在公共云中为 ASA 虚拟部署集群

上次修改日期: 2022 年 12 月 28 日

在公共云中为 ASA 虚拟部署集群

通过集群，您可以将多台 ASA 虚拟 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。您可以使用以下方法在公共云中部署 ASA 虚拟 集群：

- Amazon Web Services (AWS)

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。请参阅集群不支持的功能，第 32 页。

关于公共云中的 ASA 虚拟集群

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 ASA 虚拟 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：
  - 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。ASA 虚拟 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）。

  - 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 ASA 虚拟 故障会导致问题；如果继续使用该路由，发往故障 ASA 虚拟 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 ASA 虚拟 使之加入动态路由。

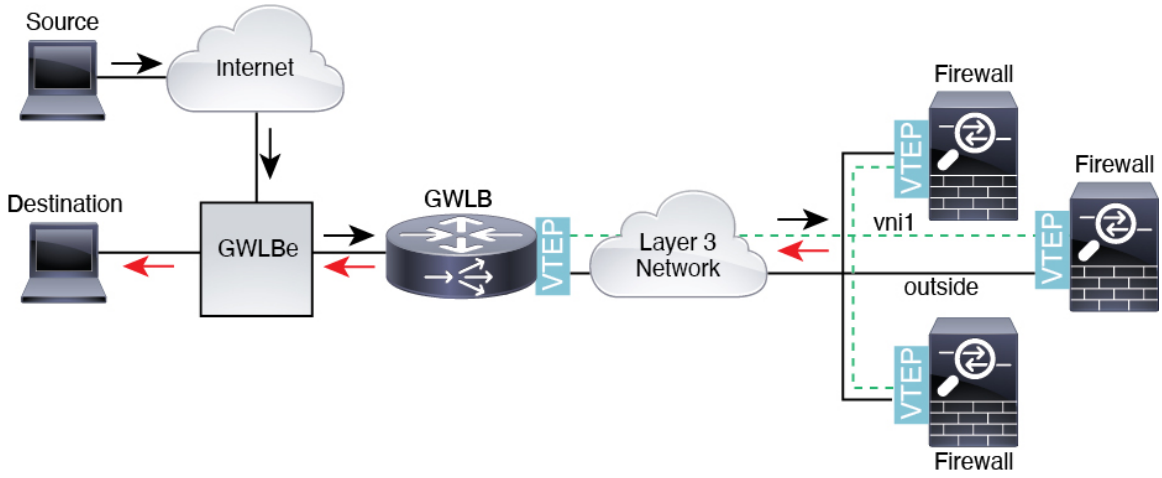
注释 负载均衡不支持第 2 层跨区以太网通道。

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。ASA 虚拟 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）。ASA 虚拟然后，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。

图 *1: Geneve* 单臂代理



集群节点

集群节点协调工作来实现安全策略和流量的共享。本节介绍每种节点角色的性质。

引导程序配置

您要在每台设备上配置最低的引导程序配置，包括集群名称、集群控制链路接口和其他集群设置。启用集群的第一个节点通常成为控制节点。在后续节点上启用集群时，这些设备将作为数据节点加入集群。

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，则控制节点由引导程序配置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。 通常，当您首次创建集群时，您添加的第一个节点会成为控制节点，因为它是到目前为止集群中的唯一节点。

必须只能在控制节点上执行所有配置（引导程序配置除外）；然后配置将被复制到数据节点中。如果是接口等物理资产，控制节点的配置将被镜像到所有数据节点。例如，如果将以太网接口 1/2 配置为内部接口，将以太网接口 1/1 配置为外部接口，则这些接口也将在数据节点上用作内部和外部接口。

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。

单个接口

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。必须仅在控制节点上配置接口配置，并且每个接口都要使用 DHCP。

注释 不支持第 2 层跨区以太网通道。

集群控制链接

每个节点必须将一个接口作为集群控制链路的 VXLAN (VTEP) 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ASA 虚拟 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，ASA 虚拟 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。

集群控制链路故障

如果某台设备的集群控制链路线路协议关闭，则集群将被禁用；数据接口关闭。当您修复集群控制链路之后，必须通过重新启用集群来手动重新加入集群。

注释 当 ASA 虚拟 处于非活动状态时，所有数据接口关闭；只有管理专用接口可以发送和接收流量。管理接口将保持打开，使用设备从 DHCP 或集群 IP 池接收的 IP 地址。如果使用集群 IP池，在重新加载而设备在集群中仍然处于非活动状态时，则管理接口将无法访问（因为它届时将使用与控制节点相同的主 IP 地址）。您必须使用控制台端口（如果可用）来进行任何进一步配置。

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。

ASA 虚拟集群管理

使用 ASA 虚拟集群的一个好处可以简化管理。本节介绍如何管理集群。

管理网络

我们建议将所有节点都连接到一个管理网络。此网络与集群控制链路分隔开来。

管理接口

使用 Management 0/0 接口进行管理。

注释 您不能为管理接口启用动态路由。您必须使用静态路由。

您可以使用静态寻址或 DHCP 作为管理 IP 地址。

如果您使用静态寻址，则可以使用集群的主集群 IP 地址是集群的固定地址，而该集群始终属于当前的控制节点。您还要为每个接口配置一个地址范围，以便包括当前控制节点在内的每个节点都可以使用该范围内的本地地址。主集群 IP 地址提供对地址的统一管理访问；当控制节点更改时，主集群 IP 地址将转移到新的控制节点，使集群的管理得以无缝继续。本地 IP 地址用于路由，在排除故障时也非常有用。例如，您可以连接到主集群 IP 地址来管理集群，该地址始终属于当前的控制节点。要

管理单个成员，您可以连接到本地 IP 地址。对于 TFTP 或系统日志等出站管理流量，包括控制节点在内的每个节点都使用本地 IP 地址连接到服务器。

如果使用 DHCP，则不使用本地地址池或主集群 IP 地址。

控制节点管理与数据节点管理

所有管理和监控均可在控制节点上进行。从控制节点中，您可以检查所有节点的运行时统计信息、资源使用情况或其他监控信息。您也可以向集群中的所有节点发出命令，并将控制台消息从数据节点复制到控制节点。

如果需要，您可以直接监控数据节点。虽然在控制节点上可以执行文件管理，但在数据节点上也可以如此（包括备份配置和更新映像）。以下功能在控制节点上不可用：

- 监控每个节点的集群特定统计信息。
- 监控每个节点的系统日志（控制台复制启用时发送至控制台的系统日志除外）。
- SNMP
- NetFlow

加密密钥复制

当您在控制节点上创建加密密钥时，该密钥将复制到所有数据节点。如果您有连接到主集群 IP 地址的 SSH 会话，则控制节点发生故障时连接将断开。新控制节点对 SSH 连接使用相同的密钥，这样当您重新连接到新的控制节点时，无需更新缓存的 SSH 主机密钥。

ASDM 连接证书 IP 地址不匹配

默认情况下，ASDM 连接将根据本地 IP 地址使用自签名证书。如果使用 ASDM 连接到主集群 IP 地址，则可能会因证书使用的是本地 IP 地址而不是主集群 IP 地址，系统会显示一则警告消息，指出 IP 地址不匹配。您可以忽略该消息并建立 ASDM 连接。但是，为了避免此类警告，您也可以注册一个包含主集群 IP 地址和 IP 地址池中所有本地 IP 地址的证书。然后，您可将此证书用于每个集群成员。有关详细信息，请参阅https://www.cisco.com/c/en/us/td/docs/security/asdm/identity-cert/cert-install.html。

ASA 虚拟集群许可证

每个集群节点都需要相同的模型许可证。我们建议为所有节点使用相同数量的 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。

注释 如果取消注册 ASA 虚拟 从而使得其未经许可，则在重新加载 ASA 虚拟 后，它将恢复到严格的速率限制状态。未经许可的低性能集群节点将对整个集群的性能产生负面影响。请务必保留所有集群节点的许可，或删除任何未经许可的节点。

ASA 虚拟集群要求和必备条件

型号要求

- ASAv30, ASAv50, ASAv100
- 以下公共云服务：
  - Amazon Web Services (AWS)
- 最多 16 个节点

另请参阅《ASA 虚拟入门指南》中有关 ASA 虚拟的一般要求。

硬件和软件要求

集群中的所有节点：

- 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。
- 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。不匹配的软件版本可能会导致性能不佳，因此请务必在同一维护窗口中升级所有节点。
- 支持单个可用性区域部署。
- 集群控制链路接口必须位于同一子网中，因此集群应部署在同一子网中。

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。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。

下表显示了建议的集群控制链路 MTU 和数据接口 MTU。

表 *1:* 建议的 *MTU*

公共云	集群控制链路 MTU	数据接口 MTU
具有 GWLB 的 AWS	1960 年	1806
AWS	1654	1500

ASA 虚拟集群准则

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。

其他规定

- 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 ASA 虚拟或交换机上的接口、添加额外的交换机形成冗余交换机系统），您应禁用运行状态检查功能，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。
- 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。

