

# VMware NSX Advanced Load Balancer GSLB 指南

VMware NSX Advanced Load Balancer 20.1.4

VMware NSX Advanced Load Balancer 20.1.4

您可以从 VMware 网站下载最新的技术文档:

<https://docs.vmware.com/cn/>。

**VMware, Inc.**  
3401 Hillview Ave.  
Palo Alto, CA 94304  
[www.vmware.com](http://www.vmware.com)

**威睿信息技术（中国）有  
限公司**  
北京办公室  
北京市  
朝阳区新源南路 8 号  
启皓北京东塔 8 层 801  
[www.vmware.com/cn](http://www.vmware.com/cn)

上海办公室  
上海市  
淮海中路 333 号  
瑞安大厦 804-809 室  
[www.vmware.com/cn](http://www.vmware.com/cn)

广州办公室  
广州市  
天河路 385 号  
太古汇一座 3502 室  
[www.vmware.com/cn](http://www.vmware.com/cn)

版权所有 © 2021 VMware, Inc. 保留所有权利。 [版权和商标信息](#)

# 目录

## 1 简介 5

请求流 9

GSLB 支持的功能 12

## 2 NSX Advanced Load Balancer GSLB 架构和术语 14

NSX Advanced Load Balancer GSLB 站点 15

NSX Advanced Load Balancer DNS 虚拟服务 20

部署场景 21

功能 23

将 GSLB 服务选择性分配给 DNS 虚拟服务 26

GSLB 的高可用性建议 27

GSLB 服务 27

GSLB 的负载均衡算法 28

GSLB 成员的基于地理位置的负载均衡算法 29

基于拓扑的 GSLB 算法 35

GSLB 池 36

GSLB 池成员 38

GSLB 运行状况监控器 39

优化运行状况检查 44

GSLB 站点持久性 45

GSLB 站点 Cookie 持久性 45

GSLB 的用户角色和帐户 56

根据特权配置 NSX Advanced Load Balancer UI 访问 57

从从属站点中启用 GSLB 配置更改 58

插入 DNS 的扩展机制 (EDNS) 客户端子网选项 61

EDNS 和 ECS 选项如何与 NSX Advanced Load Balancer DNS 一起使用 62

与第三方 GSLB 站点集成 67

附加信息 68

## 3 GSLB 配置 70

使用 NSX Advanced Load Balancer UI 配置 GSLB 站点 70

指定 GSLB 主站点并添加站点配置 75

将多个子域与 DNS 虚拟服务相关联 80

GSLB 的 DNS 配置 81

添加第三方站点 82

使用 NSX Advanced Load Balancer CLI 配置 GSLB 站点 84

使用 NSX Advanced Load Balancer CLI 配置直通服务器 87

## GSLB 的 DNS 87

NSX Advanced Load Balancer 托管的虚拟服务的 DNS 89

将 GSLB 服务选择性分配给 DNS 虚拟服务 89

## GSLB 服务配置 94

使用 NSX Advanced Load Balancer UI 配置 GSLB 服务基本设置 94

使用 NSX Advanced Load Balancer UI 配置 GSLB 服务高级设置 102

使用 NSX Advanced Load Balancer UI 配置 GSLB 运行状况监控器 111

GSLB 负载均衡算法 114

将第三方服务与第三方站点相关联 125

使用 NSX Advanced Load Balancer CLI 配置租户 127

配置企业/外部 DNS 服务器以将子域委派给 NSX Advanced Load Balancer DNS 服务 127

A 记录返回：启用解析 CNAME 128

## 4 GSLB Canary 更新 129

启用手动复制 130

## 5 使用 GSLB 133

如何将主站点更改为新的主站点 133

为 GSLB 服务配置的 VIP 和运行 VIP 不同步 136

解决方案 137

NSX Advanced Load Balancer GSLB 环境中的升级 138

解决基于地理位置的算法问题 143

错误场景 146

故障场景和解决办法 147

## 6 常见用例的配置 154

NAT 感知公用-专用 GSLB 配置 154

GSLB 通配符 FQDN 157

## 7 额外的集成 160

GSLB 与 F5 GTM 的集成 160

AWS 多区域、多可用区部署中的 NSX Advanced Load Balancer GSLB 162

方法 1 163

方法 2 166

Azure DNS 专用区域中的 GSLB 167

从一个 VNet 中解析另一个 VNet 中托管的应用程序 174

从本地解析 Azure VNet 中托管的应用程序 175

不同虚拟网络中的虚拟机之间的名称解析 176

分析 176

# 简介

# 1

本指南提供了有关使用 NSX Advanced Load Balancer 的全局服务器负载均衡 (Global Server Load Balancing, GSLB) 的信息，它为多个地理位置分散的应用程序提供负载均衡，同时提供集中的配置、应用程序监控和分析。

NSX Advanced Load Balancer 中的 GSLB 在部署到多个位置（通常是多个数据中心和/或公有云）的应用程序实例之间均衡应用程序的负载。NSX Advanced Load Balancer 或第三方应用程序交付控制器 (Application Delivery Controller, ADC) 解决方案管理每个位置中的应用程序负载。

通常实施 GSLB 是为了实现以下应用程序目标：

- 为地理位置分散的区域中的用户/客户端提供最佳的应用程序体验
- 提供恢复数据中心或网络连接中断的能力
- 执行到另一个数据中心的非中断性迁移或添加另一个数据中心

## GSLB 概览

GSLB 包括以下功能：

- 1 它选择将客户端请求传送到位置（数据中心/云）
- 2 它监控虚拟服务的运行状况以选择最佳位置（即，排除未正常运行的虚拟服务）
- 3 它在 GSLB 站点之间同步配置和状态，以便在发生特定故障时继续执行功能 1 和功能 2

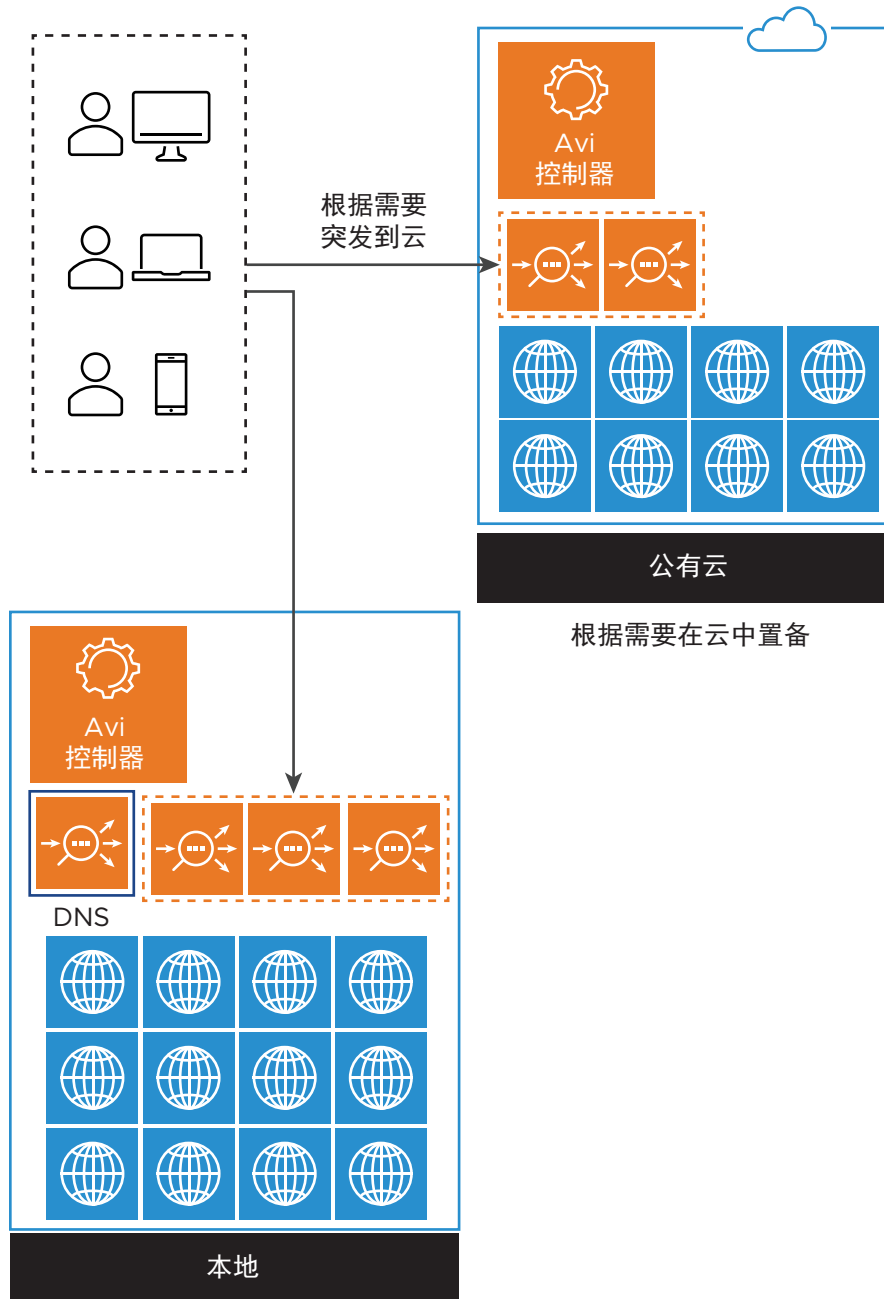
在客户端（通常是浏览器）对完全限定域名 (Fully Qualified Domain Name, FQDN) 执行 DNS 查询时，GSLB 使用最佳应用程序实例的 IP 地址 (VIP) 进行响应。最佳地址可能并且将会根据负载均衡算法、应用程序实例运行状况和客户端位置而发生变化。

## GSLB 用例

以下是 NSX Advanced Load Balancer GSLB 的一些用例：

- 地理位置分散的用户的最佳应用程序体验
  - 应用程序部署在多个数据中心。
  - GSLB 可以将用户请求重定向到最佳位置。

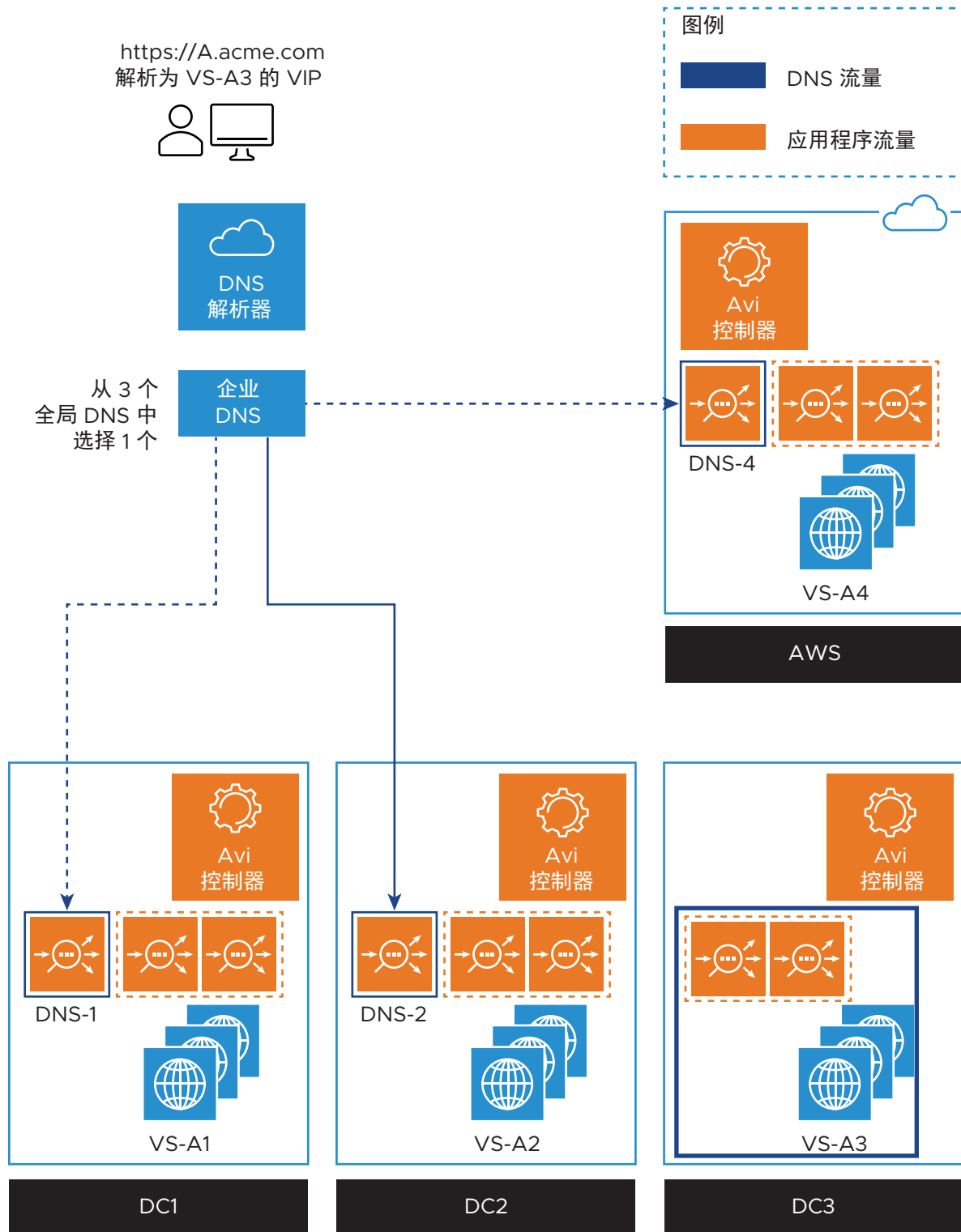
- 跨数据中心的程序高可用性
  - 应用程序部署在多个数据中心。
  - 如果数据中心发生故障，在其余数据中心运行的应用程序实例可以接管用户流量。
- 灾难恢复
  - 应用程序部署在两个数据中心。
  - 虽然两个数据中心都正常运行，但所有流量传送到主 DC。
  - 如果主 DC 发生故障，全局 DNS 将所有用户流量传送到另一个 DC。
- 具有云突发的混合云（如下所示）
  - 应用程序部署在私有云和公有云中。
  - 如果应用程序遇到异常高的请求负载，NSX Advanced Load Balancer GSLB 将突发到公有云站点以分摊负载。



## NSX Advanced Load Balancer GSLB 的工作方式

例如，请参阅下图：

图 1-1. FQDN 地址解析



- NSX Advanced Load Balancer 在 4 个位置（GSLB 站点）中运行，其中的三个位置在本地，另一个位置在 Amazon Web Services (AWS) 中。每个站点具有自己的 NSX Advanced Load Balancer 控制器集群（由单个控制器图标表示）。



- 应用程序“A”在所有 4 个位置中运行虚拟服务。这些虚拟服务是由 VS-A1 到 VS-A4 标识的。
- 4 个位置中的三个位置（DC-1、DC-2 和 AWS）具有同步的全局 DNS 服务（DNS-1、DNS-2 和 DNS4）。对于子域 A.acme.com，它们具有同等的权威性。
- 第 4 个站点 (DC-3) 不运行全局 DNS 服务。

本章讨论了以下主题：

- [请求流](#)
- [GSLB 支持的功能](#)

## 请求流

本节介绍了 GSLB 应用程序的用户请求流。

### 步骤

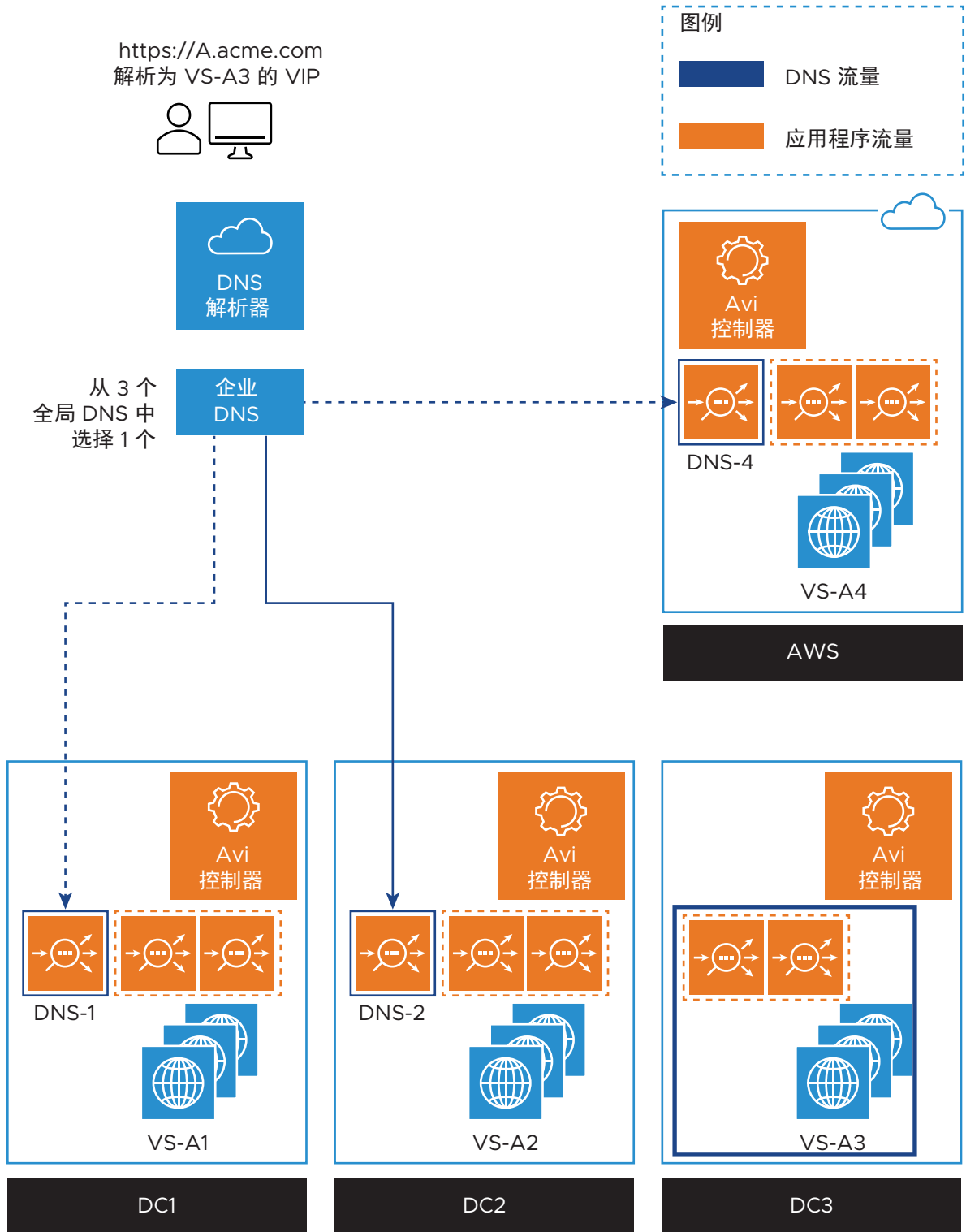
#### 1 FQDN 地址解析

图 1 显示客户端发送 HTTPS 请求以下载应用程序 A 的主页。其 FQDN (A.acme.com) 必须映射到客户端还不知道的 IP 地址。DNS 解析器的分层树最终确定 acme.com 的企业 DNS。

该企业 DNS 将请求转发到三个 GSLB DNS 实例之一，因为域 A.acme.com 已委派给 NSX Advanced Load Balancer 的全局 DNS（此处为 DNS-2）。

DNS-2 具有 4 个候选的最佳虚拟服务选项：VS-A1、VS-A2、VS-A3 和 VS-A4。它根据负载均衡算法、运行状况、客户端位置和其他因素选择了 VS-A3。DNS-2 使用 VS-A3 的 VIP 响应 DNS 查询，最终将该 VIP 传送到原始客户端。

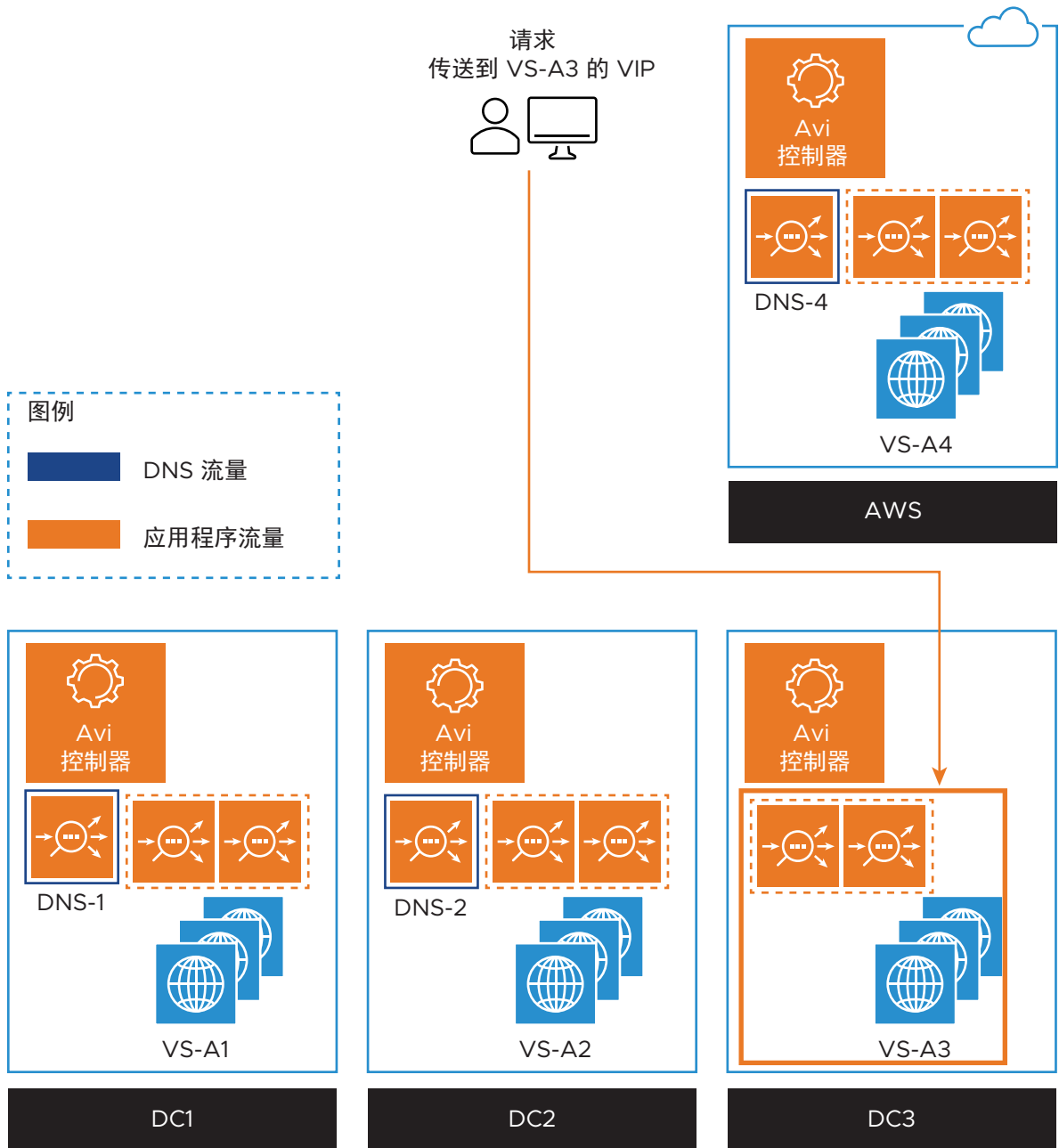
图 1-2. 1. FQDN 地址解析



## 2 应用程序流量传送到最佳虚拟服务

图 2 显示客户端使用 VS-A3 的 VIP 发送其 HTTP 请求。

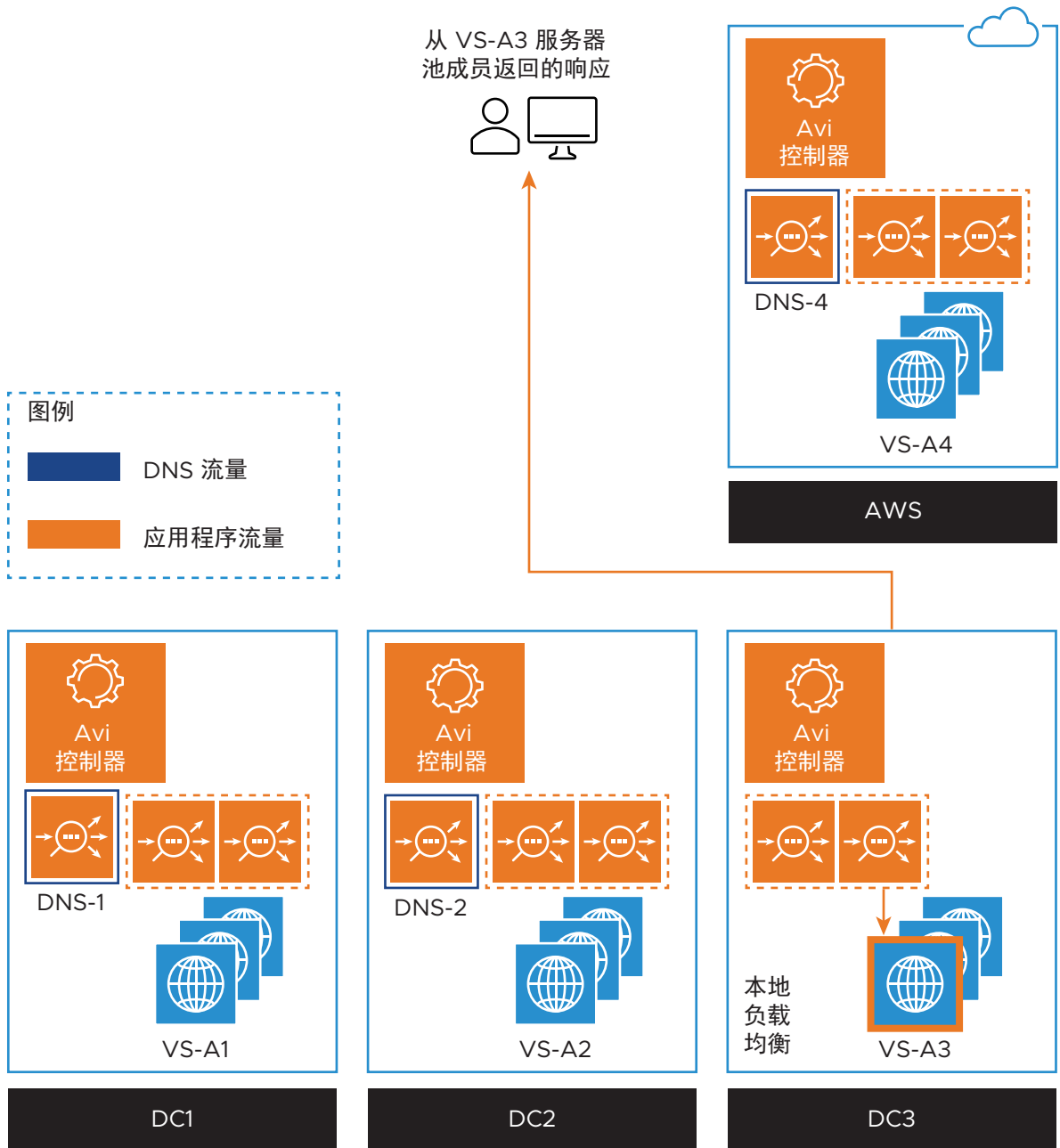
图 1-3. 2. 将应用程序流量传送到最佳 VIP



### 3 本地负载均衡

图 3 显示 SE 组中的一个 SE 接收传送到 VS-A3 的 VIP 的请求。然后，它通过 VS-A3 的 3 个服务器之一对其进行负载均衡。VS-A3 直接响应客户端。

图 1-4. 3. 本地负载均衡



## GSLB 支持的功能

本节介绍了 GSLB 支持的功能。

- 基于 DNS 的负载均衡
- 活动/DR GSLB
- 具有一致哈希的活动/活动 GSLB
- 混合云支持

- 集中的置备和可见性
- 控制平面和数据平面运行状况监控
- 多租户支持
- 第三方负载均衡器支持
- 基于地理位置的活动/活动 GSLB
- 集中的应用程序日志
- 支持两级 GSLB 算法：全局服务级别的基于位置的算法以及 GSLB 池级别的其他算法
- 支持基于 HTTP Cookie 的 GSLB 站点持久性
- 对于 GSLB 站点选择：
  - 能够定义单个回退站点并设置首选站点选项
  - 回退站点限制从 1 个增加到 16 个

# NSX Advanced Load Balancer GSLB 架构和术语

## 2

GSLB 为全局应用程序提供简化且集中的配置和监控。在典型环境中，企业名称服务器将一个或多个子域委派给 GSLB，GSLB 拥有这些域并响应来自客户端的 DNS 查询。GSLB 为备份或灾难恢复应用程序提供一个活动/备份模型，并提供一个活动/活动模型以根据远近程度等响应最佳站点。本节简要说明了 NSX Advanced Load Balancer GSLB 的架构、术语和对象模型。

### 全局应用程序

全局应用程序需要使用能够执行以下功能的解决方案：

- 定义、同步和维护 GSLB 配置。
- 监控配置组件的运行状况。
- 为客户端的 FQDN 请求提供 GSLB DNS 响应以优化客户端的应用程序服务。
- 处理全局应用程序请求。

### 重要功能

GSLB 解决方案应该能够执行以下 4 个重要功能：

功能	责任实体
定义和持续同步/维护 GSLB 配置	NSX Advanced Load Balancer 控制器承担的责任
监控配置组件的运行状况	由 NSX Advanced Load Balancer 控制器和服务引擎 (Service Engine, SE) 共同承担的责任
根据配置的 GSLB 算法，为客户端的 FQDN 请求提供 GSLB DNS 响应以优化客户端的应用程序服务。	在一个或多个 SE 中运行的 NSX Advanced Load Balancer GSLB DNS 承担的责任
处理应用程序请求	放置在 NSX Advanced Load Balancer SE 上和/或在第三方服务器/负载均衡器上运行的服务承担的责任

在 NSX Advanced Load Balancer GSLB 中，单个 GSLB 站点不会执行上述的所有 4 个功能。

### 重要实体

NSX Advanced Load Balancer GSLB 中涉及的重要实体包括：

- [NSX Advanced Load Balancer GSLB 站点](#)

- NSX Advanced Load Balancer DNS 虚拟服务
- GSLB 服务
- GSLB 池
- GSLB 池成员
- GSLB 的负载均衡算法
- GSLB 运行状况监控器

有关更多详细信息，请参阅后面的章节。

本章讨论了以下主题：

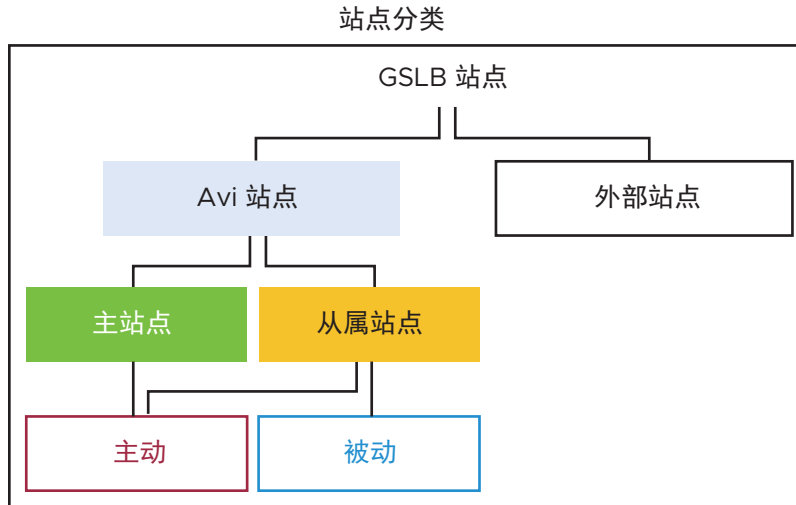
- NSX Advanced Load Balancer GSLB 站点
- NSX Advanced Load Balancer DNS 虚拟服务
- GSLB 服务
- GSLB 的负载均衡算法
- GSLB 池
- GSLB 运行状况监控器
- GSLB 站点持久性
- GSLB 的用户角色和帐户
- 插入 DNS 的扩展机制 (EDNS) 客户端子网选项
- 与第三方 GSLB 站点集成
- 附加信息

## NSX Advanced Load Balancer GSLB 站点

本节重点介绍了 NSX Advanced Load Balancer GSLB 站点。

GSLB 站点具有以下两种类型：

- NSX Advanced Load Balancer 站点：主站点和从属（主动和被动）站点
- 外部站点



## NSX Advanced Load Balancer 站点

NSX Advanced Load Balancer 站点具有一个 NSX Advanced Load Balancer 控制器集群和多个 SE，它们可以执行 4 个关键功能的任意组合。

NSX Advanced Load Balancer 站点进一步划分为两种类型 - GSLB 主站点和从属（主动和被动）站点。

- 管理员最初定义 GSLB 配置的 NSX Advanced Load Balancer 站点被自动指定为 GSLB 主站点。只能将恰好一个主动站点静态指定为 GSLB 主站点。
- 随后添加的其他主动站点是 GSLB 从属站点。GSLB 配置将从主站点传播到这些从属站点。
- 要切换主站点，唯一的方法是从从属站点中覆盖配置。可以在站点发生故障或进行维护时调用该覆盖。

## GSLB 主站点

指定的 GSLB 主站点是执行初始 GSLB 站点配置的主动站点。仅允许登录到主站点以进行 GSLB 配置更改，主站点将这些更改传播到所有可访问的从属站点。要将主站点角色切换为从属站点，唯一的方法是从从属站点中覆盖主站点的配置。可以在站点发生故障或进行维护时调用该覆盖。

### 主动主站点

主动主站点负责执行上一节中提到的重要功能（1、2、3 和 4）。

根据从属站点相对于前三个功能的行为，从属站点进一步划分为主动或被动站点。

**注** 在 NSX Advanced Load Balancer 中，GSLB 主站点定期尝试重新同步处于错误状态的对象。重新同步间隔的默认值为 300 秒。

## GSLB 从属站点

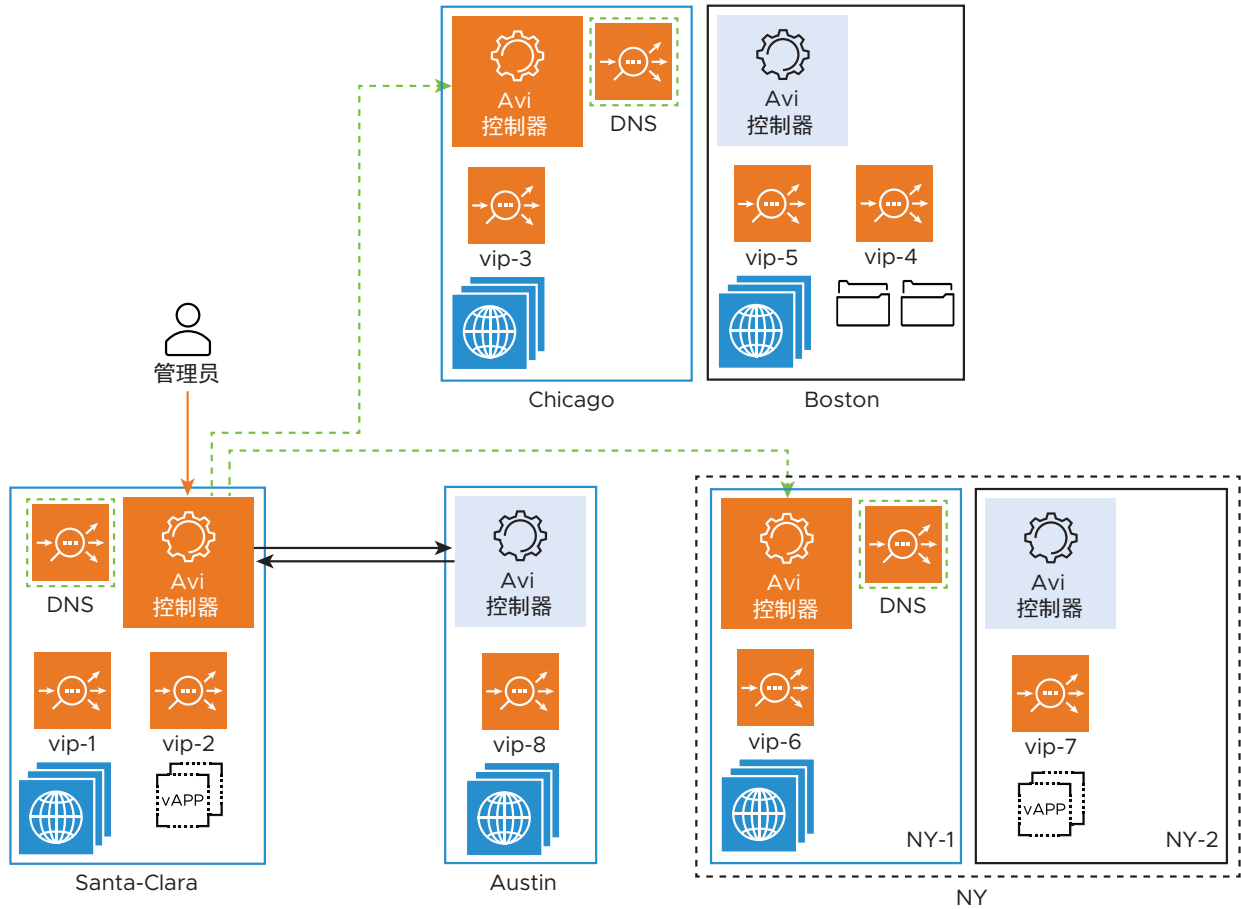
### 主动和被动站点

NSX Advanced Load Balancer GSLB 站点进一步划分为主动或被动 GSLB 站点。

- 主动站点 - 主动站点通常以某种组合形式执行所有三个重要功能 (1-3)。



- 被动站点 - 被动站点仅执行重要功能 (4)，即托管虚拟服务以响应来自全局应用程序客户端的请求。从不要求被动站点提供转向信息（功能编号 3），因此，根本不会将该信息推送到被动站点。被动站点的运行状况是由主动站点上运行的运行状况监控器确定的。它不知道其他站点的运行状况，也无法确定它们的运行状况。



从上图中，观察以下情况：

- Santa Clara、Chicago 和 NY-1 是主动站点。
- Boston、Austin 和 NY-2 是被动站点。
- Santa Clara 是 GSLB 主站点。
- 所有其他主动站点是从属站点。

单个 NSX Advanced Load Balancer 控制器图标用于描述一个 3 节点控制器集群。

---

#### 注

- 所有主动站点之间始终具有全网格连接。这包括从主站点到从属站点、从属站点到从属站点等的连接。
  - 组中的所有主动站点在从主动站点到被动站点的方向启动连接。
  - 所有站点之间的连接是持久性的。
  - 站点之间的任何连接问题是通过重试解决的。对于 GSLB，`clear_on_max_retries` 参数指定允许的最大连接重试次数。如果 NSX Advanced Load Balancer 无法在配置的重试次数内连接到远程站点，启动站点将清除所有缓存的状态，并将远程站点声明为关闭。此后，启动站点根据 `send_interval` 配置定期尝试连接到远程站点。
- 

#### 主动从属站点

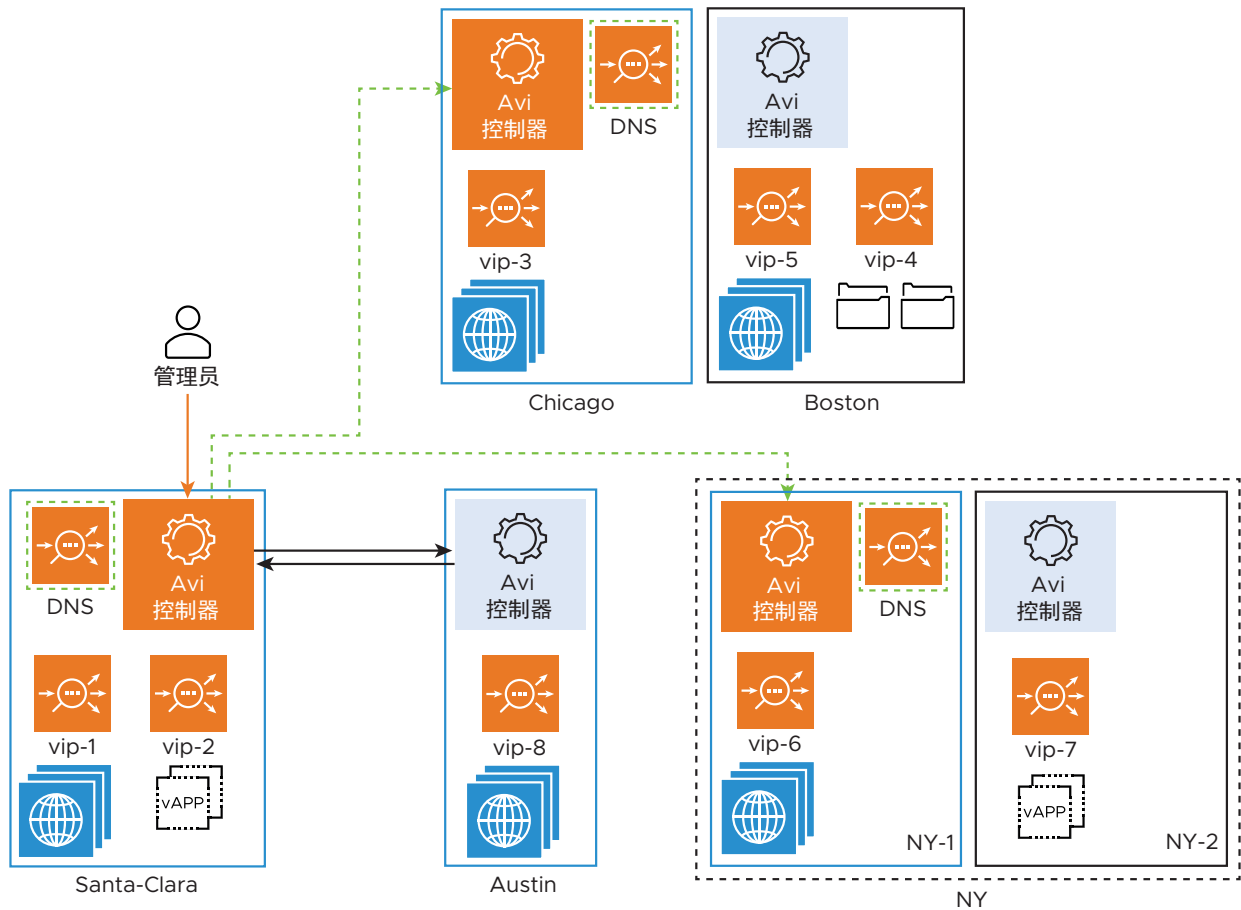
- 从主站点接收 GSLB 配置，因此，可以在主站点发生故障时接替主站点。
- 必须主动监控其他 GSLB 站点的运行状况。
- 可以为 NSX Advanced Load Balancer GSLB 定义的 NSX Advanced Load Balancer 全局应用程序托管权威 DNS。这种冗余使 GSLB 配置的 DNS 服务更加可靠，并提高了地址解析性能。

#### 被动从属站点

- 不接收 GSLB 配置，因此，无法接替发生故障的主站点。
- 不监控其他站点。其运行状况是由主动站点上运行的运行状况监控器确定的。

- 没有参与 GSLB 配置的 DNS。它可以为与 GSLB 部署无关的应用程序运行 DNS。

**注** 一个 NSX Advanced Load Balancer 站点只能恰好参与一个 NSX Advanced Load Balancer GSLB 配置。如果 site\_A 参与 GSLB\_config\_1，尝试将 site\_A 加入 GSLB\_config\_2 将产生错误。



在上面的示例中，Santa Clara、Chicago 和 NY-1 是主动站点。它们分别运行一个 DNS 服务。Boston、Austin 和 NY-2 缺少 DNS 服务；它们是被动站点。

## 外部站点

外部站点可能是第三方 ADC、任何服务器/服务器集、任何 IP 地址等。此类站点只能执行上述**重要功能 4**。外部站点的不透明性使其无法参与 GSLB 站点配置，它仅包含有关 NSX Advanced Load Balancer 控制器集群的信息，例如其地址和凭据。

**注** 并非 NSX Advanced Load Balancer 站点或外部站点上托管的每个虚拟服务都需要参与 NSX Advanced Load Balancer GSLB 解决方案。这意味着，并非每个应用程序都是全局应用程序。

## 建议

- 1 GSLB 部署可以包括或排除 NSX Advanced Load Balancer 控制器。
- 2 如果排除，在首次启用 GSLB 功能时，它将担任主站点角色。

- 3 建议在所有 GSLB 站点上使用相同的 NSX Advanced Load Balancer 版本。
- 4 担任 GSLB 主站点角色的控制器运行的版本不能高于它的任何 GSLB 从属站点。在初始配置和后续[升级](#)期间，该限制都适用。
- 5 在开始执行任何 GSLB 配置之前，必须完全设置了所有成员控制器集群。如果您创建一个 GSLB 配置，然后添加新的控制器，则该配置（尚）未同步到新控制器。

## NSX Advanced Load Balancer DNS 虚拟服务

NSX Advanced Load Balancer DNS 通过 System-DNS 应用程序配置文件类型和使用按数据包负载均衡的网络配置文件运行虚拟服务。NSX Advanced Load Balancer 域名系统 (Domain Name System, DNS) 虚拟服务是委派给适用于 GSLB 的 NSX Advanced Load Balancer 的子域的权威服务。

NSX Advanced Load Balancer DNS 虚拟服务是一个通用的 DNS 基础架构，它主要实施以下功能：

- [DNS 负载均衡](#)
- [托管手动或静态 DNS 条目](#)
- [虚拟服务 IP 地址 DNS 托管](#)
- [托管 GSLB 服务 DNS 条目](#)

### DNS 负载均衡

NSX Advanced Load Balancer 将 DNS 请求转发到后端 DNS 服务器池。将使用具有 System-DNS（或类似）应用程序配置文件的虚拟服务。必须分配加载了 DNS 软件包的后端服务器以完成该操作。

### 托管手动或静态 DNS 条目

NSX Advanced Load Balancer DNS 可以托管手动静态 DNS 条目。您可以指定是否应为给定 FQDN 返回 A、AAAA、CNAME、NS 等记录。

### 虚拟服务 IP 地址 DNS 托管

NSX Advanced Load Balancer DNS 可以托管 NSX Advanced Load Balancer 中配置的虚拟服务的名称和 IP 地址。NSX Advanced Load Balancer 充当托管的虚拟服务的 DNS 提供程序。有关完整的配置详细信息，请参阅[使用 IPAM 和 DNS 的服务发现](#)。

### 托管 GSLB 服务 DNS 条目

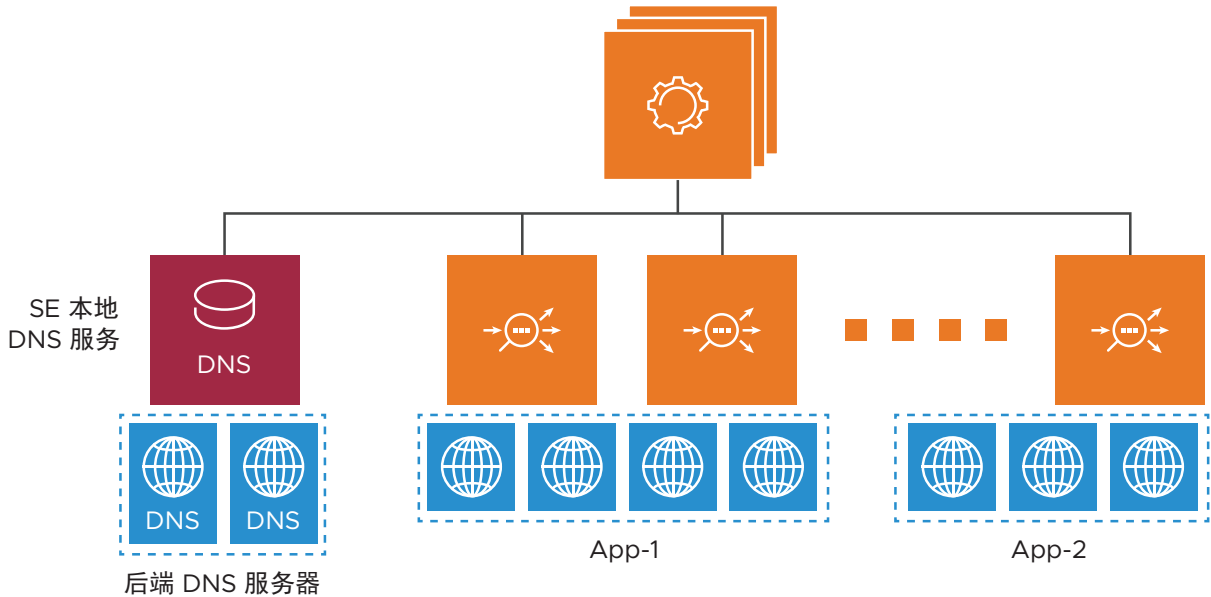
NSX Advanced Load Balancer DNS 虚拟服务可以托管 GSLB 服务 DNS 条目，并根据应用程序服务运行状况、服务负载以及客户端与实施应用程序服务的站点的远近程度自动更新其响应。NSX Advanced Load Balancer GSLB 自动填充这些 DNS 条目。有关 NSX Advanced Load Balancer GSLB 的更多详细信息，请参阅以下几节：

- NSX Advanced Load Balancer GSLB 概览（[第 1 章 简介](#)）
- NSX Advanced Load Balancer GSLB 架构和对象模型（[第 2 章 NSX Advanced Load Balancer GSLB 架构和术语](#)）

