资源创建类型
dataSubnet	字符串	数据子网名称（已创建） 示例：cisco-data-subnet	
cclSubnet	字符串	集群控制链路子网名称。 示例：cisco-ccl-subnet	
cclSubnetStartAddr	字符串	CCL 子网 IP 地址的起始范围。 示例：3.4.5.6	
cclSubnetEndAddr	字符串	CCL 子网 IP 地址的结束范围。 示例：5.6.7.8	
gwlbIP	字符串	GWLB 已在现有数据子网中创建。 示例：10.0.2.4	
dataNetworkGatewayIp	字符串	数据子网的网关 IP 地址。 示例：10.0.2.7	
outsideSecurityZoneName	字符串	在管理中心创建的安全区对象名称 示例：outside-sz	
TDvmManagementUserName	字符串	TDv 管理员用户名。 不允许提供“admin”作为用户名。	
diagSubnet	字符串	诊断子网名称（已创建）。 示例：cisco-diag-subnet	现有
insideSubnet	字符串	内部子网名称（已创建）。 示例：cisco-inside-subnet	现有
internalLbIp	字符串	内部子网的内部负载均衡器 IP 地址（已创建）。 例如：1.2.3.4	现有
insideNetworkGatewayIp	字符串	内部子网网关 IP 地址（已创建）。	现有
outsideSubnet	字符串	外部子网名称（已创建）。 示例：cisco-outside-subnet	现有

参数名	允许的值/类型	说明	资源创建类型
outsideNetworkGatewayIp	字符串	外部子网网关 IP（已创建）。	现有
deviceGroupName	字符串	防火墙管理中心中的设备组（已创建）	现有
insideZoneName	字符串	防火墙管理中心中的内部区域名称（已创建）	现有
outsideZoneName	字符串	防火墙管理中心中的外部区域名称（已创建）	现有
softwareVersion	字符串	Firewall Threat Defense Virtual 版本（在部署期间从下拉列表中选择）。	现有
vmSize	字符串	Firewall Threat Defense Virtual 实例的大小（在部署过程中从下拉列表中选择）。	不适用
ftdLicensingSku	字符串	Firewall Threat Defense Virtual 许可模式 (PAYG/BYOL) 注：PAYG 在版本 6.5+ 中受支持。	不适用
licenseCapability	逗号分隔的字符串	BASE, MALWARE, URLFilter, THREAT	不适用
tdVmManagementUserName	字符串*	Firewall Threat Defense Virtual VM 管理管理员用户名。 这**不能**是“admin”。请参阅 Azure 以了解 VM 管理员用户名准则。	New
tdVmManagementUserPassword	字符串*	Firewall Threat Defense Virtual VM 管理管理员用户的密码。 密码的长度必须为 12 至 72 个字符，而且必须具有：小写、大写、数字及特殊字符；重复字符不得超过 2 个。 **注释** 模板中不对此进行合规性检查。	New

参数名	允许的值/类型	说明	资源创建类型
ftdAdminUserPassword	字符串	Firewall Threat Defense Virtual 管理员用户密码。 **注释** 针对 **TDvmManagementUserPassword** 参数提到的条件也适用于此参数。	
fmcIpAddress	字符串 x.x.x.x	防火墙管理中心 的公共 IP 地址（已创建）	现有
fmcUserName	字符串	防火墙管理中心用户名，具有管理权限（已创建）	现有
fmcPassword	字符串	上述 防火墙管理中心 用户名的防火墙管理中心密码（已创建）	现有
policyName	字符串	在 防火墙管理中心 中创建的安全策略（已创建）	现有
clusterGroupName	字符串	在将威胁防御设备注册到管理中心时使用的集群组名称。 示例：tdv-cluster	
healthCheckPortNumber	字符串	在网关负载均衡器中创建运行状况探测器时使用的运行状况检查端口号。 示例：8080	
functionHostingPlan	字符串	功能部署托管计划（消耗使用使用量托管计划，高级：使用高级托管计划）。 默认值：功耗	
functionAppSubnet	字符串	函数应用子网名称（已创建）。 示例：tdv-fapp-subnet	
functionAppSubnetCIDR	字符串	函数应用子网的 CIDR（已创建）。 示例：10.0.4.0/27	
scalingMetricsList	字符串	用于确定扩展决定的指标。 允许：CPU 和内存	

参数名	允许的值/类型	说明	资源创建类型
scalingPolicy	POLICY-1/POLICY-2	**POLICY-1**：当任何 Firewall Threat Defense Virtual 的平均负载在所配置的持续时间内超过外向扩展阈值时，将触发外向扩展。 **POLICY-2**：当自动扩展组中所有 Firewall Threat Defense Virtual 设备的平均负载在所配置的持续时间内超过外向扩展阈值时，将触发外向扩展。 在两种情况下，内向扩展逻辑都保持不变：当所有 Firewall Threat Defense Virtual 设备的平均负载在所配置的持续时间内低于内向扩展阈值时，将触发内向扩展。	不适用
scalingMetricsList	字符串	用于制定扩展决策的指标。 允许：CPU、内存 默认值：CPU	不适用
cpuScaleInThreshold	字符串	CPU 指标的内向扩展阈值（以百分比为单位）。 默认值：10 当 Firewall Threat Defense Virtual 指标低于此值时，将触发扩展。 请参阅Azure 中的 Firewall Threat Defense Virtual 集群自动扩展逻辑，第 58 页。	不适用

参数名	允许的值/类型	说明	资源创建类型
cpuScaleOutThreshold	字符串	CPU 指标的横向扩展阈值（以百分比为单位）。 默认值：80 当 Firewall Threat Defense Virtual 指标高于此值时，将触发横向扩展。 “cpuScaleOutThreshold”应始终**大于**“cpuScaleInThreshold”。 请参阅Azure 中的 Firewall Threat Defense Virtual 集群自动扩展逻辑，第 58 页。	不适用
memoryScaleInThreshold	字符串	内存指标的内向扩展阈值（以百分比为单位）。 默认值：0 当 Firewall Threat Defense Virtual 指标低于此值时，将触发扩展。 请参阅Azure 中的 Firewall Threat Defense Virtual 集群自动扩展逻辑，第 58 页。	不适用
memoryScaleOutThreshold	字符串	内存指标的横向扩展阈值（以百分比为单位）。 默认值：0 当 Firewall Threat Defense Virtual 指标高于此值时，将触发横向扩展。 “memoryScaleOutThreshold”应始终**大于**“memoryScaleInThreshold”。 请参阅Azure 中的 Firewall Threat Defense Virtual 集群自动扩展逻辑，第 58 页。	不适用
minFtdCount	整数	在任何给定时间，规模集中可用的最小 Firewall Threat Defense Virtual 实例数。 示例：2	不适用

参数名	允许的值/类型	说明	资源创建类型
maxFtdCount	整数	规模集中允许的最大 Firewall Threat Defense Virtual 实例数。 示例：10 **注释** 此数量受 防火墙管理中心 容量的限制。 Auto Scale 逻辑不会检查此变量的范围，因此请认真填写。	不适用
metricsAverageDuration	整数	从下拉列表中选择。 此数字表示计算指标平均值的时间（以分钟为单位）。 如果此变量的值为 5（即 5 分钟），则当计划 Auto Scale Manager 时，它将检查过去 5 分钟内的指标平均值，并且基于此平均值做出扩展决定。 **注释** 由于 Azure 限制，仅 1、5、15 和 30 是有效数字。	不适用

参数名	允许的值/类型	说明	资源创建类型
initDeploymentMode	BULK/STEP	主要适用于第一次部署，或者规模集不包含任何 Firewall Threat Defense Virtual 实例时。 BULK：Auto Scale 管理器将尝试一次并行部署“minFtdCount”数量的 Firewall Threat Defense Virtual 实例。 **注释** 启动采用并行方式，但由于 防火墙管理中心 的限制，需要按顺序注册到 防火墙管理中心。 STEP：Auto Scale 管理器将按照计划间隔逐个部署“minFtdCount”数量的 Firewall Threat Defense Virtual 设备。 **注释** STEP 选项需要较长时间来启动“minFtdCount”数量的实例并使用 防火墙管理中心 进行配置，然后实现运行，但在调试时很有帮助。 BULK 选项启动所有“minFtdCount”数量的 Firewall Threat Defense Virtual 所花费的时间与一次 Firewall Threat Defense Virtual 启动相同（因为它是并行运行的），但 防火墙管理中心 注册是按顺序进行的。 部署“minFtdCount”数量的 Firewall Threat Defense Virtual 所花费的总时间 =（启动一个 Firewall Threat Defense Virtual 所用的时间 + 注册/配置一个 Firewall Threat Defense Virtual 所用的时间 * minFtdCount）。	
*Azure 对新资源的命名约定有限制。查看限制，或者直接全部使用小写字母。**不要使用空格或任何其他特殊字符**。			

Firewall Threat Defense Virtual 具有自动扩展部署过程和资源的集群

Firewall Threat Defense Virtual 在 Azure 上部署具有自动扩展功能的集群涉及以下内容：

- 部署 ARM 模板。
- 构建并部署集群功能。
- 更新并启用逻辑应用。

Azure 资源管理器模板部署资源

对于三明治拓扑 **(NLB)** - `azure_ftdv_nlb_cluster_autoscale.json`，当使用 ARM 模板在 Azure 中部署具有自动扩展功能的 Firewall Threat Defense Virtual 集群时，会在资源组中创建以下资源

- 虚拟机规模集 (VMSS)
- 外部负载均衡器
- 内部负载均衡器
- Azure 函数应用
- 逻辑应用
- 安全组（用于数据接口和管理接口）

当使用 GWLB - `azure_ftdv_gwlb_cluster_autoscale.json`在 Azure 中部署具有自动扩展功能的 Firewall Threat Defense Virtual 集群时，会在资源组中创建以下资源

- 虚拟机 (VM) 或虚拟机规模集 (VMSS)
- 网关负载均衡器 (GWLB)
- Azure 函数应用
- 逻辑应用
- 网络基础设施
- 部署所需的安全组和其他各种组件。

使用自动扩展解决方案部署 Firewall Threat Defense Virtual 集群

使用 ARM 模板在 Azure 上部署具有自动扩展解决方案的 Threat Defense Virtual 集群。根据拓扑结构、三明治 (NLB) 使用案例或 GWLB 使用案例，您需要下载并配置适当的 ARM 模板，以便在 Azure 上部署支持自动扩展的 Firewall Threat Defense Virtual 集群解决方案。

开始之前

从 GitHub 下载部署软件包

面向 Azure 的使用 NLB 解决方案的 Firewall Threat Defense Virtual 集群自动扩展是一个基于 Azure 资源管理器 (ARM) 模板的部署，它会利用 Azure 提供的无服务器基础设施（逻辑应用、Azure 函数、负载均衡器、虚拟机扩展设置等）。

面向 Azure 的使用 GWLB 解决方案的 Firewall Threat Defense Virtual 集群是一种基于 ARM 模板的部署，可创建 GWLB、网络基础设施、Threat Defense Virtual 自动扩展组、无服务器组件和其他所需资源。

两种解决方案的部署过程均类似。

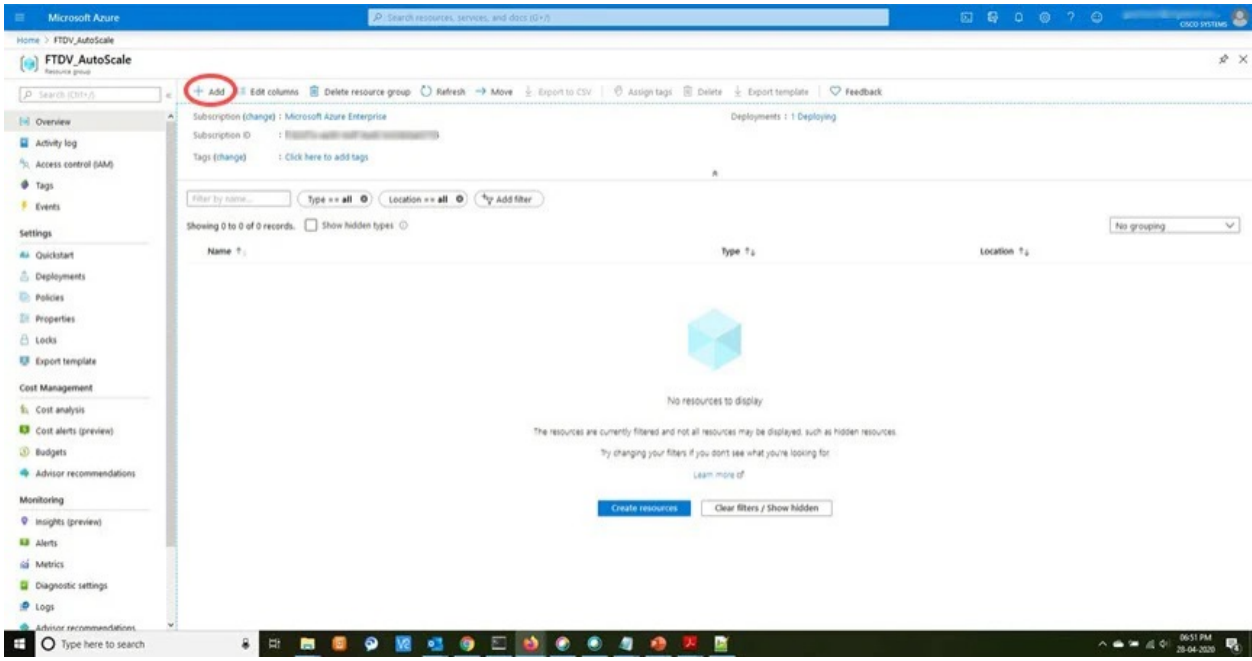
下载启动面向 Azure 的使用自动扩展解决方案的 Firewall Threat Defense Virtual 集群所需的文件。

您的版本的部署脚本和模板可从 GitHub 存储库获取。

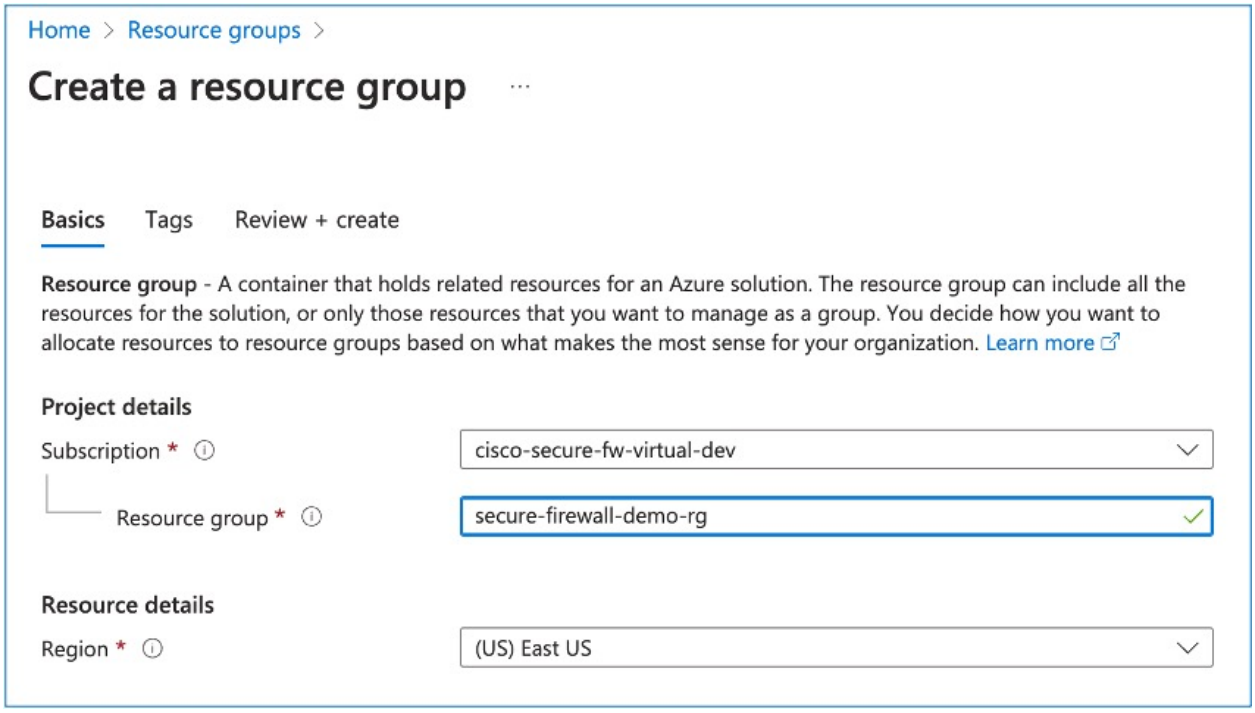
过程

步骤 1 使用您的 Microsoft 帐户用户名和密码登录 Microsoft Azure 门户 (https://portal.azure.com)。

步骤 2 点击服务菜单中的**资源组 (Resource groups)** 以访问**资源组 (Resource Groups)** 边栏选项卡。您将看到该边栏选项卡中列出您的订用中的所有资源组。创建一个新的资源组或选择一个现有的空资源组。例如， **threat defense virtual_AutoScale**。

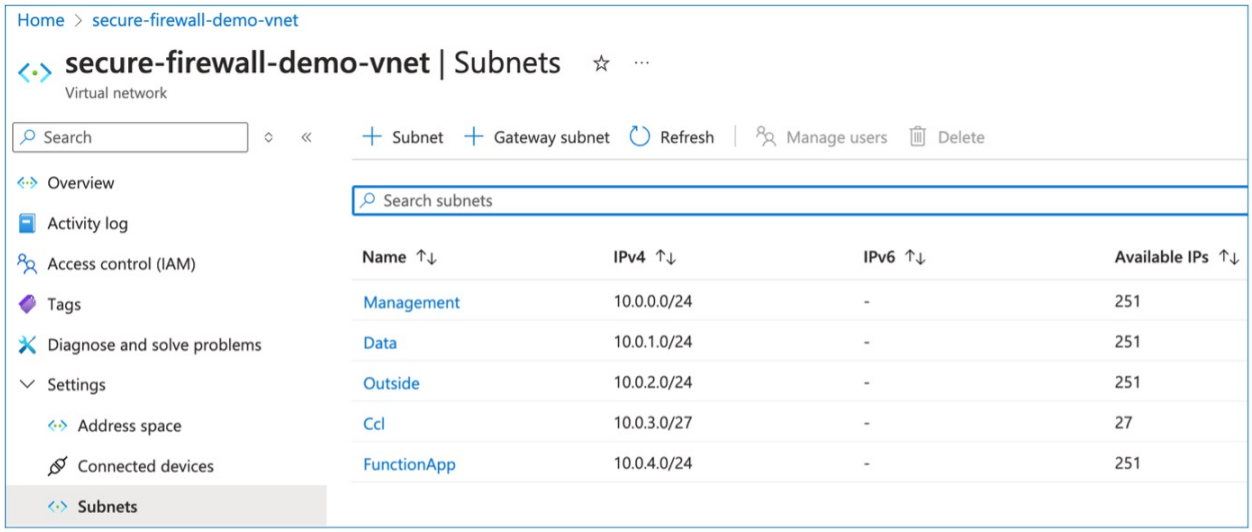


步骤 3 点击**创建资源 (+) (Create a resource [+])**，为模板部署创建新资源。此时将显示**创建资源组 (Create Resource Group)** 边栏选项卡。



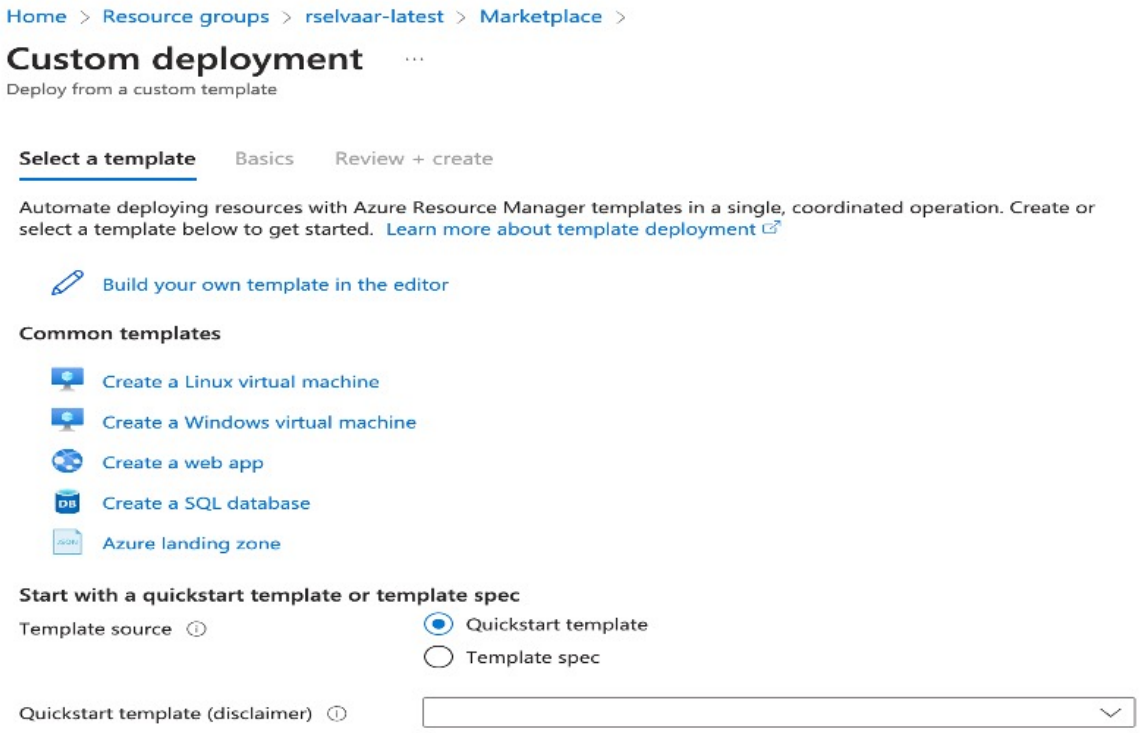
步骤 4 4. 点击服务菜单中的**虚拟网络 (Virtual Network)**，以访问“虚拟”(Virtual) 网络边栏选项卡。使用子网创建虚拟网络。

- 对于 GWLB 部署，创建包含管理、数据、CCL 子网和函数应用的虚拟网络。
- 对于 NLB 部署，创建包含管理、内部、外部、CCL 子网和函数应用的虚拟网络。