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。

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

- 您需要一台安装了 Python 3 的 Linux 计算机。

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-asav/tree/master/cluster/aws。

b) 使用所需的参数修改 **infrastructure.yaml** 和 **deploy_asav_clustering.yaml**。

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

您可以在 Linux 环境中创建 cluster_layer.zip 文件，例如安装了 Python 3.9 的 Ubuntu 18.04。

运行以下 shell 脚本以创建 cluster_layer.zip：

```
#!/bin/bash
mkdir -p layer
virtualenv -p /usr/bin/python3.9 ./layer/
source ./layer/bin/activate
pip3 install pycryptodome==3.12.0
pip3 install paramiko==2.7.1
pip3 install requests==2.23.0
pip3 install scp==0.13.2
pip3 install jsonschema==3.2.0
pip3 install cffi==1.14.0
pip3 install zipp==3.1.0
pip3 install importlib-metadata==1.6.0
echo "Copy from ./layer directory to ./python\n"
mkdir -p ./python/
cp -r ./layer/lib/python3.9/site-packages/* ./python/
zip -r cluster_layer.zip ./python
deactivate
```

d) 将生成的 **cluster_layer.zip** 文件复制到 lambda python files 文件夹。

e) 创建 **configure_asav_cluster.zip** 和 **lifecycle_asav_cluster.zip** 文件

可以在克隆存储库顶级目录中找到 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

步骤 2 部署 **Infrastructure.yaml** 并记下集群部署的输出值。

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。
d) 点击**下一步 (Next)**，然后点击**创建堆栈 (Create stack)**。
e) 在部署完成后，转到**输出 (Outputs)** 并记下 S3 **BucketName**。

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

步骤 4 部署 **deploy_asav_clustering.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_asav_clustering.yaml**。
c) 点击**下一步 (Next)** 并提供所需的信息。
d) 点击**下一步 (Next)**，然后点击**创建堆栈 (Create stack)**。

步骤 5 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。

在 AWS 中手动部署集群

要手动部署集群，请准备 day0 配置并部署每个节点。

创建 AWS 的 Day0 配置

为每个集群节点提供引导程序配置。

网关负载均衡器示例

以下示例会为网关负载均衡器创建一个配置，其中一个用于 u-turn 流量的 Geneve 接口和一个用于集群控制链路的 VXLAN 接口。请注意，每个节点需要设置唯一的**粗体**值。

```
cluster interface-mode individual force
interface management0/0
    management-only
    nameif management
    security-level 100
    ip address dhcp setroute
    no shutdown
interface TenGigabitEthernet0/0
    nameif geneve-vtep-ifc
    security-level 0
    ip address dhcp
    no shutdown
interface TenGigabitEthernet0/1
    nve-only cluster
    nameif ccl_link
    security-level 0
    ip address dhcp
    no shutdown
interface vni1
    description Clustering Interface
    segment-id 1
    vtep-nve 1
interface vni2
```

```
    proxy single-arm
    nameif uturn-ifc
    security-level 0
    vtep-nve 2
object network ccl_link
    range 10.1.90.4 10.1.90.254
object-group network cluster_group
    network-object object ccl_link
nve 2
    encapsulation geneve
    source-interface geneve-vtep-ifc
nve 1
    encapsulation vxlan
    source-interface ccl_link
    peer-group cluster_group
cluster group asav-cluster
    local-unit 1
    cluster-interface vni1 ip 10.1.1.1 255.255.255.0
    priority 1
    enable noconfirm
mtu geneve-vtep-ifc 1806
mtu ccl_link 1960
aaa authentication listener http geneve-vtep-ifc port 7575
jumbo-frame reservation
```

注释 对于 AWS 运行状况检查设置，请务必指定您在此处设置的 **aaa authentication listener http** 端口。

非本地负载均衡器示例

以下示例会创建一个配置，用于具有管理接口、内部接口和外部接口的非本地负载均衡器，以及用于集群控制链路的 VXLAN 接口。请注意，每个节点需要设置唯一的粗体值。

```
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
jumbo-frame reservation
mtu ccl_link 1654
object network ccl_link
```

```
    range 10.1.90.4 10.1.90.254
object-group network cluster_group
    network-object object ccl_link
nve 1
    encapsulation vxlan
    source-interface ccl_link
    peer-group cluster_group
cluster group asav-cluster
    local-unit 1
    cluster-interface vni1 ip 10.1.1.1 255.255.255.0
    priority 1
    enable
```

使用 AWS 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。

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

网关负载均衡器示例

以下示例会为网关负载均衡器创建一个配置，其中一个用于 u-turn 流量的 Geneve 接口和一个用于集群控制链路的 VXLAN 接口。请注意，每个节点需要设置唯一的粗体值。

```
{
    "AdminPassword": "Sam&Dean",
    "Hostname": "ftdv1",
    "FirewallMode": "Routed",
    "ManageLocally": "No",
    "run_config": [
        "cluster interface-mode individual force",
        "interface TenGigabitEthernet0/0",
            "nameif geneve-vtep-ifc",
            "ip address dhcp"
            "no shutdown",
        "interface TenGigabitEthernet0/1",
            "nve-only cluster",
            "nameif ccl_link",
            "ip address dhcp",
            "no shutdown",
        "interface vni1",
            "description Clustering Interface",
            "segment-id 1",
            "vtep-nve 1",
        "interface vni2",
            "proxy single-arm",
            "nameif uturn-ifc",
            "vtep-nve 2",
        "object network ccl_link",
            "range 10.1.90.4 10.1.90.254",
        "object-group network cluster_group",
            "network-object object ccl_link",
        "nve 2",
            "encapsulation geneve",
```

```
            "source-interface geneve-vtep-ifc",
        "nve 1",
            "encapsulation vxlan",
            "source-interface ccl_link",
            "peer-group cluster_group",
        "jumbo-frame reservation",
        "mtu geneve-vtep-ifc 1806",
        "mtu ccl_link 1960",
        "cluster group ftdv-cluster",
            "local-unit 1",
            "cluster-interface vni1 ip 10.1.1.1 255.255.255.0",
            "priority 1",
            "enable",
        "aaa authentication listener http geneve-vtep-ifc port 7777",
        ]
    }
}
```

注释 对于 AWS 运行状况检查设置，请务必指定您在此处设置的 **aaa authentication listener http** 端口。

非本地负载均衡器示例

以下示例会创建一个配置，用于具有管理接口、内部接口和外部接口的非本地负载均衡器，以及用于集群控制链路的 VXLAN 接口。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",
        "jumbo-frame reservation",
        "mtu ccl_link 1654",
        "object network ccl_link",
            "range 10.1.90.4 10.1.90.254",
        "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",
        ]
    }
}
```

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 根据 ASA 虚拟入门指南部署每个集群节点。

步骤 2 在**配置实例详细信息 (Configure Instance Details)** > **高级详细信息 (Advanced Details)** 部分中，粘贴您的 day0 配置。

步骤 3 根据负载均衡器解决方案来连接接口。

- AWS 网关负载均衡器，3 个接口 - 外部、管理、集群控制链路。
- 非本地负载均衡器，4 个接口 - 内部、外部、管理、集群控制链路。

步骤 4 配置 AWS 网关负载均衡器。

a) 创建网关负载均衡器并连接目标组。

b) 将节点注册到网关负载均衡器目标组。

自定义集群操作

作为第 0 天配置的一部分，或者在部署集群之后，您可以自定义集群运行状况监控、TCP 连接复制延迟、流移动性和其他优化。

在控制节点上执行这些程序。

配置基本 ASA 集群参数

您可以在控制节点上自定义集群设置。

过程

步骤 1 进入集群配置模式：

cluster group *name*

步骤 2 （可选） 启用数据节点到控制节点的控制台复制：

console-replicate

默认情况下会禁用此功能。对于特定的重要事件，ASA 可将某些消息直接打印输出到控制台。如果启用了控制台复制，数据节点会将控制台消息发送到控制节点，因此您只需要监控集群的一个控制台端口。

步骤 3 设置集群事件的最低跟踪级别：

trace-level 级别

根据需要设置最低级别：

- **critical**- 重要事件（严重性=1）
- **warning**- 警告（严重性 = 2）
- **informational**- 信息事件（严重性=3）
- **debug**- 调试事件（严重性=4）

配置运行状态监控并自动重新加入设置

此程序可以配置节点和接口运行状态监控。

您可能想禁用不重要的接口（例如管理接口）的运行状况检查。运行状况监控不在 VLAN 子接口上执行。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 进入集群配置模式。

cluster group *name*

示例：