- 配置和运行 NSX Advanced Load Balancer GSLB 站点（NSX Advanced Load Balancer GSLB 站点）
- NSX Advanced Load Balancer GSLB 服务运行状况监控器（GSLB 运行状况监控器）

## NSX Advanced Load Balancer DNS 即虚拟服务

下图显示在最左侧的 SE 上托管的 DNS 服务（以绿色表示）。



如果具有匹配的条目，DNS 虚拟服务将响应 DNS 查询。如果未找到匹配的条目并且配置了池成员，则 DNS 虚拟服务将请求转发到后端 DNS 池服务器（以蓝色表示）。

配置为 A/A、A/S、N+M 模式的 DNS 虚拟服务支持运行状况监控。

可以为 NSX Advanced Load Balancer 配置多个 DNS 虚拟服务。

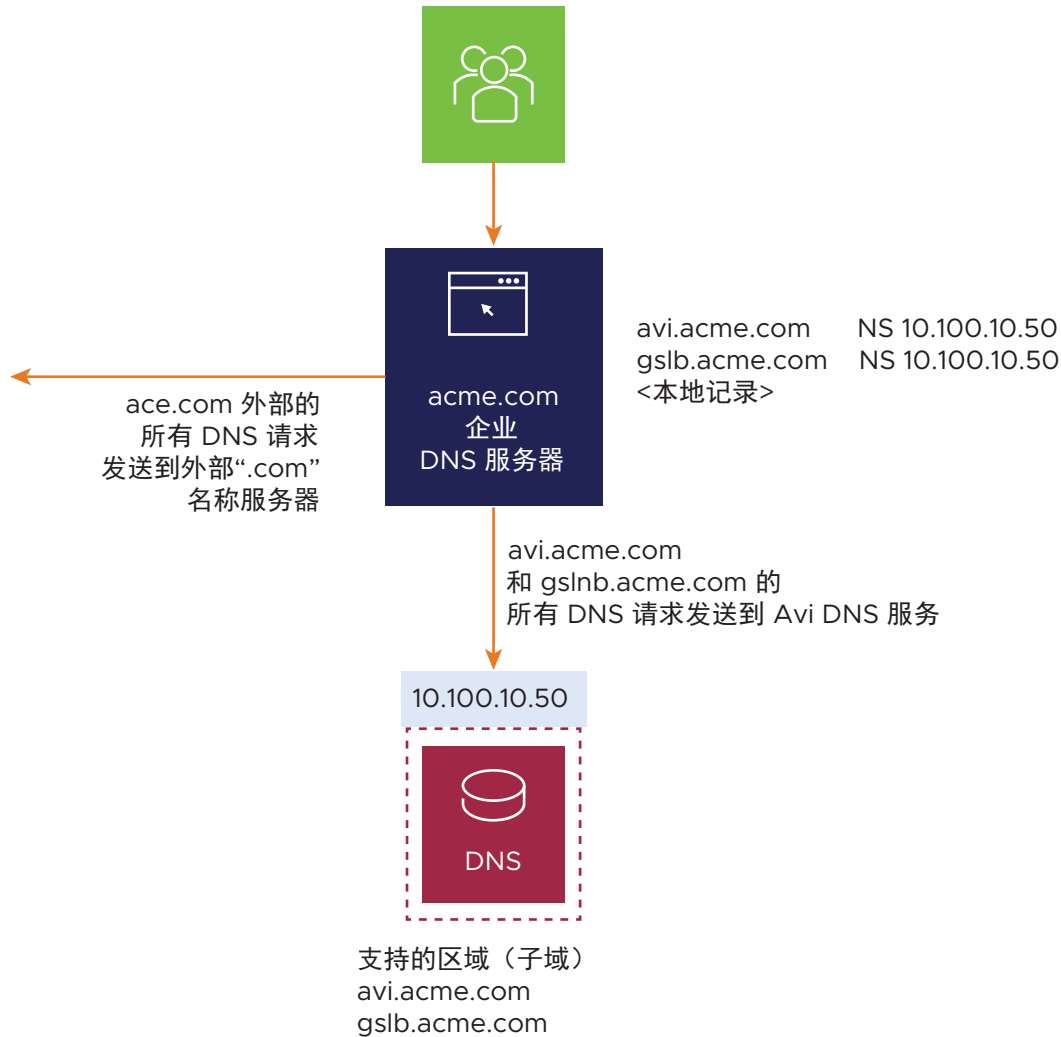
NSX Advanced Load Balancer DNS 虚拟服务支持分析和客户端日志，该服务可以充当一个或多个子域（区域）的权威 DNS 服务器。

## 部署场景

本节重点介绍了部署 NSX Advanced Load Balancer DNS 服务的几个场景。

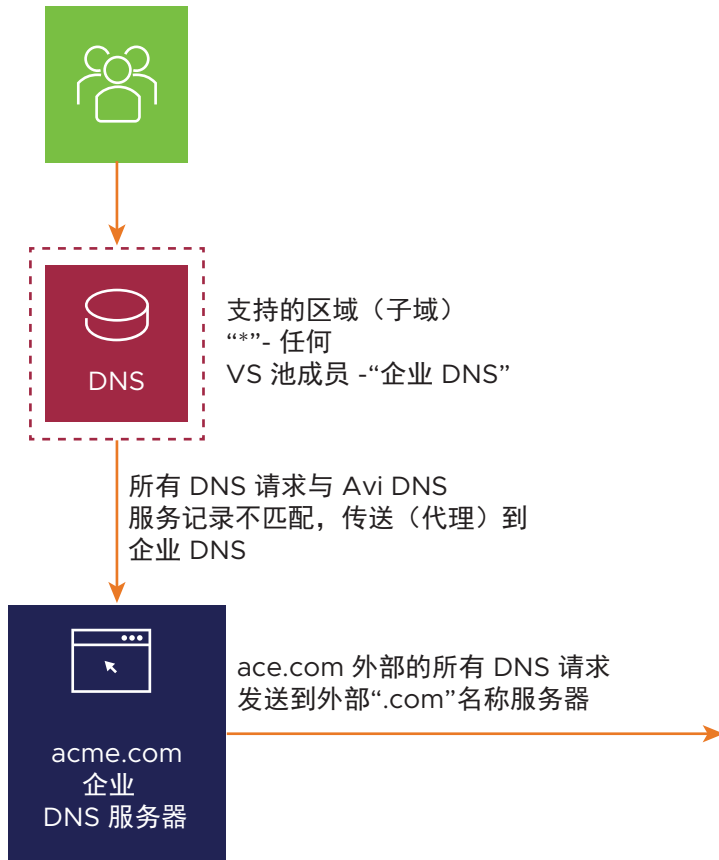
### 子域（区域）的权威名称服务器

企业名称服务器将一个或多个子域委派给 NSX Advanced Load Balancer DNS 服务，而 DNS 服务充当它们的权威 DNS 服务器。在下面显示的示例中，avi.acme.com 和 gslb.acme.com 是子域。通常，企业名称服务器具有一个指向 NSX Advanced Load Balancer DNS 服务 (10.100.10.50) 的名称服务器 (Name Server, NS) 记录。这些子域的客户端查询直接发送到 NSX Advanced Load Balancer，而 acme.com 外部的所有 DNS 请求发送到外部 “.com” 名称服务器。



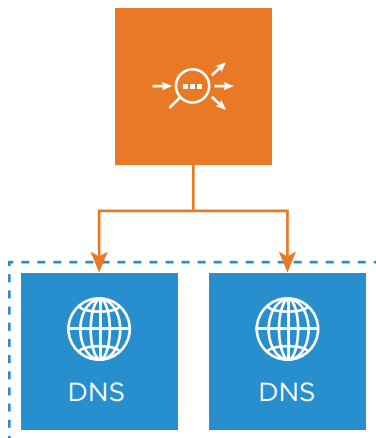
## 域的主名称服务器

在以下情况下，NSX Advanced Load Balancer DNS 响应它已配置为支持的任何区域：其中，域具有一个主名称服务器，并将请求传送到企业名称服务器。与 NSX Advanced Load Balancer DNS 记录不匹配的 DNS 查询传送（代理）到企业 DNS 服务器，这是通过为该用途创建的虚拟服务池完成的。如果该池的成员收到企业域（此处为 `acme.com`）外部的 DNS 请求，它们将这些请求发送到其外部 “.com” 名称服务器。



## 负载均衡

NSX Advanced Load Balancer SE 组汇集了企业 DNS 服务器，并将它们作为单个扩展的 DNS 服务进行公开。



## 功能

本节介绍了以下功能：

- 可见性和分析

## ■ 日志设置

### 可见性和分析

导航到**应用程序 > 虚拟服务**，然后单击为 DNS 配置的虚拟服务的名称。例如，DNS-Site-US-East。

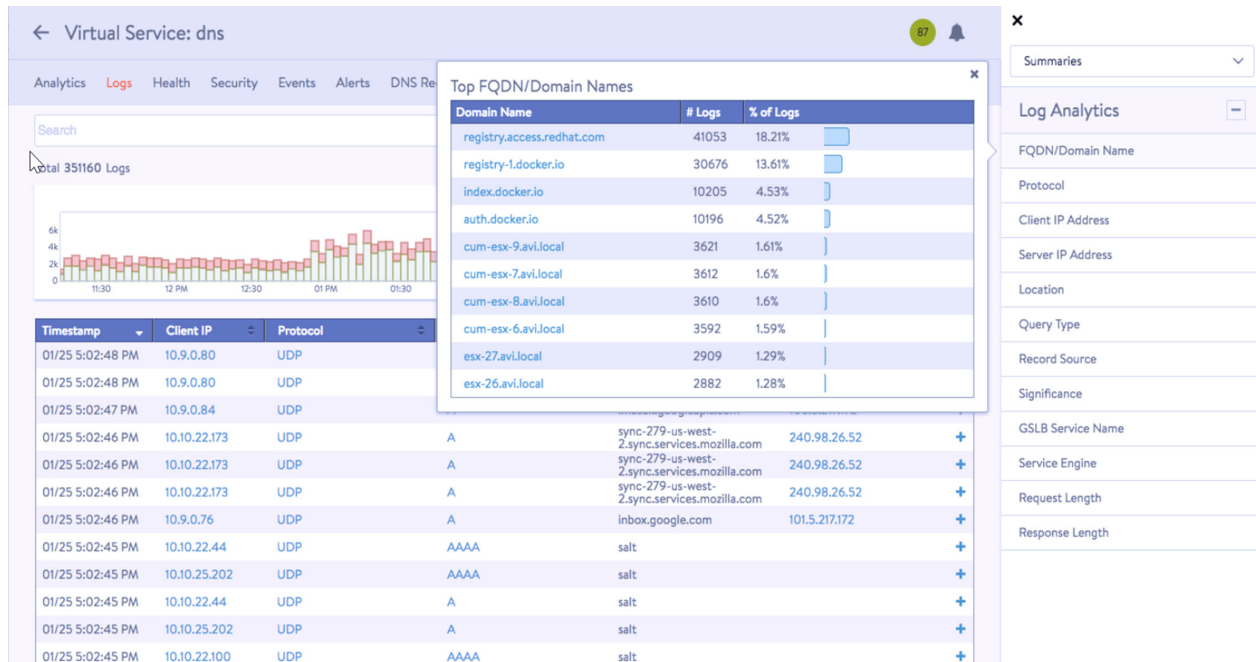
分析选项卡显示所需的衡量指标。

日志选项卡提供有关来自客户端的 DNS 查询的详细信息，包括 FQDN、查询类型、严重错误和响应（例如 IP 地址、CNAME、SRV）等。

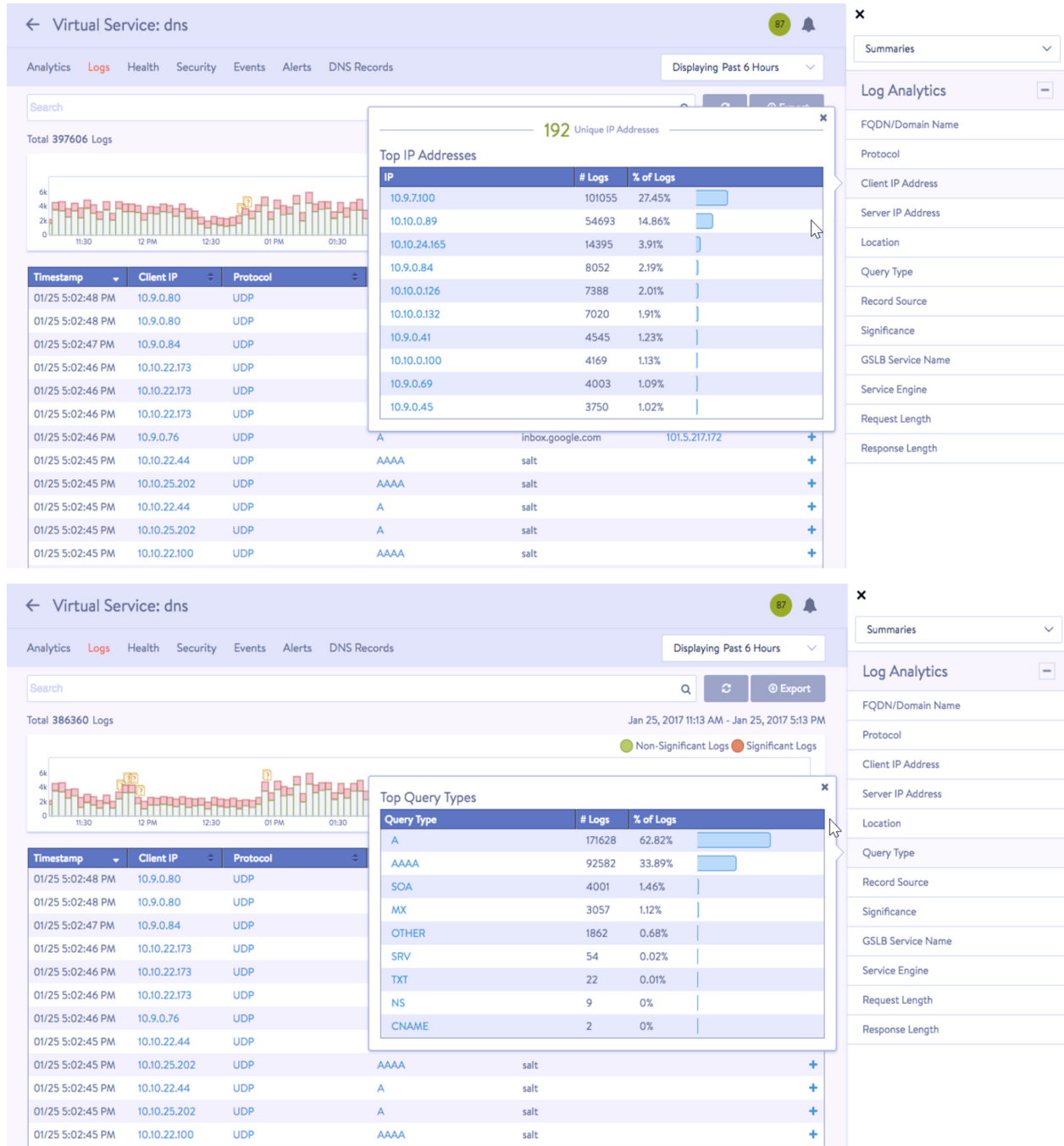
### 日志设置

- 建议不要记录非重要日志，因为 DNS 服务通常会收到大量 DNS 请求，从而导致日志条目数过多。
- 非重要日志的分类也是非常重要的。如果某些错误是特定部署中的典型错误，应从重要日志中排除这些错误。
- 有关排除 DNS 错误的更多详细信息，请参阅排除 DNS 错误一节。

根据日志分析选择器中的要求选择可用的选项，如以下示例中所示：







Virtual Service: dns

Analytics

Logs

Health

Security

Events

Alerts

DNS Records

Displaying Past 6 Hours

Search

Total 386360 Logs

Jan 25, 2017 11:13 AM - Jan 25, 2017 5:13 PM

Non-Significant Logs

Significant Logs

Timestamp	Client IP	Protocol
01/25 5:02:48 PM	10.9.0.80	UDP
01/25 5:02:48 PM	10.9.0.80	UDP
01/25 5:02:47 PM	10.9.0.84	UDP
01/25 5:02:46 PM	10.10.22.173	UDP
01/25 5:02:46 PM	10.10.22.173	UDP
01/25 5:02:46 PM	10.10.22.173	UDP
01/25 5:02:46 PM	10.9.0.76	UDP
01/25 5:02:45 PM	10.10.22.44	UDP
01/25 5:02:45 PM	10.10.25.202	UDP
01/25 5:02:45 PM	10.10.22.44	UDP
01/25 5:02:45 PM	10.10.25.202	UDP
01/25 5:02:45 PM	10.10.25.202	UDP
01/25 5:02:45 PM	10.10.22.100	UDP

Top Query Types

Query Type	# Logs	% of Logs
A	171628	62.82%
AAAA	92582	33.89%
SOA	4001	1.46%
MX	3057	1.12%
OTHER	1862	0.68%
SRV	54	0.02%
TXT	22	0.01%
NS	9	0%
CNAME	2	0%

Summaries

Log Analytics

FQDN/Domain Name

Protocol

Client IP Address

Server IP Address

Location

Query Type

Record Source

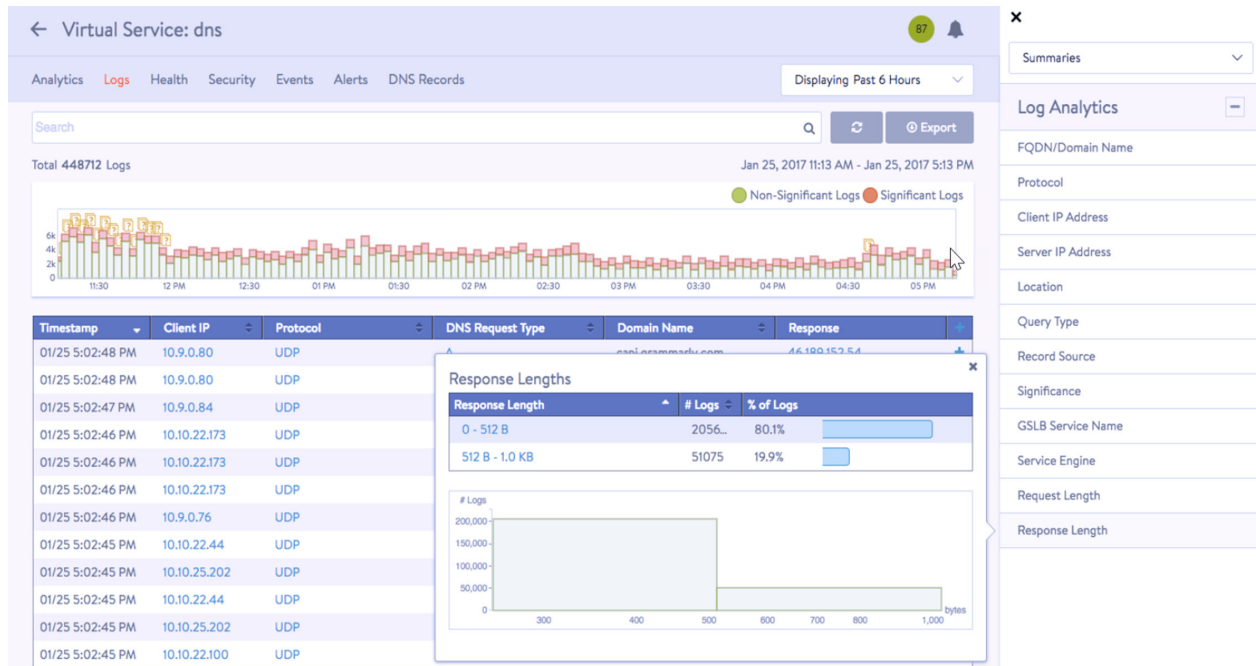
Significance

GSLB Service Name

Service Engine

Request Length

Response Length



## 注

- 可以使用子域名筛选 DNS 请求。
- 在选择衡量指标磁贴时，有时可能会显示“无数据”。这通常意味着“不适用”。例如，GSLB 服务名称可能不适用于 DNS 代理或静态条目。

DNS 记录选项卡是这种虚拟服务特有的。

## 附加信息

- 将通过域筛选来删除在 DNS 服务上未明确配置的任何域（默认设置为允许所有域）。
- 可以自定义生存期 (Time-To-Live, TTL)（默认值为 30 秒）。
- 网络安全策略可以基于客户端（源）IP 和端口。
- 通过使用完整 TCP 代理，可以防止客户端 TCP DNS 查询中的欺骗。SYN 泛洪攻击将得到缓解。
- 您可以返回 DNS 错误代码或丢弃数据包以响应失败的 DNS 请求。

## 将 GSLB 服务选择性分配给 DNS 虚拟服务

NSX Advanced Load Balancer 支持需要将每个子域的 DNS 请求处理选择性分配给特定 NSX Advanced Load Balancer DNS 虚拟服务的 GSLB 配置。

## 用例

请考虑以下场景：

- 将 DNS 职能推送到 GSLB 设置中的所有 DNS 虚拟服务
- 在多个子域中具有全局服务

- 应用程序 VIP 位于单独的路由域中

通过使用 NSX Advanced Load Balancer，您可以配置多个 GSLB DNS 虚拟服务（可能每个路由域一个虚拟服务），并将每个子域的 DNS 请求处理选择性分配给不同的 NSX Advanced Load Balancer DNS 虚拟服务，以使提供 VIP 的 SE 可以位于与提供其虚拟 IP 的 DNS 虚拟服务相同的路由域中。

## GSLB 的高可用性建议

为了获得高可用性，建议在可扩展到两个或更多服务引擎 (SE) 的 SE 组上为 GSLB 配置 DNS。还建议在多个位置中为 GSLB 实施 DNS。

可以通过以下方法进行实施：

- 1 至少具有两个地理位置分散的主动 GSLB 站点。对于每个站点，在可扩展的 SE 组上配置 DNS。
- 2 如果仅定义一个主动站点，请确保至少有一个地理位置偏远的云。在该远程云上，在可扩展 SE 组上为 GSLB 配置 DNS。还要定义所有虚拟服务以支持在原始位置中运行的任务关键型应用程序。

## GSLB 服务

GSLB 服务是全局应用程序的表示形式。它作为多个站点中部署的应用程序实例的前端。

以下是全局服务的关键元素：

- 全局应用程序服务的名称；管理员通过该名称引用 GSLB 配置。
- 应用程序的 FQDN；最终用户客户端通过该 FQDN 引用应用程序。您可以为别名提供域名列表（例如，www.foo.com 和 foo.com）。
- 在各种 GSLB 站点中运行的支持服务；划分到一个或多个 GSLB 池中。支持服务通常是 NSX Advanced Load Balancer 虚拟服务。不过，它可能是第三方 ADC 的虚拟服务，甚至是某个孤立服务器上的 IP:端口。

---

**注** GSLB 池不同于服务器池。前者汇聚支持服务，后者汇聚服务器。

---

- 运行状况监控方法；可以通过这种监控确定未正常运行的组件，以便选择替代的组件。
- 生存期 (TTL)；范围是 1-86400 秒，它决定客户端需要为客户端请求获取全新转向信息的频率。如果没有为特定的 GSLB 服务指定任何值，则 TTL 值默认为 DNS 应用程序配置文件中指定的值（默认值为 30 秒）。

---

**注** 建议在使用非常低的 TTL 值时要特别小心，因为某些 DNS 或操作系统丢弃非常低的 TTL。

---

## 与 GSLB DNS 的交互

在确定 GSLB 服务池成员（即，某些参与的虚拟服务）关闭时，GSLB DNS 将返回 4 个标准响应之一。在 GslbService 对象中，设置 GslbService.down\_response 参数以选择以下 4 个选项之一：

GSLB\_SERVICE\_DOWN\_RESPONSE\_NONE - 默认选项，直接丢弃请求。

GSLB\_SERVICE\_DOWN\_RESPONSE\_FALLBACK\_IP - 使用单个预设的回退 IP 地址进行响应，该地址通常指向一个错误页面。

GSLB\_SERVICE\_DOWN\_RESPONSE\_ALL\_RECORDS - 返回所有池的所有成员的所有 IP 地址。

GSLB\_SERVICE\_DOWN\_RESPONSE\_EMPTY - 返回空 DNS 响应；可用于在某些情况下使客户端进行重试。

## GSLB 服务运行状况监控的选项和组合

- 仅控制平面运行状况检查 - 没有为该模式配置主动数据平面运行状况监控器。所有主动控制器配置为将本地收集的运行状况与从远程控制器收集的统计信息合并在一起。

然后，将合并的统计信息从每个主动控制器（集群）传送到其本地 DNS。该方法仅适用于作为 NSX Advanced Load Balancer 虚拟服务实施的成员。

- 仅数据平面运行状况检查 - 将 `GslbService.controller_health_status_enabled` 设置为 **False**。每个 GSLB DNS 在所有 GSLB 成员虚拟服务（包括外部站点上托管的服务）上执行运行状况检查。
- 控制平面和数据平面运行状况检查 - 对于要标记为启动的成员虚拟服务，控制和数据运行状况都应报告“启动”。如果由于远程控制器关闭或无法访问而导致控制平面运行状况检查失败，但仍然可以执行数据平面运行状况检查，则该检查单独确定成员虚拟服务的状态。

## GSLB 的负载均衡算法

在选择了特定池后，GSLB 算法（如 `GslbPool.algorithm` 参数中所示）在池的成员服务之间进行负载均衡。

### 循环

在所有成员之间平均分配流量，并且可以选择按权重增加或减少流量。这些是由成员的 `GslbPoolMember.ratio` 参数值确定的，该参数默认为 1，范围是从 1 到 20。例如，如果虚拟服务 A、B 和 C 的比率分别为 1、2 和 3，虚拟服务 A 将收到六分之一的负载，B 收到三分之一的负载，C 收到二分之一的负载。

### 一致哈希

根据客户端的源 IP 地址（可能是 DNS 解析器地址）分配负载。如果启用了 DNS 的扩展机制 (Extension Mechanisms for DNS, EDNS) 处理，将会在 [插入 DNS 的扩展机制 \(EDNS\) 客户端子网选项](#) 中找到源 IP 地址。如果在某个站点上的给定网络中具有多个本地 DNS，则可以将范围从 1 到 31 的整数掩码应用于客户端 IP 地址。该算法可以提供持久性。另一种算法是 [GSLB 站点 Cookie 持久性](#)。

### 基于地理位置

根据客户端相对于 GSLB 成员的经纬度，将客户端请求传送到最佳站点。有关详细信息，请参阅 [GSLB 成员的基于地理位置的负载均衡算法](#)。

如果启用了 DNS 的扩展机制 (EDNS) 处理，将使用在 ECS 选项中找到的源 IP 地址。

### 基于拓扑的算法

有关更多信息，请参阅[基于拓扑的 GSLB 算法](#)。

NSX Advanced Load Balancer 支持从  $m$  个 GSLB 池中选择  $n$  个记录。有关更多详细信息，请参阅[从  \$m\$  个池中选择  \$n\$  个池成员](#)。

有关更多详细信息，请参阅[负载均衡算法](#)。

## 使用地理位置算法时的 GSLB 回退算法

GSLB 服务池具有一个配置选项，用于更改地理位置算法失败时的回退行为。

如果未配置回退算法，则将循环方法作为默认回退算法。

除了默认循环算法以外，还可以选择一致哈希方法以作为 GSLB 池选择的回退算法。

---

### 注

- 它仅适用于具有以下配置的 GSLB 服务池：

- 将 [GSLB 成员的基于地理位置的负载均衡算法](#)配置为主要 GSLB 算法。

在基于地理位置的负载均衡方法中，GSLB 池是根据其地理位置选择的。

- [一致哈希](#)配置为 GSLB 方法的回退算法。如果未选择回退算法，则继续使用循环回退算法。

在一致哈希负载均衡方法中，流量是根据客户端的源 IP 地址（DNS 解析器地址）分配的，除非启用了 EDNS 处理。如果启用了 EDNS 处理，则会在 ECS 选项中找到源 IP 地址。如果在某个站点上的给定网络中具有多个本地 DNS，则可以将范围从 1 到 31 的整数掩码应用于客户端 IP 地址。

---

有关 GSLB 算法的更多详细信息，请参阅 [第 2 章 NSX Advanced Load Balancer GSLB 架构和术语](#)。

## GSLB 成员的基于地理位置的负载均衡算法

GSLB 的 NSX Advanced Load Balancer DNS 地理位置算法根据客户端和 GSLB 站点的经纬度将客户端请求传送到最佳站点。NSX Advanced Load Balancer DNS 配置中的每个 SE 参考自己的本地地理位置数据库 (geo-DB) 副本以做出该决定。

### 运行

图 1 显示地理位置算法的运行方式。

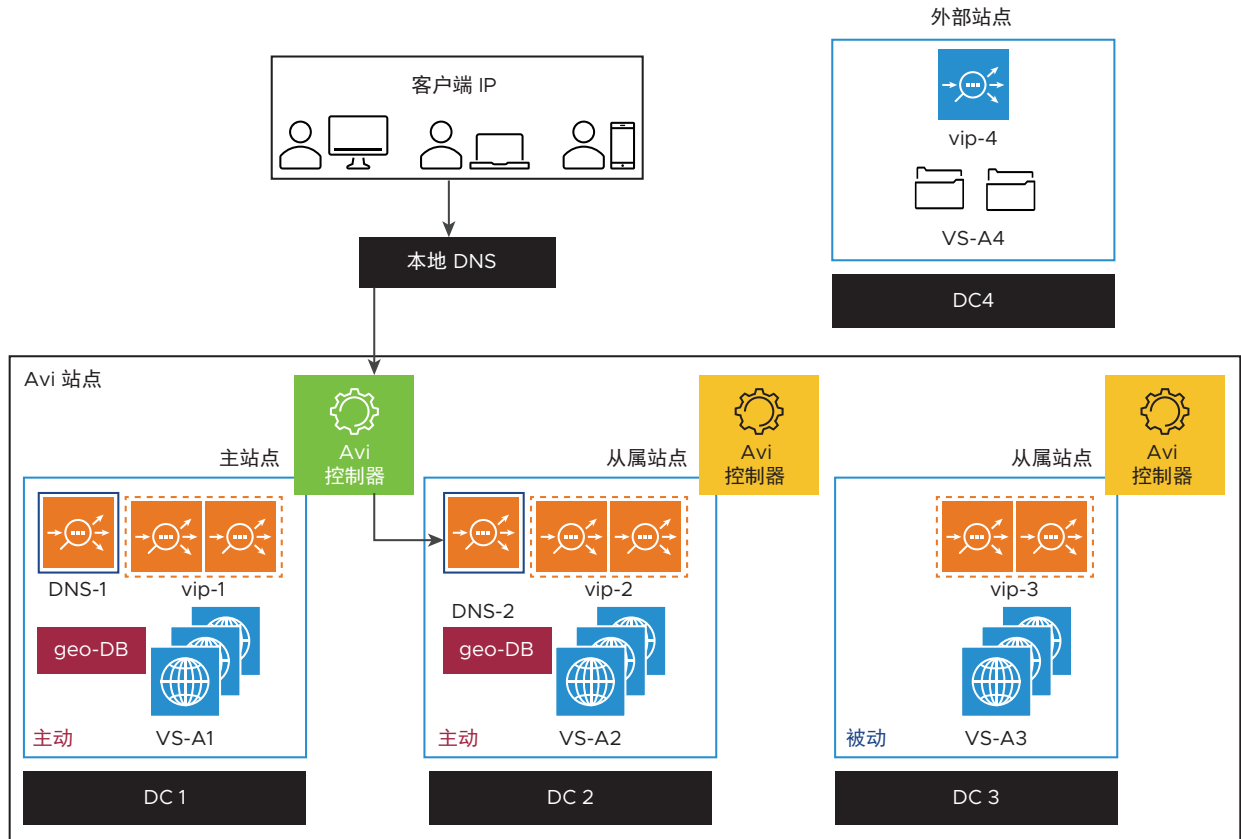
IP 地址为 client\_IP 的客户端从 4 个地理位置分散的数据中心 DC1-DC4 的 4 个虚拟服务（VS-A1 到 VS-A4）实施的多站点应用程序中请求服务，其中的一个数据中心是非 NSX Advanced Load Balancer 负载均衡站点（简称为外部站点）。客户端的本地 DNS 必须将应用程序的 FQDN 解析为 4 个潜在地址之一：vip-1、vip-2、vip-3 或 vip-4。第一步是找到能够进行该转换的 DNS。DNS-1 或 DNS-2 就足够了。每个 DNS 实例可以访问自己的相同 geo-DB。通过使用该数据库，DNS-1 或 DNS-2 可以将 5 个 IP 地址转换为基于经纬度的位置。

---

**注** 选择 DNS-2 不受 NSX Advanced Load Balancer 控制，因此，可能与地理位置无关。我们特意选择了一个更远的 DNS 以强调这一点。

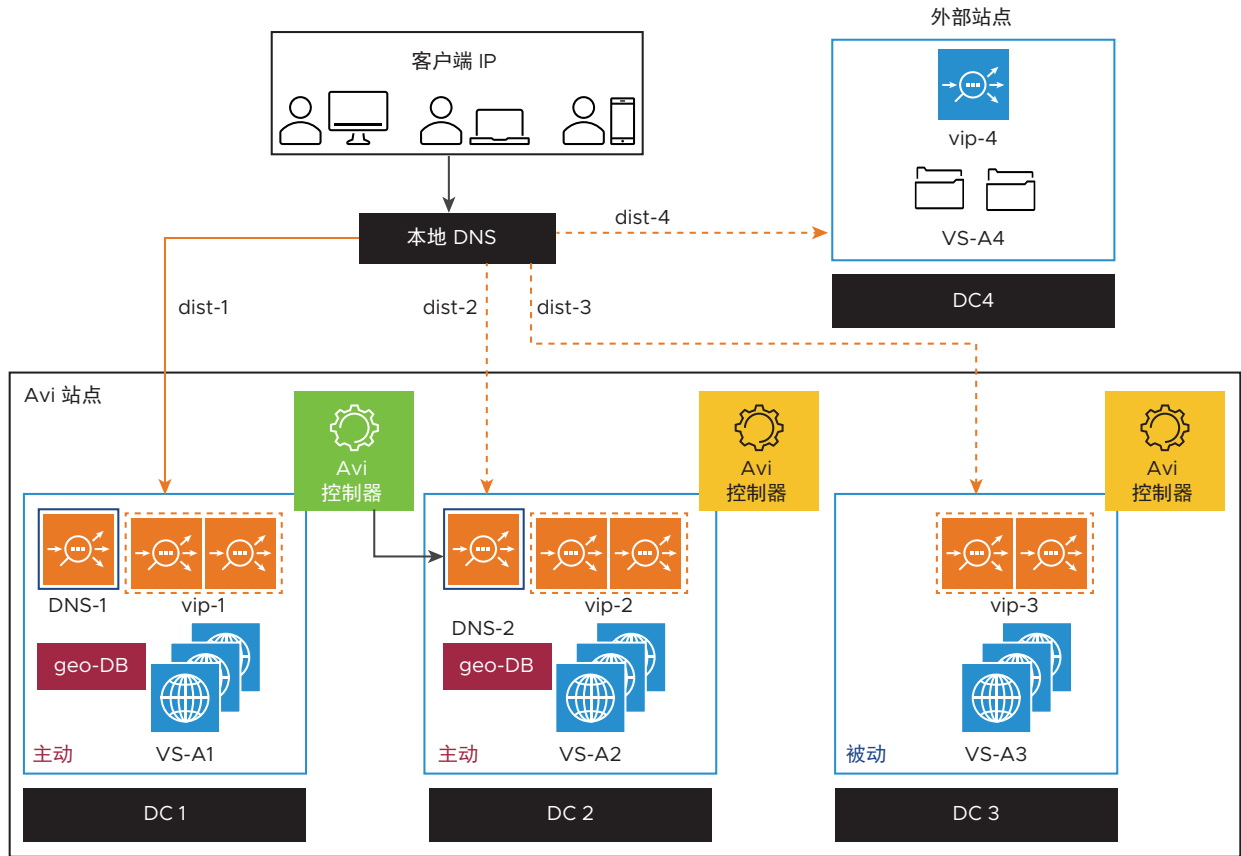
---

图 2-1.1. 找到 FQDN 的权威 DNS



DNS-2 中运行的算法计算 4 个距离，确定 dist-1 最短，因此，使用 vip-1 响应 DNS 请求。正如图 2 所示，客户端随后将其应用程序请求传送到 vip-1。

图 2-2. 2. 在 DNS-2 中运行的地理位置算法选择 vip-1



## 为 VIP 分配地理位置

每个 GSLB 服务池的算法是单独设置的。循环、一致哈希和地理位置算法是当前的选项。要实施地理位置算法，GSLB 的 NSX Advanced Load Balancer DNS 必须使用某种方法将位置分配给 GSLB 服务包含的 GSLB 站点。对于每个 GSLB 服务，这些选项如下所示：

### 从 geo-DB 中计算位置（默认）

这种方法需要在预先构建的数据库中执行查找。本指南的后面章节介绍了该数据库。

### 从站点中继承位置

在使用这种方法时，为每个参与的 GSLB 站点分配一个位置以作为 GSLB 配置对象的一部分。在站点中运行的 GSLB 服务成员虚拟服务静态继承与该站点关联的位置。如果未导入批量 geo-DB 信息，该方法可能是非常有用的。

### 明确配置

该手动过程为管理员提供最精细的完全控制，而不依靠预先填充的 geo-DB。

在为给定 GSLB 服务选择地理位置算法时，具有尚未确定位置的 VIP 的成员虚拟服务基本上是不透明的。DNS 响应从不包括其 VIP。相反，地理位置算法从一组虚拟服务中选择一个可以确定位置的 VIP。如果没有任何成员虚拟服务具有可以确定位置的 VIP，GSLB 的 NSX Advanced Load Balancer DNS 将改用（加权）循环算法。



## 其他详细信息

- 由于距离计算纯粹基于虚拟服务的 VIP，因此，NSX Advanced Load Balancer 和外部站点都是 VIP 选择的候选项。
- 根据运行状况监控状态，DNS-2 将按地理远近顺序返回 vip-2、vip-3 或 vip-4。
- 与循环算法一样，可以为 VIP 分配权重。到目前为止，我们假设每个 VIP 具有相同的权重，即比率为 1:1:1:1。如果权重更改为 1:2:1:1（按 VIP 顺序 1、2、3 和 4），则不难理解可以为该特定客户端提供 vip-1 以外的 DNS 响应。例如，假设 dist-1 = 500 英里，dist-2 = 600 英里。单看物理距离，vip-1 确实是正确的选择。但是，通过为 vip-2 分配权重 2，将导致算法将 500 英里与 600/2 英里进行比较。由于 300 英里小于 500 英里，因此，将改为选择 vip-2。这种加权的一个用例是，一个站点的服务器比其他站点的服务器快得多。在此类快速站点上，节省的服务器处理时间可以弥补通过 WAN 传输浪费的时间。即使客户端的地理位置较远而通过稍长的距离路由流量，快速站点也可以实现更短的总体往返时间。
- 有时，客户端的 IP 地址无法提供准确的客户端位置。为了解决该问题，管理员可以选择修改 DNS 应用程序配置文件以启用 EDNS。如果选择该选项，并且在 DNS 请求中具有 EDNS 子网扩展，将使用该扩展而不是客户端的 IP 地址。有关更多详细信息，请参阅[插入 DNS 的扩展机制 \(EDNS\) 客户端子网选项](#)。

## 地理位置 (Geo-DB) 数据库

本节介绍了有关地理位置算法中使用的地理位置 (Geo-DB) 数据库的信息。

数据设置为 NSX Advanced Load Balancer geo-DB 格式（在下面指定）以下载到 SE 组中的所有 NSX Advanced Load Balancer DNS SE。提醒一下，该组专用于 DNS；不允许在其中使用应用程序虚拟服务。随后，将 NSX Advanced Load Balancer geo-DB 复制到所有从属 NSX Advanced Load Balancer DNS 实例，以便其中的任一实例（上面示例中的 DNS-1 和 DNS-2）可以使用相同的最佳位置 VIP 回复客户端本地 DNS。

NSX Advanced Load Balancer 包括一个地理位置数据库以确定客户端的来源。这是一个基于 MaxMind IP-Country 和 IP-ASN 数据的固定数据库。该数据库是在控制器上维护的，并在升级控制器时合并数据库更新。

### 记录格式

NSX Advanced Load Balancer geo-DB 记录中的字段足以容纳常见的第三方地理位置数据库中定义的信息。单个记录包含 6 个以逗号分隔的字段。前 4 个字段是必填字段。第 5 个或第 6 个位置中的连字符表示未指定该字段。这些字段如下所示：

- IP 地址范围起始值
- IP 地址范围结束值
- 纬度
- 经度
- 城市的全名，例如 USA/California/San Francisco
- 标记保留用于特殊用途，例如，为区域（如“West”）存储客户定义的值



‘名称’和‘标记’字段用于两个用途：

- 它们出现在日志中
- 它们可用于合并位置条目，从而减少内存使用量，并使查找更粗略以加快查找速度

## 文件格式和语法规则

任何以“#”开头的行将作为注释而忽略。位置记录行不能包含前导或嵌入空格。第一行必须包含 V.XX，其中 XX 是 NSX Advanced Load Balancer 数据库的版本。在本文截稿时，唯一支持的值是 V.01。可选的名称字段由三部分组成，这些部分由两个斜杠分隔。将删除任何具有分析错误的行。如果错误超过 95%，geo-DB 加载操作将失败。如果一些行具有重复或重叠的地址，则以文件中最后指定的一行为准并覆盖其他条目。以下示例说明了 IPv4 格式的正确语法。

```
v.01
# start_ip,end_ip,latitude,longitude,country/region/city,tag
# Hyphens denote an unspecified region and city within Australia
1.0.0.0,1.0.0.255,-33.4940,143.2104,Australia/-/-,-
1.0.1.0,1.0.1.255,26.0614,119.3061,China/Fujian/Fuzhou,-
1.0.2.0,1.0.3.255,26.0614,119.3061,China/Fujian/Fuzhou,-
# Neither the name nor the tag fields are specified for the IP range 2.0.2.0 to 2.0.3.255
2.0.2.0,2.0.3.255,26.0614,119.3061,-,-
```

可以将多个文件指定为源 IP 地址到位置映射的输入。正如本指南后面所述，如果多个来源指定了给定 IP 地址的距离，则优先级机制确定应以哪个数据为准。

可以从其他格式转换为 NSX Advanced Load Balancer 格式。此类数据合并为一个采用 NSX Advanced Load Balancer 格式的静态复合 geo-DB 文件。在第一个版本中，可以导入 MaxMind 格式。随着时间的推移，设计可能支持从其他来源导入数据。

假设多站点应用程序的客户端具有公用或专用地址。从 NSX Advanced Load Balancer GSLB 的角度看，它们可以直接通过网络访问公用或专用 VIP，但不能同时访问两者。在公用网络中，网络地址转换可能涉及专用站点，但此类专用 IP 对控制公用客户端访问的地理位置算法是透明的。因此，geo-DB 负责包含一种或另一种地址，但不能同时包含两者。

## IPv6 支持

以下字段适用于 NSX Advanced Load Balancer geo-DB v6 记录。

- IPv6 地址
- 前缀长度
- 纬度
- 经度
- 城市的全名，例如 USA/California/San Francisco
- 标记 - 保留用于特殊用途，例如，为区域（如“West”）存储客户定义的值

前 4 个字段是必填字段。第 5 个或第 6 个位置中的连字符表示未指定该字段。

## IPv6 文件格式

以下示例说明了 IPv6 数据库格式的正确语法。

```
V.01
# IPv6 address, prefix length,latitude,longitude,country/region/city,tag
# Hyphens denote an unspecified region and city within United States
1::3,128,1,1,United States/-/-,testing
2::2,128,5,5,United States/-/-,testing
1::1,128,3,3,United States/-/-,testing

3::3,128,8,7,United States/-/-,testing
4::4,128,9,9,United States/-/-,testing
```

## 对 NSX Advanced Load Balancer 控制器和 NSX Advanced Load Balancer SE 配置的影响

为了支持地理位置算法，在配置控制器和 SE 以便为 GSLB 实施 NSX Advanced Load Balancer DNS 时，必须考虑一些特殊事项。

- 内存分配 - NSX Advanced Load Balancer geo-DB 可能非常大（例如，可以轻松包含 300 万个条目）。因此，NSX Advanced Load Balancer DNS SE 的最低建议是 8 GB。额外的控制项“主机地理配置文件”指定，其中的一些内存（建议为 2GB）专用于 geo-DB。地理配置文件允许为 geo-DB 保留一部分 SE 内存。
- 磁盘分配 - NSX Advanced Load Balancer geo-DB 可能非常大（例如，可以轻松包含 300 万个条目）。因此，建议额外增加 2 GB 以作为磁盘大小。同样需要在正常范围以外增加控制器磁盘大小，因为这是组装数据的第一个位置。
- 在 NSX Advanced Load Balancer geo-DB 很大时，DNS SE 需要一些时间以将条目加载到内存中。
- 在 CLI 一节中介绍了适用于它们的 CLI 命令。

## 覆盖数据库

可以创建自定义 IP 组以覆盖或扩充地理位置数据。

例如，创建一个名为“Internal”的新 IP 组，并添加 10.0.0.0/8 和 192.168.0.0/16。或者，使用“按国家/地区代码选择”创建新的 IP 组。在该示例中，组命名为 North America，并包括 US、MX 和 CA。

**注** 自定义 IP 组仅覆盖创建了 IP 组的租户的地理位置数据库。

## 基于拓扑的 GSLB 算法

除了下面提到的其他算法以外，GSLB 还支持基于拓扑的算法：

- 循环
- 一致哈希
- 地理

基于拓扑的负载均衡使用在 DNS 虚拟服务级别配置的拓扑策略分配 DNS 名称解析请求。这是地理负载均衡算法的扩展，并具有类似的工作方式。通过使用基于拓扑的算法，可以将 GSLB 服务从定期的 DNS 策略执行中排除。

DNS 虚拟服务现在可以选择配置拓扑策略（类似于 DNS 策略）。这些策略是为配置了基于拓扑的 GSLB 算法的服务触发的。对于其他算法，不会查询拓扑策略。

## 用例

基于拓扑的算法用于在不同租户中部署数百个 GSLB 服务的部署。要求是将循环算法用于一些 GSLB 服务；对于其他服务，您需要根据客户端 IP 地址、地理位置等定义首选的站点。

以前，上述要求是使用字符串组实现的。字符串组是 DNS 策略的一部分，用于指定 GSLB 服务 FQDN 名称。通过使用字符串组，可以触发 DNS 策略以调用首选的站点。这种方法适用于较小的环境，而不适用于大型部署。

对于多个 GSLB 服务，如果您具有基于租户的访问限制，其中租户用户无法修改 DNS 策略，则使用字符串组是不可行的。要在字符串组中添加 GSLB 服务的 FQDN，需要具有这种修改 DNS 策略的特权。

可以使用基于拓扑的 GSLB 算法以解决上述限制。

对于该用例，一些 GSLB 服务配置了循环方法，其余服务配置了基于拓扑的算法。仅为将基于拓扑的算法作为 GSLB 方法的 GSLB 服务触发拓扑策略。通过使用该方法，每次在任何租户中添加新的 GSLB 服务时，不会产生配置字符串组或更改 DNS 虚拟服务的开销。

## 注

- 拓扑策略包含与 DNS 策略相同的匹配目标和操作。对于基于拓扑的策略，建议使用首选站点或回退站点操作。
- 对于不基于拓扑的算法，不考虑使用拓扑策略。
- 拓扑策略适用于所有使用基于拓扑的 GSLB 算法的 GSLB 服务。如果要求将不同的拓扑策略用于不同的 GSLB 服务，则使用 FQDN 的字符串组。
- 如果为拓扑策略配置的操作失败，例如，如果配置的首选站点不再存在，NSX Advanced Load Balancer GSLB 将改用地理位置算法。如果地理位置算法失败，NSX Advanced Load Balancer GSLB 将改用循环算法。
- 如果 DNS 虚拟服务与两个策略（DNS 和拓扑策略）相关联，则会触发这两个策略。根据策略中配置的操作，策略是按以下顺序触发的：
  - 如果 DNS 策略配置为丢弃请求或发送错误响应，则该策略优先于拓扑策略。
  - 如果 DNS 策略将操作配置为选择站点，则拓扑策略决定覆盖 DNS 策略。

