DCYK 控制器群集手册

目录

修订记录

本文档修订内容列表.

修订	修订说明
Rev 01	初始发布

控制器群集

群集是多个托管设备协同工作的组合，可为所有客户端提供高可用性，并确保发生故障转移时的服务连续性。

AP 由单个受管设备管理。客户端负载由所有受管设备共享。集群的目标是在其一个或多个集群成员发生故障时为 AP 和无线客户端提供完全冗余。

群集中的所有成员都是活动的受管设备。

群集有助于实现大型漫游域，最大限度地减少容错域，并有助于快速恢复。

集群的目标是:

(1) 无缝园区漫游 — 当客户端在大型 L2 域内不同受管设备的 AP 之间漫游时，客户端将保留相同的子网和 IP 地址，以确保无缝漫游。客户端在整个漫游区域中仍锚定到集群中的单个托管设备，这使得其漫游体验无缝，因为它们的 L2 或 L3 信息和会话保留在同一托管设备上。

(2) 无中断客户端故障转移 - 当受管设备发生故障时，所有用户都会无缝故障转移到其备用受管设备，而不会中断其无线连接或现有的高价值会话。

(3) 客户端和 AP 负载均衡 — 当受管设备之间的工作负载过多时，客户端和 AP 负载在集群成员之间均匀平衡。客户端和 AP 均可无缝负载均衡。

以下各节介绍群集中支持的先决条件、关键注意事项和功能。

要求

群集仅在 Mobility Conductor 上受支持，群集成员只能是受管设备。

以下托管设备支持群集:

(1) 7200 系列控制器 — 支持集群中最多 12 个节点。

(2) 7000 系列控制器 — 一个集群中最多支持 4 个节点。

(3) 9004 控制器 — 一个集群中最多支持 4 个节点。

(4) 9012 控制器 — 一个集群中最多支持 4 个节点。

(5) 9240 控制器 — 支持集群中最多 12 个节点。

(6) Mobility Controller 虚拟设备 - 支持集群中最多 4 个节点。

即使使用 12 节点集群，支持的最大 AP 和客户端计数也分别限制为 10K 和 100K。

关键考虑因素

一些关键考虑因素包括:

(1) 群集中的所有受管设备都需要运行相同的软件版本。

(2) 如果启用了 HA-AP 快速故障切换，则无法启用群集。

(3) 远程 AP 支持 12 节点集群。从 神州云科 OS 8.6.0.0 开始，远程 AP 现在可以在具有 4 个以上节点的集群上终止。

(4) 不支持混合使用硬件设备和基于移动控制器虚拟设备的控制器。

(5) 只能使用相同的 SKU 型号设置移动控制器虚拟设备群集。Mobility Controller 虚拟设备仅支持同类群集。

(6) 由于两个控制器系列型号之间的容量存在差异，因此不建议在同一集群中混合使用 7200 系列控制器和 7000 系列控制器。但是，如果要从较小的集群（如 7000 系列控制器）迁移到具有 7200 系列控制器的较大集群，则可以在同一集群中使用这些设备。

(7) 9004 托管设备仅支持同类群集。

(8) 在群集中，受管设备不必完全相同。

(9) 受管设备可以是 L2 或 L3 连接，也可以是两者的混合。

(10) PSK-RAP 不支持群集。

(11) ClearPass Policy Manager 服务器中远程 AP 的外部允许列表数据库支持集群。

(12) 无需许可证即可启用群集功能。

(13) 独立控制器不支持群集。

(14) 支持园区 AP、远程 AP 和 Mesh AP。

(15) 启用群集时，拆分隧道模式虚拟 AP 和有线 AP 不支持强制网络门户。

(16) 当环回 IP 地址设置为控制器 IP 时，群集不起作用，因为群集进程不会从环回接口获取检测信号数据包。

(17) 集群在双栈部署中同时支持 IPv4 和 IPv6 AP。适用于园区 AP 和远程 AP。

支持同构集群

同构集群是使用相同平台类型的所有节点构建的集群。

集群 AP 容量

集群大小取决于所需的集群 AP 计数数，以确保每个 AP 都具有 AAC 和 S-AAC，这些 AAC 和 S-AAC 具有足够的容量供所有 AP 进行故障转移。此集群的建议 AP 负载应为集群总容量的一半。因此，集群 AP 计数应等于集群容量的 50%。

例如，如果集群由四个 7220 托管设备组成，则四个 7220 托管设备的总容量为 4096 个 AP，因此 AP 计数将为 2048。

支持异构集群

以下列表提供了当集群具有异构托管设备组合时集群容量（AP 和客户端）要考虑的要点。例如，7210、7220 和 7240 控制器。

(1) 禁用冗余时，群集中单个受管设备的总容量。

(2) 当群集节点涉及 7000 系列受管设备时，群集节点的数量限制为 4 个。

(3) 当 7200 系列托管设备添加到由其他 7000 系列托管设备组成的集群时，7200 系列托管设备的容量将减少到当前属于集群的 7000 系列托管设备的最大容量。

(4) 将 7000 系列托管设备添加到由 7200 系列托管设备组成的群集中时，将满足以下条件之一：

1. 如果群集中有三个以上的 7200 系列托管设备，则不允许 7000 系列托管设备加

入集群。

2. 如果 7200 系列托管设备上的当前 AP 或工作站计数大于新添加的 7000 系列托管设备上支持的最大 AP 或工作站容量，则不允许 7000 系列托管设备加入集群。要检查是否允许 7000 系列受管设备加入集群，请执行 show lc-cluster groupmembership 命令。
3. 如果 7200 系列受管设备上的当前 AP 或工作站计数小于新添加的 7000 系列受管设备上支持的最大 AP 或工作站容量，则群集中 7200 系列受管设备的容量将下降到 7000 系列受管设备上支持的最大容量，并且 7200 系列受管设备中现有支持的 AP 不受影响。

(5) 9240 受管设备不在异构群集中运行。

集群 AP 容量

集群 AP 大小应等于集群总容量的 50% 或最坏情况下负载的最小值。最坏的情况是，在最大容量的集群成员出现故障时，集群中其余节点处理的 AP 负载。

以下示例详细说明了如何根据受管设备的容量计算集群 AP 大小：

示例 1：

在具有一台 7220 托管设备和两台 7240 托管设备的群集中。7220 托管设备的容量为 1024,7240 托管设备的容量为 1024。现在，让我们计算总容量的 50% 为 （1024+1024 +1024 /2 = 1536 AP。现在，假设一个 7240 托管设备已关闭，因此，最坏情况负载为 （1024 + 1024） = 2048。

因此，此示例中的集群 AP 大小为 1536 个 AP，因为它是集群总容量的 50% 与最坏情况负载之间的最低值。

示例 2：

在具有两个 7210 托管设备和一个 7240 托管设备的集群中。7210 管理设备的容量为 512 个 AP，7240 管理设备的容量为 512 个 AP。因此，总容量的 50% 为 （512+512+512）/2=768 个 AP。现在，假设 7240 托管设备已关闭，因此，最坏情况负载为 （512+512） = 1024 AP。

因此，此示例中的集群 AP 大小为 1024 个 AP，因为它是集群总容量的 50% 与最坏情况负载之间的最低值。

群集连接类型

群集支持群集成员的以下两种连接类型：

(1) L2 连接 — 集群成员共享相同的用户 VLAN。每个节点上的所有用户 VLAN 也存在于所有节点中。

(2) L3 连接 — 集群成员不一定共享相同的用户 VLAN。某些用户 VLAN 在其他节点上不存在。

提示: 集群可以通过 L2 或 L3 网络形成。为简单起见，建议使用 L2。

角色

本部分介绍集群中成员的角色：

集群领导者

当多个托管设备形成群集时，这些设备会相互交换握手或你好消息以形成群集。当所有集群成员都位于完全连接的网格中时，将选出集群领导者。集群领导者是根据配置的优先级、平台值和设备的 MAC 地址派生的最高有效优先级选出的。

集群领导者计算哪个客户端映射到哪个集群成员。

当负载增加且集群成员之间的负载不平衡时，集群主节点还会动态、无缝地平衡客户端负载。集群领导者为客户端和 AP 识别备用托管设备，以确保无中断故障转移。

AAC - AP 锚点控制器

从单个 AP 的角度来看，此角色被赋予受管设备。这是 AP 的锚点。AP 使用其 LMS-IP 设置活动隧道，并且 AAC 负责处理 AP 及其无线电的所有管理功能。

UAC - 用户锚点控制器

这是用户的锚点。用户关联到 AP，AP 创建到客户端 UAC 的动态隧道。UAC 处理所有无线客户端流量，包括关联或取消关联通知、身份验证以及受管设备与客户端之间的所有单播流量。UAC 用于确保客户端在 AP 之间漫游时，托管设备在集群中保持不变。

S-AAC - 备用 AP 锚控制器

备用 AAC 是从其他集群成员动态分配的。AP 使用 S-AAC 建立备用隧道。如果 AAC 发生故障，S-AAC 会检测到故障，并确保 AP 故障转移到 S-AAC。在原 AAC 发生故障且 SAAC 成为新 AAC 后，集群主节点动态地为 AP 选择新的 S-AAC。

S-UAC - 备用用户锚控制器

从用户角度来看，这是备用托管设备。当活动 UAC 关闭时，用户故障转移到此托管设备。S-UAC 是当活动 UAC （A-UAC） 关闭时用户故障转移到此受管设备时分配给受管设备的角色。

锚定到单个受管设备

用户通过 AP 级别的哈希算法映射到 UAC。在 AP 上，有一个单一的哈希算法，它基于客户端的 MAC 地址创建索引。此索引指向该用户的实际 UAC 的映射表。此映射由集群领导者，然后，AAC 将此映射发送到相应的 AP。因此，集群中的所有 AP 都具有相同的映射信息。集群主服务器在考虑集群上的 AP 负载后，将 S-AAC 分配给每个 AP。

远程 AP 支持

使用远程 AP，配置隧道模式 VPN，并为每个 AP 分配一个内部 IP 或远程 IP。相同的远程 IP 或内部 IP 分配给集群中每个受管设备上的远程 AP。从 神州云科 OS 8.0.0.0 开始，群集设置同时支持 IPv4 和 IPv6 客户端，并且 IPv6 客户端会话也会在故障转移后同步并继续。

从 神州云科 OS 8.7.0.0 开始，当远程 AP 同时配置了内部 IPv4 地址和内部 IPv6 地址池时，将基于远程 AP 的外部 IP 地址建立隧道。如果外部 IP 为 IPv4 地址，则使用来自远程 AP 内部 IP 池的集群内部 IPv4 地址来形成隧道。同样，如果外部 IP 是 IPv6 地址，则使用集群内部 IPv6 地址来形成隧道。

以下 CLI 命令支持集群配置中远程 AP 的 IPv4 地址：

（host）[mynode]（config）#lc-rap-pool <pool_name> [{pool_start_address} {pool_end_ address}]

以下 CLI 命令支持集群配置中远程 AP 的 IPv6 地址：

（host）[mynode]（config）#lc-rap-pool-v6 <pool_name> [{pool_start_address} {pool_end_ 地址}]

神州云科 OS 现在支持 ClearPass Policy Manager 将集群环境中的远程 AP 列入允许名单。

IPv6 群集支持

从 神州云科 OS 8.2.0.0 开始，支持 IPv6 集群。受管设备必须通过 IPv6 IPsec 隧道在 Mobility Conductor 上终止。

只有 IPv6 AP 可以在 IPv6 集群上终止，客户端可以是 IPv4 或 IPv6 类型。

以下 CLI 命令显示 IPv6 群集信息：

(host) #show lc-cluster group-membership

提示：IPv6 群集不支持 VRRP-IP 和 VRRP-VLAN。

神州云科 OS 现在允许 IPv4 和 IPv6 AP 在双堆栈部署中无缝连接到集群，而不考虑集群 IP 地址系列。在集群编队中，IPv4 和 IPv6 地址在集群成员之间交换。因此，集群可以将节点列表中的 IPv4 和 IPv6 地址发送到 AP，以便 AP 能够连接到集群成员。

下表提供了集群和 AP 之间支持的地址模式的信息：

支持的地址模式

群集地址模式	支持 IPv4 接入点	支持 IPv6 接入点
IPv4 集群	是	否
IPv6 集群	否	是
双栈 IPv4 集群	是	是
双栈 IPv6 集群	是	是