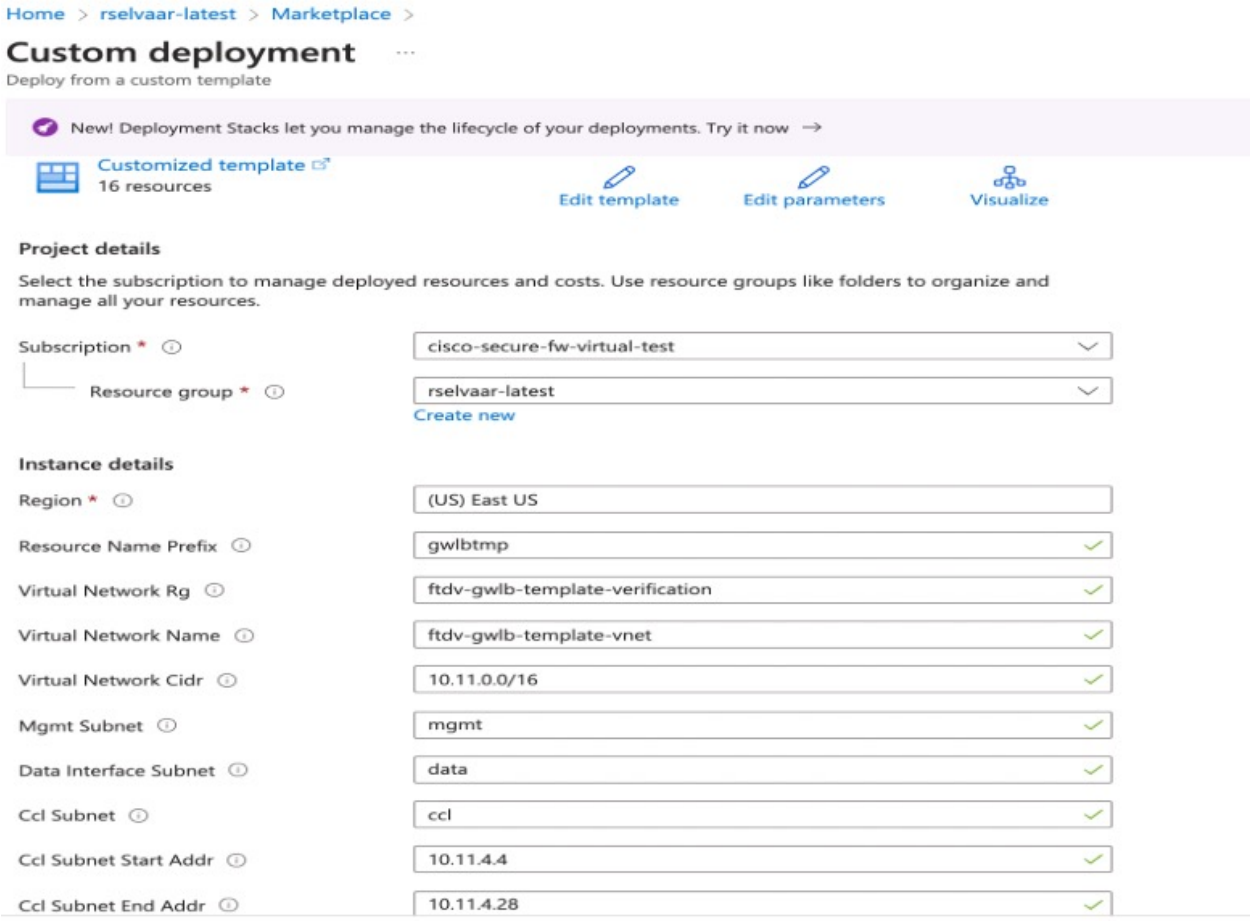


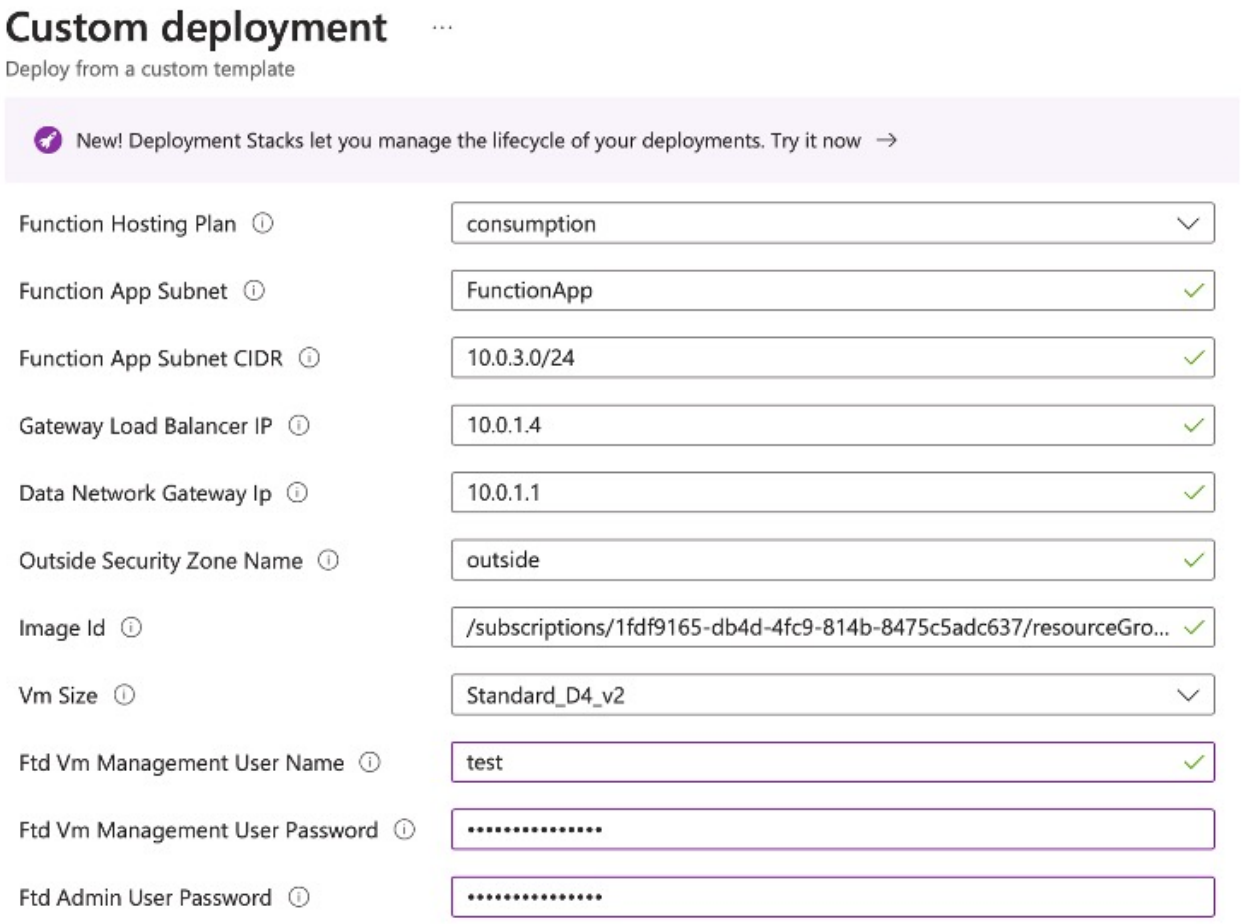
步骤 5 在**搜索市场 (Search the Marketplace)** 中，键入**模板部署 (Template deployment)**（使用自定义模板部署），然后按 **Enter**。

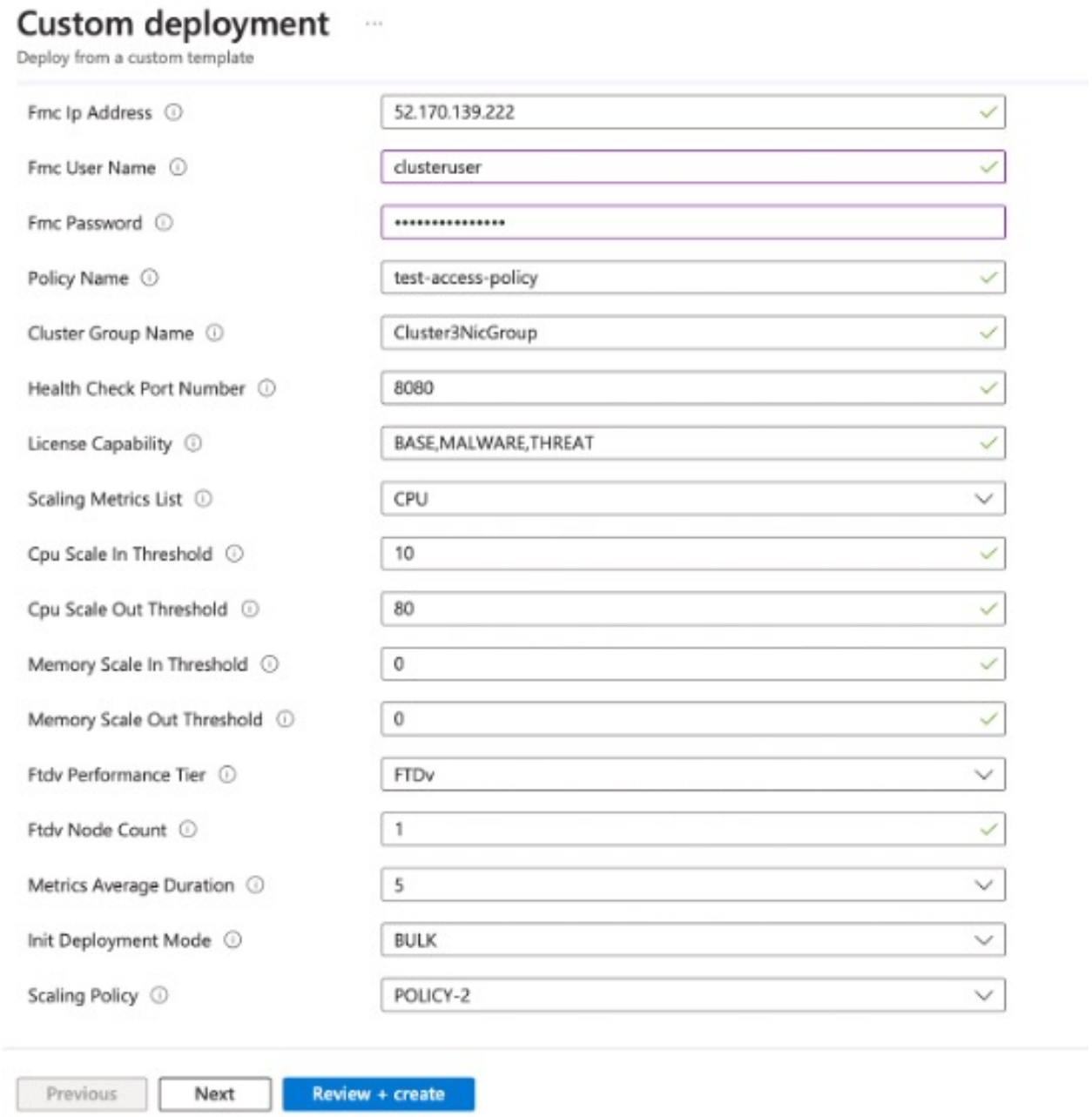
步骤 6 点击**创建 (Create)**。创建模板时有多个选项。选择**在编辑器中选择构建您自己的模板 (Build your own template in editor)**。



步骤 7 在**编辑模板**窗口中，删除所有默认内容并从更新的 `azure_ftdv_gwlb_cluster_custom_image.json` 或 `azure_ftdv_nlb_cluster_custom_image.json`（具体取决于您在 Azure 上部署的自动扩展解决方案的类型）复制内容，然后点击**保存**。或者点击**加载文件 (Load file)**，从您的计算机浏览并上传此文件。


Home > rselvaar-latest > Marketplace >
Custom deployment
Deploy from a custom template
New! Deployment Stacks let you manage the lifecycle of your deployments. Try it now →
Customized template
16 resources
Edit template
Edit parameters
Visualize
Project details
Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.
Subscription *
cisco-secure-fw-virtual-test
Resource group *
rselvaar-latest
Create new
Instance details
Region *
(US) East US
Resource Name Prefix
gwlbtmp
Virtual Network Rg
ftdv-gwlb-template-verification
Virtual Network Name
ftdv-gwlb-template-vnet
Virtual Network Cidr
10.11.0.0/16
Mgmt Subnet
mgmt
Data Interface Subnet
data
Ccl Subnet
ccl
Ccl Subnet Start Addr
10.11.4.4
Ccl Subnet End Addr
10.11.4.28


Custom deployment
Deploy from a custom template
New! Deployment Stacks let you manage the lifecycle of your deployments. Try it now →
Function Hosting Plan
consumption
Function App Subnet
FunctionApp
Function App Subnet CIDR
10.0.3.0/24
Gateway Load Balancer IP
10.0.1.4
Data Network Gateway Ip
10.0.1.1
Outside Security Zone Name
outside
Image Id
/subscriptions/1fdf9165-db4d-4fc9-814b-8475c5adc637/resourceGro...
Vm Size
Standard_D4_v2
Ftd Vm Management User Name
test
Ftd Vm Management User Password
Ftd Admin User Password



步骤 8 在参数字段部分中填写所有参数。有关每个参数的详细信息，请参阅输入参数，然后点击**查看+创建 (Review+Create)**。

步骤 9 模板部署成功后，就会为 Azure 解决方案创建 Threat Defense Virtual 自动扩展所需的所有资源。请参阅下图中的资源。**类型 (Type)** 列描述了每个资源，包括逻辑应用、VMSS、负载均衡器、公共 IP 地址等。

下一步做什么

部署 Azure Functions 应用 ， 第 75 页。

部署 Azure Functions 应用

部署 ARM 模板时，Azure 会创建名称为 **<resourceNamePrefix>-function-app** 的功能应用。

过程

步骤 1 转到部署 ARM 模板时创建的 Function 应用，并执行以下操作：

从本地计算机运行以下命令，将集群自动扩展 Azure Functions 部署到函数应用。

```
az functionapp deployment source config-zip -g <Resource Group Name>
-n <Function App Name> --src  <cluster_functions.zip> --build-remote true
```

步骤 2 部署 Azure Functions 后，您可以在函数应用的概述部分中查看上传的函数。

更新 Azure 逻辑应用

逻辑应用充当Autoscale功能的协调器。ARM模板会创建一个主干逻辑应用，然后您需要手动更新，提供使之作为 Auto Scale 协调器发挥作用所需的信息。

过程

步骤 1 从存储库中将文件 *LogicApp.txt* 恢复到本地系统，然后如下所示进行编辑。

重要事项
在继续之前，阅读并理解所有这些步骤。

这些手动步骤不会在 ARM 模板中自动执行，以便稍后只能独立升级逻辑应用。

a) 必需： 查找所有“SUBSCRIPTION_ID”并替换为您的订用 ID 信息。
b) 必需： 查找所有“RG_NAME”并替换为您的资源组名称。
c) 必需： 查找所有“FUNCTIONAPPNAME”并替换为您的函数应用名称。

以下示例显示了 *LogicApp.txt* 文件中的几行：

```
  "AutoScaleManager": {
      "inputs": {
          "function": {
              "id":
"/subscriptions/SUBSCRIPTION_ID/resourceGroups/RG_NAME/providers/Microsoft.Web/sites/FUNCTIONAPPNAME/functions/AutoScaleManager"

          }
.
```

```
.
                        },
                        "Deploy_Changes_to_FTD": {
                            "inputs": {
                                "body": "@body('AutoScaleManager')",
                                "function": {
                                    "id":
"/subscriptions/SUBSCRIPTION_ID/resourceGroups/RG_NAME/providers/Microsoft.Web/sites/FUNCTIONAPPNAME/functions/DeployConfiguration"

                                }
.
.
                        "DeviceDeRegister": {
                            "inputs": {
                                "body": "@body('AutoScaleManager')",
                                "function": {
                                    "id":
"/subscriptions/SUBSCRIPTION_ID/resourceGroups/RG_NAME/providers/Microsoft.Web/sites/FUNCTIONAPPNAME/functions/DeviceDeRegister"

                                }
                            },
                            "runAfter": {
                                "Delay_For_connection_Draining": [
```

d) （可选） 编辑触发间隔，或保留默认值 (5)。这是定期触发 Autoscale 的时间间隔。以下示例显示了 *LogicApp.txt* 文件中的几行：

```
"triggers": {
    "Recurrence": {
        "conditions": [],
        "inputs": {},
        "recurrence": {
            "frequency": "Minute",
            "interval": 5
        },
```

e) （可选） 编辑要进行排空的时间，或保留默认值 (5)。这是内向扩展操作期间，在删除设备之前从 Firewall Threat Defense Virtual 中排空现有连接的时间间隔。以下示例显示了 *LogicApp.txt* 文件中的几行：

```
 "actions": {
      "Branch_based_on_Scale-In_or_Scale-Out_condition": {
          "actions": {
              "Delay_For_connection_Draining": {
                  "inputs": {
                      "interval": {
                          "count": 5,
                          "unit": "Minute"
                      }
```

f) （可选） 编辑冷却时间，或保留默认值 (10)。这是在外向扩展完成后不执行任何操作的时间。以下示例显示了 *LogicApp.txt* 文件中的几行：

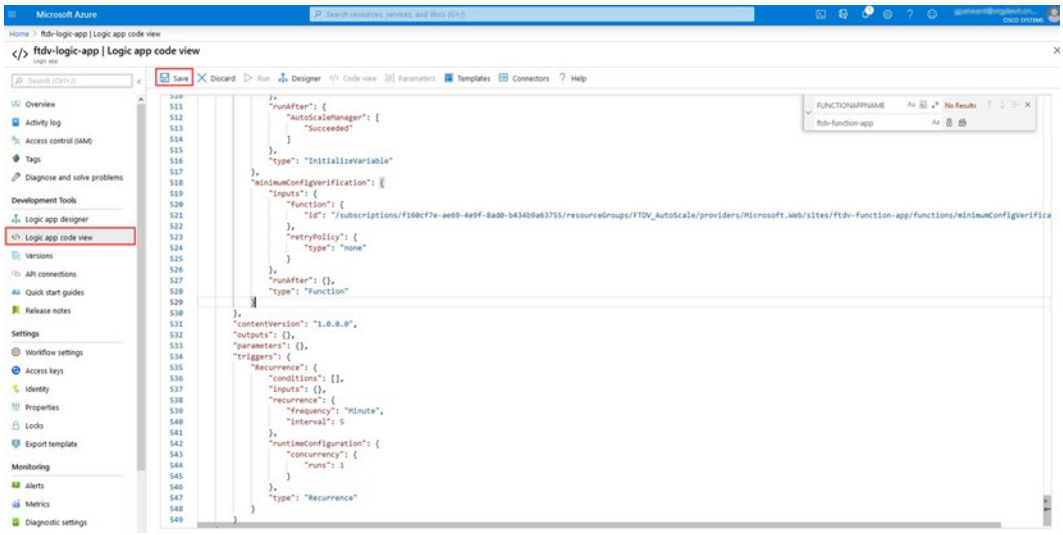
```
    "actions": {
        "Branch_based_on_Scale-Out_or_Invalid_condition": {
            "actions": {
                "Cooldown_time": {
```

```
"inputs": {
    "interval": {
        "count": 10,
        "unit": "Second"
 }
```

注释
这些步骤也可以从 Azure 门户完成。有关详细信息，请参阅 Azure 文档。

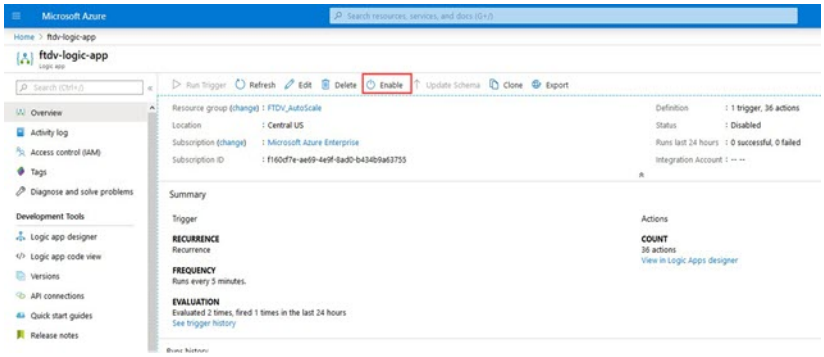
步骤 2 转至**逻辑应用代码视图 (Logic App code view)**，删除默认内容并粘贴编辑后的 *LogicApp.txt* 文件内容，然后点击**保存 (Save)**。

图 ***15:*** 逻辑应用代码视图



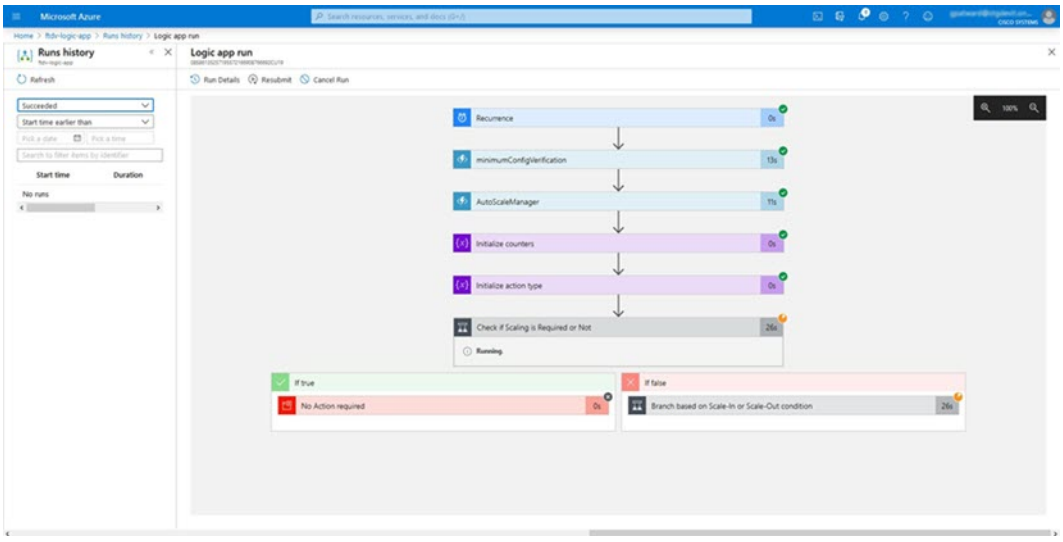
步骤 3 保存逻辑应用时，它处于“禁用”状态。当要启动 Auto Scale Manager 时，请点击**启用 (Enable)**。

图 ***16:*** 启用逻辑应用



步骤 4 启用后，任务就会开始运行。点击“正在运行”(Running) 状态可查看活动。

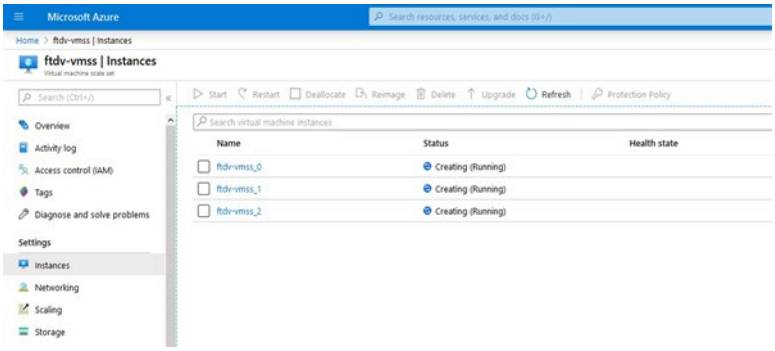
图 *17:* 逻辑应用运行状态



步骤 5 逻辑应用启动后，所有与部署相关的步骤都将完成。

步骤 6 在 VMSS 中验证是否正在创建 Firewall Threat Defense Virtual 实例。

图 *18: Threat Defense Virtual* 实例运行



在此示例中，由于在 ARM 模板部署中将 'minFtdCount' 设置为“3”并将“initDeploymentMode”设置为“批量”，因此启动了三个 Firewall Threat Defense Virtual 实例。