建议在 DNS 策略中配置丢弃或响应策略，并在拓扑策略中配置首选或回退站点选择策略。

## GSLB 池

可以在多个 GSLB 池中包含某个 GSLB 服务。GSLB 服务可以根据池优先级（如以下示例中所述）或地理位置在多个 GSLB 池之间切换负载。

### 优先级

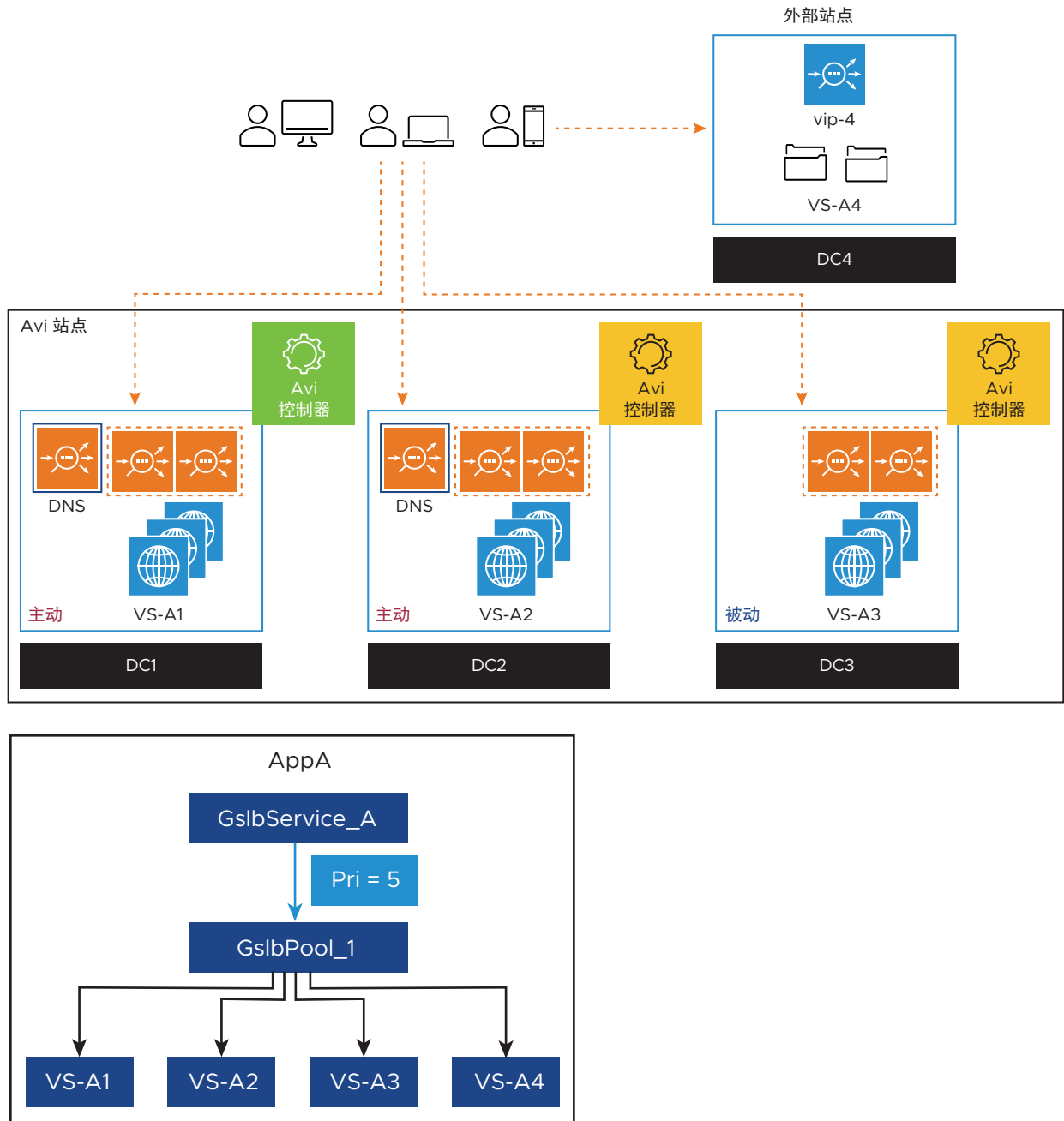
GSLB 池是根据其池优先级选择的。该算法通常用于灾难恢复 (Disaster Recovery, DR) 场景。请求将由具有最高优先级的 GSLB 池成员进行处理。如果该成员关闭/未正常运行，请求将传送到具有第二高优先级的 GSLB 池。

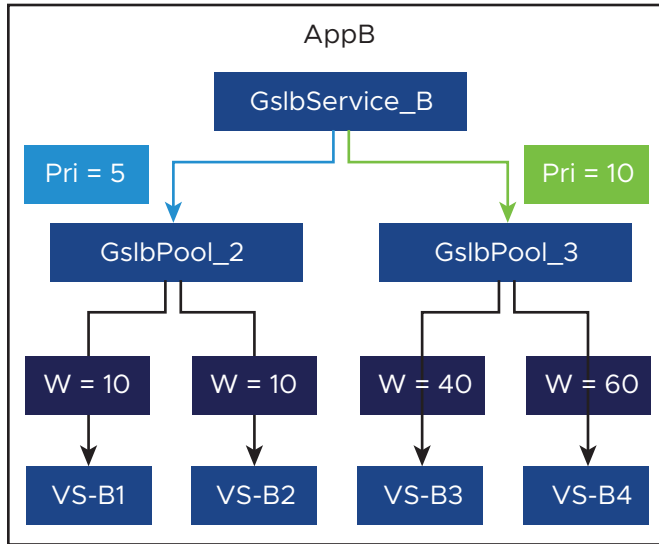
请参阅下面所示的图表。

- 对于 AppB，它对应于 GslbService\_B，该服务包含在两个池中，优先级分别为 5 和 10。
- 只要具有最高优先级的池 (GslbPool\_3) 已启动并且未达到其连接限制，就会将所有流量传送到该池。

- GslbPool\_2 将保持空闲状态。不过，如果一个池无法进行访问、关闭或达到最大容量，则会选择具有较低优先级的池。

下面显示全局应用程序 AppA，它跨 4 个站点（DC1 到 DC4）。GSLB 池对象 GslbPool\_1 汇聚服务 VS-A1 到 VS-A4，将在这些服务之间进行负载均衡。





有关更多详细信息，请参阅 [GSLB 的负载均衡算法](#)。

## GSLB 池成员

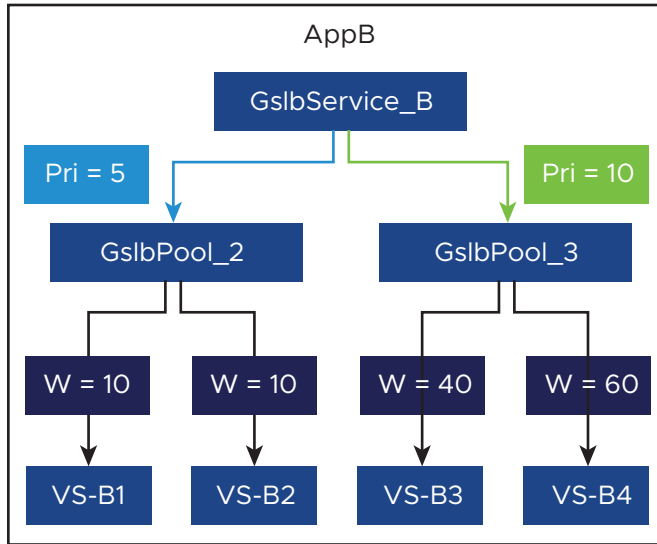
组成 GSLB 池的服务（例如，下图中所示的 VS-B3 和 VS-B4）称为 GSLB 池成员。

可以使用以下参数以指定成员：

- 虚拟服务名称
- IP 地址：用于指定由第三方负载均衡器定义的单独服务器或 VIP 以及/或者
- DNS 名称：例如，用于指定基于 DNS 的负载均衡器（例如 AWS ELB）。

## GSLB 池成员权重

GSLB 池的所有成员采用相同的优先级，但池中的每个成员可能具有不同的权重。在选择一个池并通过循环算法在成员之间分配其负载时，这些权重决定了传送到每个成员的负载比例。在下面所述的示例中，由于 GslbPool\_3 具有较高的优先级，只要 VS-B3 和 VS-B4 正常运行并且能够接受负载，所有负载就会传送到该池，但权重导致 NSX Advanced Load Balancer 将 40% 的负载传送到 VS-B3，并将 60% 的负载传送到 VS-B4。



## GSLB 运行状况监控器

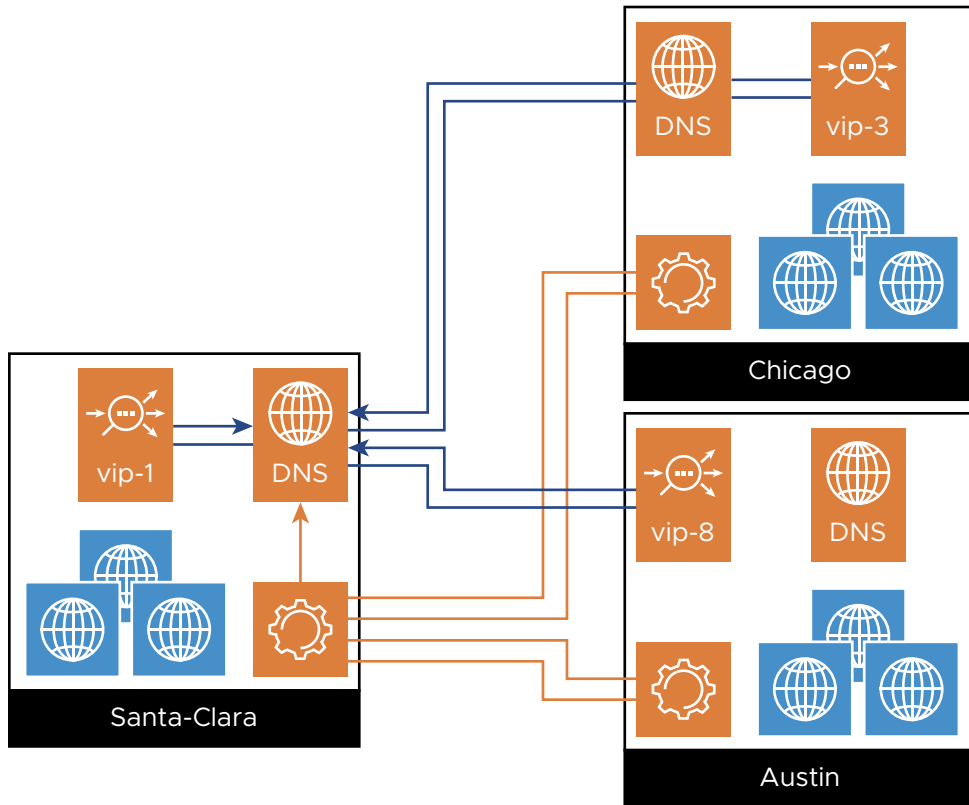
GSLB 服务是在多个站点中部署的全局应用程序的表示形式。GSLB 服务配置定义应用程序的 FQDN、不同站点中的虚拟服务支持情况以及控制在任何给定时间选择特定虚拟服务的优先级或比率。该配置还定义运行状况监控方法，可以通过这些方法确定未正常运行的组件，以便选择最佳的替代组件。

## GSLB 服务运行状况监控

GSLB 服务运行状况监控分为以下两类：

- 控制平面
- 数据平面
  - 默认行为
  - HM 代理
  - HM 分片

可以为每个应用程序应用一个或两个类别。



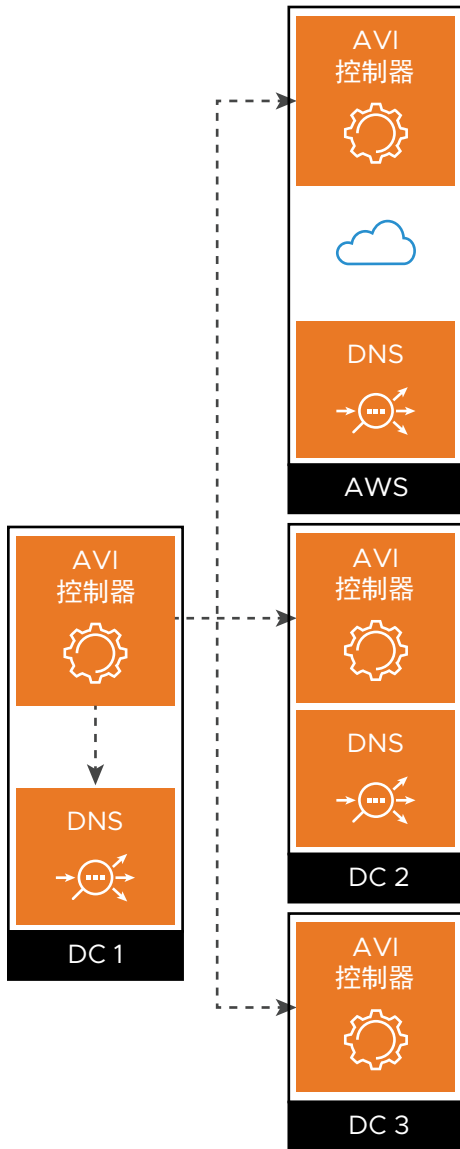
### 基于控制平面的全局应用程序运行状况监控

独立于 NSX Advanced Load Balancer GSLB，每个 NSX Advanced Load Balancer 控制器集群定期执行本地运行状况检查，以收集它直接控制的虚拟服务的运行状况分数和性能衡量指标。此外，如果 `GslbService.controller_health_status_enabled` 为 `True`，主动 GSLB 站点还会定期查询 GSLB 站点配置中指定的所有其他站点（主动和被动站点）中的 NSX Advanced Load Balancer 控制器。

**注** 控制平面运行状况监控不适用于在第三方负载均衡器 VIP 或单独服务器上配置的虚拟服务。

下图显示仅 DC1 中的主动控制器从 3 个其他控制器收集运行状况信息。DC1 的控制器将合并的运行状况信息传送到其本地 DNS（实线箭头）。实际上，DC2 和 AWS 中的主动控制器使用基于控制平面的运行状况信息更新相应的本地 DNS 虚拟服务。





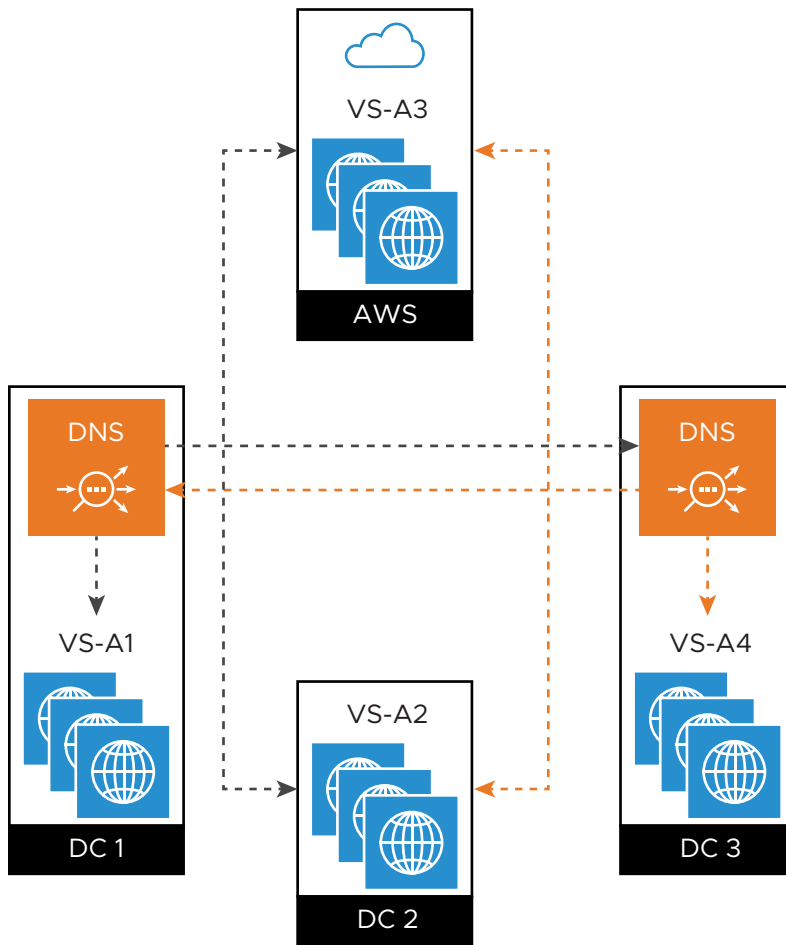
### 基于数据平面的全局应用程序运行状况监控

这是基于数据平面的运行状况监控的默认行为。与基于控制平面的运行状况监控相比，该监控不会查询站点的控制器集群。相反，运行状况检查直接查询参与服务，即数据平面。在主动站点上，托管 GSLB DNS 虚拟服务的 SE 对所有 GSLB 池成员（包括它本地的虚拟服务）执行定期运行状况检查。应配置一个专用的 SE 以执行这些运行状况检查。主动监控器从 DNS SE 中生成综合流量，以根据 GSLB 池成员响应将其标记为启动或关闭。下图显示 DC1（唯一主动站点）中的 DNS 对其本地虚拟服务 (VS-A1) 以及 VS-A2、VS-A3 和 VS-A4 执行该功能。同样，如果 NSX Advanced Load Balancer DNS 虚拟服务在其他站点上运行，这些 DNS SE 将以相同方式执行数据平面运行状况监控。

正如“配置运行状况监控”一节中所述，支持 Ping、TCP、UDP、DNS 和 HTTP(S) 运行状况监控器。此外，还可以根据要求配置自定义监控器。

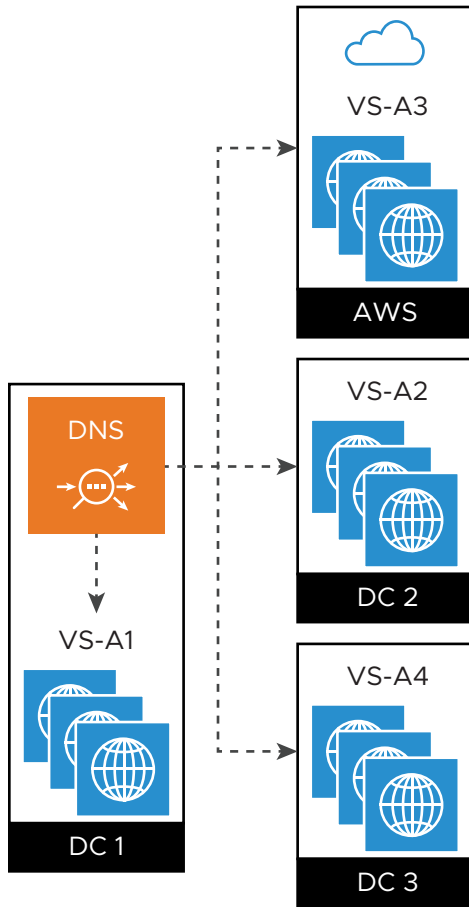
**注** 建议为 GSLB DNS 和负载均衡虚拟服务配置不同的 SE 组。

有关运行状况监控器的更多信息，请参阅 [NSX Advanced Load Balancer 上的运行状况监控器](#)。



## 基于数据平面的本地全局应用程序运行状况监控

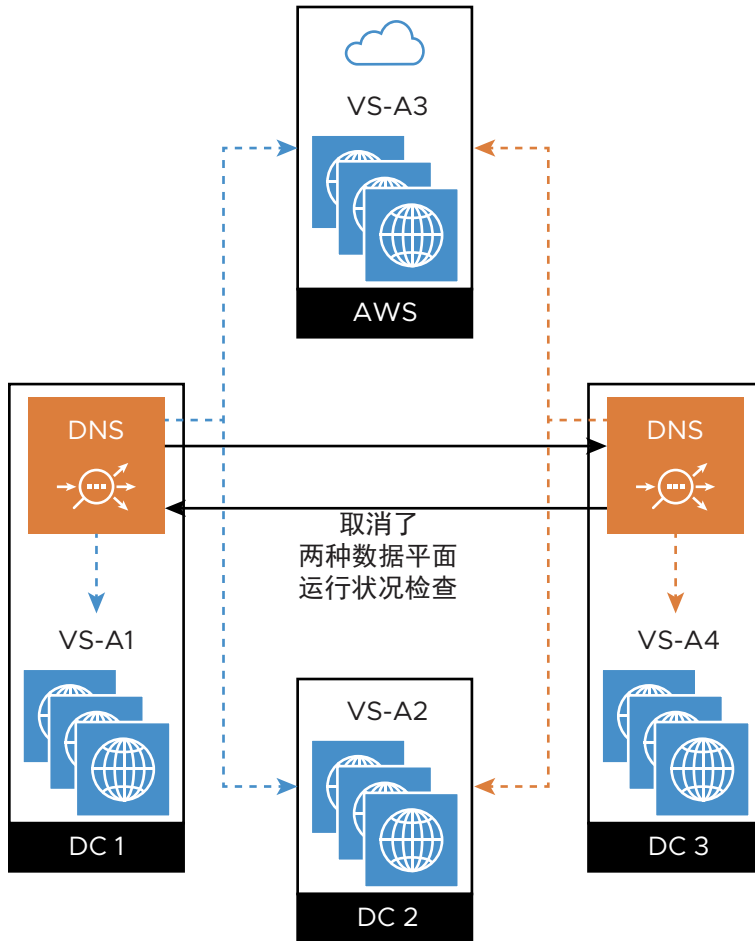
下图显示通过部署 NSX Advanced Load Balancer DNS SE 将 DC3 转换为主动站点。这名义上添加了 4 个额外的数据平面运行状况检查，从 DC3 的 NSX Advanced Load Balancer DNS SE 到 4 个成员虚拟服务。



请注意 VS-A4 的 DC1 DNS 检查以及 VS-A1 的 DC3 DNS 检查。由于下面的一个或两个原因，应避免执行这些检查：

- 保护 DC1 和 DC3 的防火墙已配置为允许 NSX Advanced Load Balancer 控制器进行通信，但它们阻止直接访问 VS-A4（从 DC1 中）和 VS-A1（从 DC3 中）。
- 我们希望最大限度减少每个 NSX Advanced Load Balancer DNS SE 必须执行的运行状况检查次数以提高每个 DNS SE 的性能。由于每个成员虚拟服务已由本地 DNS 执行数据平面检查，因此，远程 DNS 不必重复执行这些检查。

为了实现下图所示的优化，选择 VS-A1 和 VS-A4 进行本地数据平面运行状况检查。撤消了两个数据平面运行状况检查。每个 DNS SE 查询远程站点的 NSX Advanced Load Balancer 控制器以获取它所需的运行状况信息。



这种混合方法合并了控制平面和数据平面运行状况检查，将针对各个成员虚拟服务为全局服务启用该方法。唯一的限制是，成员虚拟服务在主动 NSX Advanced Load Balancer 站点上运行。

有关运行状况监控器分片的更多信息，请参阅[运行状况监控器分片](#)。

可以配置 DNS 运行状况监控器以监控配置为 DNS 服务池成员的 DNS 服务器的运行状况。

有关更多详细信息，请参阅[DNS 运行状况监控器](#)。

有关更多详细信息，请参阅[与 GSLB DNS 的交互](#)。

有关更多详细信息，请参阅[GSLB 服务运行状况监控的选项和组合](#)。

## 优化运行状况检查

可以使用以下方法优化 GSLB 站点或服务的运行状况检查：

- 正确设置数据平面运行状况监控器范围
- 限制主动站点数

### 正确设置数据平面运行状况监控器范围

**GslbService.health\_monitor\_scope**

该参数可用于根据要求配置数据运行状况监控器范围。默认情况下，它设置为 `GSLB_SERVICE_HEALTH_MONITOR_ALL_MEMBERS`，在这种情况下，DNS SE 主动探测 NSX Advanced Load Balancer 和外部站点中的池成员。不过，可以将该参数设置为 `GSLB_SERVICE_HEALTH_MONITOR_ONLY_NON_AVI_MEMBERS`，以便收集外部成员状态是唯一可行的方法，同时将运行状况检查负载从 DNS SE 分流到 GSLB 池成员的本地 NSX Advanced Load Balancer 控制器。

## 用例：优化运行状况监控

只能将数据路径运行状况监控应用于第三方成员。通过将 GSLB 池外部成员收集到第三方站点，可以轻松优化运行状况监控。首先，确定运行状况监控最高效的主动 NSX Advanced Load Balancer 站点（与第三方站点的远近程度和其他因素将影响选择的站点）。然后，使用 GSLB 第三方站点编辑器从“运行状况监控器代理”下拉菜单中选择所选的 NSX Advanced Load Balancer 站点。有关通过代理进行运行状况监控的更多详细信息，请参阅[基于数据平面的本地全局应用程序运行状况监控](#)。

## GSLB 站点持久性

本节介绍了检查站点持久性状态的方法。

### GSLB 站点 Cookie 持久性

GSLB 应用程序中来自客户端的长期事务可以配置为持久保存到启动其事务的站点。该功能是使用 NSX Advanced Load Balancer SE 创建的 HTTP 站点 Cookie 实施的。

#### 概览

一些应用程序需要在客户端和服务端之间具有粘性。换句话说，来自客户端的长期事务中的所有请求必须发送到同一服务器；否则，应用程序会话可能会中断，从而对客户端造成不利影响。这是通过启用 GSLB 站点 Cookie 持久性来实现的，站点持久性优先于配置的 GSLB 算法。

在活动-活动 GSLB 部署中，站点持久性是极其重要的。通常，站点持久性在活动-备用部署中不会出现问题。

#### 限制

NSX Advanced Load Balancer 检查下面列出的条件；如果尝试违反这些条件，将发出相应的错误消息。在阅读本节的全部内容后，您将更好地了解这些限制的必要性。

- 站点持久性仅适用于 NSX Advanced Load Balancer VIP；非 NSX Advanced Load Balancer（也称为第三方）VIP 不能参与。
- 不支持跨同一控制器集群中的多个虚拟服务的站点持久性。
- 要为全局应用程序启用站点持久性，它的所有成员必须在主动站点上运行。相反，如果参与站点持久性 GSLB 服务的 NSX Advanced Load Balancer 全局服务 (Global Service, GS) 成员在站点上运行，则站点无法从主动转换为被动。
- 要使站点持久性正常工作，NSX Advanced Load Balancer GS 成员在所有 GSLB 服务中必须是唯一的。换句话说，它不能是多个 GSLB 服务中的 GSLB 池成员。

- 站点持久性池是由控制器创建的内部池结构，并在启用了站点持久性时与 GSLB 虚拟服务成员相关联。用户不能执行或更改此关联。不能为站点持久性池配置 NSX Advanced Load Balancer 池组功能。
- `is_federated` 选项添加到所需的 PKI 配置文件中，以确保它可以在所有 GSLB 成员之间进行复制。只能定义一个 `is_federated` PKI 配置文件。由于只有一个配置文件，因此，不需要明确将联合的 PKI 配置文件与任何 GSLB 服务相关联。
- 联合的 PKI 和应用程序持久性配置文件
  - 不能与未联合的配置文件相关联。
  - 如果未启用 GSLB，则不能创建该配置文件。

## 基于 Cookie 的站点持久性的工作方式

图 1 显示长期事务生命周期中的阶段 1。

- 1 客户端要求其 DNS 解析器解析 `x.foo.com`。
- 2 企业 DNS 确定两个权威 DNS（在 Site1 和 Site2 中），并建议 DNS 解析器尝试使用 Site1 DNS。
- 3 Site1 中的 DNS 收到 DNS 解析器的查询，并使用任何有效的全局负载均衡算法。此外，它还向 DNS 解析器建议 Site1 中的 VS1 并设置 TTL。
- 4 DNS 解析器又将建议和 TTL 传送到客户端。
- 5 实施 VS1 的组中的每个 SE 知道启用了站点持久性。客户端的第一个请求不包含站点 Cookie，因此，SE 创建一个 Cookie 并将其传回。该 Cookie 使用 AES-256 进行加密，并基于 `cluster_uuid` 和 `vs_uuid` 字符串。以下是此类 Cookie 的示例：

```
Set-Cookie: F00=1S509ceebd-0913-4aomuTiRccdU0ujbfY6eCVkL9muOBwIsnT5fhrMTMM4-fapeQ2SEGb3ny69-iJQYG6Xg6SmLq9x7crxFEZbZVsCNDYdqXSwx5GIiuEJqlXFbehC2obJUDbYBciac; path=/
```

只要组中的 SE 看到该 Cookie，双头蓝色箭头指示的双向对话就会继续进行。

图 2-3. 1. 基于 Cookie 的 GSLB 站点持久性的阶段 1

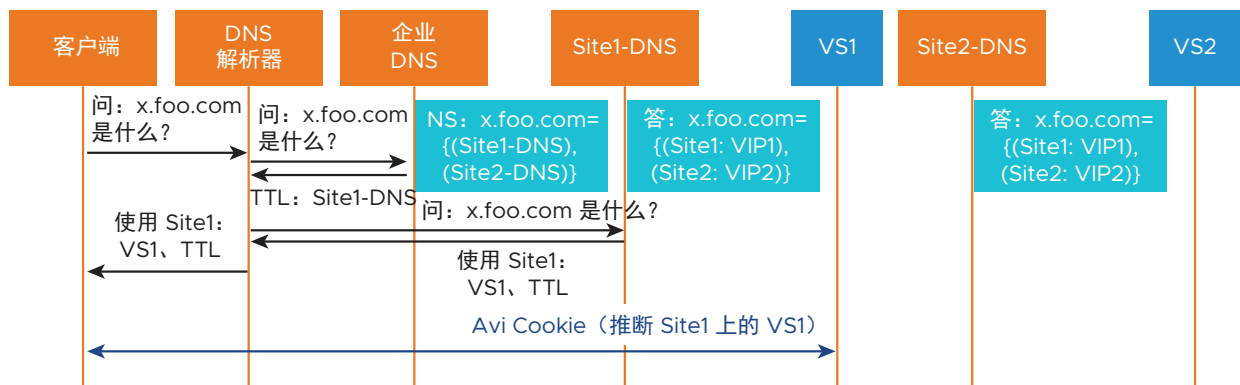


图 2 显示在 TTL 过期后的某个时间发生的情况。

- 1 这种过期迫使客户端再次请求 DNS 解析器提供 `x.foo.com` 的 IP 地址。

- 2 DNS 解析器再次请求企业 DNS 提供权威 DNS。从其缓存中，企业 DNS 建议 Site2 的 DNS。
- 3 客户端查询 Site2 DNS 并且它提供 VIP2，即 VS2 的本地 IP 地址。

图 2-4. 2. 基于 Cookie 的 GSLB 站点持久性的阶段 2

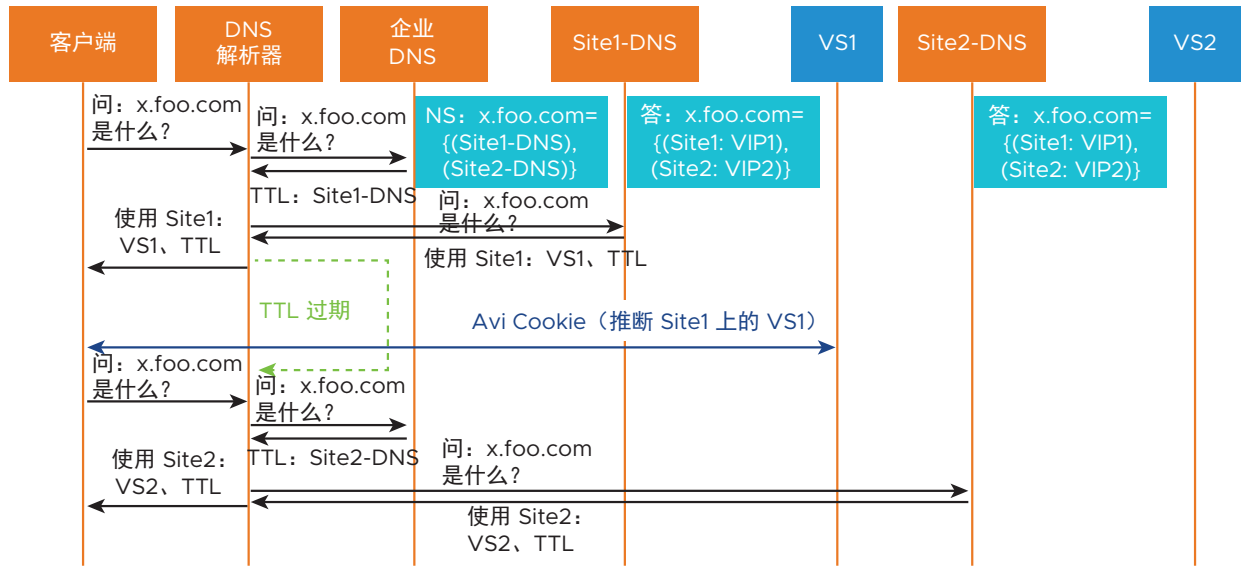
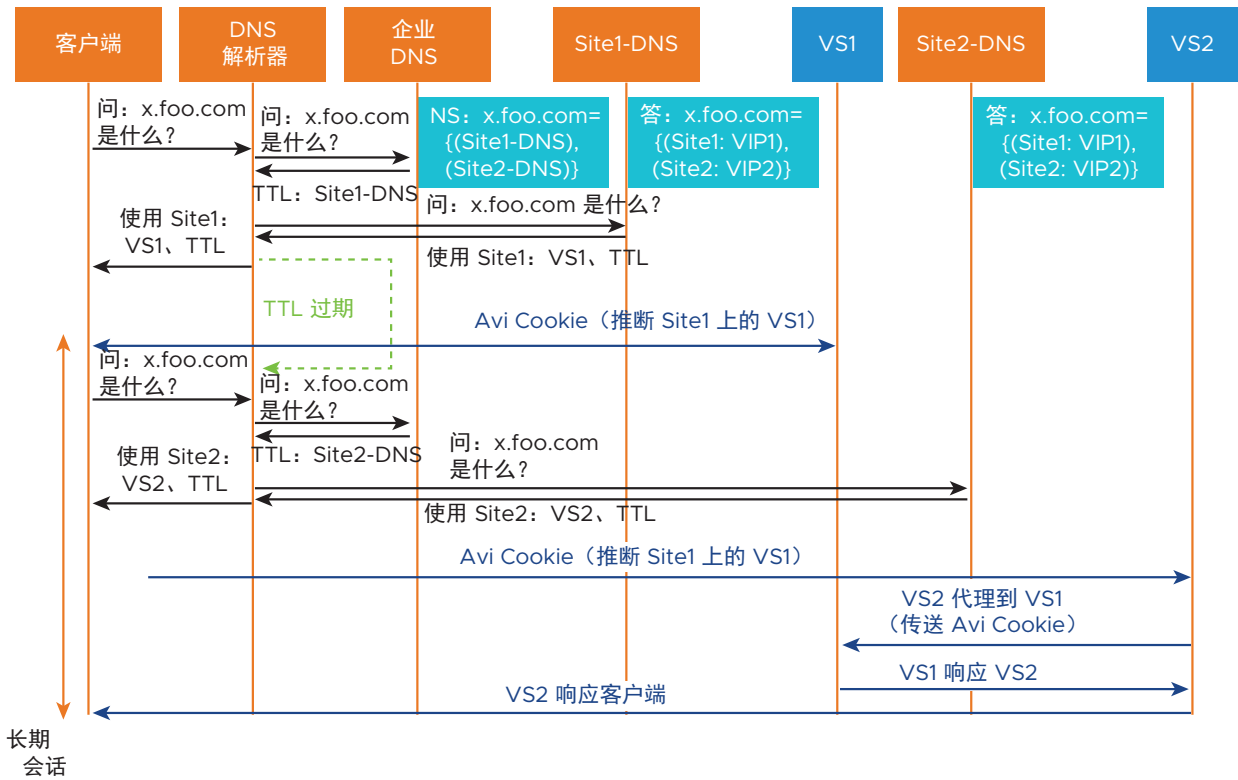


图 3 显示客户端启动与 Site2 中的 VS2 的对话。它不知道的是，随该请求提供了以前获取的 Cookie。

- 1 Site2 中的 SE 收到请求以及站点 Cookie。它解密该 Cookie，并立即发现该请求是未在其站点上启动的对话的延续。相反，需要将该对话代理到 Site1 中的 VS1。
- 2 在将请求代理到 VS1 时，VS2 将请求传送到 VS1，从而确保将返回地址设置为自身。
- 3 SE 使用 Site1 中的 VS1 提供的内容以响应客户端。

图 2-5. 3. 基于 Cookie 的 GSLB 站点持久性的阶段 3



## 同时定义 HTTP 和 HTTPS 端口的全局服务

在具有站点持久性 (SP=ON) 的全局服务同时定义 HTTP 和 HTTPS 端口时，需要注意一些特殊事项，而无论是默认端口（80 和 443）还是任何其他端口对。

### 案例 1: 同一全局应用程序在端口 80 上公开 HTTP, 并在端口 443 上公开 HTTPS

您需要在参与全局服务的每个虚拟服务的关联应用程序配置文件中将 `http_to_https` 设置为 `True`。在 NSX Advanced Load Balancer UI 中，使用应用程序配置文件，如下所示：



图 2-6. 只需单击一下鼠标按钮，即可启用 HTTP 到 HTTPS 重定向

Edit Application Profile: applicationprofile-securepay

General Security Compression Caching DDoS

• Security Information •

Secure HTTP

☐ SSL Ever Client requests received via HTTP will be redirected to HTTPS.

☒ HTTP-to-HTTPS Redirect ?

☐ Secure Cookies ?

☐ HTTP Strict Transport Security (HSTS) ?

☐ HTTP-only Cookies ?

☐ Rewrite Server Redirects to HTTPS ?

☐ X-Forwarded-Proto ?

• Client SSL Certificate Validation •

Validation Type ? **None** Request Required

Cancel Save

**案例 2：同一全局应用程序公开非默认 HTTP 和非默认 HTTPS 端口**

例如，假设为参与具有站点持久性 (SP=ON) 的全局服务的虚拟服务定义了用于 HTTP 的端口 91 和用于 HTTPS 的端口 9443。

除了选择 `http_to_https ON`（使用 UI、CLI 或 REST API）以外，还要为每个参与的虚拟服务定义 HTTP 规则，以便将 HTTP 端口 91 重定向到 HTTPS 端口 9443，如下所示。

图 2-7. 定义 HTTP 请求规则以定义端口

The screenshot shows the 'Edit Virtual Service: securepay@site\_A' interface. The 'HTTP Request' tab is selected. A new rule is being added, named 'Rule 3'. The 'Matching Rules' section shows 'Service Port' set to 'Is' with 'Ports' set to '91'. The 'Action' section shows 'Redirect' with 'Protocol' set to 'HTTPS', 'Port' set to '9443', 'Status Code' set to '302', 'Host' set to 'Keep Existing Host', 'Path' set to 'Keep Existing Path', and 'Keep query' checked. The 'Cancel' and 'Save Rule' buttons are at the bottom.

### 案例 3：没有实施 HTTP 到 HTTPS 重定向

无论端口设置是默认值（80 和 443）还是任何其他值，如果没有实施 HTTP 到 HTTPS 重定向，站点持久性流量将无法正常工作。

### GSLB 服务站点持久性状态

本节介绍了用于执行以下操作的 CLI 命令：

- 检查站点持久性 GSLB 服务的运行状态。
- 确定从其他虚拟服务代理回要持久保存客户端的虚拟服务的请求百分比。

在以下 CLI 序列中，我们具有：

- 1 一个名为 `gs-1` 的全局服务
- 2 该全局服务由两个名为 `pay@site_A` 和 `pay@site_B` 的虚拟服务组成
- 3 这些虚拟服务在相应命名的主动站点 `site_A` 和 `site_B` 上运行
- 4 两个站点中的站点持久性代理池相应地命名为 `SP-gs-1-pay@site_A` 和 `SP-gs-1-pay@site_B`。请注意，NSX Advanced Load Balancer 在以连字符连接的 GSLB 服务名称和虚拟服务名称前面添加 SP-以自动组成站点的代理池名称
- 5 有关站点持久性的运行状态为“启动”

下面的 `show` 命令输出反映了第 1 点到第 5 点。在命令输出的右侧，我们插入了注释以指导您查看哪一点。可以从任何主动站点中获取这些数据。

**注** 要查看站点持久性相关数据，您必须包含参数运行时筛选器 `sp_status`。

```
show gslbservice gs-1 runtime filter sp_status
```

Field	Value	
uuid	gslbservice-ff1b4e8d-663d-4cb9-932b-d007c81efba6	
name	gs-1	
POINT 1		
ldr_state		
last_changed_time	Tue Feb 6 00:11:02 2018 ms(242588) UTC	
flr_state[1]		
status	SYSERR_SUCCESS	
reason		
site_uuid	cluster-1e560f44-c898-41c3-818b-3433edbf9391	
last_changed_time	Tue Feb 6 00:11:02 2018 ms(904114) UTC	
groups[1]		
name	group2	
members[1]		
cluster_uuid	cluster-1e560f44-c898-41c3-818b-3433edbf9391	
site_name	site_B	
POINT 3		
vs_uuid	virtualservice-8a68c656-6a89-46d7-b9a5-1b693ae9798a	
vs_name	pay@site_B	
POINT 2		
ip	10.90.174.72	
oper_ips[1]	10.90.174.72	
vip_type	AVI_VIP	
services[1]		
port	80	
enable_ssl	False	
port_range_end	80	
app_type	APPLICATION_PROFILE_TYPE_HTTP	
sp_pools[1]		
uuid	pool-8a68c656-6a89-46d7-b9a5-1b693ae9798a	
name	SP-gs-1-pay@site_B	
POINT 4		
num_servers	1	
num_servers_up	1	
controller_status		
state	OPER_UP	
last_changed_time	Tue Feb 6 00:15:17 2018 ms(352917) UTC	
groups[2]		
name	group1	
members[1]		
cluster_uuid	cluster-3a179b95-dff9-444b-9986-ba89c4e19c44	
site_name	site_A	
POINT 3		
vs_uuid	virtualservice-dc871051-35e8-4bec-bd1f-3c63fb6b7087	
vs_name	pay@site_A	
POINT 2		

	ip		10.90.173.73	
	oper_ips[1]		10.90.173.73	
	vip_type		AVI_VIP	
	services[1]			
	port		80	
	enable_ssl		False	
	port_range_end		80	
	app_type		APPLICATION_PROFILE_TYPE_HTTP	
	sp_pools[1]			
	uuid		pool-dc871051-35e8-4bec-bd1f-3c63fb6b7087	
	name		SP-gs-1-pay@site_A	
	POINT 4			
	num_servers		1	
	num_servers_up		1	
	controller_status			
	state		OPER_UP	
	last_changed_time		Tue Feb 6 00:15:17 2018 ms(353741) UTC	
	services_state		Services-In-Sync	
	tenant_name		admin	
	checksum		e298eb000bb6d5bcaeaaf10d08e609441823c69fc83e7d9a50014769d7ed2b03	
	sp_oper_status			
	state		OPER_UP	
	POINT 5			
	last_changed_time		Tue Feb 6 00:15:17 2018 ms(353976) UTC	
+-----+-----+-----+-----+-----+				

### GSLB 服务的成员虚拟服务的状态

要了解组成 GSLB 服务的各个虚拟服务的更多信息，用户必须登录到相关的站点。下面显示的虚拟服务命令在 **site\_A** 上执行以报告本地虚拟服务 **pay@site\_A**。请注意最底部的站点持久性池引用。**site\_A** 上的 **SP** 池参与另一个主动站点上的某个虚拟服务提供的服务，客户端的请求必须持久保存到该站点中。在该示例中，只有一个额外站点 (**site\_B**)，但通常可能具有多个站点。

```
show virtualservice pay@site_A
```

+-----+-----+-----+-----+-----+	
Field	Value
+-----+-----+-----+-----+-----+	
uuid	virtualservice-dc871051-35e8-4bec-bd1f-3c63fb6b7087
name	pay@site_A
enabled	True
services[1]	
port	80
enable_ssl	False
port_range_end	80
application_profile_ref	System-HTTP
network_profile_ref	System-TCP-Proxy
pool_ref	pay
se_group_ref	Default-Group
analytics_policy	
full_client_logs	
enabled	True
duration	0 min
all_headers	True
throttle	0 per_second

client_insights	NO_INSIGHTS	
udf_log_throttle	10_per_second	
significant_log_throttle	10_per_second	
enabled	True	
vrf_context_ref	global	
enable_autogw	False	
analytics_profile_ref	System-Analytics-Profile	
weight	1	
delay_fairness	False	
max_cps_per_client	0	
limit_doser	False	
type	VS_TYPE_NORMAL	
cloud_type	CLOUD_NONE	
use_bridge_ip_as_vip	False	
flow_dist	LOAD_AWARE	
ign_pool_net_reach	False	
ssl_sess_cache_avg_size	1024	
remove_listening_port_on_vs_down	False	
close_client_conn_on_config_update	False	
tenant_ref	admin	
cloud_ref	Default-Cloud	
east_west_placement	False	
scaleout_ecmp	False	
active_standby_se_tag	ACTIVE_STANDBY_SE_1	
flow_label_type	NO_LABEL	
vip[1]		
vip_id	0	
ip_address	10.90.173.73	
enabled	True	
auto_allocate_ip	False	
auto_allocate_floating_ip	False	
avi_allocated_vip	False	
avi_allocated_fip	False	
vsvip_ref	vsvip-5c8iRv	
sp_pool_refs[1]	SP-gs-1-pay@site_A	
SP POOL ON site_A		
use_vip_as_snat	False	
+-----+		

## 代理池与其他池一起显示

下面的 `show pool` 命令在 `site_A` 上执行，它说明了站点持久性池使用与其他池相同的方式进行显示。与列出的最后 4 个池相比，两个 SP 池的“servers”（服务器）实际是唯一的一个额外站点上的虚拟服务。

```
show pool
```

Name	Port	Cloud	Oper State	Servers (up/total)	
+-----+					
SP-gs-2-securepay@site_A	80	Default-Cloud	OPER_UP	1/1	
SP-gs-1-pay@site_A	80	Default-Cloud	OPER_UP	1/1	
ship	80	Default-Cloud	OPER_UP	1/1	
securepay	80	Default-Cloud	OPER_UP	2/2	
pay	80	Default-Cloud	OPER_UP	1/1	

```
| securesship | 80 | Default-Cloud | OPER_UP | 2/2 |
+-----+-----+-----+-----+-----+
```

## 代理池状态

不会在 GSLB 级别汇总有关代理池的详细信息。用户需要登录到相关的站点，然后在与特定 GSLB 服务关联的代理池上执行 `show pool` 命令。在下面的示例中，我们登录到 `site_A` 以查看名为 `sp-gs-1-pay@site_A` 的站点持久性池。

请注意，SP 池中的一个“server”（服务器）由 `site_B` 上的虚拟服务的 VIP (10.90.174.72) 标识。

```
show pool sp-gs-1-pay@site_A
+-----+
+-----+
| Field |
+-----+
| Value |
+-----+
+-----+
| uuid | pool-dc871051-35e8-4bec-
| bdlf-3c63fb6b7087 |
| name | SP-gs-1-
| pay@site_A |
| default_server_port |
| 80 |
| graceful_disable_timeout | 1
| min |
| connection_ramp_duration | 10
| min |
| max_concurrent_connections_per_server |
| 0 |
| health_monitor_refs[1] | ghm-
| ping |
| servers[1] |
| | "SERVER" IS A VS ON
| site_B |
| ip |
| 10.90.174.72 | 10.90.174.72 IS ON site_B
| hostname |
| 10.90.174.72 |
| enabled |
| True |
| ratio |
| 1 |
| verify_network |
| False |
| resolve_server_by_dns |
| False |
| prst_hdr_val |
| 16077db5be5a5402f8185e02769756a3f0deffcdcd0ab28fe8a60ac13d0219e32 |
| static |
| False |
| rewrite_host_header |
| False |
| description | Gslb site-persistence
```

```

server
|
| server_count
1
| lb_algorithm
LB_ALGORITHM_LEAST_CONNECTIONS
| application_persistence_profile_ref
gap-1
| inline_health_monitor
True
| use_service_port
True
| capacity_estimation
False
| server_auto_scale
False
| vrf_ref
global
| fewest_tasks_feedback_delay
10
sec
| enabled
True
| request_queue_enabled
False
| request_queue_depth
128
| host_check_enabled
False
| sni_enabled
True
| rewrite_host_header_to_sni
False
| rewrite_host_header_to_server_name
False
| lb_algorithm_core_nonaffinity
2
| gslb_sp_enabled
True
| lookup_server_by_name
False
| description
Gslb site-persistence proxy
pool
| tenant_ref
admin
| cloud_ref
Default-Cloud
+-----+
+-----+

```

### 确定代理的客户端请求比例

对于每个 GSLB 服务，使用 NSX Advanced Load Balancer UI 在运行 GSLB 服务的虚拟服务成员的主动站点上监控每个池的活动。对于每个站点，收集：

- 1 GSLB 服务的本地虚拟服务的入站请求率。

## 2 其 SP 池请求率。

在所有站点中计算第 1 项总数和第 2 项总数。如果总体 SP 池请求率比总体虚拟服务请求率高，您可能希望增加 TTL 值。

# GSLB 的用户角色和帐户

多租户架构的预期隔离和管理限制扩展到 NSX Advanced Load Balancer GSLB。

## 预定义的角色

导航到**管理 > 帐户 > 角色**以检查默认的预定义角色。这些角色分配给授权的控制器用户。在该示例中，单击 **Tenant-Admin** 角色行右端的加号将展开所有 10 列，从而显示有关 NSX Advanced Load Balancer 平台的不同方面的更多详细信息。GSLB 权限（红色矩形）侧重于访问三个 GSLB 实体 - GSLB 配置、全局应用程序（服务）和支持地理位置的地理位置数据库。

Role	Application	Profiles	Group & Script	Security	Policy	WAF	Error Page	Operations	Infrastructure	Administration	Accounts	GSLB
Application-Admin	Write	Assorted	Write	Assorted	Write	Read	Write	Assorted	Assorted	Assorted	No Access	Assorted
Application-Operator	Read	Read	Read	Read	Read	Read	Read	Assorted	Read	Assorted	No Access	Read
Demo-AppOwner	Assorted	Assorted	Write	Write	No Access	No Access	No Access	Assorted	No Access	No Access	No Access	No Access
Foo-Bar	No Access	No Access	No Access	No Access	No Access	No Access	No Access	No Access	No Access	No Access	No Access	No Access
ReadOnly	Assorted	No Access	No Access	No Access	No Access	No Access	No Access	No Access	Assorted	Assorted	No Access	Assorted
Security-Admin	No Access	Assorted	No Access	Assorted	No Access	Read	Read	No Access	No Access	Assorted	No Access	No Access
System-Admin	Write	Write	Write	Write	Write	Write	Write	Write	Write	Assorted	Write	Write
Tenant-Admin	Write	Write	Write	Write	Write	Write	Write	Write	Write	Assorted	No Access	Assorted