集群功能

以下各节介绍集群支持的功能：

增强型组播代理

受管设备充当连接到它的所有无线客户端的组播代理。受管设备对组播流的订阅是通过单个 VLAN 完成的。因此，只有多播流的一个副本将传送到客户端。

提示：群集仅支持 IGMP 代理和 MLD。

启用 IGMP 代理或 MLD 后，客户端报告将到达 UAC。然后，UAC 将订阅信息传输到 AAC 。两个托管设备（AAC 和 UAC）都充当上行链路组播 VLAN 中客户端的代理。

AP 锚定在 AAC 上，用户锚定在 UAC 上。当 AP 启动时，它会使用 AAC 建立隧道。同一隧道也用于 UAC 流量。当客户端启动时，AP 确定其 UAC 并与 UAC 建立隧道。当客

户端从一个 AAC 漫游到另一个 AAC 时，PIM 会通过 STA（站）通道检测到此漫游，并从旧 AAC 中删除客户端的组播订阅，并将其添加到新的 AAC 中。为此，将在 UAC 中维护存储每个客户端订阅的群集代理表。

如果组播流源自无线站，则受管设备会通过客户端所在的 VLAN 将流转发到组播路由器。下游仍通过配置的 VLAN 从组播路由器到群集中的每个受管设备进行组播代理操作。如果两个 VLAN 相同，则源客户端 UAC 上的代理不会接收来自组播路由器的流。

在 L3 连接的集群中，当 AAC 与 UAC 的 VLAN 不同时，来自上行链路的组播流量不会到达 AAC。因此，集群必须通过 L2 连接才能流式传输组播流量。

以下 CLI 命令配置具有组播 VLAN 的集群：

```
(host) [multicast] (cluster1) #controller 10.15.128.102 mcast-vlan

<mcast_vlan>                VLAN id
```

如果集群配置了组播 VLAN，则会显示以下 CLI 命令：

```
(host) #show lc-cluster group-profile cluster1

IPv4 Cluster Members

--------------------

CONTROLLER-IP   PRIORITY   MCAST-VLAN   VRRP-IP   VRRP-VLAN

-------------   --------   ----------   -------   ---------

10.15.128.103       128         29          0.0.0.0     0

10.15.128.104       128         29          0.0.0.0     0

10.15.128.104       128         29          0.0.0.0     0

10.15.128.102       128         29          0.0.0.0     0

Redundancy:

Active Client Rebalance Threshold:50%

Standby Client Rebalance Threshold:75%

Unbalance Threshold:5%
```

客户端状态同步

客户端状态同步功能有助于解决有关无缝故障转移、服务可用性和高可用性的问题。若要实现无中断故障转移，应满足以下两个条件：

- 需要启用冗余模式，默认情况下启用此模式。
- L2 连接类型，即集群成员必须共享相同的 VLAN。

有状态故障转移是通过从 UAC 到 S-UAC 的完全客户端同步实现的。例如，工作站表、用户表、L2 用户状态、L3 用户状态、密钥缓存、PMK 缓存等在 UAC 和 S-UAC 之间同步。用户会话在 S-UAC 上同步或复制。仅同步 FTP 和 DPI 等高价值会话。但是，某些被视为低值的会话（如常规 HTTP 流量）不会同步。

发生故障转移时，不会取消任何客户端的身份验证，因此，客户端会无缝故障转移到 SUAC。

提示：每个客户端最多支持 10 个会话。IPv6 客户端和双栈现在支持客户端状态同步。

在现有集群中，当添加新的受管设备并且现有受管设备的负载超过阈值时，负载均衡器会确保来自过载的 UAC 的流量重定向到新的受管设备。在此方案中，在负载均衡器从其他 UAC 切换用户之前，将执行这些用户的会话同步，以确保可靠性。

从 神州云科 OS 8.6.0.0 开始，在 UAC 故障期间，当客户端在 BSSID 之间漫游时，支持语音等高价值应用程序流量的无中断故障。

客户端状态同步在两种不同的方案中很有用：

- 当冗余关闭时 — 当冗余模式关闭时，不会为 AP 或客户端创建备用副本以进行故障转移保护。作为负载平衡的一部分，在计划的 UAC 切换之前，会话将同步到新的 UAC。
- 当冗余处于打开状态时 — 当冗余模式打开时，系统将为所有 AP 和客户端分配备用受管设备。会话将同步到备用 UAC。

对其中一个集群成员执行以下命令，查看当前连接到 S-UAC 的重复用户列表。

(host) #show user-table standby

AP LACP 支持

条带化 LMS IP 不能再用于条带化流量，因为每个 AP 都有到多个受管设备的 GRE 隧道。因此，从 神州云科 OS 8.2.0.0 开始，集群 LACP 用于基于每个 UAC 对流量进行条带化。也就是说，在集群设置中，同一 AP 上的客户端或用户被引导到不同的 UAC，流量被条带化到这些 UAC。

启用集群时，即使单节点集群，也不会使用条带化 IP;以太网接口的流量条带化根据 UAC 节点进行。

对于非集群设置，条带化 LMS IP 的使用方式与以前相同。

对于上游流量，群集 LACP 会在以太网端口之间对这些 UAC 进行负载均衡。

对于下行流量，由于 GRE 数据包的源 IP 和 MAC 地址与 AP 的 Source-IP 和 MAC 地址不同，因此 AP 的上行链路交换机会分散流量。

以下 CLI 命令在非集群拓扑中配置 AP LACP:

在 AP 的上行链路交换机上，使用以下命令在 AP 的两个以太网端口之间配置 LACP:

(host) [md] (config) #ap-lacp-striping-ip

(host) [md] (AP LACP LMS map information) #aplacp-enable

(host) [md] (AP LACP LMS map information) #striping-ip 10.15.127.2 lms 10.15.127.3

The following CLI command displays the configuration:

(host) #show ap-lacp-striping-ip

AP LACP LMS map information

Parameter Value

--- ---

AP LACP Striping IP Enabled

GRE Striping IP 10.15.127.2 LMS 10.15.127.3

提示：ap-system-profile 中的 lms-ip 值将用作在 ap-lacp 配置文件中查找条目的键。

提示：建议不要为独立控制器部署配置 GRE 条带化 IP 地址。

授权服务器交互

该功能支持使用多个 VRRP 实例的集群中的 CoA 请求。此功能可确保当 UAC 因控制器故障或客户端负载平衡而更改时，不会丢弃 CoA 请求。

CoA 是授权变更，是对 RADIUS 属性和功能的扩展。CoA 请求消息由 RADIUS 服务器发送到 NAS 设备，用于动态修改现有的会话授权属性。CoA 请求包含用于动态更改会话授权的信息。如果 NAS 能够成功更改用户会话的授权，则会使用 CoA-ACK 进行响应。否则，它会将 CoA-NAK 返回到 RADIUS 服务器。

为了支持此功能，将动态创建多个 VRRP 实例，每个集群节点一个实例。在这里，集群节点是该实例的指挥者。在集群中，每个 VRRP 实例的虚拟 IP 在向 RADIUS 服务器发送 RADIUS 请求时用作 NAS-IP。

提示：这些实例的 VRRP ID 是保留的，保留的 ID 范围为 220 到 255。

例如，对于具有 5 个节点的集群，有 5 个 VRRP 实例和 5 个虚拟 IP 地址。也就是说，每个 VRRP 实例一个虚拟 IP 地址。集群使用实例的虚拟 IP 作为 RADIUS 请求中的 NAS-IP。也就是说，当群集节点代表尝试对 RADIUS 服务器进行身份验证的客户端发送 RADIUS 请求时，它会将虚拟 IP 作为 NAS-IP 插入该 RADIUS 数据包中。

提示：VRRP VLAN 可以与控制器 IP 的 VLAN 相同。如果将同一 VLAN 用于所有集群成员，则 VRRP VLAN 也可能不同。

要将 A-UAC 的 VRRP IP 地址设置为 NAS IP，必须为每个集群成员分配 VRRP IP。此分配过程会自动为群集的其他成员配置 VRRP 成员身份，并正确设置 VRRP 优先级，以便主 A-UAC 在虚拟 IP 启动时拥有虚拟 IP。

VRRP IP 地址和 VRRP VLAN 的设置步骤如下：

1. 配置新群集时，请在“托管网络”节点层次结构中选择托管设备所在的组文件夹。

2.导航到“配置>服务”>“群集”选项卡。

3.单击 Clusters 表中的 + 以创建新的集群配置文件。

此时将显示 New Cluster Profile （新建集群配置文件） 表格。

4.输入集群的名称。

5.单击“控制器”（Controllers） 表格中的 + 以添加新控制器。

将显示“添加控制器”（Add Controller）表。

6.输入受管设备的 VRRP IP 和 VRRP VLAN 字段值。

7.单击“确定”。

8.同样，输入所有托管设备的 VRRP IP 和 VRRP VLAN 值。

提示：神州云科 建议您使用与 VRRP-VLAN 相同的 controller-ip 子网。

以下 CLI 命令将 A-UAC 的 VRRP IP 地址设置为 NAS IP：

(host) [MD-cluster1]#lc-cluster group-profile primary-cluster

(host) [MD-cluster1](Classic Controller Cluster Profile "primary-cluster") #controller

10.15.43.2 vrrp-ip 100.1.1.2 vrrp-vlan 100

以下是如何为具有两个托管设备的群集设置 VRRP IP 的示例：

(host) [MD]#lc-cluster group-profile primary-cluster

(host) [MD-cluster1](Classic Controller Cluster Profile "primary-cluster") #controller

10.15.43.2 vrrp-ip 100.1.1.2 vrrp-vlan 100

(host) [MD-cluster4](Classic Controller Cluster Profile "primary-cluster") #controller

10.15.43.5 vrrp-ip 100.1.1.5 vrrp-vlan 100

以下 CLI 命令验证两个受管设备的 VRRP 状态：

(host) [MD-cluster1] #show vrrp

Virtual Router 220:

Description

Admin State UP, VR State CONDUCTOR

IP Address 100.1.1.2, MAC Address 00:00:5e:00:01:dc, vlan 100

Priority 255, Advertisement 1 sec, Preemption Enable Delay 0

Auth type NONE ********

tracking is not enabled

(host) [MD-cluster4] #show vrrp

Virtual Router 220:

Description

Admin State UP, VR State BACK

IP Address 100.1.1.2, MAC Address 00:00:5e:00:01:dc, vlan 100

Priority 235, Advertisement 1 sec, Preemption Enable Delay 0

Auth type NONE ********

tracking is not enabled

AP 故障转移到不同的集群

从 神州云科 OS 8.0.0.0 开始，AP 可以在集群之间进行故障转移。支持跨地理位置分散的数据中心的冗余。AP 在集群中的 AAC 上终止。如果集群中的成员发生故障，AP 将故障转移到同一集群中的 S-AAC。如果 AP 无法与第一个集群中的任何成员建立通信，则它将在备份数据中心中的另一个集群设置上终止。仅当 AP 系统配置文件中提供其他集群成员 IP 作为备份 LMS 时，它才会在另一个集群上终止。

例如，在西海岸数据中心部署了一个具有四个托管设备的集群。同样，在东海岸数据中心部署了一个具有四个托管设备的集群。AP 配置为在西海岸数据中心具有主终端，在东海岸数据中心具有备份终端。如果受管设备在西海岸数据中心发生故障，则 AAC 将移动到同一数据中心中的另一个受管设备。但是，如果 AP 无法访问整个西海岸数据中心，则它会故障转移到东海岸数据中心。

神州云科 OS 现在允许您在 AP 故障转移期间禁用有线下行链路端口的以太网链路和/或 PoE PSE。当 AP 故障转移到位于其他数据中心的备份集群时，您必须断开有线客户端的连接。这是为了确保客户端可以重新启动 DHCP 请求，以从不同的 IP 地址池中获取新的 IP 地址。此外，还必须应用有线端口停机时间，以便客户端可以释放 IP 地址。有线端口停机时间到期后，AP 可以恢复停机期间未应用的配置。