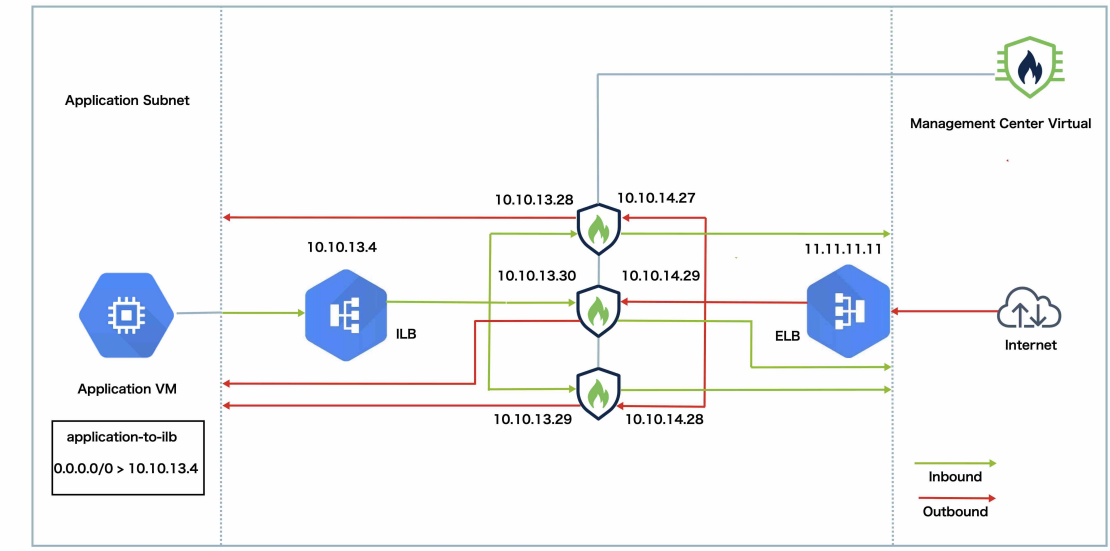
在 GCP 中部署集群

要在 GCP 中部署集群，您可以手动部署，或者使用实例模板来部署实例组。您可以将集群与本地 GCP 负载均衡器或非本地负载均衡器（例如思科云服务路由器）配合使用。

注释 出站流量需要使用接口 NAT 并被限制为 64K 连接。

GCP 集群 Autoscale 解决方案的拓扑示例

图 *19:* 拓扑示例



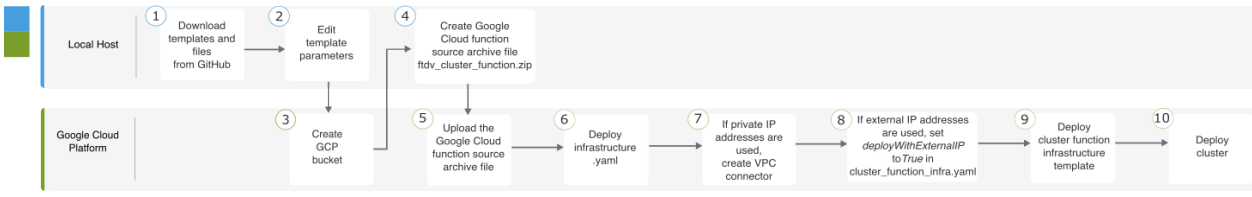
此拓扑描述入站和出站流量。

1. Threat Defense Virtual 集群位于内部和外部负载均衡器之间。Management Center Virtual 实例用于管理集群。
2. 来自互联网的入站流量会进入外部负载均衡器，然后该负载均衡器会将流量传输到 Threat Defense Virtual 集群。
3. 集群中的 Threat Defense Virtual 实例会检查流量，在检查后会将流量转发到应用虚拟机。
4. 来自应用虚拟机的出站流量将传输到内部负载均衡器。负载均衡器会将此流量转发到 Threat Defense Virtual 集群，由该集群将其发送到互联网。

在 GCP 中部署 Threat Defense Virtual 集群的端到端流程

基于模板的部署

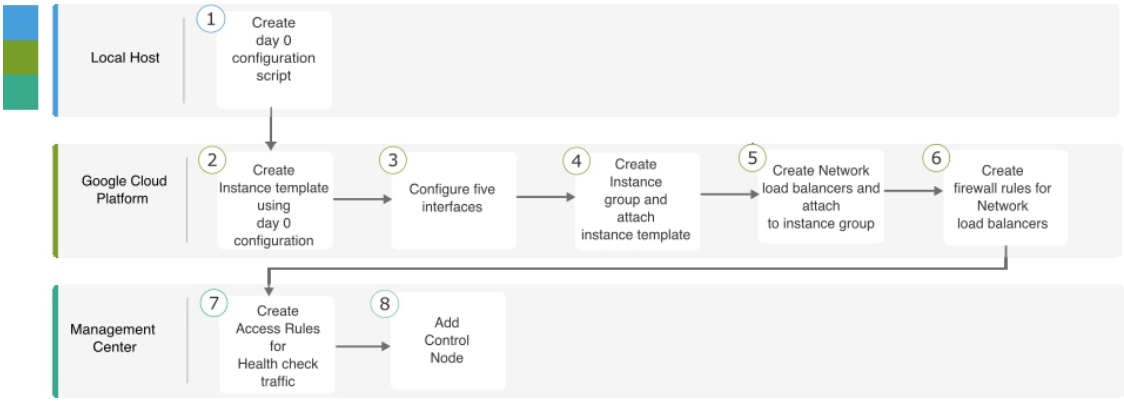
以下流程图说明了在 GCP 上基于模板部署 Threat Defense Virtual 集群的工作流程。



	工作空间	步骤
1	本地主机	从 GitHub 下载模板和文件。
2	本地主机	编辑模板参数。
3	Google Cloud Platform	创建 GCP 存储桶。
4	本地主机	创建 Google Cloud 函数源存档文件 *ftdv_cluster_function.zip*。
5	Google Cloud Platform	上传 Google 函数源存档文件。
6	Google Cloud Platform	部署 infrastructure.yaml。
7	Google Cloud Platform	如果使用私有 IP 地址，请创建 VPC 连接器。
8	Google Cloud Platform	如果使用外部 IP 地址，请在 *cluster_function_infra.yaml* 中将 *deployWithExternalIP* 设置为 *True*。
9	Google Cloud Platform	部署集群功能基础设施模板。
10	Google Cloud Platform	部署集群。

手动部署

以下流程图说明了在 GCP 上手动部署 Threat Defense Virtual 集群的工作流程。



	工作空间	步骤
1	本地主机	创建 Day 0 配置脚本。
2	Google Cloud Platform	使用 Day 0 配置创建实例模板。

	工作空间	步骤
3	Google Cloud Platform	配置接口。
4	Google Cloud Platform	创建实例组并附加实例模板。
5	Google Cloud Platform	创建 NLB 并附加到实例组。
6	Google Cloud Platform	创建 NLB 的防火墙规则。
7	管理中心	创建运行状况检查流量的访问规则。
8	管理中心	添加控制节点。

模板

以下提供的模板可在 GitHub 中获取。参数值是不言自明的，参数名称和值在模板中给出。

- 东西流量的集群部署模板 - *deploy_ngfw_cluster_yaml*
- 南北流量的集群部署模板 - deploy_ngfw_cluster.yaml

使用实例模板在 GCP 中部署实例组

使用实例模板在 GCP 中部署实例组。

开始之前

- 使用 Google Cloud Shell 进行部署。或者，您可以在任何 macOS/Linux/Windows 计算机上使用 Google SDK。
- 要允许集群自动向管理中心注册，您需要在管理中心创建一个具有管理权限的用户，该用户可以使用 REST API。请参阅*Cisco Secure Firewall Management Center* 管理指南。
- 在管理中心中添加与您在 *cluster_function_infra.yaml*中指定的策略名称匹配的访问策略。

过程

步骤 1 将模板从 GitHub 下载到本地文件夹。

步骤 2 使用所需的 *resourceNamePrefix* 参数（例如 ngfwvcls）和其他所需的用户输入来编辑 **infrastructure.yaml**、**cluster_function_infra.yaml** 和 **deploy_ngfw_cluster.yaml**。

从 Cisco Secure Firewall 版本 7.4.1 开始，您可以在没有诊断接口的情况下部署集群。要部署仅具有外部、内部、管理和 CCL 接口的集群，请在 **Infrastructure.yaml** 和 **deploy_ngfw_cluster.yaml** 文件中将 *withDiagnostic* 变量设置为 **False** 。

请注意，GitHub 的 **east-west** 和 **north-south** 文件夹中都有一个 **deploy_ngfw_cluster.yaml** 文件。根据流量要求下载相应的模板。

步骤 3 使用 Google Cloud Shell 创建存储桶，以上传 Google 云函数源存档文件 *ftdv_cluster_function.zip*。

gsutil mb --pap enforced gs://*resourceNamePrefix***-ftdv-cluster-bucket/**

确保此处的 *resourceNamePrefix* 变量与您在 **cluster_function_infra.yaml**中指定的 *resourceNamePrefix* 变量匹配。

步骤 4 为集群基础设施创建一个存档文件。

示例：

```
zip -j ftdv_cluster_function.zip ./cluster-function/*
```

步骤 5 上传您之前创建的 Google 源存档。

gsutil cp ftdv_cluster_function.zip gs://*resourceNamePrefix***-ftdv-cluster-bucket/**

步骤 6 部署集群的基础设施。

gcloud deployment-manager deployments create *cluster_name* **--config infrastructure.yaml**

步骤 7 如果您使用的是专用 IP 地址，请执行以下步骤：

a) 使用 Threat Defense Virtual 管理 VPC 启动并设置 Management Center Virtual。

b) 创建 VPC 连接器，以将 Google Cloud 功能与 Threat Defense Virtual 管理 VPC 连接。

gcloud compute networks vpc-access connectors create *vpc-connector-name* **--region us-central1 --subnet** *resourceNamePrefix***-ftdv-mgmt-subnet28**

步骤 8 如果管理中心相对于 Threat Defense Virtual 是远程，并且 Threat Defense Virtual 需要外部 IP 地址，请确保在 **cluster_function_infra.yaml** 中将 **deployWithExternalIP** 设置为 **True** 。

步骤 9 部署集群功能基础设施。

gcloud deployment-manager deployments create *cluster_name* **--config cluster_function_infra.yaml**

步骤 10 部署集群。

1. 对于北-南拓扑部署：

   gcloud deployment-manager deployments create *cluster_name* **--config north-south/deploy_ngfw_cluster.yaml**

2. 对于东-西拓扑部署：

   gcloud deployment-manager deployments create *cluster_name* **--config east-west/deploy_ngfw_cluster.yaml**

在 GCP 中手动部署集群

要手动部署集群，请准备 day0 配置，部署每个节点，然后将控制节点添加到 防火墙管理中心。

为 GCP 创建 Day0 配置

您可以使用固定配置或自定义配置。

使用 GCP 的固定配置来创建 Day0 配置

固定配置将自动生成集群引导程序配置。

```
{
    "AdminPassword": "password",
    "Hostname": "hostname",
    "FirewallMode": "Routed",
    "ManageLocally": "No",
                "Diagnostic": "OFF",       //Optional user input from version 7.4.1 - use
to deploy cluster without Diagnostic interface
    "Cluster": {
        "CclSubnetRange": "ip_address_start ip_address_end",
        "ClusterGroupName": "cluster_name"
    }
}
```

例如：

```
{
    "AdminPassword": "DeanW1nche$ter",
    "Hostname": "ciscoftdv",
    "FirewallMode": "Routed",
    "ManageLocally": "No",
    "Cluster": {
        "CclSubnetRange": "10.10.55.2 10.10.55.253",     //mandatory user input
        "ClusterGroupName": "ftdv-cluster"               //mandatory user input
    }
}
```

注释 如果要复制并粘贴上面给出的配置，请确保从配置中删除 **//mandatory user input** 。

请注意，对于 **CclSubnetRange** 变量，不能使用子网中的前两个 IP 地址和后两个 IP 地址。有关详细信息，请参阅 IPv4 子网中的保留 IP 地址 。确保您至少有 16 个可用于集群的 IP 地址。下面给出了开始和结束 IP 地址的一些示例。

注释 所有集群基础设施子网都必须使用 /27 CIDR。

表 *5:* 开始和结束 *IP* 地址示例

CIDR	起始 IP 地址	结束 IP 地址
10.1.1.0/27	10.1.1.2	10.1.1.29
10.1.1.32/27	10.1.1.34	10.1.1.61
10.1.1.64/27	10.1.1.66	10.1.1.93
10.1.1.96/27	10.1.1.98	10.1.1.125
10.1.1.128/27	10.1.1.130	10.1.1.157
10.1.1.160/27	10.1.1.162	10.1.1.189
10.1.1.192/27	10.1.1.194	10.1.1.221
10.1.1.224/27	10.1.1.226	10.1.1.253

使用 GCP 的自定义配置来创建 Day0 配置

您可以使用命令来输入整个集群引导程序配置。

```
{
    "AdminPassword": "password",
    "Hostname": "hostname",
    "FirewallMode": "Routed",
    "ManageLocally": "No",
    "run_config": [comma_separated_threat_defense_configuration]
    }
```

以下是为集群控制链路创建包含管理接口、内部接口和外部接口的配置的示例。请注意，每个节点需要设置唯一的粗体值。

```
{
 "AdminPassword": "W1nch3sterBr0s",
 "Hostname": "ftdv1",
 "FirewallMode": "Routed",
 "ManageLocally": "No",
 "run_config": [
  "cluster interface-mode individual force",
  "interface Management0/0",
  "management-only",
  "nameif management",
  "ip address dhcp",
  "interface GigabitEthernet0/0",
  "no shutdown",
  "nameif outside",
  "ip address dhcp",
  "interface GigabitEthernet0/1",
  "no shutdown",
  "nameif inside",
  "ip address dhcp",
  "interface GigabitEthernet0/2",
  "nve-only cluster",
  "nameif ccl_link",
  "ip address dhcp",
  "no shutdown",
  "interface vni1",
  "description Clustering Interface",
```

```
  "segment-id 1",
  "vtep-nve 1",
  "object network ccl#link",
  "range 10.1.90.2 10.1.90.17",
  "object-group network cluster#group",
  "network-object object ccl#link",
  "nve 1",
  "encapsulation vxlan",
  "source-interface ccl_link",
  "peer-group cluster#group",
  "cluster group ftdv-cluster",
  "local-unit 1",
  "cluster-interface vni1 ip 10.1.1.1 255.255.255.0",
  "priority 1",
  "enable",
  "mtu outside 1400",
  "mtu inside 1400"
 ]
}
```

注释 对于集群控制链路网络对象，仅指定所需数量的地址（最多16个）。较大的范围可能会影响性能。

手动部署集群节点

部署集群节点，以便它们形成集群。对于GCP上的集群，您不能使用4 vCPU机器类型。4 vCPU机器类型仅支持4个接口，但需要5个接口。使用支持五个接口的机器类型，例如c2-standard-8。

过程

步骤 1 使用day 0配置（在**元数据 > 启动脚本**部分中）创建具有5个接口的实例模板：外部、内部、管理、诊断和集群控制链路。

请参阅Cisco Secure Firewall Threat Defense Virtual 入门指南。

步骤 2 创建实例组，然后附加实例模板。

步骤 3 创建 GCP 网络负载均衡器（内部和外部），然后附加实例组。

步骤 4 对于GCP网络负载均衡器，允许在管理中心上的安全策略中进行运行状况检查。请参阅允许对GCP网络负载均衡器进行运行状况检查，第 85 页。

步骤 5 将控制节点添加到管理中心。请参阅将集群添加到管理中心（手动部署），第 100 页。

允许对 GCP 网络负载均衡器进行运行状况检查

Google Cloud 可提供运行状况检查，以确定后端是否对流量做出响应。

请参阅https://cloud.google.com/load-balancing/docs/health-checks，以便为网络负载均衡器创建防火墙规则。然后，在防火墙管理中心中创建访问规则以允许运行状况检查流量。有关所需的网络范围，请参阅https://cloud.google.com/load-balancing/docs/health-check-concepts。请参阅访问控制规则。

您还需要配置动态手动NAT规则，以便将运行状况检查流量重定向到位于169.254.169.254的Google元数据服务器。请参阅配置动态手动 NAT。

您可以设置跨所有接口进行GCP运行状况检查的路由，这些接口用于配置其运行状况探测。如果用于 GCP 运行状况检查的路由尚不可用，则可以通过在接口上创建具有更高指标的路由来实现此目的。

北-南 NAT 规则示例配置

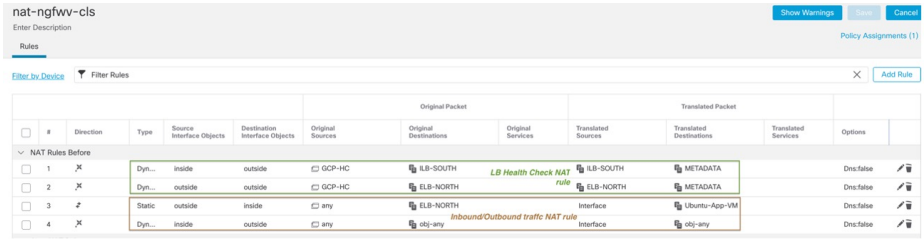
```
nat (inside,outside) source dynamic GCP-HC ILB-SOUTH destination static ILB-SOUTH METADATA
nat (outside,outside) source dynamic GCP-HC ELB-NORTH destination static ELB-NORTH METADATA

nat (outside,inside) source static any interface destination static ELB-NORTH Ubuntu-App-VM
nat (inside,outside) source dynamic any interface destination static obj-any obj-any

object network Metadata
 host 169.254.169.254

object network ILB-SOUTH
host <ILB_IP>
object network ELB-NORTH
host <ELB_IP>

object-group network GCP-HC
 network-object 35.191.0.0 255.255.0.0
 network-object 130.211.0.0 255.255.252.0
 network-object 209.85.204.0 255.255.252.0
 network-object 209.85.152.0 255.255.252.0
```



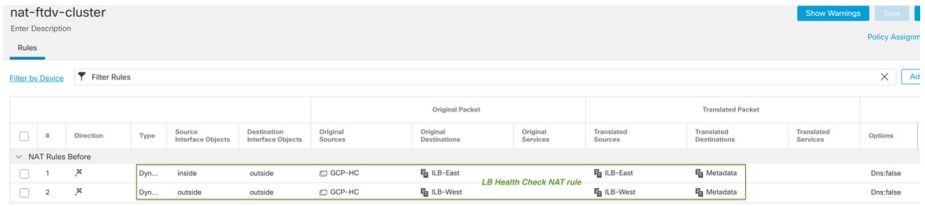
东-西 NAT 规则示例配置

```
nat (inside,outside) source dynamic GCP-HC ILB-East destination static ILB-East Metadata
nat (outside,outside) source dynamic GCP-HC ILB-West destination static ILB-West Metadata

object network Metadata
 host 169.254.169.254

object network ILB-East
host <ILB_East_IP>
object network ILB-West
host <ILB_West_IP>

object-group network GCP-HC
 network-object 35.191.0.0 255.255.0.0
 network-object 130.211.0.0 255.255.252.0
 network-object 209.85.204.0 255.255.252.0
 network-object 209.85.152.0 255.255.252.0
```



南北和东西流量路由配置示例

```
route outside 0.0.0.0 0.0.0.0 <Outside_Gateway> 1
route inside 35.191.0.0 255.255.0.0 <Inside_Gateway> 1
route inside 130.211.0.0 255.255.252.0 <Inside_Gateway> 1
route inside 209.85.152.0 255.255.252.0 <Inside_Gateway> 1
route inside 209.85.204.0 255.255.252.0 <Inside_Gateway> 1
```

如果没有默认路由，则可使用策略型路由来路由流量，以进行运行状况检查。

注释 将 NAT > 已转换目标端口设置为 80。

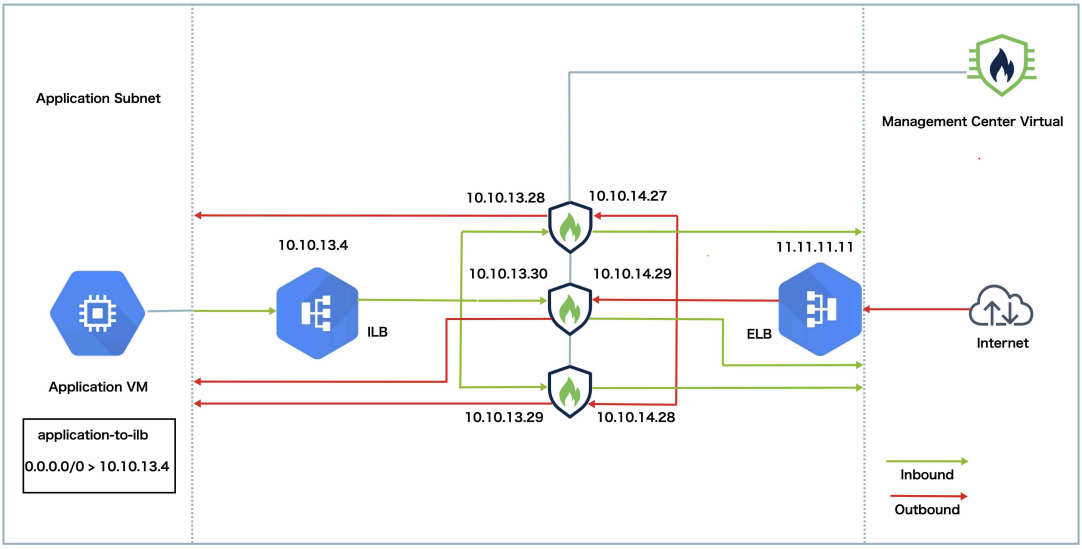
GCP 中的 Threat Defense Virtual 集群 Autoscale 解决方案

从版本 10.0.0 开始，通过动态自动扩展功能增强了 Google 云平台 (GCP) 中的 Threat Defense Virtual 集群解决方案。自动扩展解决方案基于 CPU 利用率指标，有助于实现最佳资源使用。它使用基于 Terraform 的模板进行部署。

您可以根据自己的要求选择扩展选项：动态集群或固定节点集群。您还可以定义CPU阈值，超过该阈值将启动扩展。

GCP 集群 Autoscale 解决方案的拓扑示例

图 *20:* 拓扑示例



此拓扑描述入站和出站流量。

1. Threat Defense Virtual 集群位于内部和外部负载均衡器之间。Management Center Virtual 实例用于管理集群。
2. 来自互联网的入站流量会进入外部负载均衡器，然后该负载均衡器会将流量传输到 Threat Defense Virtual 集群。
3. 集群中的 Threat Defense Virtual 实例会检查流量，在检查后会将流量转发到应用虚拟机。
4. 来自应用虚拟机的出站流量将传输到内部负载均衡器。负载均衡器会将此流量转发到 Threat Defense Virtual 集群，由该集群将其发送到互联网。

要求和前提条件

本部分列出了 GCP 上的 Threat Defense Virtual 集群自动扩展解决方案的要求和支持的配置。

型号要求

- 支持的 Threat Defense Virtual 型号：FTDv20、FTDv30、FTDv50 和 FTDv100。
- 需要有效的 Google 云平台 (GCP) 账户。
- Google Cloud SDK 必须安装在本地，或者您应该有权访问 GCP Cloud Shell。
- 需要思科智能许可账户才能许可管理中心。

Firepower 管理中心系统要求

- 确保已配置访问控制策略。
- 确保已定义数据接口的安全区域。
- 需要具有管理角色的用户才能自动注册。
- 确保 NAT 规则配置为响应负载均衡器的运行状况检查。

许可

- 控制节点的许可证适用于集群中的所有数据节点，无论其在启动过程中的初始性能级别配置如何。
- 集群组建后，不允许更改任何单个 Threat Defense Virtual 的性能级别。
- 默认情况下，每台设备随附一个 100 kbps 评估许可证。
- 许可证注销
  - 重新启动前：设备保留现有吞吐量。
  - 重启后：吞吐量恢复为默认的 100 kbps。
- 仅支持 BYOL（自带许可证）许可证类型。
- 不支持 PAYG（即用即付）许可证类型。