Application	Profiles	Group & Script	Security	Policy	WAF	Error Page	Operations	Infrastructure	Administration	Accounts	GSLB
Virtual Service: Write Access	TCP/UDP Profile: Write Access	IP Address Group: Write Access	SSL/TLS Profile: Write Access	NAT Policy: Write Access	WAF Profile: Write Access	Error Page Profile: Write Access	Alert Config: Write Access	Cloud: Write Access	System Settings: No Access	Users: No Access	GSLB Configuration: Read Access
Pool: Write Access	Application Profile: Write Access	String Group: Write Access	Authentication Profile: Write Access	WAF Policy: Write Access	WAF Policy: Write Access	Error Page Body: Write Access	Alerts: Write Access	Service Engine: Write Access	Controller: No Access	Roles: No Access	GSLB Services: Write Access
Pool Group: Write Access	Persistence Profile: Write Access	DataScript: Write Access	PingAccess Agent: Write Access	Positive Security: Write Access	Positive Security: Write Access		Alert Action: Write Access	Service Engine Group: Write Access	Reboot: No Access	Tenant: No Access	GSLB Geo Profile: Read Access
HTTP Policy Set: Write Access	Health Monitor: Write Access	ProtocolParserScript: Write Access	PKI Profile: Write Access				Syslog: Write Access	Network: Write Access	Upgrade: No Access		
Network Security Policy: Write Access	Analytics Profile: Write Access		SSL/TLS Certificates: Write Access				Email: Write Access	VNF Context: Write Access	Troubleshooting: No Access		
AutoScale: Write Access	IPAM/DNS Profile: Write Access		Certificate Management Profile: Write Access				SNMP Traps: Write Access	User Credentials: Write Access	Internal: No Access		
DNS Policy: Write Access	Custom IPAM/DNS Profile: Write Access		Hardware Security Module Group: Write Access				Traffic Capture: Write Access	Controller Slot: Write Access	Software: Read Access		
	Traffic Clone: Write Access		SSO Policy: Write Access								
	ICAP Profile: Write Access										

对于系统中的每个角色，可以单独设置访问权限。下表简要说明了三个预定义角色的 GSLB 访问权限。

预定义的角色	访问权限
System-Admin	GSLB 配置
	GSLB 服务
	GSLB 地理位置数据库
Tenant-Admin	GSLB 配置
	GSLB 服务
	GSLB 地理位置数据库
Application-Admin	GSLB 配置



预定义的角色		访问权限
	GSLB 服务	该用户分配到的所有租户中的所有全局应用程序的写入访问权限
	GSLB 地理位置数据库	地理位置数据库的读取访问权限

## GSLB 管理员、全局应用程序管理员

根据要求，授权的用户可以使用一组不同的访问权限。

GSLB 只能由具有 GSLB 配置的写入访问权限的用户帐户进行配置。该访问权限是在 **System-Admin** 角色中预定义的。只能在管理员租户中配置 GSLB。系统管理员将 DNS 虚拟服务放置在管理员租户或某个其他租户中。不过，只能通过 CLI 使用站点的 GSLB DNS 虚拟服务的 UUID 在非管理员租户中配置该 DNS 虚拟服务。然后，与 NSX Advanced Load Balancer 租户关联的每个应用程序管理员可以将共享的 DNS 虚拟服务用于其全局应用程序。

具有 GSLB 服务的写入访问权限以及 GSLB 配置的读取访问权限的用户可以在自己的租户中定义全局应用程序（GSLB 服务）。所需的 DNS 记录是在共享的 DNS 服务上注册的。租户管理员可以获取仅为该租户定义的 GSLB 服务的分析结果。

### 注

- 能否创建 GSLB 服务取决于 GSLB 用户的权限，而不是登录的租户用户。
- 为了获得更好的审核跟踪，建议登录到为 GSLB 配置设置的用户帐户。例如，您可以创建一个名为 **gslb** 的用户，并在所有控制器集群中为其分配管理员角色。

## 根据特权配置 NSX Advanced Load Balancer UI 访问

在 NSX Advanced Load Balancer 中，如果 GSLB 配置的特权设置设为“无权访问”，并且 GSLB 服务的特权设为“读取”或“写入”，则可以访问 NSX Advanced Load Balancer UI 上的“GSLB 服务”选项卡。

### 注意事项

以下是提供的额外功能，但具有一些限制，如下所述：

- 上述访问仅适用于只读模式。您无法编辑现有的 GSLB 服务或创建新的 GSLB 服务。
- 您能够查看表，单击“服务”以及查看“成员状态”和“事件”子选项卡，但不能查看“FQDN 详细信息”子选项卡。
- “创建”选项将灰显，悬停文本显示：必须将 GSLB 配置权限设置为读取或写入才能创建 GSLB 服务。

以下是保持不变的选项：

- 如果 GSLB 服务的特权设置为只读模式，并且“GSLB 配置”为“读取”或“写入”，则您仍处于只读模式，但可以使用“FQDN 详细信息”子选项卡。
- 如果 GSLB 服务设置为“无权访问”，则无法使用整个“GSLB 服务”选项卡。

- 如果 GSLB 服务权限设置为“写入”，但服务站点是子站点，“创建”选项将灰显，并且 NSX Advanced Load Balancer UI 将 GSLB 站点 {主站点名称} 显示为主站点。

**注** 可以根据 GSLB 管理员的特权配置 GSLB 站点。

## 从从属站点中启用 GSLB 配置更改

本节重点介绍了如何从从属站点中启用 GSLB 配置更改。

也可以从从属站点中执行以下配置更改：

- 启用或禁用 GSLB 服务组
- 启用/禁用 GSLB 服务组成员

如果仅要求避免将流量发送到 GSLB 从属站点上的某些服务器，并且您无权访问主站点，这是非常有用的。在 NSX Advanced Load Balancer 版本 20.1.6 之前，只能从主站点中进行配置更改。通过使用该功能，您也可以从从属站点中启用或禁用 GSLB 组或 GSLB 组成员。需要进行以下配置更改或满足以下必备条件，从属站点上的用户才能执行更改：

- 配置每字段授权
- 在主站点中配置 JWT 配置文件
- 从从属站点中启用配置

### 配置每字段授权

- 配置角色 `GSLB_Group_Enabled` 和 `GSLB_Group_Member-Enabled`

### 配置角色 `GSLB_Group_Enabled` 和 `GSLB_Group_Member-Enabled`

要从从属站点中执行更改，用户应具有以下关联的角色：

- `Gslb_Group_Member_Enabled` - 该角色应具有 GSLB 服务的写入访问权限。
- `Gslb_Group_Enabled` - 该角色应具有 GSLB 服务的写入访问权限。

有关配置按字段授权的更多信息，请参阅[按字段 RBAC](#)。

```
[admin:10-10-10-2]: > configure role Gslb_Group_Member_Enabled
[admin:10.10.10.2]: role> privileges
New object being created
[admin:10.10.10.2]: role:privileges> type write_access
[admin:10.10.10.2]: role:privileges> resource PERMISSION_GSLBSERVICE
[admin:10.10.10.2]: role:privileges> save
```

在下面的 CLI 片段中，为用户 `gslbsitegroupmemberadmin` 配置了 `Gslb_Group_Member_Enabled` 角色。配置的用户具有 GSLB 服务的写入访问权限，以及启用或禁用指定 GSLB 服务中的 GSLB 组的特权。

```
[admin:10-10-10-2]: > show user gslbsitegroupmemberadmin
+-----+-----+
| Field          | Value                                     |
+-----+-----+
| uuid           | user-52a6e643-d55d-45e9-8bca-0601b53d5b20 |
```

```

| username      | gslbsitegroupmemberadmin      |
| password      | <sensitive>                    |
| name          | gslbsitegroupmemberadmin      |
| email         |                                |
| access[1]     |                                |
|   role_ref    | Gslb_Group_Member_Enabled     |
|   all_tenants | True                          |
| access[2]     |                                |
|   role_ref    | Gslb_Health_Monitor           |
|   all_tenants | True                          |
| is_superuser  | False                         |
| local         | True                          |
| user_profile_ref | Default-User-Account-Profile |
+-----+-----+

```

```

[admin:10-10-10-2]: > show role Gslb_Group_Member_Enabled
+-----+-----+
| Field          | Value                          |
+-----+-----+
| uuid           | role-95e82558-1883-47af-8802-a6834c5feb76 |
| name           | Gslb_Group_Member_Enabled     |
| privileges[1]  |                                |
|   type         | WRITE_ACCESS                  |
|   resource     | PERMISSION_GSLBSERVICE       |
|   subresource  |                                |
|   exclude_subresources | False                      |
|   subresources[1] | SUBRESOURCE_GSLBSERVICE_GROUP_MEMBER_ENABLED |
| allow_unlabelled_access | True                      |
| tenant_ref     | admin                         |
+-----+-----+

```

同样，在下面的 CLI 片段中，为用户 `gslbsitegroupadmin` 配置了 `Gslb_Group_Enabled` 角色。配置的用户具有 GSLB 服务的写入访问权限，以及启用或禁用指定 GSLB 服务中的 GSLB 组的特权。

```

[admin:10-10-10-2]: > show user gslbsitegroupadmin
+-----+-----+
| Field          | Value                          |
+-----+-----+
| uuid           | user-27a528f5-2e8e-42bb-b5b0-2229123215ec |
| username       | gslbsitegroupadmin            |
| password       | <sensitive>                    |
| name          | gslbsitegroupadmin            |
| email         |                                |
| access[1]     |                                |
|   role_ref    | Gslb_Group_Enabled           |
|   all_tenants | True                          |
| access[2]     |                                |
|   role_ref    | Gslb_Health_Monitor          |
|   all_tenants | True                          |
| is_superuser  | False                         |
| local         | True                          |

```

```
| user_profile_ref | Default-User-Account-Profile |
+-----+-----+
```

```
[admin:10-10-10-2]: > show role Gslb_Group_Enabled
+-----+-----+
| Field | Value |
+-----+-----+
| uuid | role-0facf895-c551-4cd0-b1f6-73b4c890c746 |
| name | Gslb_Group_Enabled |
| privileges[1] | |
| type | WRITE_ACCESS |
| resource | PERMISSION_GSLBSERVICE |
| subresource | |
| exclude_subresources | False |
| subresources[1] | SUBRESOURCE_GSLBSERVICE_GROUP_ENABLED |
| allow_unlabelled_access | True |
| tenant_ref | admin |
+-----+-----+
```

**注** 需要在所有从属站点和主站点上添加上述角色。

## 配置联合 JWT 配置文件

GSLB 从属站点使用 JWT 令牌与主站点通信以执行配置 API 调用。出于这个原因，所有站点需要使用 JWT 服务器配置文件加密/解密令牌，以从令牌中获取所需的信息。JWT 服务器配置文件需要配置为一个联合对象，从而在 JWT 服务器配置文件配置中启用 `is_federated` 标记。这是在主站点上执行的必需步骤；如果未执行该步骤，则无法启用与 GSLB 站点无关的配置。可以使用 `configure jwtserverprofile` 命令在主站点上配置 JWT 服务器配置文件，并将 `is_federated` 标记值设置为 `True`。

以下是 JWS 密钥支持的算法：

- 密钥长度为 32 字节的 HS256
- 密钥长度为 48 字节的 HS384
- 密钥长度为 64 字节的 HS512

可以使用以下 API 生成在 JWT 服务器配置文件中使用的密钥：

```
https://10.79.169.140/api/symmetric-key?alg=HS512
```

应用上述 API 后的示例输出如下所示：

```
{
  "kid": "5105e67b-85c0-4d27-aaf1-3bef8020d8ac",
  "alg": "HS512",
  "kty": "oct",
  "key":
    "TTA2Zk5Kb2NWTWE4ZmZ2bnRrbHNDZ0xNbUV2Z211ZThHMnBtaFE1Nm1DM0tZMmFqWjlHcjRBcmI2NDdyNGhoQg"
}
```

算法参数是可选的，默认值为 HS256。

可以使用 `configure jwtserverprofile` 命令在主站点上配置 JWT 服务器配置文件，将 `is_federated` 标记值设置为 `True`，并将 `jwt_profile_type` 值设置为 `CONTROLLER_INTERNAL_AUTH`。

在以下 CLI 片段中，为 JWT 配置文件 `gslb_jwt_server_profile` 配置了 HS256 算法：

```
[admin:10-79-169-140]: > show jwtserverprofile gslb_jwt_server_profile
+-----+-----+
| Field                | Value                                |
+-----+-----+
| uuid                 | jwtserverprofile-03201645-2556-4d13-9d0c-8415c80faa73 |
| name                 | gslb_jwt_server_profile             |
| tenant_ref           | admin                               |
| jwt_profile_type      | CONTROLLER_INTERNAL_AUTH            |
| controller_internal_auth |                                     |
| symmetric_jwks_keys[1] |                                     |
|   alg                | HS256                               |
|   kty                | OEpZREZsTThXU2RxdjJVd0g5WG5pRHVoMkNQaHU2Mjc       |
|   kid                | ef0ae791-2380-4447-bf79-d3d01575d3e2                 |
|   key                | <sensitive>                                     |
| is_federated          | True                                |
+-----+-----+
[admin:10-79-169-140]: >
```

## 从从属站点中启用配置更改

在主站点上的 GSLB 全局配置中将 `enable_config_by_members` 标记值设置为 `True`。必须配置并提供联合 JWT 配置文件以启用该配置。

```
[admin:10-10-10-1]: > show gslb glb-1
+-----+-----+
| Field                | Value                                |
+-----+-----+
| uuid                 | gslb-c8ebc3e3-16e1-47f2-9f70-5ade3f1e1221           |
| name                 | glb-1                                                  |
| ...                  | ...                                                    |
| ...                  | ...                                                    |
| tenant_scoped         | False                                                  |
| enable_config_by_members | True                                                  |
+-----+-----+
```

在执行上述步骤后，具有所需角色的从属站点用户可以启用或禁用 GSLB 服务组或 GSLB 服务组成员。

## 插入 DNS 的扩展机制 (EDNS) 客户端子网选项

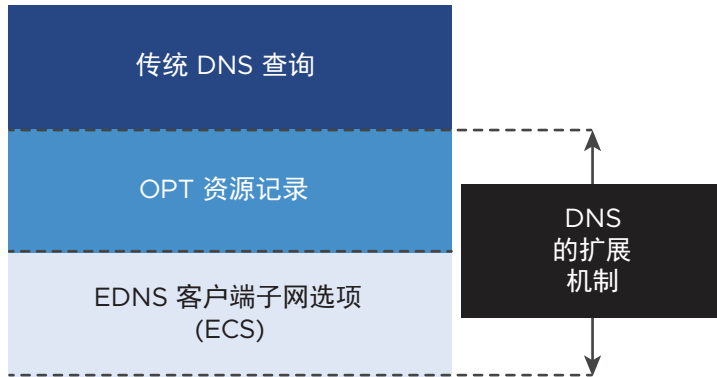
如果 DNS 查询没有 ECS 选项，则 NSX Advanced Load Balancer 支持在查询中插入 ECS 选项。如果 DNS 查询已具有 ECS 选项，它支持更新 ECS 选项。

DNS 自最初开发以来就需要不断进行改进。由于基本 DNS 协议中提供的某些标记字段、返回代码和标签类型的大小受到限制，因此，决定以向后兼容的方式扩展 DNS 以适应新的标记和响应代码以及更长的响应。自 1999 年以来，DNS 的扩展机制 (EDNS) 已成为解决这一难题的方法。

图 1 显示 OPT 资源记录 (OPT RR) 对于 DNS 扩展至关重要。它采用的结构允许使用各种不同的选项，包括 EDNS 客户端子网选项 (ECS)，这允许权威 DNS 提供程序使用额外信息以做出更明智的流量路由决策。例如：

- 为地理算法提供更准确的客户端位置信息
- 为一致哈希算法提供客户端的源 IP 地址
- 为来自混合的专用和公用网络的客户端提供服务时

图 2-8. 1. 如何扩展传统 DNS 查询



**注** IPv6 地址也支持 DNS 配置文件的 EDNS 选项。

## EDNS 和 ECS 选项如何与 NSX Advanced Load Balancer DNS 一起使用

本节重点介绍了 EDNS 和 ECS 选项如何与 NSX Advanced Load Balancer DNS 一起使用。

### 在 NSX Advanced Load Balancer DNS 虚拟服务上启用 EDNS

正如前面所述，在充当权威 DNS 的同时，NSX Advanced Load Balancer DNS 虚拟服务可以直接通过 OPT RR 和 ECS 选项获取信息。要让它分析该信息并将 EDNS 扩展信息附加到客户端日志中，请在 NSX Advanced Load Balancer UI 中选中**处理 EDNS 扩展**框（如下面的屏幕截图所示），或者在 NSX Advanced Load Balancer CLI 中将相应的 EDNS 参数设置为 True。

图 2-9. 应用程序配置文件编辑器显示的 DNS 设置

**• DNS Settings •**

**Valid subdomains** ?

**TTL** ?

Sec

**Number of IPs returned by DNS server** ?

**(Options for) Invalid DNS Query processing** ?

Drop unhandled DNS requests
▼

**Subnet prefix length** ?

☒ **Process EDNS Extensions** ?

☒ **Respond to AAAA queries with empty response** ?

## 案例 1: NSX Advanced Load Balancer DNS 虚拟服务是权威 DNS，并收到 OPT RR + ECS 选项

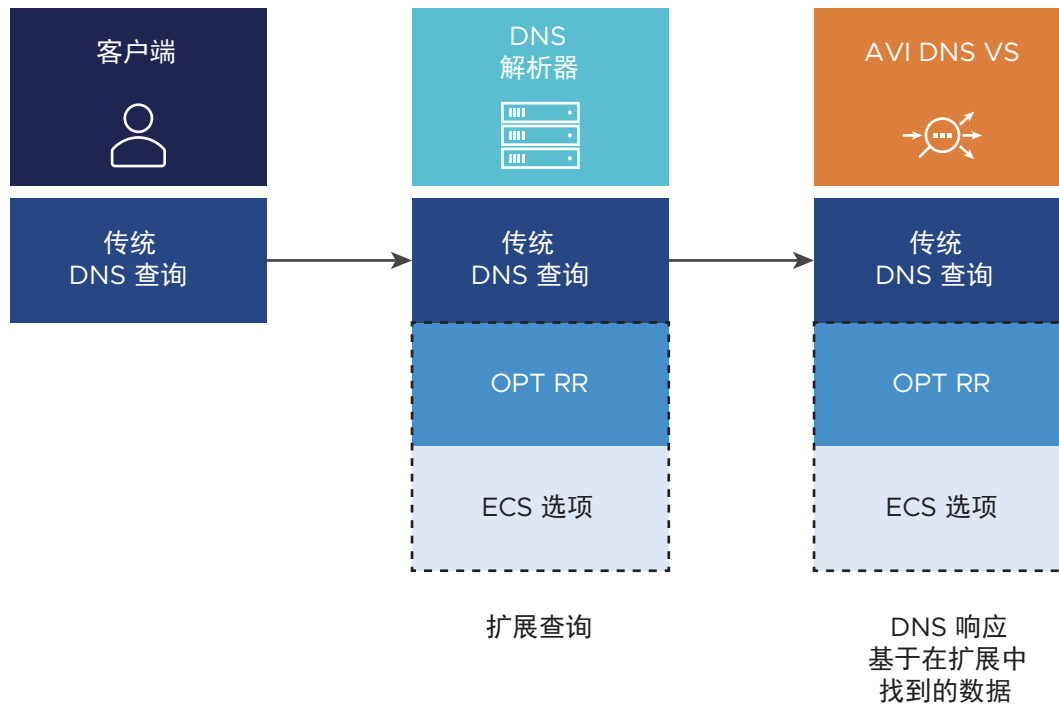
除了已选中**处理 EDNS 扩展**框以外，还要确保提供权威域名列表。例如，在下面的 NSX Advanced Load Balancer CLI 序列中：

```
configure applicationprofile System-DNS
dns_service_profile
authoritative_domain_names avi.com
authoritative_domain_names foo.com
save
save
```

假设图 2 中的入站 DNS 请求针对以下域之一：

- 客户端系统向其 DNS 解析器发送传统 DNS 查询。请注意，它发送的请求既不包含 OPT RR，也不包含 ECS 选项。
- 根据客户端的源地址，DNS 解析器可能会修改它收到的 DNS 查询。这样做是为了使权威 DNS 能够以更明智的方式做出响应，即，根据客户端的地址做出响应，而不是根据 DNS 解析器本身的源 IP。
- NSX Advanced Load Balancer DNS 根据它在 ECS 选项中的地址信息组成响应。

图 2-10. 2. 权威 NSX Advanced Load Balancer DNS 根据 ECS 选项响应查询

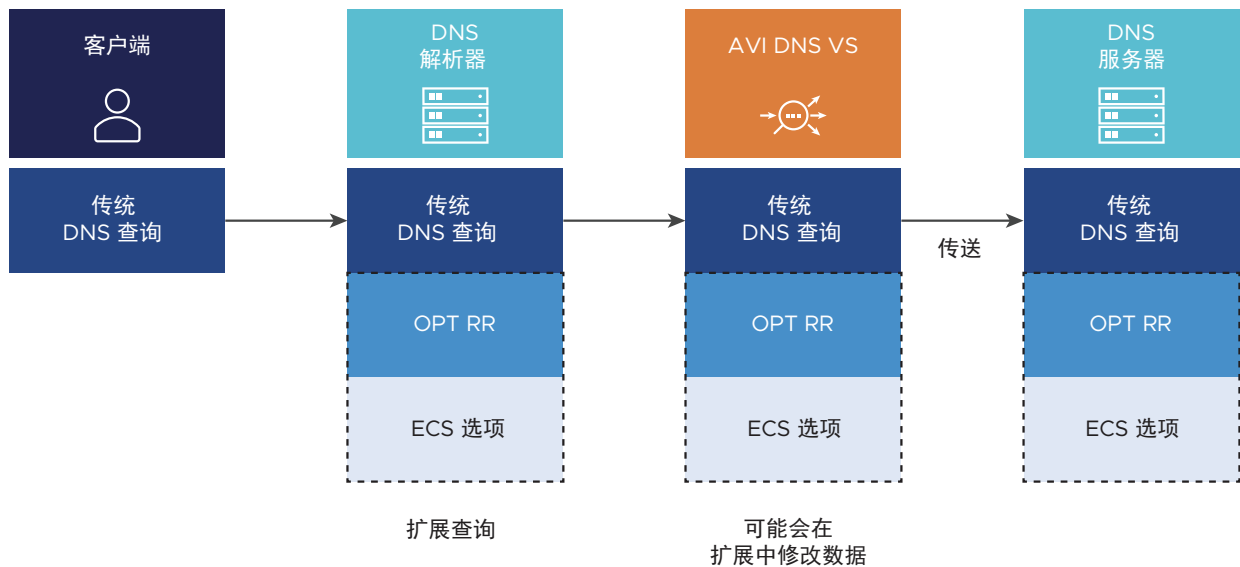


## 案例 2: NSX Advanced Load Balancer DNS 虚拟服务不是权威 DNS，并收到 OPT RR + ECS 选项

与案例 1 相比，图 3 显示 NSX Advanced Load Balancer DNS 虚拟服务不是权威 DNS 的查询。如果已为 NSX Advanced Load Balancer DNS 虚拟服务定义 DNS 服务器池，请求将传送到该池。在转发的请求的 ECS 选项中包含的客户端子网地址信息取决于两个值：

- 1 DNS 解析器附加并发送的 ECS 选项中包含的子网前缀长度参数值
- 2 edns\_client\_subnet\_prefix\_len，这是管理员通过 CLI 设置的 NSX Advanced Load Balancer DNS 虚拟服务应用程序配置文件参数。它的值范围是 1 到 32 之间

图 2-11. 3. NSX Advanced Load Balancer DNS 将 DNS 请求传送到 DNS 服务器



前缀长度是以两种方式解释的：

- 1 它表示前导地址位数，之后的所有地址位均为 0
- 2 在舍入到八位的整数倍时，它指定需要传送的八位字节数

例如，前缀长度 19 表示有关子网的以下信息：

- 子网地址中的第 20 到第 32 位为 0
- 仅需要传送 24 位（即三个八位字节）以标识子网。第 4 个八位字节是多余的

在通过 DNS 服务器传送 ECS 选项时，NSX Advanced Load Balancer DNS 虚拟服务将确保客户端子网地址由两个前缀长度中的较小者控制。也就是说：

- 如果入站子网前缀长度小于 NSX Advanced Load Balancer DNS 的 edns\_client\_subnet\_prefix\_len 参数值（请参阅图 2 中的 NSX Advanced Load Balancer UI），ECS 选项在传送时将保持不变。

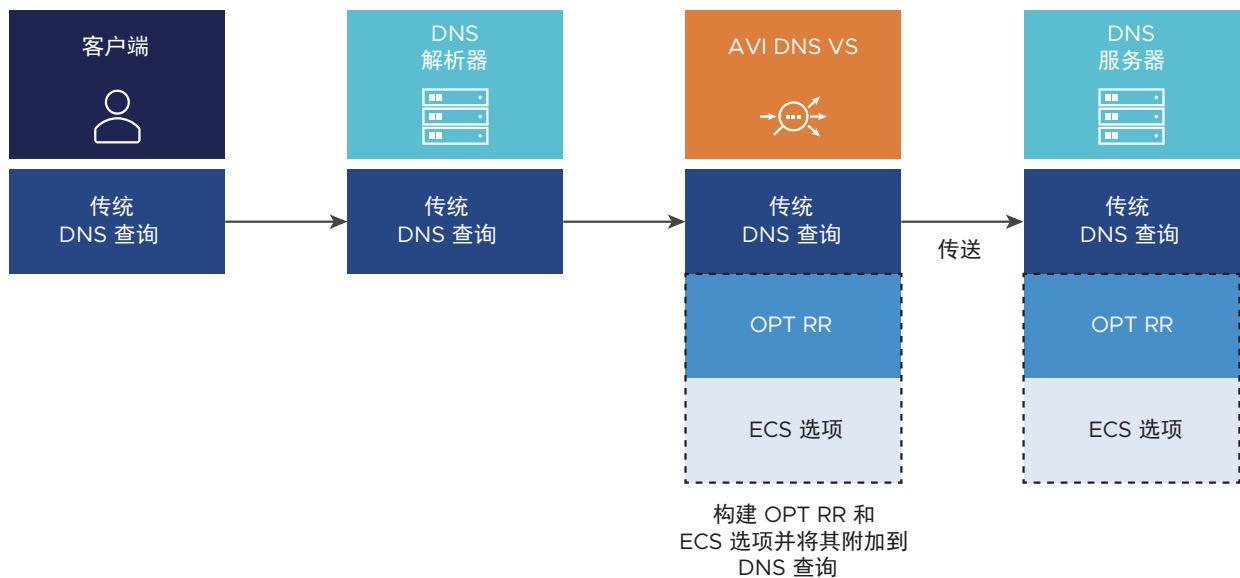


- 如果入站子网前缀长度（例如，26）大于 NSX Advanced Load Balancer DNS 的 `edns_client_subnet_prefix_len` 参数值（例如，16），则 NSX Advanced Load Balancer 将一些入站位（例如，此处为 10 个）设置为 0，如果长度足够长，则将较少的八位字节（例如，2 个而不是 4 个）转发到图 2 右侧所示的 DNS 服务器。

### 案例 3: NSX Advanced Load Balancer DNS 虚拟服务不是权威 DNS，并且未收到 OPT RR 和 ECS 选项

图 4 显示从 DNS 解析器收到的 DNS 请求不包含 EDNS 信息。此外，该 DNS 请求针对 NSX Advanced Load Balancer DNS 不是权威 DNS 的域。因此，需要进行转发。在这种情况下，NSX Advanced Load Balancer DNS 虚拟服务将创建一个 OPT RR，并插入具有 1 到 4 个八位字节和相应数量的尾随 0 的客户端子网地址（对于 ECS 选项），如上所述。

图 2-12. 4. NSX Advanced Load Balancer DNS 将 OPT RR 和 ECS 选项附加到转发的 DNS 查询



### 默认启用的 EDNS 选项

默认情况下，将为 System-DNS 配置文件启用 EDNS 选项。如果 NSX Advanced Load Balancer 是从旧版本升级的，则不会在现有 DNS 配置文件中默认启用 EDNS。不过，如果在同一 NSX Advanced Load Balancer 控制器上创建了新的 DNS 配置文件，则默认启用 EDNS。

执行 `show application profile <profile name>` 命令以检查 `edns` 标记值（设置为 `True`），如下所示。

```
[admin:10-155-1-175]: > show applicationprofile DNS_profile1

| uuid | applicationprofile-104c53ff-eca7-4fed-9480-33e00c23bf8b |
| name | new -DNS|
| type | APPLICATION_PROFILE_TYPE_DNS |
| dos_rl_profile | |
```

```

| dos_profile | |
| thresh_period | 5 sec |
| dns_service_profile | |
| num_dns_ip | 1 |
| ttl | 30 sec |
| error_response | DNS_ERROR_RESPONSE_NONE |
| edns | True |

```

“处理 EDNS 扩展”是 NSX Advanced Load Balancer 控制器 UI 上为 EDNS 功能提供的选项。

- 1 要选中该选项，请导航到**模板 > 配置文件 > 应用程序**，然后根据需要选择所需的 DNS 配置文件或 System-DNS 配置文件。
- 2 如果未启用该选项，请启用**处理 EDNS 扩展**的复选框。

General

Name\* <sup>?</sup>

Type <sup>?</sup> L4 SSL/TLS L4 **DNS** SYSLOG HTTP SIP

Description

• DNS Settings •

Number of IPs returned by DNS server <sup>?</sup>

Negative TTL <sup>?</sup>  Sec

TTL <sup>?</sup>  Sec

(Options for) Invalid DNS Query processing <sup>?</sup> Drop unhandled DNS requests ▼

Subnet prefix length <sup>?</sup>

☒ Process EDNS Extensions <sup>?</sup>

☒ Respond to AAAA queries with empty response <sup>?</sup>

Cancel Save

## 响应中的 ECS 信息

支持响应中的 ECS 信息。如果来自客户端的 DNS 请求包含 ECS 信息，并且应用程序配置文件启用了“处理 EDNS 扩展”，则 SE 的 NSX Advanced Load Balancer 控制器 DNS 生成的响应将 ECS 信息添加到响应中。响应中的范围前缀长度将等于请求中的源前缀长度。

## 与第三方 GSLB 站点集成

可以将 NSX Advanced Load Balancer 上下文外部运行的应用程序服务合并到 NSX Advanced Load Balancer GSLB 配置的全局应用程序中，从而为全局应用程序提供单一可见性和控制点。可以将多组第三方应用程序划分到第三方站点以简化管理任务，例如，站点维护。

### 将第三方服务与第三方站点相关联

就像本机 NSX Advanced Load Balancer 成员服务一样，第三方成员服务也需要加入到某个 NSX Advanced Load Balancer GSLB 池中。事实上，它可能是第一个加入到 GSLB 池的服务。这实际就是下面的 GSLB 服务编辑器屏幕截图中显示的内容。

New GSLB Service

Name\*

GSLBServiceName1

Application Name\*

app1.alpha.com

+ Add Domain Name

Subdomain\*

.alpha.com

Health Monitor

Health Monitor Scope

☐ Only Non Avi Members
 ☒ All Members

Controller Health Status

Select Group Type

Active Active

Active Standby

LB Algorithm\*

Round Robin

Pool Member

☒ IP Address
 ☐ Virtual Service

IP Address or FQDN\*

1.2.3.4

Third-party Site Cluster Controller

NonAviSite1

Public IP Address

Description

First of several services not running under an Avi Controller. Other IP addresses planned for this pool.

Add GSLB Pool Member

Save

通常，您可以按 IP 地址标识池成员，也可以将其标识为默认选择的本机 NSX Advanced Load Balancer 虚拟服务。如果按 IP 地址标识，NSX Advanced Load Balancer 自动推断该成员为非 NSX Advanced Load Balancer 服务，并且必须输入 IP 地址或 FQDN 以查找该成员。

对于加入的每个第三方池成员，您可以选择提供预先存在或新创建的第三方站点名称（使用**第三方站点集群控制器**字段）。与 NSX Advanced Load Balancer 站点类似，其他第三方成员服务可能位于给定的第三方站点上。

## 用例：禁用第三方站点

通过将外部服务聚合到第三方站点，管理员可以禁用站点的所有成员，而不必明确修改很多 GSLB 服务的成员。例如，在单个站点中执行硬件或软件维护时，用户只需一步即可禁用一组常驻成员服务。例如，从双站点配置开始。

## 用例：优化运行状况监控

只能将数据路径运行状况监控应用于第三方成员。通过将 GSLB 池外部成员收集到第三方站点，可以轻松优化运行状况监控。首先，确定运行状况监控最高效的主动 NSX Advanced Load Balancer 站点（与第三方站点的远近程度和其他因素将影响选择的站点）。然后，使用 GSLB 第三方站点编辑器从“运行状况监控器代理”下拉菜单中选择所选的 NSX Advanced Load Balancer 站点。有关通过代理进行运行状况监控的更多详细信息，请参阅[基于数据平面的本地全局应用程序运行状况监控](#)。

有关第三方 GSLB 站点的详细配置步骤，请参阅[添加第三方站点](#)。

## 附加信息

### 绕过负载均衡算法

在某些情况下，可能希望根据满足的特定条件为某些客户端绕过负载均衡算法。有关更多详细信息，请参阅[使用回退和首选站点选项选择 GSLB 站点](#)。

### 启动的最少成员数

GSLB 服务最小成员数参数考虑给定 GSLB 服务池中的启动成员服务数，以修改选择过程中的第一步。如果启动服务数降到池的最小成员数以下，则不会将流量传送到该池，即使可能已选择了该池（基于其优先级或远近程度）。

## 两级 GSLB 池成员服务选择

- 选择 GSLB 池成员服务是一个两级过程：先选择池，然后选择服务。有关更多详细信息，请参阅[如何在服务和池级别设置 GSLB 算法](#)文章。
- GSLB 服务中的每个 GSLB 池分配了不同的优先级。可以为具有 GSLB 服务的多个 GSLB 池分配相同的优先级。如果一组池具有相同的优先级并超过其他池的优先级，只要满足最小成员数逻辑，NSX Advanced Load Balancer 就会以循环方式在这组池中进行选择。有效的优先级范围包括优先级 0。如果将池的优先级设置为 0，将使该池不符合选择条件。这可能是临时设置的，例如，对组成池的服务执行维护。

---

**注** 将池优先级设置为 0 并不等同于将其禁用。将继续监控 0 优先级池的运行状况；其状态显示为“启动”或“关闭”，而不是“已禁用”。

---

## 防火墙设置

防火墙设置必须允许所有主动站点之间的双向控制器通信。此外，要使数据平面运行状况监控器正常工作，所有主动站点需要能够探测每个站点中参与 GSLB 服务并配置为进行探测的所有虚拟服务（可以将 GSLB 服务配置为探测所有成员或仅探测非 NSX Advanced Load Balancer 成员）。

# GSLB 配置

# 3

本节介绍了以下 GSLB 配置：

- GSLB 站点配置
- GSLB 的 DNS 配置
- GSLB 服务配置
- GSLB 站点 Cookie 持久性

本章讨论了以下主题：

- 使用 NSX Advanced Load Balancer UI 配置 GSLB 站点
- 使用 NSX Advanced Load Balancer CLI 配置 GSLB 站点
- GSLB 的 DNS
- GSLB 服务配置
- 使用 NSX Advanced Load Balancer CLI 配置租户
- 配置企业/外部 DNS 服务器以将子域委派给 NSX Advanced Load Balancer DNS 服务
- A 记录返回：启用解析 CNAME

## 使用 NSX Advanced Load Balancer UI 配置 GSLB 站点

本节介绍了设置 GSLB 站点所需的以下配置步骤。

- 设置单个控制器集群
- 在托管 DNS 的所有主动站点上配置本地 DNS 虚拟服务
- 配置本地应用程序虚拟服务
- 指定 GSLB 主站点并添加站点配置
- 配置额外的域

### 设置单个控制器集群

创建两个或更多控制器集群（取决于 DC/位置数），并运行初始系统配置步骤。每个控制器集群可能是单节点（测试和开发）集群或三节点（生产）集群。在以下示例中，Santa Clara (10.10.25.10) 和 Boston (10.160.0.20) 是在相应位置/DC/站点上运行的两个 NSX Advanced Load Balancer 控制器。

## 在托管 DNS 的所有主动站点上配置本地 DNS 虚拟服务

在所有需要托管 DNS 服务的集群上配置一个本地 DNS 虚拟服务，并将其绑定到本地 g-dns SE 组。

对于每个控制器集群，配置一个 SE 组（在该示例中名为 g-dns）以托管 DNS 虚拟服务。要配置 SE 组，请导航到**基础架构 > 云 > 服务引擎组**。

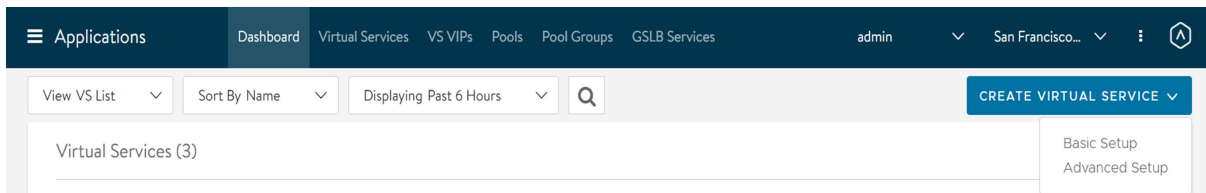
### 注

- 假设控制器已启动并正在运行，并且已完成云配置。
- 虚拟服务和 SE 组名称不需要在所有 GSLB 站点中完全相同。

在以下屏幕截图中，作为建议的最佳做法，**每个服务引擎的虚拟服务数值**设置为 1（默认值为 10）。

在 Santa Clara (10.10.25.10) 中：

- 1 在所有需要托管 DNS 服务的集群上配置一个 DNS 虚拟服务，并将其绑定到 g-dns SE 组：
- 2 在“高级设置”中创建一个虚拟服务。



- 3 选择一个**应用程序配置文件**以作为 **System-DNS**。接受“TCP/UDP 配置文件”字段的默认值 (System-UDP-Per-Pkt)。

**New Virtual Service: g-dns**

Step 1: Settings | Step 2: Policies | Step 3: Analytics | Step 4: Advanced | Step 5: Static DNS Records

Name <sup>\*</sup> <sup>?</sup>  Enabled <sup>?</sup> ☒

**• VIP Address •** Switch to Advanced

VIP Address <sup>\*</sup> <sup>?</sup>  ☒

**• Profiles •**

Application Profile <sup>\*</sup> <sup>?</sup>

TCP/UDP Profile <sup>\*</sup> <sup>?</sup>

WAF Policy <sup>?</sup>

Error Page Profile <sup>?</sup>

**• Service Port •** Switch to Advanced

Services <sup>?</sup>

+ Add Port

**• Pool •**

☒ Pool ☐ Pool Group

Pool <sup>?</sup>

☐ Ignore network reachability constraints for the server pool <sup>?</sup>

**• Other Settings •**

Description

Cancel Next ▶

- 4 单击下一步以执行步骤 2 策略。
- 5 单击服务端口部分中的切换到高级，添加新端口 53，为该端口选择覆盖 TCP/UDP 配置文件，然后选择 **System-TCP-Proxy**。这是可选的；如果您需要使用 DNS 而不是 TCP，则是必需的。如果您仅将 NSX Advanced Load Balancer DNS 用于 GSLB，并且 NSX Advanced Load Balancer DNS 不是此处提到的主 DNS 服务器，则不需要使用池。



**New Virtual Service: g-dns**

Step 1: Settings | Step 2: Policies | Step 3: Analytics | Step 4: Advanced

Name \*  Enabled ☒

VIP Address \*  [Switch to Advanced](#)

Service Port \*  [Switch to Basic](#)

Services  TO  ☐ Override TCP/UDP

☒ Override TCP/UDP

TO  ☐ Override TCP/UDP

☒ Override TCP/UDP

[+ Add Port](#)

Profiles

Application Profile \*

TCP/UDP Profile \*

Pool

☒ Pool ☐ Pool Group

Pool

☐ Ignore network reachability constraints for the server pool

[Cancel](#) [Next](#)

- 6 如果需要，请配置网络安全规则。
- 7 单击下一步以执行步骤 3 分析。
- 8 接受分析默认值或更改它们，如下面的屏幕截图中所示：

**New Virtual Service: g-dns**

Step 1: Settings | Step 2: Policies | Step 3: Analytics | Step 4: Advanced | Step 5: Static DNS Records

You may want to select a pool.

Analytics Profile

Metric Update Frequency ☒ Real Time Metrics  min

Client Log Settings

Significant Log Throttle  Logs/Second

UDF Log Throttle  Logs/Second

Non-significant Logs:

☒ Enabled  Minutes  Logs/Second

Displaying 0 item(s)

☐ Enabled

No items found.

[Cancel](#) [Previous](#) [Next](#)

- 9 单击下一步以执行步骤 4 高级。
- 10 在“其他设置”下面，选择为托管该 DNS 虚拟服务而创建的 SE 组。

**New Virtual Service: g-dns** Help

Step 1: Settings Step 2: Policies Step 3: Analytics Step 4: Advanced Step 5: Static DNS Records

You may want to select a pool.

**Performance Limit Settings**

☐ Performance Limits

**Quality of Service**

Weight 1

Fairness Throughput And Delay Fairness **Throughput Fairness**

**Virtual IP Placement Settings**

Placement Network Any Network

**Other Settings**

☒ Auto Gateway ☐ Use VIP as SNAT SE Group g-dns

☐ Advertise VIP via BGP ☐ Advertise SNAT via BGP

SNAT IP Address x.x.x.x, x.x.x.y

☐ Remove Listening Port when VS Down

Traffic Clone Profile Select Traffic Clone Profile

Cancel Previous Next

11 （可选）创建静态 DNS 记录。

**New Virtual Service: g-dns** Help

Step 1: Settings Step 2: Policies Step 3: Analytics Step 4: Advanced Step 5: Static DNS Records

You may want to select a pool.

**Static DNS Records**

Create DNS Record

Displaying 0 item(s)

FQDN	Type	Record Data	TTL	Algorithm
No items found.				

Cancel Previous Save

12 单击**保存**以完成为 Santa Clara 站点定义 DNS 虚拟服务的过程。

同样，在另一个站点/DC（即 Boston，我们的示例中为 10.160.0.20）上创建一个 DNS 虚拟服务。DNS 虚拟服务命名为 colo-dns，VIP 为 10.160.110.100。

## 配置本地应用程序虚拟服务

创建应用程序虚拟服务。例如，在控制器集群 1 中创建 HTTP 虚拟服务 vs-1，在控制器集群 2 中创建虚拟服务 vs-2。

有关更多详细信息，请参阅[配置虚拟服务](#)：

在 10.10.25.10 (Santa Clara) 上：

### Virtual Service: vs-1

[Scale Out](#)[Scale In](#)[Migrate](#)**Service Engine**

10.10.25.27 (primary)  
(Default-Group)

**Uptime**

13s

**Address**

10.90.12.100

**Application Profile**

System-HTTP

**Service Port**

80

**TCP/UDP Profile**

System-TCP-Proxy

在 10.160.0.20 (Boston) 上：

### Virtual Service: vs-2

[Scale Out](#)[Scale In](#)[Migrate](#)**Service Engine**

10.160.2.150 (primary)  
(Default-Group)

**Uptime**

23s

**Address**

10.160.110.200

**Application Profile**

System-HTTP

**Service Port**

80

**TCP/UDP Profile**

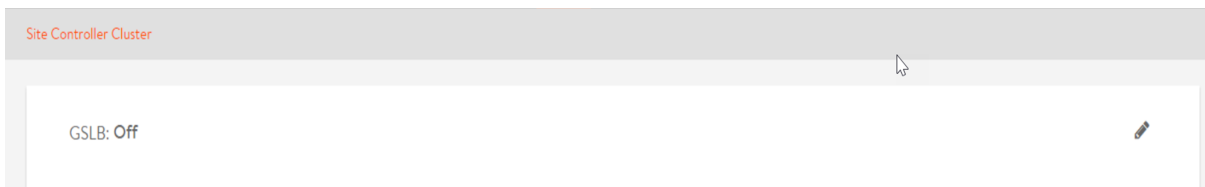
System-TCP-Proxy

## 指定 GSLB 主站点并添加站点配置

选择其中的一个控制器集群以作为主集群，并在其中执行 GSLB 配置。在示例拓扑中，选择 Santa Clara 站点 (10.10.25.10) 以作为 GSLB 主站点。

### 步骤

- 1 导航到[基础架构 > GSLB](#)。



- 2 编辑并创建 GSLB 主站点。

请注意，NSX Advanced Load Balancer 如何正确假设在首次激活 GSLB 时该控制器将成为主动成员。特别是主站点成员。

## New GSLB Configuration

Name\* ?

☒ Active Member ?

Username\* ?

Password\* ?

IP Address\* ?

Port\* ?

+ Add IP Address

GSLB Subdomain ?

+ Add GSLB Subdomain

Save

Save and Set DNS Virtual Services

- 3 在高级设置下面，您可以配置客户端组 IP 地址类型和运行状况监控器代理。有关更多详细信息，请参阅 [NAT 感知公用-专用 GSLB 配置](#)和[使用 NSX Advanced Load Balancer UI 配置 GSLB 运行状况监控器](#)。

要配置地理位置源，请填写相关字段 - 名称、标记、纬度和经度。纬度和经度表示为度.分。纬度范围是 -90.0（南）到 +90.0（北），经度范围是 -180.0（西）到 +180.0（东）。输入的值精度限制为 4 位十进制数字。

## Edit GSLB Site

### Advanced Settings

Client Group IP Address Type ?  
Public  
+ Add Group IP Address

Health Monitor Proxy ?  
+ Health Monitor Proxy

Geo Location Source ?  
User Configured

Name ?  
user\_geo\_location

Tag ?  
geo\_tag

Latitude ?  
77.1234

Longitude ?  
77.1234

Save

Save and Set DNS Virtual Services

在成功配置后，“类型”字段将标记为“所有者(当前)”，表明这是主站点。

单击**保存并设置 DNS 虚拟服务**。对于没有 DNS 虚拟服务的被动站点，单击**保存**以保存站点配置。

← Edit GSLB Site

DNS Virtual Service

g-dns

+

Add DNS VS

Subdomains

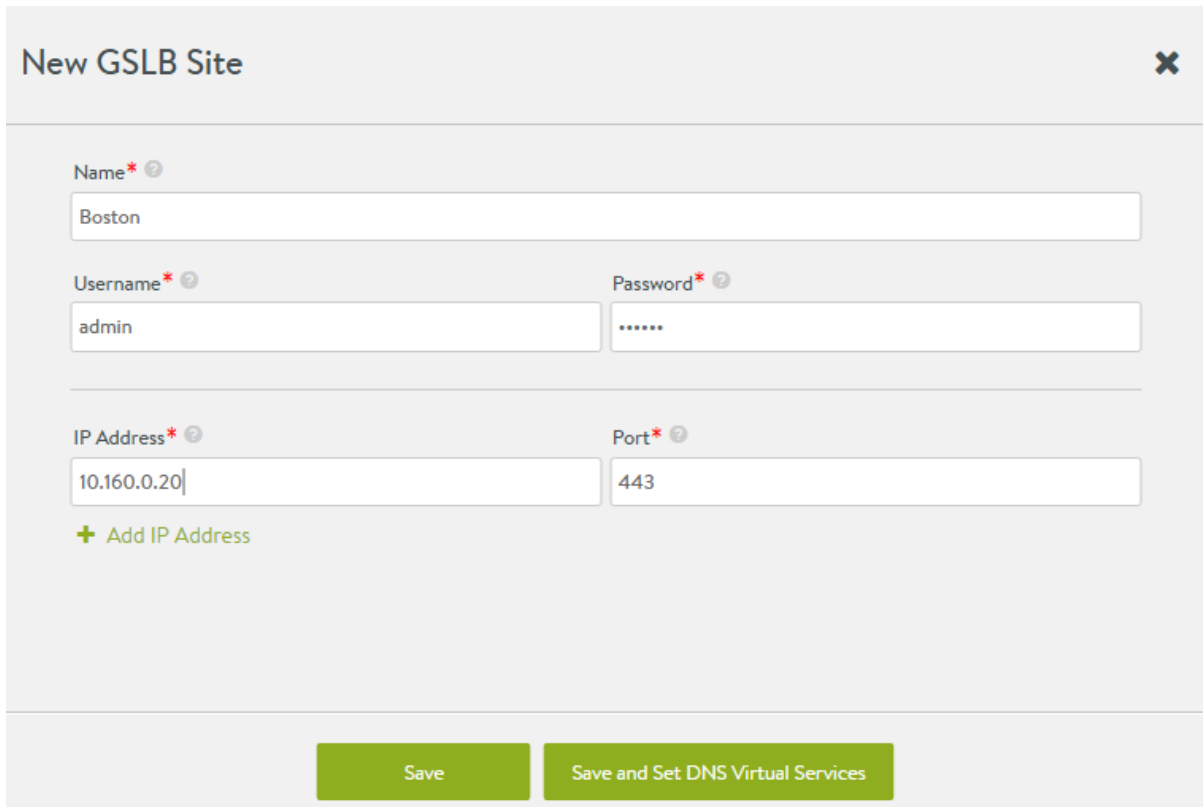
All subdomains

✕

☐ Health Monitor Sharding

Save

- 4 单击**添加新的站点**以添加第二个站点。将显示**新的 GSLB 站点**屏幕。输入详细信息，如下所示：



**New GSLB Site** ✕

Name\* ?  
Boston

Username\* ? Password\* ?  
admin .....