您可以配置 AP 故障转移到备份集群或回退到主集群后的有线端口停机时间。您可以为以

太网链路或 PoE 配置端口跳回，也可以在受管设备的 AP 系统配置文件中配置两者的停机时间。

以下过程在 AP 系统配置文件中配置端口跳回功能：

1. 在“托管网络”节点层次结构中，导航到“配置”>“系统>配置文件”选项卡。
2. 在“所有配置文件”列表中，展开“AP”菜单，然后选择“AP 系统”。
3. 选择要编辑的 AP 系统配置文件，或单击 + 创建新配置文件。
4. 在“常规”下，执行以下步骤之一： n 输入一个介于 0 到 60 之间的值，用于“Wired Port Down-Time By Shutdown Ethernet Link”（有线端口停机时间按关闭以太网链路）字段。
   - 输入一个介于 0 到 60 之间的值，用于 Wired Port Down-Time By Shutdown POE 字段。
   - 为“按关闭以太网链路的有线端口停机时间”和“按关闭 POE 的有线端口停机时间”字段输入一个介于 0 到 60 之间的值。
5. 单击提交。
6. 单击“挂起的更改”（Pending Changes）。
7. 在“挂起的更改”窗口中，选中该复选框，然后单击“部署更改”。

以下 CLI 示例配置以太网链路和 PoE 的有线端口停机时间：

```
(host)[mynode](config)#ap system-profile <profile-name>

(host)[mynode] (AP system profile "<profile-name>") # wired-poe-bounce-interval 10

(host)[mynode] (AP system profile "<profile-name>") # wired-port-bounce-interval 40

(host)[mynode] (AP system profile "<profile-name>") # write memory

Saving Configuration...

Configuration Saved.
```

以下 CLI 示例显示 AP 的有线端口状态以及从控制器转发的有线端口退回配置：

```
(host) [mynode] #show ap remote debug wired-port-down-state ap-name ap-303h1

The configurations pushed from the controller

-------------------------------------------
```

The port bounce time by disable POE: 30

The port bounce time by shutdown ethernet link: 60

AP's wired port is in down time, the port status as below

All wired ports' status

Wired port	Ethernet link status	Whether Support PSE	PSE status
eth0	up	no	
eth1	down	no	
eth2	down	no	
eth3	up		enable

在群集中对受管设备进行分组

从 神州云科 OS 8.2.0.0 开始，您可以将托管设备分组到集群中，这有助于影响 S-AAC 和 S-UAC 分配。与配置了 AAC 和 UAC 的组相比，S-AAC 和 S-UAC 的优先级将提供给不同组中的受管设备。

在 lc-cluster group-profile 命令中引入了一个新参数 group。

(host) #lc-cluster group-profile <profile> controller <ip> [priority <prio>] [mcast-vlan <mcast_vlan>] [vrrp-ip <vrrp_ip> vrrp-vlan <vrrp_vlan> group <group number>]

AP 节点列表

当 AP 加入集群时，它会学习所有集群成员的 IP 地址。这些 IP 地址存储在节点列表中，该列表作为环境变量保存在 AP 的闪存中。因此，当 AP 重新启动并重新启动时，AP 会检查节点列表，联系节点列表中最先列出的集群成员。如果节点列表中第一个集群成员关闭或

无法访问，则 AP 会动态尝试节点列表中列出的第二个集群成员，依此类推。

只要集群中至少有一台受管设备处于活动状态，AP 就会始终找到受管设备。

如果无法访问整个节点列表，则 AP 将重新启动。

AP 移动

此功能允许最终用户将特定 AP 从当前受管设备移动到目标受管设备。apmove 命令将 AP 或 AP 组重新分配给任何受管设备。

在以下情况下，使用 apmove 命令将特定 AP 移动到特定分配的受管设备：

- 在不更改任何配置的情况下将某些特定 AP 移动到其他受管设备。
- 如果当前受管设备和目标受管设备之间没有故障转移或重新引导配置。

您可以在以下设置中执行 apmove 命令：

- 同一集群组 — apmove 只能在集群托管设备主服务器上执行。
- 相同的 HA — 此命令在 HA 活动节点上执行，AP 故障转移到 HA 备用节点。
- 正常拓扑 — 在非集群设置中，可以在节点上执行 apmove，以将 AP 从当前受管设备移动到另一个受管设备。

以下 CLI 命令移动特定 AP：

如果启用了集群，系统访问点监视器进程将检查当前节点是否为集群主节点。否则，它会显示错误，并将集群主的 IP 地址提供给最终用户。然后，最终用户可以找到集群主服务器，并在正确的受管设备中执行该命令。

apmove 命令的执行方式如下：

(host) [mynode] (config) #apmove <ap-mac> <target-ip>

(host) [mynode] (config) #apmove <ap-group/all> <source-ip> <target-ip>

参数说明	描述
ap-mac	特定 AP 的 MAC 地址
ap-group/all	特定组中的所有 AP 或特定受管设备中的所有 AP。
source-ip	要从中移动特定 AP 的特定受管设备。

target-ip	要将 AP 移动到的特定受管设备。

当目标 IP 位于集群内时，APmove 将从集群主服务器启动。当目标 IP 位于集群外部时，Apmove 将在 AAC 或 S-AAC 上启动。

当 APmove 从 AAC 启动时，AP 获取目标 IP 并设置 APmove 导体变量。如果 APmove 目标是当前集群外部的受管设备，则 AP 将重新启动并连接到该目标受管设备。无论目标节点是否在另一个集群中，如果目标 IP 位于集群外部，则会清除 AP 节点列表。如果目标受管设备是另一个集群的一部分，则会向 AP 发送新的节点列表。如果 AP 无法连接到节点列表中的任何节点，它将回退到其他已知实体，例如 previous_lms、backup_lms、导体等。

在集群环境中，AP 启动 APmove 时给出的优先级如下：

1. APmove 导体（仅用于集群升级场景）
2. 集群节点列表
3. 以前的 LMS（仅限启用 CPsec）
4. 导体变量 引入节点列表以避免多次重定向到 AP，并允许 AP 直接连接

提示：到以前已知的 AAC。但是，如果先前已知的 AAC 关闭，则 AP 将连接到节点列表中的任何节点。

对群集的 EST 支持

在群集设置中，AP 使用 AAC、S-AAC 和 UAC 建立 IPsec 隧道。从 神州云科 OS 8.4.0.0 开始，集群成员使用已注册的证书进行 IPsec 隧道身份验证，而不是使用工厂证书。

在群集设置中启用安全传输注册 （EST） 时，AAC 会将 EST 参数发送到 AP，AP 将进行注册，并使用这些已注册的证书与所有群集成员建立 IPsec 隧道。

现有集群在 EST 激活时断开连接，所有 AP 都会作为 EST 注册的一部分重新启动。在此过程中，群集对等体上的 IPsec 隧道将被删除，这会导致群集在该对等体上断开连接。这可确保群集流量在未加密或封装的情况下不会流向对等方。

提示：建议在启用集群组成员资格之前，先在所有集群成员上启用 EST。

NAT 后面的集群的远程 AP 支持

只有群集部署中所有受管设备的公共 IP 地址支持远程 AP。但是，NAT 后面的集群无法与远程 AP 一起使用，因为集群中的受管设备使用专用域中的交换机 IP;远程 AP 无权访问。从 神州云科 OS 8.4.0.0 开始，远程 AP 可以通过从集群获取私有 IP 和公网 IP 地址映射，将受管设备的私有地址映射到公网空间。因此，远程 AP 支持 NAT 后面的集群。

关键考虑因素

- 远程 AP 预配了群集正在使用的任何公共 IP 地址。
- NAT 映射在客户 NAT 设备中根据群集配置文件使用的配置进行配置
- 即使配置了防火墙，也必须允许映射。

局限性

- 不允许为同一群集配置文件中的不同节点配置相同的公共 IP。
- 仅当一个配置文件在所有集群成员中处于活动状态时，才在不同的集群配置文件中配置相同的公共 IP。
- 外部 allowlist-db 不支持群集。

提示：群集配置文件中配置的公共地址和专用地址之间的映射也必须在 NAT 设备中配置。

以下过程介绍如何使用远程 AP 在 NAT 后面启用集群：

1. 在“托管网络”节点层次结构中，导航到“配置>服务>群集”选项卡。
2. 单击“集群”（Clusters） 表格中的 + 以创建新的集群配置文件。此时将显示 New Cluster Profile （新建集群配置文件） 表格。
3. 在 Cluster Name （集群名称） 字段中输入集群名称 rapcluster。
4. 输入 RAP 公共 IP 以及

5. 点击提交。

6. 在 Cluster Profile 选项卡中，从 cluster group-membership 下拉列表中选择 rapcluster。

7. 点击提交。

8. 单击“挂起的更改”。

9. 在“挂起的更改”窗口中，选中该复选框，然后单击“部署更改”。

以下 CLI 命令将公有和私有地址与集群配置文件中的远程 AP 映射：

```
(host) [cluster] (config) #lc-cluster group-profile rapcluster

(host) [cluster] (Classic Controller Cluster Profile "rapcluster") controller 10.10.10.1 rap-public-ip 100.100.100.101

(host) [cluster] (Classic Controller Cluster Profile "rapcluster")controller 10.10.10.2 rap-public-ip 100.100.100.102

(host) [cluster] (Classic Controller Cluster Profile "rapcluster")controller 10.10.10.3 rap-public-ip 100.100.100.103

(host) [cluster] (Classic Controller Cluster Profile "rapcluster")controller 10.10.10.4 rap-public-ip 100.100.100.104
```

提示：在 group-membership 中配置此配置文件时，将使用该集群成员的相应公共 IP。

以下 CLI 命令检查远程 AP 的公网 IP 是否基于控制器的专用 IP 地址进行配置：

```
(host) #Show lc-cluster group-profile

IPv4 Cluster Members

--------------------

CONTROLLER-IP PRIORITY MCAST-VLAN VRRP-IP VRRP-VLAN GROUP-ID RAP-PUBLIC-IP

------------- -------- ---------- ------- --------- -------- -------------

10.17.62.194    128      0          1.1.1.1   200       0        10.10.10.11

10.17.62.195    128      0          1.1.1.2   200       0        10.10.10.12
```

拒绝用户间桥接

拒绝用户间桥接可防止有线或无线用户之间转发第 2 层流量，即使用户位于群集中的不同托管设备上也是如此。群集中的所有受管设备都支持此功能。

该功能也适用于所有客户端的所有部署类型，例如园区 AP、远程 AP、无线用户、有线用

户、隧道用户和拆分隧道用户。

在以前的版本中，当启用拒绝用户间桥接时，客户端能够访问受信任的设备。但是，从 神州云科 OS 8.8.0.0 开始，客户端将无法访问其网络上的这些受信任设备，除非自动学习或手动将其添加到允许列表中。

仅当地址已添加到 allowed-address-list 表中时，才允许来自客户端的流量。如果第 3 层数据包的目标未包含在 allowed-address-list 表中，则任何流量（包括广播、组播或其他第 2 层帧）都将被丢弃。

某些第 2 层设备会自动学习并允许其第 3 层地址，例如来自 DHCP 响应的默认网关和 DNS 地址。

对于所有其他必需的本地网络地址，例如具有多个路由器的非默认网关，请确保手动将它们添加到允许列表表中。否则，前往这些目标的第 2 层流量将被丢弃。

要进行故障排除，请在 CLI 中运行以下 show 命令以检查丢帧：

```
(host) [mynode] #show datapath frame
```

提示：桥接模式部署不支持此功能，因为桥接用户的流量由 AP 本地桥接。

自动学习地址

在每个 VLAN 中，托管设备通过窥探 DHCPv4、DHCPv6 和 IPV6 RA 自动学习网关和 DNS 地址。因此，用户无需手动将这些地址添加到允许列表中。如果未配置 DHCP，则用户需要手动添加网关和 DNS 条目。如果需要与其他本地地址通信，则用户需要手动添加地址。除了这些自动学习的地址外，用户最多可以配置 256 个 IP 地址。

提示：

- 对于 IPv4 地址，只能自动学习一个网关和三个 DNS 条目。对于 IPv6 地址，可以自动学习 1 个 RA 网关和 3 个 DNS 条目。
- 如果网关不同且非默认（相同的第 2 层网络），请确保将非默认网关地址添加到控制器允许列表中。

- 如果 RA 和 DHCPv6 服务器不同（同一第 2 层网络），请确保将 DHCPv6 服务器链路本地地址添加到控制器允许列表中。
- 如果 RA 和 DHCPv6 中继不同（同一第 2 层网络），请确保将 DHCPv6 中继服务器链路本地地址添加到控制器允许列表中。