支持的配置

- 集群大小：1-16 个节点。
- 流量拓扑：南北和东西向。
- 部署模式：使用 Terraform 模板部署。

模板

GitHub 上提供了以下模板：

- infrastructure/main.tf – 用于基础设施部署模板。
- cluster_deployment/main.tf – 用于集群部署模板。

在 GCP 上部署带有 Autoscale 的 Threat Defense Virtual 集群解决方案

部署过程分为两个步骤：

1. 基础设施部署（可选）- 部署所需的网络基础设施。
2. 集群部署 — 部署 Threat Defense Virtual 集群。

注释 如果选择使用自己的基础设施来部署 Threat Defense Virtual，则可以跳过基础设施部署步骤。但是，请务必确保提供使解决方案正常运行所需的所有资源。

基础设施部署参数

以下参数用于基础设施部署：

表 *6:* 用于基础设施部署的模板参数列表 *(infrastructure_params.tfvars)*

参数	说明	示例
project_id	GCP 项目 ID	test-project-12345
resource_name_prefix	字符串（仅限小写字母）。	demoftdv
region	要部署的 GCP 区域	us- Central1
mgmt_ip_cidr_range	子网 CIDR	10.112.0.0/27
vpc_connector_ip_cidr_range	仅管理 VPC 连接器 CIDR /28 子网	10.112.50.0/28
with_diagnostic	是否启用诊断接口。	true 或 false（false 是仅从版本 7.4.1 开始支持。）
diag_ip_cidr_range	诊断子网 CIDR	10.112.19.0/27
inside_ip_cidr_range	内部子网	10.112.1.0/27
outside_ip_cidr_range	外部子网 CIDR	10.112.2.0/27
ccl_ip_cidr_range	CCL 子网 CIDR（建议使用 /27 子网）	10.112.100.0/27

在 GCP 上使用 Terraform 部署基础设施

GCP 基础设施管理器可作为堆栈促进 Terraform 部署。从此界面中，可以管理资源并执行清理。

过程

步骤 1 导航到 GCP 控制台 并使用您的凭证登录。

步骤 2 打开 Cloud Shell 或本地终端。

如果您使用的是本地终端，请确保已在系统上配置 GCP CLI。

步骤 3 创建新目录。

示例：

使用命令 **mkdir infra** 在 Cloud Shell 或本地终端中创建名为 infra 的 目录。

步骤 4 导航到新创建的目录。

示例：

使用命令 **cd infra** 切换到新目录。

步骤 5 从 Cisco GitHub 存储库复制或下载 infrastructure_params. tfvars 文件，并将其保存到新的 infra 文件夹。

步骤 6 打开 infrastructure_params. tfvars 文件，并根据需要更新所有占位符值。请参阅 基础设施部署参数，第 90 页。

步骤 7 更新占位符值后，使用以下命令启动部署。

```
gcloud infra-manager deployments \
apply
"projects/<project_id>/locations/<region>/deployments
/<deployment_name>" \
--location="<region>" \
--git-source-repo="<repo name>" \
--git-source-directory="infrastructure” \
--git-source-ref="<branch name>" \
--serviceaccount="
projects/<project_id>/serviceAccounts/<servi
ce_account_name>" \
--artifacts-gcs-bucket="gs://<bucket_name>/artifacts"
\
--inputs-file="/path/to/your/infra_params.tfvars"
```

表 7: 参数说明

参数	说明
deployment_name	将显示在 GCP 基础设施管理器中的 Terraform 部署堆栈的名称。
location	将应用部署的位置或区域。
git-source-repo	包含源代码的 Git 存储库的名称（Cisco GitHub 链接）。
git-source-directory	Git 存储库中基础设施代码所在的目录。
git-source-ref	Git 存储库中用于部署的分支名称。
service-account	服务账户的名称。
artifacts-gcs-bucket	用于存储与部署相关的构件的 Google Cloud Storage 存储桶（可选）。
inputs-file	基础设施配置的输入参数的文件路径。

注释
如果不使用该模板来部署基础设施，则必须提供以下资源，以便正确部署解决方案并确保解决方案正常运行。

- 管理 VPC 的名称。
  - 管理子网
  - VPC 连接器的管理子网
  - 管理防火墙规则的名称。
- 内部 VPC
  - 内部子网
  - 防火墙规则名称
- 外部 VPC
  - 外部子网
  - 外部防火墙规则的名称
  - NAT GW
- CCL VPC
  - CCL 子网
  - 防火墙规则名称
- 诊断 VPC（可选）
  - 诊断子网
  - 诊断防火墙规则名称
- 具有管理子网的 VPC 连接器

集群部署参数：

以下输入参数用于部署集群。

表 *8:* 适用于集群部署的模板参数列表

参数	说明	示例
常规配置		
type_of_deployment	部署类型 (north_south 或 east_west)	north_south
项目信息		

参数	说明	示例
project_id	GCP 项目 ID	test-project-12345
region	部署区域	us-east1
zone1	部署区域	a
zone2	部署区域	b
zone3	部署区域	c
resource_name_prefix	用于命名资源的前缀	democluster
serviceAccountMailId	服务账户电子邮件	service-account-mail@example-project.iam.gserviceaccount.com
VPC 和子网配置		
mgmt_vpc_name	管理 VPC 名称	<resource-name>-ftdv-mgmt-vpc
mgmt_subnet_name	管理子网名称。	<resource-name>-ftdv-mgmt-子网
inside_vpc_name	内部 VPC 名称	<resource-name>-ftdv-inside-vpc
inside_subnet_name	内部子网	<resource-name>-ftdv-inside-subnet
outside_vpc_name	外部 VPC 名称	<resource-name>-ftdv-outside-vpc
OutsideSubnetNames	外部子网名称	<resource-name>-ftdv-outside-子网
diag_vpc_name	VPC 名称 “诊断”	<resource-name>-ftdv-diag-vpc
diag_subnet_name	子网名称“诊断”	<resource-name>-ftdv-diag-subnet
ccl_vpc_name	CCL VPC 名称	<resource-name>-ftdv-ccl-vpc
ccl_subnet_name	输入 CCL 子网名称	<resource-name>-ftdv-ccl-subnet
防火墙规则		
diag_firewall_rule_name	用于诊断的防火墙规则	<resource-name>-ftdv-diag-firewall-rule
ccl_firewall_rule_name	用于 CCL 的防火墙规则	<resource-name>-ftdv-ccl-firewall-rule
mgmt_firewall_rule_name	用于管理的防火墙规则	<resource-name>-ftdv-mgmt-firewall-rule
inside_firewall_rule_name	内部网络的防火墙规则	<resource-name>-ftdv-inside-firewall-rule
outside_firewall_rule_name	外部网络的防火墙规则	<resource-name>-ftdv-outside-firewall-rule
inside_hc_firewall_rule_name	内部网络的防火墙规则	<resource-name>-ftdv-inside-hc-firewall-rule
outside_hc_firewall_rule_name	外部网络的防火墙规则	<resource-name>-ftdv-outside-hc-firewall-rule
实例详细信息		
machine_type	GCP 计算机类型支持	n1-standard-8

参数	说明	示例
source_image_url	Threat Defense Virtual 的源映像位置	项目/cisco-public/global/images/cisco-ftdv-10-0-0
public_key	用于 SSH 访问的公钥	ssh-rsa AAAAB3NzaC1yc2EAAADAQAAAAAAQC4v
自动扩展详细信息		
auto_scaling	启用自动扩展	true/false
cpu_utilization_target	自动扩展的目标 CPU 使用率 [0.0-1.0]	0.60
min_ftd_count	Threat Defense Virtual 的最小实例数	0
max_ftd_count	Threat Defense Virtual 的最大实例数	2
Threat Defense Virtual 特定配置		
ftd_password_secret_name	密钥管理器中用于设备将使用此密码的新管理员密码的 Threat Defense Virtual 密钥的名称，设备将在首次登录后使用此密码。	ftd-password-secret
hostname	Threat Defense Virtual 的主机名	cisco-ngfwv
ccl_subnet_range	CCL 的子网范围，空格分隔	10.112.100.2 10.112.100.30
cluster_grp_name	Threat Defense Virtual 的集群组名称	ftdv-cluster
with_diagnostic	是否启用诊断	true/false
Assign_public_ip_to_mgmt	是否将公共 IP 分配给管理接口	true/false
ftd_reg_ via_public_ip	是否向公共 IP 注册 Threat Defense Virtual	true/false
管理中心信息和 Threat Defense Virtual 配置		
reg_id	管理中心注册 ID	cisco
nat_id	管理中心的 NAT ID	cisco

参数	说明	示例
policy_id	在管理中心创建的初始策略 ID	ftdv-ini-pol
fmc_ip	源 Firewall Management Center 的 IP 地址	10.112.0.2 / 34.113.15.29
fmc_password_secret_name	密钥管理器中新管理员密码的 FMC 密钥名称，设备将在首次登录后使用此密码。	fmc-password-secret
fmc_username	管理中心登录用户名	restapi
license_caps	许可证功能	BASE, MALWARE, URLFilter, THREAT
performance_tier	Threat Defense Virtual 的性能级别	FTDv20、FTDv30
vpc_connector_name	VPC 连接器的名称	<resource-name>-connector
检查负载均衡器配置		
ilb_frontend_protocol	前端协议 (TCP/UDP)	TCP
ilb_backend_protocol	后端协议:	TCP
ilb_health_check_port	ILB运行状况检查平衡器端口，管理中心需要 NAT	8989
ilb_timeout_sec	负载均衡器超时（秒）	5
ilb_draining_timeout_sec	排空连接超时（秒）	60
ilb_check_interval_sec	ILB运行状况检查的间隔（秒）	10
ilb_unhealthy_threshold	标记为不正常之前失败的运行状况检查数	1
仅在north_south 部署情况下外部负载均衡器特定配置		
elb_frontend_protocol	外部负载均衡器的前端协议名称 (TCP/UDP)	TCP
elb_backend_protocol	外部负载均衡器的后端协议名称 (TCP/UDP/未指定)	TCP
elb_front_end_ports	ELB前端（侦听程序）端口列表	all 或 [22, 80, 443]

参数	说明	示例
elb_health_check_port	ELB运行状况检查端口，管理中心需要 NAT	87878
elb_timeout_sec	负载均衡器超时（秒）	5
elb_unhealthy_threshold	标记为不正常之前失败的运行状况检查数	2
elb_check_interval_sec	ELB运行状况检查的间隔（秒）。	10
elb_draining_timeout_sec	排空连接超时（秒）	60

使用 Terraform on GCP 部署集群

GCP 基础设施管理器可作为堆栈促进 Terraform 部署。从此界面中，可以管理资源并执行清理。

过程

步骤 1 导航到 GCP 控制台 并使用您的凭证登录。

步骤 2 打开 Cloud Shell 或本地终端。

如果您使用的是本地终端，请确保已在系统上配置 GCP CLI。

步骤 3 创建新目录。

示例：

使用命令 **mkdir cluster** 在 Cloud Shell 或本地终端中创建名为 cluster 的目录。

步骤 4 导航到新创建的目录。

示例：

使用命令 **cd cluster** 切换到新目录。

步骤 5 从思科 GitHub 存储库复制或下载 cluster_params.tfvars 文件，并将其保存到新的 集群 文件夹。

步骤 6 打开 cluster_params.tfvars 文件并根据需要更新所有占位符值。请参阅 集群部署参数：，第 92 页。

步骤 7 更新占位符值后，使用以下命令启动部署。

```
gcloud infra-manager deployments \
apply "projects/<project_id>/locations/<region>/deployments/<deployment_name>" \
--location="<region>" \
--git-source-repo="<repo name>" \
--git-source-directory="cluster_deployment" \
--git-source-ref="<branch name>" \
--service-account="projects/<project_id>/serviceAccounts/<service_account_name>" \
--artifacts-gcs-bucket="gs://<bucket_name>/artifacts" \
--inputs-file="/path/to/cluster_params.tfvars"
```

表 *9:* 参数说明

参数	说明
deployment_name	将显示在 GCP 基础设施管理器中的 Terraform 部署堆栈的名称。
location	将应用部署的位置或区域。
git-source-repo	包含源代码的 Git 存储库的名称（Cisco GitHub 链接）。
git-source-directory	Git 存储库中基础设施代码所在的目录。
git-source-ref	Git 存储库中用于部署的分支名称。
service-account	服务账户的名称。
artifacts-gcs-bucket	用于存储与部署相关的构件的 Google Cloud Storage 存储桶，例如 Terraform 状态文件。
inputs-file	集群部署输入参数的文件路径。

集群部署后的部署配置

要在 VPC 内创建路由以通过 Google Cloud Shell 上的内部负载均衡器转发所需流量，请执行以下步骤：

```
gcloud compute routes create <ilb-route-name>
--network=<inside-vpc-name> --priority=1000 --destination-range=0.0.0.0/0
--next-hop-ilb=<ilb-forwarding-rule-name> --next-hop-ilb-region=<region>
```

注释 您也可以从 GCP UI 中创建路由。要从 GCP UI 创建路由，请执行以下步骤：

1. 在GCP UI中，导航至路由 (Routes)、路由管理 (Route Management)、创建路由 (Create route)。
2. 填写 Create a route 对话框。
   1. **名称 (Name)**：指定路由名称。
   2. **网络**：选择<inside-vpc-name>请参阅
   3. 选择 **静态路由**。
   4. **目标 IPv4 范围 (Destination IPv4 range)**：输入 **0.0.0.0/0**。
   5. **优先级**：设置为 **1000**。
   6. **下一跳**：选择 **指定内部直通 网络负载均衡器的转发规则**。
   7. **转发规则名称**：选择<forwarding-rule-for-ilb>请参阅
3. 点击**创建 (Create)** 以创建角色。

在 GCP 中手动部署集群

为 GCP 创建 Day0 配置

要手动部署集群，请准备 Day-0 配置并部署每个节点。

```
{
    "AdminPassword": "password",
    "Hostname": "hostname",
    "FirewallMode": "Routed",
    "ManageLocally": "No",
    "Diagnostic": "OFF",       //Optional user input from version 7.4.1
    "Cluster": {
      "CclSubnetRange": "ip_address_start ip_address_end",
      "ClusterGroupName": "cluster_name"
    }
}
```

例如：

```
{
"AdminPassword": “C15co@!23",
"Hostname": "cisco-ftd",
"FirewallMode": "routed",
"Diagnostic": "OFF",
"ManageLocally": "No",
"Cluster": {
  "CclSubnetRange”: “10.10.65.2 10.10.65.29”,
  "ClusterGroupName": “gcp-cls-ftd"
}
}
```

允许对 GCP 网络负载均衡器进行运行状况检查

Google Cloud 可提供运行状况检查，以确定后端是否对流量做出响应。

请参阅https://cloud.google.com/load-balancing/docs/health-checks，以便为网络负载均衡器创建防火墙规则。然后，在防火墙管理中心中创建访问规则以允许运行状况检查流量。有关所需的网络范围，请参阅https://cloud.google.com/load-balancing/docs/health-check-concepts。请参阅访问控制规则。

您还需要配置动态手动 NAT 规则，以便将运行状况检查流量重定向到位于 169.254.169.254 的 Google 元数据服务器。请参阅配置动态手动 NAT。

您可以设置跨所有接口进行 GCP 运行状况检查的路由，这些接口用于配置其运行状况探测。如果用于 GCP 运行状况检查的路由尚不可用，则可以通过在接口上创建具有更高指标的路由来实现此目的。

北-南 NAT 规则示例配置

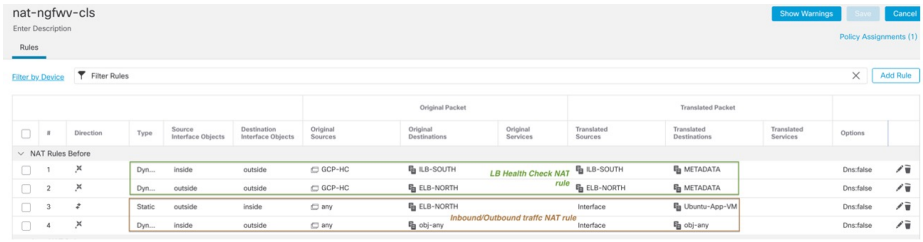
```
nat (inside,outside) source dynamic GCP-HC ILB-SOUTH destination static ILB-SOUTH METADATA
nat (outside,outside) source dynamic GCP-HC ELB-NORTH destination static ELB-NORTH METADATA

nat (outside,inside) source static any interface destination static ELB-NORTH Ubuntu-App-VM
nat (inside,outside) source dynamic any interface destination static obj-any obj-any

object network Metadata
 host 169.254.169.254

object network ILB-SOUTH
host <ILB_IP>
object network ELB-NORTH
host <ELB_IP>

object-group network GCP-HC
 network-object 35.191.0.0 255.255.0.0
 network-object 130.211.0.0 255.255.252.0
 network-object 209.85.204.0 255.255.252.0
 network-object 209.85.152.0 255.255.252.0
```



东-西 NAT 规则示例配置

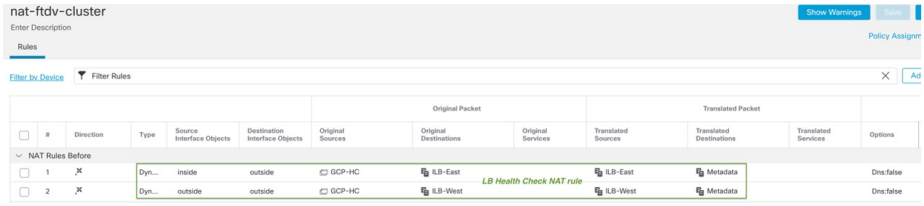
```
nat (inside,outside) source dynamic GCP-HC ILB-East destination static ILB-East Metadata
nat (outside,outside) source dynamic GCP-HC ILB-West destination static ILB-West Metadata

object network Metadata
 host 169.254.169.254

object network ILB-East
host <ILB_East_IP>
```

```
object network ILB-West
host <ILB_West_IP>

object-group network GCP-HC
 network-object 35.191.0.0 255.255.0.0
 network-object 130.211.0.0 255.255.252.0
 network-object 209.85.204.0 255.255.252.0
 network-object 209.85.152.0 255.255.252.0
```



南北和东西流量路由配置示例

```
route outside 0.0.0.0 0.0.0.0 <Outside_Gateway> 1
route inside 35.191.0.0 255.255.0.0 <Inside_Gateway> 1
route inside 130.211.0.0 255.255.252.0 <Inside_Gateway> 1
route inside 209.85.152.0 255.255.252.0 <Inside_Gateway> 1
route inside 209.85.204.0 255.255.252.0 <Inside_Gateway> 1
```

如果没有默认路由，则可使用策略型路由来路由流量，以进行运行状况检查。

注释 将 NAT > 已转换目标端口设置为 80。

通过 Autoscale 对 GCP 集群进行故障排除

问题：集群未组建

解决办法

- 检查 nve-only 集群接口的 IP 地址。确保您可以 ping 其他节点的仅 NVE 集群接口。
- 检查仅 NVE 集群接口的 IP 地址是对象组的一部分。
- 确保为 NVE（网络虚拟化边缘）接口配置了相应的对象组。
- 集群组中的集群接口具有正确的 VNI 接口。此 VNI 接口具有相应对象组的 NVE。
- 每个节点都有自己的集群接口 IP 地址。确保节点可以相互执行 ping 操作，以验证连接性。

将集群添加到管理中心（手动部署）

如果您手动部署了集群，请使用此程序将集群添加到防火墙管理中心。如果您使用模板，则集群会自动注册到 防火墙管理中心。

将集群设备之一作为新设备添加到 防火墙管理中心；防火墙管理中心 会自动检测所有其他集群成员。

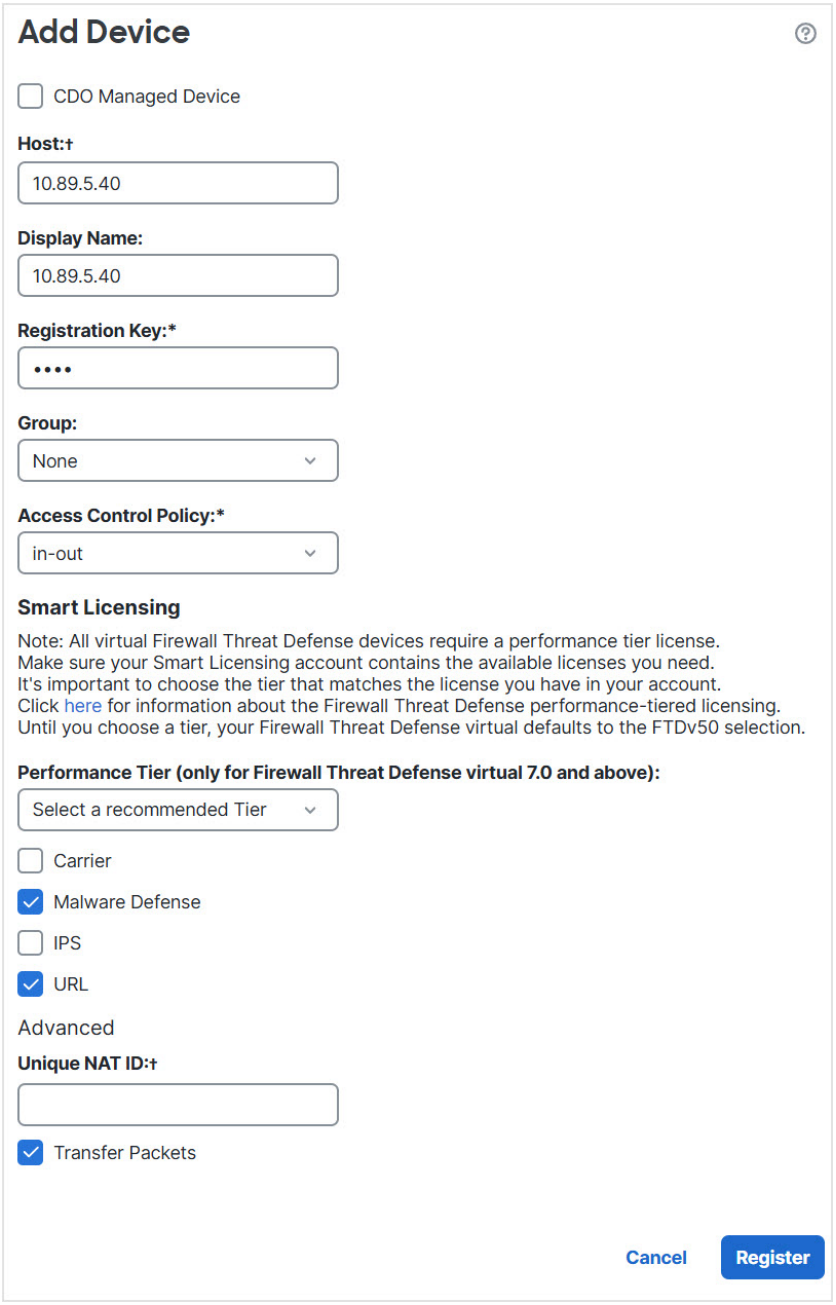
开始之前

- 所有集群设备必须位于成功建立的集群中，才能将集群添加到 防火墙管理中心。还应检查哪个是控制单元。使用 Firewall Threat Defense **show cluster info** 命令。