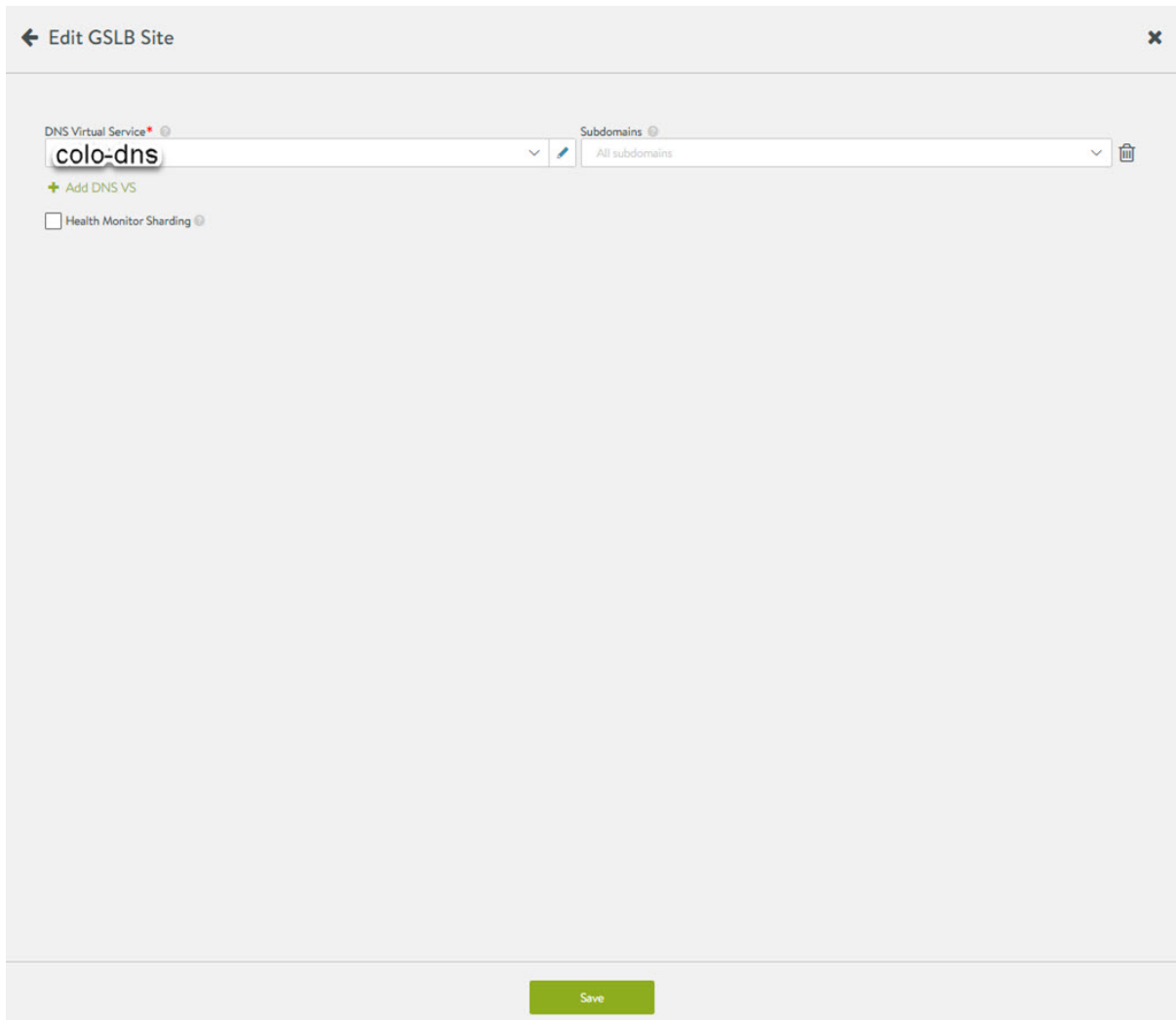
IP Address\* ? Port\* ?  
10.160.0.20 443

+ Add IP Address

Save Save and Set DNS Virtual Services

要指示站点是主动站点，请确保选中**主动成员**复选框。

对于具有 DNS 虚拟服务的主动站点，请单击**保存并设置 DNS 虚拟服务**。对于没有 DNS 虚拟服务的被动站点，单击**保存**以保存站点配置。



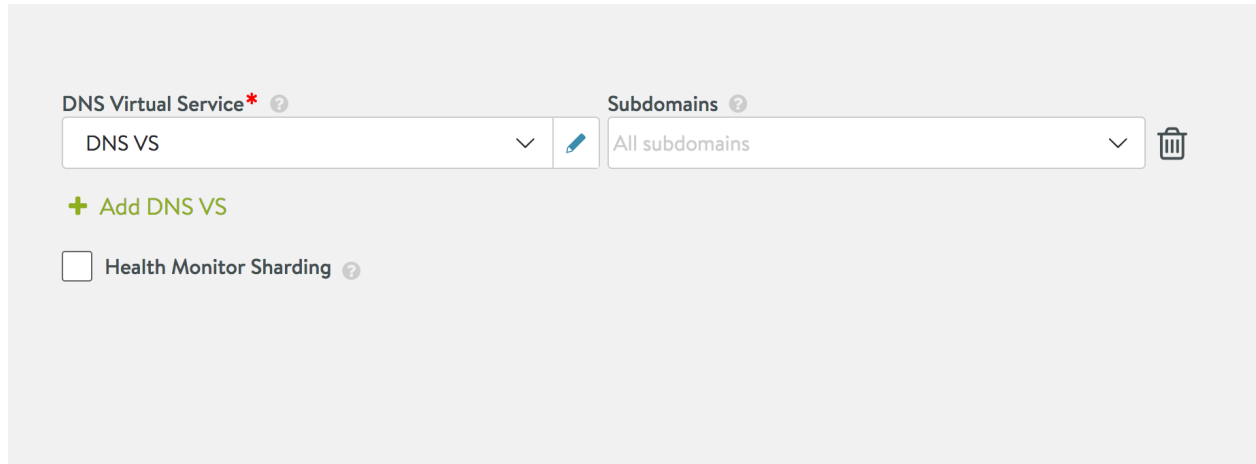
此时，两个站点相互通信，并启用了配置同步。

## 将多个子域与 DNS 虚拟服务相关联

为现有 DNS 虚拟服务配置一个额外的域。

将子域字段设置为所有子域，如下所示：





DNS Virtual Service\* ?

DNS VS

Subdomains ?

All subdomains

+ Add DNS VS

☐ Health Monitor Sharding ?

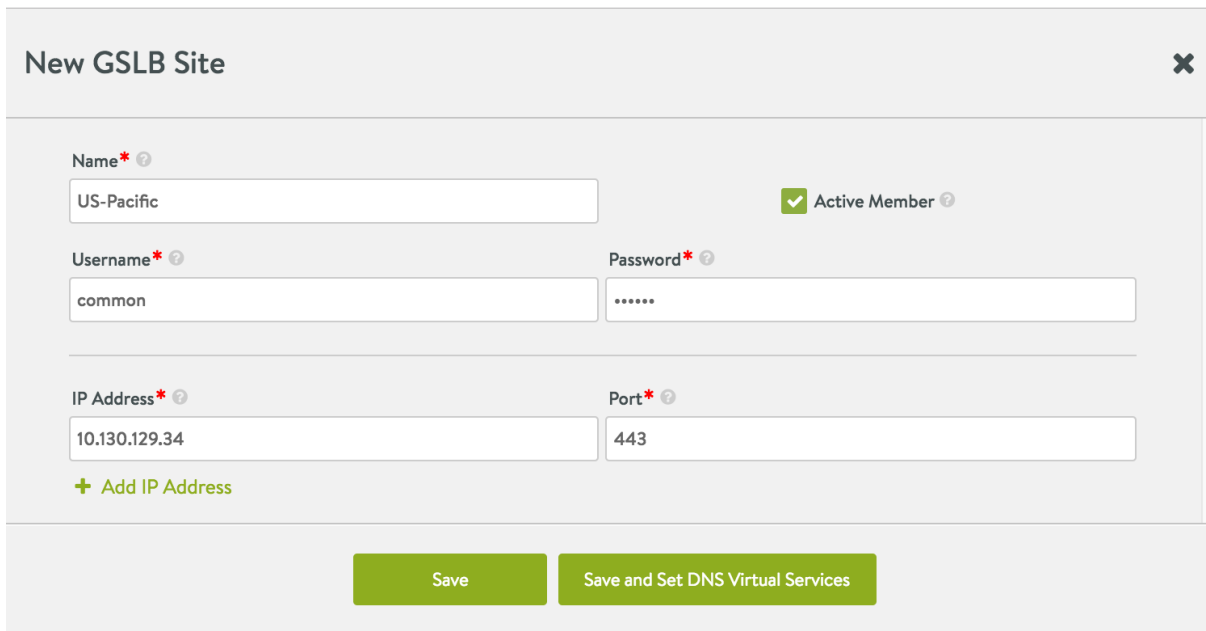
## GSLB 的 DNS 配置

对于 GSLB 配置，DNS 不是由 DNS 虚拟服务定义的，而是配置为 GSLB 站点对象。

要为 GSLB 配置 DNS，请执行以下操作：

### 步骤

- 1 导航到**基础架构 > GSLB**。
- 2 单击**站点配置**选项卡中的**添加新的站点**按钮。
- 3 在编辑器中输入所有字段的相关信息。启用**主动成员**选项的复选框，然后单击**保存并设置 DNS 虚拟服务**。



New GSLB Site

Name\* ?

US-Pacific

Active Member ?

Username\* ?

common

Password\* ?

.....

IP Address\* ?

10.130.129.34

Port\* ?

443

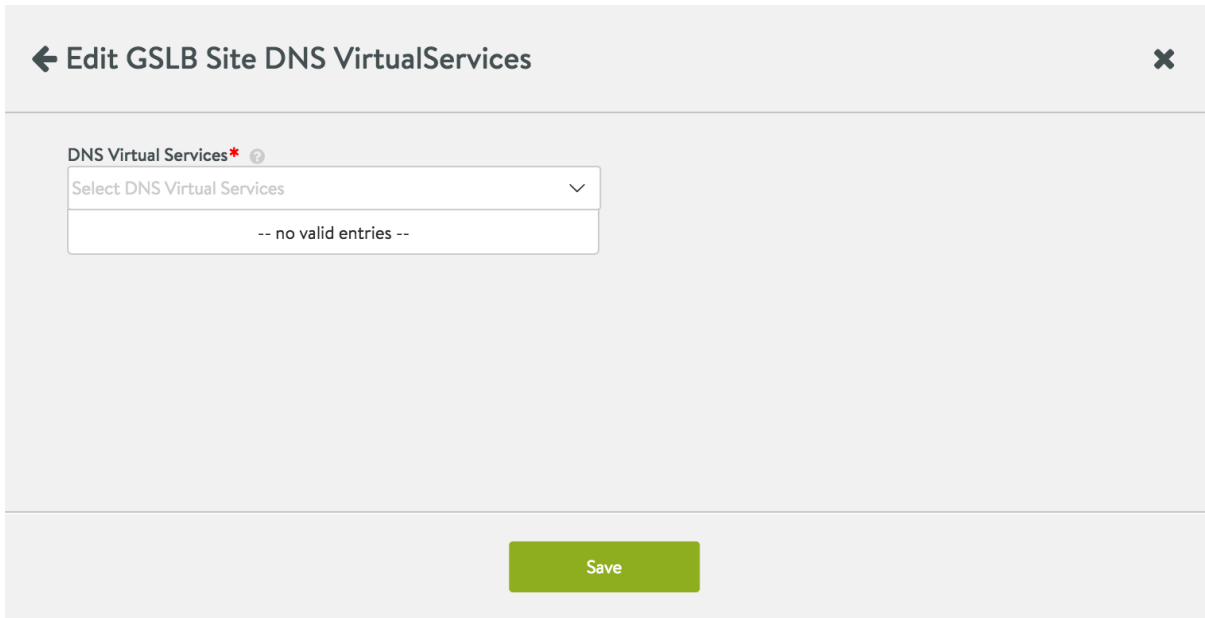
+ Add IP Address

Save

Save and Set DNS Virtual Services

- 4 从下拉列表上的一个或多个 DNS 虚拟服务中进行选择，然后单击**保存**，以便为该服务启用 GSLB 配置。

以下屏幕截图显示没有可供选择的 DNS 虚拟服务的情况。主动 GSLB 站点不需要使用 DNS，但最好配置 DNS，如下一节中所述。



← Edit GSLB Site DNS VirtualServices ×

DNS Virtual Services\* ?

Select DNS Virtual Services ▼

-- no valid entries --

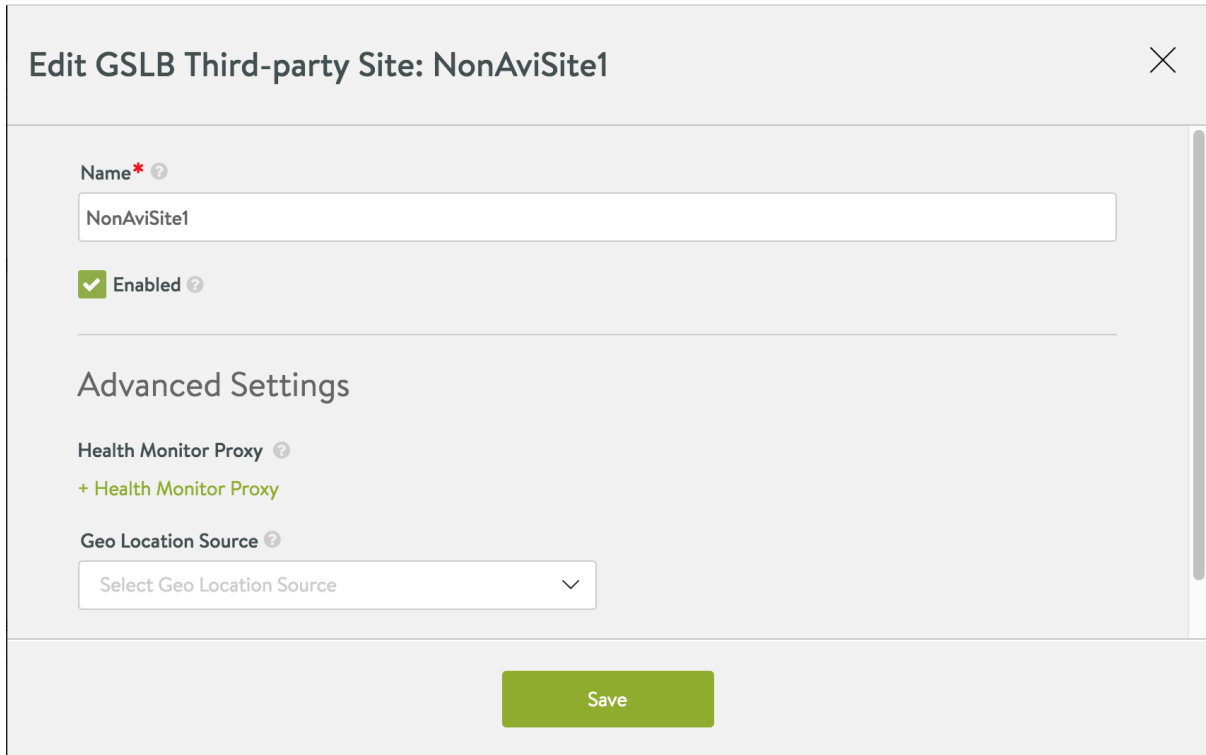
Save

## 添加第三方站点

本节重点介绍了如何配置和运行第三方 GSLB 站点。

### 定义 GSLB 站点

- 1 在授权的管理员首次导航到**基础架构 > GSLB** 时，唯一可见的子选项卡是“站点配置”，这表示默认禁用了 GSLB。在单击**铅笔**图标并提供配置名称后，将显示额外的选项卡和按钮。
- 2 通过使用右上角的绿色按钮，可以定义 NSX Advanced Load Balancer 站点和非 NSX Advanced Load Balancer（第三方）站点。用于创建第三方站点的编辑器如下所示：



- 3 在创建一个 NSX Advanced Load Balancer 站点（默认情况下，第一个 NSX Advanced Load Balancer 站点成为 GSLB 主站点）和一个第三方站点后，我们将会看到双站点配置。
- 4 NSX Advanced Load Balancer 站点可能是主动站点或被动站点，上面所示的站点配置显示具有此类特征的站点。不过，第三方站点无法成为主动站点或被动站点；此类站点始终显示在自己的部分中。  
有关更多详细信息，请参阅[将第三方服务与第三方站点相关联](#)。

### 用例：禁用第三方站点

要禁用 NonAviSite1 中运行的每个第三方成员服务，请单击该站点的行右端的**铅笔**图标。在“编辑 GSLB 第三方站点”中，取消选中**已启用**选项并单击**保存**。

“站点配置”屏幕的“第三方站点”部分将确认该更改。

## 使用 NSX Advanced Load Balancer CLI 配置 GSLB 站点

本节重点介绍了如何使用 NSX Advanced Load Balancer CLI 配置 GSLB 站点。

### 指定 GSLB 主站点并创建全局配置

创建以下 GSLB 全局配置：

示例：两个控制器集群（10.10.25.10 和 10.160.0.25）

将 10.10.25.10 指定为 GSLB 主集群。因此，在 GSLB 主集群上创建配置。

找到两个控制器集群的集群 UUID。

在 10.10.25.10 上：

```
: > show cluster

+-----+-----+
| Field      | Value                                     |
+-----+-----+
| uuid       | cluster-42301dd3-0529-ada4-ec02-69a2c593df6d |
: > configure gslb glb
: gslb> dns_configs
New object being created

: gslb:dns_configs> domain_name avi.com
```

```

: gslb:dns_configs>
: gslb> site_controller_clusters
New object being created

: gslb:site_controller_clusters> ip_addresses 10.10.25.10
: gslb:site_controller_clusters> cluster_uuid cluster-42301dd3-0529-ada4-ec02-69a2c593df6d
: gslb:site_controller_clusters> username admin
: gslb:site_controller_clusters> password admin
: gslb:site_controller_clusters> name SantaClara
: gslb:site_controller_cluster> save
: gslb> site_controller_clusters
New object being created

: gslb:site_controller_clusters> ip_addresses 10.160.0.20
: gslb:site_controller_clusters> cluster_uuid cluster-42215c91-6280-6016-31f6-7416a1f4c4ad
: gslb:site_controller_clusters> username admin
: gslb:site_controller_clusters> password admin
: gslb:site_controller_clusters> name Boston
: gslb:site_controller_clusters> save
: gslb> save
+-----+-----+
| Field | Value |
+-----+-----+
| uuid | gslb-cafe8f98-c411-47cd-96d2-1a6d4e3bad74 |
| name | glb |
| dns_configs[1] | |
| domain_name | avi.com |
| site_controller_clusters[1] | |
| cluster_ref | cluster-42301dd3-0529-ada4-ec02-69a2c593df6d |
| name | SantaClara |
| ip_addresses[1] | 10.10.25.10 |
| port | 443 |
| username | admin |
| site_controller_clusters[2] | |
| cluster_ref | cluster-42215c91-6280-6016-31f6-7416a1f4c4ad |
| name | Boston |
| ip_addresses[1] | 10.160.0.20 |
| port | 443 |
| username | admin |
| owner_controller_cluster_ref | cluster-42301dd3-0529-ada4-ec02-69a2c593df6d |
| tenant_ref | admin |
+-----+-----+
: >

```

现在，已设置同步。

要验证配置，请执行以下操作：

转到辅助站点，然后尝试执行 **show** 命令。GSLB 主和从属站点 UUID 将匹配。

```

: > show gslb
+-----+-----+
| Name | UUID |
+-----+-----+

```

```
| glb | gslb-cafe8f98-c411-47cd-96d2-1a6d4e3bad74 |
+-----+-----+
```

## 配置本地 DNS 虚拟服务

在两个控制器集群上配置新的 SE 组以托管 DNS 虚拟服务（称为 g-dns SE 组）。

在所有托管 DNS 服务的集群上配置一个 DNS 虚拟服务，并将其绑定到 g-dns SE 组：

- 配置由 DNS 虚拟服务托管的域名（可选）

从 CLI 中，创建一个应用程序配置文件以选择该虚拟服务（在所有控制器集群上）托管的域名。

```
: > configure applicationprofile dns
: applicationprofile> type application_profile_type_dns
: applicationprofile> dns_service_profile
: applicationprofile:dns_service_profile> domain_names avi.com
: applicationprofile:dns_service_profile> save
: applicationprofile> save
```

从 UI 或 CLI 中，创建一个应用程序配置文件以选择该虚拟服务托管的域名。

## 配置本地应用程序虚拟服务

正常创建应用程序虚拟服务。例如，在控制器集群 1 中创建 HTTP 虚拟服务 vs-1，在控制器集群 2 中创建虚拟服务 vs-2。

有关更多详细信息，请参阅[配置虚拟服务](#)。

## 为 DNS 虚拟服务配置路由以访问本地虚拟服务

DNS SE 监控 GSLB 服务成员的运行状况。添加静态路由（或默认网关）以确保可以访问这些成员。

例如，在 10.10.25.10 (Santa Clara) 上：

```
For example, on 10.10.25.10 (Santa Clara):: > configure vrfcontext global
Updating an existing object. Currently, the object is:
```

```
+-----+-----+
| Field          | Value                                     |
+-----+-----+
| uuid           | vrfcontext-fde3b826-b19c-449c-8dec-ddeb119f2498 |
| name           | global                                   |
| system_default | True                                     |
| tenant_ref     | admin                                    |
| cloud_ref      | Default-Cloud                           |
+-----+-----+
: vrfcontext> static_routes
: vrfcontext:static_routes> prefix 10.0.0.0/8 next_hop 10.90.12.1
: vrfcontext:static_routes> save
: vrfcontext> save

+-----+-----+
| Field          | Value                                     |
+-----+-----+
```

```

+-----+-----+
| uuid          | vrfcontext-fde3b826-b19c-449c-8dec-ddeb119f2498 |
| name          | global                                           |
| static_routes[1] |
|   prefix      | 10.0.0.0/8                                       |
|   next_hop    | 10.90.12.1                                       |
|   route_id    | 1                                                 |
| system_default | True                                             |
| tenant_ref    | admin                                            |
| cloud_ref     | Default-Cloud                                    |
+-----+-----+
: >

```

## 使用 NSX Advanced Load Balancer CLI 配置直通服务器

本节介绍了使用 NSX Advanced Load Balancer CLI 配置直通服务器的步骤。

如果在 DNS 虚拟服务上缺少 FQDN，NSX Advanced Load Balancer 可以将该请求通过负载均衡器传递到一个或多个后端 DNS 服务器。要启用该功能，请配置一个包含这些服务器的池，并将其连接到 DNS 虚拟服务。

如果在虚拟服务的应用程序筛选器中配置了域筛选器，则仅为位于该子域中的 FQDN 执行传递。将丢弃所有其他查询。

不支持的查询也会转发到直通服务器。

### ■ 配置由 DNS 虚拟服务托管的域名（可选）

从 CLI 中，创建一个应用程序配置文件以选择该虚拟服务（在所有控制器集群上）托管的域名。

```

: > configure applicationprofile dns
: applicationprofile> type application_profile_type_dns
: applicationprofile> dns_service_profile
: applicationprofile:dns_service_profile> domain_names avi.com
: applicationprofile:dns_service_profile> save
: applicationprofile> save

```

从 UI 或 CLI 中，创建一个应用程序配置文件以选择该虚拟服务托管的域名。

## GSLB 的 DNS

本节介绍了为 GSLB 配置 DNS 的步骤。

### 自定义 DNS 应用程序配置文件

（可选）创建一个自定义 DNS 配置文件以在定义 DNS 虚拟服务时引用。

有关更多详细信息，请参阅“应用程序配置文件”主题的 [DNS 配置文件](#) 一节。

## DNS 虚拟服务

在 NSX Advanced Load Balancer 中，可以为 DNS 虚拟服务配置 IPv4 VIP、IPv6 VIP 或双 VIP。

导航到**应用程序 > 虚拟服务**，然后单击**创建虚拟服务**（高级设置）。

在以下几节中介绍了与 DNS 关联的配置选项卡。

## 设置

- 1 在**配置文件**部分下面，从**应用程序配置文件**的下拉列表中选择默认或自定义 DNS 配置文件。
- 2 在**TCP/UDP 配置文件**下面，为网络设置选择一个合适的配置文件，例如 System-UDP-Per-Pkt。
- 3 在**服务端口**部分下面，为**服务**字段输入 53。

在**池**部分下面，从下拉列表中选择一个相关的 IPv4、IPv6 或 IPv4 + IPv6 池，或单击**创建池**以配置新的池。导航到**服务器**选项卡以输入 IPv4、IPv6 或 IPv4v6 成员信息。

Status	Server Name	IP Address	Port	Ratio	Network	Header Value	Rewrite Host Header
<input type="checkbox"/> Enabled	IPv4 Server	10.2.2.2	Inherit	1		Header Value	<input type="checkbox"/>
<input type="checkbox"/> Enabled	IPv6 Server	fd00:0:0:116::100	Inherit	1		Header Value	<input type="checkbox"/>



## NSX Advanced Load Balancer 托管的虚拟服务的 DNS

NSX Advanced Load Balancer 上托管的 DNS 虚拟服务将托管的虚拟服务的 FQDN 转换为 IP 地址。

要为 NSX Advanced Load Balancer 托管的虚拟服务配置 DNS，请执行以下操作：

### 步骤

- 1 导航到**管理 > 设置**。
- 2 选择 **DNS 服务**。
- 3 在 **DNS 虚拟服务** 部分下面，单击下拉列表以选择预定义的 DNS 虚拟服务或创建一个虚拟服务。

### 后续步骤

有关 DNS 虚拟服务的配置步骤的更多详细信息，请参阅[在托管 DNS 的所有主动站点上配置本地 DNS 虚拟服务](#)。

## 将 GSLB 服务选择性分配给 DNS 虚拟服务

本节介绍了使用 NSX Advanced Load Balancer UI 配置将 GSLB 服务选择性分配给 DNS 虚拟服务的配置步骤。

### NSX Advanced Load Balancer UI 配置

导航到**基础架构 > GSLB > 站点配置**以查看和/或更改与将 GSLB 服务选择性分配给 DNS 虚拟服务相关的设置。

图 3-1. 定义 GSLB 子域

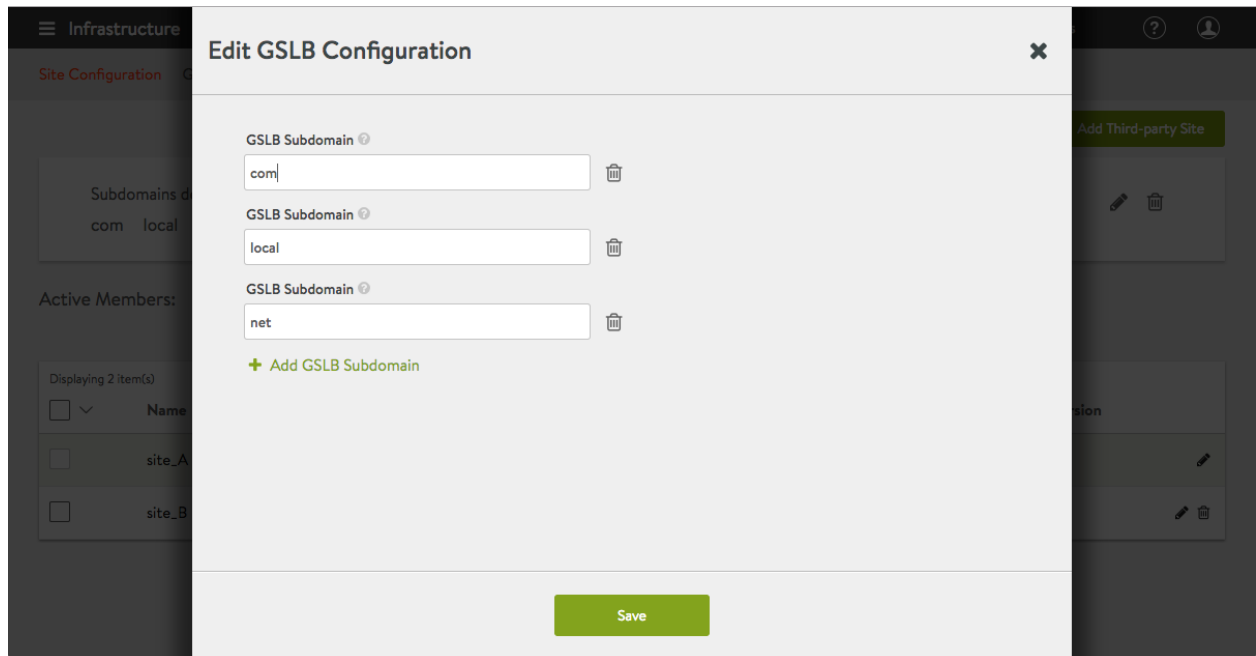


图 3-2. 编辑 GSLB site\_A

## Edit GSLB Site ✕

Name\* ?

site\_B|

☒ Active Member ?

Username\* ?

gslbadmin

Password ?

.....

IP Address\* ?

10.10.24.111

Port\* ?

443

+ Add IP Address

### Advanced Settings

Client Group IP Address Type ?

Client Group IP Address Type

▼

Health Monitor Proxy ?

+ Health Monitor Proxy

+ Add Group IP Address

Geo Location Source ?

Select Geo Location Source

▼

Save

Save and Set DNS Virtual Services

图 3-3. 将子域分配给 DNS 虚拟服务

← Edit GSLB Site DNS VirtualServices

DNS Virtual Service\* ? Subdomains ?

dns-1@site\_A com

DNS Virtual Service\* ? Subdomains ?

dns-2@site\_A local

+ Add DNS VS

Save

图 3-4. 将子域分配给站点 B 的 DNS 虚拟服务

← Edit GSLB Site DNS VirtualServices

DNS Virtual Service\* ? Subdomains ?

dns-1@site\_B com

DNS Virtual Service\* ? Subdomains ?

dns-2@site\_B net

+ Add DNS VS

Save

## 使用 NSX Advanced Load Balancer CLI 配置将 GSLB 服务选择性分配给 DNS 虚拟服务

要使用 NSX Advanced Load Balancer CLI 配置为 DNS 虚拟服务配置选择性 GSLB 服务分配，请执行以下操作：

### 步骤

- 1 通过使用具有管理特权的 ID，登录到 GSLB 主站点控制器的 NSX Advanced Load Balancer Shell。

## 2 调用 `configure gslb` 命令，并指定配置的名称。

例如: `configure gslb Default`

## 3 在响应 `gslb` 提示时，在两个选项卡中输入内容将显示可供您使用的子命令：

```
[admin:topol-controller]: gslb>
cancel                Exit the current submode without
saving

clear_on_max_retries  Max retries after which the remote site is treated as a fresh
start. In fresh start all the configs are downloaded.
client_ip_addr_group  (submode)
description           Help string not found for
argument

dns_configs           (submode)
do                   Execute a show command
is_federated          This field indicates that this object is replicated across GSLB
federation.
leader_cluster_uuid   Mark this Site as leader of GSLB configuration. This site is the
one among the Avi sites.
maintenance_mode      This field disables the configuration operations on the leader for
all federated objects. CUD operations on Gslb, GslbService, GslbGeoDbProfile and other
federated objects will be rejected. The rest-api disabling helps in upgrade scenarios
where we don't want configuration sync operations to the Gslb member when the member is
being u...
name                 Name for the GSLB object.
new                  (Editor Mode) Create new object in editor
mode
no                   Remove field
save                 Save and exit the current
submode

send_interval         Frequency with which group members
communicate.

show_schema           show object schema
sites                (submode)
tenant_ref           Help string not found for
argument

third_party_sites     (submode)
view_id              The view-id is used in change-leader mode to differentiate
partitioned groups while they have the same GSLB namespace. Each partitioned group will be
able to operate independently by using the view-id.
watch                Watch a given show command
where                Display the in-progress object
```

#### 4 调用了三次 sites 子命令，每个要分配的 DNS 调用一次：

将 DNS vs-1 分配给子域 com

```
si[admin:naveen-ctrl]: gslb> sites index 1
[admin:naveen-ctrl]: gslb:sites> dns_vses index 1
[admin:naveen-ctrl]: gslb:sites:dns_vses> domain_names com
[admin:naveen-ctrl]: gslb:sites:dns_vses> save
```

将 DNS vs-2 分配给子域 edu

```
[admin:naveen-ctrl]: gslb:sites> dns_vses index 2
[admin:naveen-ctrl]: gslb:sites:dns_vses> domain_names edu
[admin:naveen-ctrl]: gslb:sites:dns_vses> save
[admin:naveen-ctrl]: gslb:sites> save
[admin:naveen-ctrl]: gslb> save
```

将 DNS vs-3 分配给子域 net

```
[admin:naveen-ctrl]: gslb:sites> dns_vses index 3
[admin:naveen-ctrl]: gslb:sites:dns_vses> domain_names net
[admin:naveen-ctrl]: gslb:sites:dns_vses> save
[admin:naveen-ctrl]: gslb:sites> save
[admin:naveen-ctrl]: gslb> save
```

#### 5 保存配置：

GSLB 将保存该站点。

Field	Value
uuid	gslb-10c15641-2cc9-4fc3-b8ae-30651d3a31d9
name	Default
dns_configs[1]	
domain_name	avi.com
dns_configs[2]	
domain_name	vmware.com
sites[1]	
cluster_uuid	cluster-37cabcaa-c2c8-4a9e-9bcc-2849cf29ad81
name	glb-12
ip_addresses[1]	10.102.64.51
port	443
username	admin
password	<sensitive>
member_type	GSLB_ACTIVE_MEMBER
enabled	True
dns_vses[1]	
dns_vs_uuid	virtualservice-3ff9baea-556a-46e5-a086-090fd681b6e6
domain_names[1]	avi.com
dns_vses[2]	
dns_vs_uuid	virtualservice-7ef9efc8-4b95-43f4-b670-62979bb1f0e0
domain_names[1]	vmware.com
hm_shard_enabled	False

```

|   suspend_mode           | False |
| leader_cluster_uuid      | cluster-37cabcaa-c2c8-4a9e-9bcc-2849cf29ad81 |
| send_interval            | 15 sec |
| clear_on_max_retries     | 20 |
| view_id                  | 0 |
| async_interval           | 0 sec |
| error_resync_interval    | 300 sec |
| replication_policy        | |
|   replication_mode       | REPLICATION_MODE_CONTINUOUS |
| maintenance_mode        | False |
| is_federated             | True |
| tenant_ref               | admin |
| tenant_scoped            | True |
| enable_config_by_members | False |
+-----+-----+
[admin:naveen-ctrl]: >

```

## GSLB 服务配置

本节重点介绍了 GSLB 服务配置的各种方法和可用选项。

在单个 NSX Advanced Load Balancer GSLB 配置中，一组在多个站点中运行的相同服务可以组成一个 GSLB 服务。

## 必备条件

需要由具有写入访问权限的用户配置 GSLB 服务，如 Tenant-Admin 角色的 GSLB 部分中所示。

Roles	Application	Profiles	Group & Script	Security	Policy	WAF	Error Page	Operations	Infrastructure	Administration	Accounts	GSLB
Application-Admin	Write	Assorted	Write	Assorted	Write	Read	Write	Assorted	Assorted	Assorted	No Access	Assorted
Application-Operator	Read	Read	Read	Read	Read	Read	Read	Assorted	Read	Assorted	No Access	Read
Demo-AppOwner	Assorted	Assorted	Write	Write	No Access	Write	No Access	Assorted	No Access	No Access	No Access	No Access
foo-bar	No Access	No Access	No Access	No Access	No Access	No Access	No Access	No Access	No Access	No Access	No Access	No Access
ReadOnly	No Access	No Access	No Access	No Access	No Access	No Access	No Access	Assorted	Assorted	Assorted	No Access	Assorted
Security-Admin	No Access	Assorted	No Access	Assorted	No Access	Read	Read	No Access	No Access	Assorted	No Access	No Access
System-Admin	Write	Write	Write	Write	Write	Write	Write	Write	Write	Assorted	Write	Write
Tenant-Admin	Write	Write	Write	Write	Write	Write	Write	Write	Write	Assorted	No Access	Assorted

## 使用 NSX Advanced Load Balancer UI 配置 GSLB 服务基本设置

本节介绍了使用 NSX Advanced Load Balancer UI 配置 GSLB 服务基本设置的步骤。

要使用 NSX Advanced Load Balancer UI 配置 GSLB 服务基本设置，请执行以下操作：

### 步骤

1 导航到应用程序 > GSLB 服务。

- 2 单击**创建**选项，然后选择**基本设置**选项。

### New GSLB Service

Name\*

Application Name\*

Subdomain\*

.igslb.avi.local

+ Add Domain Name

Health Monitor

Health Monitor Scope

Only Non Avi Members

All Members

Controller Health Status

Groups Load Balancing Algorithm

Priority-based

Minimum number of Servers

0

Site Persistence

Application Persistence Profile

#### Pool

Select Group Type

Active Active

Active Standby

Pool Members Load Balancing Algorithm\*

Round Robin

#### Pool Member

IP Address

Virtual Service

Site Cluster Controller\*

Select Site

Public IP Address

Description

Add GSLB Pool Member

Save

是上面显示的选项进行操作。

## Pool Member

☒ IP Address ☐ Virtual Service

IP Address or FQDN \* ?

Third-party Site Cluster Controller ?  

Select Site

Public IP Address ?

Description



### 3 创建一个 GSLB 基本服务。

- a 导航到**应用程序 > GSLB 服务 > 创建 > 基本设置 > 添加服务**。

活动/活动模式的“新建 GSLB 服务”屏幕如下所示：

## New GSLB Service ✕

Name\* ?

Application Name\* ?

Subdomain\*  

.subd

+ Add Domain Name

Health Monitor ?

Health Monitor Scope ?  

Only Non Avi Members

All Members

Controller Health Status ?

Select Group Type  

Active Active

Active Standby

Groups Load Balancing Algorithm ?  

Priority-based

☐ Site Persistence ?

Application Persistence Profile ?

Minimum number of Servers ?  

0

### Pool

Pool Members Load Balancing Algorithm\* ?  

Geo

Pool Members Fallback Load Balancing Algorithm ?  

Round Robin

### Pool Member

IP Address

Virtual Service

Site Cluster Controller\* ?

Save

使用可用的下拉列表选项为池成员选择负载均衡算法和回退负载均衡算法。

VMware, Inc.

98

请注意，“池成员负载均衡算法”设置为“地理”。

- 在使用 NSX Advanced Load Balancer UI 中的**基本**选项创建 GSLB 服务时，现在可以使用回退算法选项。
- 为“组负载均衡算法”下拉列表提供了选择组类型的选项。只有在选择了**活动-活动**模式时，才能使用“组负载均衡算法”下拉列表。
- 在选择“地理”以作为池成员的负载均衡算法时，可以使用**池成员后退负载均衡算法**下拉列表。

#### 4 下表介绍了 GSLB 服务的各种配置实体：

名称	这是对 NSX Advanced Load Balancer 上托管的全局应用程序的引用。
应用程序名称	该字段与“子域”连接在一起以组成应用程序的 FQDN。
子域	<p>该下拉菜单预填充了与 GSLB 配置关联的子域。导航到<b>基础架构 &gt; GSLB &gt; 站点配置</b>以在集合中添加或减少一些子域。</p> <hr/> <p><b>注</b></p> <ul style="list-style-type: none"> <li>■ 首次输入时，子域应采取以下形式 <code>alpha.beta.com</code>。当它出现在下拉菜单时，NSX Advanced Load Balancer 自动在它前面添加一个点。</li> <li>■ 为了支持别名，GSLB 服务可能将一个或多个 FQDN 与之关联。例如，<code>www.foo.com</code> 和 <code>www.foo.us</code> 可能指向同一个 GSLB 服务。别名避免了必须创建多个相同的 GSLB 服务。</li> </ul>
运行状况监控器	<p>如果 DNS SE 生成综合流量以将服务标记为启动或关闭，则该字段确定要使用哪个监控器。</p> <p>可以使用<b>创建</b>选项以创建自定义监控器。或者，导航到<b>模板 &gt; 配置文件 &gt; 运行状况监控器</b>以定义要用于全局应用程序的自定义监控器。</p>
运行状况监控器范围	默认情况下，运行状况监控器将评估所有 GSLB 池成员（NSX Advanced Load Balancer 虚拟服务或外部（第三方）VIP）的运行状况。如果 NSX Advanced Load Balancer 成员的数据路径监控对于控制路径运行状况监控来说是重复的，请选择“仅非 NSX Advanced Load Balancer 成员”。
控制器运行状况	默认设置为从 NSX Advanced Load Balancer 成员服务的本地 NSX Advanced Load Balancer 控制器收集虚拟服务运行状况以评估其运行状况。该选项与外部 VIP 无关，只能通过数据路径运行状况检查来评估这些 VIP 的运行状况。
组负载均衡算法	负载均衡算法在 GSLB 服务的可用池列表选择一个 GSLB 池。选择两种算法之一：基于优先级的算法或基于地理位置的算法。

最少服务器数	<p>将流量分配到的最小成员数。如果不为 0，则该值的范围是 1 到 65535。0 是一种禁用限制的特殊情况。min_members 类似于池组的 min_servers。</p> <p>请考虑以下设置：</p> <ul style="list-style-type: none"> <li>■ 两个 GSLB 池 <ul style="list-style-type: none"> <li>■ 优先级为 10 的 P1（4 个成员）</li> <li>■ 优先级为 5 的 P2（3 个成员）</li> </ul> </li> <li>■ min_members 值设置为 3</li> </ul> <p>只要 P1 至少启动了 3 个成员，就会仅选择 P1。如果 P1 中处于启动状态的服务器数降到 3 个以下，则同等选择 P1 和 P2。</p>
站点持久性	<p>可以选中该框，以便为 GSLB 服务启用站点持久性。有关更多详细信息，请参阅 <a href="#">GSLB 站点 Cookie 持久性</a>。</p>
应用程序持久性配置文件	<p>单击 <b>创建</b> 以启动一个编辑器，以便创建新的 <b>站点 Cookie 应用程序持久性配置文件</b>。</p>  <p>应用程序持久性配置文件与 GSLB 站点 Cookie 持久性一起使用。</p>
选择组类型	<p>选择池的行为。如果选择默认的“活动-活动”，则可以选择 4 种负载均衡算法之一。</p>
池成员负载均衡算法	<p>对于活动-活动池配置，选择一种负载均衡算法，以便在 GSLB 服务的可用成员列表中选择一个本地成员。</p> <p>选项如下所示：</p> <ul style="list-style-type: none"> <li>■ 循环（默认）</li> <li>■ 一致哈希</li> <li>■ 地理</li> <li>■ 拓扑</li> </ul>
IP 地址/虚拟服务	<p>接受“虚拟服务”（默认）以指定本机 NSX Advanced Load Balancer 虚拟服务。如果选择了“IP 地址”，则会显示一组不同的选项。在该列表后面的步骤列表中介绍了这些选项。</p> <p>选择“IP 地址”以指定外部（第三方）GSLB 池成员。请参阅相关的 <a href="#">NSX Advanced Load Balancer AWS 多区域、多可用区部署中的 GSLB</a> 和 <a href="#">配置和运行第三方站点</a> 文章。</p> <p><b>注</b> 对于第三方成员，第三方控制器是可选的，而无论是否冗余配置了该控制器。如果您选择了 <b>IP 地址</b> 选项，请跳过以下步骤。</p>

站点集群控制器	要指定本机 NSX Advanced Load Balancer 虚拟服务，需要先通过该字段选择其控制器。必须预配置控制器，才会在下拉列表中显示其名称。
虚拟服务	在选择站点集群控制器后，才会显示该字段。从下拉列表中选择预配置的虚拟服务。
公用 IP 地址	这是池成员的备用 IP 地址。在通常的部署中，第三方服务的 VIP 是一个专用 IP 地址；它是在 GSLB 服务的 IP 字段中配置的。在该字段中，您可以指定 VIP 的公用 IP 地址；防火墙将其转换为专用 IP。来自 Intranet 内部的客户端 DNS 请求应在 A 记录中提供专用 IP，而来自外部的请求应提供公用 IP 地址。
描述	如果需要，请添加注释。
添加 GSLB 池成员	在为 GSLB 池定义第一个（最低要求）成员服务后，单击该超链接以创建额外的服务。
IP 地址或 FQDN	外部池成员配置了完全限定的域名，控制器将其解析为一个 IP 地址。DNS 服务运行状况监控解析的地址。 有关更多详细信息，请参阅在 <a href="#">NSX Advanced Load Balancer DNS 虚拟服务中添加自定义 A 记录</a> 。
第三方站点集群控制器	从下拉列表中，选择与第三方 VIP 关联的第三方站点名称。

## 使用 NSX Advanced Load Balancer CLI 配置 GSLB 服务基本设置

本节介绍了使用 NSX Advanced Load Balancer CLI 配置 GSLB 服务基本设置的步骤。

在 10.160.0.20 (Boston) 上:

```
: > configure gslbservice view
: gslbservice> domain_names view.avi.com
: gslbservice> health_monitor_refs global-http-hm
: gslbservice> num_dns_ip 1
: gslbservice> groups
New object being created

: gslbservice:groups> algorithm gslb_algorithm_round_robin
: gslbservice:groups> name active-sc
: gslbservice:groups> priority 10
: gslbservice:groups> members
New object being created

: gslbservice:groups:members> ip 10.90.12.100
: gslbservice:groups:members> save
: gslbservice:groups> save
: gslbservice> groups
: gslbservice:groups:members> ip 10.160.110.200
: gslbservice:groups:members> save
: gslbservice:groups> save
: gslbservice> save
```

```
+-----+-----+-----+-----+-----+-----+
| Field                                | Value                                |
+-----+-----+-----+-----+-----+-----+
```



## 2 单击**创建**，然后选择**高级设置**选项。

**New GSLB Service**

Name\*

Application Name\* Subdomain\*   
Add Domain Name

Health Monitor

Health Monitor Scope   
☒ All Members ☐ Only Non Avi Members ☒ Controller Health Status

Groups Load Balancing Algorithm   
Priority-based

☐ Site Persistence   
Minimum number of Servers   
0

GSLB pool\* Add Pool

Number of IPs returned by DNS server TTL served by DNS Service   
Default from DNS Service Default from DNS Service Sec

Down Response   
No Response ☐ Resolve CNAME

Save


请注意，基本设置编辑器的**池成员**部分已替换为**GSLB 池**部分，如下所示。

### 3 单击 **编辑** 图标以打开 **GSLB 池** 编辑器。

## GSLB pool \*

Add Pool >

Displaying 1 item(s)

Name ↕	Priority ? ▾	Algorithm	Description
	10	Round Robin	

Number of IPs returned by DNS server ?

Default from DNS Service

TTL served by DNS Service ?

Default from DNS Service

Sec

Down Response ?

No Response ▾

在**基本设置**编辑器中未提供这些额外的选项。

有关高级设置中提供的额外配置选项，请参阅下表。



4 创建一个 GSLB 池。

- a 导航到应用程序 > **GSLB 服务** > 创建 > 高级设置 > 添加池。

← New GSLB Pool

Name\* ?

Name

Priority ?

10

Pool Members Load Balancing Algorithm\* ?

Geo

Pool Members Fallback Load Balancing Algorithm ?

Consistent Hash

Pool Members Fallback Load Balancing Algorithm Mask ?

Description

Pool Member

☐ IP Address

☒ Virtual Service

Site Cluster Controller\* ?

Select Site

Public IP Address ?

Ratio\* ?

1

Geo Location Source ?

Select Geo Location Source

Description

Enabled ?

Done

在 NSX Advanced Load Balancer 中，已更改基本设置和高级设置的池和组负载均衡算法位置。

5 下表介绍了 GSLB 池成员的各种配置实体：

优先级	DNS 服务选择正常运行并具有最高优先级的池。该可选参数的值在 0 到 100 之间。允许在组之间使用不唯一的值。可以将该值保持未设置状态。值 10 只是一个占位符。
负载均衡算法	对于活动-活动池配置，请选择循环（默认）、一致哈希、地理或拓扑。
DNS 服务返回的 IP 数	如果为 0，则返回所有 IP 地址。您可以指定 1 到 20 之间的数字。

DNS 服务提供的 TTL	如果 DNS 服务中的默认值不合适，则可以为代表所有 GSLB 池成员提供的所有 DNS 记录选择 1 到 86400 秒之间的值。
关闭响应	在该服务关闭时，该字段将控制来自 DNS 的响应。您可以选择无响应、空响应、回退 IP 或包含所有记录的响应。

## 按 IP 地址或虚拟服务标识 GSLB 池成员

本节重点介绍了按 IP 地址或虚拟服务标识 GSLB 池成员。

← Edit GSLB Pool

✕

Name\* ?

Name

Priority ?

10

LB Algorithm\* ?

Round Robin

Description

Pool Member

☒ IP Address

☐ Virtual Service

IP Address or FQDN\* ?

sub.corp.com <or> 10.0.0.1

Third-party Site Cluster Controller ?

Select Site

Public IP Address ?

Ratio\* ?

1

Geo Location Source ?

Select Geo Location Source

Description

Enabled ?

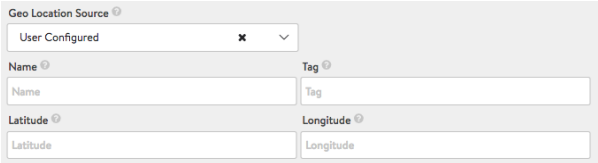
Add GSLB Pool Member

Done

VMware, Inc.