```
ciscoasa(config)# cluster group test
ciscoasa(cfg-cluster)#
```

步骤 2 自定义集群节点运行状况检查功能。

health-check [**holdtime** 超时]

为了确定节点运行状况，ASA 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。

- **holdtime** 超时 - 用于确定两次设备 heartbeat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。

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 ASA、或交换机上的接口），您应禁用运行状态检查功能，还要禁用对已禁用接口的接口监控 (**no health-check monitor-interface**)。当拓扑结构更改完成且配置更改已同步到所有节点后，您可以重新启用运行状况检查功能。

示例：

```
ciscoasa(cfg-cluster)# health-check holdtime 5
```

步骤 3 在接口上禁用接口运行状况检查。

no health-check monitor-interface *interface_id*

接口运行状态检查将监控链路故障。ASA 在多长时间后从集群中删除成员取决于该节点是既定成员还是正在加入集群的设备。默认情况下，为所有接口启用运行状况检查。您可以使用此命令的 **no** 形式逐个接口将其禁用。您可能想禁用不重要的接口（例如管理接口）的运行状况检查。

- *interface_id* - 禁用接口监控。运行状况监控不在 VLAN 子接口上执行。您不能为集群控制链路配置监控；它始终处于被监控状态。

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 ASA、或交换机上的接口），您应禁用运行状态检查功能 (**no health-check**)，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，您可以重新启用运行状况检查功能。

示例：

```
ciscoasa(cfg-cluster)# no health-check monitor-interface management1/1
```

步骤 4 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。

health-check {**data-interface** | **cluster-interface** | **system**} **auto-rejoin** [**unlimited** | *auto_rejoin_max*] *auto_rejoin_interval auto_rejoin_interval_variation*

- **system**- 指定内部错误的自动重新加入设置。内部故障包括：应用程序同步超时、不一致的应用程序状态等。
- **unlimited** —（**cluster-interface** 的默认值）不限制重新加入尝试的次数。
- *auto-rejoin-max* — 设置重新加入尝试次数，介于 0 和 65535 之间。**0** 禁用自动重新加入。**data-interface** 和 **system** 的默认值为 3。
- *auto_rejoin_interval* - 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）。
- *Auto_rejoin_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。对于集群接口，默认值为 **1**，而对于数据接口和系统，默认值为 **2**。

示例：

```
ciscoasa(cfg-cluster)# health-check data-interface auto-rejoin 10 3 3
```

步骤 5 配置 ASA 将接口视为发生故障并将节点从集群中删除之前经过的防反跳时间。

health-check monitor-interface debounce-time *ms*

示例：

```
ciscoasa(cfg-cluster)# health-check monitor-interface debounce-time 300
```

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，ASA 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。

步骤 6 （可选） 配置流量负载监控。

load-monitor [**frequency** *seconds*] [**intervals** *intervals*]

- **frequency** *seconds* — 设置监控消息之间的时间（以秒为单位），范围介于 10 到 360 秒之间。默认值为 20 秒。
- **intervals** *intervals* — 设置 ASA 维护数据的间隔的数量，该值介于 1 到 60 之间。默认值为 30。

您可以监控集群成员的流量负载，包括总连接计数、CPU 和内存使用情况以及缓冲区丢弃。如果负载过高，且剩余的节点可以处理负载，您可以选择在节点上手动禁用集群，或调整外部交换机上的负载均衡。默认情况下启用此功能。您可以定期监控流量负载。如果负载过高，您可以选择手动禁用节点上的集群。

使用 **show cluster info load-monitor** 命令查看流量负载。

示例：

```
ciscoasa(cfg-cluster)# load-monitor frequency 50 intervals 25
ciscoasa(cfg-cluster)# show cluster info load-monitor
ID  Unit Name
0  B
1  A_1
Information from all units with 50 second interval:
Unit     Connections    Buffer Drops   Memory Used   CPU Used
Average from last 1 interval:
   0           0            0            14              25
   1           0            0            16              20
Average from last 25 interval:
   0           0            0            12              28
   1           0            0            13              27
```

示例

以下示例将 health-check holdtime 配置为 0.3 秒；禁用GUANLI 0/0 接口上的监控；将数据接口的 auto-rejoin 设置为从 2 分钟开始的 4 次尝试，将 duration 增至上一次间隔的 3 倍；以及将集群控制链路的 auto-rejoin 设为 6 次尝试，每隔 2 分钟一次。

```
ciscoasa(config)# cluster group test
ciscoasa(cfg-cluster)# health-check holdtime .3
ciscoasa(cfg-cluster)# no health-check monitor-interface management0/0
ciscoasa(cfg-cluster)# health-check data-interface auto-rejoin 4 2 3
ciscoasa(cfg-cluster)# health-check cluster-interface auto-rejoin 6 2 1
```

管理集群节点

部署集群后，您可以更改配置和管理集群节点。

成为非活动节点

要成为集群的非活动成员，请在节点上禁用集群，同时保持集群配置不变。

注释 当ASA处于非活动状态（以手动方式或因运行状况检查失败）时，所有数据接口都将关闭；只有管理专用接口可以发送和接收流量。要恢复流量传输，请重新启用集群；或者，您也可以从集群中完全删除该节点。管理接口将保持打开，使用节点从集群 IP 池接收的 IP 地址。但如果您重新加载，而节点仍在集群中处于非主用状态（例如，您保存了已禁用集群的配置），则管理接口将被禁用。您必须使用控制台端口来进行任何进一步配置。

过程

步骤 1 进入集群配置模式：

cluster group *name*

示例：

```
ciscoasa(config)# cluster group pod1
```

步骤 2 禁用集群：

no enable

如果此节点是控制节点，则会进行新的控制选择，并且其他成员将成为控制节点。

集群配置保持不变，因此您可于稍后再次启用集群。

从控制节点停用数据节点

要禁用您登录的节点以外的成员，请执行以下步骤。

注释 当ASA处于非活动状态时，所有数据接口关闭；只有管理专用接口可以发送和接收流量。要恢复流量流，请重新启用集群。管理接口将保持打开，使用节点从集群 IP 池接收的 IP 地址。但如果您重新加载，而节点仍在集群中处于非主用状态（例如，假设您保存了已禁用集群的配置），管理接口将被禁用。您必须使用控制台端口来进行任何进一步的配置。

过程

从集群中删除该节点：

cluster remove unit *node_name*

引导程序配置保持不变，从控制节点同步的最新配置也保持不变，因此您可于稍后重新添加该节点而不会丢失配置。如果在数据节点上输入此命令来删除控制节点，则会选择新的控制节点。

要查看成员名称，请输入 **cluster remove unit ?**，或者输入 **show cluster info** 命令。

示例：

```
ciscoasa(config)# cluster remove unit ?

Current active units in the cluster:
asa2

ciscoasa(config)# cluster remove unit asa2
WARNING: Clustering will be disabled on unit asa2. To bring it back
to the cluster please logon to that unit and re-enable clustering
```

重新加入集群

如果从集群中删除了某个节点（例如针对出现故障的接口），或者如果您手动停用了某个成员，那么您必须手动重新加入集群。

过程

步骤 1 在控制台中，进入集群配置模式：

cluster group *name*

示例：

```
ciscoasa(config)# cluster group pod1
```

步骤 2 启用集群。

enable

退出集群

要完全退出集群，需要删除整个集群引导程序配置。由于每个节点上的当前配置相同（从主用设备同步），因此退出集群就意味着要么从备份恢复集群前的配置，要么清除现有配置并重新开始配置以免 IP 地址冲突。

过程

步骤 1 对于数据节点，禁用集群：

cluster group *cluster_name* **no enable**

示例：

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)# no enable
```

在数据节点上启用集群时，您无法进行配置更改。

步骤 2 清除集群配置：

clear configure cluster

ASA 将关闭所有接口，包括管理接口和集群控制链路。

步骤 3 禁用集群接口模式：

no cluster interface-mode

模式并非存储于配置中，因此必须手动重置。

步骤 4 如果有备份配置，可将备份配置复制到正在运行的配置中：

copy *backup_cfg* **running-config**

示例：

```
ciscoasa(config)# copy backup_cluster.cfg running-config

Source filename [backup_cluster.cfg]?

Destination filename [running-config]?
ciscoasa(config)#
```

步骤 5 将配置保存到启动配置：

write memory

步骤 6 如果没有备份配置，请重新配置管理访问。例如，确保更改接口 IP 地址，并恢复正确的主机名。

更改控制节点

⚠

注意 要更改控制节点，最好的方法是在控制节点上禁用集群，等到新的控制选举后再重新启用集群。如果必须指定要成为控制节点的具体节点，请使用本节中的程序。但是请注意，对集中功能而言，如果使用本程序强制更改控制节点，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。