过程

步骤 1 在 防火墙管理中心 中，选择 **设备** > **设备管理**，然后选择**添加** > **添加设备**以使用管理 IP 来添加控制设备。

图 *21:* 添加设备



a) 在 **主机** 字段中，输入控制单元的 IP 地址或主机名。

虽然您可以添加任何集群单元，但我们建议添加控制单元备以获得最佳性能。

如果在设备设置期间使用了 NAT ID，则可能不需要输入此字段。有关详细信息，请参阅NAT 环境。

b) 在 **显示名称** 字段中，输入要在 防火墙管理中心中显示的控制单元名称。

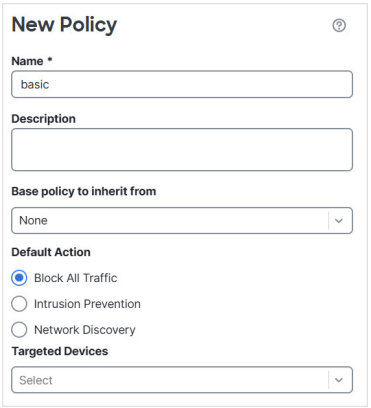
此显示名称不适用于集群；它仅适用于要添加的控制单元。您可以稍后更改其他集群成员的名称和集群显示名称。

c) 在**注册密钥 (Registration Key)** 字段中，输入在设备设置时所使用的同一注册密钥。注册密钥是一个一次性的共享密钥。

d) （可选） 将设备添加到设备 **组**。

e) 选择初始**访问控制策略**以在注册时部署到设备，或创建一个新策略。

如果创建新策略，则仅创建基本策略。您可以稍后根据需要自定义策略。



f) 选择要应用到设备的许可证。

g) 如果在设备安装过程中使用了 NAT ID，请展开**高级**部分，并在**唯一 NAT ID** 字段中输入相同的 NAT ID。

h) 选中**传输数据包**复选框以允许设备将数据包传输到 防火墙管理中心。

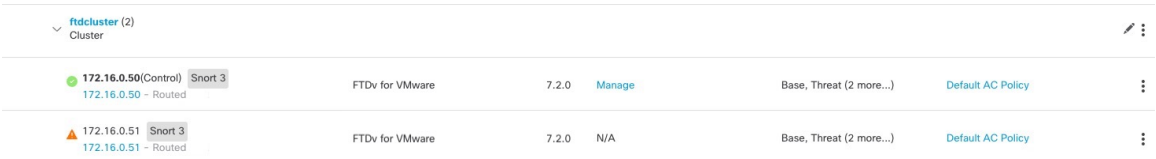
默认情况下，此选项已启用。如果在启用此选项时触发了 IPS 或 Snort 等事件，设备会将事件元数据信息和数据包数据发送到 防火墙管理中心进行检测。如果禁用此选项，则仅发送事件信息到 防火墙管理中心，不发送数据包数据。

i) 点击**注册 (Register)**。

防火墙管理中心 会识别并注册控制单元，接着注册所有数据单元。如果控制单元未注册成功，则不会添加集群。如果集群未运行或存在其他连接问题，则注册会失败。在这种情况下，我们建议尝试重新添加集群设备。

集群名称显示在 **设备** > **设备管理** 页面上；展开集群可查看集群单元。

图 *22:* 集群管理

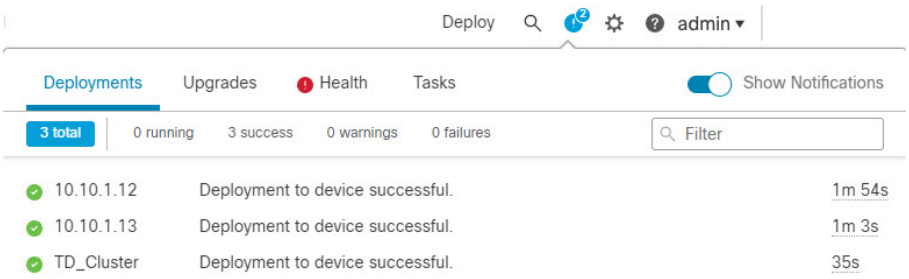


当前正在注册的设备会显示加载图标。

图 *23:* 节点注册

注释
在集群节点发现过程中，GCP 会优先选择具有公共 IP 地址的节点。要确保 Firewall Threat Defense Virtual 集群使用专用 IP 地址注册到 Management Center Virtual，您必须先在 Firewall Threat Defense Virtual 集群节点上禁用公有 IP 地址。这将允许 GCP 节点发现使用向 Management Center Virtual 注册节点的专用 IP 地址继续。

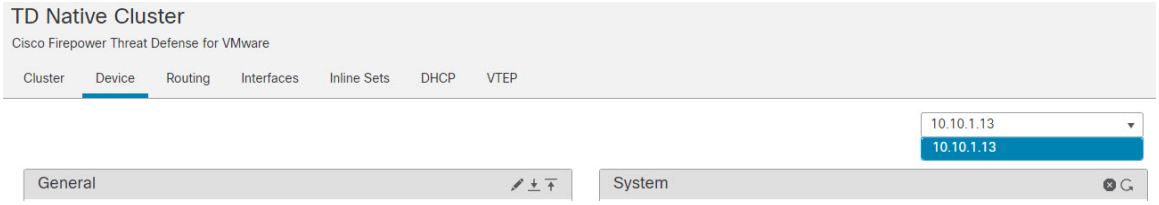
您可以通过点击 **通知** 图标并选择 **任务** 来监控集群设备的注册情况。防火墙管理中心 会在每个设备注册时更新“集群注册”任务。如有任何设备无法注册，请参阅调整集群节点，第 113 页。



步骤 2 通过点击集群的 **编辑** (✎)，配置设备特定设置。

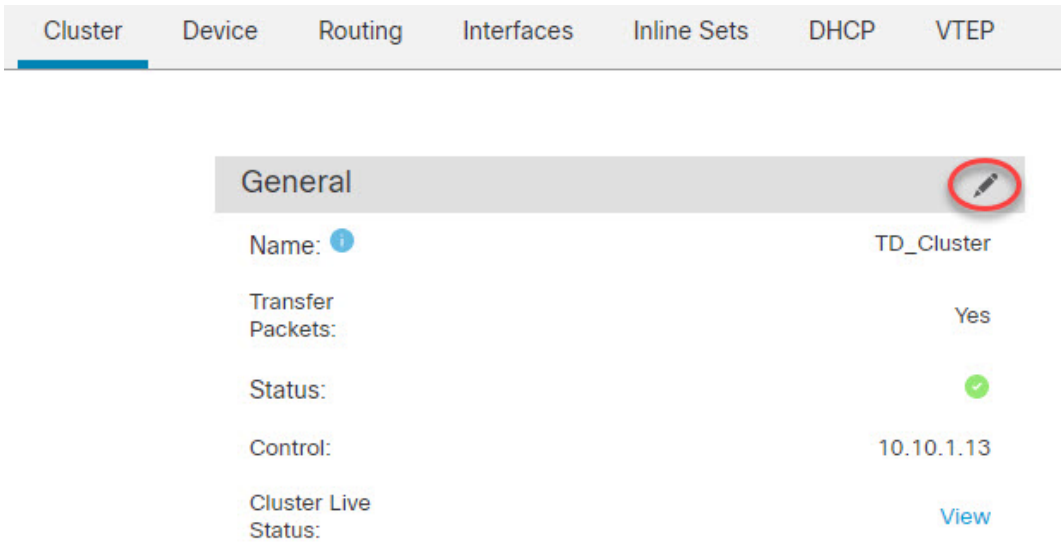
大多数配置可以应用于整个集群，而不适用于集群中的节点。例如，可以更改每个节点的显示名称，但只能配置整个集群的接口。

步骤 3 在 **设备** > **设备管理** 上选择**添加**、**集群**屏幕，您会看到**常规**、**许可证**、**系统**和**运行状态**设置。

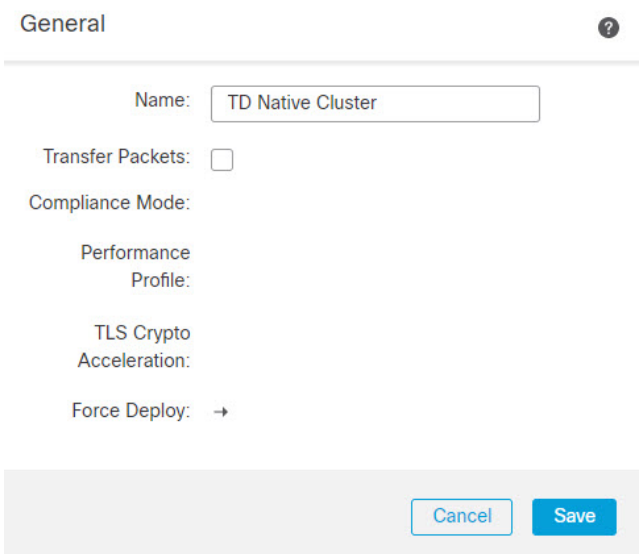


请参阅以下集群特定项：

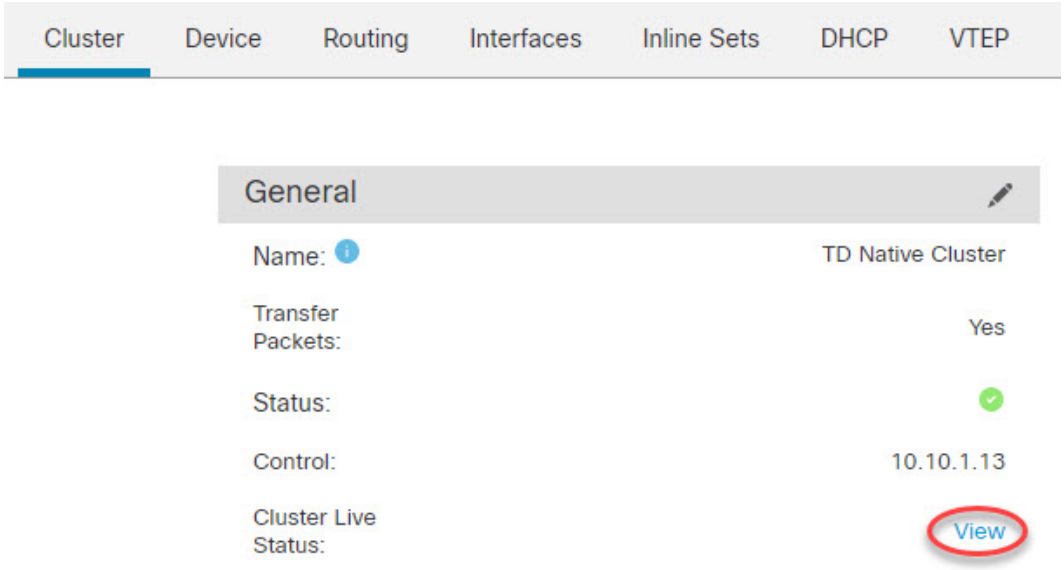
- **常规 (General)** > **名称 (Name)** - 通过点击 **编辑** (✎)更改集群显示名称。



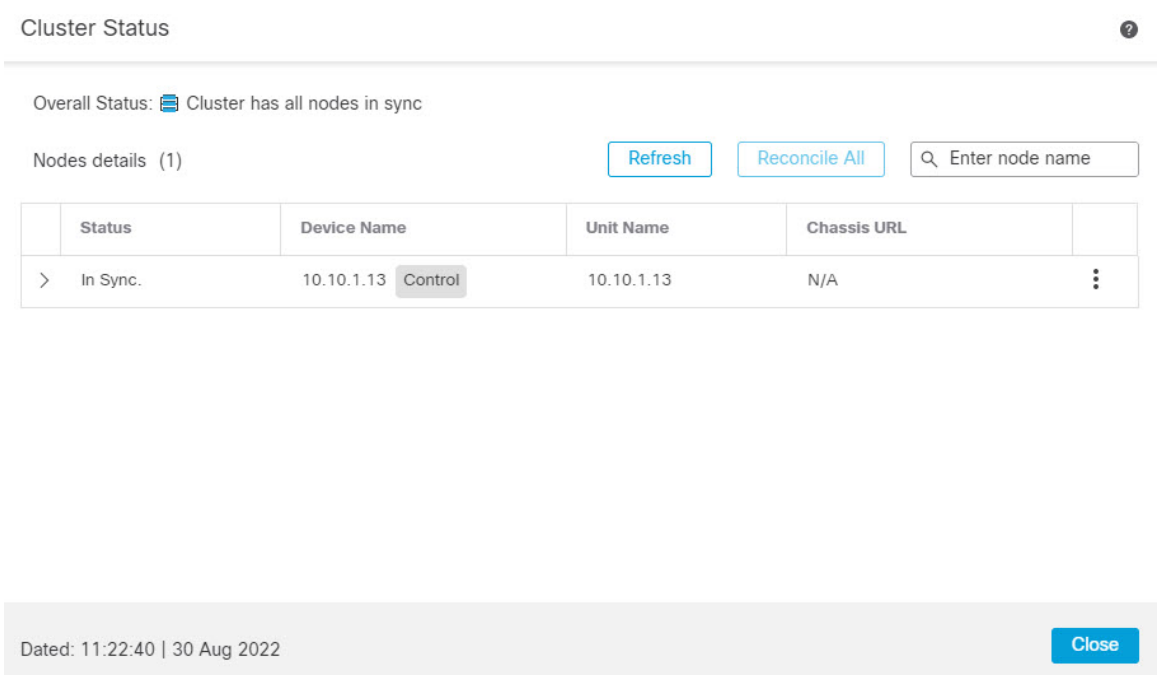
然后设置 **名称** 字段。



- **常规 (General) > 查看集群状态 (View cluster status)** - 点击 **查看 (View)** 链接来打开 **集群状态 (Cluster Status)** 对话框。

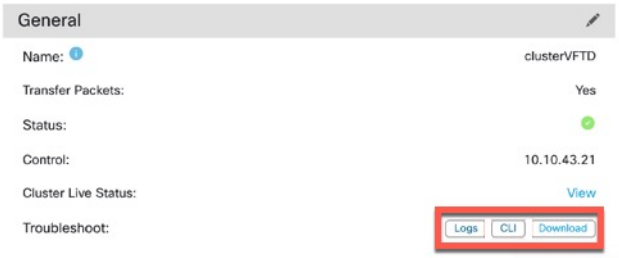


还可在**集群状态 (Cluster Status)** 对话框中点击**协调 (Reconcile)** 以重新注册数据单元。您还可以从节点 ping 通集群控制链路。请参阅在集群控制链路上执行 Ping，第 121 页。



- **常规 > 故障排除**- 可以生成和下载故障排除日志，还可以查看集群 CLI。请参阅对集群进行故障排除，第 121 页。

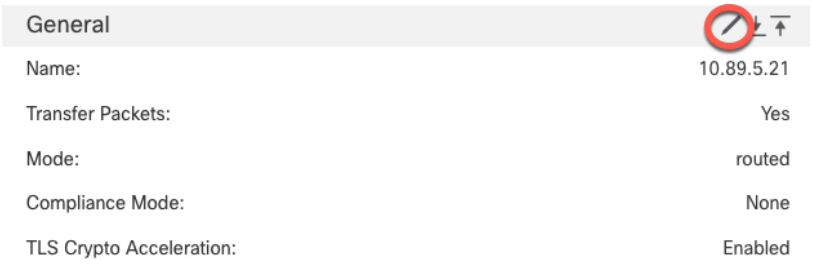
图 *24:* 故障排除



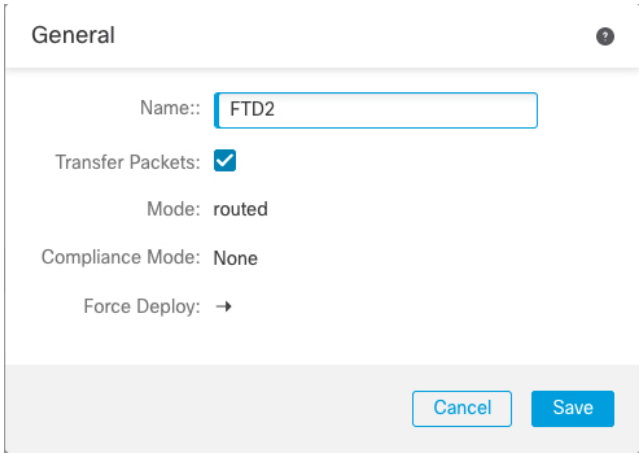
- **许可证** - 点击 **编辑** (✎) 可设置许可证授权。

步骤 4 在 **设备** > **设备管理** 上，然后点击**添加** > **设备**，您可以从右上角的下拉菜单中选择集群中的每个成员并配置以下设置。

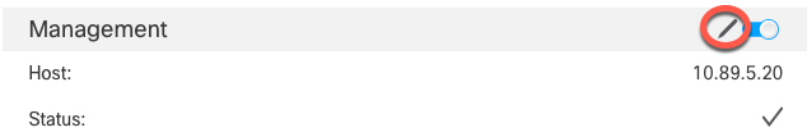
- **常规 (General)** > **名称 (Name)** - 通过点击 **编辑** (✎)更改集群成员显示名称。



然后设置 **名称** 字段。



- **管理** > **主机**-如果在设备配置中更改了管理 IP 地址，则必须在 防火墙管理中心 中匹配新的地址以便管理 IP 地址访问网络上的设备；编辑 **管理** 区域中的 **主机** 地址。



配置集群运行状况监控设置

集群 (Cluster) 页面的**集群运行状况监控设置 (Cluster Health Monitor Settings)** 部分会显示下表所述信息。

图 *25:* 集群运行状况监控设置

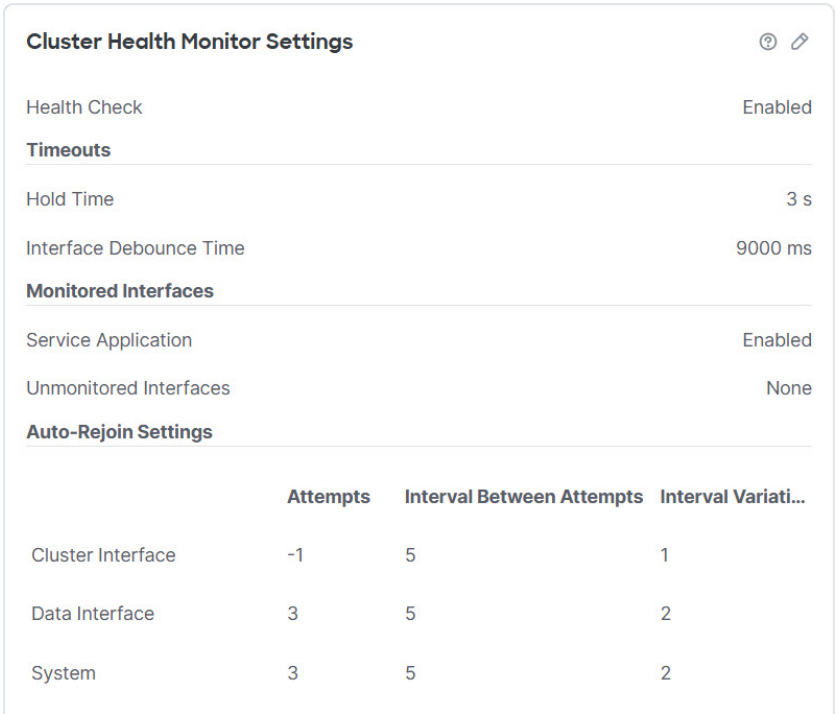


表 *10:* 集群运行状况监控设置部分表格字段

字段	说明
超时	
保持时间	0.3 到 45 秒之间；默认值为 3 秒。为了确定节点系统运行状况，集群节点会在集群控制链路上将 heartbeat 消息发送到其他节点。如果节点在保持期内未接收到来自对等节点的任何 heartbeat 消息，则对等节点被视为无响应或无法工作。

字段	说明
接口防退回时间	介于 300 和 9000 毫秒之间。默认值为 500 毫秒。接口防退回时间是节点将接口视为发生故障并将节点从集群中删除之前经过的时间。
受监控接口	接口运行状态检查将监控链路故障。如果特定逻辑接口的所有物理端口在特定节点上发生故障，但在其他节点上的同一逻辑接口下仍有活动端口，则会从集群中删除该节点。节点在多长时间后从集群中删除成员取决于接口的类型以及该节点是既定节点还是正在加入集群的设备。
服务应用	显示是否对 Snort 和磁盘已满进程进行监控。
不受监控的接口	显示不受监控的接口。
自动重新加入设置	
集群接口	显示集群控制链路故障的自动重新加入设置。
尝试次数	介于 1 和 65535 之间。默认值为 1（不受限制）。设置尝试重新加入的次数。
尝试之间的间隔	介于 2 和 60 之间。默认值为 5 分钟。定义两次重新加入尝试之间的间隔持续时间（以分钟为单位）。
间隔变化	介于 1 和 3 之间。默认值为间隔持续时间的 1 倍。定义是否增加每次尝试的间隔持续时间。
数据接口	显示数据接口故障的自动重新加入设置。
尝试次数	介于 1 和 65535 之间。默认值为 3。设置尝试重新加入的次数。
尝试之间的间隔	介于 2 和 60 之间。默认值为 5 分钟。定义两次重新加入尝试之间的间隔持续时间（以分钟为单位）。
间隔变化	介于 1 和 3 之间。默认值为间隔持续时间的 2 倍。定义是否增加每次尝试的间隔持续时间。
系统	显示内部错误的自动重新加入设置。内部故障包括：应用同步超时、不一致的应用状态等。
尝试次数	介于 1 和 65535 之间。默认值为 3。设置尝试重新加入的次数。
尝试之间的间隔	介于 2 和 60 之间。默认值为 5 分钟。定义两次重新加入尝试之间的间隔持续时间（以分钟为单位）。
间隔变化	介于 1 和 3 之间。默认值为间隔持续时间的 2 倍。定义是否增加每次尝试的间隔持续时间。

注释 如果禁用系统运行状况检查，则在禁用系统运行状况检查时不适用的字段将不会显示。

您可以从此部分更改这些设置。

您可以监控任何端口通道 ID、单个物理接口 ID，以及 Snort 和磁盘已满进程。运行状况监控不在 VLAN 子接口或虚拟接口（例如，VNI 或 BVI）上执行。您不能为集群控制链路配置监控；它始终处于被监控状态。

过程

步骤 1 选择 **设备** > **设备管理**。

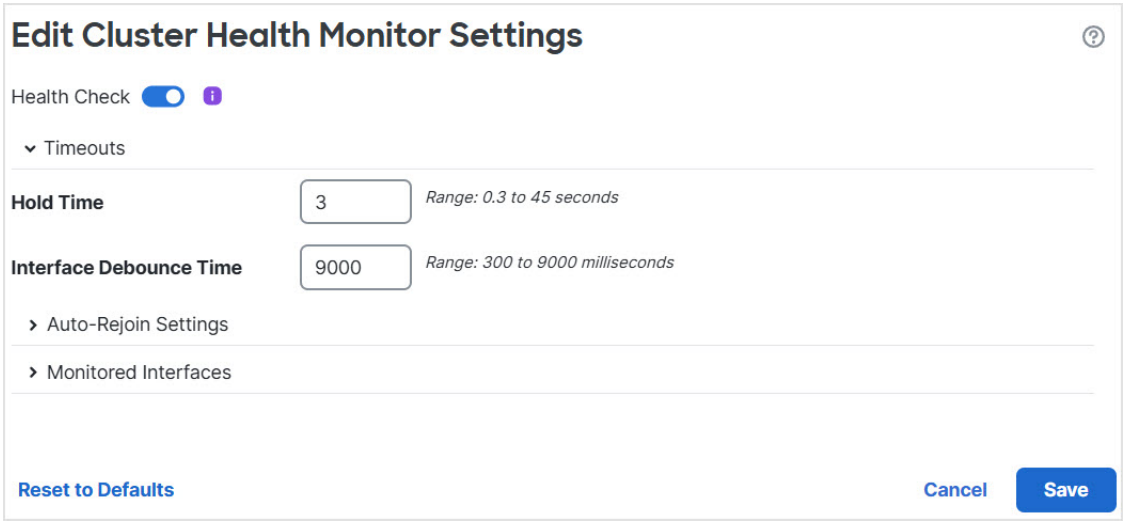
步骤 2 在要修改的集群旁边，点击 **编辑** ()。

步骤 3 点击**集群 (Cluster)**。

步骤 4 在**集群运行状况监控器设置 (Cluster Health Monitor Settings)** 部分，点击 **编辑** ()。

步骤 5 通过点击**运行状况检查 (Health Check)** 滑块禁用系统运行状况检查。

图 *26:* 禁用系统运行状况检查



当拓扑发生任何更改时（例如添加或删除数据接口、启用或禁用节点、或交换机上的接口、或者添加额外的交换机形成 VSS、vPC 或 VNet），您应禁用系统运行状态检查功能，还要禁用对已禁用接口的接口监控。当拓扑结构更改完成且配置更改已同步到所有节点后，您可以重新启用系统运行状况检查功能和被监控的接口。