108

下表介绍了 GSLB 池成员的各种配置实体：

IP 地址或 FQDN	池成员是由其 IP 地址或 FQDN（控制器将其解析为 IP 地址）标识的。DNS 服务运行状况监控解析的地址。如果用户配置了一个 IP 地址（除了 FQDN 以外），每次控制器执行定期 FQDN 刷新时，都会覆盖该 IP 地址。
第三方站点集群控制器	有关更多详细信息，请参阅 <a href="#">添加第三方站点</a> 。
公用 IP 地址	该字段用于托管虚拟服务的公用 IP 地址。防火墙将其转换为专用 IP。来自 Intranet 内部的客户端 DNS 请求应在 A 记录中提供专用 IP，而来自外部的请求应提供公用 IP 地址。
已启用	默认设置为“开启”，以便在 DNS 响应中提供该成员的 IP 地址。
比率	该字段覆盖默认比率 1。它减少了选择与对等项关联的 GSLB 池成员的负载均衡算法百分比。允许的值范围是 1 到 20 之间。
地理位置源	指定地理位置源，或者从下拉列表中设置 <a href="#">用户配置</a> 选项以输入有关特定位置的数据。有关更多详细信息，请参阅 <a href="#">GSLB 成员的基于地理位置的负载均衡算法</a> 。动态定义位置时提供的字段如下所示。 

## GSLB 池成员的主机名字段

NSX Advanced Load Balancer 支持为 GSLB 池成员配置主机名字段。如果已配置，该字段将用作 GSLB HTTP 和 HTTPS 运行状况监控器中的主机标头。如果未配置主机名字段，则在 GSLB 监控器中使用 CNAME/FQDN。

### 使用 NSX Advanced Load Balancer CLI 配置主机名字段

登录到 NSX Advanced Load Balancer CLI，然后在 select gslbservice 模式下使用 hostname <hostname\_string> 命令以将主机名用于所需 GSLB 服务的 GSLB 监控器。

- 详细步骤如下所示：

```
[admin:ctrlr-1]: > configure gslbservice <gslb service name>
```

- 使用 where 命令确定池（组）索引：

```
[admin:ctrlr-1]: gslbservice> where
```

```
-----+
Field
Value
-----+
```

```

uuid gslbservice-ebdd873c-85e8-41d5-be5d-7f0145c68831

name gsl

domain_names[1] abcd.com

groups[1]

name  gsl-pool

priority 9

algorithm GSLB_ALGORITHM_ROUND_ROBIN

members[1]

ip 10.140.61.13

ratio 1

enabled True

hostname xyz

enabled True

down_response

type GSLB_SERVICE_DOWN_RESPONSE_NONE

health_monitor_refs[1] System-GSLB-HTTPS

controller_health_status_enabled True

```

在上面的示例中，`gs-pool1` 的索引值为 1。

### 3 使用 `group index` 命令选择所需的池。

```
[admin:ctrlr-1]:gslbservice> groups index <pool_index>
```

### 4 使用 `where` 命令确定池成员索引：

```

[admin:ctrlr-1]:gslbservice:groups> where

-----+
Field
Value
-----+

name  gsl-pool

```

```

priority 9

algorithm GSLB_ALGORITHM_ROUND_ROBIN

members[1]

ip 10.140.61.13

ratio 1

enabled True

hostname xyz

enabled True

-----+

```

在上面的示例中，池成员 (10.140.61.13) 索引为 1。

#### 5 使用索引值选择池成员。

```
[admin:ctrlr-1]:gslbservice:groups> members index <pool_memeber_index>
```

#### 6 选择池成员后配置主机名。

```
[admin:ctrlr-1]:groups:members> hostname <hostname_string>
```

#### 7 保存配置（池成员配置）。

```
[admin:ctrlr-1]:groups:members>save pool -> save gslbservice
```

**注** 在 NSX Advanced Load Balancer 中，GSLB HTTPS 运行状况监控器还支持 SNI 扩展。在该方法中，主机名用作服务器名称。如果未配置主机名，则将 CNAME 或 FQDN 用于运行状况监控器。

## 使用 NSX Advanced Load Balancer UI 配置 GSLB 运行状况监控器

以下规范适用于本节中使用 NSX Advanced Load Balancer UI 显示的示例。

- 客户有多个数据中心。
- 每个应用程序都需要配置运行状况监控器。
- view.sales.avi.local 将在 US-West 中运行，并依靠 US-Central 以作为灾难恢复站点。
- pay.sales.avi.local 将在 US-West 以及 US-East 中运行，以实现高可用性和最佳用户体验。

只能由登录到 GSLB 主控制器的授权用户执行该操作。

**模板 > 配置文件 > “全局运行状况监控”选项卡**显示 5 个预先存在的系统标准监控器。

对于系统标准监控器，更好的做法是单击**创建**以定义全新的监控器。将在编辑器窗口中填充适用的默认值，然后可以根据需要进行修改。请参阅下面的**新建 GSLB 运行状况监控器**编辑器窗口。

New Health Monitor: our-gslb-tcp-monitor

Name <sup>?</sup>

our-gslb-tcp-monitor

Type <sup>?</sup>

TCP

Description

Successful Checks <sup>?</sup>

2

Send Interval <sup>?</sup>

5

sec

Failed Checks <sup>?</sup>

2

Receive Timeout <sup>?</sup>

4

sec

☐ Is Federated <sup>?</sup>

• TCP Settings •

☐ Half-Open (Close connection before completion) <sup>?</sup>

Client Request Data <sup>?</sup>

None/Empty

Server Response Data <sup>?</sup>

None/Empty

Health Monitor Port <sup>?</sup>

Use Server Port

• Server Maintenance Mode •

Maintenance Server Response Data <sup>?</sup>

Maintenance Server Response Data

Cancel

Save

检查成功	在将虚拟服务标记为启动之前连续成功的运行状况检查次数。
检查失败	在将虚拟服务标记为关闭之前连续失败的运行状况检查次数。
发送间隔	给定虚拟服务进行运行状况检查间隔的秒数。
接收超时	应在该秒数内从服务器收到有效的响应。它必须小于发送间隔。如果服务器状态经常在启动和关闭之间波动，请考虑增加该值。
已联合？	<p>此选项有助于定义对象的复制范围。如果启用，则在联合中复制对象。否则，它在控制器集群及其关联的 SE 中可见。</p> <p>只有在启用了 GSLB 时，Is_federated 才会设置为 True。联合运行状况监控器用于 GSLB 目的，但不适用于常规运行状况监控器。这意味着 GSLB 服务不能与常规运行状况监控器相关联，因为 GSLB 服务是一个联合对象，而运行状况监控器不是。反过来，池不能与联合运行状况监控器相关联，因为池不是一个联合对象。</p>
运行状况监控器端口	无论关联的虚拟服务使用哪个端口，该监控器都会将其运行状况检查传送到端口 80。HTTP(S)、TCP、UDP 和外部运行状况监控器必须使用一个监控器端口。



在新的 GSLB 运行状况监控器编辑器中单击**保存**时，将完成创建自定义监控器的过程。

**注** 在 NSX Advanced Load Balancer 中，配置为活动/备用模式的 DNS NSX Advanced Load Balancer 支持运行状况监控。

## 在 NSX Advanced Load Balancer UI 中启用基于数据平面的全局应用程序运行状况监控

本节介绍了在 NSX Advanced Load Balancer UI 中启用基于数据平面的全局应用程序运行状况监控的配置步骤。

GSLB 站点将其他 GSLB 站点指定为运行状况监控代理以优化运行状况检查。在下图中，**运行状况监控器代理**字段的下拉菜单提供了三个能够为 GSLB 执行本地检查的 NSX Advanced Load Balancer GSLB 站点。

**New GSLB Site**

Name\*

Username\* Password\*

IP Address\* 1.2.3.4

Port 443

**Advanced Settings**

Client Group IP Address Type Private

10.0.0.0-10.255.255.255

Health Monitor Proxy

- US-vCenter
- India-vCenter
- US-AWS-West2

Geo Location Source Select Geo Location Source

Save Save and Set DNS Virtual Services

User can designate certain Avi sites to run health monitor probes for VIPs/VS(es) for this site. This is useful in network deployments where the VIPs/VS(es) are reachable only from certain sites. A typical scenario is a firewall between two GSLB sites. User may want to run health monitor probes from sites on either side of the firewall so that each designated site can derive a datapath view of the reachable members. If the health monitor proxies are not configured, then the default behavior is to run health monitor probes from all the active sites.

## 使用 NSX Advanced Load Balancer CLI 配置 GSLB 运行状况监控器

登录到主节点 (10.10.25.10)，并使用 `configure gslbhealthmonitor <monitor name>` 命令提供监控器的类型和端口号。

```
> configure gslbhealthmonitor global-http-hm
gslbhealthmonitor> type health_monitor_http
gslbhealthmonitor> monitor_port 80
gslbhealthmonitor> save
```

## 配置 GSLB 外部运行状况监控器

外部运行状况监控器允许编写脚本以提供高度自定义和精细的运行状况检查。脚本可以是 Linux Shell、Python 或 Perl，它们可用于执行 wget、netcat、curl、snmpget、mysql-client 或 dig。外部监控器限制了对 CPU 和内存等资源的访问，以确保 NSX Advanced Load Balancer SE 正常运行。与任何自定义脚本一样，在将实施的脚本指向生产服务器之前，请全面验证该脚本的长期稳定性。

以下是使用外部运行状况监控器的示例脚本。

下面是一个示例脚本/示例：

```
#curl -v $IP:$PORT >/run/hmuser/$HM_NAME.$IP.$PORT.out
#echo "$IP" > "/tmp/myfile"
#echo "$PORT" > "/tmp/myfile"
if [[ $IP =~ : ]];
then curl -v [$IP]:$PORT;
else curl -v $IP:$PORT;
fi
```

\$IP 和 \$PORT 是池成员的 IP 地址和运行状况监控器的端口。

**注** 建议不要将该 tmp 文件信息日志记录用于生产设置，而仅将其用于调试。

除了 GSLB 池成员以外，还可以使用外部运行状况监控器监控其他实体。

示例脚本：

```
#!/bin/bash
curl -I https://www.avinetworks.com:443 2>/dev/null | head -n 1 | grep "200"
```

**注** 在外部运行状况监控器用于 GSLB 池成员以外的实体时（如上面的脚本中所示），DNS 和负载均衡虚拟服务必须使用不同的 SE 组。

## GSLB 负载均衡算法

本节介绍了以下 GSLB 服务选择算法：

- 配置 GSLB 回退算法
- 配置基于地理位置的算法
- 配置拓扑算法
- 配置 GSLB 站点 Cookie 持久性

### GSLB 服务选择算法

本节介绍了如何配置以下 GSLB 服务选择算法：

- 配置 GSLB 回退算法
- 配置基于地理位置的算法
- 配置拓扑算法

## ■ 配置 GSLB 站点 Cookie 持久性

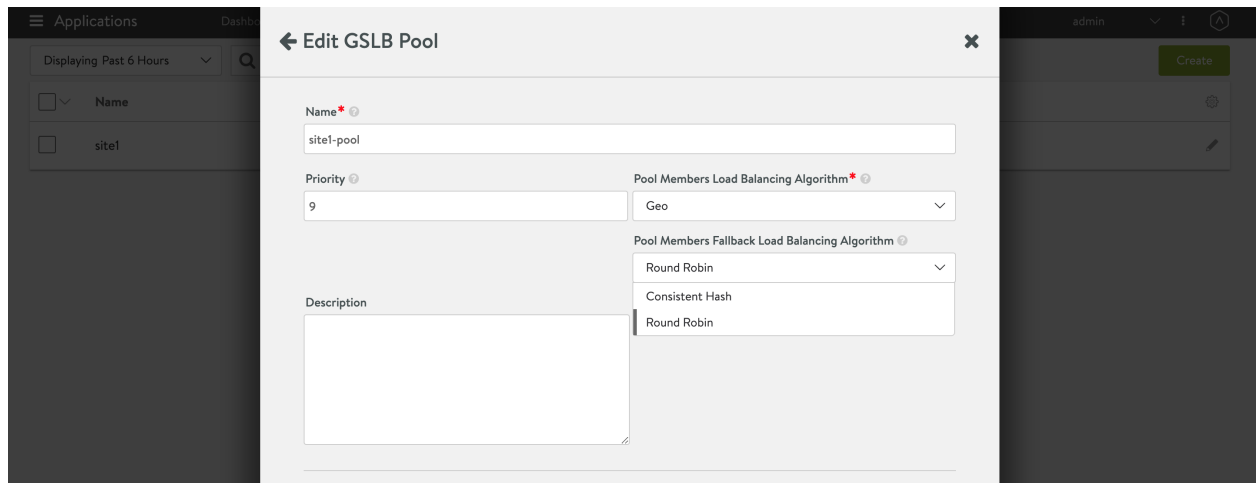
### 使用 NSX Advanced Load Balancer UI 为 GSLB 配置回退算法

本节介绍了使用 NSX Advanced Load Balancer UI 为 GSLB 配置回退算法的步骤。

要将 GSLB 池成员的回退算法设置为“一致哈希”，请执行以下操作：

- 1 选择所需的 GSLB 池成员。
- 2 单击 **编辑** 图标，将“池成员负载均衡算法”值设置为“地理”，将“池成员回退负载均衡算法”值设置为“一致哈希”，如下所示。

**注** 下面的屏幕截图显示可以选择“循环”或“一致哈希”以作为回退算法。



要创建新的 GSLB 服务和新的 GSLB 池成员，请参阅[如何为 GSLB 服务和 GSLB 池成员设置 GSLB 算法](#)。

### 使用 NSX Advanced Load Balancer CLI 为 GSLB 配置回退算法

登录到 NSX Advanced Load Balancer Shell 提示符，使用 `configure gslbservice <service name>` 命令将 GSLB 方法的主要算法设置为 `gslb_algorithm_geo`，并将备份算法设置为 `gslb_algorithm_consistent_hash`。

```
admin@ctlr-1:~$ shell
Login: admin
Password:

[admin:ctlr-1]: > configure gslbservice gs21
[admin:ctlr-1]: gslbservice> groups index 1
[admin:ctlr-1]: gslbservice:groups> algorithm gslb_algorithm_geo
Overwriting the previously entered value for algorithm
[admin:ctlr-1]: gslbservice:groups> fallback_algorithm gslb_algorithm_consistent_hash
[admin:ctlr-1]: gslbservice:groups> save
[admin:ctlr-1]: gslbservice> save
```

## 使用 NSX Advanced Load Balancer UI 配置基于地理位置的算法

本节介绍了使用 NSX Advanced Load Balancer UI 配置基于地理位置的算法的步骤。

要使用 NSX Advanced Load Balancer UI 配置 Geo-DB，请执行以下操作：

### 步骤

- 1 导航到**基础架构 > GSLB**，然后选择**上载地理文件**选项卡以选择将包含到所需地理位置配置文件中的候选文件。

请注意下拉列表中提供的格式选项，这些文件也可能包含具有 IPv6 地址的位置。

- 2 指定要上载的地理文件。要创建地理位置配置文件，请导航到**基础架构 > GSLB > 地理配置文件**。
- 3 单击**创建**以打开地理配置文件编辑器。

为配置文件指定一个名称。指定一个或多个以前上载的文件。对于每个文件，指定从 1（最低）到 100（最高）的优先级，并从支持的格式下拉列表中选择文件的格式。在确定给定地址或地址范围的位置时，NSX Advanced Load Balancer 将从最高优先级文件开始搜索文件，并从最高优先级文件中选取条目。

## 使用 NSX Advanced Load Balancer CLI 配置基于地理位置的算法

本节介绍了使用 NSX Advanced Load Balancer CLI 配置基于地理位置的算法的步骤。

要使用 NSX Advanced Load Balancer CLI 启用基于地理位置的算法，请执行以下操作：

### 步骤

- 1 在将使用地理位置算法的环境中设置 SE 组属性时，请特别注意内存配置。

```
[admin:10-10-24-207]: > configure serviceenginegroup mySEgrp
[admin:10-10-24-207]: serviceenginegroup> where
Tenant: admin
+-----+-----+
| Field | Value |
+-----+-----+
| name  | mySEgrp |
+-----+-----+
```

```
[admin:10-10-24-207]: serviceenginegroup> memory_per_se 8196
[admin:10-10-24-207]: serviceenginegroup> extra_shared_config_memory 2048
[admin:10-10-24-207]: serviceenginegroup> save
[admin:kh-cl]: serviceenginegroup>
```

## 2 上载一个或多个 geo-DB 文件。

```
[admin:10-10-24-207]: > upload gslbfiles [FILENAME]
```

## 3 以类似于 NSX Advanced Load Balancer 编辑器的方式创建一个 GSLB 地理位置配置文件。

```
[admin:10-10-24-207]: > configure gslbgeodbprofile mygslbprofile
[admin:10-10-24-207]: gslbgeodbprofile> where
Tenant: admin
+-----+-----+
| Field | Value          |
+-----+-----+
| name  | mygslbprofile |
+-----+-----+
[admin:10-10-24-207]: gslbgeodbprofile> [TAB][TAB]
cancel          Exit the current submode without saving
description     Help string not found for argument
do              Execute a show command
entries         (submode)
name            A user-friendly name for the geodb profile.
new             (Editor Mode) Create new object in editor mode
no             Remove field
save            Save and exit the current submode
show_schema    show object schema
tenant_ref     Help string not found for argument
watch          Watch a given show command
where          Display the in-progress object
[admin:10-10-24-207]: gslbgeodbprofile> where
Tenant: admin
+-----+-----+
| Field | Value          |
+-----+-----+
| name  | mygslbprofile |
+-----+-----+
[admin:10-10-24-207]: gslbgeodbprofile> new
# description: ' # Field Type: Optional'
# entries:
# - file:
#   checksum: ' # Field Type: Optional'
#   file_id: ' # Field Type: Optional'
#   filename: ' # Field Type: Optional'
#   format: '<choices: GSLB_GEODB_FILE_FORMAT_MAXMIND_CITY |
GSLB_GEODB_FILE_FORMAT_AVI>
#   # Field Type: Optional'
#   timestamp: ' # Field Type: Optional'
#   priority: ' # Field Type: Optional'
# name: ' # Field Type: Required'
# tenant_uuid: ' # Field Type: Required'
```

```
# uuid: ' # Field Type: Required'
#
name: mygslbprofile
</code></pre>
```

#### 4 为 GSLB 服务池选择地理位置负载均衡算法。

```
[admin:10-10-24-207]: > configure gslbservice gs-1
[admin:10-10-24-207]: gslbservice> new
# - algorithm: '<choices: GSLB_ALGORITHM_CONSISTENT_HASH |      GSLB_ALGORITHM_ROUND_ROBIN
#   | GSLB_ALGORITHM_GEO> # Field Type: Optional'
#   consistent_hash_mask: ' # Field Type: Optional'
#   members:
#   - cluster_uuid: ' # Field Type: Optional'
#     enabled: '(true | false) # Field Type: Optional'
#     fqdn: ' # Field Type: Optional'
#     hm_proxies:
#     - proxy_type: ' # Field Type:
#       Optional'
#       site_uuid: ' # Field Type: Optional'
#   ip:
#     addr: ' # Field Type: Required'
#     type: '<choices: V4 | DNS> # Field Type: Required'
#   location:
#     latitude: ' # Field Type: Optional'
#     longitude: ' # Field Type: Optional'
#     name: ' # Field Type: Optional'
#     tag: ' # Field Type: Optional'
#     source: '<choices: GSLB_LOCATION_SRC_FROM_GEODB | GSLB_LOCATION_SRC_USER_CONFIGURED
#   | GSLB_LOCATION_SRC_INHERIT_FROM_SITE> # Field Type: Optional'
#     ratio: ' # Field Type: Optional'
#     vs_uuid: ' # Field Type: Optional'
#     name: ' # Field Type: Optional'
#     priority: ' # Field Type: Optional'
#   health_monitor_scope: '<choices: GSLB_SERVICE_HEALTH_MONITOR_ONLY_NON_AVI_MEMBERS
#   | GSLB_SERVICE_HEALTH_MONITOR_ALL_MEMBERS> # Field Type: Optional'
#   health_monitor_uuids:
#     name: ' # Field Type: Required'
#     num_dns_ip: ' # Field Type: Optional'
#     tenant_uuid: ' # Field Type: Required'
#     ttl: ' # Field Type: Optional'
#     use_edns_client_subnet: '(true | false) # Field Type: Optional'
#     uuid: ' # Field Type: Required'
#     wildcard_match: '(true | false) # Field Type: Optional'
#
groups:
- algorithm: GSLB_ALGORITHM_GEO
name: gs-1
</code></pre>
```

- 5 使用地理位置算法的 GSLB 服务将显示位置（以及可能已使用 `configure gslbservice` 设置的任何其他值）。

```
[admin:10-10-24-207]: > show gslbservice gs-1
-----+
Field      Value
-----+
uuid       gslbservice-90a4becd-0051-48b2-b19d-e3e2aa30f101
name       gs-1
domain_names[1]   abcd.com
groups[1]
name       gs11
priority   10
algorithm   GSLB_ALGORITHM_GEO
members[1]
ip         1.0.0.0
ratio      1
enabled     True
controller_health_status_enabled   True
health_monitor_scope   GSLB_SERVICE_HEALTH_MONITOR_ALL_MEMBERS
enabled     True
tenant_ref   admin
-----+

[admin:10-10-24-207]: > show gslbservice gs-1 runtime
-----+
Field      Value
-----+
uuid       gslbservice-90a4becd-0051-48b2-b19d-e3e2aa30f101
name       gs-1
groups[1] | |
name       gs11
members[1]
ip         1.0.0.0
oper_ips[1]   1.0.0.0
```

### 后续步骤

有关 Geo-DB 的更多详细信息，请参阅链接。

### 使用 NSX Advanced Load Balancer UI 配置拓扑算法

NSX Advanced Load Balancer UI 具有一个在 GSLB 算法设置为**拓扑**时使用的**拓扑策略**选项。可以使用以下步骤配置基于拓扑的 GSLB 算法以选择池成员。

配置主要分为以下几点：

- 将**基于拓扑的 GSLB 算法策略**与虚拟服务相关联
- 将 GSLB 服务的 GSLB 算法设置为“拓扑”

使用 NSX Advanced Load Balancer UI 配置拓扑算法：

## 步骤

- 1 登录到 NSX Advanced Load Balancer UI 并导航到**应用程序 > 虚拟服务**。选择所需的虚拟服务，然后单击编辑选项。
- 2 导航到**策略 > 拓扑策略**选项卡。
- 3 单击加号图标以创建新的拓扑策略。
- 4 提供新规则所需的名称、匹配标准和操作。在配置所有字段后，单击**提交**。

**New DNS Policy Rule: TopologyRule1** [X]

**Name\*** ?  
 ✓

---

**Matches**

Geographical Location ×

☒ is ☐ is not ✓ **Use EDNS Client IP** ?

**Geolocation Name** ?

**Geolocation Tag** ?

---

▼

---

**Actions**

GSLB Site ×

**GSLB Site Name\*** ?  
 ▼ ✓ **Site Preferred** ?

---

- 5 导航到**应用程序 > GSLB 服务**，然后选择所需的 GSLB 服务。
- 6 在 **GSLB 池**部分中选择适用于池的编辑选项。
- 7 从**池成员负载均衡算法**字段的下拉列表中选择**拓扑**。

## 使用 NSX Advanced Load Balancer CLI 配置拓扑算法

本节介绍了使用 NSX Advanced Load Balancer CLI 配置拓扑算法的步骤。

要使用 NSX Advanced Load Balancer CLI 配置拓扑算法，请执行以下操作：



## 步骤

- 1 登录到 NSX Advanced Load Balancer CLI Shell 提示符，然后使用所需的规则和操作配置拓扑策略。

```
[admin-cntrl]: configure dnspolicy <dnspolicy name>
name          Name of the DNS Policy
rule          (submode)
save          Save and exit the current submode
```

- 2 配置或编辑虚拟服务，并关联在上一步中创建的拓扑策略。

```
[admin-cntrl: configure virtualservice <virtual service name>
[admin-cntrl: virtualservice> topology_policies dns_policy_ref foo
[admin-cntrl: virtualservice> : save
```

- 3 配置 GSLB 服务，并将算法设置为 `gslb_algorithm_topology`。

```
[admin:ctrl-1]: > configure gslbservice gsl
[admin:ctrl-1]: gslbservice> groups index 1
[admin:ctrl-1]: gslbservice:groups> algorithm gslb_algorithm_topology
[admin:ctrl-1]: gslbservice:groups> save
[admin:ctrl-1]: gslbservice> save
```

## 配置 GSLB 站点 Cookie 持久性

本节介绍了配置 GSLB 站点 Cookie 持久性的步骤。

以下步骤采用已存在的基本 GSLB 配置：

- 1 恰好配置一个联合 PKI 配置文件。可以通过 NSX Advanced Load Balancer UI 轻松完成这种一次性操作，该操作适用于所有 GSLB 服务。
- 2 配置联合应用程序持久性配置文件。可以定义多个该类型的配置文件。
- 3 配置运行状况监控器。可以定义多个该类型的运行状况监控器。
- 4 配置 GSLB 服务。将其指定为站点持久性，并将其与以下内容相关联：
  - a 一个联合应用程序持久性配置文件
  - b 一个或多个运行状况监控器

---

**注** 在运行 NSX Advanced Load Balancer 时，可以使用 NSX Advanced Load Balancer UI 完成步骤 4a 以外的所有其他步骤。提供了完整的 UI 支持（如步骤 4b 中所述）。

---

## 使用 NSX Advanced Load Balancer UI 进行配置

该任务帮助您使用 NSX Advanced Load Balancer UI 配置 GSLB 站点 Cookie 持久性。

### 步骤

#### 1 配置 PKI 配置文件

- a 导航到**模板 > 安全性 > PKI 配置文件**。
- b 单击**创建**，并确保选择**已联合**选项。

这是一次性操作。

**注** 如果适用，NSX Advanced Load Balancer 对象的 `is_federated` 选项描述其复制范围。如果该选项设置为 `False`，则对象仅在控制器集群及其关联的 SE 中可见。如果该选项设置为 `True`，则在联合中复制对象。

图 3-5. PKI 配置文件编辑器

**Edit PKI Profile: gpki-server**

Name\* ?  
gpki-server

☐ Ignore Peer Chain ? ☐ Enable CRL Check ? ☒ Is Federated ?

This field describes the object's replication scope. If the field is set to false, then the object is visible within the controller-cluster and its associated service-engines. If the field is set to true, then the object is replicated across the federation.

• Certificate Authority (CA) •

+ Add CA

Displaying 1 item(s)

<input type="checkbox"/> <span>▼</span> Name	Issued By	Expiration Date
<input type="checkbox"/> Test CA (1024 bit RSA)	Test CA (1024 bit RSA)	2021-12-16 19:27:41

Cancel Save

在创建了联合 PKI 配置文件并启用了站点持久性 GSLB 后，无法删除 PKI 配置文件。如果选中左侧的框并按**删除**按钮，则会出现错误。

## 2 配置联合应用程序持久性配置文件

- a 导航到**模板 > 配置文件 > 持久性**。
- b 单击**创建**以打开持久性配置文件编辑器。
- c 将**类型**字段设置为 **GSLB 站点**，然后单击**已联合**选项。

图 3-6. 持久性配置文件编辑器

The screenshot shows the 'Edit Persistence Profile: gap-1' window. It contains the following fields and controls:

- Name**: A text input field containing 'gap-1'.
- Type**: A dropdown menu set to 'GSLB Site'.
- Select New Server When Persistent Server Down**: Two radio buttons, 'Immediate' (selected) and 'Never'.
- Is Federated**: A checkbox that is checked.
- Description**: A large text area for additional information.
- Save**: A green button at the bottom right.

将显示配置的持久性配置文件的部分列表，前三个配置文件将其“类型”字段设置为“GSLB 站点”。

## 3 步骤 3. 配置运行状况监控器

- a 导航到**模板 > 配置文件 > 运行状况监控器**。
- b 单击**创建**以打开运行状况监控器编辑器。确保选中了“已联合”选项。

## 4 配置 GSLB 服务

- a 导航到**应用程序 > GSLB 服务**。
- b 单击**创建**，然后选择**高级设置**。确保指定一个运行状况监控器配置文件，并选中**站点持久性**选项。

使用 NSX Advanced Load Balancer UI 将 GSLB 服务与联合应用程序配置文件相关联

本节介绍了使用 NSX Advanced Load Balancer UI 将 GSLB 服务与联合应用程序配置文件相关联的步骤。

在高级设置编辑器的最后部分中添加了第 4 个字段（“应用程序持久性配置文件”）。

### 使用 NSX Advanced Load Balancer CLI 配置 GSLB 站点 Cookie 持久性

在以下示例中，我们使用上述 UI 配置中所用的相同对象名称，即 `gs-1`、`gpci-server`、`gap-1` 和 `ghm-ping`。每个 Shell 命令具有很多子命令；我们仅显示与 GSLB 站点持久性特别相关的子命令。

#### 步骤

##### 1 配置 PKI 配置文件

Shell 命令：configure pkiprofile gpci-server

子命令：is\_federated

##### 2 配置联合应用程序持久性配置文件

Shell 命令：configure applicationpersistenceprofile gap-1

子命令：is\_federated、persistence\_type、server\_hm\_down\_recovery

##### 3 配置运行状况监控器

Shell 命令：configure healthmonitor ghm-ping

子命令：is\_federated

##### 4 配置 GSLB 服务

Shell 命令：configure gslbservice gs-1

子命令：application\_persistence\_profile\_ref、health\_monitor\_refs、is\_federated  
site\_persistence\_enabled

使用 NSX Advanced Load Balancer CLI 将 GSLB 服务与联合应用程序配置文件相关联

本节介绍了使用 NSX Advanced Load Balancer CLI 将 GSLB 服务与联合应用程序配置文件相关联的步骤。

必须通过 NSX Advanced Load Balancer CLI 执行以下步骤：

- 登录到相应控制器集群的 NSX Advanced Load Balancer Shell
- 键入 configure gslbservice gs-1
- 键入 application\_persistence\_profile\_ref gap-1 以响应 gslbservice 提示
- 要使关联生效，请键入 save

作为参考，下面提供了启用的 GSLB 服务（名为 `gs-1`）的所有参数：

Field	Value
-------	-------

uuid	gslbservice-2efeea54-12b4-4c1d-9fe0-ffd58e5125c3	
name	gs-1	
domain_names[1]	a.com	
groups[1]		
name	group1	
priority	13	
algorithm	GSLB_ALGORITHM_ROUND_ROBIN	
members[1]		
cluster_uuid	cluster-a7ba9c02-adf6-48d7-aa3d-41f664d45f85	
vs_uuid	virtualservice-da9efdc9-7204-4b69-afc2-4fccaf961e1d	
ip	10.90.173.73	
ratio	1	
enabled	True	
groups[2]		
name	group2	
priority	12	
algorithm	GSLB_ALGORITHM_ROUND_ROBIN	
members[1]		
cluster_uuid	cluster-fc6fa719-054d-42d0-a18b-a8a7577a3829	
vs_uuid	virtualservice-f4bdb96d-4de3-4b2f-bf51-1bb924783443	
ip	10.90.174.72	
ratio	1	
enabled	True	
health_monitor_refs[1]	ghm-ping	
controller_health_status_enabled	True	
health_monitor_scope	GSLB_SERVICE_HEALTH_MONITOR_ALL_MEMBERS	
enabled	True	
use_edns_client_subnet	True	
wildcard_match	False	
site_persistence_enabled	True	
application_persistence_profile_ref	gap-1	
pool_algorithm	GSLB_SERVICE_ALGORITHM_PRIORITY	
min_members	0	
is_federated	True	
tenant_ref	admin	
+-----+-----+-----+		

## 将第三方服务与第三方站点相关联

本节重点介绍了如何将第三方服务与第三方站点相关联。

- 1 要添加另一个第三方站点，管理员需要返回到**站点配置**屏幕，单击绿色的**添加第三方站点**按钮，然后提供前面所述的所需信息。
- 2 要将第三方应用程序扩展到该新定义的第三方站点，请先返回到 **GSLB 服务列表**。
  - a 单击与 GSLB 服务关联的**铅笔**图标。
- 3 单击 **GSLBServiceName1-pool** 的**铅笔**图标以打开 **GSLB 池编辑器**。滚动到编辑器底部，然后单击**添加 GSLB 池成员**超文本。将展开编辑器窗口。向下滚动并填写第二个池成员的详细信息，该成员将与新创建的第三方站点（名为 **NonAviSite2**）相关联。单击**完成**以完成编辑。

← Edit GSLB Pool

×

☒ IP Address
 ☐ Virtual Service

IP Address or FQDN\* ?

1.2.3.4

Third-party Site Cluster Controller ?

NonAviSite1

Public IP Address ?

Ratio\* ?

1

Geo Location Source ?

Select Geo Location Source

Description

First of several services not running under an Avi Controller. Other IP addresses planned for this pool.

☒ IP Address
 ☐ Virtual Service

IP Address or FQDN\* ?

5.6.7.8

Third-party Site Cluster Controller ?

NonAviSite2

Public IP Address ?

Ratio\* ?

1

Geo Location Source ?

Select Geo Location Source

Description

Second third-party member service is located at a differently named third-party site.

Add GSLB Pool Member

☒ Enabled

☒ Enabled

Done

现在，名为 GSLBServiceName1 的第三方 GSLB 服务将部署在两个站点上。

## 使用 NSX Advanced Load Balancer CLI 配置租户

本节介绍了使用 NSX Advanced Load Balancer CLI 配置租户的步骤。

在配置 GSLB 服务时，虚拟服务选择根据 GSLB 配置中的租户列出服务。默认情况下，在 GSLB 服务中，系统将显示所有虚拟服务。不过，从 NSX Advanced Load Balancer 版本 20.1.5 开始，您可以更改 `tenant_scope` 以仅查看租户范围的虚拟服务。

`tenant_scope` 是 GSLB 特定的配置参数，在设置为 `True`（默认）时，仅限从当前租户中选择虚拟服务；在设置为 `False` 时，允许从所有可访问的租户中选择虚拟服务。

---

**注** NSX Advanced Load Balancer 版本 20.1.5 中的默认行为是将 `tenant_scoped` 设置为 `True`。

---

示例：

要设置 `tenant_scoped`，请使用以下 CLI：

```
[admin:avi-controller]: > configure gslb glb-1
[admin:avi-controller]: gslb> tenant_scoped
[admin:avi-controller]: gslb> save
```

要禁用 `tenant_scoped`，请使用以下 CLI：

```
[admin:avi-controller]: > configure gslb glb-1
[admin:avi-controller]: gslb>no tenant_scoped
[admin:avi-controller]: gslb> save
```

## 配置企业/外部 DNS 服务器以将子域委派给 NSX Advanced Load Balancer DNS 服务

本节介绍了配置企业/外部 DNS 服务器以将子域委派给 NSX Advanced Load Balancer DNS 服务的步骤。

将 `avi.com` 委派给 NSX Advanced Load Balancer GSLB。

为了在实验室中尝试执行该操作，在客户端安装了 `dnsmasq` 并添加了以下条目：

在客户端 1 上：

```
server=/avi.com/10.10.25.10
```

```
server=/avi.com/10.160.110.100
```

```
dig pay.avi.com </code>
```

在客户端 2 上：

```
server=/avi.com/10.160.110.100
```

```
server=/avi.com/10.10.25.10 </code>
```

## A 记录返回：启用解析 CNAME

如果收到 GSLB 服务的 DNS 查询，并且选择配置了 FQDN 的成员（如上面的方法 1 中所述），NSX Advanced Load Balancer 将使用指向池成员 FQDN 的 CNAME 响应进行响应。然后，解析器需要为返回的 FQDN 执行另一次查找以完全解析该查询。

除了 CNAME 响应以外，NSX Advanced Load Balancer 还可能会在响应中添加 A 记录。

### 启用解析 CNAME

登录到 NSX Advanced Load Balancer CLI，然后在 `configure gslbservice` 模式下使用 `resolve_cname` 标记以允许或禁止为 CNAME 查询添加 A 记录。

```
[admin:ctrlr-1]: > configure gslbservice <gslb service name  
[admin:ctrlr-1]: gslbservice> resolve_cname
```

要禁止使用 `no resolve_cname` 标记，请运行以下命令：

```
[admin:ctrlr-1]: gslbservice> no resolve_cname
```

---

**注** 如果 GSLB 池成员 FQDN 映射到多个 IP 地址，NSX Advanced Load Balancer 仅选择其中的一个地址。

---



# GSLB Canary 更新

# 4

在早期 NSX Advanced Load Balancer 版本中，在主站点上执行任何配置更改后，将立即自动执行从 GSLB 主站点到 GSLB 从属站点的配置同步。在主站点上执行任何配置更改后，主站点将立即自动启动到所有从属站点的配置复制。这种复制方法称为连续复制方法。

在 NSX Advanced Load Balancer 中，除了连续复制方法以外，还支持手动复制方法。

## GSLB 复制方法

连续复制方法是唯一支持在所有站点之间同步配置的方法。到所有从属站点的配置同步是从主站点中自动启动的。由于更改立即推送到所有站点，因此，任何错误的配置可能会影响所有从属站点。

在手动复制中，配置同步是根据特定从属站点的提取请求启动的。用户可以根据需要选择配置同步。这有助于避免选定 GSLB 站点发生应用程序停机或无法进行访问。

在手动复制方法中，不会立即从主站点中启动配置同步。这种复制方法比连续复制方法更高效、灵活且可控。

在 GSLB 站点之间复制配置时，您可以控制以下内容：

- 选择从属站点
- 复制时间 - 您可以决定应何时执行复制，并考虑如何将对最终用户造成的影响降到最低和其他因素

## 连续复制模式

在连续 GSLB 复制模式下，主站点保留一个复制队列以将配置推送到所有 GSLB 站点。在主站点上完成配置更改后，该更改自动推送到从属站点。此复制模式具有以下限制：

- 用户无法控制复制，因为这是由主站点启动的自动过程。
- 复制队列保留在 NSX Advanced Load Balancer SE 的内存中。如果在热重新启动之前未完成复制，对于大型部署，复制队列将会急剧增大。
- 应用程序正常运行时间：在复制过程中无法访问 GSLB 应用程序。
- 配置同步优先于运行状况探测。如果配置更新所花的时间比预期时间长，将无法确定跨不同站点的各种 GSLB 服务的准确状态。

## 手动复制模式

在这种模式下，用户可以对复制进行控制。根据主站点中的配置同步触发器，配置从主站点同步到主动从属站点。对于 GSLB 站点中的新应用程序部署，如果在应用程序使用高峰时段访问其他应用程序和 GSLB 站点至关重要，这是非常有用的。可以将任何配置更改部署到主站点中，只有在流量较低或对最终用户的影响非常小时，才会将更改推送到从属站点。只有在完全保证新更改不会影响应用程序后，从属站点才会请求进行复制。

## 用例

如果需要以分阶段的方式在 GSLB 站点中部署应用程序，并最大限度减少停机时间和对最终用户的影响，这是非常有用的。可以先在一个站点上测试任何新应用程序，然后才能将其部署到所有站点中。

本章讨论了以下主题：

- 启用手动复制

## 启用手动复制

手动复制方法在主站点上使用检查点，它定义了从属站点可以安全使用的配置，并且从属站点将该配置作为上次保存的配置的基准点。

在从属站点发出提取请求以复制特定检查点时，主站点仅推送特定检查点之前的配置，而不是完整的配置。

以下是执行手动复制过程的步骤：

- 在主站点上执行 CUD（创建、更新或删除）操作
- 在主站点上验证应用程序
- 在主站点上创建配置检查点
- 在计划时间从 GSLB 主站点复制到选定从属站点或启动 GSLB 同步
- 在从属站点上测试新同步的应用程序
- 为其他从属站点计划一个更改时段，将以前在主站点上创建的检查点作为复制过程的基准点并完成复制过程

使用以下步骤从 GSLB 主站点中执行从属站点的 GSLB Canary 更新：

## 步骤

- 1 出于演示目的，请考虑下面显示的 GSLB 设置。主站点是 siteA，从属站点是 siteB。

Subdomains delegated to GSLB:  
com

Active Members (Continuous Replication)

Displaying 2 items

<input type="checkbox"/>	Name	Type	IP Address	Port	Username	DNS Vses	Site Status	SW Version	Replication
<input type="checkbox"/>	siteA	Leader (cur...	10.79.109.12	443	admin		<span style="color: green;">●</span>	20.1.1	Sync Not Applicab...
<input type="checkbox"/>	siteB	Active	10.79.109.13	443	admin		<span style="color: green;">●</span>		In Sync

- 2 使用 NSX Advanced Load Balancer CLI 登录到 GSLB 主站点 (siteA)。创建检查点 CP1。使用 `configure federationcheckpoint >checkpoint name>` 命令创建一个检查点。

```
[admin:controller]: > configure federationcheckpoint CP1
[admin:controller]: > save
```

- 也可以使用 NSX Advanced Load Balancer UI 创建检查点。导航到**基础架构 > GSLB > 联合检查点**。单击**创建**以创建新的检查点。

- 3 在主站点上启用手动复制模式，并将 CP1 作为手动模式的检查点基准。

```
[admin:controller]: > configure gslb Default
[admin:controller]: gslb> replication_policy replication_mode replication_mode_manual
checkpoint_ref CP1
[admin:controller]: gslb:replication_policy> save
```

Subdomains delegated to GSLB:  
com

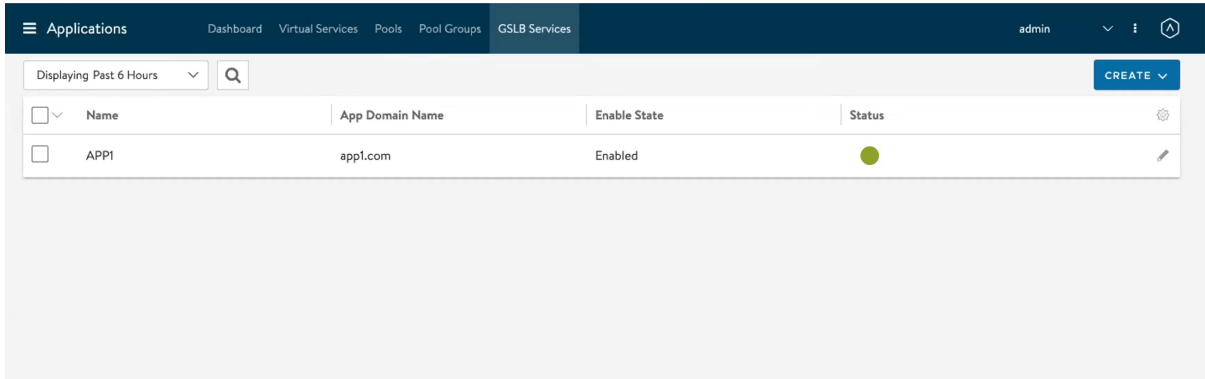
Active Members (Manual Replication)

Displaying 2 items

<input type="checkbox"/>	Name	Type	IP Address	Port	Username	DNS Vses	Site Status	SW Version	Replication
<input type="checkbox"/>	siteA	Leader (cur...	10.79.109.12	443	admin		<span style="color: green;">●</span>	20.1.1	Sync Not Applicab...
<input type="checkbox"/>	siteB	Active	10.79.109.13	443	admin		<span style="color: green;">●</span>	20.1.1	Synced Till Check...

- 4 对所需的应用程序执行计划的操作，或根据需要创建新的应用程序。

出于演示目的，在主站点上添加了应用程序 APP1，如下所示。



Applications				
Dashboard Virtual Services Pools Pool Groups <b>GSLB Services</b>				
admin				
Displaying Past 6 Hours				
<input type="checkbox"/>	Name	App Domain Name	Enable State	Status
<input type="checkbox"/>	APP1	app1.com	Enabled	<span style="color: green;">●</span>

- 5 在添加应用程序 APP1 后，根据需要为应用程序 APP1 执行所需的性能和稳定性检查。
- 6 在进行这些更改后，创建一个新的检查点 - 如果配置更改适合在其他从属站点之间复制，则创建另一个检查点 (CP2)。导航到**基础架构 > GSLB > 联合检查点**。单击**创建**以创建新的检查点 CP2。
- 7 将检查点更改为活动检查点 - 要将检查点 CP2 作为复制的基准点，请选择该检查点以作为活动检查点。在 NSX Advanced Load Balancer UI 上，活动检查点 (CP1) 带有星形标记。
  - a 单击**星形**图标或“设置为活动”选项，以将 CP2 检查点作为活动检查点。  
星形标记将移动到当前处于活动状态的 CP2 检查点。
- 8 如果选择 CP2 以作为从属站点复制过程的活动检查点，在创建该检查点后所做的任何配置更改不会复制到主动从属站点。
- 9 配置同步 - 选择需要进行复制的主动从属站点。单击**已同步到检查点**选项以开始将配置复制到选定的主动从属站点。单击**开始复制**选项以执行到主动从属站点的 GSLB 复制。
- 10 检查从属站点 siteB 上的配置更新状态。选定的从属站点反映了从主站点复制的配置更改。可以观察到，新应用程序 APP1 也复制到了从属站点。

# 使用 GSLB

# 5

本节介绍了以下内容：

- 如何将从属站点更改为新的主站点
- 为 GSLB 服务配置的 VIP 和运行 VIP 不同步
- 解决 Geo-DB 问题
- 故障场景和解决办法

本章讨论了以下主题：

- 如何将从属站点更改为新的主站点
- 为 GSLB 服务配置的 VIP 和运行 VIP 不同步
- 解决基于地理位置的算法问题
- 错误场景
- 故障场景和解决办法

## 如何将从属站点更改为新的主站点

本节重点介绍了如何手动将从属站点更改为新的主站点。

以下是需要手动更改 GSLB 站点的场景：

- 无法将 GSLB 从属站点与无响应的主站点断开连接。无法进行配置更改，因为仅在主站点上进行配置更改。
- 在网络分区场景中，也需要手动选举 GSLB 主站点。网络分区类似于裂脑情况，这是由于站点之间的 Internet 或 VPN 基础架构发生故障或中断而出现的。

如果发生网络故障，每个站点根据控制平面和数据平面运行状况监控器更新 GSLB 成员状态。网络的两个部分充当独立且排他的子网。不会在另一个网络分区上自动选举新的主站点（根据设计）。

- 在要求将主站点角色转移到另一个站点以执行更新或维护工作时。

在 GSLB 主站点关闭并且其他从属站点仍在运行时，流量将由所有站点中的 SE 进行处理，而不会出现任何问题。如果不需要进行 GSLB 配置更改，应避免更改主站点。如果您遇到临时中断，并预计在短时间内恢复主站点，建议避免更改主站点。请仅在以下情况下更改主站点：

- 需要进行配置更新

- 主站点将关闭相当长的一段时间
- 从长远来看，您确实需要将新站点更改为主站点

## 说明

可以按照以下步骤将 GSLB 部署中的从属站点手动提升为主站点角色：

- 登录到将成为主站点的从属站点的 Shell 提示符。执行 `show cluster` 命令，请注意以下输出中的 `uuid` (`vm_uuid`) 值。以下输出中的 `uuid` 值为 `005056b0333f`：

```
> show cluster
-----+

Field      Value
-----+

uuid       cluster-005056b0333f
name       cluster-0-1
nodes[1]
name       10.10.30.55
ip         10.10.30.55
vm_uuid    005056b0333f
vm_mor     vm-118231
vm_hostname node1.controller.local
-----+
```

- 在将成为新主站点的从属节点上，运行 `gslb changeleader new_leader cluster-UUID` 命令。使用从  
上一步中捕获的集群 UUID (`005056b0333f`)：

```
> gslb changeleader new_leader cluster-005056b0333f
```

示例输出如下所示：

```
> gslb changeleader new_leader cluster-005056b0333f
-----+

Field      Value
-----+

new_leader  cluster-005056b0333f
view_id     1525803021
details[1]  Review event-logs for additional information
-----+
```

**注** 在完成上述步骤后，从属站点开始将 **GSLB** 配置同步到自身。由于无法访问另一个站点（旧主站点），新主站点在达到最大重试次数后停止尝试同步信息。

在以前的主站点启动时进行的更改

建议恢复以前的主站点，以便 **GSLB** 设置在两个站点之间完全正常工作。在恢复网络分区状况时，两个节点可以相互通信。为了避免任何冲突问题，需要进行配置更改以将以前的主站点更改为从属站点。以前的主站点应将新的主站点视为唯一的实际主站点。

为了避免任何冲突，请执行以下命令以使以前的主站点成为从属站点：

- 在新主站点上运行 `show gslb Default | grep -i view` 命令并记下 `view_id`，如下所示：

```
> show gslb Default | grep -i view

view_id      1525801573
```

此外，在新主站点上执行 `show cluster` 命令并记下 `uuid` (005056b0333f)。

```
> show cluster
-----+

Field      Value
-----+

uuid       cluster-005056b0333f
name       cluster-0-1
nodes[1]
name       10.10.30.55
ip         10.10.30.55
vm_uuid    005056b0333f
vm_mor     vm-118231
vm_hostname node1.controller.local
-----+
```

- 登录到旧主站点的 **Shell** 提示符（它显示旧主站点必须如何充当从属站点），并执行 `gslb changeleader new_leader cluster-UUIS view_id <view-id>` 命令。

```
gslb changeleader new_leader cluster-005056b0333f view_id 1525801573
```

---

**注** 在前面的示例中，`cluster-uuid` 和 `view_id` 是新主站点中的值。

---

上述步骤确保在 **GSLB** 设置中只有一个主站点。配置再次从新主站点推送到新从属站点。

## 确认更改

要检查 **GSLB** 主站点选举是否成功，请在所有站点上执行以下命令：

```
show gslb runtime
```

输出将指示新的主站点。

## 注意事项

以下是进行这些更改时应注意的几点，因为 **GSLB** 站点可能会显示一些不一致问题：

- 如果手动更改主站点，则可能在两个站点之间存在配置同步问题。
- 将在进行这些更改时出现流量中断，因为更改主站点启动从新主站点到旧主站点的配置同步。

- DNS 记录也可能存在不一致问题，因为新主站点可能将较少的记录同步到以前的主站点（新从属站点）。

## 为 GSLB 服务配置的 VIP 和运行 VIP 不同步

GSLB 服务处于禁用状态，并在 GSLB 站点之间观察到同步问题。NSX Advanced Load Balancer UI 显示处于禁用状态的原因是，配置的 VIP 和运行 VIP 不同步。

### 原因

在本地管理 GSLB 应用程序部署的组件是可行且合理的。例如，本地站点管理员可以选择更改某个 GSLB 池的本地虚拟服务成员的虚拟 IP。在这样做时，全局应用程序进入某种状态，其中配置的 GSLB 池成员 VIP 和运行 VIP 不同步（不一致）。这种不一致问题是自然而然的结果，NSX Advanced Load Balancer 自动检测到该问题。本节详细介绍了这种不一致问题，并提供恢复为一致状态的步骤。

### 这种不一致问题是如何产生的

NSX Advanced Load Balancer GSLB 池成员是一个 NSX Advanced Load Balancer 虚拟服务（具有关联的 VIP:端口号）。要配置这种成员，用户需要唯一地标识站点 ID、站点中的虚拟服务以及虚拟服务的相应 VIP。

GSLB 池成员对象中的相关参数包括：

- `GslbPoolMember.site-cluster-uuid`
- `GslbPoolMember.virtual-service-uuid`
- `GslbPoolMember.ip`

有关更多详细信息，请参阅[适用于 GSLB 服务的 API](#)。

现在考虑以下场景：

**实施中：** GSLB 池成员的三个参数设置为 `site-cluster-uuid-W`、`virtual-service-uuid-X` 和 `ip-Y`。这些值表示为虚拟服务配置的状态和运行状态。NSX Advanced Load Balancer 的 GSLB 配置（一个全局实体）与由站点 W 本地定义并在其中运行的虚拟服务同步。

**实施后：** 出于任何原因，站点 W 的管理员更改了特定虚拟服务的 NSX Advanced Load Balancer 本地配置，以使其 VIP 现在为 `ip-Z`。

**情况：** 虽然本地 VIP `ip-Z` 正常运行，但 GSLB 配置（还）不知道其地址；它不再作为全局应用程序的一部分进行通告；对 `ip-Y` 的引用无效。GSLB 主站点和主动成员检测实施中 VIP (`ip-Y`) 和实施后 VIP (`ip-Z`) 之间的差异。然后，NSX Advanced Load Balancer 禁用相关的 `GslbPoolMember` 并通知管理员“配置的 VIP 和运行 VIP 不同步”。

请按照以下步骤解决该问题。



## 解决方案

本节介绍了解决上述问题的步骤。

### 方法 1: 使用 NSX Advanced Load Balancer UI

在使用 NSX Advanced Load Balancer UI 时，无法直接重置禁用的成员虚拟服务的已更改 VIP。应改用 GSLB 池编辑器删除成员虚拟服务（例如，以下屏幕截图中的 VS-Site-US-East），然后重新添加该虚拟服务。重新指定站点集群控制器和虚拟服务字段值将导致 NSX Advanced Load Balancer 在站点中查询新的 IP 地址。

**Edit GSLB Pool**

☐ IP Address ☒ Virtual Service

Site Cluster Controller\* ? Virtual Service\* ?