要更改控制节点，请执行以下步骤：

过程

将新节点设置为控制节点：

cluster control-node unit*node_name*

示例：

```
ciscoasa(config)# cluster control-node unit asa2
```

您需要重新连接到主集群 IP 地址。

要查看成员名称，请输入 **cluster control-node unit ?**（可查阅除当前节点之外的所有名称），或输入 **show cluster info** 命令。

在集群范围内执行命令

要向集群中的所有节点或某个特定节点发送命令，请执行以下步骤。向所有节点发送 **show** 命令以收集所有输出并将其显示在当前节点的控制台上。也可在整个集群范围内执行其他命令（如 **capture** 和 **copy**）。

过程

发送命令到所有节点，或者如果指定了节点名称，则发送到特定节点：

cluster exec [**unit** *node_name*] *command*

示例：

```
ciscoasa# cluster exec show xlate
```

要查看节点名称，请输入 **cluster exec unit ?**（可查阅除当前节点之外的所有名称），或输入 **show cluster info** 命令。

示例

要同时将同一捕获文件从集群中的所有节点复制到TFTP服务器，请在控制节点上输入以下命令：

```
ciscoasa# cluster exec copy /pcap capture: tftp://10.1.1.56/capture1.pcap
```

多个PCAP文件（一个文件来自一个节点）将复制到TFTP服务器。目标捕获文件名会自动附加节点名称，例如capture1_asa1.pcap、capture1_asa2.pcap等。在本例中，asa1和asa2是集群节点名称。

监控集群

您可以监控集群状态和连接并排除故障。

监控集群状态

请参阅以下命令来监控集群状态：

- **show cluster info** [**health** [**details**]]

  如果没有关键字，**show cluster info** 命令将显示所有集群成员的状态。

  show cluster info health 命令将显示接口、节点和整个集群的当前运行状况。**details** 关键字显示心跳消息失败的次数。

  请参阅 **show cluster info** 命令的以下输出：

```
ciscoasa# show cluster info
Cluster stbu: On
  This is "C" in state DATA_NODE
      ID        : 0
      Site ID   : 1
            Version   : 9.4(1)
      Serial No.: P3000000025
      CCL IP    : 10.0.0.3
      CCL MAC   : 000b.fcf8.c192
      Last join : 17:08:59 UTC Sep 26 2011
      Last leave: N/A
Other members in the cluster:
  Unit "D" in state DATA_NODE
      ID        : 1
      Site ID   : 1
```

```
            Version   : 9.4(1)
        Serial No.: P3000000001
        CCL IP    : 10.0.0.4
        CCL MAC   : 000b.fcf8.c162
        Last join : 19:13:11 UTC Sep 23 2011
        Last leave: N/A
    Unit "A" in state CONTROL_NODE
        ID        : 2
        Site ID   : 2
            Version   : 9.4(1)
        Serial No.: JAB0815R0JY
        CCL IP    : 10.0.0.1
        CCL MAC   : 000f.f775.541e
        Last join : 19:13:20 UTC Sep 23 2011
        Last leave: N/A
    Unit "B" in state DATA_NODE
        ID        : 3
        Site ID   : 2
            Version   : 9.4(1)
        Serial No.: P3000000191
        CCL IP    : 10.0.0.2
        CCL MAC   : 000b.fcf8.c61e
        Last join : 19:13:50 UTC Sep 23 2011
        Last leave: 19:13:36 UTC Sep 23 2011
```

- **show cluster info auto-join**

  显示集群节点是否将在一段延迟后自动重新加入集群，以及是否已清除故障条件（例如等待许可证、机箱运行状况检查失败，等等）。如果节点已永久禁用，或节点已在集群中，则此命令将不会显示任何输出。

  请参阅 **show cluster info auto-join** 命令的以下输出：

```
ciscoasa(cfg-cluster)# show cluster info auto-join
Unit will try to join cluster in 253 seconds.
Quit reason: Received control message DISABLE

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit will try to join cluster when quit reason is cleared.
Quit reason: Control node has application down that data node has up.

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit will try to join cluster when quit reason is cleared.
Quit reason: Chassis-blade health check failed.

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit will try to join cluster when quit reason is cleared.
Quit reason: Service chain application became down.

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit will try to join cluster when quit reason is cleared.
Quit reason: Unit is kicked out from cluster because of Application health check failure.


ciscoasa(cfg-cluster)# show cluster info auto-join
Unit join is pending (waiting for the smart license entitlement: ent1)

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit join is pending (waiting for the smart license export control flag)
```

- **show cluster info transport**{**asp** |**cp** [**detail**]}

  显示以下项目传输相关的统计信息：

  - **asp** — 数据平面传输统计信息。
  - **cp** — 控制平面传输统计信息。

    如果您输入 **detail** 关键字，您可以查看集群可靠传输协议的使用情况，以便确定控制平面中的缓冲区已满时的丢包问题。请参阅 **show cluster info transport cp detail** 命令的以下输出：

```
ciscoasa# show cluster info transport cp detail
Member ID to name mapping:
  0 - unit-1-1   2 - unit-4-1   3 - unit-2-1

Legend:
  U    - unreliable messages
  UE   - unreliable messages error
  SN   - sequence number
  ESN  - expecting sequence number
  R    - reliable messages
  RE   - reliable messages error
  RDC  - reliable message deliveries confirmed
  RA   - reliable ack packets received
  RFR  - reliable fast retransmits
  RTR  - reliable timer-based retransmits
  RDP  - reliable message dropped
  RDPR - reliable message drops reported
  RI   - reliable message with old sequence number
  RO   - reliable message with out of order sequence number
  ROW  - reliable message with out of window sequence number
  ROB  - out of order reliable messages buffered
  RAS  - reliable ack packets sent

This unit as a sender
-------------------------
        all       0         2         3
  U     123301    3867966   3230662   3850381
  UE    0         0         0         0
  SN    1656a4ce  acb26fe   5f839f76  7b680831
  R     733840    1042168   852285    867311
  RE    0         0         0         0
  RDC   699789    934969    740874    756490
  RA    385525    281198    204021    205384
  RFR   27626     56397     0         0
  RTR   34051     107199    111411    110821
  RDP   0         0         0         0
  RDPR  0         0         0         0

This unit as a receiver of broadcast messages
----------------------------------------------
        0         2         3
  U     111847    121862    120029
  R     7503      665700    749288
  ESN   5d75b4b3  6d81d23   365ddd50
  RI    630       34278     40291
  RO    0         582       850
  ROW   0         566       850
  ROB   0         16        0
  RAS   1571      123289    142256
```

```
This unit as a receiver of unicast messages
-------------------------------------------
        0         2         3
  U     1         3308122   4370233
  R     513846    879979    1009492
  ESN   4458903a  6d841a84  7b4e7fa7
  RI    66024     108924    102114
  RO    0         0         0
  ROW   0         0         0
  ROB   0         0         0
  RAS   130258    218924    228303

Gated Tx Buffered Message Statistics
------------------------------------
    current sequence number: 0

    total:                   0
    current:                 0
    high watermark:          0

    delivered:               0
    deliver failures:        0

    buffer full drops:       0
    message truncate drops:  0

    gate close ref count:    0

    num of supported clients:45

MRT Tx of broadcast messages
============================
Message high watermark: 3%
  Total messages buffered at high watermark: 5677
  [Per-client message usage at high watermark]
  ------------------------------------------------------------
  Client name                          Total messages  Percentage
  Cluster Redirect Client                        4153         73%
  Route Cluster Client                            419          7%
  RRI Cluster Client                             1105         19%

Current MRT buffer usage: 0%
  Total messages buffered in real-time: 1
  [Per-client message usage in real-time]
  Legend:
        F - MRT messages sending when buffer is full
        L - MRT messages sending when cluster node leave
        R - MRT messages sending in Rx thread
  ------------------------------------------------------------------------------
  Client name                          Total messages  Percentage    F   L   R
  VPN Clustering HA Client                          1        100%    0   0   0

MRT Tx of unitcast messages(to member_id:0)
===========================================
Message high watermark: 31%
  Total messages buffered at high watermark: 4059
  [Per-client message usage at high watermark]
  ------------------------------------------------------------
  Client name                          Total messages  Percentage
  Cluster Redirect Client                        3731         91%
  RRI Cluster Client                              328          8%

Current MRT buffer usage: 29%
  Total messages buffered in real-time: 3924
```

```
  [Per-client message usage in real-time]
  Legend:
        F - MRT messages sending when buffer is full
        L - MRT messages sending when cluster node leave
        R - MRT messages sending in Rx thread
  ------------------------------------------------------------------------------
  Client name                          Total messages  Percentage    F   L   R
  Cluster Redirect Client                        3607         91%    0   0   0
  RRI Cluster Client                              317          8%    0   0   0

MRT Tx of unitcast messages(to member_id:2)
==========================================
Message high watermark: 14%
  Total messages buffered at high watermark: 578
  [Per-client message usage at high watermark]
  ---------------------------------------------------------------
  Client name                          Total messages  Percentage
  VPN Clustering HA Client                       578        100%

Current MRT buffer usage: 0%
  Total messages buffered in real-time: 0

MRT Tx of unitcast messages(to member_id:3)
==========================================
Message high watermark: 12%
  Total messages buffered at high watermark: 573
  [Per-client message usage at high watermark]
  ---------------------------------------------------------------
  Client name                          Total messages  Percentage
  VPN Clustering HA Client                       572         99%
  Cluster VPN Unique ID Client                     1          0%

Current MRT buffer usage: 0%
  Total messages buffered in real-time: 0
```