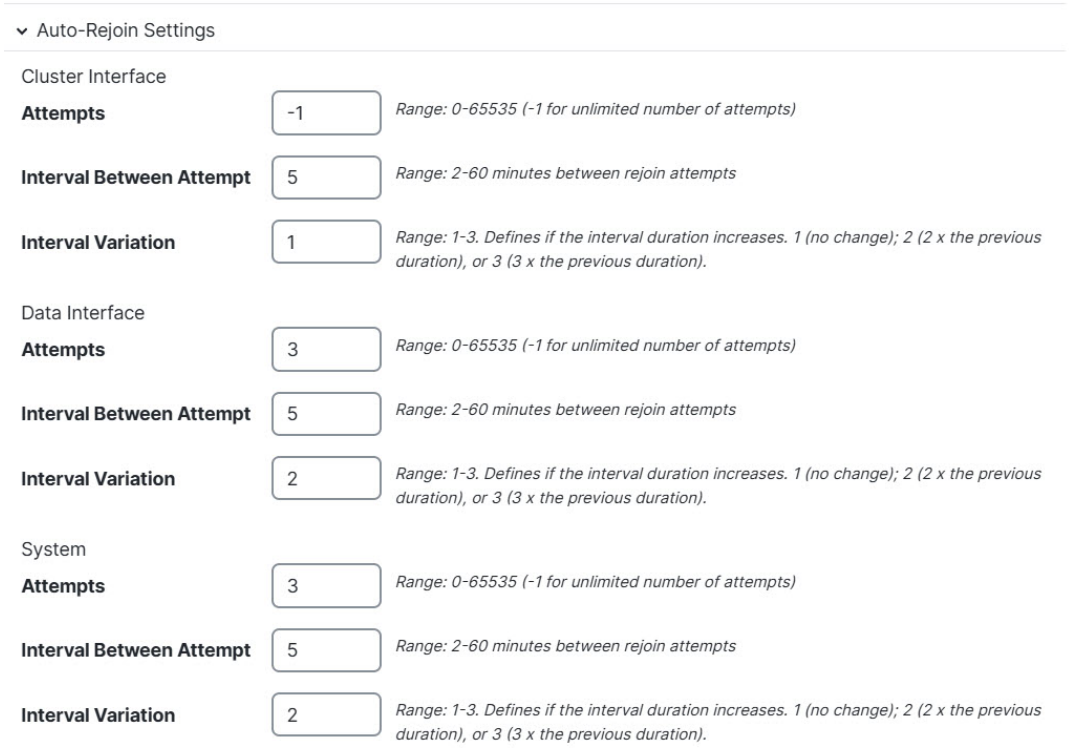
步骤 6 配置保持时间和接口防反跳时间。

- **保持时间 (Hold Time)** - 设置保持时间以确定两次节点心跳状态消息之间的时间间隔，其值介于 0.3 到 45 秒；默认值为 3 秒。

- **接口防反跳时间 (Interface Debounce Time)** - 将防反跳时间设置为 300 到 9000 毫秒之间。默认值为 500 毫秒。较小的值可以加快检测接口故障的速度。请注意，如果配置的防反跳时间较低，会增加误报几率。在发生接口状态更新时，节点会等待指定的毫秒数，然后才将接口标记为发生故障，并将节点从集群中删除。对于从故障状态转换为正常运行状态的 EtherChannel（例如，交换机重新加载或交换机启用 EtherChannel）而言，更长的防反跳时间可以防止集群节点上的接口仅仅因为另一个集群节点在绑定端口时的速度更快便显示为故障状态。

步骤 7 自定义在运行状况检查发生故障后的自动重新加入集群设置。

图 *27:* **配置自动重新加入设置**



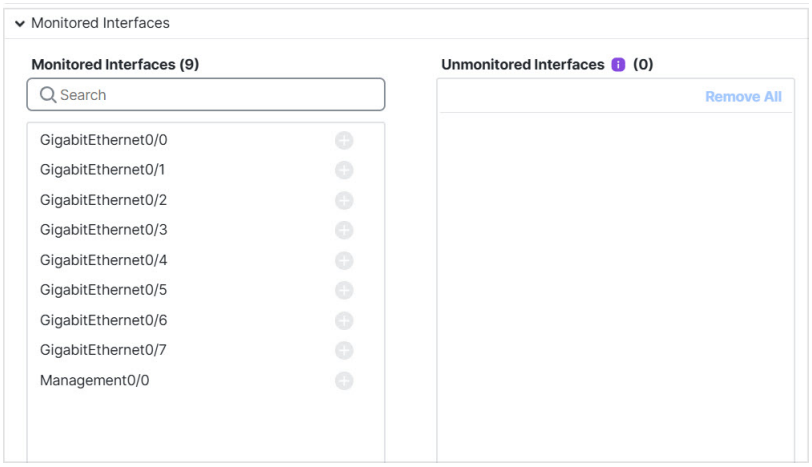
为**集群接口 (Cluster Interface)**、**数据接口 (Data Interface)** 和**系统 (System)** 设置以下值（内部故障包括：应用同步超时、应用状态不一致等）：

- **尝试次数 (Attempts)** - 设置重新加入尝试次数，介于 -1 和 65535 之间。**0** 将禁用自动重新加入。**集群接口 (Cluster Interface)** 的默认值为 -1（无限制）。**数据接口 (Data Interface)** 和**系统 (System)** 的默认值为 3。
- **尝试之间的间隔 (Interval Between Attempts)** - 定义两次重新加入尝试之间的间隔持续时间（以分钟为单位），介于 2 和 60 之间。默认值为 5 分钟。节点尝试重新加入集群的最大总时间限制为自上次失败之时起 14400 分钟（10 天）。
- **间隔变化 (Interval Variation)** - 定义是否增加间隔持续时间。设置介于 1 和 3 之间的值：**1**（无更改）；**2**（2 倍于上一次持续时间）或 **3**（3 倍于上一次持续时间）。例如，如果您将间隔持续时间设置为 5 分钟，并将变化设置为 2，则在 5 分钟后进行第 1 次尝试；在 10 分钟 (2 x 5) 后

进行第 2 次尝试；在 20 分钟 (2 x 10) 后进行第 3 次尝试。**集群接口 (Cluster Interface)** 的默认值为 **1**，**数据接口 (Data Interface)** 和**系统 (System)** 的默认值为 **2**。

步骤 8 通过移动**受监控接口 (Monitored Interfaces)**或**不受监控接口 (Unmonitored Interfaces)** 窗口中的接口来配置受监控接口。您还可以选中或取消选中**启用服务应用监控 (Enable Service Application Monitoring)**，以启用或禁用对 Snort 和磁盘已满进程的监控。

图 *28:* 配置受监控的接口



接口运行状态检查将监控链路故障。如果特定逻辑接口的所有物理端口在特定节点上发生故障，但在其他节点上的同一逻辑接口下仍有活动端口，则会从集群中删除该节点。节点在多长时间后从集群中删除成员取决于接口的类型以及该节点是既定节点还是正在加入集群的设备。默认情况下，为所有接口以及 Snort 和磁盘已满进程启用运行状况检查。

您可能想禁用不重要的接口的运行状况检查。

当拓扑发生任何更改时（例如添加或删除数据接口、启用或禁用节点、或交换机上的接口、或者添加额外的交换机形成 VSS、vPC 或 VNet），您应禁用系统运行状态检查功能，还要禁用对已禁用接口的接口监控。当拓扑结构更改完成且配置更改已同步到所有节点后，您可以重新启用系统运行状况检查功能和被监控的接口。

步骤 9 点击**保存**。

步骤 10 部署配置更改；请参阅 部署配置更改。

管理集群节点

禁用集群

您可能需要停用节点，以准备删除节点，或临时进行维护。此程序旨在暂时停用节点；节点仍将显示在 防火墙管理中心 设备列表中。当节点变为非活动状态时，所有数据接口都将关闭。

注释 在禁用集群之前，请勿关闭节点。

过程

步骤 1 对于要禁用的设备，选择 **设备** > **设备管理**，点击 **更多** (⋮)，然后选择**禁用节点集群**。

步骤 2 确认要在节点上禁用集群。

该节点在 **设备** > **设备管理** 列表中其名称旁边会显示（**已禁用**）。

步骤 3 重新启用集群，请参阅 重新加入集群，第 113 页。

重新加入集群

如果从集群中删除了某个节点（例如对于出现故障的接口），或者如果您手动禁用集群，必须手动将其重新加入集群。确保故障已解决，再尝试重新加入集群。有关可从集群中删除节点的原因的更多信息，请参阅重新加入集群，第 130 页。

过程

步骤 1 对于要重新激活的设备，请选择 **设备** > **设备管理**，点击 **更多** (⋮)，然后选择**启用节点集群**。

步骤 2 确认要在节点上启用集群。

调整集群节点

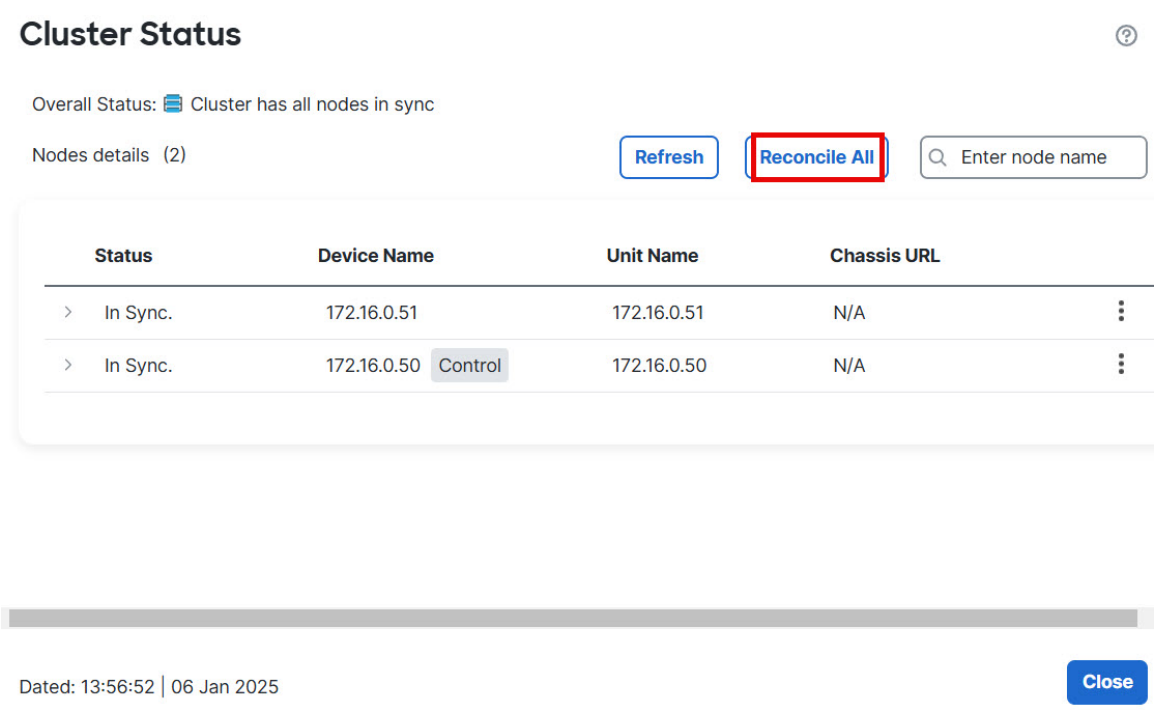
如果集群节点注册失败，则可将集群成员身份从设备协调至防火墙管理中心。例如，数据节点在防火墙管理中心 被占用或存在网络问题时注册失败的情况下。

过程

步骤 1 选择集群的 **设备** > **设备管理** **更多** (⋮)，然后选择**集群实时状态**，以打开**集群状态**对话框。

步骤 2 点击**协调全部 (Reconcile All)**。

图 *29:* 协调全部



有关集群状态的详细信息，请参阅监控集群，第 115 页。

取消注册集群或节点并注册到新防火墙管理中心

您可以从 防火墙管理中心 中取消注册集群，从而使集群保持不变。如果要将集群添加到新的 防火墙管理中心，则可能需要取消注册该集群。

您还可以从 防火墙管理中心 取消注册节点，而不会中断集群中的节点。虽然该节点不会显示在 防火墙管理中心 中，但它仍然是集群的一部分，并且它会继续传递流量，甚至可能成为控制节点。您无法取消注册当前的控制节点。如果无法再从防火墙管理中心访问该节点，您可能会希望将其取消注册，但在排除管理连接故障时，您仍希望将其作为集群的一部分。

取消注册集群：

- 会切断 防火墙管理中心和该集群之间的所有通信。
- 从 **设备管理** 页面删除集群。
- 如果集群的平台设置策略配置为使用 NTP 从 防火墙管理中心 接收时间，则将集群返回本地时间管理。
- 保持配置不变，以便集群继续处理流量。

  NAT 和 VPN、ACL 等策略以及接口配置保持不变。

将集群再次注册到相同或不同的防火墙管理中心会导致配置被删除，因此集群将在该点停止处理流量；集群配置保持不变，因此您可以将集群作为一个整体添加。您可以在注册时选择访问控制策略，但必须在注册后重新应用其他策略，然后在再次处理流量之前部署配置。

开始之前

此过程需要 CLI 对一个节点拥有访问权限。

过程

步骤 1 选择 **设备** > **设备管理**，点击集群或节点的 **更多** (⋮)，然后选择**取消注册**。

步骤 2 系统会提示您取消注册集群或节点；点击**是**。

步骤 3 您可以通过将其中一个集群成员添加为新设备来将集群注册到新的（或相同的）防火墙管理中心集群。

您只用将其中一个集群节点添加为设备，然后便可发现其余集群节点。

a) 连接到一个集群节点的 CLI，并使用 **configure manager add** 命令识别新 防火墙管理中心。

b) 选择 **设备** > **设备管理**，然后点击**添加设备**。

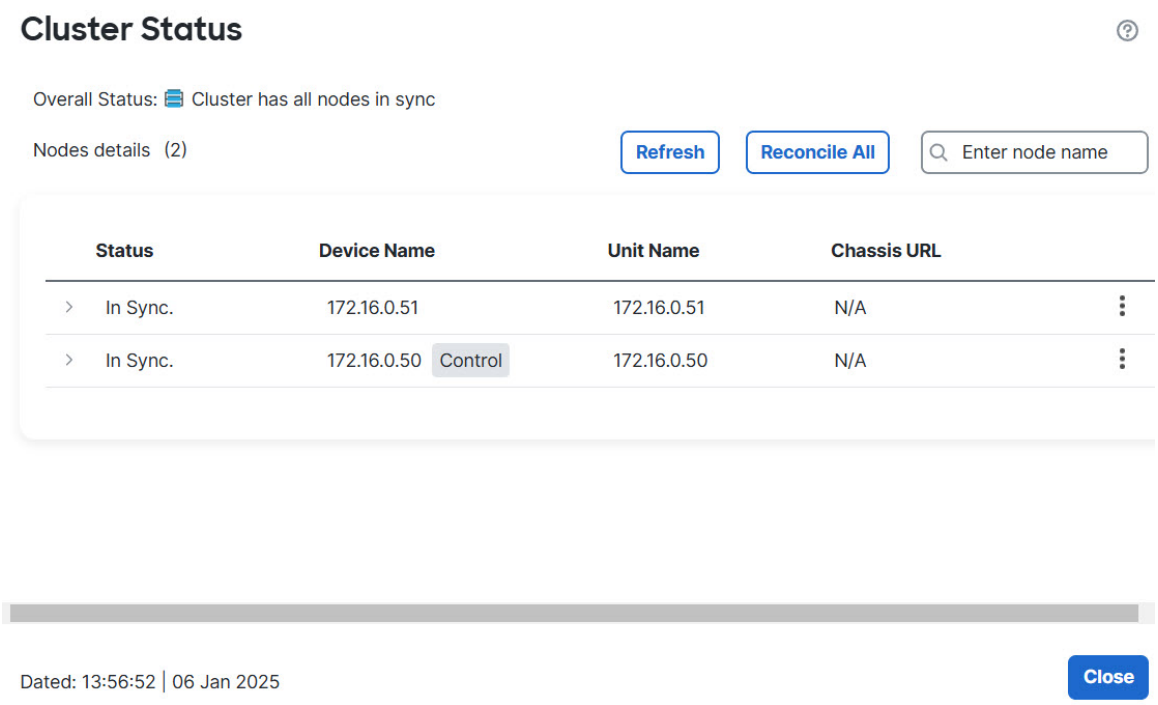
步骤 4 要重新添加已删除的节点，请参阅调整集群节点，第 113 页。

监控集群

您可以在 防火墙管理中心 中和 Firewall Threat Defense CLI 上监控集群。

- **集群状态**对话框，可从 **设备** > **设备管理**、**更多** (⋮) 图标或 **设备** > **设备管理** 访问，或点击**添加**，选择**集群**页面**常规**区域**集群实时状态**链接。

图 *30:* 集群状态



控制节点有一个标识其角色的图形指示器。

集群成员 **状态** 包括以下状态：

- 正在同步 (In Sync.) - 节点已向 防火墙管理中心 注册。
- 待处理注册 (Pending Registration) - 节点是集群的一部分，但尚未向 防火墙管理中心 注册。如果节点注册失败，则可点击**协调所有 (Reconcile All)** 以重试注册。
- 集群已禁用 (Clustering is disabled) - 节点已向 防火墙管理中心 注册，但它是集群的非活动成员。如果您打算稍后重新启用集群配置，集群配置将保持不变，或者您可以从集群中删除节点。
- “正在加入集群...”(Joining cluster...) - 节点正在加入机箱上的集群，但尚未完成加入。设备将在加入集群后向 防火墙管理中心 注册。

对于每个节点，您可以查看**摘要 (Summary)** 或**历史记录 (History)**。

图 *31:* 节点摘要

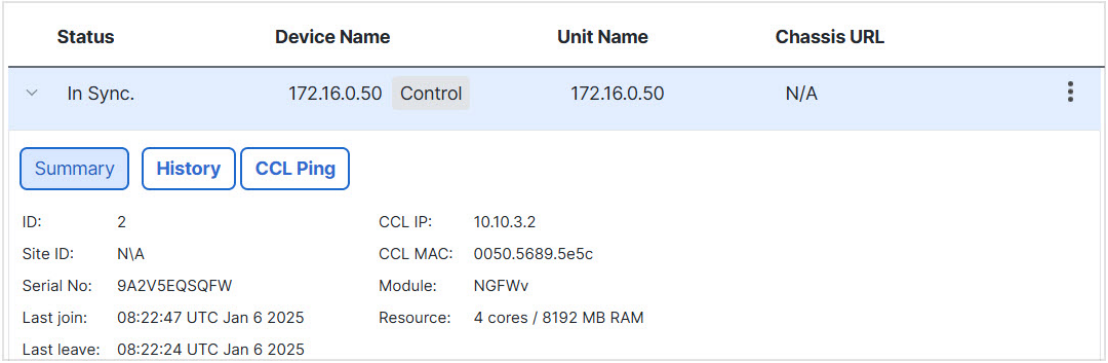
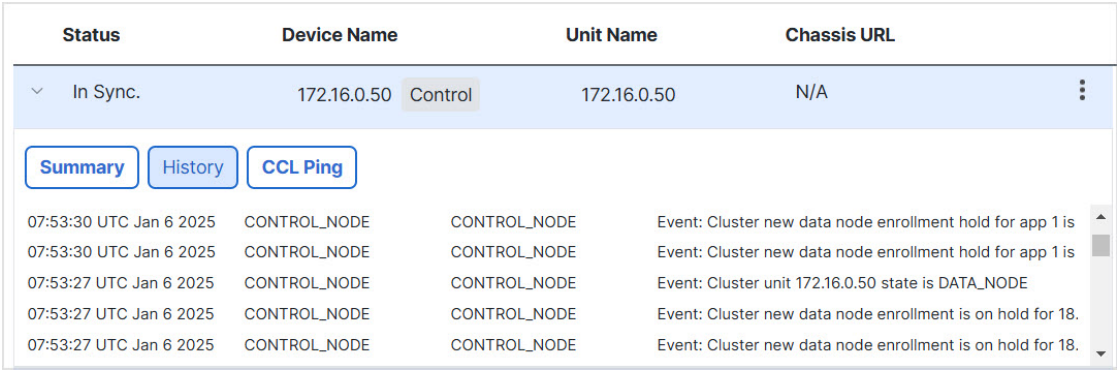


图 *32:* 节点历史记录



- 系统 (⚙) > 任务 页面。

  任务 **(Tasks)** 页面会在每个节点注册时更新“集群注册”(Cluster Registration) 任务。

- 设备 > 设备管理 然后点击添加 > 设备 *cluster_name*。

  展开设备列表页面上的集群时，您可以看到所有成员节点，包括 IP 地址旁显示其角色的控制节点。对于仍在注册的节点，则可看到加载图标。

- **show cluster** {**access-list** [*acl_name*] | **conn** [**count**] | **cpu** [**usage**] | **history** | **interface-mode** | **memory** | **resource usage** | **service-policy** | **traffic** | **xlate count**}

  要查看整个集群的聚合数据或其他信息，请使用 **show cluster** 命令。

- **show cluster info** [**auto-join** | **clients** | **conn-distribution** | **flow-mobility counters** | **goid** [*options*] | **health** | **incompatible-config** | **loadbalance** | **old-members** | **packet-distribution** | **trace** [*options*] | **transport** { **asp** | **cp**}]

  要查看集群信息，请使用 **show cluster info** 命令。

集群运行状况监控器控制面板

集群运行状况监控器

当 Firewall Threat Defense 是集群的控制节点时， 防火墙管理中心 会定期从设备指标数据收集器收集各种指标。集群运行状况监控器由以下组件组成：

- 概述控制面板 - 显示有关集群拓扑、集群统计信息和指标图表的信息：
  - 拓扑部分显示集群的实时状态、单个威胁防御的运行状况、威胁防御节点类型（控制节点或数据节点）以及设备的状态。设备的状态可以是 已禁用 （当设备离开集群时）、 已添加（在公共云集群中，不属于防火墙管理中心的其他节点）或 正常（节点的理想状态）。
  - 集群统计信息部分显示集群的当前指标，包括CPU 使用率、内存使用率、输入速率、输出速率、活动连接和 NAT 转换。