手动配置允许的地址列表

要启用拒绝用户间桥接功能，请在 WebUI 中执行以下步骤：

1. 在托管网络层次结构中，导航到“配置>服务”>“防火墙”。
2. 展开“用户间桥接”（Inter User Bridging accordion），然后单击“拒绝用户间桥接”（Deny inter user bridgeing toggle） 按钮。
3. 单击“允许的地址”表中的“+”图标以添加受信任设备的 IP 地址。
   a. 在 IP 版本字段中，输入 IP 版本为 IPv4 或 IPv6。
   b. 在 IP 地址字段中，输入 IP 地址。
4. 重复步骤 3 以添加所有允许的 IP 地址。
5. 单击提交。
6. 单击“挂起的更改”（Pending Changes）。
7. 在“挂起的更改”窗口中，选中该复选框，然后单击“部署更改”。

若要在启用拒绝用户间桥接功能时添加允许的 IP 地址，请在 CLI 中运行以下命令：

```
(host) [mynode] #allowed-address-list ipv4 <IP address>

(host) [mynode] #allowed-address-list ipv6 <IP address>
```

要查看允许的 IP 地址列表，请在 CLI 中运行以下 show 命令：

```
(host) [mynode] #show allowed-address-list all

Allowed address list

----------------------

Type    :    Address
```

```
----------------------

IPv4          2.2.2.2

IPv6          2002::2

IPV4          192.168.1.1

Total : 3

(host) [mynode] #show datapath allowed-address-list ipv4

Allowed address list

----------------------

Type    :    Address

----------------------

IPv4          2.2.2.2

IPV4          192.168.1.1

Total   :   2

(host) [mynode] #show datapath allowed-address-list ipv6

Allowed address list

----------------------

Type   :   Address

----------------------

IPv6        2002::2

Total : 1

(host) [mynode] #show datapath allowed-address-list counters

------------------------------

Allowed   address   stats   counter

------------------------------

IPv4 drop    :              126

IPv6 drop    :              1526
```

要从允许列表中删除 IP 地址，请在 CLI 中运行以下命令：

(host) [mynode] #no allowed-address-table ipv4 <IP address>

(host) [mynode] #no allowed-address-table ipv6 <IP address>

VRRP ID 和密码

集群允许用户在集群配置文件中设置虚拟 IP 的 VRRP ID 和密码的起始值，以避免 VRRP 冲突。也就是说，将从配置的值开始为群集 VRRP 成员分配连续的 VRRP ID。

传统上，当用户在集群中配置虚拟 IP 时，神州云科 OS 会自动在 220 - 225 范围内配置 VRRP 组。当多个集群共享同一个 L2 网络时，这会导致 VRRP 冲突。因此，为了避免 VRRP 冲突，集群现在允许用户在集群配置文件中为虚拟 IP 设置 VRRP ID。

用户可以在群集配置文件中设置以下参数：

- 指定起始 VRRP ID
- 指定用于保护 VRRP 会话的 VRRP 密码

以下 CLI 命令配置 VRRP ID 和 VRRP 密码：

lc-cluster group-profile <profile-name>

vrrp-id <starting id> [vrrp-passphrase <vrrp passphrase string>]

参数说明	描述
vrrp-id	这是一个可选参数，用于指定启动集群成员的 VRRP ID。如果未配置，系统会自动在 220-225 范围内配置 VRRP 组。
vrrp-passphrase	这是一个最多 8 个字符的可选密码，用于可以在其广播中对 VRRP 对等体进行身份验证。如果未配置此项，则没有身份验证密码。

以下 CLI 命令检查配置：

(host) #show lc-cluster group-profile v4cluster

IPv4 Cluster Members

CONTROLLER-IP PRIORITY MCAST-VLAN VRRP-IP VRRP-VLAN GROUP-ID RAP-PUBLIC-IP

10.20.101.12 128 0 0.0.0.0 0 0 0.0.0.0

10.20.101.5 128 0 0.0.0.0 0 0 0.0.0.0

10.20.101.20 128 0 0.0.0.0 0 0 0.0.0.0

10.20.101.7 128 0 0.0.0.0 0 0 0.0.0.0

Redundancy:

Active Client Rebalance Threshold:20%

Standby Client Rebalance Threshold:40%

Unbalance Threshold:5%

Active AP Load Balancing:

Active AP Rebalance Threshold:20%

Active AP Unbalanced Threshold:5%

Active AP Rebalance Count:50

Active AP Rebalance Timer:1 mins

Starting VRRP ID:99

VRRP Passphrase:********

集群配置

本节介绍使用 WebUI 和 CLI 设置集群和编辑集群配置文件的过程。

配置集群

以下部分介绍如何使用 WebUI 配置集群。配置分两个阶段进行:

- 创建群集配置文件。
- 将创建的配置文件附加到群集组成员身份。

执行以下步骤以添加集群配置文件：

1. 在“托管网络”节点层次结构中，导航到“配置>服务>群集”选项卡。

2.单击 Clusters 表中的 +。

3.在 Name （名称） 字段中输入群集配置文件的名称。

4.点击提交。

5.要配置创建的集群，请从集群表中选择集群。

6.在“群集配置文件> <群集名称>窗口中，展开”基本折叠“。

7.要将控制器添加到集群，请单击“控制器”表中的“+”。

将显示“添加控制器”窗口。

8.定义上表中列出的参数。

9.单击“确定”。

10.展开“高级”。

11.选中“冗余”复选框以在群集中启用冗余。

12.或者，可以设置活动客户端重新平衡阈值、备用客户端重新平衡阈值、不平衡阈值和检测信号阈值。但是，这些参数具有默认设置，神州云科 强烈建议您使用默认设置。

提示：对于以毫秒为单位的最小检测信号阈值，端口通道的默认值为 2000 毫秒，单个以太网连接（无端口通道）的默认值为 900 毫秒。但是，如果检测信号阈值配置为自定义值，则该值优先于默认值。

13. 单击提交。

若要将群集配置文件附加到群集组成员身份，请执行以下步骤：

1.在托管网络节点层次结构中，选择要添加到集群的托管设备。

2.导航到“配置>服务”>“群集”选项卡，然后展开“群集配置文件”折叠面板。

3.从群集组成员身份下拉列表中选择群集配置文件。

4.通过键入或从下拉列表中进行选择来设置排除 VLAN 字段，以构建以逗号分隔的 VLAN ID 列表。

提示：在排除 VLAN 下拉列表中，如果用户选择 VLAN ID，则所选值将添加到字段中

已存在的内容中。例如，如果文本字段包含“2”，并且用户从下拉列表中选择“5”，则该字段必须显示“2,5”。还可以添加值范围，例如 1-5。

5. 单击提交。

6. 单击“挂起的更改”（Pending Changes）。

7. 在“挂起的更改”窗口中，选中该复选框，然后单击“部署更改”。

Cluster Profile 参数

参数说明	描述
IP version	选择 IP 版本 - IPv4 或 IPv6。
IP address	IP 地址必须设置为受管设备的交换机 IP。
Group	这用于影响集群领导者所做的 S-UAC 和 S-AAC 分配。为组 ID 输入一个介于 1 和 12 之间的整数值。
VRRP IP	用于为外部身份验证服务器（如 CoA）发起的所有请求提供服务的 IP。
VRRP VLAN	用于为外部身份验证服务器发起的所有请求提供服务的 VLAN，例如 CoA
MCast VLAN	用于将组播流量订阅到上游组播路由器的 VLAN。
Priority	这用于影响集群领导者的选举。

以下 CLI 命令设置集群:

1. 创建集群节点:

```
(host) [mynode] (config) #configuration node /md/cluster
```

2. 要更改为您创建的配置群集节点:

```
(host) [mynode] (config) #change-config-node /md/cluster
```

3. 在先前创建的节点下配置受管设备。

提示：确保在 /managed device/cluster 中配置的 SSID、VAP 和 AAA 配置文件等通用配置文件一致。

```
(host) [mynode] (config) #configuration device 00:1a:1e:02:04:88 device-model A7210 /md/cluster
```

4. 对多个受管设备重复此配置。

5. 集群中的所有受管设备都需要时间同步。因此，建议在群集设置中具有 NTP 服务器。

要配置 NTP 服务器，请执行以下操作：

(host) [cluster] (config) #ntp server <ip address> iburst

(host) [cluster] (config) #ntp authentication-key 1 md5 <password>

6. 要在 Mobility Conductor 中配置集群组配置文件：

(host) [cluster] (config) #lc-cluster group-profile 6NodeCluster

7. lc-cluster group-profile 中的受管设备 IP 地址可以是 IPv4 或 IPv6，也可以是两者的组合。但是，在 Mobility Conductor 上，我们可以分别配置 IPv4 集群和 IPv6 集群。两个集群独立运行，Mobility Conductor 可以将配置更新发送到相应的受管设备。

8. 要将受管设备添加到组配置文件：受管设备的交换机 IP 用作以下配置中的 IP 地址。提示：AP 的终端点还必须设置为受管设备的交换机 IP。AP 系统配置文件中 AP 的 LMSIP 成为 AP 的 active-AAC （A-AAC）。

9. 对于 IPv6 网络：

(host) [cluster] (Classic Controller Cluster Profile "6NodeCluster")controller-v6 2000:192:168:28::24 priority 128 mcast-vlan 0 vrrp-ip-v6 :: vrrp-vlan 0 group 0

(host) [cluster] (Classic Controller Cluster Profile "6NodeCluster")controller-v6 2000:192:168:28::26 priority 128 mcast-vlan 0 vrrp-ip-v6 :: vrrp-vlan 0 group 0

(host) [cluster] (Classic Controller Cluster Profile "6NodeCluster")controller-v6 2000:192:168:28::22 priority 128 mcast-vlan 0 vrrp-ip-v6 :: vrrp-vlan 0 group 0

(host) [cluster] (Classic Controller Cluster Profile "6NodeCluster")controller-v6 2000:192:168:28::23 priority 128 mcast-vlan 0 vrrp-ip-v6 :: vrrp-vlan 0 group 0

10. 对于 IPv4 网络：

(host) [cluster] (Classic Controller Cluster Profile "6NodeCluster")controller 192.168.28.22 priority 128 mcast-vlan 0 vrrp-ip 0.0.0.0 vrrp-vlan 0 group 1

(host) [cluster] (Classic Controller Cluster Profile "6NodeCluster")controller 192.168.28.23 priority 128 mcast-vlan 0 vrrp-ip 0.0.0.0 vrrp-vlan 0 group 1

(host) [cluster] (Classic Controller Cluster Profile "6NodeCluster")controller 192.168.28.24 priority 128 mcast-vlan 0 vrrp-ip

0.0.0.0 vrrp-vlan 0 group 2

(host) [cluster] (Classic Controller Cluster Profile "6NodeCluster")controller 192.168.28.26 priority 128 mcast-vlan 0 vrrp-ip

0.0.0.0 vrrp-vlan 0 group 2

提示：IP 地址是必需参数，优先级、组、mcast、VLAN、VRRP IP 和 VRRP VLAN 是可选参数。

11. 在 Mobility Conductor 中，将配置应用于受管设备：

(host) [cluster] (Classic Controller Cluster Profile "6NodeCluster ") #write memory

12. 保存配置。

13. /md/cluster 的部分配置

14. 在每个受管设备上配置组成员身份。如果仅在形成集群的节点路径下有节点，则在该节点路径上执行命令[00:1a:1e:02:04:88].