- **show cluster history**

  显示集群历史记录，以及有关集群节点加入失败的原因或节点离开集群的原因的错误消息。

在集群范围捕获数据包

有关在集群中捕获数据包的信息，请参阅以下命令：

cluster exec capture

要支持集群范围的故障排除，您可以使用 **cluster exec capture** 命令在控制节点上启用捕获集群特定流量的功能，随后集群中的所有数据节点上将自动启用此功能。

监控集群资源

请参阅以下命令以监控集群资源：

show cluster {**cpu** | **memory** | **resource**} [*options*]

显示整个集群的聚合数据。可用 *options* 取决于数据类型。

监控集群流量

请参阅以下命令以监控集群流量：

- **show conn [detail], cluster exec show conn**

  show conn 命令显示一个传输是导向者、备用还是转发者传输。在任意节点上使用 **cluster exec show conn** 命令可查看所有连接。此命令可以显示单个流的流量到达集群中不同 ASA 的方式。集群的吞吐量取决于负载均衡的效率和配置。此命令可以让您很方便地查看某个连接的流量如何流经集群，也可以帮助您了解负载均衡器对传输的性能有何影响。

  show conn detail 命令还显示哪些流应 遵守流移动性。

  以下是 **show conn detail** 命令的输出示例：

```
ciscoasa/ASA2/data node# show conn detail
12 in use, 13 most used
Cluster stub connections: 0 in use, 46 most used
Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
       B - initial SYN from outside, b - TCP state-bypass or nailed,
       C - CTIQBE media, c - cluster centralized,
       D - DNS, d - dump, E - outside back connection, e - semi-distributed,
       F - outside FIN, f - inside FIN,
       G - group, g - MGCP, H - H.323, h - H.225.0, I - inbound data,
       i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
       k - Skinny media, L - LISP triggered flow owner mobility,
       M - SMTP data, m - SIP media, n - GUP
       O - outbound data, o - offloaded,
       P - inside back connection,
       Q - Diameter, q - SQL*Net data,
       R - outside acknowledged FIN,
       R - UDP SUNRPC, r - inside acknowledged FIN, S - awaiting inside SYN,
       s - awaiting outside SYN, T - SIP, t - SIP transient, U - up,
       V - VPN orphan, W - WAAS,
       w - secondary domain backup,
       X - inspected by service module,
       x - per session, Y - director stub flow, y - backup stub flow,
       Z - Scansafe redirection, z - forwarding stub flow
ESP outside: 10.1.227.1/53744 NP Identity Ifc: 10.1.226.1/30604, , flags c, idle 0s,
uptime
1m21s, timeout 30s, bytes 7544, cluster sent/rcvd bytes 0/0, owners (0,255) Traffic
received
at interface outside Locally received: 7544 (93 byte/s) Traffic received at interface
NP
Identity Ifc Locally received: 0 (0 byte/s) UDP outside: 10.1.227.1/500 NP Identity
Ifc:
10.1.226.1/500, flags -c, idle 1m22s, uptime 1m22s, timeout 2m0s, bytes 1580, cluster
sent/rcvd bytes 0/0, cluster sent/rcvd total bytes 0/0, owners (0,255) Traffic received
 at
interface outside Locally received: 864 (10 byte/s) Traffic received at interface NP
Identity
Ifc Locally received: 716 (8 byte/s)
```

  要对连接流进行故障排除，请先在任意节点上输入 **cluster exec show conn** 命令查看所有节点上的连接。寻找具有以下标志的流：导向者 (Y)、备用 (y) 和转发者 (z)。下例显示了三台 ASA 上的一条从 172.18.124.187:22 到 192.168.103.131:44727 的 SSH 连接；ASA 1 带有 z 标志，表示其是该连接的转发者；ASA3 带有 Y 标志，表示其是该连接的导向者；而 ASA2 则没有特殊的标志，表示其是所有者。在出站方向，此连接的数据包进入 ASA2 上的内部接口并从外部接口流

出。在入站方向，此连接的数据包进入 ASA 1 和 ASA3 上的外部接口，通过集群控制链路被转发到 ASA2，然后流出 ASA2 上的内部接口。

```
ciscoasa/ASA1/control node# cluster exec show conn
ASA1(LOCAL):**************************************************************
18 in use, 22 most used
Cluster stub connections: 0 in use, 5 most used
TCP outside  172.18.124.187:22 inside  192.168.103.131:44727, idle 0:00:00, bytes
37240828, flags z


ASA2:**************************************************************
12 in use, 13 most used
Cluster stub connections: 0 in use, 46 most used
TCP outside  172.18.124.187:22 inside  192.168.103.131:44727, idle 0:00:00, bytes
37240828, flags UIO


ASA3:**************************************************************
10 in use, 12 most used
Cluster stub connections: 2 in use, 29 most used
TCP outside  172.18.124.187:22 inside  192.168.103.131:44727, idle 0:00:03, bytes 0,
flags  Y
```

- **show cluster info** [**conn-distribution** | **packet-distribution** | **loadbalance** | **flow-mobility counters**]

  show cluster info conn-distribution 和 **show cluster info packet-distribution** 命令显示流量在所有集群节点上的分布。这些命令可以帮助您评估和调整外部负载均衡器。

  show cluster info loadbalance 命令显示连接再均衡统计信息。

  The **show cluster info flow-mobility counters** 命令显示 EID 移动和流所有者移动信息。请参阅 **show cluster info flow-mobility counters** 的以下输出：

```
ciscoasa# show cluster info flow-mobility counters
EID movement notification received  : 4
EID movement notification processed : 4
Flow owner moving requested         : 2
```

- **show cluster info load-monitor** [**details**]

  show cluster info load-monitor 命令显示最后一个间隔的集群成员的流量负载，以及已配置的总间隔数（默认情况下为 30）。使用 **details** 关键字查看每个时间间隔的每个度量值。

```
ciscoasa(cfg-cluster)# show cluster info load-monitor
ID  Unit Name
0  B
1  A_1
Information from all units with 20 second interval:
Unit     Connections    Buffer Drops   Memory Used   CPU Used
Average from last 1 interval:
   0           0            0            14              25
   1           0            0            16              20
Average from last 30 interval:
   0           0            0            12              28
   1           0            0            13              27


ciscoasa(cfg-cluster)# show cluster info load-monitor details
```

```
ID  Unit Name

 0  B

 1  A_1

Information from all units with 20 second interval


Connection count captured over 30 intervals:

Unit ID  0

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0

Unit ID  1

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0


Buffer drops captured over 30 intervals:

Unit ID  0

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0

Unit ID  1

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0
```

```
          0          0          0          0          0          0


Memory usage(%) captured over 30 intervals:

Unit ID  0
         25         25         30         30         30         35
         25         25         35         30         30         30
         25         25         30         25         25         35
         30         30         30         25         25         25
         25         20         30         30         30         30
Unit ID  1
         30         25         35         25         30         30
         25         25         35         25         30         35
         30         30         35         30         30         30
         25         20         30         25         25         30
         20         30         35         30         30         35


CPU usage(%) captured over 30 intervals:

Unit ID  0
         25         25         30         30         30         35
         25         25         35         30         30         30
         25         25         30         25         25         35
         30         30         30         25         25         25
         25         20         30         30         30         30
Unit ID  1
         30         25         35         25         30         30
         25         25         35         25         30         35
         30         30         35         30         30         30
         25         20         30         25         25         30
         20         30         35         30         30         35
```

- **show cluster** {**access-list** | **conn** | **traffic** | **user-identity** | **xlate**} [*options*]