注释 CPU 和内存指标显示数据平面和 snort 使用情况的单个平均值。

  - 指标图表（即 CPU 使用情况、内存使用情况、吞吐量和连接）以图形方式显示指定时间段内的集群统计信息。

- 负载分布控制面板 - 在两个构件中显示集群节点的负载分布：
  - “分布”构件显示整个集群节点在整个时间范围内的平均数据包和连接分布情况。此数据描述节点如何分配负载。使用此构件，您可以轻松识别负载分布中的任何异常并进行纠正。
  - “节点统计信息”构件以表格格式显示节点级别指标。它显示有关CPU 使用率、内存使用率、输入速率、输出速率、活动连接以及跨集群节点的NAT 转换的指标数据。此表视图使您能够关联数据并轻松识别任何差异。

- 成员性能控制面板 - 显示集群节点的当前指标。您可以使用选择器来过滤节点并查看特定节点的详细信息。指标数据包括CPU 使用率、内存使用率、输入速率、输出速率、活动连接和NAT 转换。
- CCL 控制面板 - 以图形方式显示集群控制链路数据，即输入和输出速率。
- 故障排除和链接 - 提供常用故障排除主题和程序的便捷链接。
- 时间范围 - 用于限制各种设备指标窗口中显示的信息的可调时间窗口。
- 自定义控制面板 - 显示有关集群范围指标和节点级指标的数据。但是，节点选择仅适用于威胁防御指标，不适用于节点所属的整个集群。

查看集群运行状况

您必须是管理员、运维或安全分析师用户才能执行此程序。

集群运行状况监控器提供集群和其节点的运行状态的详细视图。此集群运行状况监控器在一系列控制面板中提供集群的运行状况和趋势。

开始之前

- 确保您已从防火墙管理中心中的一个或多个设备创建集群。

过程

步骤 1 选择 > **运行状况** > **监控器故障排除** 。

使用监控导航窗格访问节点特定的运行状况监控器。

步骤 2 在设备列表中，点击 **展开**（>） 和 **折叠**（∨） 以展开和折叠托管集群设备列表。

步骤 3 要查看集群运行状况统计信息，请点击集群名称。默认情况下，集群监控器会在多个预定义的控制面板中报告这些运行状况和性能。指标控制面板包括：

- 概述 — 突出显示其他预定义控制面板中的关键指标，包括其节点、CPU、内存、输入和输出速率、连接统计信息；以及 NAT 转换信息。
- 负载分布 — 跨集群节点的流量和数据包分布。
- 成员性能 - 有关 CPU 使用率、内存使用率、输入吞吐量、输出吞吐量、活动连接和 NAT 转换的节点级统计信息。
- CCL - 接口状态和汇聚流量统计信息。

您可以通过点击标签浏览各种指标控制面板。有关受支持的集群指标的完整列表，请参阅 Cisco Secure Firewall Threat Defense 运行状况指标。

步骤 4 您可以从右上角的下拉列表中配置时间范围。您可以更改时间范围以反映短至前一小时（默认），或长至前一年的时间周期信息。从下拉列表中选择**自定义 (Custom)** 以配置自定义开始和结束日期。

点击刷新图标可将自动刷新设置为 5 分钟或关闭自动刷新。

步骤 5 点击“部署”图标，在趋势图上根据所选时间范围显示部署重叠。

部署图标指示所选时间范围内的部署数量。垂直条带表示部署开始和结束时间。对于多个部署，将显示多个频段/行。点击虚线顶部的图标可查看部署详细信息。

步骤 6 （对于特定节点运行状况监控器）在设备名称右侧的页面顶部的警报通知中查看节点的 **运行状况警报** 。

将鼠标指针悬停在**运行状况警报**上可查看节点的运行状况摘要。弹出窗口显示前五个运行状况警报的截断摘要。点击弹出窗口可打开运行状况警报摘要的详细视图。

步骤 7 （对于特定节点运行状况监控器）默认情况下，设备监控器会在多个预定义的控制面板中报告这些运行状况和性能。指标控制面板包括：

- 概述 — 突出显示其他预定义控制面板中的关键指标，包括CPU、内存、接口、连接统计信息；以及磁盘使用情况和关键进程信息。
- CPU - CPU 利用率，包括按进程和物理核心划分的 CPU 使用情况。
- 内存 - 设备内存使用率，包括数据平面和 Snort 内存使用率。
- 接口 - 接口状态和汇聚流量统计信息。
- 连接 - 连接统计信息（例如大象流、活动连接、峰值连接等）和 NAT 转换计数。
- Snort - 与 Snort 进程相关的统计信息。
- ASP 丢弃 — 与因各种原因而丢弃的数据包相关的统计信息。

您可以通过点击标签浏览各种指标控制面板。有关受支持设备指标的完整列表，请参阅 Cisco Secure Firewall Threat Defense 运行状况指标。

步骤 8 点击运行状况监控器右上角的加号 **添加新的控制面板**（＋），通过从可用指标组构建您自己的变量集来创建自定义控制面板。

对于集群范围的控制面板，选择集群指标组，然后选择指标。

集群指标

集群运行状况监控器跟踪与集群及其节点相关的统计信息，以及负载分布、性能和CCL流量统计信息的汇总。

表 *11:* 集群指标

指标	说明	格式
CPU	集群节点上的CPU指标平均值（分别针对数据平面和 snort）。	percentage
Memory	集群节点上的平均内存指标（分别用于数据平面和 snort）。	percentage
数据吞吐量	集群的传入和传出数据流量统计信息。	bytes
CCL 吞吐量	集群的传入和传出 CCL 流量统计信息。	bytes
连接	集群中的活动连接计数。	数字
NAT 转换	集群的 NAT 转换计数。	数字
分布	集群中每秒的连接分布计数。	数字
数据包数	集群中每秒的数据包分发计数。	数字

对集群进行故障排除

您可以使用 **CCL Ping** 工具确保集群控制链路正常运行。 您还可以使用以下适用于设备和集群的工具：

- 故障排除文件-如果节点未能加入集群，系统将自动生成故障排除文件。您还可以从 **设备** > **设备管理** > **集群** > **常规** 区域生成和下载故障排除文件。请参阅生成故障排除文件。

  您还可以通过点击 **更多** (⋮) 并选择 **文件故障排除** ，从 **设备管理**页面生成文件。

- CLI 输出-从 **设备** > **设备管理** > **集群** > **常规**区域，您可以查看一组预定义的 CLI 输出，帮助您排除集群的故障。系统会自动为集群运行以下命令：
  - **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**

  您还可以在命令字段中输入任何 **show** 命令。有关详细信息，请参阅查看 CLI 输出。

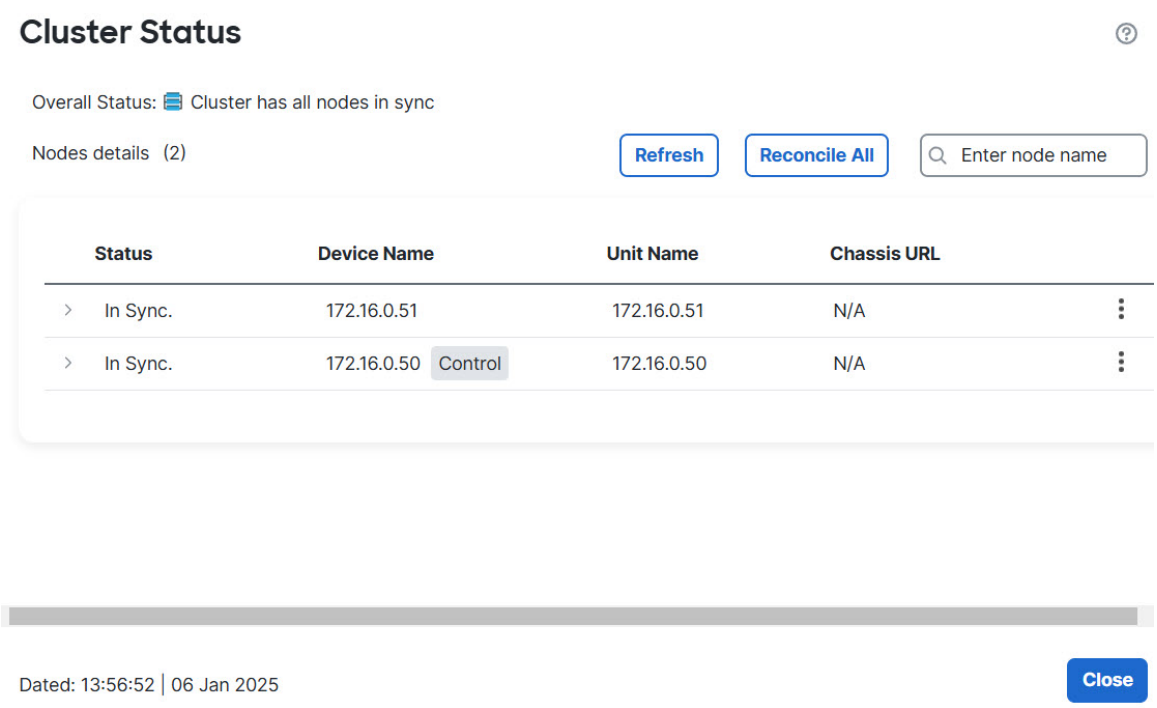
在集群控制链路上执行 Ping

当某个节点加入集群时，它会向控制节点发送 ping，其数据包大小与集群控制链路 MTU 匹配，从而检查 MTU 兼容性。如果 ping 失败，系统会生成通知，以便您纠正连接的交换机上 MTU 不匹配的问题，然后重试。如果您遇到集群控制链路连接问题，此工具允许您手动 ping 所有已加入集群的节点。

过程

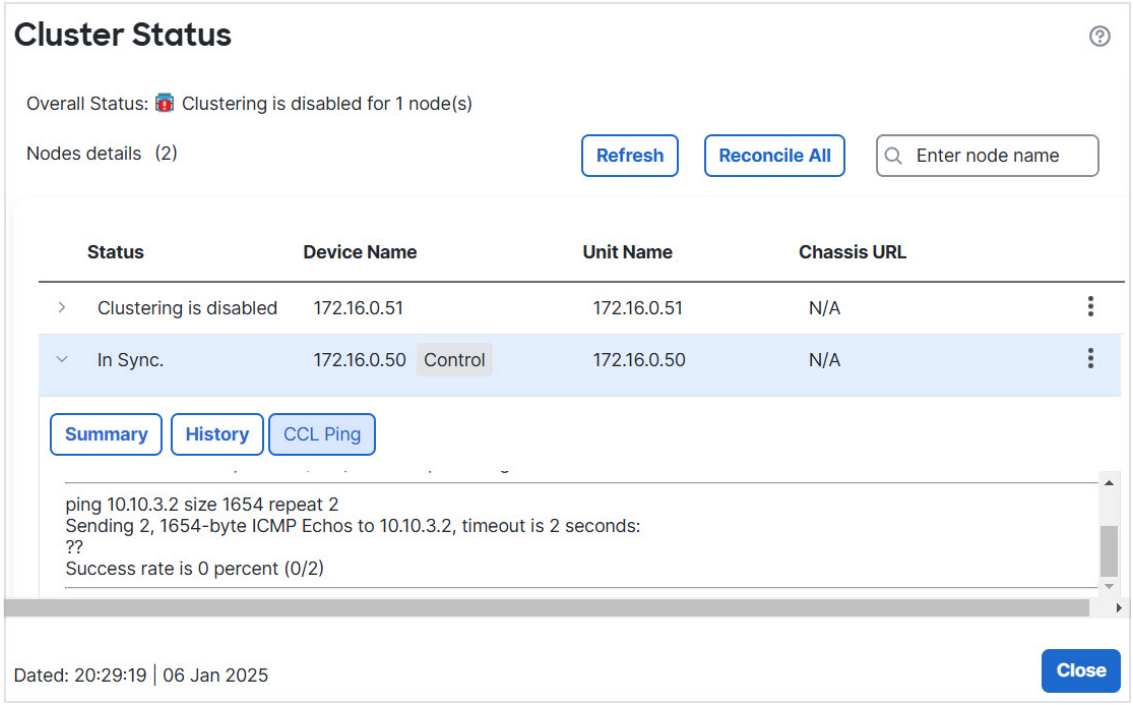
步骤 1 选择 **设备** > **设备管理**，点击集群旁边的 **更多** (⋮) 图标，然后选择**集群实时状态**。

图 *33:* 集群状态



步骤 2 展开其中一个节点，然后点击 **CCL Ping**。

图 *34: CCL Ping*



节点使用与最大 MTU 匹配的数据包大小在集群控制链路上向每个其他节点发送 ping 命令。

升级集群

要升级 Firewall Threat Defense Virtual 集群，请执行以下步骤。

开始之前

- 在公共云中升级集群之前，请将目标版本映像复制到云映像存储库，并更新集群部署模板中的映像 ID（实际上，我们建议使用修改后的副本替换现有模板）。这可确保在升级后，新实例（例如，在集群扩展期间启动的实例）将使用正确的版本。如果市场没有您需要的映像，例如在集群修补后，请从运行正确版本的独立Firewall Threat Defense Virtual实例的快照创建一个自定义映像，无需实例特定的 (Day 0) 配置。
- 对于 AWS 的Firewall Threat Defense Virtual，请在自动扩展的集群升级之前暂停 HealthCheck 和 ReplaceUnhealthy 进程。这可确保在升级后重新启动期间 Auto Scaling 组不会终止实例。您可以稍后恢复挂起的进程。有关说明，请参阅《Amazon EC2 Auto Scaling 用户指南： 暂停和恢复 Amazon EC2 Auto Scaling 进程》 。

过程

步骤 1 将目标映像版本上传到云映像存储。

步骤 2 使用更新后的目标映像版本来更新集群的云实例模板。

a) 使用目标映像版本来创建实例模板的副本。

b) 将新创建的模板附加到集群实例组。

注释
如果用户希望保留旧的接口命名约定，请在 Day 0 配置中使用"IfNamingConvention"： "Old"键值对。

步骤 3 将目标映像版本升级包上传到 防火墙管理中心。

步骤 4 对要升级的集群执行就绪性检查。

步骤 5 成功进行就绪性检查后，开始安装升级包。

步骤 6 防火墙管理中心 会一次升级一个集群节点。

步骤 7 成功升级集群后，防火墙管理中心 会显示通知。

升级后，实例的序列号和 UUID 不会变化。

集群参考

本部分包括有关集群工作原理的详细信息。

威胁防御功能和集群

部分 Firewall Threat Defense 功能不受集群支持，还有部分功能仅在控制设备上受支持。其他功能可能对如何正确使用规定了注意事项。

不支持的功能和集群

以下功能在启用集群的情况下无法配置，相关命令会被拒绝。

注释 要查看集群不支持的 FlexConfig 功能（例如 WCCP 检测），请参阅 《ASA常规操作配置指南》。FlexConfig 允许您配置 防火墙管理中心 GUI 中不存在的许多 ASA 功能。请参阅FlexConfig 策略。

- 远程访问 VPN（SSL VPN 和 IPsec VPN）
- 在公共云中不支持站点间 VPN（基于策略和路由）。
- DHCP 客户端、服务器和代理。支持 DHCP 中继。

- 虚拟隧道接口 (VTIs)
- 高可用性
- 集成路由和桥接
- 防火墙管理中心 UCAPL/CC 模式

集群集中化功能

以下功能只有在控制节点上才受支持，且无法为集群扩展。

注释 集中功能的流量从成员节点通过集群控制链路转发到控制节点。

如果使用再均衡功能，则会先将集中功能的流量再均衡到非控制节点的设备，然后再将该流量归类为集中功能；如果发生此情况，该流量随后将被发送回控制节点。

对集中功能而言，如果控制节点发生故障，则所有连接都将断开，而您必须在新的控制节点上重新建立连接。

注释 要查看也通过集群进行集中化的 FlexConfig 功能（例如 RADIUS 检测），请参阅 《ASA 常规操作配置指南》。FlexConfig 允许您配置 防火墙管理中心 GUI 中不存在的许多 ASA 功能。请参阅 FlexConfig 策略。

- 以下应用检查：
  - DCERPC
  - ESMTP
  - NetBIOS
  - PPTP
  - RSH
  - SQLNET
  - SUNRPC
  - TFTP
  - XDMCP
- 静态路由监控

思科 TrustSec 和集群

只有控制节点学习安全组标记 (SGT) 信息。然后，控制节点将 SGT 填充到数据节点，数据节点可以根据安全策略对 SGT 做出匹配决策。

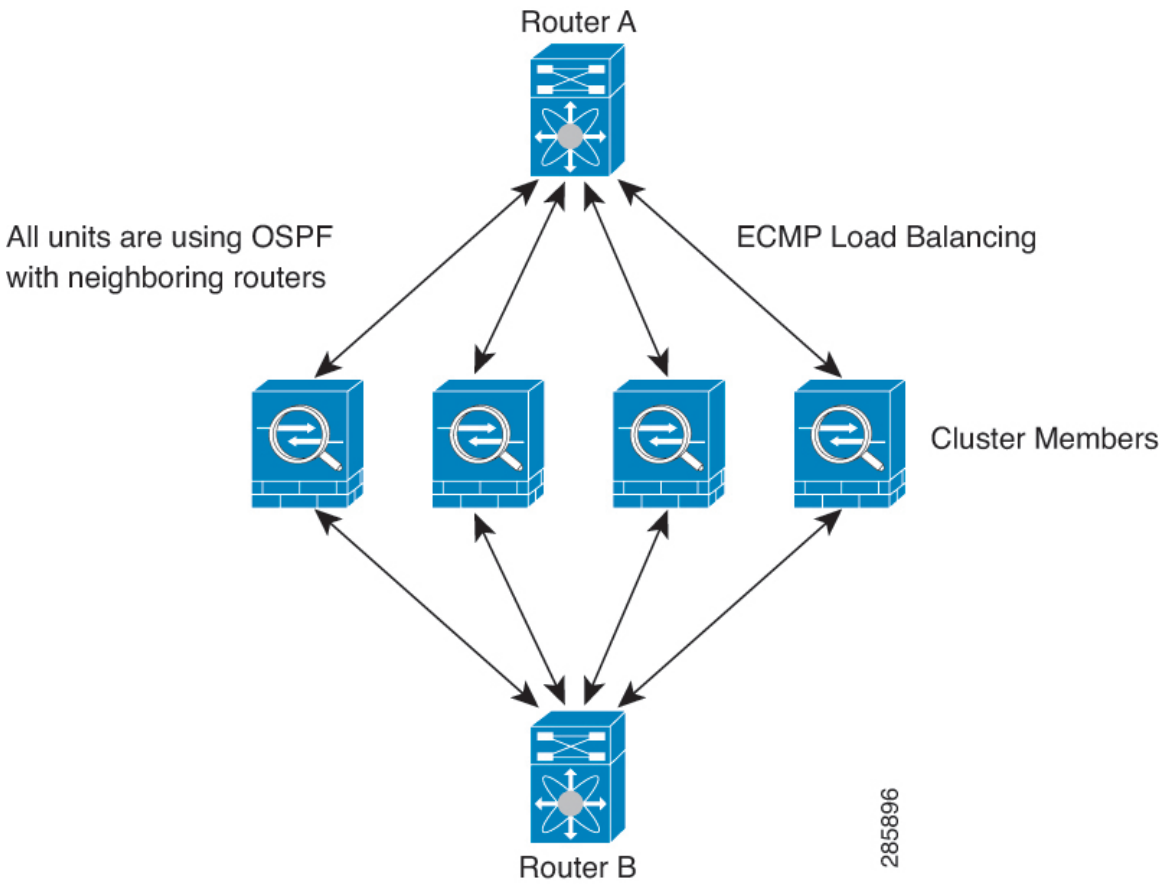
连接设置和集群

连接限制在集群范围强制实施。每个节点都有根据广播消息估计的集群范围的计数器值。出于效率考虑，在集群中配置的连接限制可能不会严格按限制数量实施。每个节点在任何指定时间都可能高估或低估集群范围内的计数器值。不过，在负载均衡的集群中，该信息将随时间而更新。

动态路由和集群

在独立接口模式下，每个节点作为独立的路由器运行路由协议，且每个节点独立获知路由。

图 *35:* 独立接口模式下的动态路由



在上图中，路由器 A 获知有 4 条等价路径通往路由器 B，每条路径都要经过一个节点。ECMP 用于在这 4 条路径之间对流量执行负载均衡。每个节点在与外部路由器通信时，都会挑选不同的路由器 ID。

您必须为路由器 ID 配置一个集群池，使每个节点都有单独的路由器 ID。

FTP 和集群

- 如果 FTP 数据通道和控制通道流量由不同的集群成员所有，则数据通道所有者会将空闲超时更新定期发送到控制通道所有者并更新空闲超时值。但是，如果重新加载控制流量所有者并重新托管控制流量，则不会再保持父/子流量关系；控制流量空闲超时不会更新。

NAT 和集群

对于 NAT 用途，请参阅以下限制。

NAT 可能会影响集群的总吞吐量。入站和出站 NAT 数据包可被发送到集群中不同的 Firewall 威胁防御，因为负载均衡算法取决于 IP 地址和端口，NAT 会导致入站和出站数据包具有不同的 IP 地址和/或端口。当数据包到达并非 NAT 所有者的 Firewall 威胁防御时，会通过集群控制链路转发到所有者，导致集群控制链路上存在大量流量。请注意，接收节点不会创建流向所有者的转发流量，因为 NAT 所有者最终可能不会根据安全和策略检查结果为数据包创建连接。

如果您仍想在集群中使用 NAT，请考虑以下准则：

- 不使用代理 ARP - 对于独立接口，切勿为映射的地址发送代理 ARP 回复。这可以防止邻接路由器与可能已经不在集群中的 ASA 保持对等关系。对于指向主集群 IP 地址的映射地址，上游路由器需要静态路由或带对象跟踪的 PBR。

- PAT 采用端口块分配 - 请参阅该功能的以下准则：
  - 每主机最大流量限制并不针对整个集群，而是单独应用于每个节点。因此，在每主机最大流量限制配置为 1 的包含 3 个节点的集群中，如果在全部 3 个节点上对来自主机的流量实行负载均衡，则可以分配 3 个端口块，每个节点 1 个。
  - 在执行每主机最大流量限制时，在备份池中的备份节点上创建的端口块不计算在内。
  - 如果进行即时 PAT 规则修改（对 PAT 池改用全新的 IP 地址范围），会导致在新的池生效时仍在传输的转换项备份请求的转换项备份创建失败。此行为并非端口块分配功能所特有，它是一个暂时性 PAT 池问题，只发现于在集群节点之间分配池并执行流量负载均衡的集群部署。
  - 在集群中操作时，不能直接更改块分配大小。只有在集群中重新加载每个设备后，新的大小才会生效。为避免重新加载每个设备，我们建议您删除所有块分配规则并清除与这些规则相关的所有转换。然后，您可以更改块大小并重新创建块分配规则。

- 对动态 PAT 使用 NAT 池地址分配 - 配置 PAT 池时，集群将池中的每个 IP 地址划分为端口块。默认情况下，每个块都是 512 个端口，但如果配置端口块分配规则，则使用块设置。这些块在集群中的各个节点之间均匀分配，因此每个节点都有一个或多个块对应 PAT 池中的每个 IP 地址。因此，在一个集群的 PAT 池中可以最少拥有一个 IP 地址，只要这足以支持您预期的 PAT 连接数即可。端口块覆盖的端口范围为 1024-65535，除非您在 PAT 池 NAT 规则中配置该选项以包含保留的端口 1-1023。

- 在多个规则中重复使用 PAT 池 - 要在多条规则中使用同一 PAT 池，必须注意规则中的接口选择。必须在所有规则中使用特定接口，或者在所有规则中使用“任意”接口。不能在规则中混