(host) [00:1a:1e:02:04:88] (config) #lc-cluster group-membership 6NodeCluster

(host) [00:1a:1e:02:04:88] (config) #write memory

15. 在每个受管设备上，检查集群状态：

(host) #show lc-cluster group-membership

16. 为确保客户端 SSO 在故障转移时正常工作，群集中的受管设备必须通过 L2 连接。以下命令显示群集中 L2 或 L3 连接的状态。

(host) [md] (cluster)#show lc-cluster vlan-probe status

17. （可选）在受管设备上，排除 VLAN 探测算法的某些 VLAN。

(host) (config) #lc-cluster exclude-vlan <vlan-number>

18. 使用上一个命令删除 VLAN 后，再次运行 VLAN 探测算法。

(host) [cluster] (config) #lc-cluster start-vlan-probe

19. 当 VLAN 探测失败时，将生成新的 SNMP 陷阱 wlsxClusterVlanProbeStatus。此陷阱指示集群 VLAN 探测状态并发送受影响的 VLAN。默认情况下，此陷阱处于禁用状态。

编辑集群配置文件

以下过程介绍如何编辑群集配置文件:

1.在“托管网络”节点层次结构中，导航到“配置>服务>群集”选项卡。

2.若要编辑现有受管设备，请从“控制器”列表中选择受管设备。要将受管设备添加到群集，请单击 Controllers 表中的 +。

3.编辑或输入表 <Cluster Profile 参数> 中描述的参数值。

4.单击“确定”。

5.展开 Advanced 折叠面板以编辑表 70 中描述的 Active AP 负载平衡参数。但是，这些参数具有默认设置，神州云科 强烈建议您使用默认设置。

提示：当基础架构网络无法处理负载时，可能会发生群集检测信号超时。若要处理此问题，请确定基础结构网络上的群集检测信号数据包的优先级，或增加群集配置文件上的检测信号超时。

6. 单击提交。

7. 单击“挂起的更改”。

8. 在“挂起的更改”窗口中，选中该复选框，然后单击“部署更改”。

使用基本 show 命令

使用以下 show 命令确保群集配置按预期工作:

检查每个受管设备上的群集状态:

```
(host) #show lc-cluster group-membership
```

查看 VLAN 探测算法的状态，该算法在群集中的每对节点之间自动运行:

```
(host) #show lc-cluster vlan-probe status
```

查看集群成员因各种事件导致的断开连接的原因，并查看上次断开连接的时间戳:

```
(host) # show lc-cluster heartbeat counters
```

查看群集检测信号计数器:

(Host) #show datapath cluster heartbeat counters

查看连接和断开连接事件的历史记录:

(host)show lc-cluster history

查看集群中 AP 的主用或备用 AP 负载分布:

(host) # show lc-cluster load distribution ap

查看客户端在群集中的活动或备用客户端负载分布:

(host) # show lc-cluster load distribution client

查看受管设备上处于待机模式的 AP 列表:

(host) # show ap standby

查看受管设备上处于待机模式的用户列表:

(host) # show user-table standby

在托管设备上查看待机模式下数据路径中的用户列表:

(host) # show datapath user standby

查看任何给定客户端的 A-UAC 和 S-UAC。此命令可以在群集的任何受管设备上运行:

(host) # show aaa cluster essid <essid name> mac <client mac address>

查看有关所有连接对等体的详细信息，包括发送的心跳请求或接收的响应、所有错过和延迟心跳的序列号以及时间戳、上次接收或发送到死对等体的序列号和时间戳， 此命令还显示当前集群成员的心跳阈值和阈值更新计数， 添加或删除的对等计数和当前时间戳。

(host) #show datapath cluster details

从受管设备收集与群集相关的调试信息:

(host) #show cluster-tech-support </flash/config/outfile>

从 AP 收集与集群相关的调试信息:

(host) #show ap cluster-tech-support ap-name <ap-name> </flash/config/ap outfile>

收集 IPv6 相关的调试信息:

(host) #show gsm debug channel sectun

查看用于群集部署的远程 AP 内部 IP 池:

(host) #show lc-rap-pool rap-cluster

集群负载均衡

集群负载均衡是通过客户端负载均衡和 AP 负载均衡等功能实现的。

本节将介绍这两个功能。

客户端负载均衡

客户端负载均衡功能可确保客户端均匀分布在集群成员之间，从而有效地使用系统资源。

如果系统检测到负载分布失真，则通过更改这些客户端的 UAC 来平衡受管设备上的负载。

无论平台类型如何，所有受管设备的负载在群集中都是平衡的。

集群管理器计算受管设备上现有客户机数量与其最大容量的比率。根据此比率和其他阈值触发器，将触发客户端负载均衡。

当任何新的受管设备（包括故障转移后启动的受管设备）添加到现有群集时，会考虑将其用于负载均衡，并相应地移动 AP 和客户端以平衡群集中的负载。

提示：默认情况下，配置集群时会启用负载均衡。

阈值触发器

- 活动客户端重新平衡阈值 - 集群成员上的实际活动负载。阈值设置为 20%，即平台容量的 20%。
- 备用客户端重新平衡阈值 - 集群成员上的备用负载。阈值设置为 40%。
- 不平衡阈值 - 最大负载集群节点上的负载与最小负载集群节点上的负载之间的差值。阈值设置为 5%，也就是说，托管设备之间的负载必须至少存在 5% 的差异。
- AP Total Load Balance 阈值— 总负载均衡阈值设置为 40%。这是默认值，无法配置。

要为活动客户端触发负载平衡，必须满足活动客户端重新平衡阈值和不平衡阈值百分比。同样，对于备用客户端，必须满足备用客户端重新平衡阈值和不平衡阈值百分比。

启用冗余模式后，集群的容量将减少到一半。

AP 负载均衡

AP 负载均衡功能可确保集群主节点根据平台容量管理负载均衡。AP 在连接到集群时会动态分配一个 AAC。这里考虑的不是客户端负载，而是 AP 负载。

主用和备用 AP 都考虑用于负载均衡。

以下是新添加受管设备时的 AP 负载平衡条件:

- 当集群节点中已达到 AP 阈值时，如果添加了新的托管设备，则首先根据设置的 AP 计数填充新托管设备的 Active AP 表。
- 当未达到阈值时，AP 将移至新添加的受管设备的备用 AP 表。
- 只有在集群稳定后，这些 AP 的计数才会根据设置的 AP 计数递增，但是，在此阶段移动的 AP 不能始终基于 AP 计数。

提示：从 神州云科 OS 8.3.0.0 开始，活动 AP 负载均衡功能默认启用。在以前的版本中，默认情况下禁用此功能。

活动 AP 负载均衡使用 VRRP 进行 L2 连接，使用 1 个集群成员的交换机 IP 进行 L3 连接。AP 总负载均衡阈值设置为 40%，活动 AP 负载均衡阈值设置为 20%。这是默认值。

提示：当 AP 与集群建立通信时，LMS IP 将被忽略。但是，在发生故障转移时，将使用备份 LMS IP。

在 神州云科 OS 8.3.0.0 之前，集群领导者会考虑每个集群成员的 AP 负载，并将总 AP 负载最少的集群成员指定为 AAC。

对于初始负载均衡，集群领导者会评估具有最低活动 AP 负载百分比的受管设备是否可以容纳其他 AP。如果是，请将此托管设备作为候选 AAC 返回。

对于定期负载均衡，集群主节点会根据以下条件执行负载均衡:

1. 查找具有最大和最小活动负载百分比的受管设备。
2. 查找具有最大和最小总负载百分比的受管设备
3. 检查最大活动负载百分比是否大于活动负载百分比阈值。此外，检查最大负载和最小负载受管设备之间的差异是否大于不平衡阈值。

4.将活动 AP 从最大负载的受管设备移动到最小负载的受管设备。但是，如果它无法移动活动 AP，它将通过将备用 AP 从最大负载百分比托管设备移动到最小负载百分比托管设备来重新平衡备用负载。

提示：每 1 分钟进行一次周期性负载重新均衡，默认值为 AP，根据 AP 计数考虑对 AP 进行负载重均，默认为 50。

在集群成员上列出 AP 后，集群管理器会定期重新计算集群成员的负载以平衡负载。例如，当新的受管设备加入群集时。

提示：客户端负载均衡和 AP 负载均衡的触发器相同。

下面列出了 AP 负载均衡的优点

- 轻松扩展群集节点。
- 无需通过 LMS-IP 进行手动分发。

配置群集负载平衡

以下过程介绍如何为群集配置负载平衡：

1. 在“托管网络”节点层次结构中，导航到“配置>服务>群集”选项卡。

2.在集群表中，选择要配置 AP 负载均衡的集群。

3.在“群集配置文件> <群集名称>窗口中，展开”高级折叠“。

4.配置表<活动 AP 负载平衡参数>中描述的活动 AP 负载均衡设置。

5.点击提交。

6.单击“挂起的更改”。

7.在“挂起的更改”窗口中，选中该复选框，然后单击“部署更改”。

活动 AP 负载平衡参数

参数说明	描述
Redundancy	启用冗余模式后，集群的容量减少到一半，只有 8000 个客户端被视为达到阈值。
Active client rebalance threshold	指示执行 AP 所需的最小总负载百分比,群集中的负

	载均衡。至少一个受管设备必须将此值作为总负载百分比才能触发 AP 负载平衡。
Standby client rebalance threshold	表示在集群中执行备用 AP 负载均衡所需的最小总负载百分比。
Unbalance threshold	如果受管设备达到总负载阈值，则 AP 负载触发平衡。当群集中最大负载的受管设备与最小受管设备上的负载之差超过不平衡阈值时，会发生这种情况。
Heartbeat threshold	最小检测信号阈值以毫秒为单位设置。默认值设置基于在每对受管设备和群集之间确定的延迟。它还取决于受管设备和分配交换机之间的连接类型（单根以太网电缆或端口通道等）。

以下过程介绍如何配置 AP 和客户端负载均衡值：

1. 在“托管网络”节点层次结构中，导航到“配置>系统”选项卡。
2. 单击配置文件。
3. 展开 Cluster 折叠面板，然后单击 Classic Controller Cluster。
4. 单击 + 创建集群配置文件。
5. 添加 AP 负载平衡值和客户端负载平衡值。
6. 单击提交。
7. 单击“挂起的更改”。
8. 在“挂起的更改”窗口中，选中该复选框，然后单击“部署更改”。

以下 CLI 命令为集群配置负载平衡：

以下是活动 AP 负载均衡的示例：

```
(7210-24) #show lc-cluster load distribution ap

Cluster Load Distribution for APs

--------------------------------

Type    IPv4 Address      Active APs      Standby APs
```

---- --------------- -------------- ---------------

peer 192.168.28.23 25 20

self 192.168.28.24 20 25

Total: Active APs 45 Standby APs 45

(host) #show lc-cluster group-membership

Cluster Enabled, Profile Name = "ap-lb"

Redundancy Mode On

Active Client Rebalance Threshold = 20%

Standby Client Rebalance Threshold = 40%

Unbalance Threshold = 5%

AP Load Balancing: Enabled

Active AP Rebalance Threshold = 20%

Active AP Unbalance Threshold = 5%

Active AP Rebalance AP Count = 50

Active AP Rebalance Timer = 1 minutes

Cluster Info Table

Type IPv4 Address Priority Connection-Type STATUS

---- --------------- -------- --------------- ------

peer 192.168.28.23 128 L2-Connected CONNECTED (Leader, last HBT_RSP 10ms ago, RTD = 0.000 ms)

self 192.168.28.24 128 N/A CONNECTED (Member)

要检查活动 AP 负载平衡是启用还是禁用:

IPv4 示例:

(host) #show lc-cluster group-membership

Cluster Enabled, Profile Name = "testLB"

Redundancy Mode On

Active Client Rebalance Threshold = 20%

Standby Client Rebalance Threshold = 40%

Unbalance Threshold = 5%

AP Load Balancing: Enabled

Active AP Rebalance Threshold = 20%

Active AP Unbalance Threshold = 5%

Active AP Rebalance AP Count = 50

Active AP Rebalance Timer = 5 minutes

Cluster Info Table

Type	IPv4 Address	Priority	Connection-Type	STATUS
self	192.168.10.38	128	N/A	CONNECTED (Leader)
peer	192.168.10.34	128	L2-Connected	CONNECTED (Member, last HBT_RSP 38ms ago, RTD= 0.000 ms)

IPv6 示例:

(host) #show lc-cluster group-membership

Cluster Enabled, Profile Name = "72xx"

Redundancy Mode On

Active Client Rebalance Threshold = 20%

Standby Client Rebalance Threshold = 40%

Unbalance Threshold = 5%

AP Load Balancing: Enabled

Active AP Rebalance Threshold = 20%

Active AP Unbalance Threshold = 40%

Active AP Rebalance AP Count = 50

Active AP Rebalance Timer = 1 minutes

Cluster Info Table

Type IPv6 Address Priority Connection-Type STATUS

---- ---------- --------- --------------- -------------------------

peer 2000:192:168:28::24 128 L2-Connected CONNECTED (Member,last HBT_RSP 68ms ago, RTD = 0.000 ms)

peer 2000:192:168:28::26 128 L2-Connected CONNECTED (Member,last HBT_RSP 66ms ago, RTD = 0.000 ms)

peer 2000:192:168:28::22 128 L2-Connected CONNECTED (Member,last HBT_RSP 69ms ago, RTD = 0.503 ms)

self 2000:192:168:28::23 128 N/A CONNECTED (Leader)