  显示整个集群的聚合数据。可用 *options* 取决于数据类型。

  请参阅 **show cluster access-list** 命令的以下输出：

```
ciscoasa# show cluster access-list
hitcnt display order: cluster-wide aggregated result, unit-A, unit-B,  unit-C, unit-D
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096) alert-interval
 300
access-list 101; 122 elements; name hash: 0xe7d586b5
access-list 101 line 1 extended permit tcp 192.168.143.0 255.255.255.0 any eq www
(hitcnt=0, 0, 0, 0, 0) 0x207a2b7d
access-list 101 line 2 extended permit tcp any 192.168.143.0 255.255.255.0 (hitcnt=0,
0, 0, 0, 0) 0xfe4f4947
access-list  101 line 3 extended permit tcp host 192.168.1.183 host 192.168.43.238
(hitcnt=1, 0, 0, 0, 1) 0x7b521307
access-list 101 line 4 extended permit tcp host 192.168.1.116 host 192.168.43.238
(hitcnt=0, 0, 0, 0, 0) 0x5795c069
access-list 101 line 5 extended permit tcp host 192.168.1.177 host 192.168.43.238
(hitcnt=1, 0, 0, 1, 0) 0x51bde7ee
access list 101 line 6 extended permit tcp host 192.168.1.177 host 192.168.43.13
(hitcnt=0, 0, 0, 0, 0) 0x1e68697c
access-list 101 line 7 extended permit tcp host 192.168.1.177 host 192.168.43.132
(hitcnt=2, 0, 0, 1, 1) 0xc1ce5c49
access-list 101 line 8 extended permit tcp host 192.168.1.177 host 192.168.43.192
(hitcnt=3, 0, 1, 1, 1) 0xb6f59512
access-list 101 line 9 extended permit tcp host 192.168.1.177 host 192.168.43.44
(hitcnt=0, 0, 0, 0, 0) 0xdc104200
access-list 101 line 10 extended permit tcp host 192.168.1.112 host 192.168.43.44
(hitcnt=429, 109, 107, 109, 104)
0xce4f281d
access-list 101 line 11 extended permit tcp host 192.168.1.170 host 192.168.43.238
(hitcnt=3, 1, 0, 0, 2) 0x4143a818
access-list 101 line 12 extended permit tcp host 192.168.1.170 host 192.168.43.169
(hitcnt=2, 0, 1, 0, 1) 0xb18dfea4
access-list 101 line 13 extended permit tcp host 192.168.1.170 host 192.168.43.229
(hitcnt=1, 1, 0, 0, 0) 0x21557d71
access-list 101 line 14 extended permit tcp host 192.168.1.170 host 192.168.43.106
(hitcnt=0, 0, 0, 0, 0) 0x7316e016
access-list 101 line 15 extended permit tcp host 192.168.1.170 host 192.168.43.196
(hitcnt=0, 0, 0, 0, 0) 0x013fd5b8
access-list 101 line 16 extended permit tcp host 192.168.1.170 host 192.168.43.75
(hitcnt=0, 0, 0, 0, 0) 0x2c7dba0d
```

要显示所有节点在用连接的汇聚计数，请输入：

```
ciscoasa# show cluster conn count
Usage Summary In Cluster:*********************************************
  200 in use (cluster-wide aggregated)
     cl2(LOCAL):************************************************************
  100 in use, 100 most used

  cl1:************************************************************************
  100 in use, 100 most used
```

- **show asp cluster counter**

  此命令对于数据路径故障排除非常有用。

监控集群路由

有关集群路由的信息，请参阅以下命令：

- **show route cluster**
- **debug route cluster**

  显示集群的路由信息。

- **show lisp eid**

  显示 ASA EID 表，表中显示了 EID 和站点 ID。

  请参阅 **cluster exec show lisp eid** 命令的以下输出。

```
ciscoasa# cluster exec show lisp eid
L1(LOCAL):*************************************************************
     LISP EID       Site ID
    33.44.33.105        2
    33.44.33.201        2
    11.22.11.1             4
    11.22.11.2             4
L2:*************************************************************************
     LISP EID       Site ID
    33.44.33.105        2
    33.44.33.201        2
    11.22.11.1   4
    11.22.11.2  4
```

- **show asp table classify domain inspect-lisp**

  该命令对于故障排除非常有用。

配置集群日志记录

有关为集群配置日志记录的信息，请参阅以下命令：

logging device-id

集群中的每个节点将独立生成系统日志消息。您可以使用 **logging device-id** 命令来生成具有相同或不同设备 ID 的系统日志消息，以使消息看上去是来自集群中的相同或不同节点。

监控集群接口

请参阅以下用于监控集群接口的命令：

- **show cluster interface-mode**

  显示集群接口模式。

调试集群

请参阅以下用于调试集群的命令：

- **debug cluster [ccp | datapath | fsm | general | hc | license | rpc | transport]**

  显示集群的调试消息。

- **debug cluster flow-mobility**

  显示与集群流移动性相关的事件。

- **debug lisp eid-notify-intercept**

  当 eid-notify 被拦截时显示事件。

- **show cluster info trace**

  show cluster info trace 命令显示调试信息，供进一步排除故障之用。

  请参阅 **show cluster info trace** 命令的以下输出：

```
ciscoasa# show cluster info trace
 Feb 02 14:19:47.456 [DBUG]Receive CCP message: CCP_MSG_LOAD_BALANCE
 Feb 02 14:19:47.456 [DBUG]Receive CCP message: CCP_MSG_LOAD_BALANCE
 Feb 02 14:19:47.456 [DBUG]Send CCP message to all: CCP_MSG_KEEPALIVE from 80-1 at
CONTROL_NODE
```

集群参考

本部分包括有关集群工作原理的详细信息。

ASA 功能和集群

部分 ASA 功能不受 ASA 集群支持，还有部分功能仅在控制节点上受支持。其他功能可能对如何正确使用规定了注意事项。

集群不支持的功能

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。

- 依靠 TLS 代理实现的统一通信功能
- 远程接入 VPN（SSL VPN 和 IPsec VPN）
- 虚拟隧道接口 (VTI)
- 以下应用检查：
  - CTIQBE
  - H323、H225 和 RAS
  - IPsec 穿透
  - MGCP
  - MMP
  - RTSP

- SCCP（瘦客户端）
- WAAS
- WCCP

- 僵尸网络流量过滤器
- 自动更新服务器
- DHCP 客户端、服务器和代理。支持 DHCP 中继。
- VPN 负载均衡
- 故障切换
- 集成路由和桥接
- FIPS 型号

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。

- 以下应用检查：
  - DCERPC
  - ESMTP
  - IM
  - NetBIOS
  - PPTP
  - RADIUS
  - RSH
  - SNMP
  - SQLNET
  - SUNRPC

- TFTP
- XDMCP

- 静态路由监控
- 网络访问的身份验证和授权。记帐被分散。
- 筛选服务
- 站点到站点 VPN
- 组播路由

应用到单个节点的功能

这些功能将应用到每个 ASA 节点而非整个集群或控制节点。

- QoS - QoS 策略将于配置复制过程中在集群中同步。但是，该策略是在每个节点上独立执行。例如，如果对输出配置管制，则要对流出特定 ASA 的流量应用符合规则的速率和符合规则的突发量值。在包含 3 个节点且流量均衡分布的集群中，符合规则的速率实际上变成了集群速率的 3 倍。
- 威胁检测 - 威胁检测在各节点上独立工作；例如，排名统计信息就要视具体节点而定。以端口扫描检测为例，由于扫描的流量将在所有节点间进行负载均衡，而一个节点无法看到所有流量，因此端口扫描检测无法工作。

用于网络访问的 AAA 和集群

用于网络访问的 AAA 由三部分组成：身份验证、授权和记账。身份验证和授权作为集中功能在集群控制节点上实施，且数据结构复制到集群数据节点。如果选举出控制节点，新的控制节点将拥有所需的所有信息，以继续不间断运行经过验证的既有用户及其相关授权。当控制节点发生变化时，用户身份验证的空闲和绝对超时将保留。