合使用特定接口和“任意”接口，否则系统可能无法将返回流量与集群中的正确节点进行匹配。每条规则使用唯一的 PAT 池是最可靠的方案。

- 不使用轮询 - 集群不支持 PAT 池轮询。
- 无扩展 PAT - 集群不支持扩展 PAT。
- 控制节点管理的动态 NAT 转换 - 控制节点保留转换表并复制到数据节点。当数据节点收到需要动态 NAT 的连接并且转换不在表中时，它将请求从控制节点转换。数据节点拥有该连接。
- 过时 xlate - 连接所有者上的 xlate 空闲时间不会更新。因此，空闲时间值可能会超过空闲超时值。如果空闲计时器值高于配置的超时值（refcnt 为 0），则表示 xlate 过时。
- 对以下检查不使用静态 PAT：
  - FTP
  - RSH
  - SQLNET
  - TFTP
  - XDMCP
  - SIP
- 如果您有大量 NAT 规则（超过一万条），则应使用设备 CLI 中的 **asp rule-engine transactional-commit nat** 命令启用事务提交模型。否则，节点可能无法加入集群。

SIP 检测和集群

控制流可以在任何节点上创建（由于负载均衡），但其子数据流必须位于同一节点上。

SNMP 和集群

您应始终使用本地地址而非主集群 IP 地址进行 SNMP 轮询。如果 SNMP 代理轮询主集群 IP 地址，则当选举出新的控制节点时，对新控制节点的轮询将失败。

当使用 SNMPv3 进行集群时，如果您在初始集群形成后添加新的集群节点，则 SNMPv3 用户不会复制到新节点。您必须删除用户并重新添加，然后重新部署配置，以强制用户复制到新节点。

系统日志和集群

- 集群中的每个节点都会生成自己的系统日志消息。您可以配置日志记录，使每个节点在系统日志消息的报头字段中使用相同或不同的设备 ID。例如，集群中的所有节点都会复制和共享主机名配置。如果将日志记录配置为使用主机名作为设备 ID，则所有节点生成的系统日志消息都会看似来自一个节点。如果将日志记录配置为使用集群引导程序配置中指定的本地节点名称作为设备 ID，系统日志消息就会看似来自不同节点。

性能换算系数

将多台设备组成一个集群时，预计可以达到近似 80% 最大组合吞吐量的集群总体性能。

例如，如果您的型号在单独运行时可以处理大约 10 Gbps 的流量，则对于 8 台设备的集群，最大组合吞吐量约为 80 Gbps（8 台设备 x 10 Gbps）的 80%：64 Gbps。

控制节点选择

集群节点通过集群控制链路通信，如下选举控制节点：

1. 当为节点启用集群（或当节点首次启动时已启用集群）时，设备会每 3 秒广播一个选举请求。
2. 具有较高优先级的任何其他设备都会响应选举请求；优先级设置在 1 和 100 之间，其中 1 为最高优先级。
3. 如果某节点在 45 秒后未收到另一个具有较高优先级的节点的响应，则该设备会成为控制节点。

注释 如果多个节点并列获得最高优先级，则使用集群节点名称和序列号确定控制节点。

4. 如果节点稍后加入具有更高优先级的集群，它不会自动成为控制节点；现有控制节点始终保持为控制节点，除非它停止响应，此时会选择新的控制节点。
5. 在“裂脑”场景中，当临时存在多个控制节点时，具有最高优先级的节点将会保留角色，而其他节点则恢复为数据节点角色。

注释 您可以手动强制节点成为控制节点。对集中功能而言，如果强制更改控制节点，则所有连接都将断开，而您必须在新的控制节点上重新建立连接。

集群中的高可用性

集群通过监控节点和接口的运行状况并在节点之间复制连接状态来提供高可用性。

节点运行状况监控

每个节点通过集群控制链路定期发送广播保持连接心跳数据包。如果控制节点在可配置的超时期限内未从数据节点接收任何keepalive心跳数据包或其他数据包，则控制节点会从集群中删除该数据节点。如果数据节点未从控制节点接收数据包，则从其余节点中选择新的控制节点。

如果节点因为网络故障而不是因为节点实际故障而无法通过集群控制链路相互访问，则集群可能会进入“裂脑”场景，其中隔离的数据节点将选择自己的控制节点。例如，如果路由器在两个集群位置之间发生故障，则位于位置1的原始控制节点将从集群中删除位置2数据节点。同时，位置2的节点将选择自己的控制节点并形成自己的集群。请注意，在这种情况下，非对称流量可能会失败。恢复集群控制链路后，优先级较高的控制节点将保留控制节点的角色。

接口监控

每个节点都会监控使用中的所有已命名的硬件接口的链路状态，并向控制节点报告状态更改。

监控所有物理接口；只能监控已命名的接口。 可以选择性地禁用对每个接口的监控。

如果某个节点被监控的接口发生故障，则将从集群中删除该设备。节点将在 500 毫秒后删除。

发生故障后的状态

如果控制节点发生故障，则优先级最高（数字最小）的另一个集群成员将成为控制节点。

Firewall Threat Defense将自动尝试重新加入集群，具体取决于故障事件。

注释 当 Firewall Threat Defense 变成不活动状态且无法自动重新加入集群时，所有数据接口都会关闭，仅管理接口可以发送和接收流量。

重新加入集群

当集群成员从集群中删除之后，如何才能重新加入集群取决于其被删除的原因：

- 集群控制链路在最初加入时出现故障 - 在解决集群控制链路存在的问题后，您必须通过重新启用集群来手动重新加入集群。
- 加入集群后出现故障的集群控制链路 - FTD 无限期地每 5 分钟自动尝试重新加入。
- 数据接口发生故障 - Firewall Threat Defense 会依次在第 5 分钟、第 10 分钟和第 20 分钟时自动尝试重新加入。如果在 20 分钟后未成功加入，则 Firewall Threat Defense应用会禁用集群。在解决数据接口的问题之后，必须手动启用集群。
- 节点存在故障 - 如果节点因节点运行状况检查失败而从集群中删除，则如何重新加入集群取决于失败的原因。例如，临时电源故障意味着节点会在重新启动后重新加入集群，只要集群控制链路开启即可。Firewall Threat Defense应用会每隔 5 秒尝试一次重新加入集群。
- 内部错误 - 内部故障包括：应用同步超时；应用状态不一致等。
- 失败的配置部署-如果从 FMC 部署新配置，并且在某些集群成员上部署失败，但在其他集群成员上成功部署，则从集群中删除失败的节点。您必须通过重新启用集群来手动重新加入集群。如果控制节点上的部署失败，则会回滚部署，并且不会删除任何成员。如果在所有数据节点上部署失败，则会回滚部署，并且不会删除成员。

数据路径连接状态复制

每个连接在集群中都有一个所有者和至少一个备用所有者。备用所有者在发生故障时不会接管连接；而是存储TCP/UDP状态信息，使连接在发生故障时可以无缝转移到新的所有者。备用所有者通常也是导向器。

有些流量需要 TCP 或 UDP 层以上的状态信息。请参阅下表了解支持或不支持此类流量的集群。

表 *12:* 在集群中复制的功能

流量	状态支持	备注
运行时间	是	跟踪系统运行时间。
ARP 表	是	-
MAC 地址表	是	-
用户标识	是	—
IPv6 邻居数据库	支持	—
动态路由	支持	—
SNMP 引擎 ID	否	-

集群管理连接的方式

连接可以负载平衡到集群的多个节点。连接角色决定了在正常操作中和高可用性情况下处理连接的方式。

连接角色

请参阅为每个连接定义的下列角色：

- 所有者 - 通常为最初接收连接的节点。所有者负责维护 TCP 状态并处理数据包。一个连接只有一个所有者。如果原始所有者发生故障，则当新节点从连接接收到数据包时，导向器会从这些节点中选择新的所有者。
- 备用所有者 - 存储从所有者接收的 TCP/UDP 状态信息的节点，以便在出现故障时可以无缝地将连接转移到新的所有者。在发生故障时，备用所有者不会接管连接。如果所有者处于不可用状态，从该连接接收数据包的第一个节点（根据负载均衡而定）联系备用所有者获取相关的状态信息，以便成为新的所有者。

  只要导向器（见下文）与所有者不是同一节点，导向器也可以是备用所有者。如果所有者选择自己作为导向器，则选择一个单独的备用所有者。

  对于 Firepower 9300 上的在一个机箱中包括多达 3 个集群节点的集群，如果备用所有者与所有者在同一机箱上，则将从另一个机箱中选择一个额外的备用所有者来保护流量免受机箱故障的影响。
- 导向器 - 处理来自转发器的所有者查找请求的节点。当所有者收到新连接时，会根据源/目的 IP 地址和端口的散列值（有关 ICMP 散列详细信息，请参见下文）选择导向器，然后向导向器发送消息来注册该新连接。如果数据包到达除所有者以外的任何其他节点，该节点会向导向器查询哪一个节点是所有者，以便转发数据包。一个连接只有一个导向器。如果导向器发生故障，所有者会选择一个新的导向器。

只要导向器与所有者不是同一节点，导向器也可以是备用所有者（见上文）。如果所有者选择自己作为导向器，则选择一个单独的备用所有者。

ICMP/ICMPv6 散列详细信息：

- 对于 Echo 数据包，源端口为 ICMP 标识符，目的端口为 0。
- 对于 Reply 数据包，源端口为 0，目的端口为 ICMP 标识符。
- 对于其他数据包，源端口和目的端口均为 0。

- 转发器 - 向所有者转发数据包的节点。如果转发者收到并非其所有的连接的数据包，则会向导向器查询所有者，然后为其收到的此连接的任何其他数据包建立发往所有者的流量。导向器也可以是转发者。请注意，如果转发者收到 SYN-ACK 数据包，它可以从数据包的 SYN Cookie 直接获知所有者，因此无需向导向器查询。（如果禁用 TCP 序列随机化，则不会使用 SYN Cookie；必须向导向器查询。）对于 DNS 和 ICMP 等持续时间极短的流量，转发者不会查询，而是立即将数据包发送到导向器，然后由其发送到所有者。一个连接了可以有多个转发器；采用良好的负载均衡方法可以做到没有转发器，让一个连接的所有数据包都由所有者接收，从而实现最高效率的吞吐量。

注释 不建议您在使用集群时禁用 TCP 序列随机化。由于 SYN/ACK 数据包可能会被丢弃，因此少数情况下可能无法建立某些 TCP 会话。

- 分段所有者 - 对于分段的数据包，接收分段的集群节点使用分段源 IP 地址、目的 IP 地址和数据包 ID 的散列确定分段所有者。然后，所有片段都通过集群控制链路转发给片段所有者。片段可能均衡分发给不同的集群节点，因为只有第一个分段包含交换机负载均衡散列中使用的 5 元组。其他片段不包含源端口和目的端口，可能会均衡分发给其他集群节点。片段所有者临时重组数据包，以便根据源/目标 IP 地址和端口的散列来确定导向器。如果是新连接，则片段所有者将注册为连接所有者。如果是现有连接，则片段所有者将所有片段转发给集群控制链路上提供的连接所有者。然后，连接所有者将重组所有片段。

端口地址转换连接

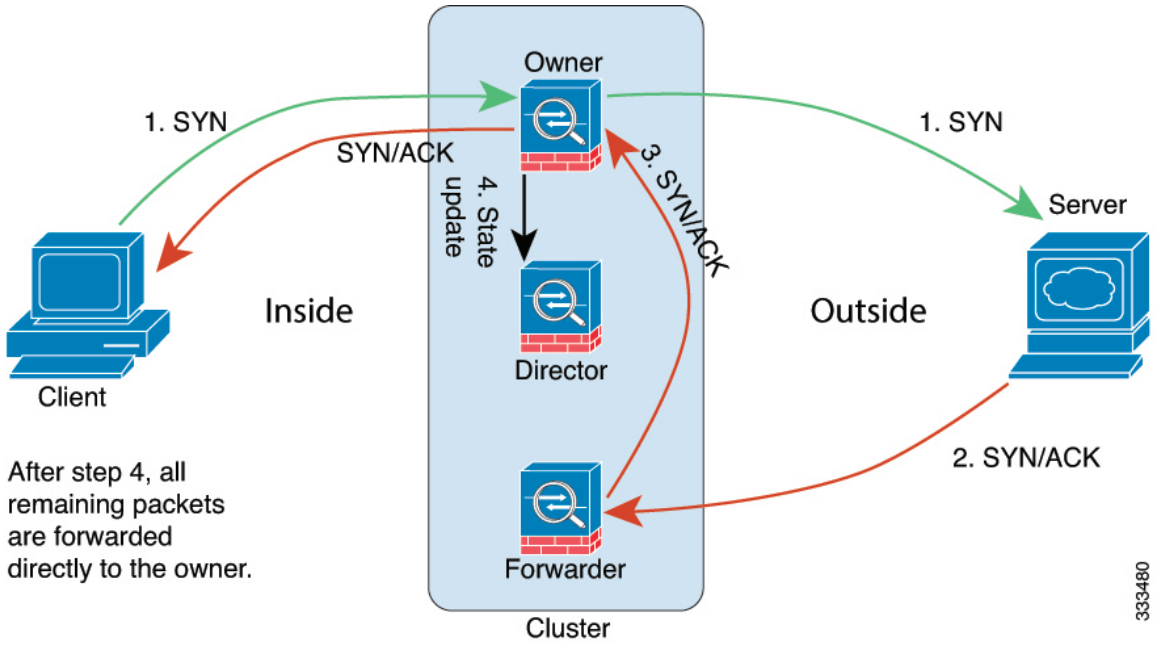
新连接所有权

此版本不支持流量重定向。通过负载均衡将新连接定向到集群节点时，该连接的两个方向都由此节点所有。同一连接的所有后续数据包都应到达同一节点。如果任何连接数据包到达其他节点，它们将被丢弃。如果反向流量到达其他节点，也将被丢弃。对于集中功能，如果连接不到达控制节点，则它们会被丢弃。

默认情况下，AWS GWLB 使用 5 元组来保持流粘性。建议在 AWS GWLB 上启用 2 元组或 3 元组粘性，以确保将相同的流发送到同一节点。

TCP 的数据流示例

以下图例显示了新连接的建立。

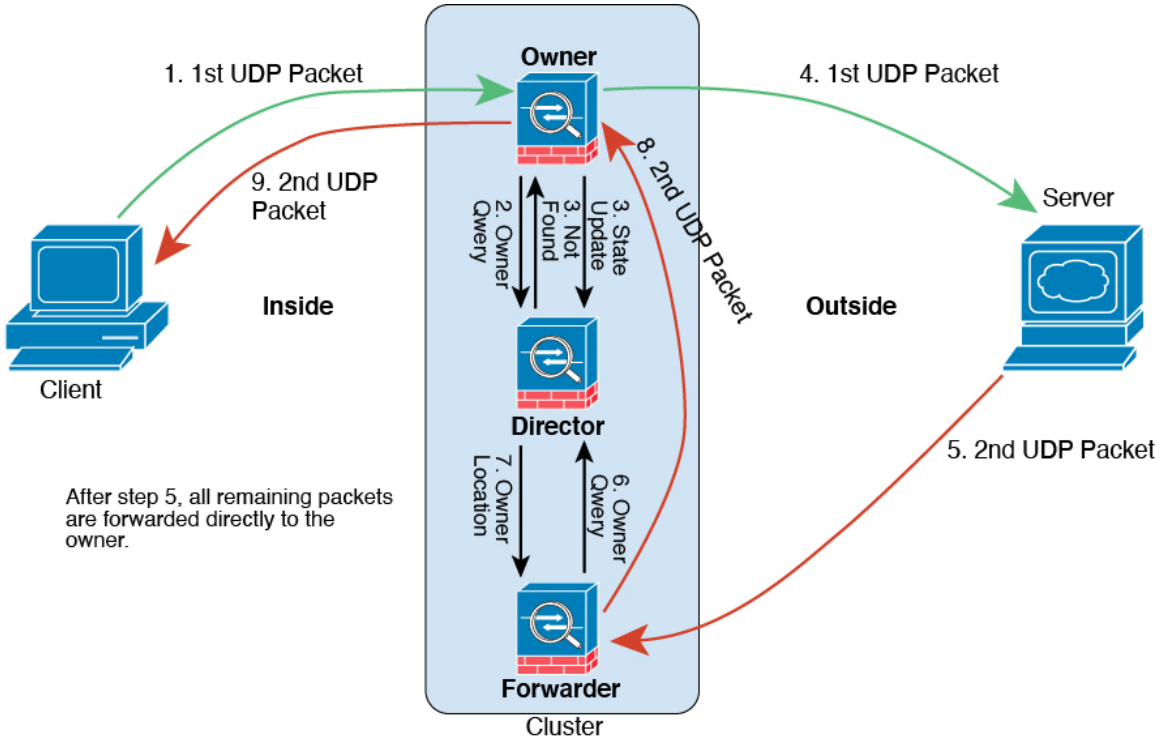


1. SYN 数据包从客户端发出，被传送到一台 Firewall 威胁防御（基于负载均衡方法），该设备将成为所有者。所有者创建一个流量，将所有者信息编码为 SYN Cookie，然后将数据包转发到服务器。
2. SYN-ACK 数据包从服务器发出，被传送到一台不同的 Firewall 威胁防御（基于负载均衡方法）。此 Firewall 威胁防御是转发者。
3. 由于转发器不是该连接的所有者，因此它将解码 SYN Cookie 中的所有者信息，然后创建发往所有者的转发流量，并将 SYN-ACK 数据包转发到所有者。
4. 所有者将状态更新发送到导向器，然后将 SYN-ACK 数据包转发到客户端。
5. 导向器接收来自所有者的状态更新，创建发往所有者的流量，并记录 TCP 状态信息以及所有者。导向器将充当该连接的备用所有者。
6. 传送到转发器的任何后续数据包都会被转发到所有者。
7. 如果数据包被传送到任何其他节点，它将向导向器查询所有者并建立一个流量。
8. 该流量的任何状态更改都会导致所有者向导向器发送状态更新。

ICMP 和 UDP 的数据流示例

以下图例显示了新连接的建立。

1. 图 *36: ICMP* 和 *UDP* 数据流



第一个 UDP 数据包从客户端发出，被传送到一个Firewall 威胁防御（基于负载均衡方法）。

2. 收到第一个数据包的节点查询基于源/目的 IP 地址和端口的散列值选择的导向器节点。
3. 导向器找不到现有流，创建导向器流并将数据包转发回前一个节点。换句话说，导向器已为此流选择了所有者。
4. 所有者创建流，向导向器发送状态更新，然后将数据包转发到服务器。
5. 第二个 UDP 数据包从服务器发出，并被传送到转发器。
6. 转发器向导向器查询所有权信息。对于 DNS 等持续时间极短的流量，转发者不会查询，而是立即将数据包发送到导向器，然后由其发送到所有者。
7. 导向器向转发器回复所有权信息。
8. 转发器创建转发流以记录所有者信息，并将数据包转发给所有者。
9. 所有者将数据包转发到客户端。

关于公共云中的 Threat Defense Virtual 集群的历史记录

表 *13:*

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
集群节点加入时的 MTU ping 测试通过尝试较小的 MTU 来提供更多信息	10.0.0	10.0.0	当某个节点加入集群时，它会向控制节点发送 ping，其数据包大小与集群控制链路 MTU 匹配，从而检查 MTU 兼容性。如果 ping 失败，它将尝试除以 MTU，并继续除以 2，直到 MTU ping 成功。成功的 ping 值会显示在 **show cluster info trace** 中，因此您可以将 MTU 调整为可用值，然后重试。 即使 ping 失败，系统仍允许节点加入集群。在这种情况下，您需要尽快解决 MTU 不匹配问题。 我们建议将交换机 MTU 的大小增加到建议的值，但如果您无法更改交换机配置，则可以使用集群控制链路的工作值来形成集群。 添加/修改的命令：**show cluster info trace**、**show cluster history**。
关于节点加入时时间节点的 MTU ping 测试	7.6.0	7.6.0	节点加入集群时，会向控制节点发送数据包大小为集群控制链路 MTU 两倍的 Ping 请求，以检查 MTU 兼容性。此前，仅控制节点发送 Ping。如果 ping 失败，系统会生成通知，以便您纠正连接的交换机上 MTU 不匹配的问题，然后重试。 添加/修改的命令：**show cluster history**。
集群控制链路 ping 工具。	7.2.67.4.1	任意	您可以通过执行 ping 来检查是否所有集群节点都能通过集群控制链路相互连接。节点无法加入集群的一个主要原因是集群控制链路配置不正确，例如，集群控制链路 MTU 设置可能高于连接交换机的 MTU。 新增/修改的屏幕：**设备** > **设备管理** > **更多** > **集群实时状态**。
故障排除文件生成和下载可从“设备”(Device) 和“集群”(Cluster) 页面获取。	7.4.1	7.4.1	您可以在“设备”(Device) 页面上为每个设备以及在“集群”(Cluster) 页面上为所有集群节点生成和下载故障排除文件。对于集群，您可以将所有文件下载为一个压缩文件。您还可以为集群节点添加集群的集群日志。您也可以从**设备** > **设备管理** > **更多** > **故障排除文件**菜单中触发文件生成。 新增/修改的菜单项： • **设备 (Devices)** > **设备管理 (Device Management)** > **设备 (Device)** > **常规 (General)** • **设备 (Devices)** > **设备管理 (Device Management)** > **集群 (Cluster)** > **常规 (General)**

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
查看设备或设备集群的 CLI 输出。	7.4.1	任意	您可以查看一组预定义的 CLI 输出，帮助您排除设备或集群的故障。您还可以输入任何 **show** 命令并查看输出。 新增/修改的屏幕： **设备 (Devices)** > **设备管理 (Device Management)** > **集群 (Cluster)** > **常规 (General)**
集群运行状况监控设置。	7.3.0	任意	您现在可以编辑集群运行状况监控设置。 新增/修改的屏幕：**设备 (Devices)** > **设备管理 (Device Management)** > **集群 (Cluster)** > **集群运行状况监控设置 (Cluster Health Monitor Settings)** **注释** 如果您之前使用 FlexConfig 配置了这些设置，务必要在部署之前删除 FlexConfig 配置。否则，FlexConfig 配置将覆盖管理中心配置。
集群运行状况监控器控制面板。	7.3.0	任意	您现在可以在集群运行状况监控控制面板上查看集群运行状况。 新增/修改的屏幕：**系统** > **运行状况** > **监控器**
Azure 中的 Firewall Threat Defense Virtual 集群。	7.3.0	7.3.0	现在，您可以在 Azure 中为 Azure 网关负载均衡器或外部负载均衡器配置最多 16 个节点 Firewall Threat Defense Virtual 的集群。 新增/修改的屏幕： • **设备** > **设备管理** > **添加集群** • **设备** > **设备管理** > **更多** 菜单 • **设备 (Devices)** > **设备管理 (Device Management)** > **集群 (Cluster)** 支持的平台：Azure 中的 Firewall Threat Defense Virtual
公共云（Amazon Web 服务和 Google Cloud Platform）上 Firewall Threat Defense Virtual 的集群。	7.2.0	7.2.0	Firewall Threat Defense Virtual 支持公共云（AWS 和 GCP）上最多 16 个节点的单个接口集群。 新增/修改的屏幕： • **设备 (Devices)** > **设备管理 (Device Management)** > **添加设备 (Add Device)** • **设备** > **设备管理** > **更多** 菜单 • **设备 (Devices)** > **设备管理 (Device Management)** > **集群 (Cluster)** 支持的平台：AWS 和 GCP 上的 Firewall Threat Defense Virtual

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。