要显示受管设备在 AP 通道上发布 AP 以进行 A-AAC 分配的次数:

(host) #show ap debug gsm-counters

STM GSM Counters

Name Value

---- -----

AP Publish Events 93

AP Delete Events 29

AP Publish Events(Load Balance) 2

AP Delete Events(Load Balance) 2

Radio Publish, Activate, Activate Errors 28 11 0

Radio Delete Events 3

Radio Delete Errors 15

BSS Publish Events 41

Responses to BSS Rcvd 41

BSS Delete Events 18

BSS Delete Errors 30

BSS Delete Key Not Found (included above) 30

STA Publish Events 0

STA Delete Events 0

STA Activate on S-UAC, Errors 0 0

STA Activate for Delete, Errors 0 0

WIRED_AP Publish Events 0

要显示 AP 尝试连接到集群主节点并需要集群主节点为此 AP 分配 A-AAC 的次数，请执行以下操作:

(host) #show lc-cluster gsm counters | exclude 0

Cluster GSM Channel Counters

AP Channel: Adds >> 1

AP Channel: Deletes >> 1

BSS Channel: Adds >> 2

BSS Channel: Section Update >> 2

AP Channel: Adds and Need AAC Assignment >> 1

AP Channel: Deletes from SAPM, AP redirected >> 1

群集部署方案

集群可以部署在四种不同的场景中。以下部分介绍这些不同群集部署方案的准则。

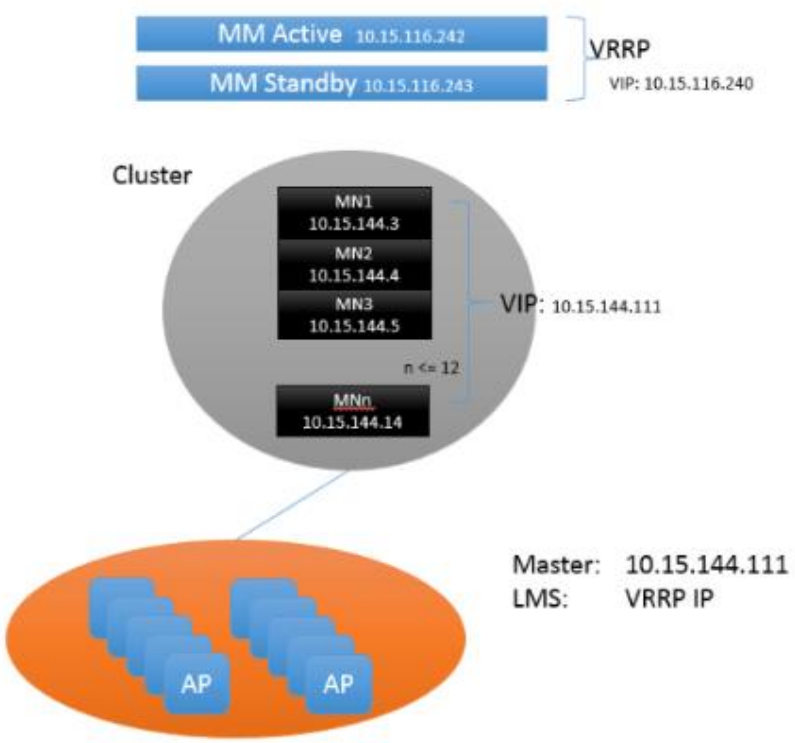
提示：神州云科 建议您使用 CLI 命令 active-ap-lb 为集群启用 AP 负载均衡。默认情况下，它处于启用状态。

提示：如果禁用 active-ap-lb，则使用 LMS 进行初始终止。LMS 抢占的使用方式如上述所有方案中所述。

方案 1：具有虚拟 IP 设置的群集

在这种情况下，如果 A-AAC （LMS） 关闭，AP 将执行到 S-AAC 的集群故障转移。如果 A-AAC 和 S-AAC 同时关闭，AP 将执行内部重启。如果 AP 在包括 LMS 在内的任何节点

上重新启动，则 AP 会记住节点列表并尝试节点列表中的所有条目。仅当 AP 无法访问任何节点时，才会执行旧版重启。



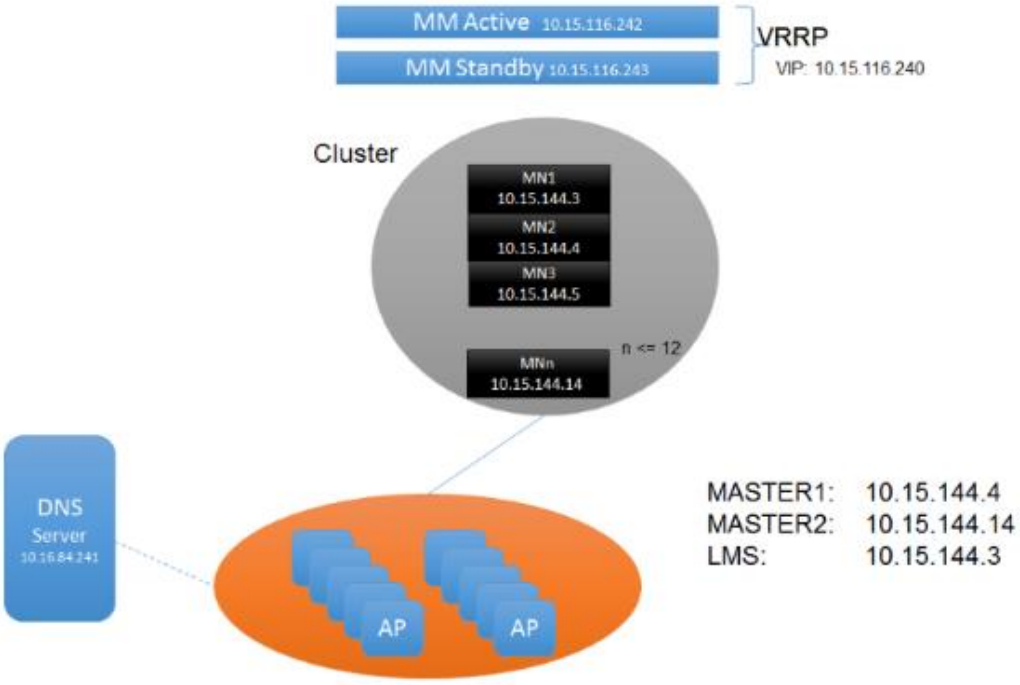
以下是确保在虚拟 IP 中成功部署群集的准则:

- AP 的 Conductor 必须配置为群集节点上的虚拟 IP。
- 如果集群配置了 VRRP IP，请在 LMS IP 地址和 backup-LMS IP 地址中设置 VRRP IP。
- 集群节点的 Nodelist 保存在 AP 上。如果 A-AAC 和 S-AAC 同时关闭，AP 将执行内部重启并尝试节点列表中的不同节点，直到节点列表耗尽。

方案 2：通过 DNS 解析使用多导线的群集

在此方案中，如果 A-AAC （LMS） 关闭，AP 将执行到 S-AAC 的集群故障转移。如果 A-AAC 和 S-AAC 同时关闭，并且 AP 尝试联系集群中的另一个节点，直到无法访问集群中的整个节点列表，则 AP 会在内部重新启动。如果 AP 在包括 LMS 在内的任何节点上重新启动，则 AP 会记住节点列表并尝试节点列表中的所有条目。仅当 AP 无法访问任何节点

时，才会执行旧版重启。



以下是确保通过 DNS 解析设置在多导体中成功部署集群的准则：

- AP 必须使用 DNS 解析获取多个导线。
- 如果集群配置了 VRRP IP，请在 LMS IP 地址和 backup-LMS IP 地址中设置 VRRP IP。
- 集群节点的 Nodelist 保存在 AP 上。如果 A-AAC 和 S-AAC 同时关闭，则 AP 将执行内部重启，并尝试节点列表中的不同节点，直到节点列表耗尽。

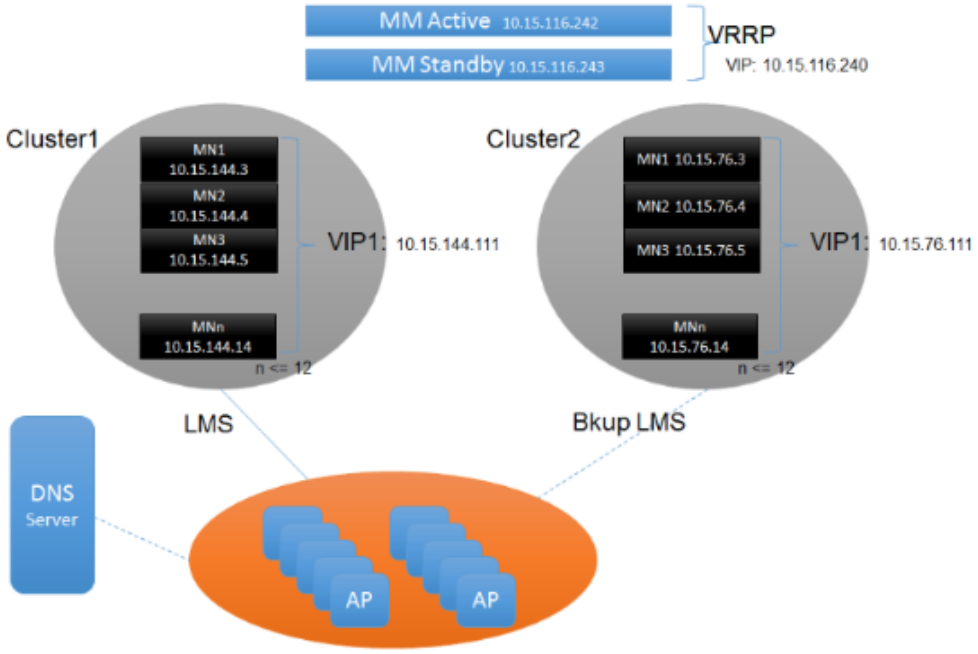
提示：在大型部署中，神州云科 建议使用此配置以避免大型故障域。

方案 3：通过跨数据中心的 DNS 解析使用虚拟 IP 的群集

在这种情况下，当 A-AAC 关闭时，AP 将故障转移到 S-AAC。如果 A-AAC 和 S-AAC 同时关闭，并且 AP 尝试联系 Cluster1 中的另一个节点，直到 Cluster1 节点列表中的所有节点都用完，则 AP 会在内部重新启动。如果 AP 无法访问 Cluster1，则会故障转移到备份 LMS。

如果启用了 LMS 抢占，则当主 LMS 节点在 Cluster1 上启动时，AP 将抢占到 Cluster1。如果禁用了 LMS 抢占，即使 Cluster1 已启动，AP 仍保留在 Cluster2 上。

如果 AP 在包括 LMS 在内的任何节点上重新启动，则 AP 会记住节点列表并尝试节点列表中的所有条目。仅当 AP 无法访问任何节点时，才会执行旧版重启。



以下是确保通过 *DNS* 解析成功部署具有虚拟 *IP* 的群集的准则：

- AP 启动并从 DNS 服务器解析两个导体（每个集群一个）。AP 的导体解析为 Cluster1 的虚拟 IP 和 Cluster2 的虚拟 IP。
- 集群节点的 Nodelist 保存在 AP 上。如果 A-AAC 和 S-AAC 同时关闭，则 AP 将执行内部重启，并尝试节点列表中的不同节点，直到节点列表耗尽。
- 如果禁用 AP 负载均衡，则 ap-group 或 ap-name 的 LMS 必须为 Cluster1 节点的 IP 地址，backup-LMS 必须为 Cluster2 中其他节点的 IP 地址。即，ap-group 或 ap-name 的 LMS 必须配置到 Cluster1 节点，backup-LMS 必须配置到 Cluster2 节点。