记账作为分散的功能在集群中实施。记账按每次流量完成，因此在为流量配置记账时，作为流量所有者的集群节点会将记账开始和停止消息发送到 AAA 服务器。

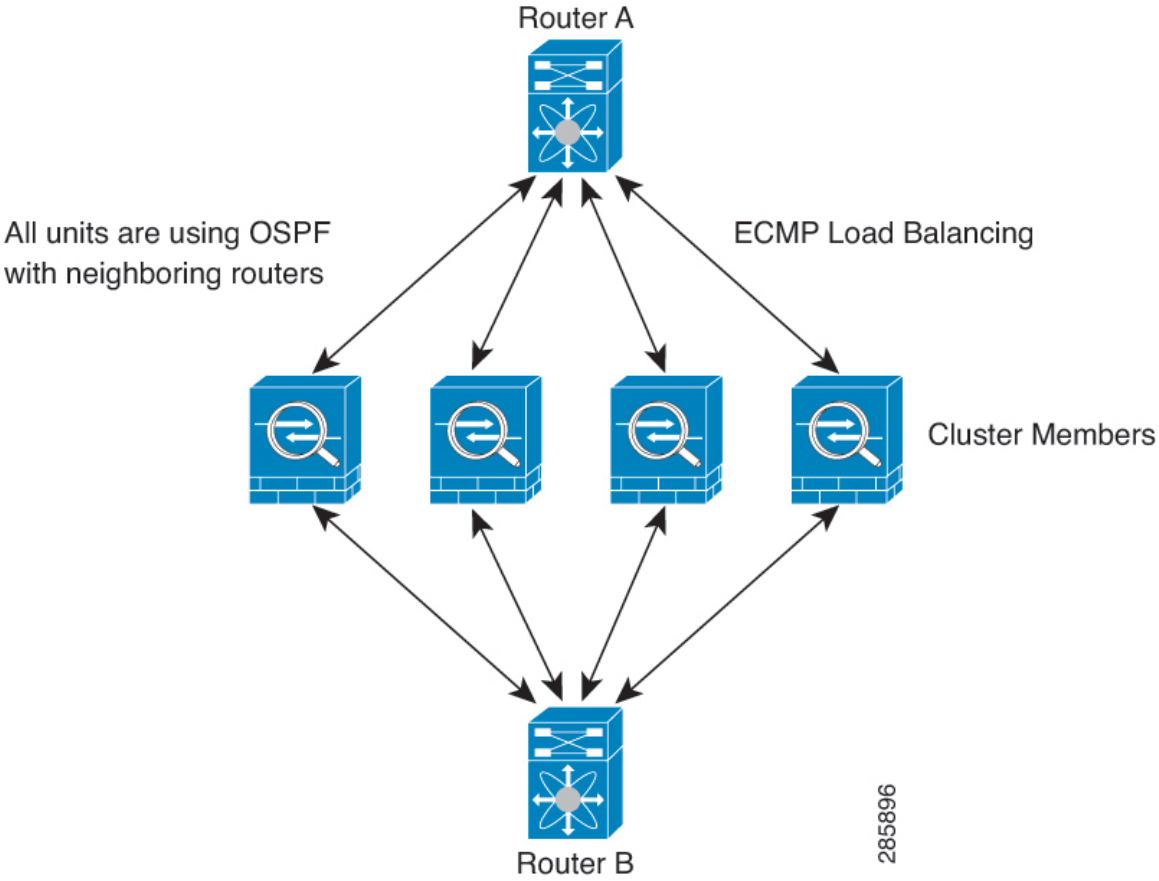
连接设置和集群

连接限制在集群范围强制实施（请参阅 **set connection conn-max**、**set connection embryonic-conn-max**、**set connection per-client-embryonic-max** 和 **set connection per-client-max** 命令）。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 2: 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台 ASA。ECMP 用于在这 4 条路径之间对流量执行负载均衡。每台 ASA 在与外部路由器通信时，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。

EIGRP 与单个接口模式下的集群对等体不构成邻居关系。

注释 如果该集群为实现冗余有多个设备与同一个路由器相邻，则非对称路由可能会造成不可接受的流量损失。要避免非对称路由，请将所有这些 ASA 接口分组到同一流量区域中。

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。
- 如果您将 AAA 用于 FTP 访问，则控制通道流集中在控制节点上。

ICMP检测和集群

ICMP 和 ICMP 错误数据包通过集群的流取决于是否启用 ICMP/ICMP 错误检查。不启用 ICMP 检查时，ICMP 是单向流，并且不支持导向器流。启用ICMP检查时，ICMP流变为双向流，并由导向器/备份流支持。被检查的ICMP流的一个不同之处在于导向器对转发数据包的处理：导向器会将ICMP回应应答数据包转发给流所有者，而不是将数据包返回给转发器。

组播路由和集群

在独立接口模式下，设备并不单独处理组播。所有数据和路由数据包都由控制设备进行处理和转发，从而避免数据包复制。

NAT 和集群

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 ASA，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 ASA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。这对跨网络 EtherChannel 来说不是问题，因为只有一个 IP 地址与集群接口关联。

- 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。
- 每会话 PAT 功能 - 每会话 PAT 功能并非集群专用功能，但它能提高 PAT 的可扩展性，而且对集群而言，它允许每个数据节点成为 PAT 连接的所有者；相比之下，多会话 PAT 连接则必须转发到控制节点并由控制节点所有。默认情况下，所有 TCP 流量和 UDP DNS 流量均使用每会话 PAT 转换，而 ICMP 和所有其他 UDP 流量均使用多会话。您可以为 TCP 和 UDP 配置每会话 NAT 规则以更改这些默认设置，但是，您不能为 ICMP 配置每会话 PAT。对于使用多会话 PAT 的流量（例如 H.323、SIP 或 Skinny），您可以禁用关联 TCP 端口的每会话 PAT（这些 H.323 和 SIP 的 UDP 端口已默认为多会话）。有关每会话 PAT 的详细信息，请参阅防火墙配置指南。
- 对以下检查不使用静态 PAT：
  - FTP
  - PPTP
  - 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。

SCTP 和集群

SCTP 关联可以在任何节点上创建（由于负载均衡），但其多宿主连接必须位于同一节点上。

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。

不支持 TLS 代理配置。

SNMP 和集群

SNMP 代理按照本地 IP 地址轮询每一个ASA。您无法轮询集群的合并数据。

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。您必须在控制节点上重新添加它们以强制用户复制到新节点，或者直接在数据节点上复制。

STUN 和集群

故障转移和集群模式支持 STUN 检查，因为针孔被复制。但是，节点之间不进行事务 ID 的复制。如果节点在收到 STUN 请求后发生故障，并且另一个节点收到 STUN 响应，则该 STUN 响应将被丢弃。

系统日志和集群

- 系统日志 - 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。
- NetFlow - 集群中的每个节点都会生成自己的 NetFlow 数据流。NetFlow 收集器只能将每台 ASA 视为单独的 NetFlow 导出器。

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。

VPN 和集群

站点到站点 VPN 是集中功能；只有控制节点支持 VPN 连接。

注释 集群不支持远程接入 VPN。

VPN 功能仅限控制节点使用，且不能利用集群的高可用性功能。如果控制节点发生故障，所有现有的 VPN 连接都将断开，VPN 用户将遇到服务中断。选择新的控制节点后，必须重新建立 VPN 连接。

对于使用 PBR 或 ECMP 时与独立接口的连接，您必须始终连接到主集群 IP 地址而非本地地址。

与 VPN 相关的密钥和证书将被复制到所有节点。

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。

当您启用运行状况监控时，默认情况下会监控所有物理接口；您可以选择按接口禁用监控。只能监控已命名接口。

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。ASA 在多长时间后从集群中删除成员取决于该节点是既定成员还是正在加入集群的设备。ASA 在节点加入集群后的最初 90 秒不监控接口。在此期间的接口状态更改不会导致 ASA 从集群中删除。无论状态如何，节点都会在 500 毫秒后被删除。

发生故障后的状态

当集群中的节点发生故障时，该节点承载的连接将无缝转移到其他节点；流量的状态信息将通过控制节点的集群控制链路共享。

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。

ASA将自动尝试重新加入集群，具体取决于故障事件。

注释 当ASA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，仅管理专用接口可以发送和接收流量。管理接口将保持打开，使用节点从集群 IP 池接收的 IP 地址。但是，如果您重新加载而节点在集群中仍然处于非活动状态，管理接口将被禁用。您必须使用控制台端口来进行任何进一步配置。

重新加入集群

当集群节点从集群中删除之后，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，您必须通过在 CLI 输入 **cluster group***name*，然后输入 **enable** 来重新启用集群 ，以手动重新加入集群。
- 加入集群后出现故障的集群控制链路 - ASA 无限期地每 5 分钟自动尝试重新加入。此行为是可配置的。
- 出现故障的数据接口 - ASA 尝试在 5 分钟时、然后在 10 分钟时、最后在 20 分钟时重新加入。如果 20 分钟后仍加入失败，ASA 将禁用集群。解决数据接口问题之后，您必须在 CLI 上通过输入**cluster group** *name*，然后输入**enable** 来手动启用集群。此行为是可配置的。
- 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，临时电源故障意味节点将在重新启动时重新加入集群，只要集群控制链路打开并且仍然使用 **enable** 命令启用集群。ASA 每 5 秒钟尝试重新加入集群。
- 内部错误 - 内部故障包括：应用同步超时；应用状态不一致等。节点将尝试以下列间隔自动重新加入集群：5 分钟，10 分钟，然后是 20 分钟。此行为是可配置的。

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 *2:* 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	包括 AAA 规则 (uauth) 。
IPv6 邻居数据库	是	—
动态路由	是	—
SNMP 引擎 ID	否	-
适用于 Firepower 4100/9300的分布式 VPN（站点间）	是	备用会话成为主用会话，并创建一个新的备用会话。

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。

如果您对站点间集群启用导向器本地化，则有两个备用所有者角色：本地备用和全局备用。所有者始终选择与自身位于同一站点（基于站点 ID）的本地备用。全局备用可以位于任何站点，甚至可以与本地备用是同一个节点。所有者向两个备用所有者发送连接状态信息。