US-East VS-Site-US-East

Ratio\* ? 1 ☐ Enabled ?

☐ IP Address ☒ Virtual Service

Site Cluster Controller\* ? Virtual Service\* ?

US-Central VS-Site-US-Central

Ratio\* ? 1 ☒ Enabled ?

☐ IP Address ☒ Virtual Service

Site Cluster Controller\* ? Virtual Service\* ?

US-West VS-Site-US-West

Ratio\* ? 1 ☒ Enabled ?

Add GSLB Pool Member

### 方法 2: 使用 NSX Advanced Load Balancer CLI

下面的命令显示实施中和实施后步骤，其中先配置 GslbPoolMember 对象，然后重新进行配置。W、X、Y 和 z 是对应于上述场景的值：

```
[admin:10-10-24-207]: > configure gslbservice gs-1
[admin:10-10-24-207]: gslbservice> groups
New object being created
[admin:10-10-24-207]: gslbservice:groups> name gs-11
[admin:10-10-24-207]: gslbservice:groups> members
New object being created
[admin:10-10-24-207]: gslbservice:groups:members>
[admin:10-10-24-207]: gslbservice:groups:members> cluster_uuid W
[admin:10-10-24-207]: gslbservice:groups:members> vs_uuid X
[admin:10-10-24-207]: gslbservice:groups:members> ip Y
```

```
[admin:10-10-24-207]: gslbservice:groups:members> save
[admin:10-10-24-207]: gslbservice:groups>
```

要消除在本地将 ip-Y 更改为 ip-Z 而导致的不一致问题，请执行以下命令：

```
[admin:10-10-24-207]: > configure gslbservice gs-1
[admin:10-10-24-207]: gslbservice> groups index 1
members index 1
[admin:10-10-24-207]: gslbservice:groups:members>
[admin:10-10-24-207]: gslbservice:groups:members> ip Z
[admin:10-10-24-207]: gslbservice:groups:members> save
```

## NSX Advanced Load Balancer GSLB 环境中的升级

本节重点介绍了已配置 GSLB 的 NSX Advanced Load Balancer 部署中的各种升级场景。

某些情况可能会要求立即停止服务；其他情况可能允许正常升级而不会中断服务。NSX Advanced Load Balancer 的 GSLB 实施支持正常升级，即使需要执行一些操作，例如：

- 1 需要在主动和被动 GSLB 站点上安装新的 NSX Advanced Load Balancer 版本。
- 2 必须进行站点范围的更改。
- 3 必须更换一个或多个应用程序服务器或更改其配置。
- 4 需要在当前运行全局应用程序的所有站点服务器上安装新版本的全局应用程序可执行文件。

### NSX Advanced Load Balancer 升级

**注** 为了避免由于站点升级而导致的服务中断，建议应将 DNS 虚拟服务扩展到 SE 组中的至少两个 SE。

有关 NSX Advanced Load Balancer 升级过程的更多详细信息，请参阅[如何升级 NSX Advanced Load Balancer 软件](#)。

有关更多详细信息，请参阅[升级前步骤](#)。

### 错误场景

#### 从属站点升级失败

如果从属站点升级失败，它最终导致 GSLB 中断。该站点将回滚到以前的版本并恢复启动。在 GSLB 主站点上，禁用维护模式。在确定失败原因并解决该问题后，继续执行升级过程。

#### 主站点升级失败

在主站点上，禁用维护模式。确定原因并解决该问题。在此期间，无法启用任何新功能。

### 混合使用 NSX Advanced Load Balancer 版本

NSX Advanced Load Balancer 建议所有参与 GSLB 的站点运行相同的 NSX Advanced Load Balancer 版本和维护版本。

在升级周期内，可能无法或不希望在单个维护时段中将所有站点升级到相同的软件版本。在这种情况下，支持将运行不同 NSX Advanced Load Balancer 版本的站点混合使用一段时间，但需要注意以下重要事项：

- 1 GSLB 主站点必须是最后一个升级的站点。明确不支持主站点运行比任何 GSLB 从属站点更高的软件版本或维护版本。
- 2 在站点运行混合软件版本期间，可以在主站点上进行 GSLB 配置更改，但需要注意的是，在升级所有站点后，才能启用更高版本软件中的新 GSLB 功能。

## 升级前步骤

GSLB 升级过程包括将 GSLB 站点设置为维护模式。在维护模式下，任何 GSLB 站点均不参与 GSLB 过程，并且不允许在任何 GSLB 站点上进行配置更改。

以下是两种适用于主动从属站点升级的模式。在启动升级过程之前，启用其中的一种模式：

- 维护模式
- 挂起模式（仅适用于主动从属站点）

### GSLB 主站点的升级前步骤

要升级主站点，只能使用维护模式。

在维护模式下，无法在任何 GSLB 站点中执行配置更改。对于任何新配置，所有站点必须等待升级过程完成。维护模式是一种全局设置，它应用于所有 GSLB 站点，而不是仅一个站点的本地设置。

有关更多详细信息，请参阅[启用挂起模式](#)。

### 维护模式

在 GSLB 主站点上：使用 REST API 或以下 CLI 命令启用 GSLB 维护模式：

```
gslb maintenancemode enabled
```

因此，NSX Advanced Load Balancer 执行以下步骤：

- 阻止 GSLB 配置更改。我们不希望在升级从属站点时在主站点中应用任何 GSLB 配置更改。
- 将 `send_interval` 更改为 30 分钟以降低运行状况监控器探测频率。
- 根据计算结果，不会刷新时间 `T` 的远程站点缓存状态：

$$T = \text{gslb\_cfg.send\_interval} \times \text{gslb\_cfg.clear\_on\_max\_retries}$$

在该间隔内，不会将远程站点声明为关闭。

### 升级 GSLB 站点

先升级从属站点，最后升级主站点。

可以使用 CLI 命令 `show upgrade status` 检查升级状态。

## 升级后

- 1 将从属站点从挂起模式更改为非挂起模式。
- 2 如果将维护模式作为升级前步骤，请使用 CLI 命令 `gslb no maintenance mode` 在主站点上禁用 GSLB 维护模式。在执行该步骤后，新升级的远程站点可以从 GSLB 生态系统的其余部分中生成其运行时状态。
- 3 另一方面，如果准备好将站点升级到下一个站点，您可以跳过步骤 3。

为所有从属站点重复步骤 1 到 3，最后为主站点本身重复这些步骤。

---

**注** 在升级所有站点后，应将 Ansible 模块迁移到最新版本。

---

## 挂起模式

在挂起模式下，仅在参与升级或维护活动的从属站点上禁止进行配置更改。其他站点（主站点和其余从属站点）仍参与 GSLB 过程。

在挂起模式下，GSLB 主站点接受配置。配置更改将同步到启用了挂起模式的站点以外的所有从属站点。如果出现任何错误或使用错误的配置，这仅是特定站点的本地错误。错误或崩溃问题不会传播到其他站点，也不会影响通过 GSLB 托管的应用程序。可以在某个主动从属站点上继续进行升级或维护工作时访问该应用程序。

在挂起模式下，不会禁止在 GSLB 主站点上进行配置。该站点可以执行所有创建、读取、更新和删除 (CRUD) 操作。在升级后，一旦从属站点设置为非挂起模式，从属站点就会从主站点收到所有配置。

---

## 注

- 这仅适用于从属站点。不能将其应用于主站点
  - 在站点退出挂起模式后，将执行所有配置同步
  - 在升级后，将在从属站点和主站点之间执行一次性配置同步
- 

## 启用挂起模式

本节介绍了启用挂起模式的步骤。

登录到 NSX Advanced Load Balancer CLI，然后执行下面提到的步骤：

```
[admin-controller]: configure gslb default
[admin-controller]: gslb> site index 1
[admin-controller]: gslb> suspended_mode
```

在升级从属站点后，在从属站点上启用了非挂起模式，并同步主站点上提供的信息。

```
[admin-controller]: configure gslb gsl
[admin-controller]: gslb> site index 1
[admin-controller]: gslb> no suspended_mode
```

---

#### 注

- 在特定站点上启用挂起模式时，请在主动从属站点上禁用 DNS 虚拟服务。在计划的活动结束后，重新启用 DNS 虚拟服务。
- 

## GSLB 部署中的各种升级场景

本节重点介绍了使用 NSX Advanced Load Balancer UI 的以下升级场景。

- 在特定服务器上升级全局应用程序 - 成员禁用-启用选项
- 全面升级全局应用程序 - 全局服务禁用-启用选项
- 升级特定站点中的所有全局应用程序 - 站点禁用-启用选项

可以从 CLI 和 REST API 中执行相同的操作。

**注意事项：**下面所述的升级操作是 GSLB 运行操作，而不是 GSLB 配置更改选项。到站点中的 VIP/虚拟服务的动态连接不受影响。更改 DNS TTL 可能会解决该问题，但某些中间 DNS 缓存可能不支持 TTL；流量可能会继续传送到以前的 VIP。

### 升级特定服务器上的全局应用程序 - 成员禁用-启用选项

在需要升级总体上正常运行的全局应用程序以修复错误和/或添加功能时，我们使用该选项。这是正常执行的，而不会出现中断。多个站点已提供服务这一事实表明，可以关闭并升级一个站点的服务，同时其余 N-1 个站点中的传统服务继续运行。这是经典的滚动升级场景。

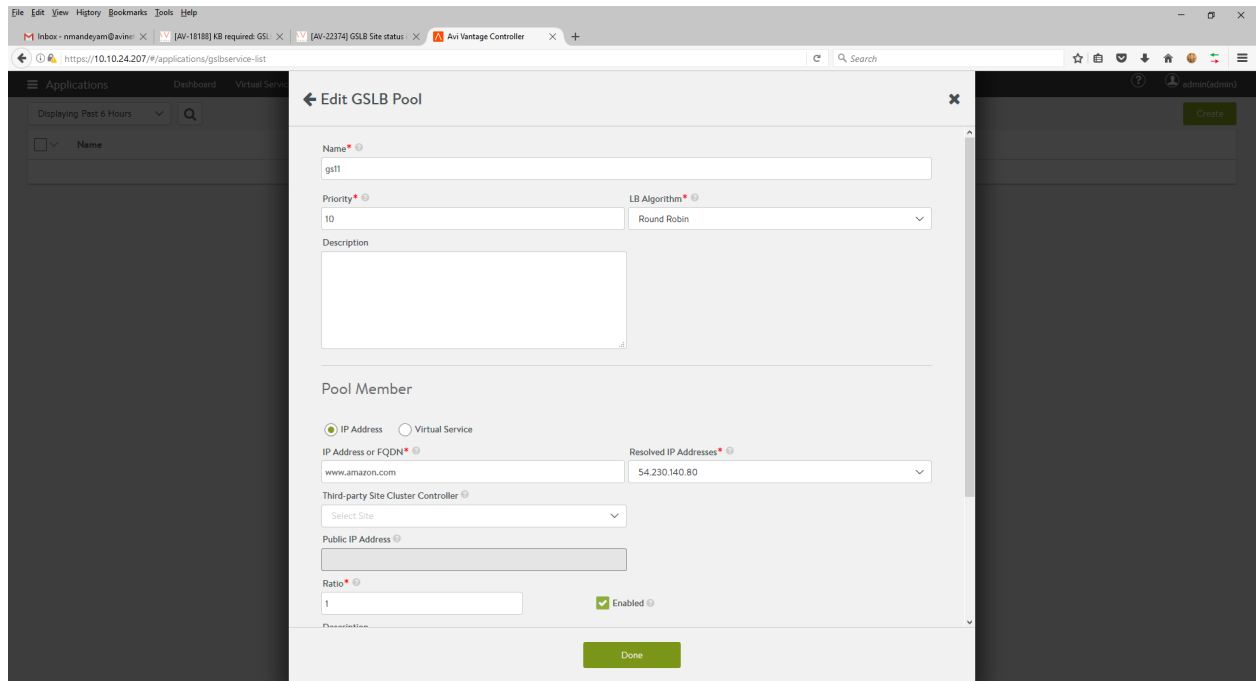
在 GSLB 主站点上，对于每个站点，使用 GSLB 池编辑器取消选中相关池成员（以下屏幕截图中的 **gs11**）的**已启用**选项。

---

**注** 我们更希望在成员虚拟服务变为非活动状态后对其进行升级。

---

接下来，对该虚拟服务的服务器池中的服务器上的应用程序进行所需的更改，重新启动该应用程序，然后选中**已启用**选项。



禁用 GSLB 池成员将导致 NSX Advanced Load Balancer 更改全局 DNS（撤销成员的 IP 地址），以便停止发送到成员虚拟服务（此处为 **gs11**）的流量。仍会在托管该应用程序的其余站点之间分配流量。

### 全面升级全局应用程序 - 全局服务禁用-启用选项

在某些情况下，需要立即并全面暂停全局应用程序，例如，直到在所有参与站点中纠正了某种错误或消除了安全漏洞为止。在这种情况下，我们希望将所有成员作为一个整体停止，而不是每次禁用一个成员（如上所述）。选项是 **global-service-disable**。

在 GSLB 主站点上，导航到**应用程序 > GSLB 服务**。单击应用程序行左侧的框。然后，单击**禁用**按钮。不要单击**删除**，因为这会从系统配置中永久移除全局服务。

NSX Advanced Load Balancer 更改全局 DNS，以便撤销 FQDN。

### 升级特定站点中的所有全局应用程序 - 站点禁用-启用选项

想象一下，一组服务器托管企业的所有虚拟化全局应用程序。如果数据中心空间有限，将它们升级到下一代服务器需要进行叉车式升级。如果在旧服务器集上同时运行这些全局应用程序，则无法也在新服务器集上启动它们。站点停机是不可避免的，在此期间，必须由其余 GSLB 站点处理客户端负载。

在 GSLB 主站点上，导航到**基础架构 > GSLB > 站点配置**。检查您希望禁用所有 GSLB 应用程序的站点。然后，单击**禁用**按钮。不要单击**删除**，因为这样做会从 GSLB 配置中永久移除指定的站点。

NSX Advanced Load Balancer 更改全局 DNS，以便撤销指定站点中参与所有全局应用程序的所有虚拟服务的 IP 地址。本地应用程序不受影响。全局应用程序 FQDN 请求的响应将包含其余 N-1 个 GSLB 站点上运行的虚拟服务的 IP 地址。

## 注

- 1 我们不允许禁用主站点。为了克服该限制，应将主站点角色移交给已升级的站点。从有利的方面看，可以随后禁用以前的主站点。
- 2 在重新启用站点后，NSX Advanced Load Balancer 将所有相关信息重新同步到新启用的站点。

## 解决基于地理位置的算法问题

本节重点介绍了确认正确运行和解决 Geo-DB 问题的各种方法。

### 检查表

- 验证所有 GSLB 站点、GSLB 服务和 DNS 虚拟服务是否已配置并正在运行。
- 确保 DNS 虚拟服务的 SE 组配置了足够的磁盘和内存。最低建议值如下所示。

• Service Engine Capacity and Limit Settings •

Max Number of Service Engines ?	Memory per Service Engine ?	vCPU per Service Engine ?	Disk per Service Engine ?
10	10 GB	2	25 GB
Maximum			

☒ Memory Reserve ☐ CPU Reserve

☒ Host Geo Profile ?

- 验证地理配置文件在定义后是否已推送到 SE。

可以使用 `show virtualservice your-dns-vs-name geodbinternal` 命令验证是否已正确应用 Geo-DB。检查以下结果：

```
[admin:naveen-ctrl]: > show virtualservice dns-vs geodbinternal
+-----+-----+
| Field      | Value                                     |
+-----+-----+
| se_uuid    | se-005056ba3198                         |
| uuid       | gslbgeodbprofile-8bb11129-383c-497d-9e39-7b622af3be56 |
| name       | geo-profile                             |
| db_entries[1] |                                           |
|   filename  | v4_only.txt.gz                           |
|   num_entries | 35                                       |
|   num_prefixes | 35                                       |
|   num_errors  | 0                                       |
|   priority   | 10                                       |
+-----+-----+
[admin:naveen-ctrl]: >
```

如果未正确应用，您可能会观察到错误输出，如下所示。FILE\_NO\_RESOURCES 表示在 SE 上没有足够的空间，如上所述。

```
[admin:naveen-ctrl]: > show virtualservice dns-vs geodbinternal
+-----+-----+
| Field          | Value                                     |
+-----+-----+
| se_uuid        | se-005056b06fda                         |
| uuid           | gslbgeodbprofile-8bb11129-383c-497d-9e39-7b622af3be56 |
| name           | geo-profile                             |
| db_entries[1]  |                                           |
|   filename     | v4_only.txt.gz                         |
|   num_entries  | 20                                      |
|   num_prefixes | 20                                      |
|   num_errors   | 1                                       |
|   priority     | 10                                      |
| error_file     | v4_only.txt.gz                         |
| error          | FILE_NO_RESOURCES                       |
+-----+-----+
[admin:naveen-ctrl]: >
```

- 验证与 GSLB 服务和/或 GSLB 池关联的地理位置算法的配置。下面的 NSX Advanced Load Balancer UI 屏幕截图显示 GSLB 池级别的地理算法。

**GSLB pool \*** Add Pool ➤

Displaying 1 item(s)

Name	Priority ? ▼	Algorithm
gslb-svc-pool	9	Geo

- 使用以下命令验证可以检测 IP 地址位置的地理位置算法：

```
show virtualservice dns-vs-name geolocationinfo [filter ip|start_ip]
```

以下输出确认位于意大利的一个位置：

```
[admin:naveen-ctrl]: > show virtualservice dns-vs geolocationinfo filter ip 2.233.236.0
+-----+-----+
| Field          | Value                                     |
+-----+-----+
| se_uuid        | Avi-Service-Engine:se-005056ba3198     |
| proc_id        | C0_I4                                    |
| entries[1]     |                                           |
|   ip           | 2.233.236.0                             |
|   mask         | 32                                       |
|   location     |                                           |
|     latitude   | 45.0                                     |
|     longitude  | 9.0                                      |
|   name         | Italy/Lombardy/Segrate                  |
+-----+-----+
```



```
| scaled_latitude | 135 |
| scaled_longitude | 189 |
+-----+-----+
[admin:naveen-ctrl]: >
```

以下输出确认位于印度的一个位置：

```
[admin:naveen-ctrl]: > show virtualservice dns-vs geolocationinfo filter ip 106.51.70.96
+-----+-----+
| Field | Value |
+-----+-----+
| se_uuid | Avi-Service-Engine:se-005056b0fa6a |
| proc_id | C0_L4 |
| entries[1] | |
| ip | 106.51.70.96 |
| mask | 32 |
| location | |
| latitude | 12.0 |
| longitude | 77.0 |
| name | India/Karnataka/Bengaluru |
| scaled_latitude | 102 |
| scaled_longitude | 257 |
+-----+-----+
[admin:naveen-ctrl]: >
```

以下输出中缺少条目意味着，Geo-DB 缺少 106.1.2.3 子网的信息，或没有足够的 SE 资源以使 Geo-DB 正常工作。

```
[admin:naveen-ctrl]: > show virtualservice dns-vs geolocationinfo filter ip 106.1.2.3
+-----+-----+
| Field | Value |
+-----+-----+
| se_uuid | Avi-Service-Engine:se-005056b081e1 |
| proc_id | C1_L4 |
+-----+-----+
[admin:naveen-ctrl]: >
```

## 有助于排除故障的其他命令

- `show gslbservice gslb-svc runtime`
- `show virtualservice dns-vs-name dnstable` - 显示绑定到 DNS 虚拟服务的 `dnstable`
- `show virtualservice dns-vs-name gslbservicedetail filter gs_ref gslb-svc-name` - 显示 GSLB 服务是否位于所有 SE 上以及该服务的状态
- `show virtualservice dns-vs-name`  
`gslbservicedetail`  
`gslbservicehmonstat`  
`gslbserviceinternal`  
`gslbsiteinternal`

需要使用筛选器限定上面的前三个选项，如以下命令中所示：

```
show virtualservice dns-vs-name gslbservicehmonstat filter gs_ref gslb-svc-namev
```

`gslbservicedetail` 和 `gslbserviceinternal` 选项还显示 GSLB 池成员的位置信息。

## 可用的日志

在向 NSX Advanced Load Balancer 支持部门寻求帮助时，请收集以下日志：

- 在 `/var/log/upstart` 目录中：`glb_mgr.log` 和 `*portal *.log`
- 在 `/opt/avi/log` 目录中：`glb_mgr.log` 和 `*portal *.log`
- 在运行 DNS 虚拟服务的 SE 上，收集 `se_trace.info`。

## 故障排除步骤

- 要从客户端的角度验证是否正确运行，请检查 NSX Advanced Load Balancer 日志。
- 如果 DNS SE 没有足够的内存以托管 Geo-DB，则会生成 SE 事件 `SE_GEO_DB_FAILURE`。如果发生这种情况，管理员必须修改 SE 组属性以重新调整 SE 大小，然后重新启动 SE。
- 以下 `show` 命令的筛选器现在支持 `v4` 和 `v6` 类型的地址：

- `show virtualservice g-dns-2 geolocationinfo <filter ip|start_ip>`
- `show virtualservice g-dns-2 geolocationinfo filter type [v6 | v4]`

---

### 注

- 根据选择的类型，将显示相应的 `v4` 或 `v6` 输出。
  - 每次显示 250 个 IPv6 地址条目和 1000 个 IPv4 地址条目。
- 

## 错误场景

本节介绍了以下错误场景：

- 从属站点升级失败
- 主站点升级失败

### 从属站点升级失败

如果从属站点升级失败，它最终导致 GSLB 中断。该站点将回滚到以前的版本并恢复启动。在 GSLB 主站点上，禁用维护模式。在确定失败原因并解决该问题后，继续执行升级过程。

### 主站点升级失败

在主站点上，禁用维护模式。确定原因并解决该问题。在此期间，无法启用任何新功能。

## 故障场景和解决办法

GSLB 部署发生故障后的 NSX Advanced Load Balancer 行为取决于故障发生在

- 1 主站点还是某个从属站点
- 2 整个站点还是仅 NSX Advanced Load Balancer 控制器

### 从属站点故障

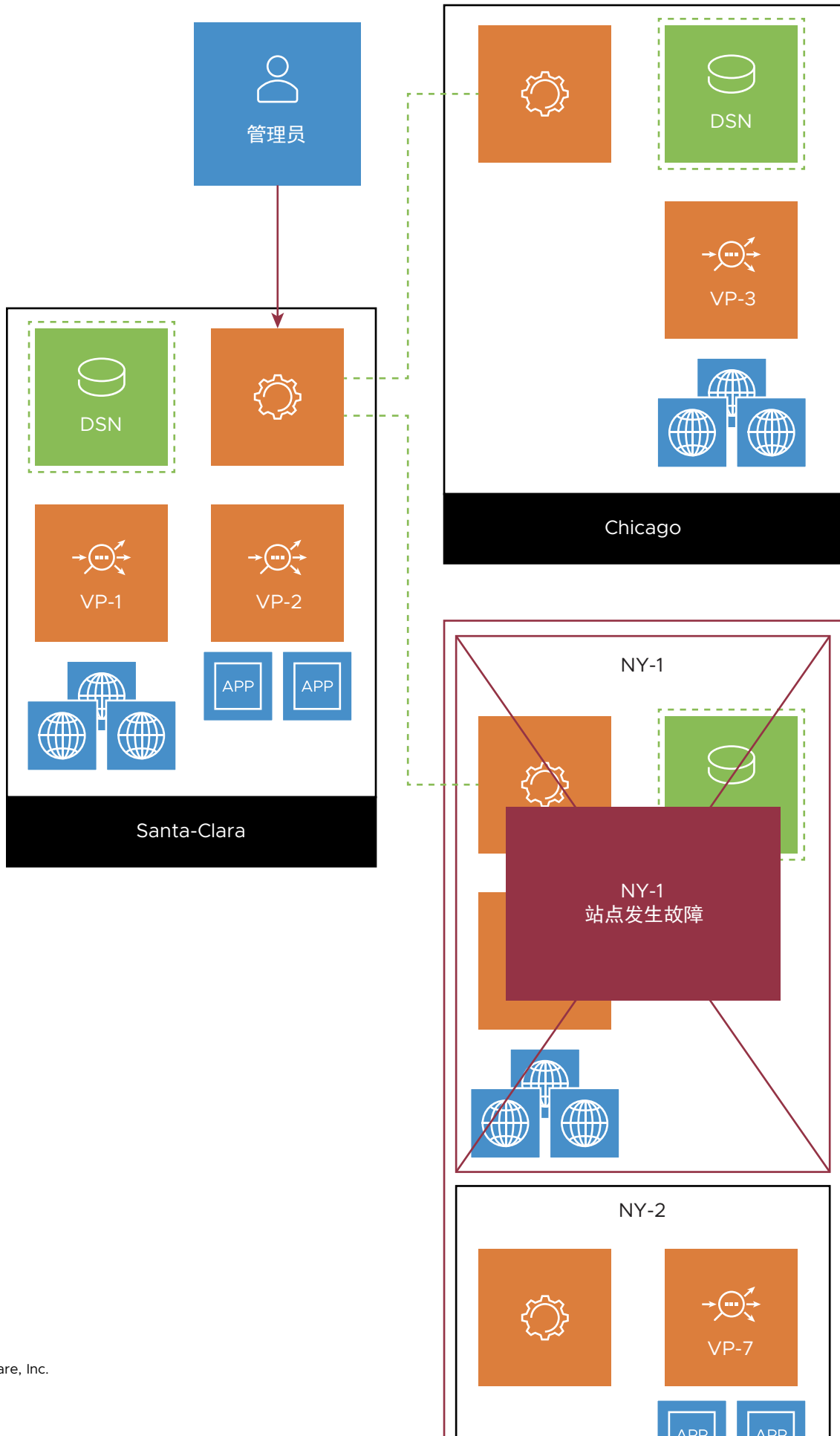
---

**注** 在我们的从属站点故障示例中，我们专注于 Santa Clara、Chicago 和 New York 中部署的基础架构。

---

#### 全站点故障

在 NY-1 从属站点中发生全站点故障，如下所示。



- 2 可以在主站点上继续对 GSLB 配置进行管理更改，但它们不会传播到 NY-1 站点。
- 3 控制平面和数据平面运行状况监控器将 NY-1 的 GS 成员标记为关闭。有关更多详细信息，请参阅 [NSX Advanced Load Balancer GSLB 服务和运行状况监控器](#)。
- 4 GSLB 配置的 DNS 服务在两个正常运行的站点中保持运行。
- 5 全局应用程序服务将在正常运行的站点（Santa Clara、Chicago 和 NY-2）上继续运行。

### 部分站点故障

如果仅 NY-1 站点中的 NSX Advanced Load Balancer 控制器发生故障，SE 继续以无控制器模式为应用程序提供服务。

- 1 Chicago 控制器（主控制器）使用其控制平面监控器检测该故障。
- 2 在主站点上进行的任何管理更改不会传播到 NY-1 站点。
- 3 在 Santa Clara 和 Chicago 中运行的数据平面运行状况监控器继续将 NY-1 的成员检测为已启动。
- 4 GSLB 配置的 DNS 服务在所有三个站点中保持运行（因为它来自于 SE，三个站点均未发生故障）。
- 5 全局应用程序服务继续在所有 4 个站点（Santa Clara、Chicago、NY-1 和 NY-2）上运行。

### 从属站点恢复

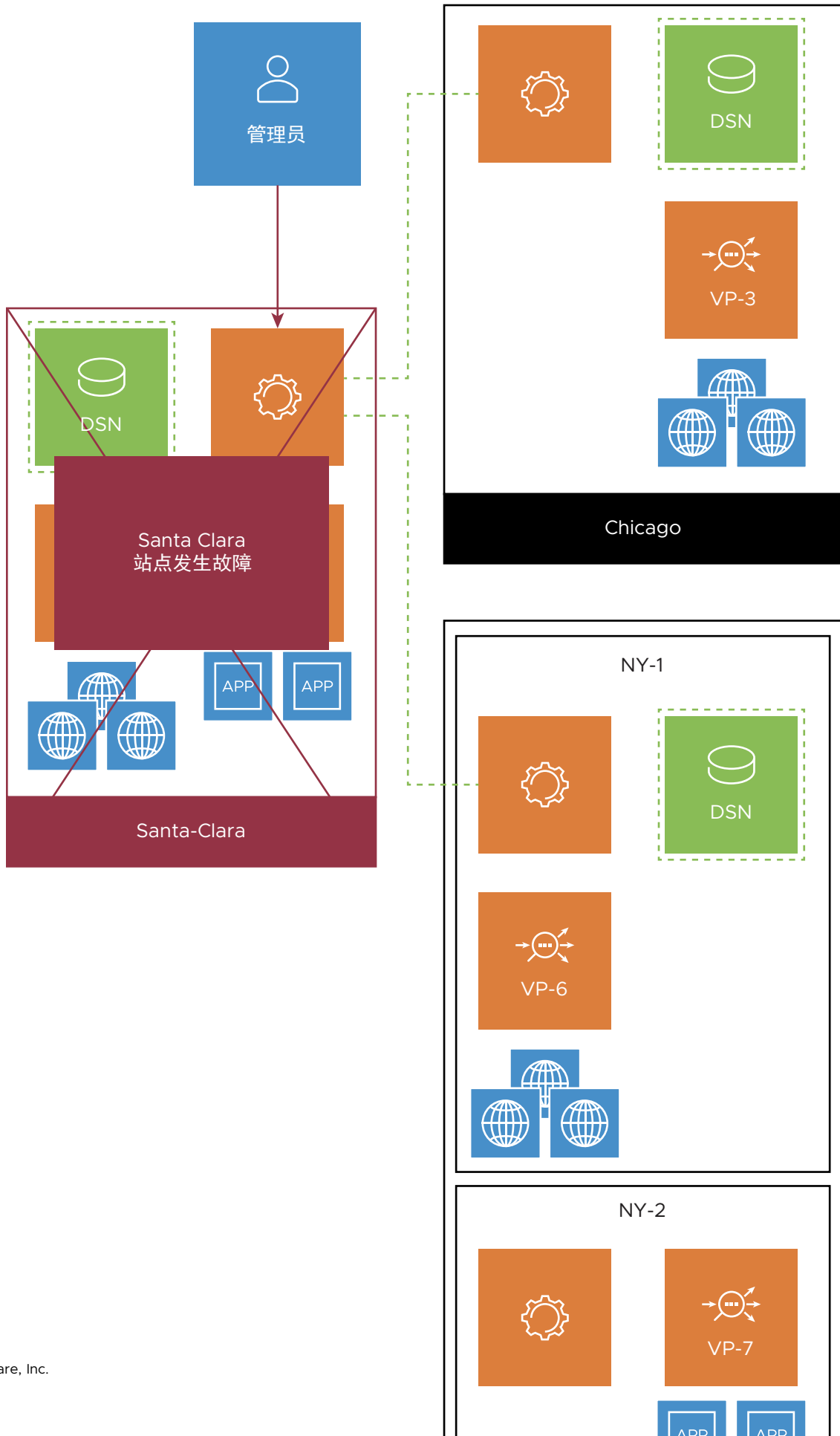
以下情况适用于全站点或部分站点故障。

- 1 Santa Clara 中的主控制器检测是否连接到 NY-1 中的（新重新引导的）从属控制器。最新的 GSLB 配置将推送到该站点。
- 2 其他主动站点同样通过其控制平面运行状况监控器检测是否成功连接到 NY-1 从属控制器。
- 3 如果数据平面从未关闭（部分站点故障），则无需执行其他操作。
- 4 如果已配置 NY-1 的 GS 成员的数据平面监控器，并且监控器以前将 NY-1 的 GS 成员标记为关闭，NY-1 的成员将标记为启动，只有在这些数据平面监控器再次检测到良好运行状况后才会恢复到它们的流量。

## 主站点故障

### 全站点故障

在 Santa Clara 主站点中发生全站点故障，如下所示。



- 2 无法对 GSLB 配置进行管理更改。
- 3 控制平面和数据平面运行状况监控器将 Santa Clara 的 GS 成员标记为关闭。
- 4 GSLB 配置的 DNS 服务在两个正常运行的主动站点（Chicago 和 NY-1）中保持运行。
- 5 全局应用程序服务继续在三个正常运行的站点（Chicago、NY-1 和 NY-2）上运行。

### 部分站点故障

如果仅 Santa Clara 站点中的 NSX Advanced Load Balancer 控制器发生故障，该站点的 SE 继续以无控制器模式为应用程序提供服务。

- 1 由于 Chicago 和 NY 是主动站点，它们都会使用其控制平面运行状况监控器检测控制器故障。
- 2 无法对 GSLB 配置进行管理更改。
- 3 在 Chicago 和 NY 中运行的数据平面运行状况监控器继续将 Santa Clara 的成员检测为已启动。
- 4 GSLB 配置的 DNS 服务在 Santa Clara、Chicago 和 NY-1 中保持运行。
- 5 全局应用程序服务将继续在所有站点上运行。

### 站点配置错误

在保存站点信息时，显示与 IP 地址和凭据相关的站点配置错误。一些示例错误屏幕如下所示：

### 身份验证失败

Boston 站点管理员的用户名和密码可能是该站点特有的，也可能在所有 NSX Advanced Load Balancer GSLB 站点中使用相同的凭据。

The screenshot shows a web form titled "New GSLB Site" with a close button (X) in the top right corner. At the top, there is an orange error message box containing the text: "LOG:(u'Authentication failed with code 401 reason msg: {'error': 'Incorrect username/password'});)". Below the error message, the form has several input fields:

- Name \***: A text input field containing "Boston".
- Username \***: A text input field containing "admin".
- Password \***: A password input field (masked with dots) containing "...".
- IP Address \***: A text input field containing "10.160.0.20".
- Port \***: A text input field containing "443".

### 登录失败达到最大重试次数

经过适当验证的个人登录到主站点以执行与 GSLB 相关的功能，例如读取 GSLB 配置或对其进行更改。此外，在后台，主 GSLB 站点自动登录到从属 GSLB 站点，以传送只能从主站点中启动的配置更改。在这两种情况下，登录尝试锁定规则可能会生效，其中一定次数的失败导致将管理帐户锁定指定的分钟数（默认值为 30 分钟）。

New GSLB Site

LOG:(MaxRetryError("HTTPSConnectionPool(host='10.160.0.21', port=443): Max retries exceeded with url: /login (Caused by NewConnectionError(<requests.packages.urllib3.connection.VerifiedHTTPSConnection object at 0x7f1703d14350>: Failed to establish a new connection: [Errno 111] Connection refused.'))",))

Name\*

Boston

Username\*

admin

Password\*

...

IP Address\*

10.160.0.21

Port\*

443

## 纠正

在定义新的 GSLB 配置或将 GSLB 站点添加到现有配置时，用户需要指定与该站点关联的帐户凭据。最佳做法是为所有参与的 GSLB 站点定义相同的 GSLB 管理帐户（例如 `gslbadmin`）。通过将 `No-Lockout-User-Account-Profile` 与该帐户相关联（如下所示），用户可以消除登录失败达到最大重试次数的情况。

要将自动操作与 GSLB 管理员个人的操作分开跟踪，请为管理员分配不同的单独 ID。

Edit User Profile: No-Lockout-User-Account-Profile

Name\*

No-Lockout-User-Account-Profile

Max Password History Count?

0

Account Lock Timeout?

30

minutes

Credentials Timeout Threshold?

0

days

Max Login Failure Count?

0

Max Concurrent Sessions?

0

Number of login attempts before lockout.  
Default is 3 attempts.

## HTTP 400 错误

在一些 GSLB 上下文中，可能会发生 400 错误。该特定示例说明了一种可以理解的限制：一个 NSX Advanced Load Balancer 站点恰好可以参与一个 GSLB 配置。将拒绝加入第二个配置的邀请。



## New GSLB Site ✕

LOG:(u'HTTP Error: 400 Error Msg ("error": "Site cluster-005056ad0f37 is member in another Group glb-1"), <Response [400]>)

Name\* ?  
Boston

Username\* ?  
admin

Password\* ?  
\*\*\*\*\*

IP Address\* ?  
10.160.0.20

Port\* ?  
443

+ Add IP Address

VMware, Inc.

153

本节介绍了常见用例的以下配置：

- NAT 感知公用-专用 GSLB 配置
- GSLB 通配符 FQDN

本章讨论了以下主题：

- NAT 感知公用-专用 GSLB 配置
- GSLB 通配符 FQDN

## NAT 感知公用-专用 GSLB 配置

NSX Advanced Load Balancer GSLB 配置可以为来自混合的公用和专用网络的客户端提供服务。

### 简介

本地虚拟服务（配置为 GSLB 池成员）中配置的 VIP 是专用 IP 地址。但是，客户端可能无法始终访问该 IP 地址。例如，笔记本电脑用户可能使用企业 Intranet 或 VPN 进行连接，也可能直接从公用 Internet 进行连接。在前一种情况下，源 IP 地址是 Intranet 专用 IP 地址。在后一种情况下，它是一个公用 IP 地址。

---

**注** 如果启用了 EDNS 处理，将会在 ECS 选项中找到客户端的 IP 地址。有关更多详细信息，请参阅[插入 DNS 的扩展机制 \(EDNS\) 客户端子网选项](#)。

---

源是一组特定的解析器 IP 地址可能表明客户端来自专用网络，而另一组 IP 地址可能表明客户端来自公用网络。

### 工作方式

来自 Intranet 内部的客户端 DNS 请求在 A 记录中提供专用 IP，而来自外部的请求提供公用 IP 地址。请注意，仅针对专用 IP 地址执行数据路径运行状况监控。

## 使用 NSX Advanced Load Balancer UI 进行配置

在 GSLB 全局配置（导航到[基础架构 > GSLB > 编辑](#)）中，用户可以指定一个 IP 地址列表（特定地址、范围或前缀），并将其划分为专用或公用地址。请参阅下面的屏幕截图。如果指定了专用地址列表，则将所有其他地址视为公用地址，反之亦然。

## Edit GSLB Configuration ✕

GSLB Subdomain ?

avi.com

✕

GSLB Subdomain ?

avi.us

✕

+ Add GSLB Subdomain

Client Group IP Address Type

Public

▼

3.1.1.1

✕

2.1.1.0-2.1.2.255

✕

1.1.1.0/24

✕

+ Add Group IP Address

Save

在 GSLB 池成员配置中，可以指定一个可选的公用 IP 地址。该字段用于托管 VIP 的公用 IP 地址，防火墙将其转换为专用 IP。请参阅下面的屏幕截图。

**Edit GSLB Pool**

SI

Priority\* ? 12

LB Algorithm\* ? Geo

**Pool Member**

☒ IP Address ☐ Virtual Service

IP Address or FQDN\* ? 10.10.10.2

Third-party Site Cluster Controller ? Select Site

Public IP Address ? 1.1.1.1

Ratio\* ? 1

☒ Enabled ?

Add GSLB Pool Member

Done

## 使用 NSX Advanced Load Balancer CLI 进行配置

在下面的 CLI 序列中，定义了专用和公用地址范围。

```
configure gslb glb-1
client_ip_addr_group

type gslb_ip_p
gslb_ip_private Private IP Address.
gslb_ip_public Public IP Address.
type gslb_ip_public
prefixes 1.1.1.0/24
addrs 2.1.1.1
ranges begin 3.3.3.0 end 3.3.3.42
New object being created
save
save
save
...
```

```

client_ip_addr_group
type                GSLB_IP_PUBLIC
addrs[1]            2.1.1.1
ranges[1]
begin               3.3.3.0
end                 3.3.3.42
prefixes[1]         1.1.1.0/24
tenant_ref          admin
-----+

```

在下面的 CLI 序列中，将一个公用 IP 地址添加到现有池成员中。

```

configure gslbservice gs-1
Updating an existing object. Currently, the object is:
groups index 1
members index 1
public_ip ip 2.2.2.2
save
save
save
save
...
members[1]
ip          10.10.10.1
ratio      1
enabled    True
public_ip
ip          2.2.2.2

```

## GSLB 通配符 FQDN

通常，NSX Advanced Load Balancer GSLB 服务仅配置了一个 FQDN。如果多个 FQDN 表示同一 GSLB 服务，将在 NSX Advanced Load Balancer 上配置这些域的通配符。

### 用例

配置了 FQDN 的通配符匹配以满足以下要求：

- foo.com 是委派给 NSX Advanced Load Balancer 的子域
- t1.test.finance.foo.com、t2.test.finance.foo.com、m1.test.finance.foo.com 等指向同一应用程序或作为同一应用程序的前端

要实现上述要求，请为 test.finance.foo.com 添加一个 GSLB 服务，并启用通配符选项以指示与 \*.test.finance.foo.com 匹配的任何 FQDN 传送到一组相同的应用程序。

## 使用 NSX Advanced Load Balancer CLI 配置通配符匹配

登录到 NSX Advanced Load Balancer CLI，然后使用 `configure gslbservice <gslb service name>` 命令启用 `wildcard_match` 标记。

```
[admin:10-10-25-10]:configure gslbservice gsvc-5
[admin:10-10-25-10]: > TAB
wildcard_match Enable wildcard match of FQDN: If an exact match is not found in the DNS
table, the longest match is chosen by wildcarding the FQDN in the DNS request. Default is
false.
[admin:10-10-25-10]: gslbservice> wildcard_match
Overwriting the previously entered value for wildcard_match
[admin:10-10-25-10]: gslbservice> save
```

仅支持使用 CLI 执行上述操作。

类似地，也可以按通配符标识静态 DNS 记录。

```
[admin:10-10-25-10]: virtualservice:static_dns_records>
wildcard_match Enable wild-card match of FQDN: If an exact match is not found in the DNS
table, the longest match is chosen by wildcarding the FQDN in the DNS request. Default is
false.
[admin:10-10-25-10]: virtualservice:static_dns_records> save
```

### 场景 1

- 子域名是 `foo.com`
- 应用程序域名是 `demo.foo.com`

满足上述要求的通配符选项是，将 `*.demo.foo.com` 作为通配符选项，如下所示：

```
[admin:testcontroller-2]: > configure gslbservice gsl
[admin:testcontroller-2]: gslbservice> domain_names demo.foo.com
[admin:testcontroller-2]: gslbservice> wildcard_match
Overwriting the previously entered value for wildcard_match
[admin:testcontroller-2]: gslbservice> save
```

#### 注

- `domain_names: demo.avi.com`：也可以从 GUI 中配置该应用程序域名
- `gslbservice> wildcard_match`：用于启用通配符的标记

### 场景 2：子域本身的通配符

如果需要使用子域本身的通配符（即 `*.foo.com`），请从 NSX Advanced Load Balancer CLI 中配置应用程序域名并启用通配符匹配，如下所示。

```
[admin:testcontroller-2]: > configure gslbservice gsl
[admin:testcontroller-2]: gslbservice> domain_names foo.com
[admin:testcontroller-2]: gslbservice> wildcard_match
```

```
Overwriting the previously entered value for wildcard_match  
[admin:testcontroller-2]: gslbservice> save
```

## 注

- 应用程序域名: foo.com
- 无法使用 NSX Advanced Load Balancer UI 配置此类域名。

## 配置 DNS 静态记录

也可以从 NSX Advanced Load Balancer UI 中配置静态记录。导航到[应用程序 > 虚拟服务](#)，然后单击[静态 DNS 记录](#)。

FQDN\* ?

FQDN

Type\* ?

A

TTL ?

TTL

A Record

IP Address\* ?

IP Address

+ Add A record IP Address

Advanced Settings

Number of records in response ?

0

Algorithm ?

Round Robin

☐ Enable wild-card match ?

☐ Delegated domains ?