提示：在大型部署中，神州云科 建议使用此配置以避免大型故障域。

方案 4：通过跨数据中心的 DNS 解析实现具有多导线的集群

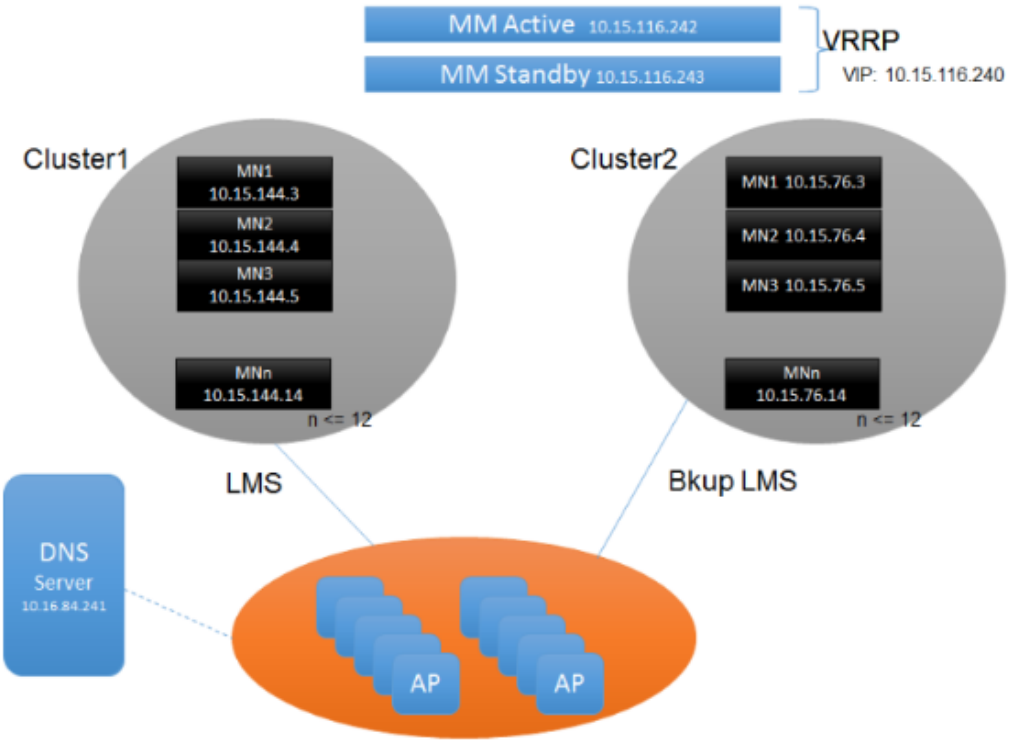
在这种情况下，当 A-AAC 关闭时，AP 将故障转移到 S-AAC。如果 A-AAC 和 S-AAC 同时关闭，并且 AP 尝试联系 Cluster1 中的另一个节点，直到 Cluster1 的节点列表中的所有节点都耗尽，则 AP 会在内部重新启动。如果 AP 无法访问 Cluster1，则故障转移到备份 LMS。

AP 在 Cluster2 的节点上终止，该节点使用旧版故障转移配置为备份 LMS。

如果启用了 LMS 抢占，则当主 LMS 节点在 Cluster1 上启动时，AP 将抢占到 Cluster1。

如果 LMS 抢占被禁用，即使 Cluster1 已启动，AP 仍保留在 Cluster2 上。

如果 AP 在包括 LMS 在内的任何节点上重新启动，则 AP 会记住节点列表并尝试节点列表中的所有条目。只有当 AP 无法访问任何节点时，才会执行旧版重启。



以下是确保通过 DNS 解析跨数据中心成功部署具有多个导线的集群的准则：

- AP 启动并从 DNS 服务器解析四个导体（每个集群两个）。AP 的导体必须解析为 Cluster1 中的两个节点和 Cluster2 中的两个节点。
- 集群节点的 Nodelist 保存在 AP 上。如果 A-AAC 和 S-AAC 同时关闭，则 AP

将执行内部重启，并尝试节点列表中的不同节点，直到节点列表耗尽。

- 如果 AP 负载均衡开启，则 ap-group 或 ap-name 的 LMS 必须为 Cluster1 节点的 IP 地址，backup-LMS 为 Cluster2 其他节点的 IP 地址。即，ap-group 或 ap-name 的 LMS 必须配置到 Cluster1 节点，备份 LMS 必须配置到 Cluster2 节点。

提示：导体分辨率最多支持 10 个条目。Cluster1 和 Cluster2 中的节点组合可用于 DNS 导体解析。

升级集群

实时升级功能允许您将集群中的受管设备和 AP 升级到最新的 神州云科 OS 版本。通过指定新的映像文件和目标分区，可以无缝升级集群中的受管设备。这是一种实时网络升级，托管设备和 AP 可自动升级，无需任何计划内维护停机。

您还可以将升级安排到指定时间，以避免手动干预。集群将在预定时间自动升级。您可以查看、删除或重新安排计划的集群升级。

实时升级过程经过优化，升级所有设备所需的时间更短。升级过程在实时升级期间跳过网点和网格门户升级，但当集群中的最后一个受管设备成功升级时，这些 AP 将进行标准升级。

从 神州云科 OS 8.8.0.0 开始，Mobility Conductor 上的闪存将用作实时升级的文件服务器，此本地存储的映像将由受管设备使用 HTTP 协议下载。您可以通过从 神州云科 网站下载固件映像，从 Mobility Conductor 的 WebUI 上传固件映像。

升级集群时，将执行以下操作：

1.集群升级管理器将 AP 的信息发送到 AirMatch。

2.AirMatch 创建 AP 的逻辑组，并使用此信息更新集群升级管理器。

3.目标受管设备分配给每个分区中的所有 AP。

4.受管设备将下载新固件。固件下载后发生以下事件：

a.对于每个受管设备，无论分区如何，都会为 AP 平台的小容量启动 AP 映像预加载。例如，一次 AP 平台的 1/8 容量。

b.预加载每个受管设备的所有 AP 后，预加载接下来的几个 AP，并重复此步骤，

直到预加载所有 AP。

5.预加载所有 AP 后，将选择目标受管设备并重新启动。

6.目标受管设备启动后，将选择以此受管设备为目标的分区，并启动 AP 移动。重新启动所有 AP 后，将选择下一个分区并启动 AP 移动。

7.成功升级目标受管设备的所有分区后，将选择另一个目标受管设备，并重复步骤 6，直到所有受管设备成功重新启动。

以下部分介绍如何配置实时升级以及实时升级的限制：

配置实时升级

以下过程介绍如何升级群集：

1. 登录 Mobility Conductor。

2.在“托管网络”节点层次结构中，导航到“维护>软件管理”。

3.从表中选择一个或多个集群。该表仅列出集群，而不列出集群成员。

该表显示集群的名称、托管设备的数量、集群中的 AP 数量以及集群的托管设备上运行的软件版本。

4.在“安装设置”>“时间”菜单中，选择“立即”。

5.在“映像文件”部分中，指定映像文件位置、名称和要使用的协议。输入以下参数的值：

- 服务器 IP 地址 - 服务器的 IP 地址。支持 IPv4 和 IPv6 地址。
- 图像路径 - 图像文件的路径
- 要安装的软件 - 要升级到的版本
- 协议 - 用于传输文件的协议。有效值为：FTP、TFTP 和 SCP。默认值为 TFTP。
- 用户名 - 影像服务器上帐户的用户名。
- 密码 - 服务器上帐户的密码。

6.在“要升级的分区”部分中，指定要安装固件的受管设备分区以及要从中启动固件的位置。选择以下任一分区：

- 分区 0

- 分区 1
- auto

7.单击“安装”以启动升级。

8.若要检查升级状态，请在“托管网络”节点层次结构中导航到“群集>配置”>“服务”。

9.集群名称部分的升级状态与升级状态一起显示。升级的状态可以是以下任何值：

- 升级挂起
- AP 分区正在进行中
- 升级正在进行中
- 升级失败
- 升级完成

10.将显示每个受管设备的状态。同样，也会显示集群中每个 AP 的状态。

您可以通过执行以下命令来使用 Mobility Conductor 文件服务器执行实时升级：

```
(host) [mynode] #lc-cluster <cluster name> initiate upgrade version <img_version>

fileserver http download_from_mm partition <partition_id>
```

要检查升级状态，对于 Cluster1，请执行以下 show 命令：

```
(host)#show lc-cluster cluster1 controller details

(host)#show lc-cluster cluster1 ap details

(host)#show lc-cluster cluster1 upgrade status

(host)#show lc-cluster cluster1 upgrade status verbose

(host)#show lc-cluster cluster1 upgrade stats
```

或者，您也可以执行以下命令以在 Mobility Conductor 中触发集群升级：

```
(host) [mm] [cluster1] #lc-cluster <cluster_name> initiate upgrade version <img_

version> partition <partition_id>
```

- cluster_name - 配置的群集配置文件名称;对应需要升级的集群关联的托管设备和 AP。
- img_version - 目标映像版本，例如 8.2.1_XXXXX。

- partition_id - 要将新映像复制到的受管设备上的分区，有效值为 0 或 1，这是可选的。如果未指定分区，它会自动选取备用引导分区。

提示：文件服务器在升级配置文件中配置。在使用 CLI 升级集群之前，请确保已配置升级配置文件。

提示：从 神州云科 OS 8.9.0.0 开始，“托管”中的“维护”>“软件管理”页面，网络节点层次结构显示存在 RAP，升级具有远程 AP 的集群时，升级可能需要更长的时间消息。

使用 Mobility Conductor File Server 进行升级

传统上，如果不使用外部文件服务器，就无法执行实时升级。但是，从 神州云科 OS 8.8.0.0 开始，Mobility Conductor 上的闪存将用作实时升级的文件服务器，并且此本地存储的映像将由受管设备使用 HTTP 协议下载。您可以通过从 神州云科 网站下载固件映像，从 Mobility Conductor 的 WebUI 上传固件映像。有关详细信息，请参阅计划托管设备的升级。

优化实时升级

以下是为缩短升级时间而执行的优化：

AP 镜像预加载

在实时升级过程中，如果 AP 在 5 分钟内预加载失败，则 AP 将标记为镜像预加载失败重试暂时挂起。预加载所有 AP 映像后，将对所有挂起的 AP 执行重试，等待时间为 5 分钟。如果预加载再次失败，则这些 AP 将标记为映像预加载失败，并且不会执行进一步的重试。与旧版本相比，此机制将整体 AP 映像预加载时间减少了 60%。

控制器和 AP 重新启动失败

在以前的版本中，如果控制器在 30 分钟内无法重新启动，则控制器将被标记为重新启动失败，并且集群升级将中止。因此，群集在升级后的映像中将具有很少的控制器，而在旧映像中将具有很少的控制器。从 神州云科 OS 8.8.0.0 版本开始，即使控制器无法重新启动，集群升级也不会中止，其余控制器也会升级。此外，初始控制器重新启动时间从 30 分钟减少到 15 分钟。

同样，AP 重新启动等待时间从 15 分钟减少到 8 分钟，无需重试。

集群不稳定的计时器重试减少

如果集群不稳定，系统将启动集群不稳定计时器，该计时器为 3 分钟，最大尝试次数为 6 次。在以前的版本中，最大尝试次数设置为 15 次。因此，这有助于在 18 分钟而不是 45 分钟内宣布集群不稳定。

限度

此功能具有以下限制：

- 由于存在映像预加载限制，因此如果不重新加载受管设备，则无法使用两个不同的版本进行群集升级。目前只允许每次托管设备重新启动一次预加载。
- 在集群升级期间，AP 预加载的状态不会显示在 WebUI 中。
- 如果之前的升级导致子集群拆分，则无法触发集群升级。
- 网状节点不支持集群滚动升级。因此，无法对网格部署执行集群升级。
- 建议不要在多区域部署中使用实时升级。每个区域都可以使用实时升级，但数据区域上的升级并非无中断。
- 远程 AP 不支持实时升级，原因如下：
  - 在实时升级过程中，当远程 AP 被预加载、重新启动并移动到升级后的受管设备时，预加载的远程 AP 将使用受管设备交换机 IP 而不是公共 IP 移动到受管设备。因此，远程 AP 无法在集群上启动。
  - 在远程 AP 部署中，集群实时升级需要很长时间，因为没有连续的 RF 域，因此，远程 AP 的信道分区可能过多。由于每个分区都将被预加载、重新启动，然后移动到升级后的受管设备，因此完成升级过程需要很长时间。

计划集群升级

从 神州云科 OS 8.4.0.0 开始，计划集群升级允许您将升级计划到指定时间，以避免手动干预。集群将在预定时间自动升级。您可以查看、删除或重新安排计划的集群升级。