如果启用站点冗余，并且备用所有者与所有者位于同一站点，则将从另一个站点选择一个额外的备用所有者来保护流量免受站点故障的影响。机箱备份和站点备份是独立的，因此流量在某些情况将同时具有机箱备份和站点备份。

- 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。

  如果您对站点间集群启用导向器本地化，则有两个导向器角色：本地导向器和全局导向器。所有者始终选择与它自身位于同一站点（基于站点 ID）的本地导向器。全局导向器可以位于任何站点，甚至可以与本地导向器是同一节点。如果原始所有者发生故障，本地导向器将在同一站点选择新的连接所有者。

  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。如果启用导向器本地化，转发器将始终向本地导向器查询。如果本地导向器未获知所有者，例如，当集群成员收到所有者位于其他站点上的连接的数据包时，转发者将仅查询全局导向器。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。

当连接使用端口地址转换 (PAT) 时，PAT 类型（每会话或多会话）会对哪个集群成员将成为新连接的所有者产生影响：

- 每会话 PAT - 所有者是接收连接中的初始数据包的节点。

  默认情况下，TCP 和 DNS UDP 流量均使用每会话 PAT。

- 多会话 PAT - 所有者始终是控制节点。如果多会话 PAT 连接最初由数据节点接收，则数据节点会将连接转发给控制节点。

  默认情况下，UDP（DNS UDP 除外）和 ICMP 流量使用多会话 PAT，因此这些连接始终归控制节点所有。

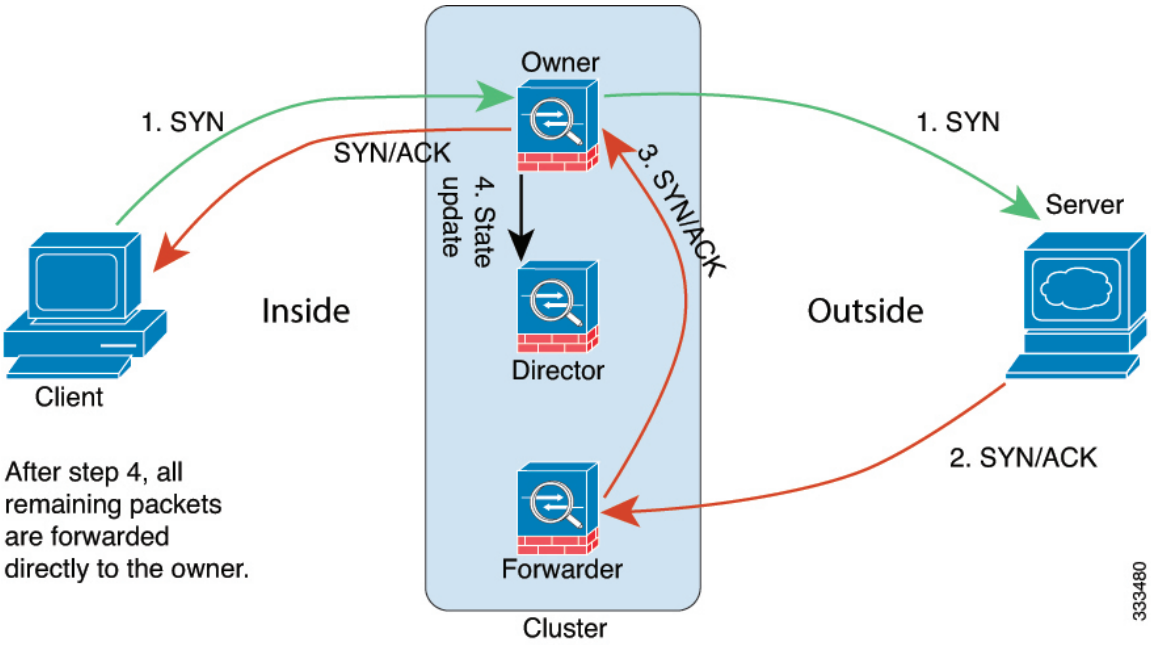
您可以更改 TCP 和 UDP 的每会话 PAT 默认设置，以便根据配置按每会话或多会话处理这些协议的连接。对于 ICMP，您不能更改默认的多会话 PAT。有关每会话 PAT 的详细信息，请参阅防火墙配置指南。

新连接所有权

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。如果该连接有任何数据包到达其他节点，这些数据包都会通过集群控制链路被转发到所有者节点。为了获得最佳性能，对于要到达同一个节点的流量的两个方向以及要在节点之间均摊的流量，都需要执行适当的外部负载均衡。如果反向流量到达其他节点，会被重定向回原始节点。

TCP 的数据流示例

以下图例显示了新连接的建立。

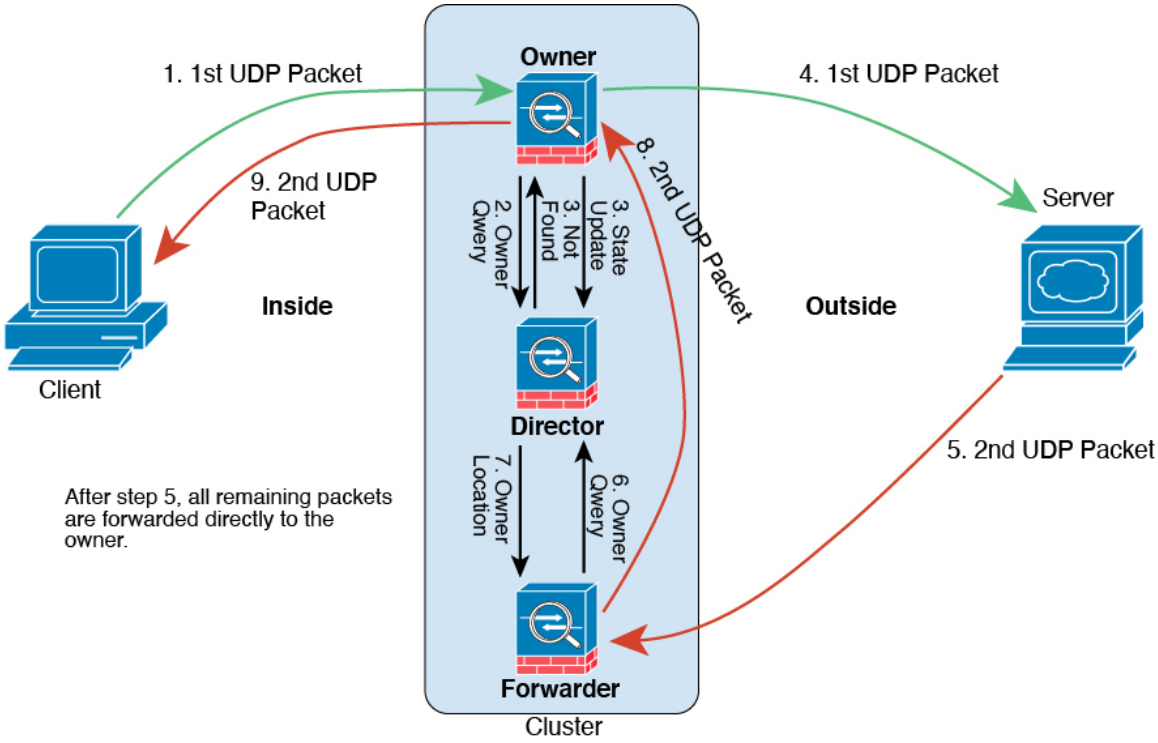


1. SYN 数据包从客户端发出，被传送到一台 ASA（基于负载均衡方法），该设备将成为所有者。所有者创建一个流量，将所有者信息编码为 SYN Cookie，然后将数据包转发到服务器。
2. SYN-ACK 数据包从服务器发出，被传送到一台不同的 ASA（基于负载均衡方法）。此 ASA是转发者。
3. 由于转发器不是该连接的所有者，因此它将解码 SYN Cookie 中的所有者信息，然后创建发往所有者的转发流量，并将 SYN-ACK 数据包转发到所有者。
4. 所有者将状态更新发送到导向器，然后将 SYN-ACK 数据包转发到客户端。
5. 导向器接收来自所有者的状态更新，创建发往所有者的流量，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 *3: 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ASA（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。

跨集群实现新 TCP 连接再均衡

如果上游或下游路由器的负载均衡功能导致流量分摊不均衡，您可以将过载的节点配置为将新的TCP流量重定向到其他节点。现有流量将不会移至其他节点。

关于公共云中的威胁防御虚拟集群的历史记录

特性	版本	详细信息
ASA 虚拟 Amazon Web Services (AWS) 集群	9.19(1)	ASA 虚拟支持 AWS 上最多 16 个节点的单个接口集群。无论是否有 AWS 网关负载均衡器，您都可以使用集群。

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。