# 额外的集成

# 7

本节介绍了以下内容：

- GSLB 与 F5 GTM 的集成
- AWS 多区域、多可用区部署中的 NSX Advanced Load Balancer GSLB
- Azure DNS 专用区域中的 GSLB

本章讨论了以下主题：

- [GSLB 与 F5 GTM 的集成](#)
- [AWS 多区域、多可用区部署中的 NSX Advanced Load Balancer GSLB](#)
- [Azure DNS 专用区域中的 GSLB](#)

## GSLB 与 F5 GTM 的集成

为了确保跨地理区域或数据中心的高可用性，NSX Advanced Load Balancer 建议使用多个数据中心以分散风险并减少故障域。NSX Advanced Load Balancer 适用于大多数 GSLB 解决方案，但集成级别取决于使用的供应商。

这在以下部署中是非常有用的：具有来自其他供应商的 GSLB，它们在地理位置之间提供基于 DNS 的负载均衡。有关配置 NSX Advanced Load Balancer 的 GSLB 功能的更多详细信息，请参阅 [第 3 章 GSLB 配置](#)。

## 假设

本节的范围涵盖 NSX Advanced Load Balancer 与 F5 GTM 的集成。

以下是假设：

- NSX Advanced Load Balancer 安装在一个或多个数据中心
- 安装了 F5 的 BIG-IP GTM

GTM 可能安装在 NSX Advanced Load Balancer 提供本地应用程序交付服务的同一数据中心，也可能安装在不同的数据中心。



## 配置 NSX Advanced Load Balancer

通过 GSLB 进行负载均衡的虚拟服务不需要使用特殊配置。虚拟服务可能位于单个 NSX Advanced Load Balancer 控制器集群上，也可能位于不同数据中心的多个控制器集群中。

### 在 F5 上创建 GTM 池

导航到 **DNS > GSLB > 池**。选择**创建**并配置以下字段：

#### 名称

输入 GTM 池的名称。

#### 运行状况检查

应用适合应用程序类型的运行状况监控器。

#### TCP 监控器

如果使用基本 TCP 运行状况监控器，则建议对 NSX Advanced Load Balancer 虚拟服务进行额外的配置更改。从 NSX Advanced Load Balancer UI 中，编辑所需的虚拟服务并导航到**高级**选项卡。在虚拟服务关闭时，启用**移除侦听端口**。如果未启用该选项（默认），则 NSX Advanced Load Balancer 接受 TCP 连接，然后发送重置。GTM 将该虚拟服务标记为启动，即使它收到了重置。如果启用了该选项，则 NSX Advanced Load Balancer 不接受连接，这会确保在 GTM 上将关闭的虚拟服务正确标记为关闭。

#### 成员列表

从**虚拟服务器**下拉菜单中，从列表中选择相应的虚拟服务，然后单击**添加**。在以前的“创建 LB”步骤中，应该添加了虚拟服务。

### 在 F5 上创建 GTM WideIP

导航到 **DNS > GSLB > WideIP**。单击**创建**并配置以下字段：

#### 名称

输入应用程序的 FQDN。

#### 池列表

将 GTM 池添加到列表中。

### 在 F5 上创建负载均衡器服务器对象

首先，必须将 NSX Advanced Load Balancer 作为负载均衡器对象添加到 GTM 中。从 GTM GUI 中，导航到 **DNS > GSLB > 服务器**，然后选择**创建**。在“常规属性”部分中配置以下字段：

#### 名称

唯一的 NSX Advanced Load Balancer 实例名称，例如“NSX Advanced Load Balancer\_DC1”。

#### 产品

通用负载均衡器。

### 地址

对于建议的配置，GTM 从不使用该 IP 地址。尽管如此，该字段必须具有一个值，因此，输入集群中的 NSX Advanced Load Balancer 控制器的任何 IP 地址，然后单击**添加**。

### 数据中心

选择预配置的 GTM 数据中心对象，例如“DataCenter1”。GTM 使用该信息以确定哪个设备将向 NSX Advanced Load Balancer 发送运行状况检查。

在“配置”部分中：

### 运行状况监控器

建议将运行状况监控器字段保留空白。添加运行状况检查以验证对 NSX Advanced Load Balancer 的访问是可选的。这涉及到 GTM 向 NSX Advanced Load Balancer 控制器 IP 地址发送查询。默认情况下，建议不要进行这种额外的检查，因为它要求 GTM 能够访问控制器，这些控制器通常位于受保护的管理网络上。如果需要进行该检查，NSX Advanced Load Balancer 服务器对象的地址和转换地址必须正确无误。用于检查对 NSX Advanced Load Balancer 控制器的访问的运行状况监控器是使用“运行状况监控器”设置添加的。请记住，访问控制器并不反映能够成功访问应用程序虚拟服务。

在“资源”部分中，每个虚拟服务必须添加到 NSX Advanced Load Balancer 服务器对象中：

### 名称

虚拟服务的名称。

### 地址

VIP 的 IP 地址。

### 服务端口

用于访问虚拟服务的端口。

### 转换

如果在 NSX Advanced Load Balancer 和客户端之间转换了虚拟服务，请输入客户端应访问的公用 IP 地址。

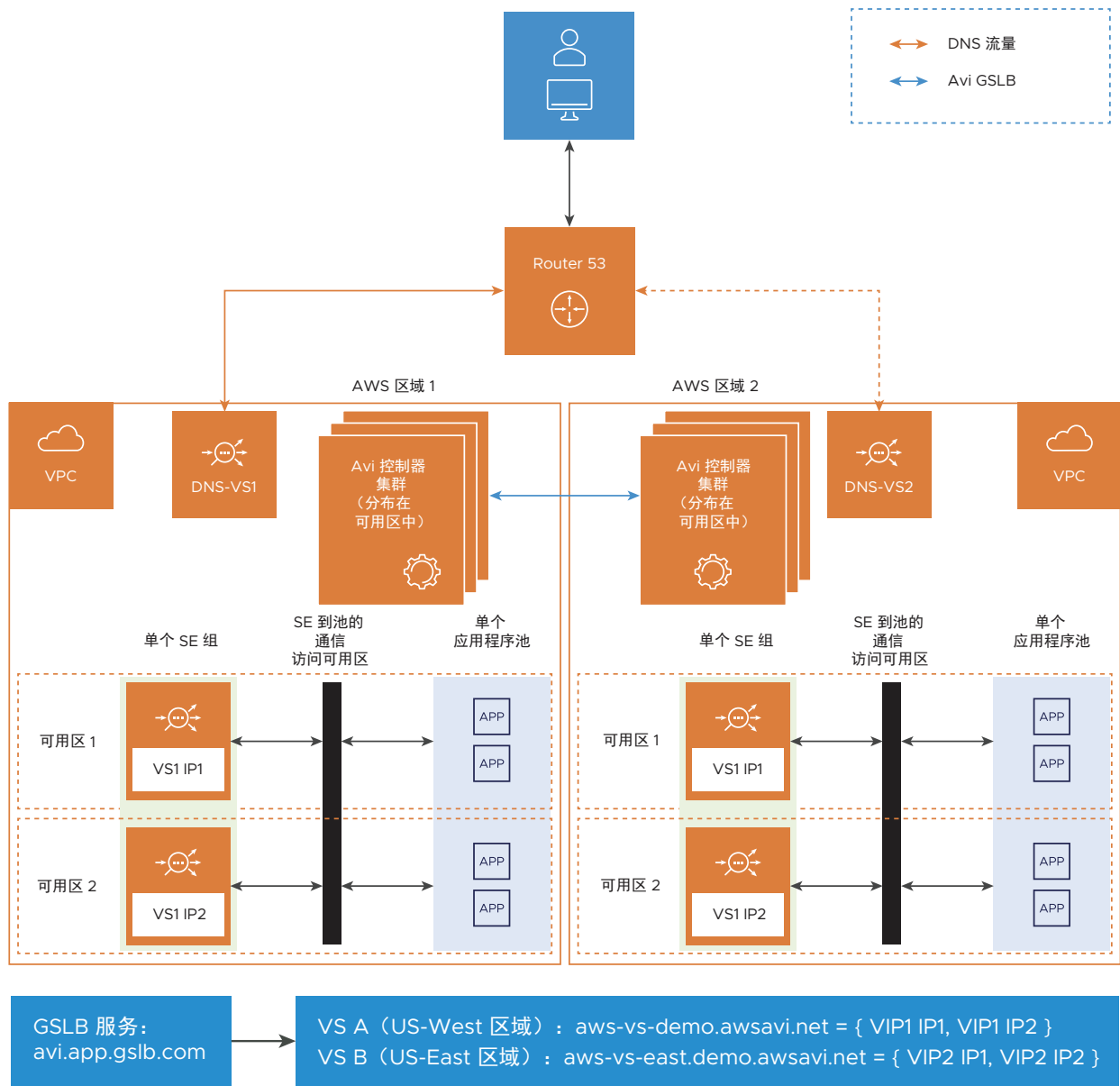
### 转换端口

如果在 NSX Advanced Load Balancer 和客户端之间转换了虚拟服务（更改了端口），请输入客户端应访问的公用端口。

## AWS 多区域、多可用区部署中的 NSX Advanced Load Balancer GSLB

“AWS 的多可用区支持”一节重点介绍了单个应用程序（即虚拟服务）如何跨多个 AWS 可用区 (Availability Zone, AZ)。通过使用单个 SE 组，NSX Advanced Load Balancer 将 VIP 放置在每个可用区中运行的 SE 上。多 VIP 功能对跨多个可用区的应用程序后端服务器进行负载均衡。

相比之下，本节介绍了一个场景，其中多个应用程序实例跨多个 AWS 区域中的多个可用区 (AZ)，并且 NSX Advanced Load Balancer GSLB 在区域之间进行流量负载均衡。结果是，最佳用户体验基于远近程度和高可用性。



## 配置

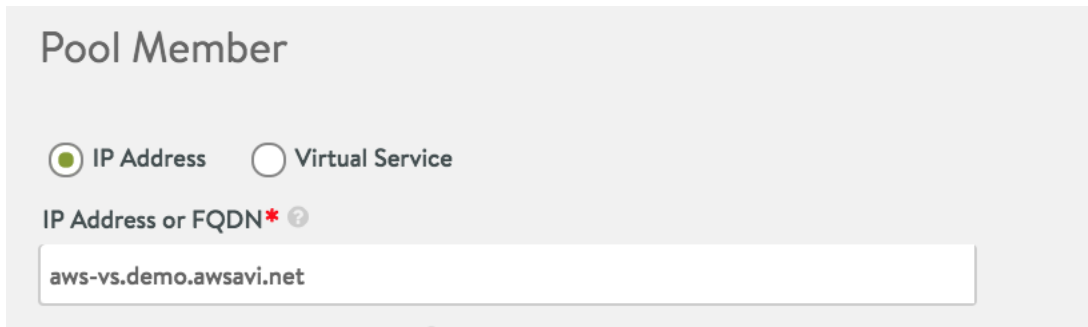
初始配置步骤类似于此处提到的步骤。不同之处在于配置 GSLB 服务的方式。在本节中，我们介绍了两种为该场景配置 GSLB 服务的方法。

## 方法 1

按照以下步骤为上述场景配置 GSLB 服务：

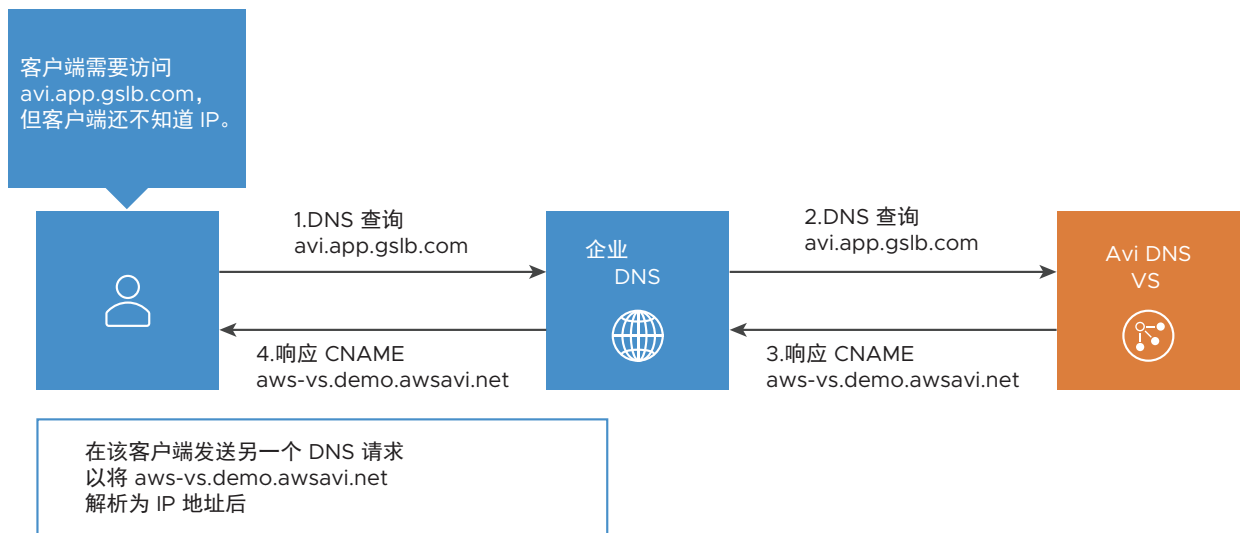
- 使用 IP 地址选项配置 GSLB 池成员。

- 指定多个 VIP 的 FQDN。正如下面的屏幕截图所示，FQDN 是 `aws-vs.demo.awsavi.net` 或 `aws-vs-east.demo.awsavi.net`。



- 正如上面的屏幕截图所示，池成员配置了 FQDN。
  - FQDN 解析为控制器上的 IP 地址。
  - DNS 虚拟服务监控解析的地址的运行状况，同时在其响应中返回 CNAME。
  - 如果用户配置了一个 IP 地址，只要控制器完成了定期 FQDN 刷新，就会覆盖该 IP 地址。
  - 仅监控其中的一个 IP，而不是监控所有 IP。NSX Advanced Load Balancer 控制器或 AWS 撤销未启动的 IP 地址/成员。


## 请求流




- 1 客户端发送请求以访问 `avi.app.gslb.com`。
- 2 请求发送到 NSX Advanced Load Balancer DNS 虚拟服务，该服务确定最佳池成员。在这种情况下，将根据指定的 GSLB 方法选择 `aws-vs.demo.awsavi.net` 或 `aws-vs-east.demo.awsavi.net`（池成员）。
- 3 NSX Advanced Load Balancer DNS 虚拟服务在响应中提供 CNAME 以响应客户端。

Timestamp	Client IP	Protocol	DNS Request Type	Domain Name	Response
11/16 10:56:13 AM	10.140.8.155	UDP	A	avi.app.gslb.com	aws-vs.demo.awsavi.net



Client



LB

Client IP: 10.140.8.155:62725

Location: Internal

DNS Query Type: A

Domain Name: avi.app.gslb.com

ID: 61711

RX Bytes: 87 B

TX Bytes: 112 B

Start time: 2018-11-16, 10:56:13 am

Virtual Service IP: 10.130.150.200:53

GSLB Service Name: AWS\_az

GSLB Pool Name: aws\_az\_pool

Service Engine: AvDNSAdmin-se-sofm (vcpu 0)

Record Source: GSLB

Opcode: QUERY

Records:

Type: CNAME, Name: aws-vs.demo.awsavi.net TTL: 1

Response Code: NOERROR

Authoritative: True

Truncated: False

Recursion Available: False

Recursion Desired: True

Question Count: 1

Answer Record Count: 1

Nameserver Records Count: 0

Additional Records Count: 0

Query: False

- 4 相同的 CNAME 将发送到客户端。
- 5 在客户端获得 CNAME 后，客户端根据 DNS 服务器配置发送另一个 DNS 查询以解析 CNAME。可能将 AWS 配置为子域 demo.awsavi.net 的权威 DNS，NSX Advanced Load Balancer 可能是权威的，也可能以某种其他方式配置了 DNS 设置。
- 6 CNAME 解析为各个 VIP 的 IP 地址之一（基于客户端使用的 DNS 服务器：Route 53 或 NSX Advanced Load Balancer DNS）。

在这两种情况下，多 VIP 虚拟服务的这些 FQDN（aws-vs.demo.awsavi.net 或 aws-vs-east.demo.awsavi.net）在 DNS 中自动记录/注册为指向各个 VIP 的 A 记录。例如，如果在部署云时将 Route 53 作为 DNS，则在 Route 53 上注册 FQDN，如下所示。

Infrastructure VPC/Network/Encryption

AWS VPC and Availability Zones

VPC: AVI-WEST2-VPC - 10.144.0.0/16

☒ Free Unused Elastic IP Address

Select SE Management Network for required Availability Zones

Availability Zone	SE Management Network
us-west-2a	2A-public - 10.144.0.0/24
us-west-2b	2B-ext - 10.144.64.0/24
us-west-2c	2C-ext - 10.144.128.0/24

☐ Add Availability Zone

☐ Enable Simple Queue Service (SQS) for Autoscale Groups Monitoring

☐ Allow wildcard access to SEs

DNS Settings

Register Virtual Service Names

☐ None ☒ Amazon Route 53 ☐ DNS Profile

Encryption

☐ Use Encryption for SE S3 Bucket

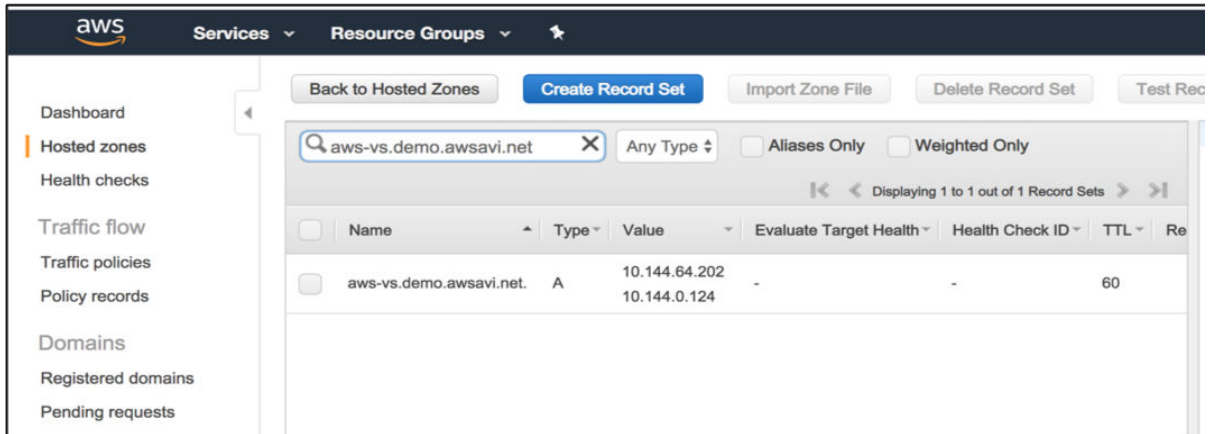
☐ Use Encryption for SE AMI/EBS volumes

Other Settings

ASG Polling Interval: 600 Sec

Custom Tag Key: Project Custom Tag Value: PMDDemoUS

Cancel Save



如果改用 NSX Advanced Load Balancer DNS，则以类似的方式在 NSX Advanced Load Balancer 中注册 FQDN。

## 方法 2

按照以下步骤为上述场景配置 GSLB 服务：

- 使用单独的 VIP IP 地址进行配置，即 VIP1 IP1、VIP2 IP2 等。

**Pool Members**

☐ IP Address ☒ Virtual Service

Site Cluster Controller\*  Virtual Service\*

Public IP Address  IP Address\*

Ratio\*  ☒ Enabled

Geo Location Source

Description

☐ IP Address ☒ Virtual Service

Site Cluster Controller\*  Virtual Service\*

IP Address\*

- 这允许为多 VIP 虚拟服务配置单独的 VIP。如果希望在 GSLB 服务中添加所有 VIP，则需要手动添加所有这些 VIP。

- 在客户端发送 `avi.app.gslb.com` 的请求时，请求先传送到 NSX Advanced Load Balancer DNS 虚拟服务，然后根据配置的 GSLB 算法选择最佳端点。
- 接下来，DNS 虚拟服务使用 VIP 的 IP 地址之一进行响应。
- 由于在该方法中明确添加了每个 VIP，因此，NSX Advanced Load Balancer 使用数据路径运行状况检查以单独监控每个成员的运行状况。

上面所述的第二种方法具有一些限制：

- 可能会在多 VIP 虚拟服务中添加新的 VIP（即，将 VS1 IP3 添加到预先存在的 2 个 IP 中）。在这种情况下，用户必须手动编辑 GSLB 服务，并将新 VIP 添加到 GSLB 池中。
- 作为多 VIP 虚拟服务，可能存在更改 VIP 的 IP 地址的情况，从而可能导致不一致，除非在 GSLB 服务中未手动更改池。

NSX Advanced Load Balancer GSLB 池成员是一个虚拟服务（具有关联的 VIP:端口号）。要配置这种成员，用户需要唯一地标识站点 ID、站点中的虚拟服务以及虚拟服务的相应 VIP。相关参数是 `GslbPoolMember` 对象中的 `cluster_uuid`、`vs_uuid` 和 `GslbPoolMember.ip`。

站点管理员更改特定虚拟服务的 NSX Advanced Load Balancer 本地配置，以使其 VIP1 从 IP2 更改为 IP4。

**情况：**虽然本地 VIP IP4 正常运行，但 GSLB 配置（还）不知道其地址；它不再作为全局应用程序的一部分进行通告；对 IP2 的引用无效。GSLB 主站点和主动成员检测 VIP (IP2) 和 VIP (IP4) 之间的差异。然后，NSX Advanced Load Balancer 禁用相关的 GSLB 池成员并通知管理员“配置的 VIP 和运行 VIP 不同步”。

有关更多详细信息，请参阅[更改 GSLB 池的本地虚拟服务成员的 VIP](#)。

为了避免这些情况，建议使用第一种方法为多 VIP 场景配置 GSLB 池成员。优点包括：

- 无需添加各个 VIP。
- 在虚拟服务级别更改 IP 时不会出现不一致。

## Azure DNS 专用区域中的 GSLB

Microsoft Azure DNS 专用区域支持在专用网络中创建可以跨多个 Azure 虚拟网络和本地 DC（使用 VPN 或 Express Route）的区域。

对于专用 DNS 区域，您可以使用自定义域名，而不是 Azure 当前提供的名称。通过使用自定义域名，您可以自定义虚拟网络架构以最符合您的组织需求。它为虚拟网络中以及虚拟网络之间的虚拟机提供名称解析。此外，您还可以使用水平分割视图配置区域名称，这允许专用和公用 DNS 区域使用相同的名称。有关更多详细信息，请参阅[将 Azure DNS 用于专用域](#)。

## Azure 中的 GSLB 的 NSX Advanced Load Balancer 集成解决方案

NSX Advanced Load Balancer 与 Microsoft Azure 合作设计了一种解决方案，以提供高可用性的最佳用户体验。该解决方案无缝地组合使用 Azure 专用 DNS 区域内的多个位置中的本地系统和服务。通过使用该解决方案，您可以在已部署到（专用 DNS 区域和本地 DC 中的）多个位置的应用程序实例之间进行负载均衡，而无需使用任何 FQDN 或公用 IP 地址。

随着网络 and 应用程序的扩展，该解决方案还有助于解决性能、恢复能力、迁移、应用程序测试等难题而无需停机，并有助于获取应用程序详细信息。

通过将 NSX Advanced Load Balancer GSLB 与 Azure 专用 DNS 区域一起部署，可以为您提供以下企业级优势：

### 不限于区域或订阅 ID

可以在同一解决方案中包含属于不同订阅 ID 或区域的虚拟网络。

### 提高了应用程序可用性

该联合解决方案监控您的端点并提供无缝故障切换，以便在查找时仅返回正常运行的服务器，从而为您的关键应用程序提供高可用性。

### 提高了应用程序性能

该解决方案将流量传送到离客户端最近的端点以提高应用程序的响应能力。

### 无需停机的服务维护

该解决方案将流量传送到备用端点，以使您能够在不停机的情况下对应用程序执行计划的维护操作。

### 为复杂的部署分配流量

可以组合使用 GSLB 方法以创建复杂且灵活的规则，以便使用两级算法根据更大和更复杂的部署的需求进行扩展。

### 弹性和自动扩展

分析驱动的扩展方法允许负载均衡器根据实时流量模式弹性地提供按需自动扩展。

### 水平分割 DNS 支持

该解决方案无缝地用于具有水平分割视图的区域。

## 功能

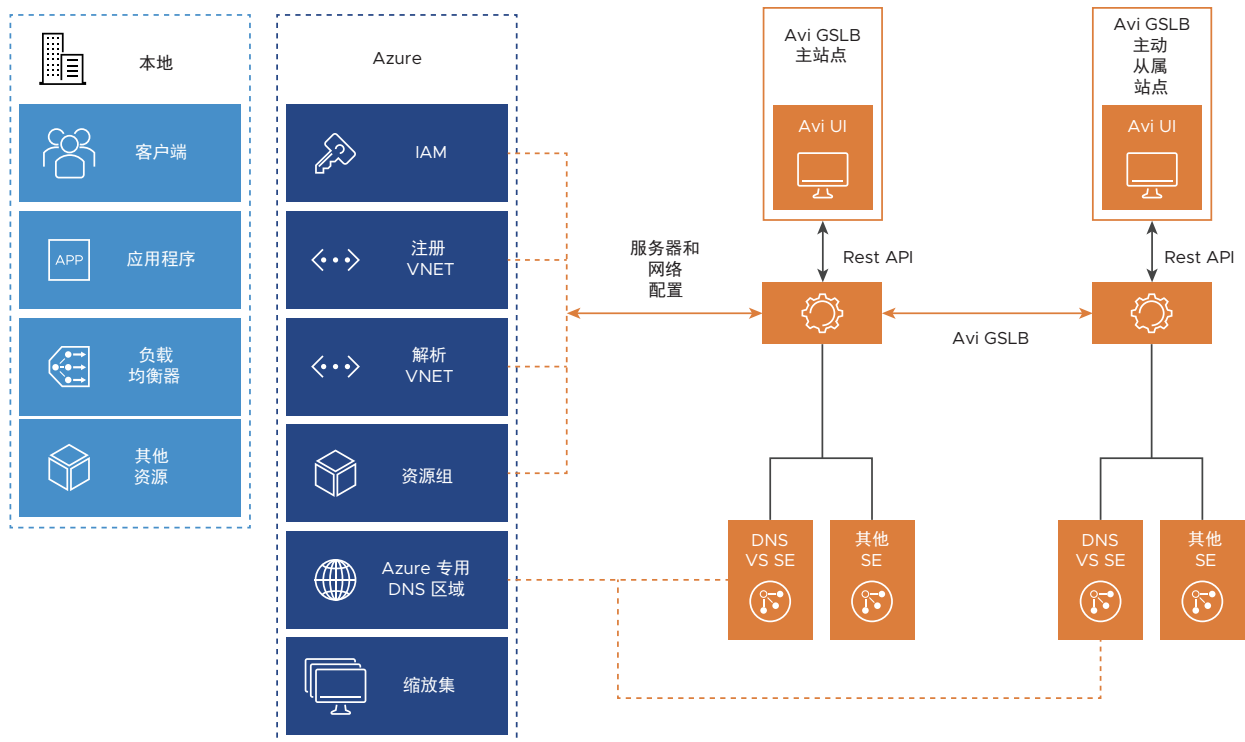
- 跨所有对等 VNet 和本地 DC 的功能。
- 提供无缝名称解析
  - 在位于同一虚拟网络中的虚拟机之间。
  - 在不同虚拟网络中的虚拟机之间。



- 适用于内部部署客户端中的 Azure 主机名。
- 提供从某个 VNet 对其他 VNet 中托管的应用程序的访问，反之亦然。此外，从 Azure VNet 中访问本地托管的应用程序，反之亦然
- 为支持 Ping、TCP、HTTP(S) 的端点提供可靠的运行状况检查以及自定义检查
- 提供基于 DNS 的无缝故障切换，而不会对生产造成任何影响
  - 如果对等组中的 VNet 关闭，则提供无缝操作，因为位于该受影响的 VNet 中的端点不会包含在任何 DNS 查询中，直到该 VNet 恢复运行
  - 确保高可用性和可靠性
- 允许选择回退到任何站点或拒绝查询
- 启用基于 DNS 的策略
- 支持使用优先级算法对新功能进行 A/B 测试，从而加快 CI/CD 部署
- 在高峰流量期间提供自动扩展功能
- 提供集中的置备功能，并跨站点自动发现应用程序
- 支持跨站点的应用程序监控、日志和分析
- 支持可自定义的 TTL
- 允许选择发送一个或多个 DNS 记录

## 主要组件

在集成中涉及的主要组件如下所示：



## NSX Advanced Load Balancer GSLB 组件

### 主站点

从中配置 GSLB 设置的站点（NSX Advanced Load Balancer 控制器集群）。

托管权威 DNS。

主动监控其他 GSLB 站点的运行状况。

### 主动从属站点

从主站点接收配置的 NSX Advanced Load Balancer 控制器集群。

通常托管权威 DNS。

主动监控其他 GSLB 站点的运行状况。

### 被动从属站点

仅托管负载均衡虚拟服务的 NSX Advanced Load Balancer 控制器集群。

- 不托管 DNS
- 不为其他站点执行运行状况监控

### 第三方站点

非 NSX Advanced Load Balancer 站点，通常是负载均衡器应用程序，例如 Azure 应用程序网关。

仅提供第三方 VIP:端口。

NSX Advanced Load Balancer 主站点/主动从属站点将为每个第三方站点执行运行状况监控。

### GSLB 服务

全局应用程序的表示形式。用作多个站点中部署的应用程序的前端。

### GSLB 池

将虚拟服务合并为单个实体，并在它们之间进行负载均衡。

### GSLB 池成员

组成 GSLB 池的虚拟服务称为 GSLB 池成员。可以按以下内容指定成员：

- NSX Advanced Load Balancer 虚拟服务名称
- IP 地址：用于指定由第三方负载均衡器定义的单独服务器或 VIP

### GSLB 运行状况监控器

支持 Ping、TCP、UDP、DNS 和 HTTP(S) 运行状况监控器。

此外，您还可以使用[外部运行状况监控器](#)选项编写和合并监控器。

有关更多详细信息，请参阅[GSLB 运行状况监控器](#)。

## Azure 专用区域组件

该服务可以与 DNS 服务器（例如上面拓扑中显示的 NSX Advanced Load Balancer DNS 虚拟服务）结合使用以解析本地和 Azure 主机名。我们可以在同一云服务中的虚拟机和角色实例之间使用名称解析，而无需使用 FQDN。

### 注册虚拟网络

如果在创建专用区域或以后更新该区域时将一个虚拟网络指定为注册虚拟网络，Azure 将在专用区域中为该虚拟网络中的虚拟机动态注册 DNS A 记录。这会跟踪在虚拟网络中添加或移除虚拟机的情况，以将专用区域保持更新状态。这是自动完成的，无需进行任何干预。

### 解析虚拟网络

您还可以在创建或更新专用区域时将最多 10 个虚拟网络指定为解析虚拟网络。转发 DNS 查询将针对其中的任何虚拟网络中的专用区域记录进行解析。

## DNS 虚拟机转发器

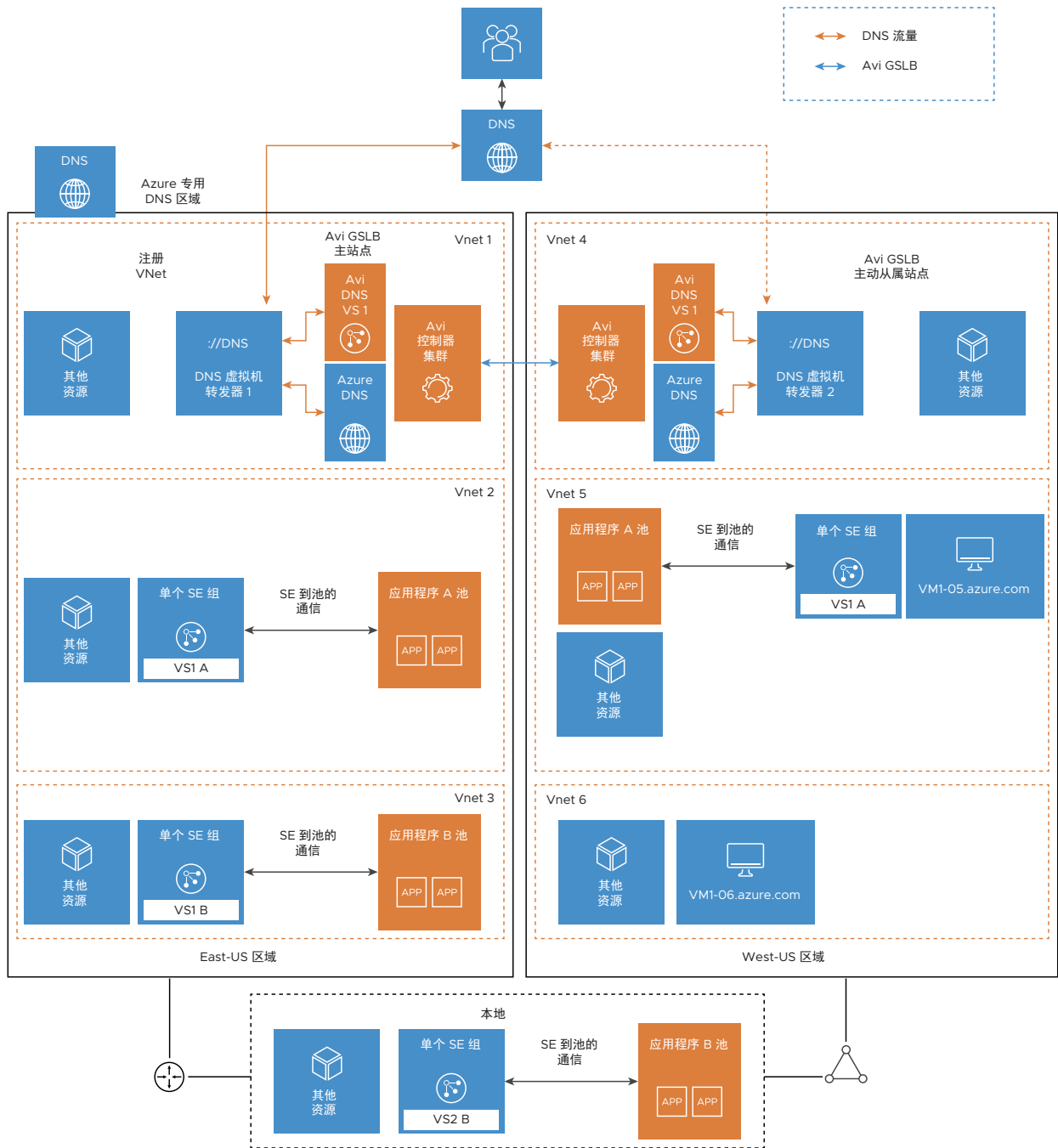
DNS 虚拟机转发器是 Azure 上托管的 BIND DNS 服务器。部署该转发器是为了根据子域有条件地转发 DNS 查询。这是 \*.azure.com 的所有入站请求的第一个联系点。在 DNS 转发器收到请求后，它检查 FQDN 名称，并根据规则将请求转发到 Azure DNS 或 NSX Advanced Load Balancer DNS 虚拟服务。NSX Advanced Load Balancer DNS 虚拟服务将处理与 GSLB 需要处理的应用程序相关的所有流量。Azure DNS 将处理所有内部主机名解析。例如，对于 azure.com 区域，配置了两个 DNS 虚拟机转发器以将请求从 gslb.azure.com 转发到 NSX Advanced Load Balancer DNS 和 Azure DNS。

---

### 注

- 您可以配置多个 DNS 虚拟机转发器。
  - 如果您计划托管 NSX Advanced Load Balancer DNS 虚拟服务，建议在相同的 VNet 中配置转发器。（请参阅上面提供的示例拓扑）
  - DNS 虚拟机转发器 IP 地址需要配置为 Azure 中的所有 VNet 的自定义 DNS。同样，需要在企业 DNS 上为本地客户端配置该地址。
-

## 示例拓扑



### 拓扑细节:

- 两个 NSX Advanced Load Balancer GSLB 站点 - 一个站点位于 Azure Vnet1 (GSLB 主站点) 中，另一个站点位于 Vnet4 (NSX Advanced Load Balancer GSLB 主动从属站点) 中。
- 一个本地 DC 使用 Express Route/VPN 网关连接到 Azure VNet。
- 客户端计算机可能位于本地或 Azure 中。
- 将 Azure 中的多个 VNet (注册和解析) 作为专用 DNS 区域的一部分。

- 必须能够从 Azure VNet 中访问位于本地的应用程序（应用程序 B）。
- 应该能够从本地客户端以及 Azure 上的客户端（同一 VNet 以及其他 VNet）中访问位于 Azure 中的应用程序（应用程序 A）。
- Azure 中托管的虚拟机应具有 VNet 间和 VNet 内通信。

## 注意事项

### NSX Advanced Load Balancer 控制器和 GSLB

- 不需要在所有 VNet 和位置中具有 NSX Advanced Load Balancer 控制器/GSLB 站点。
- GSLB 站点可以位于本地和/或 Azure 中。
- 一个 GSLB 站点/NSX Advanced Load Balancer 控制器可以执行所有 GSLB 功能。在这种情况下，在站点正常运行之前，无法执行其他 GSLB 配置。因此，如果需要，建议将至少两个站点指定为主站点和主动从属站点以进行任何 GSLB 配置更改。有关更多详细信息，请参阅 [使用 NSX Advanced Load Balancer UI 配置 GSLB 站点](#)。

### 云

在 NSX Advanced Load Balancer 控制器上创建不同的云，以便为每个 VNet 的一个云指定网络和位置详细信息。有关更多详细信息，请参阅[适用于 Microsoft Azure 的 NSX Advanced Load Balancer 部署指南](#)。

## NSX Advanced Load Balancer SE

NSX Advanced Load Balancer SE 将部署在对资源和应用程序进行负载均衡的所有 VNet 中。

- DNS 虚拟服务可以部署在两个或三个 VNet 中，具体取决于部署规模和流量大小。并非所有 VNet 都需要使用 NSX Advanced Load Balancer DNS 虚拟服务。对于本文中介绍的拓扑，NSX Advanced Load Balancer DNS 虚拟服务部署在两个位置中。
- 您可以在与控制器相同的 VNet 中运行应用程序池和 NSX Advanced Load Balancer SE。

正如拓扑中所述，DNS 虚拟机转发器组件有条件地将流量转发到 NSX Advanced Load Balancer DNS 虚拟服务或 Azure DNS，如上所述。

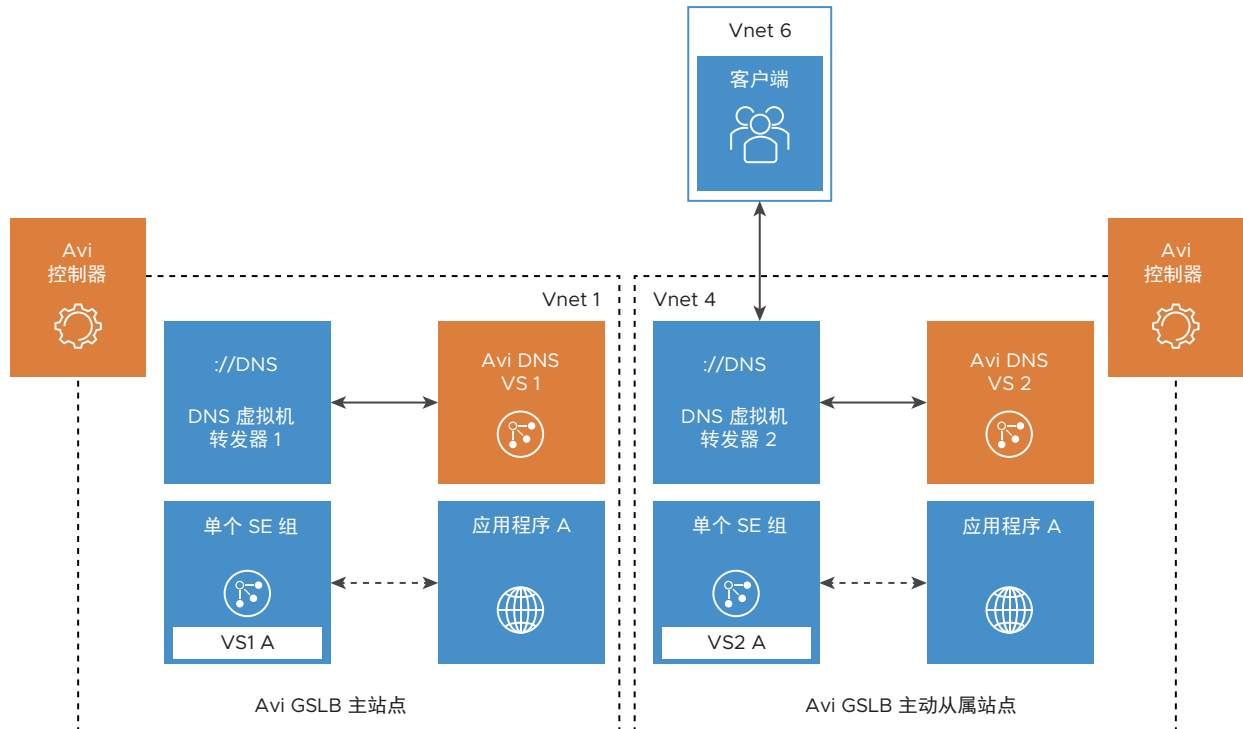
## 请求流

本节介绍了用于解析以下位置中托管的应用程序的请求流：

- 其他 VNet 之一
- 来自本地的 Azure VNet
- 不同虚拟网络中的虚拟机

## 从一个 VNet 中解析另一个 VNet 中托管的应用程序

本节介绍了如何从一个 VNet 中解析另一个 VNet 中托管的应用程序。



### FQDN 地址解析

- 1 位于本地的客户端希望访问应用程序 A。客户端发送 HTTPS 请求以下载应用程序 A 的主页。其 FQDN (A.gslb.azure.com) 需要映射到客户端（还）不知道的 IP 地址。
- 2 由于在企业 DNS 上为该子域配置的 DNS 服务器是 DNS 转发器 IP，因此，请求将传送到 DNS 转发器虚拟机以进行解析。然后，转发器虚拟机将请求转发到 NSX Advanced Load Balancer 的 DNS（两个 GSLB DNS 实例之一，此处为 DNS VS1），最终，将 A.azure.com 的 IP 返回到客户端。

### 应用程序流量传送到最佳虚拟服务

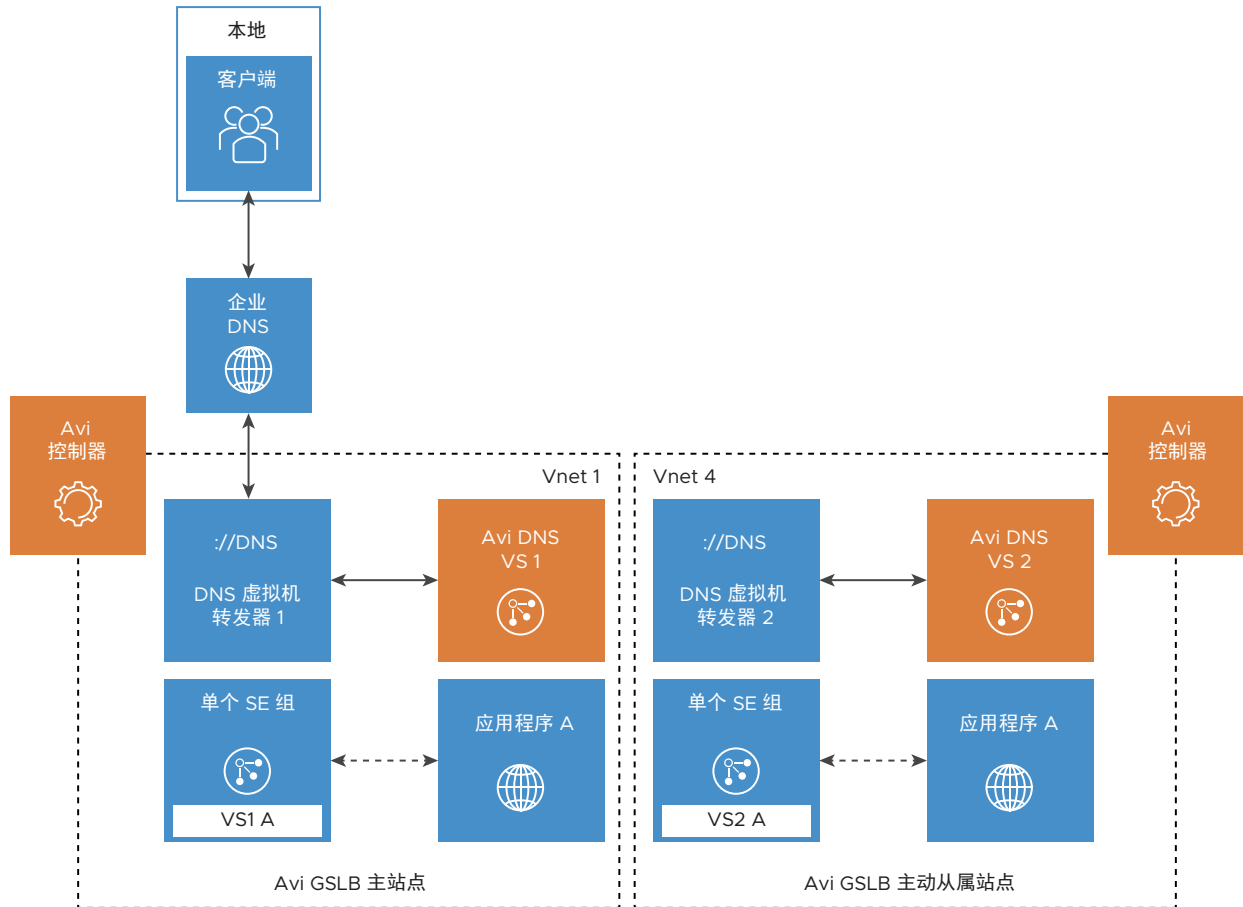
DNS-2 具有两个候选的最佳虚拟服务选项：VS1-A 和 VS2-A。它根据负载均衡算法、运行状况、客户端位置等选择了 VS2-A2。DNS-2 使用 VS2-A 的 VIP 响应 DNS 查询，最终将该 VIP 传送到原始客户端。客户端使用 VS2-A 的 VIP 发送其 HTTP 请求。

### 本地负载均衡

SE 接收已传送到 VS2-A 的 VIP 的请求。然后，它通过 VS2-A 的服务器（应用程序实例）之一对其进行负载均衡。VS2-A 直接响应客户端。

## 从本地解析 Azure VNet 中托管的应用程序

本节介绍了如何从本地解析 Azure VNet 中托管的应用程序。



### FQDN 地址解析

- 1 位于本地的客户端希望访问应用程序 A。客户端发送 HTTPS 请求以下载应用程序 A 的主页。其 FQDN (A.gslb.azure.com) 需要映射到客户端还不知道的 IP 地址。
- 2 由于在企业 DNS 上为该子域配置的 DNS 服务器是 DNS 转发器 IP，因此，请求将传送到 DNS 转发器虚拟机以进行解析。然后，转发器虚拟机将请求转发到 NSX Advanced Load Balancer 的 DNS（两个 GSLB DNS 实例之一，此处为 DNS VS1），最终，将 A.azure.com 的 IP 返回到客户端。

### 应用程序流量传送到最佳虚拟服务

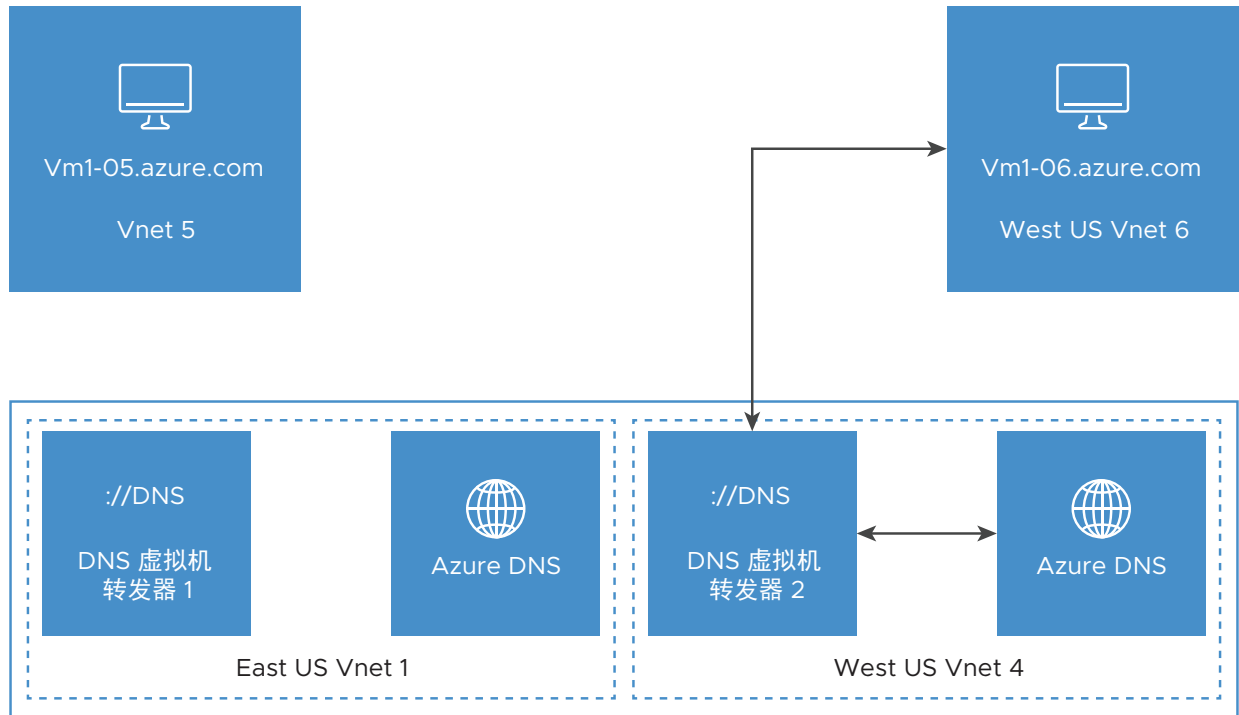
DNS VS1 具有两个候选的最佳虚拟服务选项：VS1 A 和 VS2 A。它根据负载均衡算法、运行状况、客户端位置等选择了 VS1 A。DNS VS1 使用 VS1 A 的 VIP 响应 DNS 查询，最终将该 VIP 传送到原始客户端。客户端使用 VS1 A 的 VIP 发送其 HTTP 请求。

### 本地负载均衡

SE 接收已传送到 VS1 A 的 VIP 的请求。然后，它通过 VS1 A 的两个服务器之一对其进行负载均衡。VS1 A 直接响应客户端。

## 不同虚拟网络中的虚拟机之间的名称解析

本节介绍了不同虚拟网络中的虚拟机之间的名称解析。



- 1 位于 West US Vnet 6 中的 VM1-06 需要与位于 Vnet 5 中的 VM1-05 进行通信以建立 SSH 连接。虚拟机的主机名需要映射到另一个虚拟机还不知道的 IP 地址。
- 2 由于为该 VNet 配置的 DNS 服务器是 DNS 转发器 IP，因此，请求将传送到 DNS 转发器虚拟机以进行解析，后者将请求转发到 Azure 专用 DNS（注册虚拟机的名称，如上一节中所述）。Azure DNS 将返回 VM1-05 的 IP。
- 3 VM1-06 将使用 VM1-05 的 IP 地址以建立 SSH 连接。

## 分析

NSX Advanced Load Balancer 包括具有企业级 GSLB 解决方案的内置应用程序分析。

该平台实时收集数百万个数据点，从而提供类似于网络 DVR 的功能和应用程序分析以帮助排除应用程序故障。在特定时间间隔（过去 15 分钟、上一小时、前一天、过去一周等）内显示的这种 DNS 分析提供有关来自客户端的 DNS 查询的详细和汇总信息，包括 FQDN、查询类型、严重错误和响应（IP 地址、CNAME、SRV）。

这也有助于检查在 Azure DNS 专用区域以及本地 DC 中的多个位置上部署的端点的运行状况。它还显示端点的 RTT、错误数和用户事务数，以实时提供有关您的网络的详细信息。