您还可以在同一时间或不同时间为一个或多个配置文件安排集群升级。

当 Mobility Conductor 重新启动或进程重新启动时，此功能能够保留已配置的计划升级。它还允许您将计划的升级同步到备用 Mobility Conductor。如果 Mobility Conductor 配置了主用和备用设备，则计划升级信息将通过数据库同步在主用和备用之间同步。当 Mobility Conductor 变为活动状态时，将启动升级。

关键考虑因素

- 只能将升级计划到将来的时间，从受管设备的当前时间起最多 30 天。
- 计划的时间始终参考群集中的受管设备。
- 所有网络节点都必须进行 NTP 同步。

限度

- DST 时间更改时间不会针对计划的升级自动调整。
- 在受管设备中手动更改的时间不会针对计划升级自动调整。
- 计划升级只能使用升级配置文件启动。

配置计划升级

要配置计划升级，请通过 WebUI 或 CLI 执行以下步骤：

要配置计划的集群升级。

要计划计划的群集升级，请执行以下操作：

(host) [mm] (config) #lc-cluster <cluster_prof> schedule upgrade <version> <year> <month>

<day> <hh> <mm> <ss>

参数说明	描述
cluster_prof	计划升级的集群配置文件
version	集群将升级到的版本
year	升级年份
month	升级月份
day	升级日
hh	升级小时
mm	升级分钟数

SS	升级秒数

例：

(host) [mm] (config) #lc-cluster <cluster_prof> schedule upgrade version 8.4.0.0-

sangiovese_73823 2018 04 10 00 00 00

查看计划的集群升级状态

(host) [mm] #show lc-cluster scheduled-upgrades

例：

(host) [mm] #show lc-cluster scheduled-upgrades

Cluster Scheduled Upgrade Status

Profile	To Version	Partition ID	AP Preload size	Scheduled Time	MD Timezone
v4	8.4.0.0-mm-dev_65200	Default	100	Fri Jun 8 15:00:00	2018 Asia/Tokyo

删除或中止计划的群集升级

(host) [mm] (config) #lc-cluster <cluster_prof> abort scheduled-upgrade

重新安排群集升级

(host) [mm] (config) #lc-cluster v4 re-schedule upgrade <version> <year> <month> <day><hh> <mm> <ss>

提示：若要重新计划群集升级，必须已计划升级。

例：

(host) [mm] (config)#lc-cluster v4 re-schedule upgrade version 8.2.0.1 2018 6 6 0 50 0

群集故障排除

本部分提供可用于对群集配置中的不同方案进行故障排除的命令。

集群中的不同控制平面进程是 GSM 管理器 （GSM）、集群管理器 （CM）、工作站管理器 （STM） 和 AUTH。在 AP 上，主要模块是 A-STM 和 ASAP（数据路径）。

以下是群集中一些常见故障排除方案的列表：

- 集群形成不成功
- AP 重启
- 用户无法连接到集群
- 用户正在被取消身份验证

集群形成不成功

群集中的所有托管设备统称为群集成员。当集群中的所有受管设备相互连接时，集群形成成功。

集群形成不成功的一些原因如下:

1. 如果未执行集群组成员身份。

2.如果群集中未列出所有受管设备。

3.如果存在连接问题，并且托管设备无法访问其对等设备。

4.如果未形成 IPsec SA。

要检查集群形成的状态，请执行 show lc-cluster group membership 命令。

```
(host) [mynode] #show lc-cluster group-membership

Mon Dec 21 17:30:51.952 2015

Cluster Enabled, Profile Name = "6NodeCluster"

Redundancy Mode On

Active Client Rebalance Threshold = 50%

Standby Client Rebalance Threshold = 75%

Unbalance Threshold = 5%

Cluster Info Table

------------------

Type     IPv4 Address      Priority Connection-Type   STATUS

---- --------------- -------- ---------------   ------

self     10.15.116.3       128          N/A            ISOLATED (Leader)
```

peer 10.15.116.4 128 L3-Connected CONNECTED-FROM-SELF-DISCONNECTED-FROM-PEERS

peer 10.15.116.5 128 L3-Connected CONNECTED-FROM-SELF-DISCONNECTED-FROM-PEERS

peer 10.15.116.8 128 L3-Connected CONNECTED-FROM-SELF-DISCONNECTED-FROM-PEERS

peer 10.15.116.9 128 N/A SECURE-TUNNEL-NEGOTIATING

peer 10.15.116.10 128 N/A SECURE-TUNNEL-NEGOTIATING

DISCONNECTED

INCOMPATIBLE

DISCONNECTED-FROM-SELF-CONNECTED-FROM-PEERS",

CONNECTED-FROM-SELF-DISCONNECTED-FROM-PEERS",

SECURE-TUNNEL-NEGOTIATING

SECURE-TUNNEL-ESTABLISHED

CONNECTED

群集状态

状态	原因
不兼容	在以下情况下，可能会发生此错误： 如果两个受管设备运行不同的 神州云科 OS 版本，则会发现构建字符串不匹配，并且受管设备不是集群的一部分。
断开连接	在以下情况下，可能会发生此错误： ● 如果群集中的受管设备均未处于 CONNECTED 状态。 ● 如果群集中受管设备之间的物理连接存在问题。 ● 如果其中一个端口是不受信任的节点。
安全隧道协商	此状态将在很短的时间内显示，直到设置 IPsec 隧道。如果状态仍然存在，则表示 IPsec 隧道设置存在问题。
连接自对端断开	在以下情况下，可能会发生此错误： 受管设备 1 和受管设备 2 已连接。稍后在群集中引入受管设备 3。受管设备 1 和受管设备 3 已连接，但受管设备 2 和受管设备 3 未连接。

集群进入 CONNECTED 状态后，检查它是否为 L2 连接，其中对等体上的每个 VLAN 都可以访问，具体取决于 VLAN 探测。使用以下命令检查 VLAN 探测状态：

(host) [mynode] #show lc-cluster vlan-probe status

如果对分配交换机进行了一些 VLAN 更改，请在受管设备上执行 VLAN 探测算法：

(host) [mynode] (config) #lc-cluster start-vlan-probe

AP 重启

当未为 AP 分配 S-AAC 时，AP 会重新启动。以下是 AP 重新启动的一些原因列表：

1. 平台容量 — 如果受管设备已达到其最大容量，或者已具有可以支持的最大 AP。

若要解决此问题，请执行以下步骤：

- 添加其他受管设备或升级现有受管设备以支持更多数量的 AP。
- 对网络配置进行返工。

2.多个受管设备关闭 - 如果 S-AAC 关闭，备用控制器 （S-UAC） 将成为主动控制器 （A-UAC）。但是，如果 A-AAC 也出现故障，则 AP 将重新启动。

要解决此问题，请确保正确选择配电交换机以处理所需的秤。

用户无法连接到集群

以下是用户可能无法连接到群集的一些原因列表：

1.AP 和受管设备对用户具有不同的角色。

每个用户都有一个 A-UAC，如果用户的 UAC 的 AP 信息与实际受管设备的信息不同，并且受管设备没有关于用户的此信息，则它将拒绝该用户。

2.未建立 IPsec 隧道。

如果在 AP 上启用了 CPsec，则 AP 应与群集中的所有受管设备建立 IPsec 隧道。如果未建立 IPsec 隧道，则用户无法连接到集群。

3.802.1X 客户端的 AP 配置不完整。

要连接 802.1X 客户端，组播密钥 （mkey） 必须从 AAC 转到 UAC。如果 mkey 在 UAC

中不可用，则不会显示状态，并且用户无法连接。要检查 AP 配置是否不完整，请执行 show auth-tracebuf 命令。

用户正在被取消身份验证

以下是用户可能被取消身份验证的一些原因列表：

1. 集群故障转移 - 如果用户在集群中被取消身份验证，请检查是否同时存在集群故障转移。要检查处于 DOWN 状态的受管设备何时首次断开连接，请使用 show lc-cluster heartbeat counters 命令。

a.如果在受管设备关闭时发生故障转移，请使用 show lc-cluster vlan-probe status 命令检查受管设备是否已进行 L2 连接。

b.如果受管设备已连接 L3，请使用 lc-cluster excludevlan 命令修复 VLAN 探测<vlan-number>。

2.如果受管设备已连接 L2 并且问题仍然存在，请在 AP Rebootstrap 中检查解决方案。

3.如果 AP 未重新启动且没有故障转移，请联系技术支持团队。

启用调试

在群集设置中，添加了轻量级跟踪机制，以收集调试信息，同时将对群集的性能影响降至最低。

在 7200 系列受管设备中，调试信息收集在受管设备的 flash1 分区中，可用于将来的故障排除。在 7000 系列和 7205 托管设备中，没有 flash1 分区，需要 USB 设备来收集此调试信息，这些信息可用于将来的调试或问题报告。

执行以下跟踪命令，收集集群的调试信息：

(host) #gsm trace channel ap application stm

(host) #gsm trace channel ap application dds

(host) #gsm trace channel ap application cluster_mgr

(host) #gsm trace channel radio application stm

(host) #gsm trace channel radio application dds

(host) #gsm trace channel sta application stm

(host) #gsm trace channel sta application auth

(host) #gsm trace channel sta application dds

(host) #gsm trace channel sta application cluster_mgr

(host) #gsm trace channel mac_user application auth

(host) #gsm trace channel mac_user application dds

(host) #gsm trace channel mac_user application cluster_mgr

(host) #gsm trace channel ip_user application auth

(host) #gsm trace channel ip_user application dds

(host) #gsm trace channel user application auth

(host) #gsm trace channel user application dds

(host) #gsm trace channel sectun application dds

(host) #gsm trace channel sectun application cluster_mgr

(host) #gsm trace channel key_cache application auth

(host) #gsm trace channel key_cache application dds

(host) #gsm trace channel pmk_cache application stm

(host) #gsm trace channel pmk_cache application auth

(host) #gsm trace channel pmk_cache application dds

(host) #gsm trace channel rep_key application dds

(host) #gsm trace channel rep_key application cluster_mgr

(host) #gsm trace channel cluster application dds

(host) #gsm trace channel cluster application cluster_mgr

(host) #gsm trace channel bucket_map application stm

(host) #gsm trace channel bucket_map application auth

(host) #gsm trace channel bucket_map application dds

(host) #gsm trace channel bucket_map application cluster_mgr

(host) #gsm trace channel cluster_bss application dds

(host) #gsm trace channel cluster_bss application cluster_mgr

(host) #gsm trace channel cluster_aac application dds

(host) #gsm trace channel cluster_aac application cluster_mgr

(host) #gsm trace channel cluster_ap application dds

(host) #gsm trace channel cluster_ap application cluster_mgr

(host) #gsm trace channel bss application stm

(host) #gsm trace channel bss application auth

(host) #gsm trace channel bss application cluster_mgr

(host) #dds trace receive channel sta peer $peerIP

(host) #dds trace transmit channel sta peer $peerIP

(host) #dds trace receive channel ip_user peer $peerIP

(host) #dds trace transmit channel ip_user peer $peerIP

(host) #dds trace receive channel mac_user peer $peerIP

(host) #dds trace transmit channel mac_user peer $peerIP

(host) #dds trace receive channel key_cache peer $peerIP

(host) #dds trace transmit channel key_cache peer $peerIP

(host) #dds trace receive channel pmk_cache peer $peerIP

(host) #dds trace transmit channel pmk_cache peer $peerIP

(host) #dds trace receive channel bucket_map peer $peerIP

(host) #dds trace transmit channel bucket_map peer $peerIP

(host) #dds trace receive channel cluster_bss peer $peerIP

(host) #dds trace transmit channel cluster_bss peer $peerIP

(host) #dds trace receive channel cluster_sta peer $peerIP

(host) #dds trace transmit channel cluster_sta peer $peerIP

(host) #dds trace receive channel cac_usage peer $peerIP

(host) #dds trace transmit channel cac_usage peer $peerIP

(host) #dds trace receive channel cluster_aac peer $peerIP

(host) #dds trace transmit channel cluster_aac peer $peerIP

(host) #dds trace receive channel cluster_ap peer $peerIP

(host) #dds trace transmit channel cluster_ap peer $peerIP

(host) #ap debug stm-trace category all loglevel debug

(host) #aaa auth-trace loglevel debug

(host) #scm intiate audit <peerip>